PROJETO DE GRADUAÇÃO

Decentralized Finance (DeFi): uma análise multicritério para tomada de decisão de investimento

Por
Daniel Veloso de Almeida

Brasília, 06 de maio de 2022

UNIVERSIDADE DE BRASÍLIA

FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA DE PRODUÇÃO

UNIVERSIDADE DE BRASÍLIA
Faculdade de Tecnologia
Departamento de Engenharia de Produção

PROJETO DE GRADUAÇÃO

DECENTRALIZED FINANCE (DeFi): UMA ANÁLISE MULTICRITÉRIO PARA TOMADA DE DECISÃO DE INVESTIMENTO

Por

Daniel Veloso de Almeida

Projeto de graduação submetido como requisito parcial para obtenção
do grau de Bacharel em Engenharia de Produção

Banca Examinadora

Prof. Dr. João Carlos Felix Souza, UnB/ EPR (Orientador) _____

Prof. Dr. Ricardo Fernandes Paixão, UnB/ EPR (Coorientador) _____

Prof. Msc. Ronan Damasco _____

Brasília, 06 de maio de 2022

Dedicatória

Dedico este trabalho aos meus pais, Adolfo Jorge de Almeida e Márcia Veloso de Almeida, por me ensinarem os princípios que são a base da minha vida e por sempre apoiarem as minhas escolhas. Muito obrigado por tudo!

Daniel Veloso de Almeida

Agradecimentos

À minha família, Adolfo Jorge, Márcia e Luccas Jorge, por sempre acreditarem em mim e estarem ao meu lado. Agradeço todos os dias por ter vocês na minha vida.

Aos meus avós, Dalila Veloso, Betty Almeida e Erasmo José de Almeida, um dos maiores engenheiros que já conheci.

À minha namorada, Manuela Dalpoz, que só tenho a agradecer por ser minha parceira em tudo e tornar os meus dias mais leves e felizes. Muito obrigado por sempre me incentivar e acreditar em mim.

Ao meu orientador, Ricardo Fernandes Paixão, por todo o conhecimento, suporte, paciência e amizade. Sou eternamente grato por tudo que você fez por mim.

Ao meu orientador, João Carlos Felix, por todos os ensinamentos, acompanhamento e apoio.

Ao meu grupo mais íntimo de amigos, André, Bernardo, Mateus Galuban, Ricardo, Filipe, Carlos, João Felipe, Lucas, Mateus Frota e Daniel. Vocês são amigos que levarei para a vida toda.

Aos meus colegas do LIFT, João Benício, Gabriel, Luciano, Roveré, Daniel Badra e demais.

À Daniela Prass, que tive muita sorte de errar na escolha do meu primeiro curso e ter te conhecido. Você é uma pessoa incrível e ser seu amigo é um privilégio. Muito obrigado por tudo.

Ao meu escritório, FdS Advogados, por todo o suporte, paciência e força. Obrigado Luis Gustavo, Edilene, Leandro, Júlia, Elisa, Fábio, Lara, Gabriely, Iago, Franklin, Sancler e Nikolly.

Aos meus colegas da Engenharia de Produção, Amanda Collusso, Victor, Pedro, Eduardo, Mateus Aristides, Túlio e Vinícius. Sem vocês nada disso seria possível. Muito obrigado.

À Universidade de Brasília, todos seus os professores, servidores e funcionários, por terem me acolhido e tanto me ensinado.

A todos que estiveram presentes em minha vida. Vocês são parte da minha história.

Daniel Veloso de Almeida.

RESUMO

O presente estudo objetiva realizar uma análise multicritério dos riscos presentes no ecossistema de finanças descentralizadas (*Decentralized Finance - DeFi*), de modo a fornecer insumos para tomada de decisão de investimento no setor. A análise partiu da revisão dos conceitos essenciais para compreensão da rede financeira descentralizada e, posteriormente, por meio de um experimento prático contemplando os principais protocolos desenvolvidos na rede DeFi, determinou-se os principais riscos existentes. Por fim, mediante a aplicação da ferramenta de Análise Hierárquica de Processos, foi possível determinar o grau de influência representado por cinco categorias de riscos elencados, são eles: risco de assimetria e fraudes, risco tecnológico-operacional, risco de governança, risco de integridade de mercado e risco regulatório. Nesse estudo, objetivou-se contextualizar o leitor sobre os principais aspectos constitutivos da rede financeira descentralizada, determinar parâmetros técnicos para decisão de investimento no setor e traçar um panorama do potencial disruptivo da tecnologia DeFi.

Palavras-chave:

Análise Multicritério; Análise Hierárquica de Processos; Avaliação de Projetos; Análise de Investimentos; Finanças descentralizadas, Blockchain, Sistema Financeiro.

ABSTRACT

The present study aims to perform a multi-criteria analysis of the risks inherent to the Decentralized Finance (DeFi) ecosystem, in order to provide inputs for investment decision-making in this sector. The analysis started from the review of the essential concepts for understanding the decentralized financial network and, later, through a practical experiment contemplating the main protocols developed in the DeFi network, the main existing risks were determined. Finally, through the application of the Hierarchical Process Analysis tool, it was possible to determine the degree of influence represented by five categories of risks listed, which are: risk of asymmetry and fraud, technological-operational risk, governance risk, integrity risk market and regulatory risk. In this study, the main goal was to contextualize the reader on the most relevant constitutive aspects of the decentralized financial network, as well as determine technical parameters for investment decisions in the sector and outline the disruptive potential of DeFi technology.

Key-Words:

Multicriteria Analysis; Analytic Hierarchy Process; Project Evaluation; Investment analysis; Decentralized Finance, Blockchain, Financial System.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE QUADROS

LISTA DE GRÁFICOS

1. INTRODUÇÃO

1.1. Contextualização

Com o passar das últimas décadas, a grande maioria dos setores da indústria adaptou seus modelos de negócio para uma estrutura mais eficiente baseada em inovações tecnológicas, exceto o mercado financeiro. Thomas Phillippon (2016) descreve este fenômeno como um enigma, levando em consideração que o setor financeiro, historicamente, sempre foi responsável por um custo operacional elevado em relação ao PIB norte-americano.

Assim, mesmo com os recentes avanços tecnológicos, principalmente relacionados aos sistemas de pagamentos, as barreiras de infraestrutura e regulação do mercado financeiro persistem em moldar a operação financeira tradicional. Referenciando o exemplo de Matt Hougan[1], uma transferência internacional por meio de uma das plataformas mais populares de envio de recursos custava, em 2021, aproximadamente quatro vezes mais do que no ano de 1873.

Com os ganhos exorbitantes e estruturas opacas das instituições financeiras, além do suporte governamental em decorrência da crise de 2008 e a ineficiência ao consumidor final, o criticismo sobre o sistema financeiro tradicional ganhou tração, impulsionando o surgimento de uma nova proposta de sistema monetário e de pagamentos: o Bitcoin.

Inaugurando a utilização de uma rede descentralizada de registros de transações de transferência de valor (*blockchain*), o Bitcoin representa um importante marco temporal sobre a forma de realização de operações financeiras. A ideia de uma rede sem intermediários mediada por algoritmos matemáticos de verificação questionou a dependência de instituições financeiras e reguladores, abrindo espaço para um novo horizonte de desenvolvimento tecnológico.

Logo, novos projetos de redes descentralizadas surgiram, como a Ethereum, Solana e Cardano. Em destaque, a Ethereum, desenvolvida pelo russo-canadense Vitalik Buterin (2014), introduziu uma rede descentralizada que permitiu o processamento de qualquer tipo de transferência de valor utilizando algoritmos conhecidos como *smart contracts* (contratos inteligentes). Assim, esses contratos possibilitaram a criação de novas funcionalidades, como *tokens* e criptomoedas, dentro da própria rede, sem necessidade de criar uma infraestrutura *blockchain* específica (VOSHMGIR, 2020).

Nesse sentido, investimentos em cripto passaram a representar um crescimento significativo e retornos atrativos. Bancos, gestoras e empresas manifestam crescente interesse na inclusão de criptoativos no rol de serviços. A título de exemplo, podemos citar o início da operação da Mastercard

[1] HOUGAN, Matt. Fintech Is A Colossal Disappointment. DeFi Fixes It. **Forbes**, Oct 12, 2021. Crypto & Blockchain. Disponível em: https://www.forbes.com/sites/matthougan/2021/10/12/fintech-is-a-colossal-disappointment-defi-fixes-it/. Acesso em: 27 de abril de 2022.

com criptoativos[2], bem como a *big tech* de pagamentos Paypal[3]e uma das maiores instituições financeiras dos Estados Unidos, o JPMorgan[4].

A oferta de investimentos em criptoativos também alcançou ao investidor individual no setor financeiro tradicional por meio de fundos de índice e fundos de investimento multimercado, como aqueles ofertados pela gestora Hashdex[5].

Dentre os diversos novos setores inaugurados pelos criptoativos, a rede Ethereum deu início a um novo ecossistema financeiro: a rede DeFi, ou, em português, as finanças descentralizadas.

Segundo relatório elaborado pela Organização para Cooperação e Desenvolvimento Econômico (OCDE, 2022), podemos definir DeFi como "uma tentativa de replicar certas funções do sistema financeiro tradicional de forma aberta, descentralizada e autônoma, com base em redes *blockchains*".

O setor demonstra um crescimento significativo, apresentando um volume de valor depositado (chamado de TVL – *Total Value Locked*) superior a 200 bilhões de dólares americanos, em março de 2022.[6]

Contudo, em razão do desconhecimento geral sobre a estrutura de funcionamento, do alto índice de golpes e da falta de informação sobre riscos inerentes ao ecossistema, ainda há muita incerteza sobre o potencial de investimento no setor, em especial em DeFi.

1.2. Objetivo geral

O objetivo geral do presente trabalho é definir, sob o prisma de análise de um gestor de carteiras de investimentos, a viabilidade de alocação de recursos no setor de finanças descentralizadas (DeFi), com base nos resultados obtidos em um experimento prático dos protocolos mais comuns na rede e na análise multicritério dos riscos identificados.

1.3. Objetivos específicos

São objetivos específicos do trabalho desenvolvido:

- Descrever os elementos constitutivos de uma rede de finanças descentralizadas e suas relações;
- Analisar os custos operacionais, a usabilidade e os limites das operações mais comuns da rede DeFi;
- Contextualizar o potencial disruptivo da tecnologia no setor financeiro e
- Analisar, sob a ótica de um gestor de carteiras de investimentos, a viabilidade de alocação de recursos para diversificação de investimentos no setor de finanças

[2] Disponível em: https://cointelegraph.com.br/news/mastercard-expands-consulting-with-crypto-dedicated-practices. Acesso em: 27 de abril de 2022.
[3] Disponível em: https://exame.com/future-of-money/paypal-sobe-investimentos-em-blockchain-e-quer-lancar-criptomoeda-propria/. Acesso em: 27 de abril de 2022.
[4] Disponível em: https://www.jpmorgan.com/solutions/cib/news/digital-coin-payments. Acesso em: 27 de abril de 2022.
[5] Disponível em: https://www.hashdex.com.br/indices/nci. Acesso em: 27 de abril de 2022.
[6] Disponível em: https://defillama.com/. Acesso em: 27 de abril de 2022.

descentralizadas, com base nos riscos elencados, categorizados e priorizados de acordo com a metodologia do Processo Analítico Hierárquico.

1.4. Organização do trabalho

Na primeira parte do trabalho, disposta no primeiro capítulo, procura-se, por meio de uma análise de eventos relevantes, contextualizar o leitor sobre o surgimento do movimento de descentralização no mercado financeiro.

Já o segundo capítulo propõe realizar uma descrição da metodologia abordada no projeto que consiste, sinteticamente, em delimitar um referencial teórico com base nos conceitos levantados no processo de revisão da bibliografia, realizar um experimento prático para compreender os riscos do ecossistema e, por fim, aplicar o método de análise multicritério AHP para categorizar os riscos ao final do trabalho, de modo a nortear a decisão final de investimento.

O terceiro capítulo procura aprofundar na temática do surgimento de criptoativos, descrever o funcionamento do ecossistema DeFi e realizar uma análise geral de conceitos relevantes para o estudo. Dentre os temas abordados, destaca-se a infraestrutura *blockchain*, *wallets, smart contracts, DApps, tokens* e *Decentralized Autonomous Organizations* (DAO´s).

O quarto capítulo propõe a realização de um experimento prático dentro da rede DeFi, contemplando operações de *swap,* provimento de liquidez, *staking* e empréstimos. O experimento objetiva a observação de riscos presentes no arranjo, de modo a fornecer insumos para a análise de multicritério.

Finalmente, no quinto capítulo é realizada aplicação da metodologia de análise multicritério para os riscos elencados e exemplificados. Com o resultado obtido por meio da priorização dos riscos, será, também, realizada a tomada de decisão de alocação de investimento, conforme disposto no capítulo anterior.

2. METODOLOGIA

A metodologia utilizada no presente trabalho foi desenvolvida com base em três principais fases, são elas: (i) a revisão do histórico, conceitos e estruturas descritos na bibliografia e referências suplementares, (ii) a realização de um experimento prático para compreensão dos protocolos da rede financeira descentralizada e (iii) a aplicação do método de análise multicritério baseado nos riscos elencados para determinar a alocação de recursos da carteira de investimentos gerenciada.

A primeira fase procurou delimitar o objeto de estudo, caracterizando o histórico de desenvolvimento da rede de finanças descentralizadas e os seus elementos constitutivos. Assim, foi possível compreender os motivos que impulsionaram o desenvolvimento do DeFi e estabelecer um referencial teórico para balizar a decisão de alocação de investimento.

Posteriormente, foi realizado um experimento prático com a alocação de R$ 1.000 (mil reais) na rede DeFi, de modo a compreender os protocolos mais comuns na rede e as suas respectivas estruturas de funcionamento, além de identificar vulnerabilidades, riscos e eventual potencial de retorno.

Com os resultados obtidos por meio do experimento prático, adotou a metodologia de análise multicritério para a tomada de decisão de investimento, de modo que o gestor de carteira de investimentos foi responsável por mensurar e categorizar os riscos elencados.

Por fim, delimitou a tomada de decisão de investimento com base na categorização dos riscos e nos aprendizados obtidos por meio do experimento prático.

2.1. Análise multicritério e o Processo Analítico Hierárquico (AHP)

Segundo Greco *et al*. (2016), a metodologia MCDA (*Multiple Criteria Decision Analysis*) é, além de um compilado de teorias, metodologias e técnicas, uma perspectiva para lidar com a tomada de decisão. Montibeller & Franco (2010) afirmam que a utilização de métodos de análise multicritério, por meio da estruturação e ponderação de riscos, pode favorecer a tomada de decisões estratégicas.

Dentre os vários métodos utilizados para a análise multicritério, destaca-se o Processo Analítico Hierárquico (AHP), proposto do Saaty em 1971, que, de acordo com o proponente (1987), é uma teoria geral de mensuração utilizada para derivar escalas de razão comparativas discretas e contínuas por meio da comparação entre pares.

O método AHP pode resumir-se em quatro principais etapas: (i) decomposição dos critérios em uma estrutura hierárquica; (ii) realização de comparação entre os critérios hierarquicamente iguais; (iii) aplicação da normalização aos valores obtidos por meio das classificações dos riscos; (iv) aplicação da análise de inconsistência.

A primeira etapa parte da definição de uma decisão a ser tomada, seguido pelas forças (critérios) que podem influenciar essa decisão, e, por fim, as possibilidades decisórias (sendo a última não obrigatória). Assim, segundo Pimenta *et al*. (2019), é possível organizar as percepções, julgamentos e informações dos fatores que atuam sobre o processo de decisão.

Saaty (1987), estabelece uma escala absoluta (de 1 a 9) para a determinação da intensidade dos pesos atribuídos aos critérios selecionados, vejamos:

Tabela 1: Adaptação da escala fundamental de Saaty (1987)

Intensidade da importância da escala absoluta	**Definição**	**Justificativa**
1	Igual importância	Os dois critérios contribuem da mesma forma para o objetivo.
3	Importância moderada de um sobre o outro fator	Julgamento e experiência favorecendo fortemente um critério sobre o outro.
5	Essencial ou forte importância	Julgamento e experiência favorecendo fortemente um critério sobre o outro.
7	Importância muito forte	Um critério é fortemente favorecido e sua dominância é demonstrada na prática.
9	Importância Extrema	Evidência favorecendo um critério sobre o outro, é a mais expressiva possível na ordem de afirmação.
2, 4, 6, 8	Valores intermediários entre os julgamentos adjacentes	Quando há necessidade de compromisso.

Fonte: Saaty (1987) (adaptado)

Conforme descrito por Pimenta *et al*. (2019), na intenção de afastar dificuldades relacionadas aos erros de mensuração dos atributos, ambiguidades e eventual parcialidade na decisão, alguns estudos adotam uma escala de importância relativa, em que o julgador determina uma importância relativa entre os critérios analisados. A comparação utilizada pode ser sintetizada da seguinte forma:

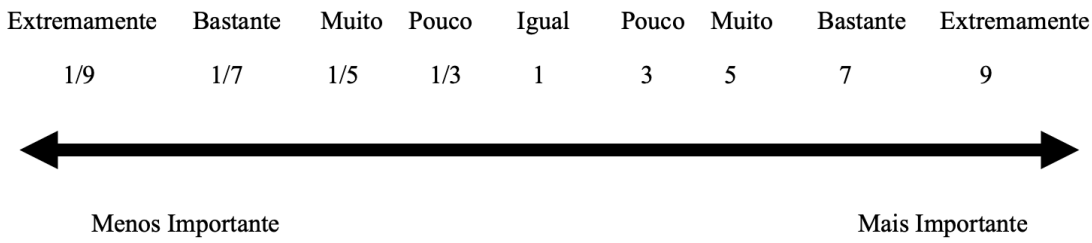

Figura 1: Escala relativa de classificação par a par

Fonte: Pimenta *et al*. (2019).

Posteriormente, é realizada a comparação entre os critérios conforme a escala acima e os respectivos pesos atribuídos de acordo com seu grau de importância. Santos *et al*. (2010) destacam que essa matriz é quadrada e com valores recíprocos, sendo que os valores da diagonal são unitários.

Em seguida, realiza-se o processo de normalização, em que os valores elencados nas matrizes são divididos pelo somatório da coluna em questão. Assim, resultam os valores normalizados de cada fator ponderante.

De acordo com Marins (2006), na intenção de evitar contradições nos resultados comparativos, também é necessário realizar a verificação de consistências dos resultados obtidos.

O primeiro passo é realizar o cálculo da média aritmética dos resultados de cada linha, resultando no vetor prioridade (*w*). Assim, com o resultado, é realizada a soma do produto de cada valor de cada linha da matriz de comparação pela respectiva prioridade correspondente. Então, dividem-se os valores encontrados em cada vetor pela prioridade da alternativa que corresponde (vetor de prioridade). Com os resultados, obtemos o λmax, resultado da média ponderada obtida para cada linha. Merece destaque que o λmax deve ser próximo ao número de critérios utilizados.

Conforme aponta Rezende *et al*. (2017), deve-se, então, realizar o cálculo do Índice de Consistência (IC) por meio da seguinte equação:

$$IC = \frac{\lambda_{max} - n}{(n-1)} \qquad (1)$$

Nesse sentido, deve calcular a Razão de Consistência (RC), a depender do Índice Randômico (IR) descrito por Saaty (1980), que é condicionado ao número de critérios utilizados na análise, senão vejamos:

Tabela 2: Valores de IR em relação ao número de critérios utilizados

Número de Critérios	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
Índice Randômico	**0**	**0**	**0,52**	**0,89**	**1,11**	**1,25**	**1,35**	**1,40**	**1,45**	**1,49**

Fonte: Saaty (1980) (adaptada).

Por fim, com os resultados, basta realizar a divisão entre os valores de IC e IR para obtenção do RC. Segundo Saaty (1987), para que os dados sejam consistentes, a Razão de Consistência deve ser inferior a 10% (dez por cento).

Assim, garantida a confiabilidade dos resultados, os riscos devem ser priorizados e analisados para determinação da tomada de decisão final.

3. FUNDAMENTAÇÃO TEÓRICA

3.1. A crise de confiança no sistema financeiro tradicional

O final do ano de 2008 foi marcado pela perda de um dos mais importantes ativos da economia: a confiança. Segundo Sapienza & Zingales (2012), mesmo não mensurada nas estatísticas e modelos econômicos padrões, a confiança é crucial para o desenvolvimento, e sua ausência é a causa de grande parte do retrocesso econômico no mundo.

Nesse sentido, é importante esclarecer sobre um dos eventos mais marcantes do mercado financeiro no século XXI, a crise financeira do *subprime*. Tal crise de 2008 foi essencialmente ocasionada por falta de liquidez no mercado, em decorrência da alavancagem excessiva no setor imobiliário por meio de diversas garantias (hipotecas) sobre os mesmos imóveis, sob o fundamento de uma especulação no aumento do preço dos imóveis. Contudo, a verdadeira raiz do problema da crise estava na estrutura disfuncional de securitização de ativos de risco instaurada no mercado financeiro.

O início dos nos 2000 nos EUA foi marcado por um período de estabilidade, rápido crescimento econômico, baixa taxa de juros e inflação, impulsionando o mercado de acesso ao crédito. Assim, os direitos de recebimento das hipotecas, modalidade de crédito da qual o imóvel é dado em garantia por um empréstimo bancário, eram considerados títulos com nível de segurança elevada.

Ocorre que as instituições financeiras, restritas ao potencial de alavancagem por barreiras regulatórias, desenvolveram produtos financeiros envelopando os direitos creditórios relativos às hipotecas. Os produtos, denominados CDO´s (*Colletarized Debt Obligations*), eram vendidos de forma agressiva a investidores de todas as partes do mundo, se tornando, inclusive, uma grande fatia do mercado de *asset-backed securities* (ABS).

Assim, os CDO´s, aliviando a razão entre o valor de empréstimos concedidos pelos bancos sobre o total dos depósitos realizados, viabilizaram uma alavancagem estrutural do setor financeiro como um todo.

Segundo Mehrling (2010), esses pacotes de empréstimos eram categorizados conforme o grau de risco, de modo que apenas a parcela com classificação mais alta (títulos *prime*) era mantida e financiada pelos bancos (também chamados, no caso, de *shadow banks)* por meio de fundos *money-market.* Já a parcela de títulos com alto risco foi projetada para ser mantida por fundos de pensão, fundos de *hedge* e, em especial, seguradoras. Merece destaque que os CDO´s de alto risco eram financiados pelos próprios passivos das empresas seguradoras, não sendo demandantes, portanto, de liquidez de financiamento, mas, sim, de liquidez de mercado.

Como forma de alavancar ainda mais a estrutura desenvolvida, as instituições financeiras passaram a fornecer acesso ao crédito sem necessidade de comprovação de renda e realizar o mesmo procedimento de envelopar garantias de crédito para revenda no mercado, mas, agora, sendo títulos com grau de risco maior, chamados títulos *subprime.*

A fonte de liquidez de mercado (consequentemente, o preço) para os títulos de alto risco estava na negociação de títulos de seguro do inadimplemento das hipotecas contidas nos CDO´s, chamados de

Credit Default Swap (CDS), estes negociados e até mantidos, novamente, pelos próprios bancos de investimento (MEHRLING, 2010).

A *default,* ou seja, o calote na dívida pelos devedores da hipoteca, ocasionou um rompimento sistêmico do complexo arranjo, de forma que o valor dos imóveis passou a diminuir e, com a frágil base oriunda dos fundos de curto prazo *money-market* para o financiamento de títulos de longo prazo (hipotecas), os títulos (CDO´s e CDS´s) passaram a perder valor.

Com a diminuição de valor dos títulos, um grande pânico instalou-se no mercado financeiro mundial. A corrida por saques iniciou um movimento de desconfiança que culminou na decretação de falência de um dos maiores bancos de investimentos dos EUA, o *Lehman Brothers*.

Com o colapso do *Lehman* e de outras instituições, como a seguradora AIG, os EUA e a economia mundial entraram em recessão acelerada, sendo motivada pela perda de confiança no setor financeiro e no sistema econômico em geral (SAPIENZA & ZINGALES, 2012).

Em 16 de setembro, o FED (*Federal Reserve*) anunciou o resgate da AIG por 85 bilhões de dólares. O suporte governamental total chegou na margem de 700 bilhões de dólares. Curiosamente, menos de um ano depois, a AIG anunciou o pagamento de 165 milhões de dólares em bônus para executivos.

Além do governo dos EUA, outros países ofereceram pacotes de suporte aos bancos em resposta à crise financeira, como o caso de governo britânico, que injetou aproximadamente 850 bilhões de dólares[7].

O colapso econômico, além de questionar o grau de confiança na estabilidade do sistema financeiro, colocou em pauta a confiança nas instituições governamentais, conforme aponta Uslaner (2010). Com isso, diante do cenário de criticismo em face da governança monetária e da transferência de dinheiro governamental para salvar instituições financeiras, o Bitcoin surgiu.

A criptomoeda, descrita com mais detalhes na próxima subseção, inaugurou a primeira transação da rede reproduzindo a manchete de um dos jornais de maior circulação nos Reino Unido: “Chanceler à beira do segundo resgate para bancos”.

[7] Disponível em: http://news.bbc.co.uk/2/hi/business/7658277.stm. Acesso em: 27 de abril de 2022.

THE TIMES

Saturday January 3 2009 timesonline.co.uk No 69521 £1.50

Eat Out from £5

More than 900 great restaurants, including four Gordon Ramsay favourites from £15

Start collecting tokens today. Pullout inside

Israel prepares to send tanks and troops into Gaza

Michael Sheen Frost, Nixon and me

Working mums So that's how she does it

Detox in style The best spas on the planet

Salman Rushdie I won't marry again

Giant killing? Guide to the FA Cup third round

Chancellor on brink of second bailout for banks

Billions may be needed as lending squeeze tightens

99p

Figura 2: Capa do Jornal The Times

Fonte: The Times

```
00000000   01 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   ................
00000010   00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   ................
00000020   00 00 00 00 3B A3 ED FD   7A 7B 12 B2 7A C7 2C 3E   ....;£íýz{.²zÇ,>
00000030   67 76 8F 61 7F C8 1B C3   88 8A 51 32 3A 9F B8 AA   gv.a.È.Ã^ŠQ2:Ÿ¸ª
00000040   4B 1E 5E 4A 29 AB 5F 49   FF FF 00 1D 1D AC 2B 7C   K.^J)«_Iÿÿ...¬+|
00000050   01 01 00 00 00 01 00 00   00 00 00 00 00 00 00 00   ................
00000060   00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   ................
00000070   00 00 00 00 00 00 FF FF   FF FF 4D 04 FF FF 00 1D   ......ÿÿÿÿM.ÿÿ..
00000080   01 04 45 54 68 65 20 54   69 6D 65 73 20 30 33 2F   ..EThe Times 03/
00000090   4A 61 6E 2F 32 30 30 39   20 43 68 61 6E 63 65 6C   Jan/2009 Chancel
000000A0   6C 6F 72 20 6F 6E 20 62   72 69 6E 6B 20 6F 66 20   lor on brink of
000000B0   73 65 63 6F 6E 64 20 62   61 69 6C 6F 75 74 20 66   second bailout f
000000C0   6F 72 20 62 61 6E 6B 73   FF FF FF FF 01 00 F2 05   or banksÿÿÿÿ..ò.
000000D0   2A 01 00 00 00 43 41 04   67 8A FD B0 FE 55 48 27   *....CA.gŠý°þUH'
000000E0   19 67 F1 A6 71 30 B7 10   5C D6 A8 28 E0 39 09 A6   .gñ¦q0·.\Ö¨(à9.¦
000000F0   79 62 E0 EA 1F 61 DE B6   49 F6 BC 3F 4C EF 38 C4   ybàê.aÞ¶Iö¼?Lï8Ä
00000100   F3 55 04 E5 1E C1 12 DE   5C 38 4D F7 BA 0B 8D 57   óU.å.Á.Þ\8M÷º..W
00000110   8A 4C 70 2B 6B F1 1D 5F   AC 00 00 00 00            ŠLp+kñ._¬....
```

Figura 3: Primeiro bloco de transações do Bitcoin

Fonte: Bloco gênesis do Bitcoin

Além de inaugurar o conceito de ativo digital, o Bitcoin representou um marco temporal em relação à crítica sobre o sistema financeiro tradicional e colocou a descentralização como pauta de discussões dos mais diversos setores.

3.1.1. Bitcoin

Em 2008, por uma ou mais pessoas sob o pseudônimo Satoshi Nakamoto, foi publicado o *white paper* do Bitcoin, descrevendo a criação de uma moeda digital baseada em um protocolo descentralizado de registro de estados com garantia de segurança baseada em um algoritmo matemático.

De acordo com Nakamoto (2008), o Bitcoin é uma moeda digital capaz de permitir transações *peer-to-peer* (*P2P*), ou seja, entre duas partes, sem a necessidade de intermediários confiáveis para

processar as operações. Assim, por meio de um registro na rede *blockchain,* é solucionada a questão do *double-spending,* qual seja a necessidade de garantir irreversibilidade da transição de estados e, consequentemente, a impossibilidade de utilização da mesma moeda para diferentes transações. O conceito de *blockchain* pode ser encontrado na subseção 3.3.1.

O Bitcoin também viabilizou a solução de um antigo problema criptográfico: o problema dos generais bizantinos. Tal questão pode ser resumida com a analogia da teoria dos jogos, em que vários generais objetivam realizar uma invasão a uma cidade, porém, para que o ataque seja bem-sucedido, devem decidir realizar um ataque conjunto, mesmo sem comunicação entre eles. Então, deve o leitor indagar-se: como os generais deveriam então se organizar?

No caso específico da moeda, o problema mencionado se aplica para a hipótese de aceitação da veracidade da transação e do ativo, tendo em vista que a sociedade precisaria de um ativo universalmente aceito e confiável. No sistema financeiro tradicional, esse papel é ocupado pelos governos, entidades centralizadoras que garantem a moeda fiduciária.

Pensemos agora na hipótese descentralizada, em que não há uma moeda universal e não há uma entidade centralizadora que poderia garantir a veracidade dessa moeda, como isso seria possível?

A garantia de consenso da rede descentralizada pelo algoritmo *Proof of Work* é capaz de solucionar tal problemática, na medida que é estabelecida uma série de regras e objetivos para inclusão de determinado bloco de transações na cadeia de registros, a *blockchain*. Os registradores das transações, denominados mineradores, são remunerados com base em uma taxa de mineração fixa e regressiva com períodos determinados (6,25 BTC até 2024).

Assim, leciona Zaghloul *et al*. (2020) sobre o processo de validação das transações na rede, também chamado de mineração de blocos:

> Os mineradores começam selecionando transações de seus pools de transações que serão colocadas em um bloco onde um bloco não pode exceder 1 MB de tamanho. Uma pequena parte desse espaço é especificada para transportar transações de alta prioridade. A prioridade é baseada no tamanho e na idade das entradas da transação. O resto do bloco é preenchido com outras transações que possuem taxas de transação maiores para maximizar o lucro que um minerador pode obter se conseguir minerar o bloco primeiro. Uma transação com taxas baixas ou sem taxas provavelmente permanecerá no pool de transações do minerador até envelhecer e se tornar uma transação de alta prioridade.
>
> Em seguida, o minerador monta uma transação especial, conhecida como transação *coinbase*. Esta transação é uma transação de pagamento de recompensa ao minerador no caso de vencer uma competição de mineração. Ele não possui entradas e consiste em uma única saída endereçada à carteira do minerador. O valor incorporado na saída é a taxa de mineração de recompensa (12,5 BTC no momento da redação) mais a soma de todas as taxas de transação incluídas em cada transação.
>
> Todas as transações selecionadas junto com a transação *coinbase* são então combinadas em uma árvore Merkle conforme discutido anteriormente. Neste ponto, o minerador tem todos os componentes necessários para construir o cabeçalho do bloco do novo bloco, exceto o nonce. O nonce é um valor que, se concatenado com o cabeçalho do bloco do grupo de transações escolhidas e, em seguida, com *hash* duplo, produz um resumo com um prefixo específico de zeros em sua representação binária. A busca por este valor é realizada de forma bruta e está diretamente correlacionada com o poder computacional disponível. Quanto mais poder computacional disponível, mais rápido um minerador é capaz de encontrar o nonce correto. Um minerador bem-sucedido transmitirá sua prova de trabalho para provar que consumiu recursos

> computacionais para encontrar o nonce correto (ZAGHLOUL *et al*., 2020. Grifos do autor).

Nakamoto (2008) aponta que o algoritmo PoW é capaz de solucionar o problema da determinação de representação da maioria, levando em consideração que a decisão é sempre representada pela cadeia mais longa de transações, ou seja, aquela que tem o maior esforço computacional nela investido. Assim, se a *blockchain* é controlada por agentes honestos, a rede de nós honestos sempre crescerá mais rápida.

Deste modo, para que um agente malicioso altere qualquer registro na *blockchain*, ele deve refazer a validação do nó atual e de todos os nós anteriores previamente à validação do próximo bloco. Logo, a probabilidade de ataque diminui exponencialmente com a inserção de novos blocos na rede *blockchain*.

Em resumo, o Bitcoin representou uma das maiores inovações no contexto financeiro: a criação de um ativo digital seguro e transparente. A aplicação da tecnologia *blockchain* para a transferência de valores deu origem ao desenvolvimento de diversos novos protocolos e criptomoedas que, conjuntamente, originaram o objeto do presente estudo, as finanças descentralizadas.

3.2. *Decentralized Finance* (DeFi)

Inspirado em aprimorar o protocolo Bitcoin, a Ethereum (BUTERIN, 2014), rede *blockchain touring complete*, ou seja, capaz de ler e executar contratos inteligentes, viabilizou o surgimento de um novo ecossistema: as finanças descentralizadas. A rede *Decentralized Finance*, ou DeFi, pode ser definida com uma transformação de produtos financeiros do mercado financeiro tradicional em modelos que operam sem a necessidade de agentes intermediários por meio de contratos inteligentes tipicamente em determinadas redes *blockchain* (MEEGAN & KOENS, 2021).

Até a data de defesa do presente trabalho, o ecossistema DeFi registrava um valor de depósito (TVL – *Total Value Locked*) de aproximadamente 212 bilhões de dólares, apontando um crescimento superior a 900% em apenas um ano.

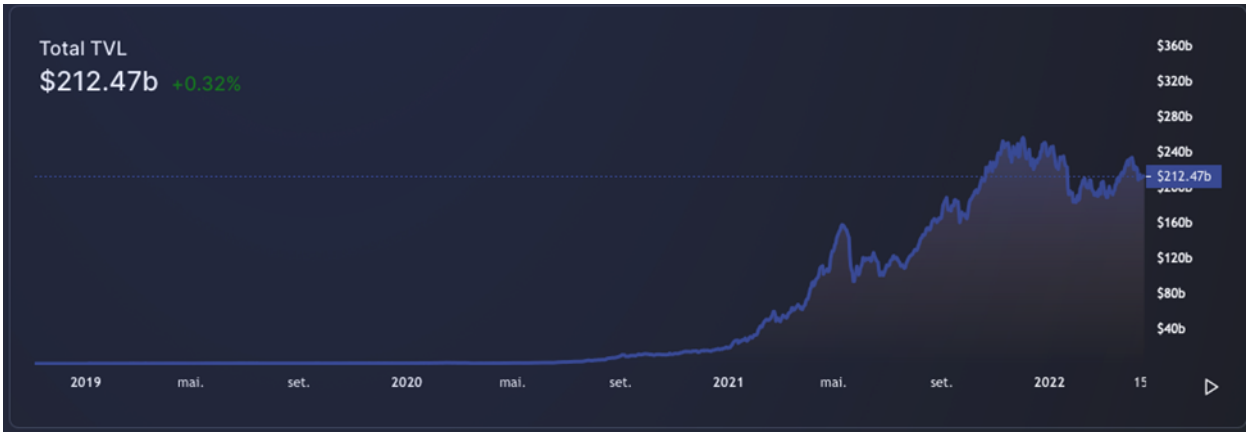

Figura 4: TVL da rede DeFi (abril de 2022)

Fonte: DeFillama.

Além da promessa de descentralização também proposta pelo Bitcoin, a rede de finanças descentralizadas surgiu com o propósito de garantir um sistema financeiro imutável e altamente interoperável, assegurando transparência e acessibilidade.

Os projetos, ou, como normalmente são chamados, protocolos que desenvolvem produtos financeiros, são diversos, a incluir *exchanges,* plataformas de empréstimos, derivativos, dentre outros produtos exclusivos do ecossistema.

A rede DeFi é estruturada sob uma arquitetura multicamadas, em que cada camada é modular e possui um propósito específico, i.e., garante a interoperabilidade entre os mais diversos protocolos e serviços financeiros. Desse modo, a estrutura desenhada sob o formato de módulos faz com que a rede seja um verdadeiro "lego financeiro" (VOSHMGIR, 2020).

A possibilidade de integração e dependência entre as camadas é objeto do trabalho desenvolvido por Schär (2021), que também propõe um *framework* de organização da rede DeFi em cinco camadas: liquidação, ativos, protocolo, aplicação e integração.

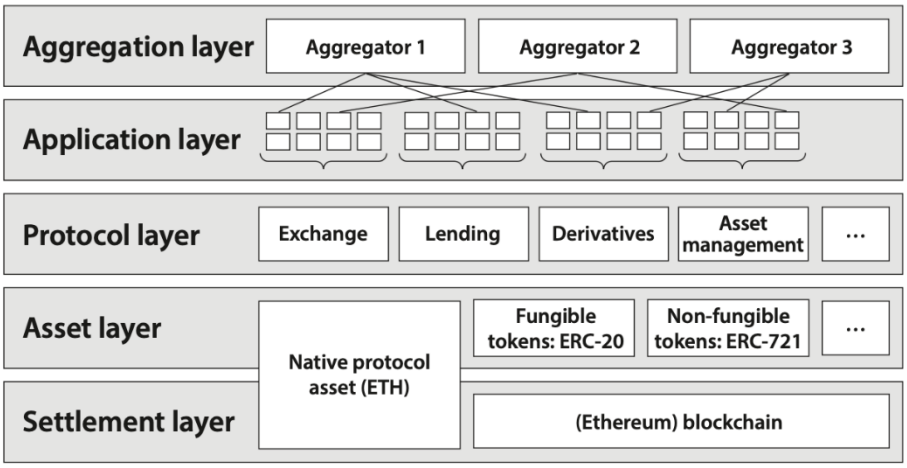

Figura 5: Camadas da rede DeFi

Fonte: Schär (2021).

A primeira camada, a camada de liquidação (*settlement layer)*, é a estrutura base de todas as atividades no sistema DeFi, que consiste na *blockchain* e seu *token* nativo dos protocolos, como a Ethereum e o *token* ETH.

A segunda camada (*asset layer)* refere-se a todos os ativos que são garantidos no topo da camada de liquidação, incluindo os ativos próprios da rede. Nessa categoria enquadram-se os *tokens* padrão (ERC-20), *tokens* não-fungíveis (ERC-721), dentre outros novos padrões em desenvolvimento.

Já a terceira camada (*protocol layer)* representa as funcionalidades existentes no ecossistema DeFi, incluindo, mas não se limitando a *Exchanges*, plataformas de empréstimo, derivativos e outros. Em razão dos protocolos serem desenvolvidos sob *smart contracts* modulares, essa camada possui um alto grau de interoperabilidade.

A quarta camada (*application layer)* é caracterizada pela simplificação de acesso ao usuário final por meio do desenvolvimento de interfaces intuitivas e acessíveis. Em geral, podemos observar a existência da quarta camada em páginas *web* de protocolos.

Por fim, a quinta camada (*aggregation layer)* é uma extensão da camada anterior, sendo responsável por conectar diversas aplicações como mecanismo de conveniência ao usuário final. Dentre os aplicativos dentro desta camada, podemos citar os agregadores de *Exchange*[8] e os aplicativos de otimização de estratégia.

Realizada breve contextualização sobre o universo DeFi, é incontroverso o potencial disruptivo do ecossistema, tendo em vista a facilidade para desenvolver e replicar produtos financeiros sob a forma de algoritmos. Contudo, é fundamental atentar-se aos riscos e compreender as barreiras operacionais e regulatórias que ainda impedem a rede de tornar-se amplamente difundida, conforme exposto nos tópicos subsequentes.

3.3. Conceitos essenciais

Para compreender os aspectos técnicos do experimento realizado, bem como tornar mais claro e acessível o ecossistema de criptoativos e das finanças descentralizadas, o presente subcapítulo objetiva estabelecer os conceitos relevantes com base na bibliografia levantada.

3.3.1. *Blockchain*

Dentre as *Distribuited Ledger Technologies (DLT´s)*[9], a *blockchain,* pilar estrutural do desenvolvimento do Bitcoin, se destaca como uma das aplicações com maior relevância no contexto de finanças descentralizadas. Apesar de comumente os termos DLT´s e *blockchain* serem adotados como sinônimos, é importante destacar que esta é uma espécie daquelas.

Segundo Natarajan *et al*. (2017), uma *blockchain* trata-se de uma estrutura de dados conjugada com criptografia e algoritmos de registro de dados que transmite dados por meio de pacotes chamados "blocos" conectados em uma espécie de "corrente" virtual. Nesse sentido, o desenvolvimento de uma rede *blockchain* pressupõe o cumprimento de três principais propriedades: descentralização, transparência e segurança (TASCA *et al*., 2017).

A descentralização refere-se à própria natureza da rede, de modo que os integrantes (também chamado de nós) podem interagir diretamente, sem a necessidade de um agente intermediário para a verificar a veracidade das transações realizadas[10].

Com relação à transparência, todas as transações realizadas em uma *blockchain* são auditáveis, i.e., são registradas na cadeia de blocos, sendo possível a análise por todos que possuem acesso. Sendo assim, todos os registros são transparentes e rastreáveis.

[8] Disponível em: https://furucombo.app/combo. Acesso em: 27 de abril de 2022.
[9] DLT´s referem-se a um conjunto de formas de gravar e compartilhar dados por meio de diversos servidores de armazenamento (*ledgers).* Essa tecnologia viabiliza transações de dados, bem como o seu registro, compartilhamento e sincronização por determinada rede distribuída formada por diferentes participantes (NATARAJAN *et al*., 2017).
[10] Alguns modelos de *blockchains*, como as *blockchains* privadas, são deixados de lado.

Já a segurança diz respeito, essencialmente, ao princípio da imutabilidade da rede. A principal função de uma *blockchain* é realizar o registro de dados de forma irreversível, de modo que, assim, é eliminada a necessidade de revalidação de dados.

Para melhor compreensão, válido realizar breve ilustração da estrutura:

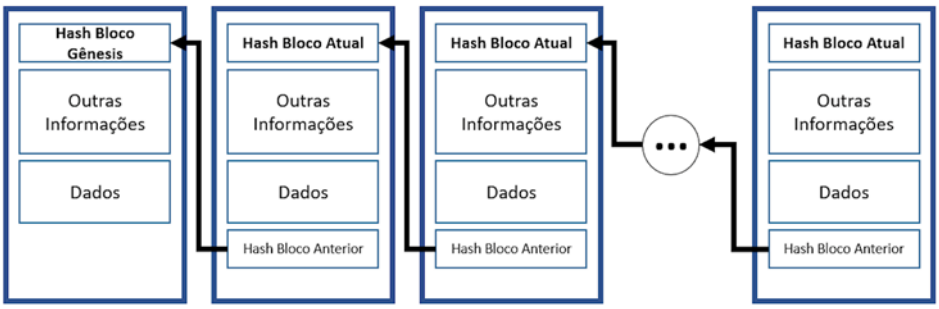

Figura 6: Estrutura genérica de uma rede *blockchain*

Fonte: Gomes, 2020.

Não há um consenso na academia sobre categorias específicas de *blockchain*, tendo em vista a existência de diversos fatores possíveis de categorizar. Contudo, para o presente estudo, adotamos a classificação proposta por Shrivas & Yeboah (2018), em que são classificados critérios relacionados à disponibilidade de dados e à participação na rede.

Tabela 3: Classificação dos tipos de *blockchains*

	Pública	**Privada**	**Comunitária**	**Híbrida**
Disponibilidade de dados	Qualquer usuário pode ler e submeter transações na rede.	Apenas uma organização ou organizações subsidiárias podem ler e submeter transações.	Grupo múltiplo de organizações são permitidas a ler e submeter transações.	Pode ser configurada como uma combinação de qualquer uma das outras categorias.
Participação na rede	Não é necessário permissão para participada da rede. Qualquer usuário pode participar do processo de validação e verificação das transações.	É necessário a permissão para participar da rede. Apenas participantes podem operar nós da rede e realizar a validação de transações.	Aplica-se o mesmo das *blockchains* privadas.	Admite múltiplas combinações das opções anteriores.

Fonte: Shrivas & Yeboah (2018) (adaptado).

Em se tratando de *blockchains* públicas, um ponto fundamental são os algoritmos de validação das transações. Os também chamados algoritmos de consenso refletem uma série de regras e

procedimentos que permitem a manutenção e o crescimento da rede *blockchain* de forma segura, confiável e autêntica.

Dentre os diversos algoritmos existentes, como *Proof of Authority*, *Proof of Storage* e *Proof of Burne,* destacam-se dois principais: *Proof of Work* e *Proof of Stake.*

O algoritmo utilizado atualmente por duas das *blockchains* mais populares, o Bitcoin e a Ethereum, trata-se do *Proof of Work.* A estrutura de funcionamento desse algoritmo de validação é pautada no processo de mineração, em que agentes da cadeia (também chamados de mineradores) realizam uma competição computacional para determinar a solução de um complexo problema matemático. Então, o nó que soluciona o problema de forma mais rápida recompensado com a autoridade de inserir um novo bloco de transações na rede e com *tokens* nativos da rede.

Já o algoritmo de validação *Proof of Stake* propõe uma seleção pseudorrandômica dos agentes validadores, levando consideração a quantidade de recursos depositados para tal finalidade (*staking)*. Nesse caso, o valor depositado pelo agente validador determina a probabilidade de seleção para inserção do novo bloco[11]. Assim, o agente selecionado realiza a verificação da validade de todas as transações contidas no novo bloco e é remunerado com uma parcela de todas as taxas das referidas transações. Nesse caso, também há um incentivo indireto para uma validação correta, tendo em vista a existência de depósitos do próprio validador. Portanto, na hipótese de uma validação maliciosa, o agente validador também perderia recursos.

Ademais, o custo operacional de validação de novos blocos é consideravelmente menor por meio do algoritmo *Proof of Stake,* pois não é necessário grande poder computacional para processamento do bloco, fator que implica em altos custos com equipamento e energia elétrica.

Por fim, outro ponto que merece atenção sobre *blockchains* é o trilema da escalabilidade proposto por Buterin (2021). Resumidamente, o trilema estabelece que sistemas em *blockchain* apenas podem contemplar duas das três propriedades: descentralização, escalabilidade e segurança. Em regra, isso deve-se ao fato de que o processamento de estados compete um alto custo operacional e, portanto, sempre que uma das propriedades cresce, outra é afetada.

Apesar de novos métodos para potencializar a escalabilidade de redes *blockchais* já existirem e alguns estarem em desenvolvimento, é fundamental compreender que se trata de uma grande barreira para o desenvolvimento da rede, incluindo a rede de finanças descentralizadas.

3.3.2. *Wallets*

Wallets são interfaces de gerenciamento de endereços de registro dentro de um protocolo *blockchain*, formadas por duas chaves criptográficas: a chave pública e a chave privada. Assim, realizando uma comparação entre as eras da internet *Web*2 e *Web*3, são comparáveis aos navegadores de internet na era da *Web*2, como *Google Chrome*, *Safari* e *Microsoft Edge*.

Lau *et al*. (2020) categorizam as *wallets* em dois principais grupos: custodiantes e não-custodiantes.

[11] O valor depositado possui uma correlação linear com a probabilidade de seleção para validar o novo bloco.

O primeiro grupo refere-se ao modelo em que empresas terceiras mantêm a controle dos ativos do usuário, não disponibilizando o acesso à chave privada e, portanto, reduzindo um dos principais riscos das carteiras: a perda da chave privada (e a consequente perda de todos os ativos nela contidos). Como exemplos de carteiras custodiantes, podemos citar a *Binance*[12], Mercado Bitcoin[13] e *CoinBase*[14].

Além da transferência da custódia dos ativos para um terceiro, a utilização de carteiras custodiantes agrega outros inconvenientes, como a necessidade de verificação de identidade (KYC – *Know Your Customer*), o risco regulatório e eventuais instabilidades nas plataformas de negociação.

Apesar de irem na contramão do princípio da descentralização, carteiras custodiantes também oferecem benefícios, como a possibilidade de recuperação de conta e, principalmente, a facilidade de integração com o sistema financeiro tradicional.

O segundo grupo, das carteiras não-custodiantes, trata-se de um modelo em que os usuários são detentores das próprias chaves, a pública e a privada. Nesse caso, não há um agente custodiante intermediário, transferindo o risco de perda ou roubo da chave privada para o usuário final (OCDE, 2022). Tais *wallets* transferem ao usuário o controle completo das chaves e, consequentemente, dos ativos nela contidos. Assim, convergindo com a ideia de descentralização, esta modalidade de controle de ativos possibilita ao usuário o fácil cadastro (sem a necessidade de verificação de identidade) e a transparência que nenhuma instituição terceira poderá vincular seus ativos à sua identidade.

Além do exposto, carteiras não-custodiantes são essenciais para uma plena interação com os DApps da rede financeira descentralizada, tendo em vista a dispensabilidade de contratos com as empresas terceiras custodiantes e o maior número de aplicações disponíveis. Como exemplos de carteiras não-custodiantes, podemos citar a *MetaMask*, *Ledger*, *Trezor* e *Jaxx Wallet*.

No quadro abaixo há o resumo das diferenças entre wallets custodiantes e não-custodiantes:

Quadro 1: Comparação entre *wallets* custodiantes e não-custodiantes

CRITÉRIO	*WALLETS* CUSTODIANTES	*WALLETS* NÃO-CUSTODIANTES
Acesso aos recursos	O controle das chaves privadas é atribuído às custodiantes, implicando na transferência do controle dos recursos para elas.	Apenas o usuário possui controle completo e acesso à sua chave privada e, consequentemente, aos recursos associados a ela.
Recuperação de Recursos	Opções simplificadas para a recuperação de acesso à carteira na hipótese de perda das credenciais.	Impossibilidade de recuperação dos recursos da carteira na hipótese de perda da chave privada ou frase de recuperação.
Segurança	Relativamente vulneráveis a invasões de hackers.	Sem conexão com a internet, *wallets* não-custodiantes não representam riscos relacionados ao cyber ataques,

[12] https://www.binance.com/. Acesso em: 27 de abril de 2022.
[13] https://www.mercadobitcoin.com.br/. Acesso em: 27 de abril de 2022.
[14] https://www.coinbase.com/. Acesso em: 27 de abril de 2022.

		mas os usuários devem realizar o armazenamento de sua chave privada e frase de recuperação.
Criação de contas	Necessidade de registro de informações pessoais e passagem por procedimentos de *compliance* (prevenção à lavagem de dinheiro).	Sem necessidade de registro de informações pessoais e procedimentos de *compliance*
Facilidade para o uso	Interfaces com alto grau de usabilidade, incluindo manuais e tutoriais.	Menor grau de usabilidade, sendo necessário o mínimo conhecimento técnico para operação.

Fonte: 101blockchains.com (adaptado).

Dentre as carteiras não-custodiantes, merecem destaque as *wallets* que atuam como extensões de navegadores de internet e que não realizam o armazenamento da chave privada do usuário no próprio servidor, como as carteiras *MetaMask*, *WalletConnect* e *TrustWallet*.

3.3.3. *Smart Contracts*

Segundo Mohanta *et al*. (2018), *smart contracts*, ou em português, contratos inteligentes, são "programas de computador com propriedades de auto verificação, auto execução e resistentes a adulterações".

O precursor da ideia de contratos inteligentes, Nick Szabo (1994), defendia a possibilidade de cláusulas contratuais serem atreladas a determinados *hardwares* e *softwares*, permitindo, assim, a execução de determinados processos sem a necessidade de terceiros intermediários.

A taxonomia de um *smart contract* pode ser resumida nos seguintes elementos: valor, endereço, funções e estado. Ademais, o contrato inteligente deve receber *inputs*, executar o código correspondente e acionar *outputs* programáveis, conforme exposto por Zheng *et al*. (2020).

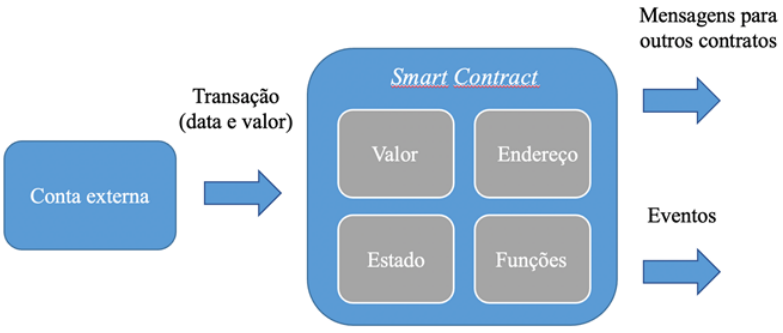

Figura 7: Estrutura básica de um contrato inteligente

Fonte: Zheng *et al*. (2020) (adaptado).

Apesar de viabilizar apenas o desenvolvimento de contratos inteligentes simples (com lógica simplificada), o Bitcoin ampliou o horizonte de análise de integrações dos contratos inteligentes com a rede *blockchain*, se tornando um ponto focal de estudos e pesquisas. Sinteticamente, no caso de contratos

inteligentes baseados em *blockchains*, os contratos não são nada mais do que *scripts* de código que executam e registram na própria rede.

A Ethereum, outra *blockchain* pública, conforme abordado nos tópicos seguintes, representou um marco temporal na utilização de contratos inteligentes, na medida que disponibilizou aos usuários uma máquina virtual descentralizada, *touring-complete (EVM)*, capaz de executar contratos com alto nível de complexidade. Zheng *et al*. (2020) apontam que sua utilização integrada na rede *blockchain* pode garantir diversos benefícios, como a velocidade, acurácia, redução de risco de redução, corte de intermediário, menor custo e novos modelos de negócio.

A versatilidade do uso de *smart contracts* é reflexo de sua utilização em diversos setores, como *supply chain, Internet of Things,* sistemas de saúde, imobiliário, seguros e, em especial, sistema financeiro.

Contudo, apesar de inovador, o cenário de desenvolvimentos de contratos inteligentes ainda se encontra em um estágio incipiente, pois problemas relacionados com a escalabilidade, privacidade e disponibilização como código aberto ainda representam barreiras para o crescimento do uso.

No caso do setor financeiro, objeto do presente estudo, é inquestionável que o uso de *smart contracts* é uma ferramenta essencial para o desenvolvimento de produtos financeiros com diversos graus de sofisticação, mas não se limitando à operação com derivativos e a operações estruturadas.

3.3.3.1. DApps

DApps, ou *Decentralized Applications*, são aplicativos que executam contratos inteligentes sem a necessidade de um servidor único ou entidade controladora. Em contraponto aos aplicativos centralizados, que usualmente envolvem a análise de dados dos usuários por meio de uma empresa ou grupo, os DApps utilizam a rede *blockchain* como estrutura de armazenamento e processamento de dados. Assim, são implementados por meio de contratos inteligentes e uma *User Interface* (UI), esta em geral desenvolvida em modelos de *website* (METCALFE, 2020).

Segundo Johnston *et al*. (2014), DApps devem cumprir os seguintes requisitos:

(i) Serem totalmente de código aberto, operando de forma autônoma, sem que nenhuma entidade controle a maioria de seus *tokens*, e seus dados e registros de operação devem ser armazenados criptograficamente em uma *blockchain* pública e descentralizada.

(ii) Devem gerar *tokens* de acordo com um algoritmo padrão de um conjunto de critérios e possivelmente distribuir alguns ou todos os *tokens* no início de sua operação. Esses tokens devem ser necessários para o uso do aplicativo e qualquer contribuição dos usuários deve ser recompensada pelo pagamento nos *tokens* do aplicativo.

(iii) Devem adaptar seus protocolos em resposta a melhorias propostas e *feedback* do mercado, mas todas as alterações devem ser decididas por consenso da maioria de seus usuários.

Necessário atentar-se que nem todos os DApps são transparentes e legítimos, de modo que, antes de utilizá-lo, é fundamental realizar uma análise detalhada do histórico do aplicativo e *White Paper* da plataforma.

Os DApps representam um avanço tecnológico considerável, porque viabilizam o desenvolvimento de aplicativos por qualquer um com expertise em programação. No caso específico do setor financeiro, o custo operacional para desenvolver qualquer serviço sempre foi muito alto, em razão da necessidade de cumprimento de obrigações regulatórias. DApps, portanto, representam um interessante potencial disruptivo para a pulverização de inovadores e descentralizados serviços financeiros.

3.3.4. Criptoativos, criptomoedas e *tokens*

Não é incomum a troca de conceitos quando falamos em *tokens*, criptomoedas e criptoativos. Nesse sentido, para melhor compreensão dos termos utilizados no presente trabalho, é fundamental realizar breve explicação.

Segundo a Comissão de Valores Mobiliários – CVM[15], criptoativos são "ativos virtuais, protegidos por criptografia, presentes exclusivamente em registros digitais, cujas operações são executadas e armazenadas em uma rede de computadores." Assim, resumidamente, criptoativos englobam outras representações digitais de valores ou direitos disponíveis em redes *blockchain*, incluindo *tokens*, criptomoedas, dentre outras.

Já criptomoedas são caracterizadas como moedas digitais privadas criadas em redes descentralizadas de computadores e protegidas por criptografia. Ragazzo & Cataldo (2021) estabelecem algumas características comuns às criptomoedas, como o uso de redes descentralizadas (DLT´s ou *blockchains*), a fungibilidade e a existência de mecanismos de consenso para validação de transações. Alguns autores, como Voshmgir (2020), acreditam que o termo criptomoeda é equivocadamente associado a qualquer espécie de criptoativo e, por isso, propõe utilizar termos mais genéricos, como ativo criptográfico.

Por fim, *tokens* podem ser definidos como a representação digital de direitos de acesso às propriedades ou serviços públicos e privados. Em síntese, representam uma série de regras, determinadas em contratos inteligentes, também chamados *token contracts*. Portanto, podemos caracterizar *tokens* como registros de entradas na rede distribuída mapeados por meio de um endereço *blockchain* que representa a identidade do detentor do ativo **(**VOSHMGIR, 2020).

Não há um consenso sobre como categorizar *tokens*, mas já existem algumas propostas de taxonomia[16]. Dentre as propostas mais utilizadas, merece enfoque a qualificação genérica de *tokens* fungíveis proposta pelo órgão regulador suíço FINMA[17], em que os *tokens* são segregados em três macro categorias relacionadas com o seu propósito: *tokens* de pagamento, *tokens* de utilidade e *tokens* de ativos. É possível conjugar mais de uma categoria por *token*.

Importante destacar a categoria de *tokens* não fungíveis, também chamados de *Non-fungible tokens* – NFTs, que são basicamente registros únicos de identificação de determinada coisa (WANG,

[15] Disponível em: https://www.investidor.gov.br/publicacao/Alertas/alerta_CVM_CRIPTOATIVOS_10052018.pdf. Acesso em: 27 de abril de 2022.
[16] Ver: https://entethalliance.org/enterprise-ethereum-alliance-launches-blockchain-neutral-token-taxonomy-initiative-to-accelerate-a-token-powered-blockchain-future/. Acesso em: 27 de abril de 2022.
[17] https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung. Acesso em: 27 de abril de 2022.

2021). São registros comuns em NFT's as artes digitais colecionáveis e ativos relacionados a jogos digitais.[18]

Segundo a taxonomia proposta pelo FINMA, *tokens* de pagamento são sinônimos de criptomoedas e possuem a principal característica de serem utilizados como meio de pagamento. A definição não engloba a conexão dessa categoria de *token* com determinados projetos, sendo que os *tokens* de pagamento devem apenas fornecer a funcionalidade necessária. Exemplos típicos dessa categoria são o Bitcoin (BTC), o Litecoin (LTC) e a *stablecoin* USDT.

Já os *tokens* de utilidade (*utility tokens*), possuem um vínculo direto com acesso a determinado serviço ou produto, incluindo, mas não se limitando a poderes de governança. Assim, enquadram-se a grande maioria dos *tokens* disponíveis na rede DeFi, e podemos citar como exemplos os *tokens* LINK, AAVE e QUICK.

Tokens de ativos (*asset tokens*) procuram representar ativos securitizados, considerados semelhantes a ativos financeiros tradicionais, como títulos de dívida, *equity*, bens imóveis, futuros, dentre outros.

Voshmgir (2020) destaca outras possíveis perspectivas para classificar determinado *token*, são elas: técnica, legal, fungibilidade, transferência, duração, regulatória, incentivos, disponibilidade, fluxo operacional, privacidade e estabilidade

Outro interessante método de definição taxonômica é proposto por Euler (2018)[19], em que *tokens* são classificados de acordo com cinco camadas de categorias: técnica, propósito, valor subjacente, utilidade e status legal.

3.3.4.1. *Stablecoins/Stabletokens*

Stablecoins (ou *Stabletokens*) são ativos digitais desenvolvidos com o objetivo de replicar em uma rede *blockchain* o valor de moedas fiduciárias, como o dólar, euro ou real, ou de qualquer *commodity*, por meio de ferramentas de estabilização (BULLMAN *et al*., 2019).

Para analisar a complexidade do arranjo de *stablecoins*, é fundamental compreender a sua principal função: a garantia de estabilidade. É incontroverso que a estabilidade de curto prazo é um dos fatores mais importantes de uma moeda, pois, desse modo, é possível garantir um dos elementos que caracterizam a moeda: a unidade de conta. Em verdade, a estabilidade é essencial para assegurar que a moeda cumpra suas duas outras principais funções: a reserva de valor e o meio de troca, partindo do pressuposto que o preço que pagamos por bens e serviços necessita ser confiável e planejado (SOUTELO, 2020).

Ao passo em que protocolos como o Bitcoin ou Ethereum não apresentam um algoritmo sofisticado de controle de política monetária, a volatilidade emerge como um fator determinante motivado pela especulação. Voshmgir (2020) elenca os seguintes fatores que contribuem para a instabilidade de *tokens* de protocolos e que justificam a impossibilidade de utilizá-los em transações diárias:

[18]Ver: https://axieinfinity.com/. Acesso em: 27 de abril de 2022.
[19] Disponível em: http://www.untitled-inc.com/the-token-classification-framework-a-multi-dimensional-tool-for-understanding-and-classifying-crypto-tokens/. Acesso em: 27 de abril de 2022.

a) uma política monetária estática decorrente da emissão de *tokens* não ajustável ao seu preço;

b) mudanças de percepção dos usuários sobre o valor do *token*;

c) o fato dos *tokens* representarem ativos em um mercado emergente que grande parte das pessoas não compreendem; e

d) potencial de reação do mercado ao cenário de instabilidade regulatória (VOSHMGIR, 2020. Tradução nossa).

Desse modo, *stablecoins* surgem como uma alternativa dentro dos protocolos *blockchain*, na medida que os usuários podem realizar transferências de valores, principalmente no contexto internacional, conforme apontado por relatório do grupo de trabalho do G7 (2019), mitigando o risco de volatilidade de *tokens* de protocolos (como o Bitcoin, Ethereum ou qualquer *token* ERC-20 dentro da rede). Ademais, a utilização de *stablecoins* contribui para a popularização do uso de criptoativos em operações de investimentos ou pagamentos cotidianos, e viabiliza o desenvolvimento de uma economia tokenizada (VOSHMGIR, 2020).

Nesse sentido, importante realizar breve distinção entre as seguintes categorias de *stablecoins* propostas por Voshmgir (2020): (i) *Stablecoins* atrelados a moedas fiduciárias (*fiat-collateralized*); (ii) *Stablecoins* atrelados a criptomoedas (*crypto-collateralized stable tokens*); e (iii) *Stablecoins* algorítmicos (*algorithmic stable tokens*).

A seguir, realizaremos breve descrição dos tipos de *stablecoin*, suas principais características e riscos.

(i) *Stablecoins* atrelados a moedas fiduciárias (*fiat-collateralized*): o tipo mais popular de *stablecoin* é aquele diretamente atrelado à moeda fiduciária com proporção de 1:1. Também chamamos de "*fiat-collateralized stablecoins*", ou seja, um *stablecoin* com garantia em moeda fiduciária.

Essa modalidade é operacionalizada por meio de um emissor central que mantém uma quantidade de moeda fiduciária em reserva e emite uma quantidade proporcional de *tokens*, de modo que todas as moedas emitidas são garantidas pelo próprio emissor ou custodiante por ele nomeado (BOLLIGER, 2020).

Ocorre que, mesmo levando em consideração que os emissores de *stablecoins* atrelados a moedas fiduciárias normalmente asseguram que o criptoativo é garantido na mesma proporção de moeda fiduciária em reserva, nem sempre isso condiz com a realidade. Alguns emissores realizam depósitos em caixa, fundos de investimento, seguros ou outros ativos (CBINSIGHTS, 2022).

Em meados de 2021, emissores das *stablecoins* Tether (USDT) e USDC, ambas atreladas ao dólar americano, foram criticados com relação à transparência das reservas que garantem os criptoativos, deixando evidente o alto risco de garantia por emissores desconhecidos, duvidosos e não transparentes (BLOOMBERG, 2021).

Destaca-se que grande parcela dos protocolos de empréstimo possui ativos em garantia classificados como *fiat-collateralized stablecoins*, acarretando um considerável risco de liquidez ao mercado.

(ii) *Stablecoins* atrelados a criptomoedas (*crypto-collateralized stable tokens*): o segundo modelo de *stablecoin* é colateralizado (garantido) em outros criptoativos. Assim, a emissão do *stablecoin* cripto-colateralizado é realizada por meio de um contrato inteligente, implicando, portanto, em maior descentralização. Vejamos as lições de Bollinger (2020):

> Como não há emissor centralizado, o usuário precisa enviar garantias na rede ao contrato inteligente do sistema para obter algumas stablecoins emitidas. O contrato inteligente cria as stablecoins e as envia ao usuário. A partir do momento em que o usuário recebe as stablecoins, ele fica responsável por garantir o valor necessário dos tokens garantidos. A transferência de stablecoins colateralizadas na rede é baseada no princípio da tecnologia blockchain, sem unidade de controle central, mas uma verificação das transações de cada usuário ativo no livro razão distribuído (tradução nossa) (BOLLINGER, 2020).

Em síntese, os usuários realizam o bloqueio de suas criptomoedas em um contrato inteligente que, posteriormente, emite o *token*. Desse modo, para realizar o saque, basta o usuário realizar o depósito das *stablecoins* no contrato inteligente. O *stablecoin* cripto-colateralizado com maior aceitação no mercado na data de publicação deste trabalho é o DAI, desenvolvido pela rede MakerDAO[20].

O método de controle de estabilidade dos criptoativos é realizado por meio de algoritmos de gatilhos que disparam na hipótese de alta volatilidade. Ademais, o protocolo também estabelece mecanismos de *shutdown*, garantias contra invasões, taxas de reserva, oráculos e auditorias periódicas

(iii) *Stablecoins* algorítmicos (*algorithmic stable tokens*): são ainda mais recentes e, por não serem diretamente atreladas a moedas fiduciárias ou criptomoedas, são lastreadas inteiramente em algoritmos e contratos inteligentes que realizam o gerenciamento e fornecimento dos *token* emitidos. Nesse sentido, os algoritmos estabelecem a política monetária de forma inspirada aos Bancos Centrais, mas levando como base estruturante a confiança nos agentes, diferentes atores independentes (e não regulados), que incentivam a estabilização do mercado por meio de arbitragem. Resumidamente, o fornecimento é vinculado ao preço da moeda fiduciária que corresponde ao *stablecoin*, de modo que há um algoritmo de injeção e redução de liquidez automática.

Considerando o alto nível de complexidade do algoritmo mencionado e o considerável risco tecnológico, grande parte dos *stablecoins* algorítmicos são descontinuados, a exemplo do que permanece ativo, o *stablecoin* FEI[21], desenvolvido pela TRIBE.

Segundo Clements (2021), os *stablecoins* algorítmicos são construídos sob uma frágil base de confiança em variáveis históricas incertas, necessitando, portanto, de uma linha de suporte para controle de demanda (na hipótese de uma queda abrupta de demanda), agentes controladores regulados e um ambiente informacional eficiente, este que é necessariamente prejudicado em tempos de crise.

Pelo exposto, não há escolha ideal de *stablecoin*, sendo necessário analisar os riscos de cada opção para determinar a alocação de recursos nessa classe de ativos.

[20] https://makerdao.com/pt-BR/. Acesso em: 27 de abril de 2022.
[21] https://fei.money/. Acesso em: 27 de abril de 2022.

3.3.4.2. Moedas digitais de bancos centrais (CBDC's)

A diminuição do uso de dinheiro físico como meio de transação, o surgimento de novas formas de dinheiro digital assegurados por instituições não-bancárias (como *stablecoins*[22]) e a aceleração da digitalização dos serviços financeiros são fatores que impulsionaram os bancos centrais a explorarem novas formas de exercer as suas funções e se adaptarem às mudanças que moldam o futuro sistema financeiro. (BIS, 2021)

Dentre as pesquisas realizadas por diversos bancos centrais, destaca-se o foco dado às moedas digitais de bancos centrais, também chamadas de CBDC´s (*Central Bank Digital Currencies*).

Segundo o pelo *Bank for Internacional Settlements- BIS* (BIS, 2020) pode-se definir CBDC como um passivo direto do banco central, instrumentalizado por meio digital e contabilizado em unidade de conta nacional. Assim, existem duas principais categorias de CBDC´s, atacado e varejo, sendo que estas podem ser arquitetadas de outras três principais formas, diretamente, por meio de intermediários e de forma híbrida. No presente estudo, as modalidades e arquiteturas de CBDC´s não serão aprofundadas, levando em consideração que se objetiva apenas contextualizar o leitor sobre os possíveis impactos que a rede financeira descentralizada pode gerar no desenvolvimento de CBDC´s e, de forma geral, como a adoção de moedas digitais pode impactar a economia.

Como benefícios da implementação de CBDC´s, podemos citar o potencial de crescimento da bancarização, aumento do controle fiscal (inclusive com relação à lavagem de dinheiro e financiamento do terrorismo) e a melhoria da implementação de políticas monetárias. Ademais, outros pontos sensíveis do sistema financeiro podem ser impactados positivamente com as CBDCs, como transações internacionais, o grau de integração com outros sistemas financeiros, e, em especial, a programalidade no sistema financeiro, ou seja, a possibilidade de implementação de contratos inteligentes para execução e desenvolvimento de novos modelos de negócios e produtos financeiros.

Contudo, surgem algumas barreiras de implementação. Dentre elas, podemos citar o risco de privacidade, em razão do controle de registros transacionais, o potencial controle excessivo do Estado em face da população, as barreiras tecnológicas, como problemas relacionados à segurança e escalabilidade e, por fim, eventual ultrapassagem dos perímetros regulatórios.

Alguns países destacam-se no desenvolvimento e pesquisas sobre CBDC´s, como a China (com o Yuan Digital), as Bahamas (*Sand Dollar*), Suécia (e-Krona) e o Brasil (Real Digital).

O caso brasileiro demonstra uma inclinação para adoção de uma infraestrutura de mercado integrada com o atual sistema de pagamentos instantâneo, o Pix. A seleção da base tecnológica, apesar de incerta, denota uma tendência para adoção de DLT´s, podendo, inclusive, utilizar-se de redes *blockchain*[23].

As intersecções com o ecossistema DeFi ainda são desconhecidas, mas, o Banco Central do Brasil permanece na vanguarda dos estudos e pesquisas. Destacam-se os projetos LIFT Challenge e

[22] As CBDC´s diferem da *stablecoins*, na medida que estas são emitidas por instituições privadas, com baixo nível de transparência e elevado risco, e aquelas são efetivamente as moedas fiduciárias emitidas pelos próprios bancos centrais.

[23] É factível a adoção de *blockchains* restritas para a implementação de CBDC´s.

LIFT Learning, que propõem esclarecer como as tecnologias presentes em protocolos comuns na rede DeFi podem ser aplicadas ao futuro do Sistema de Pagamentos Brasileiro.

3.3.5. *Decentralized Autonomous Organizations* (DAO's)

Organizações Autônomas Descentralizadas, ou DAO's, são estruturas organizacionais focadas em garantir maior grau de descentralização na governança exercida. Assim, em geral, participantes que promovem DAO's organizam-se em torno de determinada missão/missões e coordenam o crescimento por meio de uma série de regras determinadas em mecanismo baseados em *blockchains*, em que a governança é realizada por meio de votação dos detentores de *tokens* de governança (IOSCO, 2022).

Buterin (2013, p. 23) define DAO's como "uma entidade virtual que possui determinados membros ou acionistas com direitos de realizarem gastos dos recursos da entidade e modificarem o código". Essa definição, contudo, direciona a compreensão do conceito de DAO's como uma companhia tradicional.

Apesar de alguns estados americanos, como Wyoming[24], possibilitarem o registro de DAO's como companhias de responsabilidade limitada (LLC), a essência da criação de DAO's perpassa um contexto mais complexo, contemplando a independência de um controle central e a possibilidade aberta e distribuída de acesso à organização.

Um interessante exemplo das diferenças entre empresas tradicionais e DAO's pode ser observada na *startup* brasileira focada em projetos sociais e doações, a Ribon[25], em que a adoção do modelo de governança descentralizada foi motivada, essencialmente, pela maior transparência dos registros de gastos, a acessibilidade e sustentabilidade da organização. Nesse contexto, vejamos a aplicação de DAO's em outros diversos contextos:

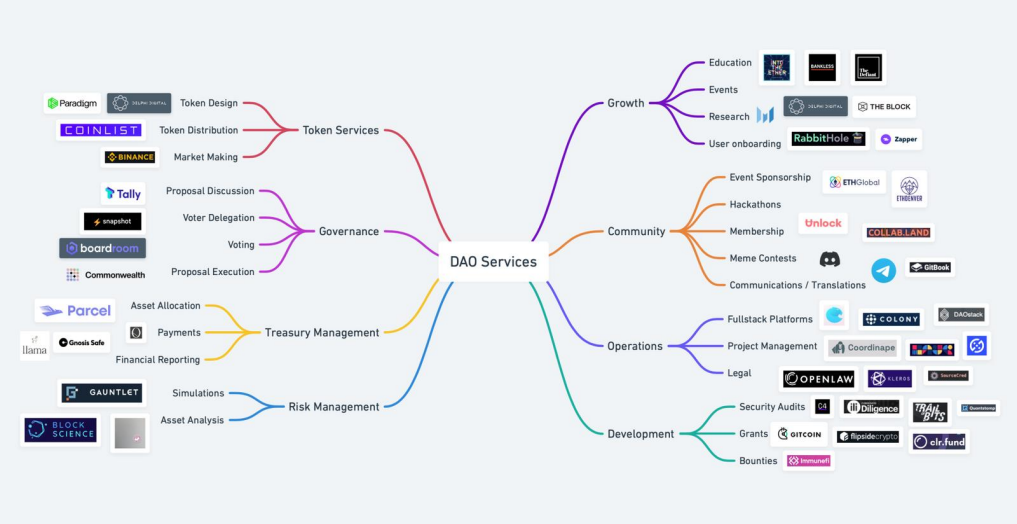

Figura 8: Possibilidade de aplicações de serviços em DAO´s

Fonte: Consensys.

[24] https://decrypt.co/75222/americas-first-dao-approved-in-wyoming. Acesso em: 27 de abril de 2022.
[25] https://ribon.io/. Acesso em: 27 de abril de 2022.

DAO’s também representam riscos. Fundamental realizar breve explanação sobre o caso da TheDAO, uma espécie de fundo de investimentos organizada sob a forma de uma DAO, de modo que os participantes da organização possuíam poder de voto nos projetos a serem investidos. Contudo, em razão de uma falha no algoritmo, uma grande parcela dos recursos foi roubada por um *hacker*, implicando em uma intervenção da fundação Ethereum (EL FAQIR *et al*., 2020).

Ainda existem muitas questões em aberto sobre problemas relacionados a efetiva distribuição da governança em DAO’s, em razão de eventuais concentrações do poder decisório, além de grau de automação das organizações e quais seriam os critérios para qualificar a participação de um usuário (JENTZSH, 2016).

4. EXPERIMENTO PRÁTICO: OPERANDO EM DEFI

No presente capítulo apresentaremos os resultados obtidos no experimento prático realizado, que, além de elucidar um tutorial lógico de utilização para o usuário final que objetiva operar na rede DeFi, procura investigar a estrutura de funcionamento dos protocolos de aplicações descentralizadas mais comuns, como o *Swap*, provimento de liquidez e empréstimo. Assim, compreendendo a estrutura de funcionamento, foi possível delimitar e categorizar os riscos presentes no setor para fornecer insumos para a análise multicritério.

Para a realização do experimento, foi depositado o montante de R$1.000,00 (um mil reais). Os detalhes do período de operação e a opção ou não por alocação da carteira de investimentos sob gestão serão apresentados no tópico relativo à análise dos riscos.

É fundamental destacar que a seleção de quaisquer plataformas, carteiras, DApp ou programas no presente experimento não possui nenhum caráter comercial e nem como sugestão de investimento, servindo apenas para fins acadêmicos.

4.1. Seleção da *wallet* para operações

A facilidade de registro e integração com diversos DApps da rede financeira descentralizada motivaram a escolha da carteira *MetaMask* para a realização dos experimentos, esta desenvolvida como uma extensão do navegador de internet. Para a criação de uma carteira empresa, foi realizado o *download* da extensão para o navegador de preferência (*Chrome*, *Firefox*, *Brave* ou *Microsoft Edge*) e selecionado a opção “criar conta”.

A extensão imediatamente gerou um endereço na *blockchain* Ethereum e disponibilizou uma plataforma simplificada de operação de *Exchange*, vejamos:

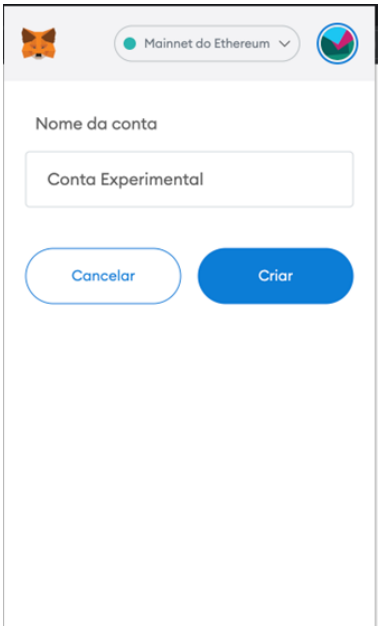

Figura 9: Passo 1 para a criação da carteira

Fonte: Captura de tela realizada pelo Autor.

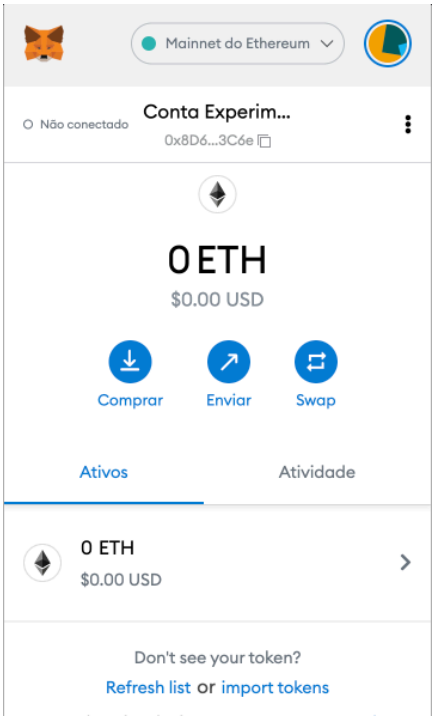

Figura 10: Página inicial da carteira *MetaMask*

Fonte: Captura de tela realizada pelo Autor.

Logo abaixo do nome dado para a conta (Conta Experimental), é possível localizar o endereço da conta, ou seja, a chave pública, esta descrita em um endereço hexadecimal.

Chave pública da Conta Experimental: 0x8D634B20647C6Aa59fa28aEaBcbc78A26d263C6e.

Passados os primeiros passos para o início do experimento, analisaremos o método de envio de recursos para o endereço mencionado.

4.2. Envio de recursos para a rede financeira descentralizada

Na intenção de reduzir os custos transacionais, o envio de recursos para a rede financeira descentralizada ocorreu por meio de uma corretora de criptomoedas, a Binance.

Apesar de se tratar de uma corretora, ou seja, um agente intermediário centralizador, a utilização de uma corretora possibilitou a conexão com o Sistema de Pagamentos Instantâneo – Pix, implicando em uma redução significativa dos custos de transação, tendo em vista que utilizando o Pix, a plataforma não realiza a cobrança de taxas de depósito.

Para realizar a transferência, basta se cadastrar na plataforma da Binance e solicitar o depósito em moedas fiduciária, no caso, o real. Há também a opção de depósito via cartão de débito ou crédito, mas é realizada a cobrança de taxas adicionais para a bandeira.

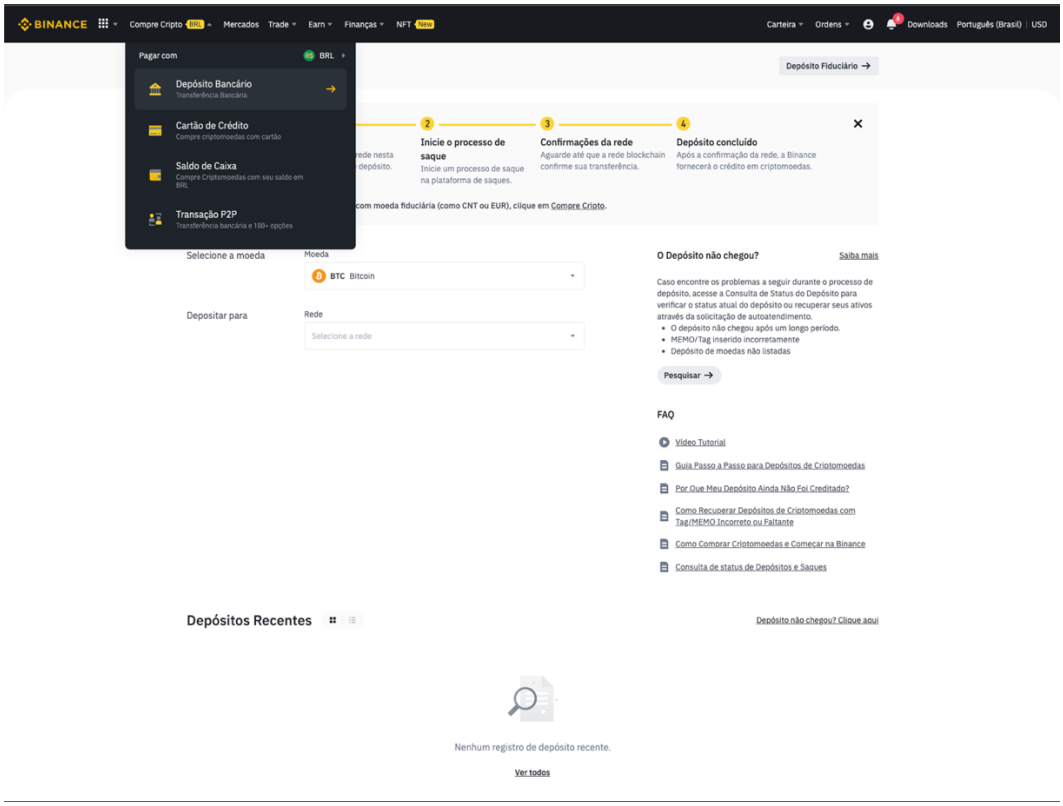

Figura 11: Plataforma da Binance para o depósito de moedas fiduciárias

Fonte: Captura de tela realizada pelo Autor.

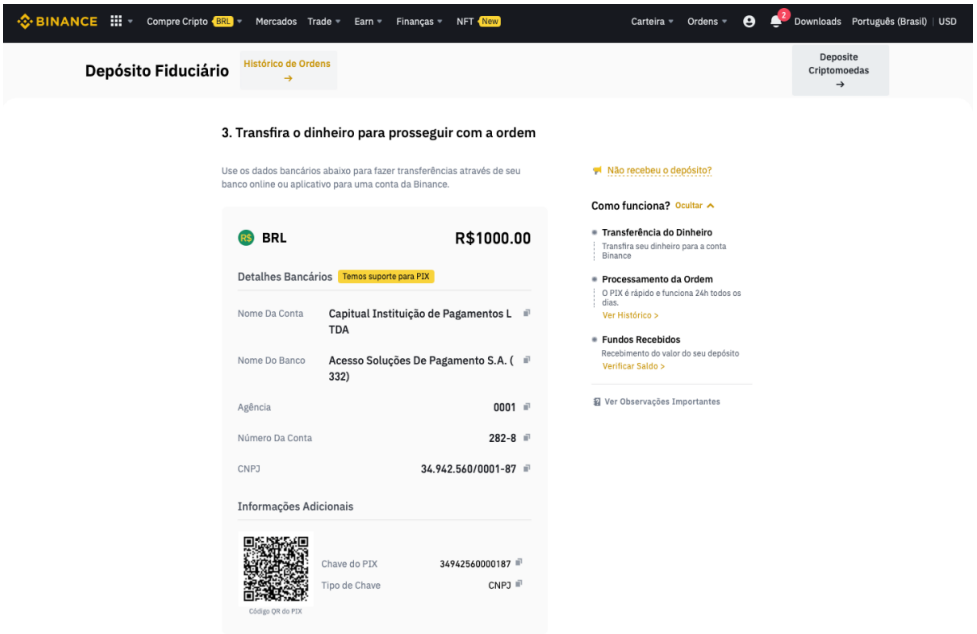

Figura 12: Realização do depósito fiduciário via Pix

Fonte: Captura de tela realizada pelo Autor.

Após a confirmação do depósito, é possível realizar a conversão do saldo em criptomoedas. Contudo, é importante destacar que a seleção do ativo a ser comprado deve estar diretamente relacionada com o protocolo escolhido para a realização das operações, conforme exposto no tópico subsequente.

Para o experimento realizado neste estudo, foi selecionada a criptomoeda Ether, oriunda da rede Ethereum, pois o protocolo escolhido trata-se de uma segunda camada do Ethereum e o ETH (código da criptomoeda Ether), e é essencial para qualquer transação dentro da rede Ethereum. Vejamos o passo-a-passo para a conversão:

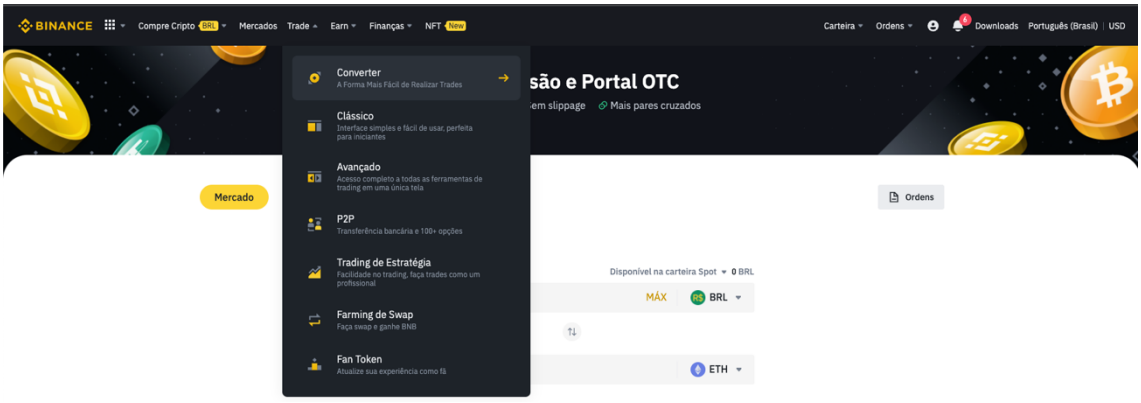

Figura 13: Aba 1 de conversão de moedas fiduciárias em criptomoedas

Fonte: Captura de tela realizada pelo Autor.

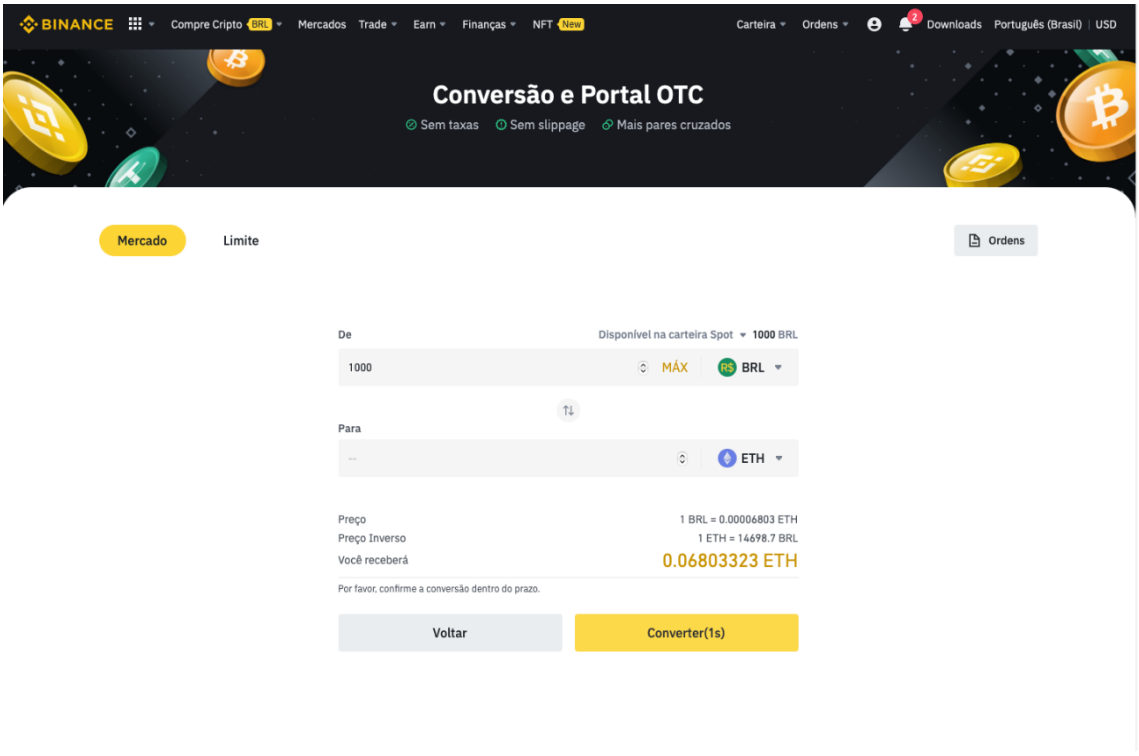

Figura 14: Aba 2 de conversão de moedas fiduciárias em criptomoedas

Fonte: Captura de tela realizada pelo Autor.

Realizada a conversão, o próximo passo do experimento foi enviar os recursos para uma *wallet* não-custodiante, a mesma criada na *MetaMask*, conforme subtópico anterior. O procedimento para envio consiste em solicitar o "Saque Cripto" por meio da própria plataforma da corretora Binance. Assim, a página solicita o endereço de destino, em que completamos com a chave pública descrita no subcapítulo 4.1, e a rede de destino que, no caso, trata-se da Ethereum.

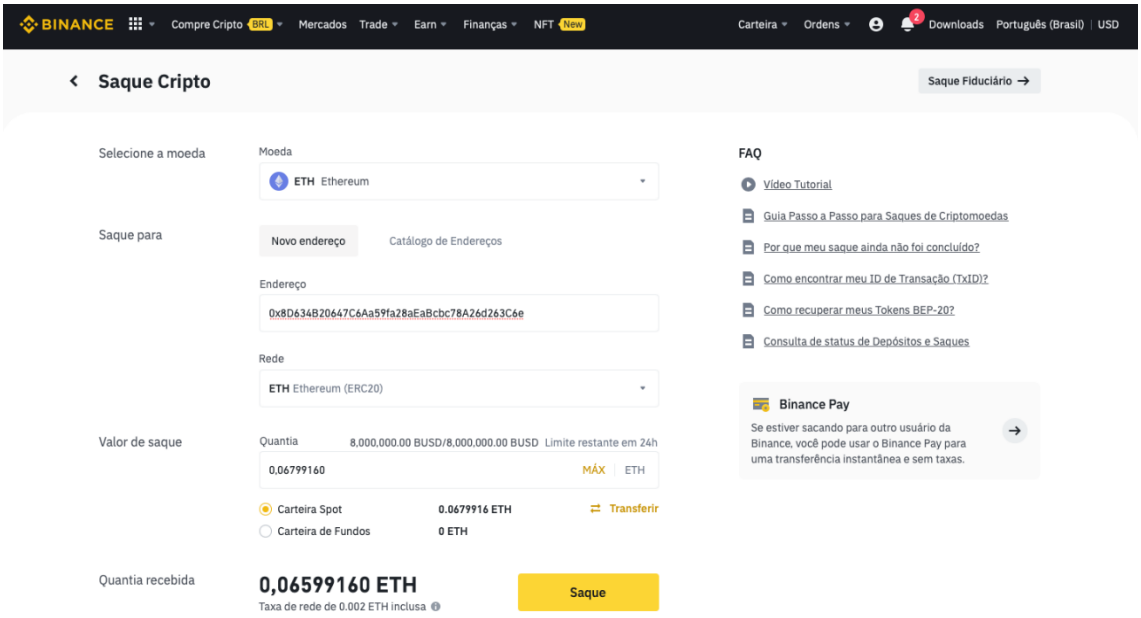

Figura 15: Saque do saldo de conta da corretora Binance

Fonte: Captura de tela realizada pelo Autor.

Destaca-se que, apesar da plataforma da Binance disponibilizar todas as operações realizadas no presente estudo, a transferência dos recursos para a Ethereum objetiva descrever a estrutura de funcionamento dos contratos inteligentes por trás dos DApps em uma rede essencialmente descentralizada.

4.3. Protocolo para operações

A seleção do protocolo trata-se de um passo fundamental para a realização das operações, tendo em vista que vincula a existência de diferentes DApps, custos transacionais, *tokens* nativos e de governança.

Nesse sentido, levando em consideração os problemas estruturais da Ethereum, o protocolo selecionado sintetiza algumas possíveis soluções e propõe um método de funcionamento da infraestrutura: a criação de uma *blockchain* (*commit chain*) para desafogar o processamento da rede principal.

A fim de compreendermos a seleção do protocolo, é importante realizar breve esclarecimento sobre os motivos que nortearam a escolha.

4.3.1. O alto custo de transações na rede Ethereum

A Ethereum foi responsável por implementar e representar um grande avanço nos protocolos *blockchain*, tendo em vista que agregou uma linguagem de programação *Turing*-completa integrada, permitindo que qualquer desenvolvedor escreva contratos inteligentes (*Smart Contracts*), aplicativos descentralizados (DApps) e estabeleça suas próprias regras arbitrárias para propriedade, formatos de transação e funções de transição de estado (BUTERIN, 2014).

Contudo, observamos algumas características correlacionadas que inviabilizaram a utilização direta da rede para a realização do experimento. O principal problema mapeado da rede Ethereum foi o alto custo das taxas transacionais. Assim, como o experimento não contempla a movimentação de um montante muito alto, algumas taxas cobradas pelas transações poderiam ser, inclusive, superiores ao valor transacionado.

Com relação aos valores médios das taxas das transações na rede Ethereum, podemos observar um crescimento significativo nos últimos dois anos, veja:

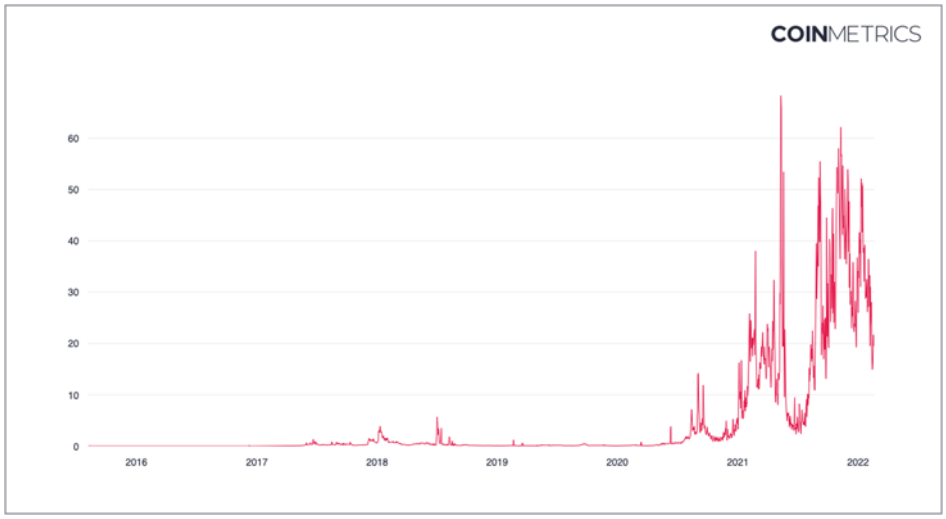

Gráfico 1: Taxa média de transações por período na rede Ethereum

Fonte: Coinmetrics.

Tal fato decorre de as taxas cobradas pela execução das transações possuírem uma relação direta com o algoritmo de consenso utilizado pela rede *blockchain* e o congestionamento da rede.

Conforme já apresentado na seção 3.3.1, os algoritmos de consenso são os métodos que os protocolos *blockchain* utilizam para realizar a validação de transações. Dentre os algoritmos mais comuns, podemos citar: *Proof of Work* (PoW), *Proof of Stake* (PoS), *Delegate Proof of Stake* (DPoS) e *Leased Proof of Stake* (LPoS).

A rede Ethereum utiliza o algoritmo de consenso *Proof of Work*, que, em síntese, consiste na validação dos blocos de transações por meio de uma competição para realizar a solução de um problema computacional de alta complexidade (PORAT *et al*., 2017). A utilização do algoritmo de consenso PoW implica em um alto custo de processamento energético, consequentemente, transferindo o custo para as taxas cobradas por transações realizadas na rede (ALIAGA & HERNIQUES, 2017). Ademais, com o

aumento do número de transações na rede Ethereum decorrente do movimento DeFi, dos NFTs, dentre outros, a capacidade de processamento computacional da rede também está sendo comprometida, por isso as taxas das transações representaram um aumento considerável.

Já o algoritmo PoS, conforme abordado no tópico referente a *Blockchains*, propõe a validação de transações por meio da seleção de usuários aleatórios que possuam maior quantidade de recursos detidos na rede (*stake*), de modo a reduzir o custo de processamento das transações.

Apesar de já haver um anúncio de futura migração do algoritmo de validação na rede Ethereum para o PoS, não houve a implementação total até a data de execução do presente experimento[26]. Contudo, soluções de escalabilidade emergiram como alternativas, são elas: *sidechains*, solução plasma, canais de estado (*state channels*) e os recentes *optmistic/ Zk rollups*.

4.3.2. *Polygon*

Para a execução do experimento, selecionamos a rede *Polygon* (ou *MATIC Network*). Importante ressaltar que a maioria dos protocolos em outras redes possui semelhanças com o protocolo selecionado.

Até meados de março de 2022, a rede *Polygon* possuía o valor aproximado de 3,74 bilhões de dólares americanos (USD) em TVL (*Total Value Locked*).

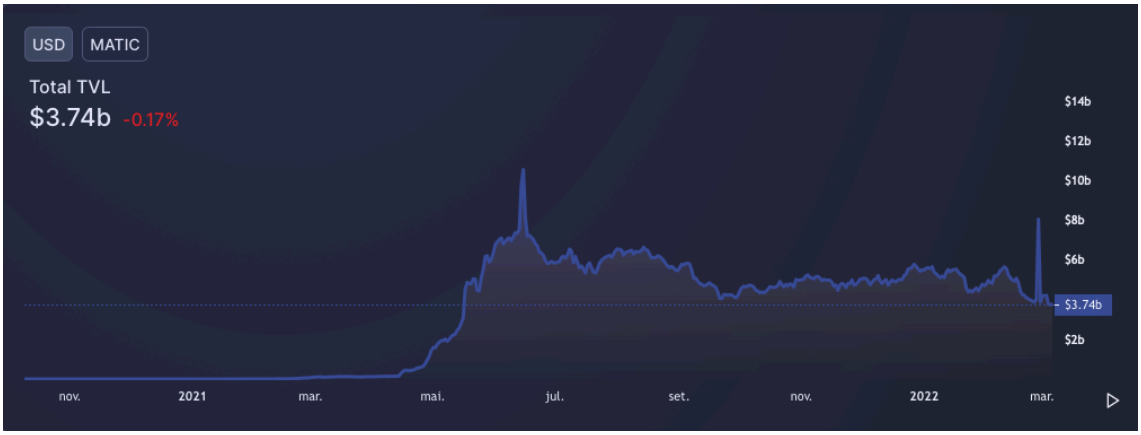

Figura 16: Total TVL na rede *Polygon*

Fonte: Defi Llama.

Em artigo publicado no portal *Medium*, um dos fundadores da rede *Polygon*, Jaynti Kanani (2021), descreve a *MATIC* como uma solução escalável da rede Ethereum que utiliza uma camada

[26] O processo de migração do protocolo Ethereum ocorrerá em diferentes fases, sendo que a primeira já foi iniciada com a instituição da chamada Beacon Chain. Verificar https://ethereum.org/en/upgrades/.

paralela da rede *blockchain* (uma *sidechain*)[27] [28], com base no algoritmo de consenso *Proof of Stake* próprio em conjunto com soluções baseadas no protocolo Plasma.[29]

Kanani (2021) elenca que a escalabilidade é uma considerável barreira para adoção em massa de redes *blockchain*, citando algumas redes que conseguiram uma grande base de usuários, mas que eventualmente apresentavam problemas de lentidão e alto custo transacional, como a própria rede Ethereum.

Na intenção de garantir a eficiência da rede descentralizada e solucionar, mesmo que parcialmente, o problema da escalabilidade, a rede *Polygon* foi desenvolvida utilizando de forma adaptada o Plasma *framework*. O objetivo de construir a *Polygon* tal Plasma é baseado na solução *offchain* do protocolo, em que a execução das transações ocorre fora da *blockchain* principal, no caso, a Ethereum[30] [31].

A estrutura da Polygon propõe o uso de uma rede *blockchain* paralela que, por meio de nós de validação PoS proprietário, replicam registros simplificados de transações na rede principal. Porém, diferentemente de *sidechains* comuns, a rede possui três camadas de validação e segurança. Podemos resumir a arquitetura da seguinte forma:

[27] *Sidechains* são *blockchains* paralelas a uma *blockchain* principal com um algoritmo de validação próprio (PoS, DPoS ou PoA, em geral). Com o desenvolvimento de soluções escaláveis da rede Ethereum, a comunidade de desenvolvedores passou a diferenciar *Sidechains* de soluções de segunda camada, na medida que apenas estas garantem um nível elevado de segurança, pois a confiabilidade é diretamente atrelada à rede principal.

[28] Alguns desenvolvedores caracterizam a rede *Polygon* como uma *commit chain* (cadeia de comprometimento). Acreditamos que essa é uma definição interessante porque leva em consideração fatores adicionais de segurança desenvolvidos pelo protocolo.

[29] Como contrastes do protocolo *Polygon* em relação à uma *sidechain* regular, podemos citar a possibilidade de qualquer usuário realizar a validação de transações (tal fato não ocorre, por exemplo, em grande parte das *sidechains* regulares, em que há uma tendência de centralização do poder de validação (interessante realizar breve leitura disponível em: https://vitalik.ca/general/2021/05/23/scaling.html. Acesso em: 27 de abril de 2022). O efetivo registro das transações na rede principal Ethereum (uso de *Roots*) e o uso dos mecanismos de segurança adicionais, como *heimdall* e *bor chain*s (disponível em: https://medium.com/the-polygon-blog/heimdall-and-bor-1f8f881cd6a4. Acesso em: 27 de abril de 2022).

[30] Disponível em: leanplasma.org. Acesso em: 27 de abril de 2022.

[31] Outro ponto relevante trata-se do Plasma (infraestrutura adaptada com o algoritmo PoS da própria *Polygon*) com uma *sidechain* regular, que a propriedade de ativos pode ser garantida pelo contrato inteligente Plasma na Ethereum e, portanto, podem sobreviver a um ataque à *sidechain*. Em termos simples, se a *sidechain* cair ou o operador for desonesto, os usuários ainda poderão recuperar seus ativos na cadeia principal.

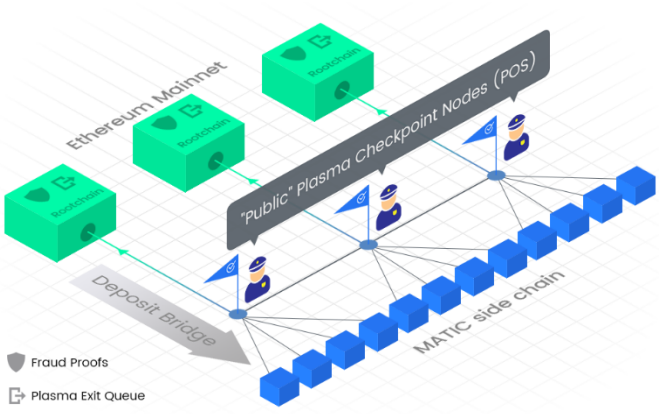

Figura 17: Arquitetura da rede *Polygon* (*MATIC NETWORK*)

Fonte: *What is Matic Network?*

A solução também utiliza mecanismos criptográficos de compromisso de estado (*state commitment*) como forma de registrar uma versão comprimida do estado das aplicações por meio da estrutura de dados chamada *Merkle Trees*.

De acordo com Kanani (2021), os modelos de *blockchains* paralelos, construídos sob adaptações do *framework* Plasma, são estruturalmente efetivos para suportar os mais diversos protocolos de DeFi disponíveis na rede Ethereum, tornando a *Polygon* ainda mais atrativa aos desenvolvedores e usuários.

A adoção de todos os mecanismos acima elencados implica em uma redução significativa das taxas transacionais e a garantia de um elevado nível de segurança, viabilizando, portanto, a execução de um experimento com um menor volume financeiro de forma segura.

4.3.3. Alternativas de escalabilidade

Além das alternativas de escalabilidade nas transações da rede *blockchain* Ethereum já expostas (*side chains* e *commit chains*), existem outros métodos disponíveis e em desenvolvimento contínuo, como os canais de estado (*state channels*) e os recentes *optmistic/ Zk rollups*.

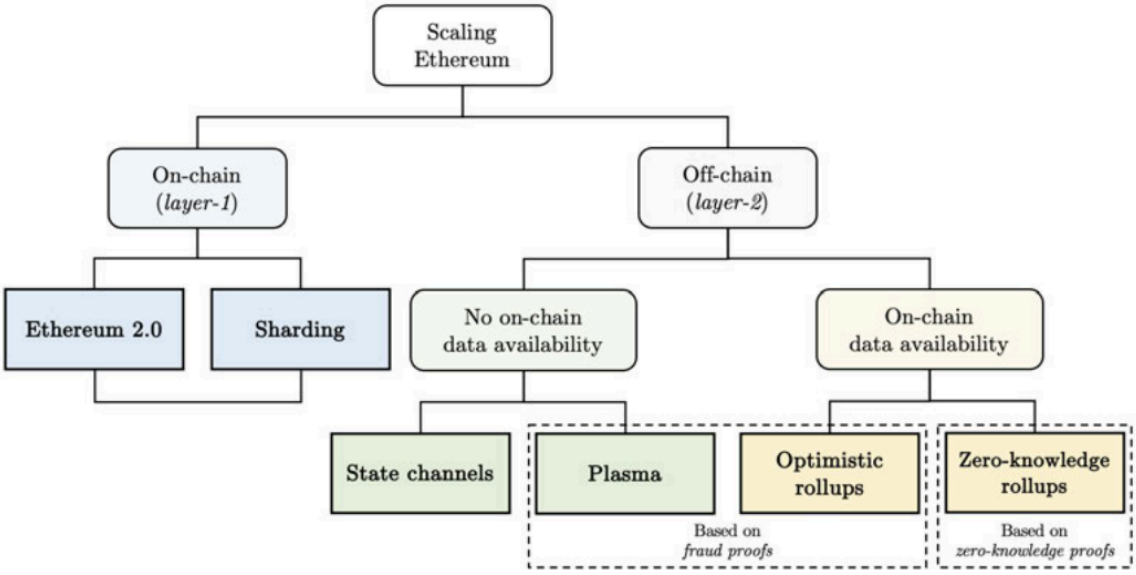

Figura 18: Estrutura de escalabilidade da rede Ethereum

Fonte: Schaffner (2021) (adaptado).

A primeira alternativa é uma das primeiras soluções de escalabilidade para a rede Ethereum, sendo baseada em uma espécie de sistemas de pagamentos, em que a transação entre participantes ocorre fora da *blockchain* (*off-chain*) dentro do contrato inteligente. Só após o usuário solicitar o saque do contrato inteligente que é realizada a publicação do saldo da *blockchain*. Exemplos populares a serem citados, *Raiden Network*[32] (para rede Ethereum) e a *Lightning*[33] (para a rede Bitcoin).

Segundo Schaffner (2021), assim podemos definir canais de estado:

> Os canais de estado são basicamente um canal de interação bidirecional entre dois partidos. Esses canais de estado podem ser baseados em transações multisig ou em contratos inteligentes, onde os participantes concordam previamente com as condições e depositam fundos no canal. Como essas interações ponto a ponto ocorreriam todas no *blockchain* principal, os canais de estado podem ser muito úteis para fornecer uma maneira muito barata e rápida de enviar e receber micro pagamentos. A principal vantagem dos canais estaduais, comparado a uma transação tradicional de *blockchain*, é a finalidade instantânea juntamente com taxas de transação insignificantes. Assim que o conjunto de interações entre as partes terminar, o estado final será publicado e adicionado ao *blockchain* (SCHAFFNER, 2021).

Pelo fato de não suportarem a execução de contratos inteligentes de propósito geral, como AMMs, é esperado que esse tipo de ferramenta de escalabilidade seja cada vez mais incomum.

Já os *rollups* representam o ponto focal de discussão sobre escalabilidade na rede Ethereum, sendo considerados a grande inovação que pode viabilizar transações cotidianas com eficiência e baixo custo. Segundo Sguanci (2021), a ideia por trás dos *rollups* é a execução das transações fora da *blockchain* principal (*off-chain*) e a realização de um registro simplificado de dados simultaneamente.

[32] https://raiden.network/. Acesso em: 27 de abril de 2022.
[33] https://lightning.network/. Acesso em: 27 de abril de 2022.

Assim, *rollups* se diferenciam dos canais de estado e *sidechains*, na medida que estas realizam o registro, de um sumário de um bloco de transações na rede principal e aqueles somente registram uma pequena quantidade de dados na *blockchain* de cada transação específica (BUTERIN, 2021).

Buterin (2021) compreende que a solução de *rollups*, diferentemente do Plasma e canais de estado, é híbrida entre a primeira e a segunda camada, tendo em vista que substitui o uso de dados por computação sempre que possível ao registrar pequena quantidade de dados por transação na rede.

Podemos sintetizar a estrutura de funcionamento de um *rollup* como um contrato inteligente executado na cadeia de blocos da *blockchain* principal que mantém um estado "raiz" contendo balanços das contas, código do contrato, dentre outros.

Nesse sentido, todos os usuários do *rollup* podem realizar a publicação de um *batch*[34], de modo que o contrato inteligente realize a verificação do estado anterior contido no *batch* com o atual estado. Caso a correspondência seja positiva, o contrato opera a alteração para o novo estado. Vejamos um diagrama exemplificativo proposto por Buterin (2021):

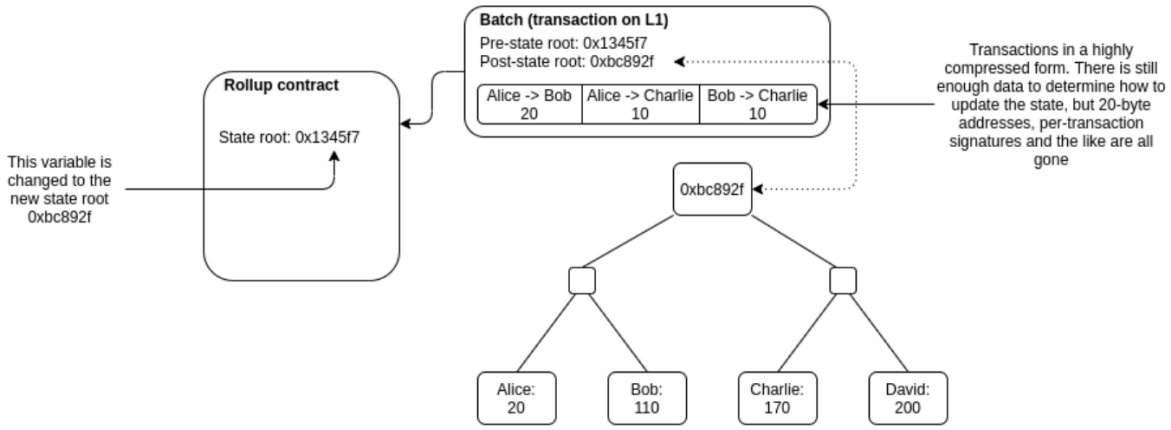

Figura 19: Estrutura funcional de um *Rollup* genérico

Fonte: Buterin (2021).

Contudo, surge um questionamento: como saber se o novo estado proposto para os *Batches* está correto? Até o momento, existem dois modelos de *rollups* para solucionar tal questão*: optmistic e ZK*. O primeiro, utiliza o registro histórico de estados de cada *batch*. Desse modo, caso haja qualquer descoberta de transação fraudulenta, o usuário pode publicar a prova de fraude (*fraud proof*) para a rede, comprovando de modo que, então, o contrato inteligente realize a verificação. Caso a prova seja verídica, o contrato reverte o *batch* falso e todos os posteriores. Nesse caso, é importante destacar o período de retirada da rede, que é de 7 (sete) dias, fornecendo tempo aos usuários protestarem as transações.

[34] O *Batch* se trata de uma coleção de transações comprimidas de forma conjunta com o estado anterior e o novo estado proposto.

Já os *rollups ZK* utilizam-se do método de prova de validação, em que cada *batch* contém um código criptográfico chamado ZK-SNARK, responsável por determinar de forma rápida se o novo estado é correto ou fraudulento.

Assim, como apresentado pelo fundador da Ethereum, Vitalik (2021), acreditamos que os *optmistic rollups* possuem uma aplicabilidade interessante para contratos inteligentes gerais (EVM), levando em consideração a facilidade de implementação e o baixo custo computacional para processamento. Com relação aos ZK *rollups*, devido à sua complexidade técnica de implementação e as vantagens relacionadas com a velocidade de verificação, podem ser melhor utilizados para sistemas de pagamentos ou *Exchanges*, ao menos até o aprimoramento da tecnologia ZK-SNARK.

4.4. Transferência para o protocolo (*bridge*)

Para a realização da transferência do protocolo Ethereum, rede em que foi possível solicitar o saque do saldo de conta da corretora Binance, para o protocolo *Polygon*, foi necessário utilizar o mecanismo de ponte entres redes *blockchain*, conhecidas no setor pela sua tradução literal: *bridges*.

Em síntese, *brigdes* são estruturas que objetivam facilitar a conexão entre dois ecossistemas *blockchain*, viabilizando, assim, a transferência de ativos e informação entre diferentes protocolos (BERENZON, 2021).

Segundo a Fundação Ethereum, as *bridges* são utilizadas para as seguintes finalidades: (i) acesso a menores taxas de transação em soluções de segunda camada da rede principal; (ii) uso de DApps em outras *blockchains*; (iii) exploração de outros ecossistemas *blockchain*; (iv) acesso a *tokens* nativos nos protocolos selecionados.

Contudo, é importante destacar que, como grande parte do ecossistema DeFi, o uso de *bridges* sujeita o usuário a riscos tecnológicos, como invasões e falhas nos contratos inteligentes. Na intenção de mitigar esse risco, a *bridge* selecionada para a transferência dos recursos trata-se da desenvolvida pelo próprio protocolo *Polygon*.

O aplicativo demonstrou elevado grau de usabilidade, deixando evidente o fluxo de transferência e afastando questões complexas que permeiam a transição entre redes *blockchain,* vejamos:

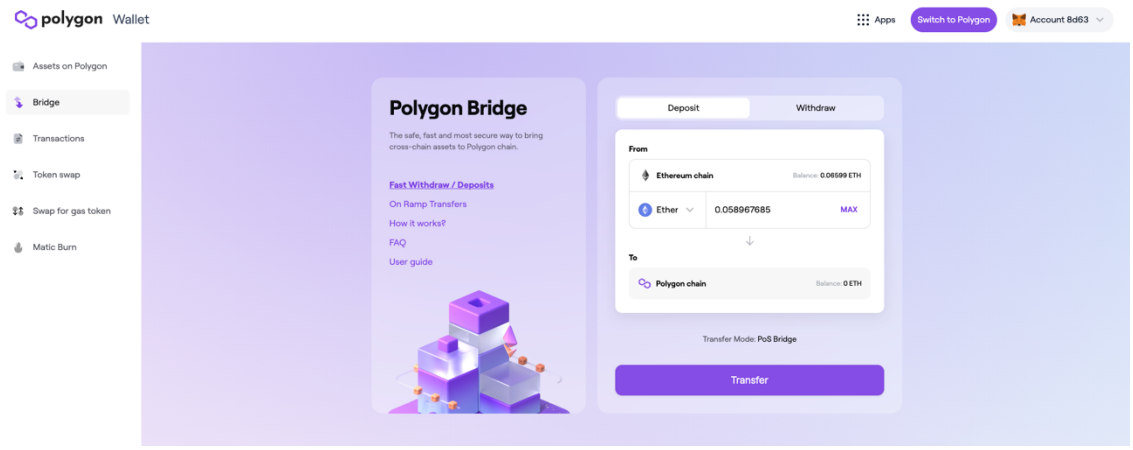

Figura 20: Aplicativo de bridge entre a rede Ethereum e a Polygon

Fonte: Captura de tela realizada pelo Autor.

Como a transferência entre *blockchains* realizada foi da criptomoeda ETH, foi registrado na *wallet* da rede Polygon o ativo WETH (*Wrapped* ETH), que replica o valor do ETH, vejamos:

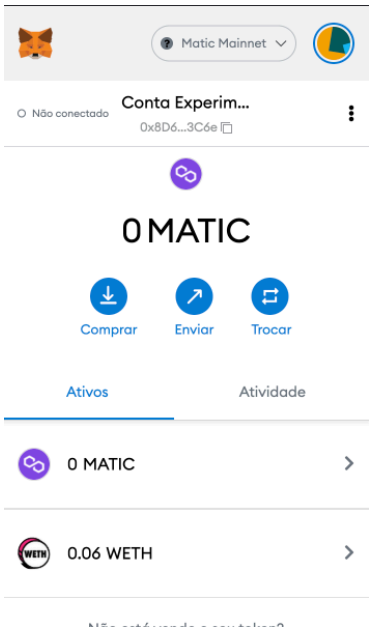

Figura 21: *Wallet* na rede *Polygon* após a transferência

Fonte: Captura de tela realizada pelo Autor.

Para a obtenção de uma quantidade mínima de criptomoedas nativas da rede *Polygon* para o pagamento das taxas de transação dentro da *blockchain*, a própria plataforma da rede disponibiliza uma *Exchange*. Segundo o site, 1 *MATIC* (*token* nativo da *Polygon*) pode pagar as taxas de 1.000 (mil) transações, em média.

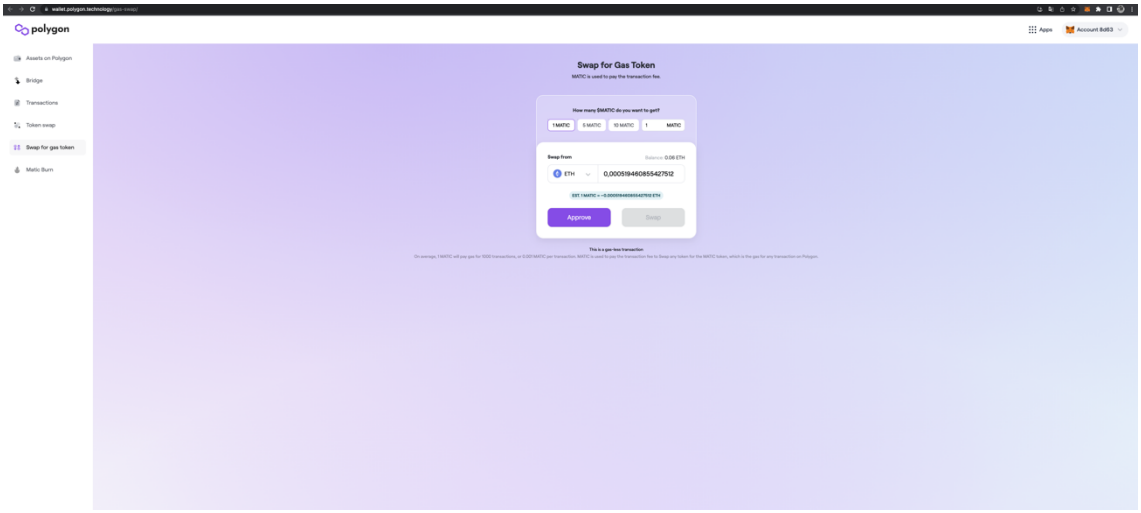

Figura 22: Primeira operação de troca por *tokens* nativos (*MATIC*)

Fonte: Captura de tela realizada pelo Autor.

Posteriormente, para a compreensão do funcionamento dos protocolos, realizamos a mesma operação de *Swap* (troca) em um DApp tipicamente utilizado na rede.

4.5. Operação de *Swap*

A segunda operação realizada no experimento também se trata de um *Swap*, que, em síntese, nada mais é do que uma operação de troca (*trade*) de *tokens*. Tal operação objetivou alocar os recursos da carteira experimental em alguns *tokens*/*stablecoins* estratégicos, conforme exposto abaixo.

O setor de *trading*, em que se enquadram as plataformas de *Exchange*, chamadas de DEXes (*Decentralized Exchanges*), respondem por uma parcela dominante do mercado de finanças descentralizadas, com aproximadamente 64 bilhões de dólares americanos em TVL e 380 protocolos ativos (DEFILLAMA, 2022).

Conforme apontado em relatório elaborado pela gestora de fundos Bitwise Asset Mangement (2021), é possível traçar um paralelo entre DEXes e bolsas de valores do mercado financeiro tradicional, como NYSE (*New York Stock Exchange*), Nasdaq ou B3, no caso brasileiro, mas atentando-se a alguns pontos relevantes.

Para compreender a arquitetura de funcionamento das plataformas de *Exchange*, é importante destacar a diferença entre o tradicional sistema de livro de ordens de operação e o mecanismo mais comum (e estruturante) de organização das operações de *Exchange* em DeFi, o chamado *Automated Market Making* (AMM - em português, formador de mercado automatizado). Sobre o AMM, vejamos as lições de Mohan (2022):

> Em geral, um *Market Maker* é uma instituição que está pronta para comprar ou vender um ativo, gerando lucro com o *spread* de compra e venda: a diferença entre a taxa de venda ou oferta (a taxa pela qual o *Market Maker* vende um ativo) e a taxa de compra (a taxa pela qual o *Market Maker* compra um ativo). Um AMM automatiza isso, permitindo que os operadores realizem ordens com o AMM, que então fornece um preço por meio de um algoritmo. Vale reiterar como esse processo é distinto do

> sistema de livro de ordens, que exige correspondências entre preço e volume de ordens fornecidos por compradores e vendedores (MOHAN, 2022. *Grifos do autor*).

Assim, AMM's são *Smart Contracts* que estabelecem o preço de determinado ativo com base em uma fórmula pré-estabelecida.

Contudo, pode o leitor indagar-se sobre qual seria a origem dos ativos para liquidez. A resposta para tal questionamento é dada no tópico 4.7, abaixo apresentada.

No presente estudo, a *Decentralized Exchange* (DEX) selecionada para a primeira operação trata-se da *QuickSwap*, DApp com a maior movimentação e TVL (aproximadamente 800 milhões de dólares) dentro do protocolo *Polygon*. E o primeiro *token* selecionado para operação trata-se do *MATIC*, *token* nativo da rede *Polygon*.

Tokens nativos são fundamentais para o pagamento de taxas transacionais dentro da rede *blockchain* selecionada, além de atribuírem ao titular do *token* o poder de voto para eventuais alterações no protocolo da rede (governança descentralizada).

O *token* que já possuíamos era o ETH, nativo da rede Ethereum e replicado na *Polygon* sob o código WETH (*Wrapped* ETH), ou seja, com o mesmo o valor do *token* na rede originária.

Assim, realizamos a operação de *Swap* de *tokens* WETH para *MATIC* de aproximadamente 10% (dez por cento) do valor total sob gestão.

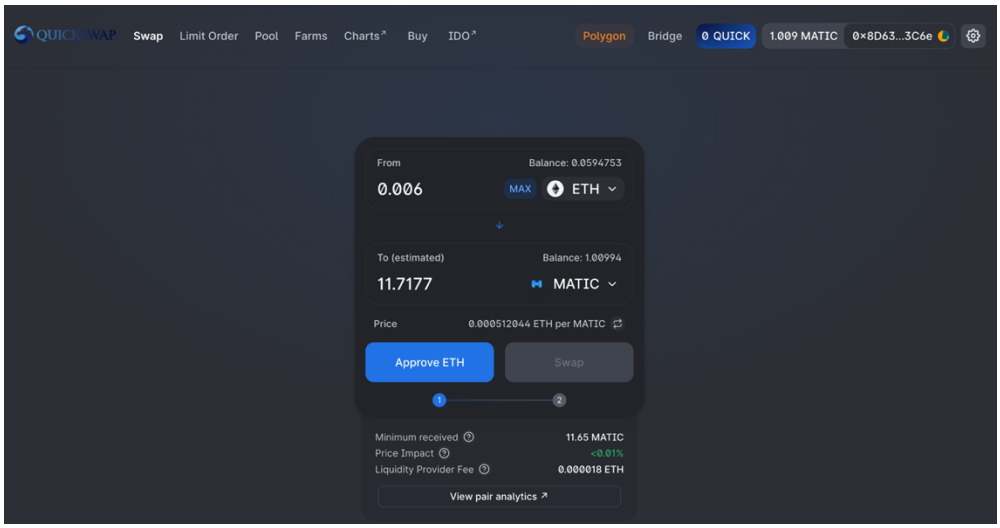

Figura 23: Operação de *Swap* entre ETH e *MATIC*

Fonte: Captura de tela realizada pelo Autor.

Merece destaque a taxa repassada aos provedores de liquidez, figura abordada no tópico 4.7.

Assim, após a confirmação da transação de *swap*, foi possível observar a estrutura de funcionamento da transferência por meio do portal de transações da rede *Polygon*[35], vejamos:

[35] Disponível em: polygonscan.com. Toda rede *blockchain* disponibiliza aos usuários uma plataforma de controle de todas as transações realizadas na rede, garantindo transparência e a imutabilidade das transações de estados.

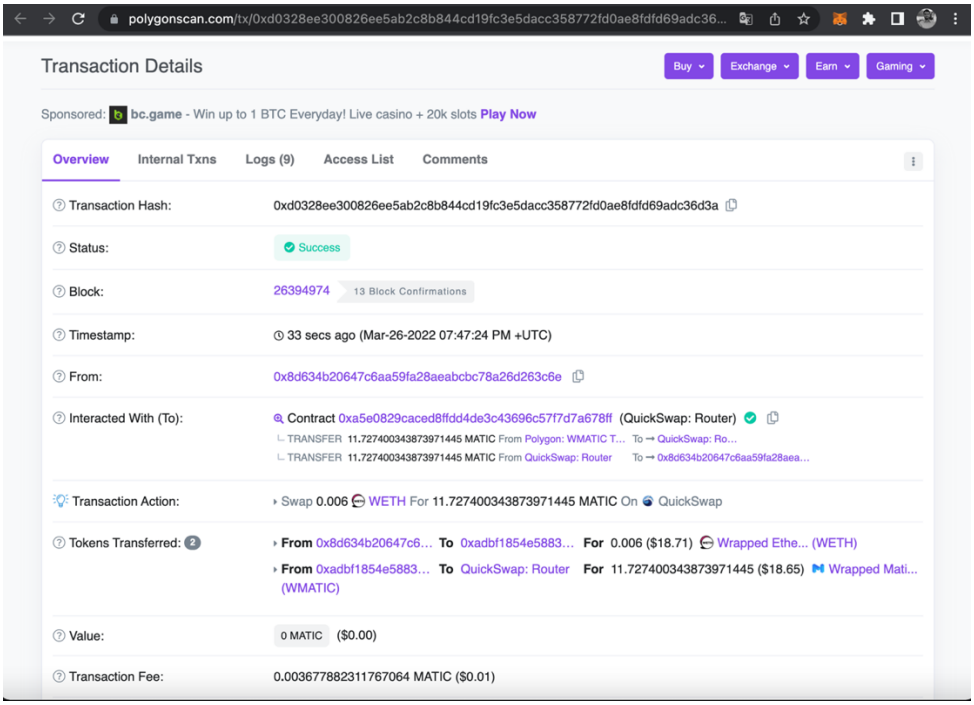

Figura 24: Detalhes da transação de *swap* registrados na rede *Polygon*

Fonte: Captura de tela realizada pelo Autor.

De acordo com o registro da transação, observamos que ao realizar uma operação de *swap*, é realizado o envio dos *tokens* (no caso, WETH) para o endereço do contrato inteligente, de modo que o próprio contrato realiza a operação (incluindo operações internas) e deposita no endereço final do usuário.

4.5.1. *Swap* por *stablecoins* (DAI)

Conforme já exposto no tópico 3.3.4.1, existem diversas opções de *stablecoins* em circulação. Contudo, para o presente experimento, selecionamos apenas uma das opções, levando em consideração os riscos e a ofertas de liquidez disponíveis nas maiores plataformas de *Exchange*.

Na intenção de mitigar o risco de transparência de *stablecoins fiat colletarized*, foi selecionado *stablecoin* cripto-colateralizado DAI, desenvolvido e mantido pela MakerDAO.

Ademais, analisando as ofertas de liquidez disponíveis no DApp *Quickswap*, observamos uma taxa de retorno considerável em ativos correlacionados com a *stablecoin* DAI.

A operação de *swap* também foi realizada por meio do DApp *QuickSwap* de modo similar ao swap por *tokens* MATIC.

4.5.2. Critérios para análise de criptoativos na composição da carteira

As peculiaridades de estruturação do mercado de criptoativos apresentadas anteriormente evidenciam a impossibilidade do uso exclusivo de metodologias fundamentalistas tradicionais para determinação do grau de risco de investimento em ativos digitais.

Indicadores fundamentalistas defendidos por Benjamin Graham e David Dodd (1894), como o lucro por ação, valor patrimonial, faturamento e resultados financeiros, por exemplo, são, em geral, inaplicáveis ao contexto de criptoativos, dada a natureza descentralizada dos projetos.

Ocorre que, durante o curso do presente experimento, nos deparamos com a necessidade de estabelecer um método, mesmo que genérico, para determinar quais criptoativos iriam compor o portfólio de investimentos. Assim, na contramão da tendência especulativa que permeia o mercado de cripto, propomos, de forma genérica, tendo em vista que este não é o objeto propriamente dito do presente trabalho, alguns indicadores qualitativos e quantitativos que podem nortear a análise de atratividade de projetos de criptoativos.

Nessa senda, separamos a análise em 3 (três) grandes grupos, sendo dois quantitativos e um qualitativo, são eles:

- Métricas Internas da Infraestrutura do Projeto;
- Métricas Financeiras do Projeto; e
- Métricas Qualitativas de Análise do Projeto.

O primeiro grupo, de métricas internas da infraestrutura do projeto, propõe uma análise do algoritmo de consenso utilizado, de modo a identificar eventual taxa de *hash*[36](caso de redes PoW), valor travado em *staking* (caso de redes PoS, DPoS, dentre outras), processamento de transações por segundo, volume histórico de transações da rede, número de endereços ativos e valores das taxas de transação (este, inclusive, um dos motivos que norteou a seleção da rede *Polygon*).

A análise das métricas financeiras do projeto é diretamente relacionada com critérios quantitativos relativos às condições de negociação do ativo, como a capitalização de mercado (TVL), a análise de liquidez (volume negociado) e a oferta de *tokens*.

Por fim, o último grupo propõe uma análise qualitativa dos projetos de criptoativos, objetivando identificar o propósito de criação do ativo e o seu potencial de crescimento. Assim, propomos realizar uma análise dos *White Papers* dos projetos, de modo a identificar funcionalidades do *token*, a infraestrutura de validação adota, equipe de desenvolvedores e, principalmente, o chamado *Tokenomics*.

Em síntese, a análise dos *Tokenomics*, ou seja, a economia do *token*, procura evidenciar os aspectos de oferta e demanda de um *token*, considerando questões relativas ao controle inflacionário da emissão e a estrutura de incentivos dentro da rede.

Critérios relacionados ao contexto macroeconômico, por exemplo, aspectos político-sociais, também são fatores importantes, como podemos observar no recente caso da guerra entre a Rússia e a Ucrânia, em que, como resultado das sanções estrangeiras à Rússia, a adoção de criptoativos ganhou considerável repercussão (ZANATA, 2022).

Como dito anteriormente, não há um método comprovado e certo de realizar a análise de criptoativos, porém, este subtópico se destina a esclarecer quais foram os critérios adotados para a

[36] A taxa de *hash* é responsável por mensurar o grau de atratividade aos validadores de transações para manutenção do funcionamento da rede.

seleção de ativos durante a realização do experimento, sendo útil aos leitores para eventual definição de uma estratégia de investimentos.

4.6. Operação de *Staking*

Levando em consideração as restrições de escalabilidade e sustentabilidade de redes fundadas em algoritmos PoW, as *blockchains* estruturadas sob o algoritmo de consenso PoS ganharam popularidade e emergiram como uma saída para protolocos PoW já consolidados, como o caso da Ethereum (IRRESBERGER, 2021).

Sob a ótica dos algoritmos baseados no PoS, caso do utilizado pelo protocolo *Polygon*, a validação ocorre pela seleção pseudoaleatória de validadores com base em critérios relacionados com o valor em *stake* (depositado), a riqueza do nó e tempo de participação (VITALIK, 2017).

Assim, o usuário que realiza a validação de transações em redes *blockchain* baseadas no PoS é recompensado por meio do depósito de *tokens* nativos da rede, operação de investimento comum para obtenção de renda passiva, também chamada de *staking.*

A operação de *staking* pode ser realizada de duas formas distintas: (i) o usuário realiza, por conta própria, a validação de um nó da rede por meio da retenção de determinada quantidade de *tokens* nativos, opção que implica em custos de manutenção e *hardware* ou (ii) o usuário delega os *tokens* para determinado nó (também chamado de *pool*) já existente, sendo que este realiza a distribuição proporcional aos participantes e realiza a retenção de determinada taxa transacional referentes aos custos de manutenção (CONG *et al*., 2022).

Importante destacar que as operações de *staking* devem ser realizar na *blockchain* mãe, ou seja, aquelas em que são desenvolvidas eventuais soluções de escalabilidade, como é o caso da rede *Polygon*, desenvolvida paralelamente a rede Ethereum.

Para a realização do presente experimento, não foi possível realizar a operação de *staking* propriamente dita, tendo em vista o período mínimo necessário era superior ao tempo de estudo e a opção de abertura de uma *pool* própria se demonstrou completamente inviável, considerando os altos custos operacionais. Contudo, para analisar o protocolo de forma mais completa, realizamos uma comparação dos retornos disponibilizados por um simulador de retornos (próprio do protocolo) de *pools* (nós) de *staking* na Polygon, vejamos:

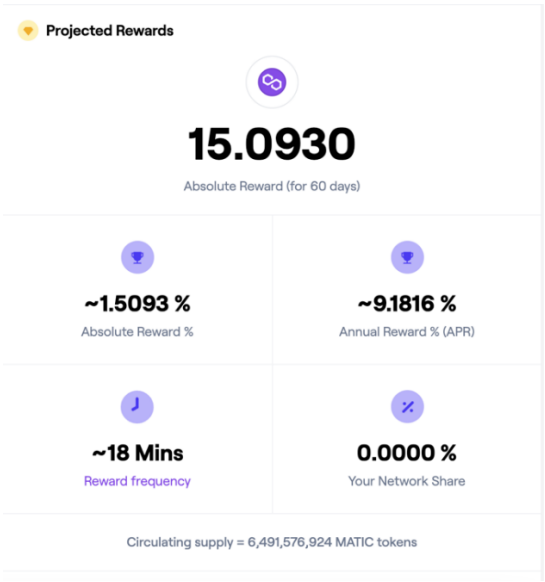

Figura 25: Simulação de retorno para operação de *staking* na rede *Polygon*

Fonte: Captura de tela realizada pelo Autor.

Nota-se que as taxas de retorno são atrativas, chegando a 9,18% (calculados em juros simples) ao ano na hipótese de retenção dos *tokens* por 60 (sessenta) dias, sem considerar a valorização ou desvalorização do *token* em relação a moedas fiduciárias.

Merece destaque que a operação de *staking* difere da operação de empréstimo, na medida que esta é relativa a recompensas por manutenção da rede e aquela é relacionada com a taxa paga por determinado usuário que realiza o empréstimo.

Por fim, analisando os riscos da operação, importante ressaltar a opinião de Gersbach *et al*. (2022), que elenca um risco sistêmico de possível falha no mecanismo de recompensas para a validação de transações de rede PoS. O argumento estrutura-se no fato de que, com o crescimento da rede (em níveis de volumetria e número de transações), os mecanismos de incentivo disponibilizados pelo protocolo são gradualmente reduzidos, implicando com que bons agentes da rede (i.e. agentes não maliciosos, que objetivam validar as transações de forma honesta) deixem de fornecer o serviço de validação na forma de nós e abrem espaço para agentes maliciosos realizarem as validações fraudulentas.

Assim, há um claro impasse sobre a metodologia de manutenção de recompensas atrativas para agentes validadores de transações.

4.7. *Pools* de liquidez e *Yield Farming*

Conforme já apresentado no tópico 4.4, as operações de *Swap* em *exchanges* descentralizadas são realizadas por meio da execução de contratos inteligentes baseados na estrutura de *Automated Market Making*, ou seja, capazes de automatizar as transações sem a dependência de agentes terceiros (como a B3, no caso do mercado financeiro brasileiro) para estabelecerem a relação *preço vs.* volume de negociação por compradores e vendedores dos ativos.

A liquidez decorre de um importante mecanismo das finanças descentralizadas: as *pools* de liquidez, essencial para a manutenção do funcionamento da rede, pois tal estrutura viabiliza a garantia de fluidez dentro das negociações de *tokens* no ecossistema e elimina a necessidade de um agente garantidor para oferta de ativos para trocas.

A estrutura de organização das *pools* de liquidez é relativamente simples, sendo essencialmente formada por 3 (três) componentes: o provedor de liquidez, o comprador/vendedor do ativo e o contrato inteligente desenvolvido dentro da DEX.

A primeira ação é do provedor de liquidez, que realiza o depósito de um par de *tokens* na mesma proporção dentro do contrato inteligente. Assim, o depósito dos *tokens* é adicionado à reserva da *pool* de liquidez e oferecido ao comprador/vendedor do ativo por meio da aba de *Swap* do protocolo. O provedor de liquidez recebe o incentivo do protocolo por meio de *tokens* das pools, chamados de *LP Tokens*, ou *Liquidity Pool Tokens*. Em síntese, *LP Tokens* representam um direito dos provedores de liquidez para determinada remuneração pelas transações realizadas como *Swap* por meio da *pool* de liquidez, conforme a parcela de contribuição. Assim, os *LP Tokens* podem ser negociados no mercado, transferidos para outro usuário ou depositados para novos ganhos (a última opção também é conhecida como *farming,* abordada logo abaixo) (HEIMBACH *et al*., 2021). Vejamos um diagrama exemplificativo:

Figura 26: Diagrama de funcionamento de uma *pool* de liquidez

Fonte: Uniswap

Importante destacar que o criador da *pool* de liquidez é o responsável por determinar a proporção de *tokens* para trocas. Ou seja, fundamental atentar-se à proporção utilizada e evitar eventuais perdas com arbitragem de valores.

No caso do presente experimento, foi realizado o provimento de liquidez para os seguintes *tokens*: DAI/ETH na proporção 1 DAI para 0.000286195 ETH. Levando em consideração o preço médio de mercado para o *Swap* dos *tokens* (1 DAI para 0.000285417 ETH), acreditamos que a margem de arbitragem estava dentro do aceitável. Nesse sentido, abaixo podemos observar o procedimento para provimento de liquidez:

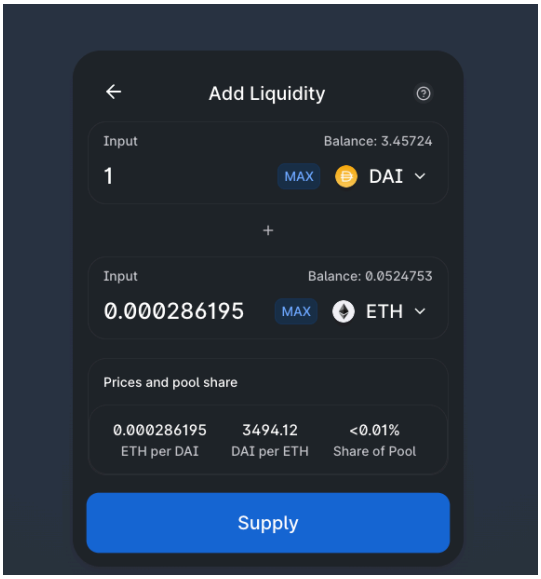

Figura 27: Primeiro passo para provimento de liquidez

Fonte: Captura de tela realizada pelo Autor.

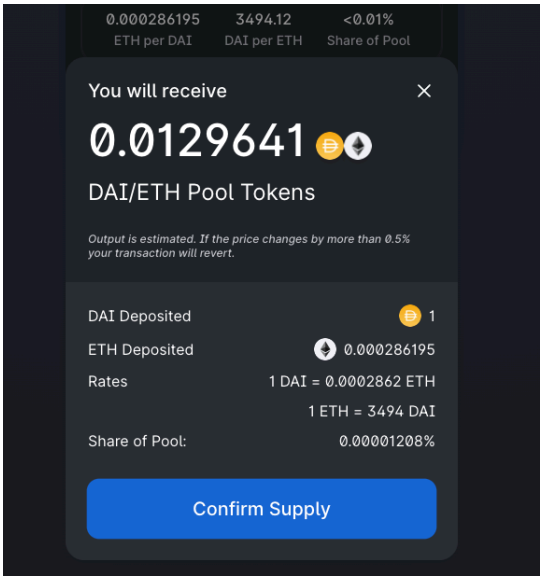

Figura 28: Segundo passo para provimento de liquidez

Fonte: Captura de tela realizada pelo Autor.

No protocolo *Quickswap*, DEX selecionada para a operação, a porcentagem das taxas de transações repassada aos provedores de liquidez é de 0,25% por meio de *LP Tokens*, sendo que 0,05% das taxas são repassadas a plataforma como remuneração aos detentores de *tokens* de governança do protocolo da *Quickswap* (*token QUICK*).

Como forma de incentivo ao provedor de liquidez, em geral, os protocolos de *Exchanges* (DEX´es) disponibilizam *Farms* para o depósito (*staking)* dos *LP tokens*. A remuneração é realizada por

meio de *tokens* nativos da rede[37]. Esse tipo de operação é conhecido como *Yield Farming*, interessante ferramenta para formar uma estratégia de alocação.

Destaca-se que é possível realizar o depósito dos *LP tokens*, não sendo necessariamente vinculado à DEX em que foi realizado o provimento de liquidez. Importantes exemplos de plataformas de *farming* reconhecidas no mercado*: harvest.finance* (*FARM*) *e yearn.finance* (*YERN*), sendo a última disponível apenas nas redes Ethereum, Fantom e Arbitrum.

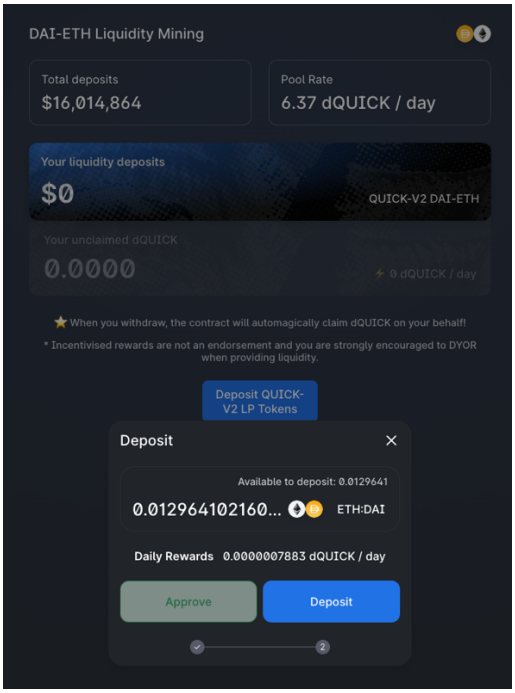

Figura 29: Depósito dos *LP tokens*

Fonte: Captura de tela realizada pelo Autor.

Após aproximadamente uma semana de depósito, foi solicitado o saque do depósito realizado a título de *liquidity mining*. Então, automaticamente, o protocolo realizou o depósito *tokens* dQUICK para *staking* da própria plataforma, de modo que, caso o usuário solicite o saque, os *tokens* dQQUICK são queimados e, finalmente, ele receberá o *token* QUICK (*token* de governança da Exchange *Quickswap*). Destaca-se que é possível realizar a troca deste *token* por qualquer outro *token* em qualquer *exchangue*, incluindo a própria *Quickswap*.

[37] O usuário é remunerado com o dQUICK, que se trata de um *token* paralelo (proporcionalmente calculado) ao *token* nativo QUICK. O dQUICK é uma parcela das taxas que a plataforma ganha com as transações. Com o crescimento de depósitos de *tokens* de governança da plataforma, o valor do *token* QUICK por dQUICK tende a aumentar, funcionando, portanto, como outra forma de remuneração ao usuário da rede.

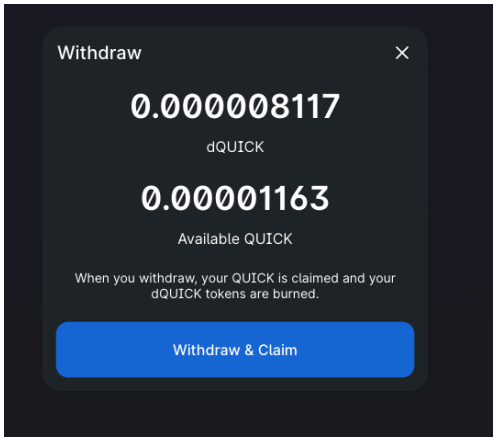

Figura 30: Resultado do saque dos *LP tokens* depositados na forma de *liquidity mining*

Fonte: Captura de tela realizada pelo Autor.

Outro ponto importante é que a plataforma *Quickswap* ainda disponibiliza outra forma de remuneração como método de incentivo ao usuário para permanência na plataforma. É possível ser remunerado com *tokens* menos conhecidos (e com taxas de retorno mais atrativas) por meio de *yield farming* na aba *Dragon Syrup*, inclusive, sem o risco da volatilidade de ativos.

4.7.1. *Impermanent loss*

No curso do experimento, observamos um importante risco sistêmico no fornecimento de liquidez, o risco de perda impermanente, ou, em inglês, *impermanent loss*.

Como descrito no tópico 4.7, o fornecimento de liquidez para operações de *swap* é uma operação comum no ecossistema DeFi, em razão dos ganhos com taxas de transações (funcionando como um intermediário de cartão, por exemplo) e a possibilidade de ganhos consideráveis com a estratégia de *Yield farming*.

Contudo, a perda impermanente, caracterizada pela diferença entre o valor obtido por meio do fornecimento de liquidez e o eventual resultado caso o usuário tivesse mantido os recursos em depósito na própria *wallet*, pode ocorrer em razão do rebalanceamento automático das *pools* de liquidez com a compra e venda de ativos.

Para tornar mais simples a compreensão do risco, vejamos um exemplo hipotético: supondo que Alice decida alocar[38] $20.000,00 dólares em uma *pool* de liquidez DAI/ETH (um *stablecoin* e o *token* nativo da rede Ethereum). Assim, Alice deverá realizar o depósito dos ativos em mesma proporção, ou seja, o mesmo valor aplicado em cada tipo de criptoativo.

Tabela 4: Depósito em Pool de Liquidez (Perda Impermanente)

[38] Os valores utilizados para o exemplo não condizem com o real valor do ativo.

CRIPTOATIVO	PREÇO	QUANTIDADE DEPOSITADA	VALOR TOTAL
DAI (*token* x)	$1 (um dólar)	10000 (dez mil)	$10.000,00 (dez mil dólares)
ETH (*token* y)	$500 (quinhentos dólares)	20 (vinte)	$10.000,00 (dez mil dólares)

Fonte: Elaborado pelo Autor.

Assim, Alice possuirá uma participação em todas as taxas de transações desses ativos por permitir que outros usuários comprem e vendam DAI/ETH sem a necessidade de um intermediário. Portanto, receberá um *LP token* relativo ao direito do depósito realizado.

Suponhamos, ainda, que o valor do ETH aumente para $550 (quinhentos e cinquenta dólares). Nesse caso, surge uma oportunidade de investimento aos que chamamos de árbitros, pois observam a disparidade entre o preço real do ativo e o disponível para operação.

Vale relembrar que, em grande parte das *pools* de liquidez, a estrutura de funcionamento é baseada em um contrato inteligente que mantém a mesma proporção de *tokens*, no caso (50% de DAI e 50% de ETH).

Desse modo, na intenção de manter a proporção de valor final dos ativos, para compreender o cálculo, devemos, primeiramente, determinar a constante de proporção. A fórmula para determinar a constante entre a quantidade depositada de cada *token*:

$$k = x * y \qquad (2)$$

No caso do exemplo, o valor de *k* é igual à 200.000 (duzentos mil), produto entre os 20 *tokens* de ETH e os 10.000 *tokens* de DAI depositados.

Posteriormente, aplica-se a fórmula fundamental do *Automated Market Maker* (AMM). Para o cálculo, considera-se a constante acima determinada e a razão entre os valores dos *tokens* (*r*), em que *t* representa o momento de análise (1 – momento inicial e 2 – segundo momento), vejamos:

$$x_t = \sqrt{k/r_t} \qquad (3)$$

$$y_t = \sqrt{k * r_t} \qquad (4)$$

A razão entre os valores para *t* iguais a 1 e 2 são, respectivamente, 500 e 550. O resultado abaixo obtido retrata o novo equilíbrio disponível na *pool* de liquidez.

$$x_1 = \sqrt{200.000/500}$$

$$x_1 = 20$$

$$y_1 = \sqrt{200.000 * 500}$$

$$y_1 = 10.000$$

$$x_2 = \sqrt{200.000/550}$$
$$x_2 = 19{,}07$$

$$y_2 = \sqrt{200.000 * 550}$$
$$y_2 = 10.488{,}08$$

O resultado do equilíbrio de *tokens* após a valorização do ativo e da atuação dos arbitradores na compra de ativos potencialmente desvalorizados pode ser resumido na tabela abaixo.

Tabela 5: Comparação entre os diferentes valores totais da *pool* liquidez

	DAI	VALOR UNITÁRIO	ETH	VALOR UNITÁRIO	VALOR TOTAL
ANTES DA ARBITRAGEM	10.000	$1	20	500	$10.000,00
APÓS A ARBITRAGEM	10.488,08	$1	19,07	550	$20.976,59

Fonte: Elaborado pelo Autor.

Tabela 6: Comparação entre valor disponível na *pool* de liquidez x hipótese de *staking* na *wallet*

	DAI	VALOR UNITÁRIO	ETH	VALOR UNITÁRIO	VALOR TOTAL
APÓS A ARBITRAGEM	10.488,08	$1	19,07	550	$20.976,59
HIPÓTESE DE DEPÓSITO NA *WALLET*	10.000	$1	20	550	$21.000,00

Fonte: Elaborado pelo Autor.

Nesse sentido, a diferença entre os valores da última tabela, $23,41 (vinte e três dólares e quarenta e um centavos), representa o *impermanent loss* do usuário.

É incontroverso que a adoção de *stablecoins* como parte do investimento em *pools* de liquidez pode diminuir o risco de perda impermanente. Ademais, necessário atentar-se a eventuais possibilidades de arbitragem no mercado e as tarifas das *pools* que se pretende depositar.

O risco da perda impermanente, apesar de relevante e fundamental análise, não deve ser um fator que inviabilize integralmente o investimento em *pools* de liquidez. A estratégia de fornecimento de liquidez possibilidade retornos que podem compensar eventuais perdas impermanentes, como taxas cobradas em transações e o *yield farming.*

Algumas soluções recentes, inclusive, eliminam o risco de perda impermanente, como a plataforma Bancor[39], porém com alguns *trade-offs* relacionados ao prazo mínimo e máximo de depósito.

4.8. Empréstimo

A parte final do experimento foi a realização de um empréstimo na rede financeira descentralizada. Para tanto, foi selecionada o protocolo AAVE[40], que, com TVL aproximado de 1 bilhão de dólares, trata-se da maior plataforma de movimentação dentro da rede *Polygon*.

A AAVE possibilita ao usuário o produto financeiro de empréstimo, tanto para fornecê-los como para realizá-los. Assim, por meio de uma interface intuitiva e simples, é relativamente fácil compreender a estrutura de funcionamento do protocolo.

Ademais, os usuários da rede AAVE são recompensados com *tokens* de governança da rede, possibilitando a participação em alterações, discussões e melhorias no protocolo. O *token* pode ser depositado na própria rede para retornos ainda maiores.

O primeiro passo do experimento de empréstimo foi realizar o fornecimento de liquidez, ou seja, o depósito de recursos (em uma estrutura semelhante aos *pools* de liquidez) para que outros usuários realizem empréstimos (*lending).*

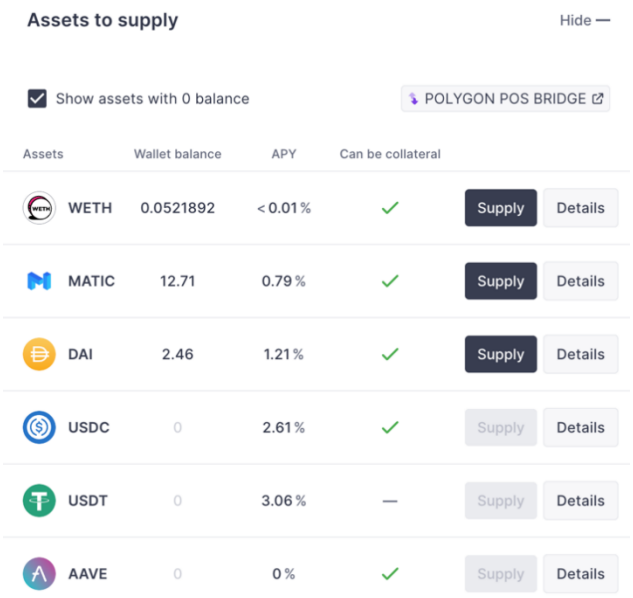

Figura 31: Fornecimento de liquidez para empréstimos

Fonte: Captura de tela realizada pelo Autor.

[39] https://www.bancor.network/. Acesso em: 27 de abril de 2022.
[40] https://app.aave.com/. Acesso em: 27 de abril de 2022.

Observa-se que as taxas de retorno para o depósito não são muito atrativas, em especial no caso de *stablecoins* consideradas mais seguras, como o DAI e USDC. Necessário ressaltar que as taxas de retorno dos empréstimos são diretamente proporcionais à oferta e demanda do ativo, i.e., quanto maior a oferta do ativo para empréstimo e menor for a sua procura, menores serão as taxas de remuneração ao mutuante.

Para fins meramente experimentais, foi realizado o depósito de dez dólares do ativo DAI.

Merece destaque a coluna relativa à possibilidade de alocar o ativo como colateral, uma das peculiaridades abordadas posteriormente sobre o funcionamento de empréstimos no ecossistema DeFi.

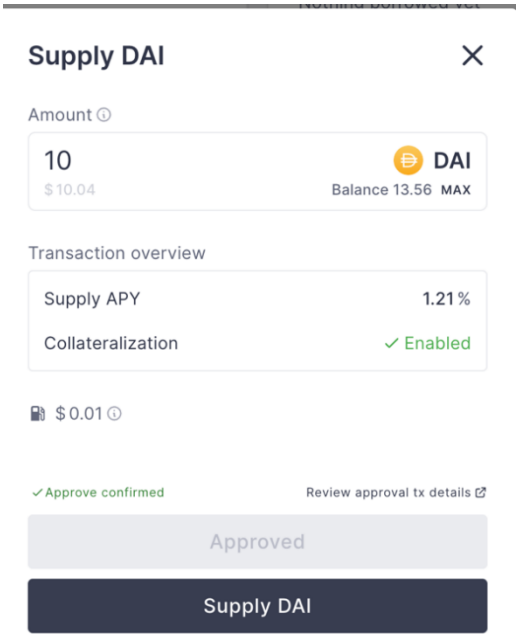

Figura 32: Efetivação do depósito na AAVE

Fonte: Captura de tela realizada pelo Autor.

Após a conclusão do depósito, foi realizado um empréstimo do *token LINK* (*borrowing)*. Observa-se que a plataforma realiza o cálculo da quantidade de *tokens* possíveis para realizar o empréstimo. O valor é diretamente relacionado com a garantia colateral oferecida (no caso do DAI, o potencial de empréstimo é igual a 75% (setenta e cinco por cento) do valor colateralizado).

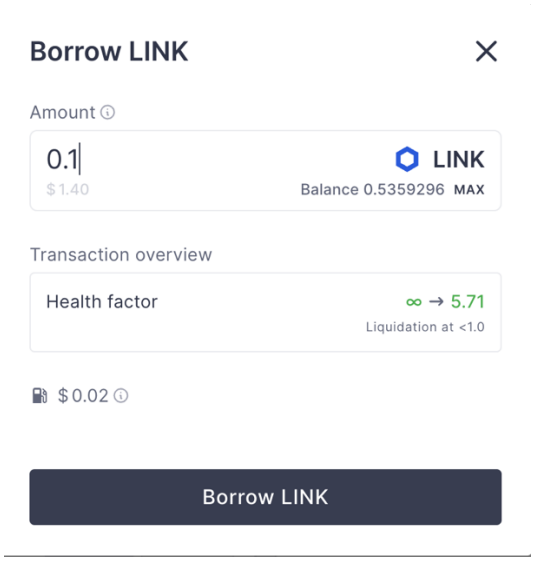

Figura 33: Realização de empréstimo na plataforma AAVE

Fonte: Captura de tela realizada pelo Autor.

Conforme observado, uma das principais diferenças do empréstimo no sistema financeiro descentralizado em comparação com o sistema tradicional, é a necessidade de aportar recursos com valor superior ao empréstimo realizado, também chamado de overcolateralização. O propósito por trás da deste fenômeno é relacionado com a alta volatilidade de criptoativos, de modo que a plataforma possui mecanismos de liquidação dos ativos em garantia na hipótese de diminuição do valor do ativo emprestado a um valor inferior ao garantido[41].

Deve indagar-se o leitor, qual seria o motivo de realizar um empréstimo dando recursos em garantia com maior valor? A resposta deste questionamento pode ser uma comparação com sistema financeiro tradicional: suponhamos que um investidor possua um imóvel e acredite que o dólar será valorizado em relação ao real em um curto prazo. Contudo, não é possível realizar a venda imediata do imóvel, tendo em vista a morosidade de transferência do bem e os custos implicados na transação. Assim, o usuário solicita um empréstimo de um valor consideravelmente inferior ao valor do seu imóvel, o colocando como garantia de cumprimento da obrigação e realizando a compra do ativo que acredita valorizar.

No caso de criptoativos, apesar de terem liquidez teórica semelhante, o empréstimo pode ser uma interessante ferramenta para especular a valorização de ativos, inclusive, alocando recursos como *stablecoins* em garantia. Alguns usuários também utilizam recursos emprestados para alavancar a posição em outras plataformas de empréstimo, os depositando como garantias.

Outro ponto importante sobre os protocolos de empréstimo são os chamados *flash loans* (empréstimos rápidos). Em síntese, trata-se de um tipo de empréstimo sem garantia.

Os *flash loans* utilizam *smart contracts*, que não permitem a troca de fundos, a menos que o mutuário possa pagar o empréstimo antes do término da transação. Caso contrário, o *smart contract*

[41] Na Plataforma AAVE, o grau de risco de liquidação dos ativos em garantia é descrito no item *health factor.*

cancela a transação. Em geral, os *flash loans* utilizam outros *smart contracts* em uma estratégia de negociação projetada para obter lucro por meio da execução de uma negociação em torno de uma oportunidade de arbitragem. Nesse sentindo, desde que a estratégia possa ser executada instantaneamente e gere lucro suficiente para pagar o empréstimo mais juros e taxas, os usuários podem usar os *flash loans* para obter acesso a grandes quantidades de capital sem garantia inicial.

Acreditamos que a estrutura de funcionamento das plataformas de empréstimo é muito simples e representa riscos sistêmicos de liquidez na hipótese de utilização dos empréstimos como mecanismos de alavancagem. Além do exposto, é fundamental atentar-se ao risco operacional-tecnológico dos protocolos utilizados.

5. APLICAÇÃO DA ANÁLISE MULTICRITÉRIO E DO AHP

Após a análise da bibliografia disponível sobre o tema, bem como a realização do experimento prático que objetivou compreender a estrutura de funcionamento do ecossistema DeFi, foi possível determinar os riscos com maior relevância presentes no setor.

5.1. Estrutura hierárquica de riscos

Conforme descrito na metodologia, foi realizada a decomposição dos riscos (critérios) em uma estrutura hierárquica, vejamos a figura 34. No caso do presente estudo, não foi realizada a definição das possibilidades decisórias, tendo em vista que eventual comparação entre critérios seria tendenciosa pelo fato de riscos atribuírem um caráter negativo à intenção de investir no setor.

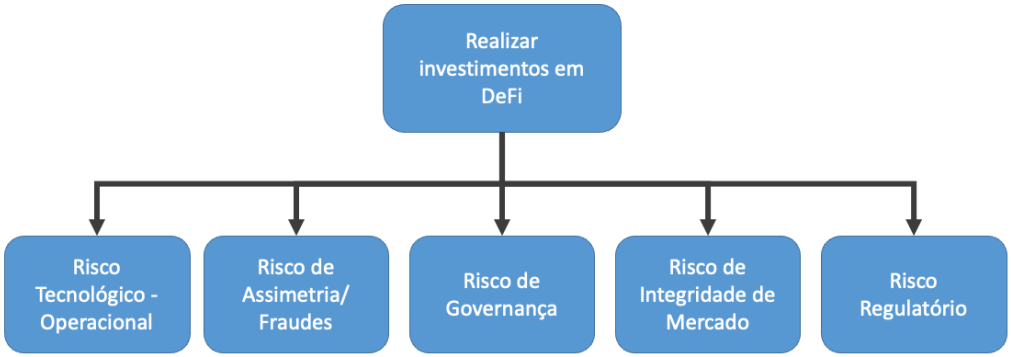

Figura 34: Estrutura hierárquica de critérios

Fonte: Elaborada pelo autor.

Neste caso, classificamos os investimentos em DeFi como o objetivo geral e, abaixo dele, os riscos (critérios) que o influenciam.

5.2. Definição dos riscos categorizados

Cada um dos riscos elencados na estrutura hierárquica é justificado abaixo.

(i) Risco de assimetria e fraudes

Aplicações em DeFi representam um considerável risco de assimetria ao investidor individual. Durante o curso do experimento, observamos que grande parte dos DApps estudados não disponibilizam um material informativo claro e acessível aos investidores, de modo que, apesar da própria infraestrutura *blockchain* garantir transparência ao registro de transações, o conhecimento técnico relativo aos *smart contracts* representa uma barreira para a tomada de decisões de investimento.

Segundo relatório de riscos elaborado pela *International Organization of Securities Commissions* – IOSCO (2022), alguns produtos disponíveis na rede DeFi requerem um conhecimento técnico ou outra expertise que nem todos os investidores possuem. Nesse sentido, existe o risco de informações obscuras sobre vantagens tecnológicas com determinados participantes em face de investidores de varejo, contribuindo, portanto, para um cenário de desigualdade.

Ainda dentro do risco de assimetria, não é raro o desenvolvimento de produtos e sistemas com tendência de eventual concentração do custo de falhas aos investidores individuais. Podemos observar alguns projetos DeFi financiados por meio de *venture capital* (VC) ou investidores institucionais, estruturados por meio de organizações descentralizadas e ante a ausência de um quadro regulatório, afastam a responsabilização na hipótese de falha do projeto.

A assimetria também é clara nos casos de DApps desenvolvidos por agentes maliciosos e moldados sob a estrutura de pirâmides financeiras com garantia de retornos não realísticos. O desconhecimento do investidor individual sobre a execução do contrato inteligente e a facilidade de transferência de recursos sem o conhecimento do efetivo proprietário do ativo, contribuem para elevar o risco de assimetria informacional.

(ii) Risco Tecnológico-Operacional

Representa uma grande barreira do ecossistema DeFi. Assim, em conjunto com o risco de liquidez e risco de crédito é categorizado como um dos principais riscos em qualquer sistema financeiro.

No caso específico da rede de finanças descentralizadas, o risco tecnológico-operacional emerge com grande nitidez, tendo em vista que todo o arranjo do ecossistema é moldado na infraestrutura *blockchain* pública e em algoritmos desenvolvidos sob a forma de *smart contracts*. Nesse sentido, há um risco tecnológico-operacional inerente ao sistema em decorrência de sua própria estrutura de formação.

Dentre os possíveis eventos que caracterizam o risco tecnológico-operacional, podemos citar:

1. Falhas na infraestrutura *blockchain* ou aplicativos da rede: levando em consideração que o ecossistema DeFi é fundado em redes *blockchain,* qualquer disrupção ou manipulação na rede pode impactar diretamente a operação de determinado produto ou serviço, e vice-versa. A identificação de vulnerabilidades em organizações dentro das redes pode implicar, também, na necessidade de novas versões do protocolo (e.g. *hard forks).* Válido citar o caso da falha de protocolo da TheDAO em 2016, uma DAO criada como uma espécie de fundo de investimento em *venture capital* descentralizado. Nesse caso, a falha no algoritmo da DAO desenvolvida sob a plataforma Ethereum (que representava aproximadamente 15% do volume de circulação) implicou em um roubo de aproximadamente 70 milhões de dólares americanos. A solução adotada pela comunidade Ethereum foi separar a rede em duas partes, criando a Ethereum Classic (ETC) e a rede Ethereum (ETH).
2. Falhas em *smart contracts*: como já abordado no referencial teórico, *smart contracts* são algoritmos programáveis executados majoritariamente em *blockchains* públicas. Apesar do

aumento das possibilidades de inovação, não há restrições aos desenvolvedores, como licenças ou qualificação profissional. Ademais, não há obrigatoriedade em procedimentos de auditoria, sendo comuns apenas em plataformas mais consolidadas no mercado. Portanto, o risco de execução dos contratos é transferido aos usuários que fazem parte da rede e utilizam as aplicações, inclusive, podendo implicar na perda integral de recursos depositados por falhas de desenvolvimento de código.

3. Falhas em Oráculos: em síntese, oráculos são mecanismos programáveis que realizam a transferência de informações fora da rede *blockchain* para contratos inteligentes, como cotações de ativos, fatos externos, dentre outros. Ocorre que grande parte dos oráculos hoje utilizados são centralizados, de forma que as informações por eles transmitidas são condicionadas a boa-fé do provedor. Oráculos descentralizados apresentam um crescimento de adoção no mercado, mas ainda representam vulnerabilidades, como erros de atraso de informação, *hackers* e *bugs* nos protocolos.
4. *Cybersecurity*: segurança cibernética e gestão de riscos de operações são elementos estruturais do mercado financeiro, principalmente em decorrência de fatores regulatórios. A natureza descentralizada dos projetos DeFi representa um risco de segurança, na medida que poucos DApps disponibilizam controle de auditoria e não há, até então, mecanismos de atribuição de responsabilidade legal a agentes maliciosos. Invasões de *hackers* são comuns em projetos DeFi, sendo que apenas em 2021 foram reportados roubos de um montante superior a 10 milhões de dólares americanos em protocolos. Apesar da infraestrutura valer-se dos princípios de códigos abertos (como *templates* para contratos inteligentes e estruturas padronizadas de *tokens* -ERC-20-), ainda observamos frequência nos ataques à rede financeira descentralizada.

(iii) Risco de Governança

Apesar da natureza descentralizada dos protocolos DeFi, existem alguns riscos inerentes aos modelos de governança e gestão por eles adotados.

Diversos protocolos realizam o gerenciamento do controle administrativo por meio de *tokens* de governança, de modo que, em teoria, os usuários da rede poderiam compartilhar o poder decisório sobre determinadas funções, melhorias e estrutura do protocolo.

Contudo, conforme aponta o Relatório IOSCO (2021), existem diversos protocolos que são geridos por fundos de investimento e pelos principais desenvolvedores da rede, estes remunerados no início do desenvolvimento com *tokens* de governança. Assim, grande parcela dos protocolos não identificam as organizações/entidades responsáveis pelo controle, implicando em um risco aos potenciais investidores.

Outros modelos de protocolo realizam a concentração do poder decisório por meio de chaves administrativas, em que determinados participantes da rede podem alterar a estrutura funcional e até

mesmo realizar o *shutdown* da plataforma. A perda ou roubo das chaves administrativas pode implicar em graves consequências para todos os usuários da rede, aumentando, portanto, o risco dos protocolos.

Pelo exposto, apesar da natureza descentralizada da rede DeFi, a intervenção humana ainda representa riscos consideráveis de governança, principalmente relacionados ao controle de administração e governança das plataformas, na medida que a concentração do poder decisório pode implicar na falha de toda a estrutura de funcionamento dos arranjos.

(iv) Risco de Integridade de Mercado

O risco de integridade de mercado é caracterizado pelos possíveis impactos na estrutura do ecossistema decorrentes de crises de liquidez, conflitos de interesse, alavancagem, arbitragem, dentre outros novos riscos introduzidos pela própria rede DeFi.

Um dos primeiros riscos de integridade de mercado identificados foi a dependência estrutural de *stablecoins* atrelados a moedas fiduciárias, como o USDT ou USDC. A falta de transparência relativa aos depósitos colaterais pode implicar em eventuais crises de confiança, causando, assim, uma falha sistêmica em diversos protocolos dependentes dos ativos, como empréstimos (alavancados ou não) e operações de *swap* (*pools* de liquidez e *yield farming*).

Outro risco tipicamente elevado no ambiente DeFi, é a possibilidade de uso das plataformas para atividades ilícitas, como lavagem de dinheiro e financiamento do terrorismo. A ausência de procedimentos KYC e as margens de criação de contratos inteligentes complexos e opacos implica em um aumento do grau de anonimização e, consequentemente, das barreiras de fiscalização. Assim, existe um significativo risco relativo à circulação de ativos obtidos ilegalmente na rede.

Por fim, podemos citar a possibilidade de alavancagem ilimitada como um risco considerável no ambiente DeFi. O uso de empréstimos para garantia de crédito colateral em outros protocolos pode ocasionar uma crise de liquidação estrutural na rede financeira descentralizada.

(v) Risco Regulatório

Ocasionado pelo cenário de incerteza de regulamentação das atividades desenvolvidas no ecossistema DeFi. Segundo Carter & Jeng (2021), transações que envolvem empréstimo, *trading*, derivativos e alavancagem são fortemente regulados no mercado financeiro tradicional, com o registro, licenciamento e exame de todos os intermediários presentes. No caso do DeFi, a descentralização como princípio estruturante desfavorece reguladores e legisladores, na medida que a própria identificação dos responsáveis pelo gerenciamento dos protocolos é muito difícil e onerosa, especialmente em um contexto multinacional.

Apesar de alguns posicionamentos ativos de agências reguladoras[42], os mecanismos de distribuição de *tokens* de governança, comuns em grande parte dos protocolos DeFi, também já encontram barreiras regulatórias em diversos países, tendo em vista que a existência de regulamentação específica para distribuição de participação acionária (*equity*).

[42] Disponível em: https://www.sec.gov/news/press-release/2018-258. Acesso em: 27 de abril de 2022.

Em síntese, a incerteza regulatória sob o ambiente DeFi é crescente, pois, além da descentralização, a possibilidade de desenvolvimento de novos protocolos inovadores por meio de contratos programáveis sem *framework* definido pode ocasionar lacunas regulatórias.

Ademais, a falta de salvaguardas regulatórias tradicionais para proteção do investidor, existentes em toda a regulamentação de serviços financeiros tradicionais, deixa os investidores e consumidores dos produtos/protocolos mais expostos a formas de perda ou erosão de valor (OECD, 2022).

5.3. Análise comparativa dos critérios

O passo seguinte foi a comparação entre os critérios de acordo com a escala relativa descrita na figura 1. Merece destaque que, como o presente estudo trata sobre a análise de riscos de investimento por parte de um gestor, a classificação dos riscos foi realizada de forma autônoma pelo autor, vejamos:

Tabela 7: Matriz de comparação de pares entre critérios

	Risco Técnológico-Operacional	Risco de Assimetria/Fraudes	Risco de Governança	Risco de Integridade do Mercado	Risco Regulatório
Risco Técnológico-Operacional	1	7	3	3	5
Risco de Assimetria/Fraudes	1/7	1	3	1/3	1/5
Risco de Governança	1/3	1/3	1	1/5	1/7
Risco de Integridade do Mercado	1/3	3	5	1	1/3
Risco Regulatório	1/5	5	7	3	1

Fonte: Elaborada pelo autor.

Assim, foi realizada a normalização da matriz e o cálculo do vetor prioridade (w), sendo que a próxima tabela exemplifica a consolidação dos pesos atribuídos aos riscos.

Tabela 8: Matriz de comparação normalizada com cálculo do vetor prioridade (w)

	Risco Técnológico-Operacional	Risco de Assimetria/Fraudes	Risco de Governança	Risco de Integridade do Mercado	Risco Regulatório	Vetor Prioridade (*w*)
Risco Técnológico-Operacional	0,497630332	0,428571429	0,157894737	0,398230088	0,7489301	45%
Risco de Assimetria/Fraudes	0,071090047	0,06122449	0,157894737	0,044247788	0,029957204	7%
Risco de Governança	0,165876777	0,020408163	0,052631579	0,026548673	0,021398003	6%
Risco de Integridade do Mercado	0,165876777	0,183673469	0,263157895	0,132743363	0,049928673	16%
Risco Regulatório	0,099526066	0,306122449	0,368421053	0,398230088	0,14978602	26%

Fonte: Elaborada pelo autor.

Observa-se que o Risco Tecnológico-Operacional representa quase metade da influência sobre a decisão de investimento, seguido do Risco Regulatório (26%) e o Risco de Integridade de Mercado. Os riscos de Assimetria/Fraudes e Governança não representaram um impacto significativo na análise.

Posteriormente, foi determinado o valor de λmax por meio da soma ponderada de cada linha dividida pela prioridade da alternativa correspondente. O resultado demonstrou que o valor resultante em λ (5,41) foi próximo ao número de critérios (5).

Por fim, aplicou-se a fórmula descrita na equação (1) para determinar o Índice de Consistência (IC), essencial para obter a Razão de Consistência (RC). Com isso, é possível demonstrar a coerência (IC) e a confiabilidade (RC) dos dados em questão (PIMENTA *et al*., 2019).

Tabela 9: Razão entre a Soma Ponderada e o Vetor Prioridade (*w*)

	Soma Ponderada	Vetor Prioridade (*w*)	Razão entre a Soma Ponderada e o Vetor Prioridade
Risco Técnológico-Operacional	2,86	45%	6,408944382
Risco de Assimetria/Fraudes	0,36247619	7%	4,973408352
Risco de Governança	0,289142857	6%	5,039734311
Risco de Integridade do Mercado	0,813333333	16%	5,112858959
Risco Regulatório	1,464	26%	5,536706229

Fonte: Elaborada pelo autor.

Tabela 10: Cálculo do λ*max*, Índice de Consistência e Razão de Consistência

Média = λmax	5,414330447
Índice de Consistência (IC)	0,103582612
Índice Randômico (IR)	1,11
Razão de Consistência (RC)	9,33%

Fonte: Elaborada pelo autor.

De acordo com a tabela 2 e a metodologia proposta por Saaty (1977), observamos que a Razão de Consistência resultou em um valor inferior à 10% (dez por cento), sendo, portanto, confiável.

Nesse sentido, necessário realizar uma análise comparativa dos resultados obtidos. Vejamos, novamente, a consolidação dos pesos atribuídos aos riscos apresentados:

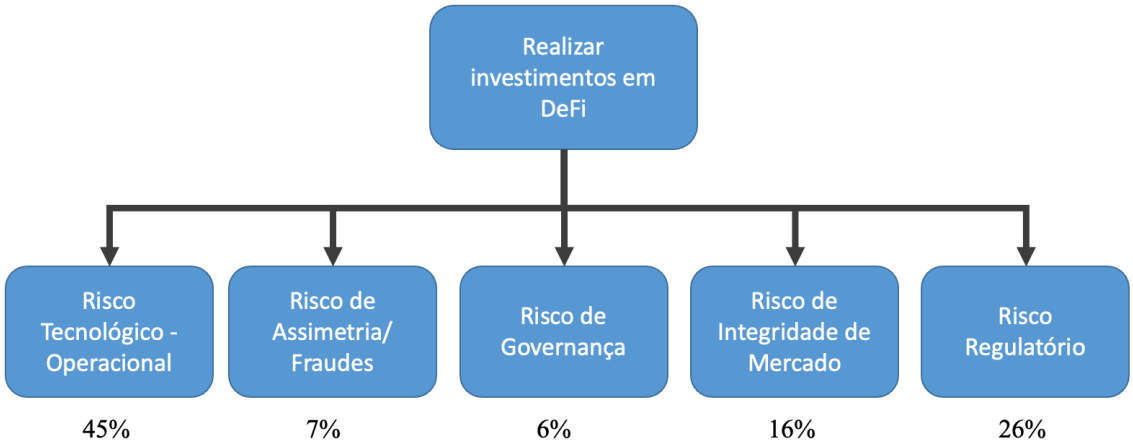

Figura 35: Estrutura hierárquica de critérios com pesos atribuídos

Fonte: Elaborada pelo autor.

O fato de o risco tecnológico-operacional representar grande parte da influência sobre a tomada de decisão (45%) relaciona-se com a própria infraestrutura de desenvolvimento de mercado no setor de finanças descentralizadas. Por tratar-se de um sistema essencialmente baseado em redes distribuídas, os riscos tecnológicos de funcionamento infraestrutura DeFi podem ocasionar falhas estruturais que, consequentemente, podem inviabilizar a utilização de determinados protocolos ou até mesmo das próprias redes *blockchain.* Ademais, o desenvolvimento de contratos inteligentes possui um risco intrínseco de eventuais erros de código, implicando em possíveis falhas do arranjo de determinado protocolo.

Também com um impacto muito significativo (26%), o risco regulatório caminha em sentido convergente, na medida que eventuais limitações legais e normativas podem ocasionar barreiras para a utilização de protocolos e restrições ao desenvolvimento de novos produtos financeiros. Contudo, a adoção de uma política regulatória mais resoluta, ao garantir maior controle e segurança, também pode

influenciar na redução dos riscos de integridade de mercado (16%), assimetria/fraudes (7%) e governança (6%).

Os três riscos com menor influência acima citados representam riscos inerentes aos atuais modelos de desenvolvimento dos protocolos estudados. Há uma grande possibilidade de que os riscos alterem a influência descrita com o avanço no desenvolvimento e com a aplicação de políticas regulatórias. Novos protocolos, conforme já apresentado no curso do presente estudo, surgem como alternativas para mitigas riscos presentes em protocolos mais consolidados.

Acredita-se, portanto, que os riscos categorizados possuem uma correlação significativa com o grau de inovação no setor. A evolução constante e as rápidas mudanças implicam na necessidade de revisões periódicas dos pesos atribuídos para garantia de maior segurança do investimento.

6. CONCLUSÃO

Neste estudo, buscou realizar uma análise pelo modelo MCDA (*Multiple Criteria Decision Analysis*), especificamente pelo método AHP (*Analytic Hierarchy Process*), dos riscos presentes do ecossistema de finanças descentralizadas (DeFi), por meio de uma revisão histórica, dos conceitos e riscos descritos na bibliografia, bem como um experimento prático para compreensão da estrutura de funcionamento e eventuais riscos dos protocolos.

Assim, levantou-se cinco principais riscos: (i) risco de assimetria e fraudes; (ii) risco tecnológico-operacional; (iii) risco de governança; (iv) risco de integridade de mercado; e (v) risco regulatório. Por fim, por meio da aplicação da ferramenta AHP, foi possível determinar a gravidade dos riscos em relação à tomada de decisão de investimento.

Com os resultados obtidos na categorização, ficou evidente a relevância que o risco tecnológico-operacional possui sobre a rede DeFi, e por se tratar de um sistema essencialmente baseado em DLT's, no caso em *blockchains,* o risco atribuído ao funcionamento de contratos inteligentes (eventuais *bugs)*, vulnerabilidades relacionadas a invasões (segurança) e a validação da estrutura *blockchain* em si representam um elevado grau de incerteza para transações financeiras.

Nesse sentido, o risco regulatório emerge como outro fator com relevância acentuada. A possível inviabilização do uso da tecnologia DeFi para pagamentos cotidianos e a introdução de uma regulação mais protetiva ao mercado financeiro tradicional também são pontos de atenção ao investidor, seja institucional ou individual.

Apesar de não apresentarem um impacto expressivo como os outros riscos acima elencados, os riscos de integridade de mercado, governança e assimetria/fraudes são essenciais para a tomada de decisão de investimento, de modo que, inclusive, devendo ser considerados para a alocação de criptoativos no portfólio e para a seleção de protocolos/produtos financeiros.

Pelo exposto, a rede DeFi apresenta um grande potencial de fornecimento de serviços financeiros mais eficientes baseados na automação e desintermediação desenvolvidos por meio de redes descentralizadas e contratos inteligentes. Contudo, ao mesmo passo, o ecossistema possui riscos intrínsecos que podem inviabilizar o seu crescimento em médio e longo prazo.

O método utilizado possibilitou uma tomada de decisão de investimento mais prudente e segura, pois, com o sopesamento do elevado grau de incerteza do setor e o potencial de retorno com a especulação de ativos, a alocação realizada adotou uma posição mais conservadora protetiva.

Assim, a decisão final foi realizar a alocação de 0,5% do patrimônio total no setor de DeFi, dividindo o portfólio, proporcionalmente, em *tokens* nativos de rede e de protocolos com maior grau de consolidação no atual contexto. A proposta ainda contempla a revisão mensal da carteira, tendo em vista as constantes oscilações do mercado de criptoativos.

Como sugestões de trabalhos futuros, propõe-se a modelagem de novos estudos de análises multicritério dos riscos com especialistas do setor de finanças descentralizadas, de modo a compreender diferentes percepções das influências geradas pelos riscos categorizados.

REFERÊNCIAS BIBLIOGRÁFICAS

ALIAGA, Yoshitomi Eduardo Maehara; HENRIQUES, Marco Aurelio Amaral. **Uma comparação de mecanismos de consenso em blockchains**. *Proceedings of the* Encontro dos Alunos e Docentes do Departamento de Engenharia de Computação e Automação Industrial, Campinas, Brasil, 2017. p. 26-27.

An Incomplete Guide to Rollups. **Vitalik Buterin's website**, Jan 05, 2021. Disponível em: https://vitalik.ca/general/2021/01/05/rollup.html. Acesso em: 27 de abril de 2022.

BEREZON, Dmitriy. Blockchain Bridges: Building Networks of Cryptonetworks. **Medium**, Sep 8, 2021. Disponível em: https://medium.com/1kxnetwork/blockchain-bridges-5db6afac44f8. Acesso em: 27 de abril de 2022.

BIS, Bank for International Settlements. **Central bank digital currencies: executive summary**. Setembro de 2021.

BIS, Bank for International Settlements. **Central bank digital currencies: foundational principles and core features.** 2020.

BULLMANN, D.; KLEMM, J.; PINNA, A. **In search for stability in crypto-assets**: *Are stablecoins the solution?* ECB Occasional Paper, n. 230, 2019. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3 444847. Acesso em: 27 de abril de 2022.

BUTERIN, V. (2013b, September 13). Bootstrapping A Decentralized Autonomous Corporation: Part I. Bitcoin Magazine. Disponível em: https://bitcoinmagazine.com/articles/bootstrapping-a-decentralized-autonomouscorporation-part-i-1379644274. Acesso em: 27 de abril de 2022.

BUTERIN, Vitalik *et al*. **A next-generation smart contract and decentralized application platform**. White paper, v. 3, n. 37, 2014.

CARTER, Nic; JENG, Linda. DeFi protocol risks: the paradox of DeFi. Regtech, Suptech and Beyond: Innovation and Technology in Financial Services. **RiskBooks – Forthcoming Q**, v. 3, 2021.

CARTER, Nic; JENG, Linda. DeFi protocol risks: the paradox of DeFi. Regtech, Suptech and Beyond: Innovation and Technology in Financial Services. **RiskBooks – Forthcoming Q**, v. 3, 2021.CLEMENTS, Ryan. Built to Fail: The Inherent Fragility of Algorithmic Stablecoins. **Wake Forest L. Rev. Online**, v. 11 p. 131, 2021. Doi: http://dx.doi.org/10.2139/ssrn.3952045.

CONG, Lin William; HE, Zhiheng; TANG, Ke. Staking, Token Pricing, and Crypto Carry. **Available at SSRN**, 2022.DARREN, LAU *et al*. **How to DeFi**. Book Starter ID, 2020.

Defi Llama. **Protocol Categories**. Disponível em: https://defillama.com/categories. Acesso em: 27 de abril de 2022. ecosystem: An empirical analysis. **NYU Stern School of Business**, 2021.

EL FAQIR, Youssef; ARROYO, Javier; HASSAN, Samer. An overview of decentralized autonomous organizations on the blockchain. *In*: **Proceedings of the 16th international symposium on open collaboration**, 2020. p. 1-8.

FAUX, Zeke. Anyone Seen Tether's Billions? **Bloomberg**, Oct 7, 2021. Disponível em: https://www.bloomberg.com/news/features/2021-10-07/crypto-mystery-where-s-the-69-billion-backing-the-stablecoin-tether

Fei Protocol. **The Stablecoin For DeFi**. Disponível em: https://fei.money. Acesso em: 27 de abril de 2022.

G7 Working Group on Stablecoins. ***Investigating the impact of global stablecoins***. 2019. Disponível em: https://www.bis.org/cpmi/publ/d187.htm. Acesso em: 27 de abril de 2022.

GERSBACH, Hans; MAMAGEISHVILI, Akaki; SCHNEIDER, Manvir. Staking Pools on Blockchains. **Jornal arXiv.** Volume abs/2203.05838, 2022.

GORTON, Gary B. The Subprime Panic. **National Board of Economic Review**, Working Paper 14398, 2008.

GRECO, Salvatore; FIGUEIRA, Jose; EHRGOTT, Matthias. **Multiple criteria decision analysis**. New York: springer, 2016.

HEIMBACH, Lioba; WANG, Ye; WATTENHOFER, Roger. Behavior of liquidity providers in decentralized exchanges. **Jornal arXiv.** Volume 2105.13822, 2021.

HOUGAN, Matt. *Fintech Is A Colossal Disappointment. DeFi Fixes It*. **Forbes**, Oct 12, 2021. Crypto & Blockchain. Disponível em: https://www.forbes.com/sites/matthougan/2021/10/12/fintech-is-a-colossal-disappointment-defi-fixes-it/. Acesso em: 27 de abril de 2022.

IRRESBERGER, Felix *et al*. The public blockchainJENTZSCH, Christoph. **Decentralized autonomous organization to automate governance**. White paper, 2016.

JOHNSTON, David *et al*. **The General Theory of Decentralized Applications, DApps**. 2014.

MEEGAN, X.; KOENS, T. **Lessons Learned from Decentralised Finance (DeFi)**. Disponível em: https://www.ingwb.com/binaries/content/assets/insights/themes/distributed-ledger technology/defi_white_paper_v2.0.pdf Acesso em:27 de abril de 2022.

MEHRLING, Perry. The new lombard street. *In*: **The New Lombard Street**. Princeton University Press, 2010.

METCALFE, William *et al*. Ethereum, smart contracts, DApps. **Blockchain and Crypt Currency**, 2020. p. 77.

MOHAN, Vijay. Automated market makers and decentralized exchanges: a DeFi primer. **Financial Innovation**, v. 8, n. 1, 2022. p. 1- 48.

MOHANTA, Bhabendu Kumar; PANDA, Soumyashree S.; JENA, Debasish. An overview of smart contract and use cases in blockchain technology. *In*: **2018 9th international conference on computing, communication and networking technologies (ICCCNT)**. IEEE, 2018. p. 1-4.

MONTIBELLER, Gilberto; FRANCO, Alberto. Multi-criteria decision analysis for strategic decision making. *In*: **Handbook of Multicriteria Analysis**. Springer, Berlin, Heidelberg, 2010. p. 25-48. Doi: 10.1007/978-3-540-92828-7_2.

NAKAMOTO, Satoshi. Re: Bitcoin P2P e-cash paper. **The Cryptography Mailing List**, 2008.

NATARAJAN, Harish; KRAUSE, Solvej; GRADSTEIN, Helen. **Distributed ledger technology and blockchain**. 2017.

OECD. *Why Decentralised Finance (DeFi) Matters and the Policy Implications*. **OECD Paris**, Jan 19, 2022. Disponível em: https://www.oecd.org/finance/why-decentralised-finance-defi-matters-and-the-policy-implications.htm. Acesso em: 27 de abril de 2022.

OR01/2022 IOSCO Decentralized Finance Report. Report of the Board of IOSCO, 24 mar 2022.

PHILIPPON, Thomas. ***The fintech opportunity***. *National Bureau of Economic Research*, 2016.

PIMENTA, Lianne Borja *et al*. Processo Analítico Hierárquico (AHP) em ambiente SIG: temáticas e aplicações voltadas à tomada de decisão utilizando critérios espaciais. **Interações (Campo Grande)**, v. 20, 2019. p. 407-420.

PORAT, Amitai *et al*. **Blockchain Consensus**: An analysis of Proof-of-Work and its applications. 2017.

RAGAZZO, Carlos; CATALDO, Bruna. **Moedas Digitais**: Entenda o que são criptomoedas, stablecoins e CBDC's. Instituto Propague, 2021.

RASMUSSEN, Ryan; LAWANT, David; HOUGAN, Matt. Decentralized Finance (DeFi): A Primer for Professional Investors. **BITWISE ASSET MANAGEMENT**. Novembro de 2021.

REZENDE, Patrícia S.; MARQUES, Daniela V.; OLIVEIRA, Luiz A. Construção de modelo e utilização do método de Processo Analítico Hierárquico–AHP para mapeamento de risco á inundação em área urbana. **Revista Caminhos da Geografia**, 2017.

SAATY, Roseanna W. The analytic hierarchy process: what it is and how it is used. **Mathematical modelling**, v. 9, n. 3-5, 1987. p. 161-176.

SAATY, T. H. A scaling method form priorities in hierarquical structures. **Journal of Mathematical Psychology**, v. 15, n. 3, 1977. p. 234-281. Doi: https://doi.org/10.1016/0022- 2496(77)90033-5

SAPIENZA, Paola; ZINGALES, Luigi. A Trust Crisis. **International Review of Finance**, v. 12, n. 2, 2012. p. 123–131. Doi:10.1111/j.1468-2443.2012.01152.x.

SCHAFFNER, Tobias. Scaling Public Blockchains. University of Basel: **A comprehensive analysis of optimistic and zero-knowledge rollups**. 2021.

SCHÄR, Fabian. Decentralized finance: On blockchain-and smart contract-based financial markets. **FRB of St. Louis Review**, 2021.

SGUANCI, Cosimo; SPATAFORA, Roberto; VERGANI, Andrea Mario. Layer 2 blockchain scaling: A survey. **Jornal arXiv.** Volume arXiv:2107.10881, 2021.

SHRIVAS, Mahendra Kumar; YEBOAH, Dr. Thomas. The disruptive blockchain: Types, platforms and applications. *In*: **Fifth Texila World Conference for Scholars (TWCS) on Transformation: The Creative Potential of Interdisciplinary**, 2018.

SOUTELO, Sara Sofia Alves Ferreira *et al*. **A estabilidade monetária e a função da moeda reserva de valor**. 2020. Dissertação de Mestrado em Economia Monetária, Bancária e Financeira – Escola de Economia e Gestão, Universidade do Minho, Minho, Portugal, 2020.

SOUZA, João Carlos Felix *et al.* Uma avaliação multicritério dos riscos do pré-sal. **XXXIV Encontro Nacional de Engenharia de Produção**, Curitiba – PR, de 07 a 10 de outubro de 2014.

TASCA, Paolo; THANABALASINGHAM, Thayabaran; TESSONE, Claudio J. Ontology of blockchain technologies. Principles of identification and classification. **SSRN Electronic Journal**, v. 10, 2017.

The Maker Protocol: MakerDAO's Multi-Collateral Dai (MCD) System. Disponível em: https://makerdao.com/pt-BR/whitepaper#interacting-with-a-maker-vault. Acesso em: 27 de abril de 2022.

USLANER, Eric M. Trust and the economic crisis of 2008. **Corporate Reputation Review**, v. 13, n. 2, 2010. p. 110-123.

VOSHMGIR, Shermin. ***Token Economy***: *How the Web3 reinvents the Internet*. Token Kitchen, 2020.

WANG, Qin *et al*. Non-fungible token (NFT): Overview, evaluation, opportunities and challenges. **Jornal arXiv.** Volume arXiv:2105.07447, 2021.

What Are Stablecoins? **CBInsights**, Jan 25, 2022. Disponível em: https://www.cbinsights.com/research/report/what-are-stablecoins/#types. Acesso em: 27 de abril de 2022.

What is Matic Network? Features and Concepts of Matic. **Simplilearn**. Disponível em: https://www.simplilearn.com/tutorials/blockchain-tutorial/matic-network Jaynti Kanani. Acesso em: 27 de abril de 2022.

WIGGINS, Rosalind; PIONTEK, Thomas; METRICK, Andrew. The Lehman Brothers Bankruptcy A: Overview. **Yale Program on Financial Stability Case Study**, v. 1, 3A, 2014. Doi: http://dx.doi.org/10.2139/ssrn.2588531.

ZAGHLOUL, Ehab *et al*. Bitcoin and blockchain: Security and privacy. **IEEE Internet of Things Journal**, v. 7, n. 10, 2020. p. 10.288-10.313.

ZANATA, Pedro. Entenda como as criptomoedas estão sendo usadas na guerra entre Ucrânia e Rússia. **CNN Brasil**, São Paulo, 12 mar 2022. Disponível em: https://www.cnnbrasil.com.br/business/entenda-como-as-criptomoedas-estao-sendo-usadas-na-guerra-entre-ucrania-e-russia/. Acesso em: 27 de abril de 2022.

ZHENG, Zibin *et al*. An overview on smart contracts: Challenges, advances and platforms. **Future Generation Computer Systems**, v. 105, 2020. p. 475-491.