Universidade Federal de Pernambuco

Centro de Informática
Engenharia da Computação

Trabalho de Graduação

2021.2

Análise SWOT de Serviços Financeiros Descentralizados

Aluno:
Victor Crisóstomo Mellia

Orientadora:
Valeria Cesario Times

26 de maio de 2022

Universidade Federal de Pernambuco

Centro de Informática

Victor Crisóstomo Mellia

Análise SWOT de Serviços Financeiros Descentralizados

Trabalho de Graduação apresentado ao curso de Engenharia da Computação do Centro de Informática da Universidade Federal de Pernambuco como requisito parcial para obtenção do grau de Bacharel em Engenharia da Computação.

Orientadora: Dra. Valeria Cesario Times

Recife
2021

Dedico esse trabalho as minhas duas mães, Ana e Edite.

Agradecimentos

Primeiramente, eu gostaria de dedicar esse trabalho à Maria Edite Campos Crisóstomo (in memoriam), que é a minha tia, a qual tenho a honra de poder chamar de mãe e que, infelizmente, não pôde ver esse momento. Contudo, tenho a certeza que de onde ela estiver, está vibrando com essa conquista. Obrigado por tudo que fez por mim. Sem a senhora nada disso seria possível.

Ademais, gostaria de agradecer aos meus avós (in memoriam), Fernando e Graça, que foram uma parte muito importante da minha criação e se tornaram meus maiores exemplos de luta e determinação.

Agradeço, também, aos meus pais, Roberto e Ana, pelos conselhos e amor incondicional proporcionado. Ao meu irmão Fernando e a todos os demais familiares não citados, meu obrigado pelo incentivo fornecido durante essa jornada. À minha querida amiga Zélia, meu obrigado pelo carinho e dedicação nas refeições produzidas e nos cuidados com a família Crisóstomo.

Outrossim, não poderia deixar de externar a minha eterna gratidão à minha namorada e futura esposa, Priscila, por estar ao meu lado há mais de dez anos, vivenciando todas as batalhas da vida. Obrigado por todo suporte que você me proporciona e por todas as horas consumidas na revisão desse trabalho, que não teria conseguido concluir de outra forma. À minha sogra, Ednay, e aos meus cunhados, Bruno Renato e Camila, obrigado pelo apoio durante toda a trajetória.

Por fim, gostaria de agradecer a todos os professores com quem já aprendi, especialmente a professora orientadora, Valeria Times, que me deu todo o suporte com suas correções e incentivos, como, também, ao seu grupo de pesquisa sobre blockchain, composto por André Araújo, Arthur Carvalho, Flaviano Viana, Henrique Couto, Rodrigo Folha, Valeria Times e Victor Mellia. Todas as nossas conversas semanais foram de grande ajuda para a confecção desse TCC.

Resumo

As finanças descentralizadas, também conhecidas como DeFi, correspondem a um sistema de serviços financeiros descentralizados construídos na blockchain, que se propõem a democratizar as finanças centralizadas, por fornecerem uma gama completa de serviços financeiros, sem a necessidade de intermediários, para qualquer pessoa ao redor do mundo, que possua acesso à internet.

Assim, o presente trabalho tem como principal objetivo fazer uma análise crítica acerca do potencial dos serviços ofertados nas finanças descentralizadas, investigando se eles oferecem reais benefícios ou apenas as mesmas vantagens dos serviços ofertados nas finanças centralizadas.

Ademais, a metodologia utilizada na realização desse trabalho envolveu uma pesquisa bibliográfica composta por quatro etapas: (1) Revisão da literatura para estabelecer os conceitos básicos necessários ao desenvolvimento desse documento; (2) A realização de um estudo comparativo entre os trabalhos existentes e relacionados ao tema proposto nesse TCC; (3) A exposição dos serviços ofertados nas finanças descentralizadas, comparando-os com os serviços ofertados nas finanças centralizadas; (4) A realização de uma análise SWOT, visando apresentar os principais pontos fortes, pontos fracos, oportunidades e ameaças das finanças descentralizadas.

Palavras-chave: Finanças Descentralizadas, Finanças Centralizadas, Análise SWOT.

Abstract

Decentralized finance, also known as DeFi, corresponds to a system of decentralized financial services built on the blockchain, which aims to democratize centralized finance by providing a full range of financial services, without the need of intermediaries, and is available to anyone around the world with internet access.

Thus, the main objective of the current work is to make a critical analysis about the potential of the services offered in decentralized finances, investigating whether they offer real benefits or just the same advantages of the services offered in centralized finances.

Furthermore, the methodology used to carry out this work involved a bibliographic research composed of four steps: (1) Literature review to establish the basic concepts necessary for the development of this document; (2) Carrying out a comparative study between existing works and studies related to the proposed theme; (3) The exposure of services offered in decentralized finance, comparing them with the services offered in centralized finance; (4) Conducting a SWOT analysis to present the main strengths, weaknesses, opportunities and threats of decentralized finance.

Keywords: Decentralized Finance, Centralized Finance, SWOT Analysis.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE TABELAS

Sumário

1 Introdução

Neste capítulo, será realizada uma apresentação da área do trabalho descrito nesse documento, incluindo a contextualização do tema, motivação, exibição dos objetivos do trabalho realizado, revisão da literatura e organização dos capítulos.

1.1 Contextualização e Motivação

Tradicionalmente, o setor financeiro segue uma abordagem baseada em instituições centrais, as quais se comportam como terceiros para oferecer serviços financeiros, além de fornecer a infraestrutura necessária para facilitar a execução de transações. Sendo assim, a sociedade passa a depender de bancos, corretoras e outras firmas de serviços financeiros para ter acesso às bolsas de valores e ao câmbio, para enviar ou receber dinheiro, realizar empréstimos, conseguir financiamento, entre outros serviços.

Por outro lado, finanças descentralizadas correspondem a um sistema de serviços financeiros, cujo objetivo é operar sem a necessidade de intermediários, como bancos ou seguradoras. Desse modo, as finanças descentralizadas atingem o seu objetivo por meio de contratos inteligentes, isto é, protocolos que replicam os serviços financeiros tradicionais mediante código.

Diante do exposto, ao utilizar finanças descentralizadas, é possível dispensar a necessidade de uma autoridade central para supervisionar as transações, que é o que ocorre nas instituições tradicionais. Dessa forma, essa dispensa pode reduzir custos, melhorar a segurança, aumentar a eficiência das transações e, principalmente, democratizar os serviços financeiros, visto que, no mercado tradicional, muitos produtos não estão disponíveis para todos os investidores.

1.2 Objetivos

O objetivo desse trabalho de conclusão de curso é buscar responder se os serviços ofertados nas finanças descentralizadas proporcionam reais benefícios ou apenas as mesmas vantagens dos serviços ofertados nas finanças centralizadas. Para tanto, será feita uma análise SWOT das finanças descentralizadas, no qual será elucidado os seus principais pontos fortes, pontos fracos, oportunidades e ameaças. Obtendo essas informações, é possível inferir sobre o futuro das finanças descentralizadas e antecipar seu potencial de impacto socioeconômico. Sendo assim, esse estudo visa:

- Realizar um levantamento bibliográfico sobre os conceitos básicos existentes em finanças descentralizadas;
- Explorar as diferenças existentes entre finanças centralizadas e finanças descentralizadas;
- Conduzir uma análise de pontos fortes, pontos fracos, oportunidades e ameaças das finanças descentralizadas.

Os resultados do estudo irão:

- Auxiliar na compreensão e destacar o valor da adoção de finanças descentralizadas.
- Servir de base para futuros estudos empíricos para comprovação de hipóteses sobre finanças descentralizadas.

1.3 Metodologia

A metodologia utilizada na realização desse trabalho envolveu uma pesquisa bibliográfica composta por quatro etapas: (1) Revisão da literatura para estabelecer os conceitos básicos necessários ao desenvolvimento desse documento; (2) A realização de um estudo comparativo entre os trabalhos existentes e relacionados ao tema proposto nesse TCC; (3) A exposição dos serviços ofertados nas finanças descentralizadas, comparando-os com os serviços ofertados nas finanças centralizadas; (4) A realização de uma análise SWOT, visando apresentar os principais pontos fortes, pontos fracos, oportunidades e ameaças das finanças descentralizadas. Figura 1 ilustra o fluxo das etapas realizadas.

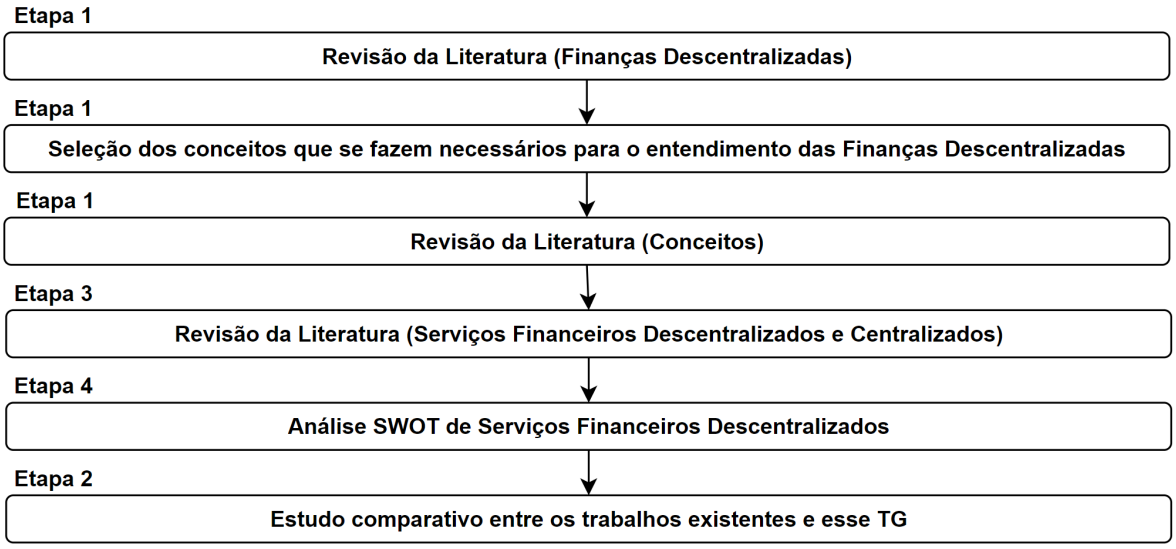

Figura 1: Fluxo do trabalho realizado.

1.4 Organização dos Capítulos

O presente trabalho de conclusão de curso está dividido em seis capítulos, incluindo o capítulo atual.

No segundo capítulo, os diferentes termos discutidos ao longo do presente trabalho serão explicados de acordo com a revisão da literatura analisada.

No terceiro capítulo, é realizada uma apresentação e um estudo comparativo entre os trabalhos existentes e relacionados ao tema desse trabalho de conclusão de curso.

No quarto capítulo, serão expostos os principais serviços ofertados nas finanças descentralizadas, os quais serão comparados com os serviços ofertados nas finanças centralizadas.

No quinto capítulo, serão mostrados resultados de uma análise SWOT apresentando os principais pontos fortes, pontos fracos, oportunidades e ameaças das finanças descentralizadas.

No sexto e último capítulo será exposta a conclusão final de acordo com os resultados discutidos e apresentados nesse documento.

2 Conceitos Básicos

Neste capítulo, será exibida uma introdução sobre os principais conceitos existentes nas finanças descentralizadas, para que o leitor obtenha um entendimento mais abrangente do assunto estudado.

2.1 Blockchain e Bitcoin

A priori, sabe-se que, até 2008, todas as transações financeiras realizadas de forma remota dependiam de um modelo baseado em confiança, no qual existe a necessidade de um poder central pré-estabelecido como confiável, tal como os bancos, para fazer as validações necessárias de uma transação [1].

Por conseguinte, com o surgimento do white paper "Bitcoin: A Peer-to-Peer Electronic Cash System", que foi publicado sob o pseudônimo de "Satoshi Nakamoto", criou-se a possibilidade de produzir um modelo baseado em prova criptográfica, ou seja, um sistema de transações que não depende de terceiros [1]. Sob tal ótica, nesse sistema, é possível enviar e receber bitcoins sem nenhum intermediário, como bancos ou emissores de cartão de crédito.

Nesse contexto, com o intuito de evitar fraudes, Satoshi [1] introduziu o conceito da blockchain, que é um banco de dados distribuído e imutável, que armazena todas as transações já feitas na ordem cronológica. Ademais, a blockchain funciona como um livro-razão compartilhado, no qual vários nós são conectados por meio de uma rede P2P baseada na Internet, para registrar e processar as transações [2]. Portanto, o funcionamento da blockchain ocorre em uma cadeia de blocos, conforme mostrado na Figura 2.

Diante do exposto, é possível verificar que o hash de qualquer bloco recém-criado é gerado com a informação do hash do bloco anterior. Se um bloco específico for modificado arbitrariamente, o valor do hash do bloco conectado e o valor do hash do bloco alterado não irão coincidir, revelando que é um bloco manipulado [1]. Esses blocos são gerados um a um em média a cada 10 minutos e são distribuídos a todos os nós participantes da rede [3]. Logo, mesmo que o bloco de um nó específico seja manipulado, os dados registrados na blockchain não podem ser substituídos, a menos que mais de 50% dos nós sejam hackeados [3].

Vale ressaltar que a blockchain do Bitcoin se limita às transações, não sendo possível a realização de serviços financeiros fornecidos pelos bancos que exigem contratos, como empréstimos, seguros, derivativos e etc.

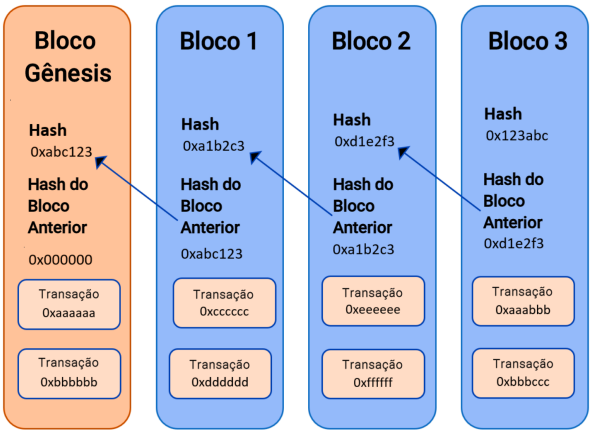

Figura 2: Diagrama conceitual da Blockchain do Bitcoin. Adaptada do livro "Solidity Programming Essentials By Ritesh Modi"

2.2 Ethereum e Contratos Inteligentes

Ethereum é uma tecnologia de blockchain 2.0 capaz de fornecer uma plataforma de aplicação distribuída para operação de contratos inteligentes [4]. Ademais, sendo desenvolvida por Vitalik Buterin, o Ethereum tem a finalidade de ampliar as aplicações da blockchain do Bitcoin, visto que esta limita-se às transferências de cunho financeiro.

Desse modo, o Ethereum expande o escopo da blockchain do Bitcoin para permitir novos serviços, que apenas são possíveis por meio de contratos inteligentes [5]. Nesse contexto, os contratos inteligentes são programas armazenados em uma blockchain, que se auto executam quando as condições pré-estabelecidas são satisfeitas, permitindo que o código de software retenha, transfira, receba ou gaste ativos digitais, dispensando, portanto, a necessidade de intermediários centralizados [6].

A Figura 3 apresenta uma comparação entre os dois possíveis cenários de um acordo. Na Figura 3(a), faz-se o uso dos contratos tradicionais, enquanto que, na Figura 3(b), os contratos inteligentes são utilizados. Conforme pode ser observado, o fato do software do contrato inteligente ter o poder de manipular ativos digitais, faz com que os intermediários centralizados se tornem obsoletos.

Vale ressaltar que, como nos contratos tradicionais, os contratos inteligentes possuem cláusulas estabelecendo os direitos e as penalidades cabíveis a qualquer uma das partes em vários cenários possíveis. Contudo, os contratos tradicionais costumam englobar uma linguagem jurídica suscetível a inúmeras interpretações, o que não ocorre nos contratos inteligentes que, por serem escritos em uma linguagem de programação, não possuem ambiguidades, reduzindo, assim, a imprecisão [7].

Além disso, o cumprimento da execução dos contratos tradicionais requer o envolvimento de terceiros e, em muitos casos, o acionamento da justiça, podendo, então, tornar-se oneroso e, consequentemente, ineficiente. Enquanto que, nos contratos inteligentes, a obtenção e processamento das informações referentes à negociação são realizados de forma autônoma e executados conforme as regras nele contido.

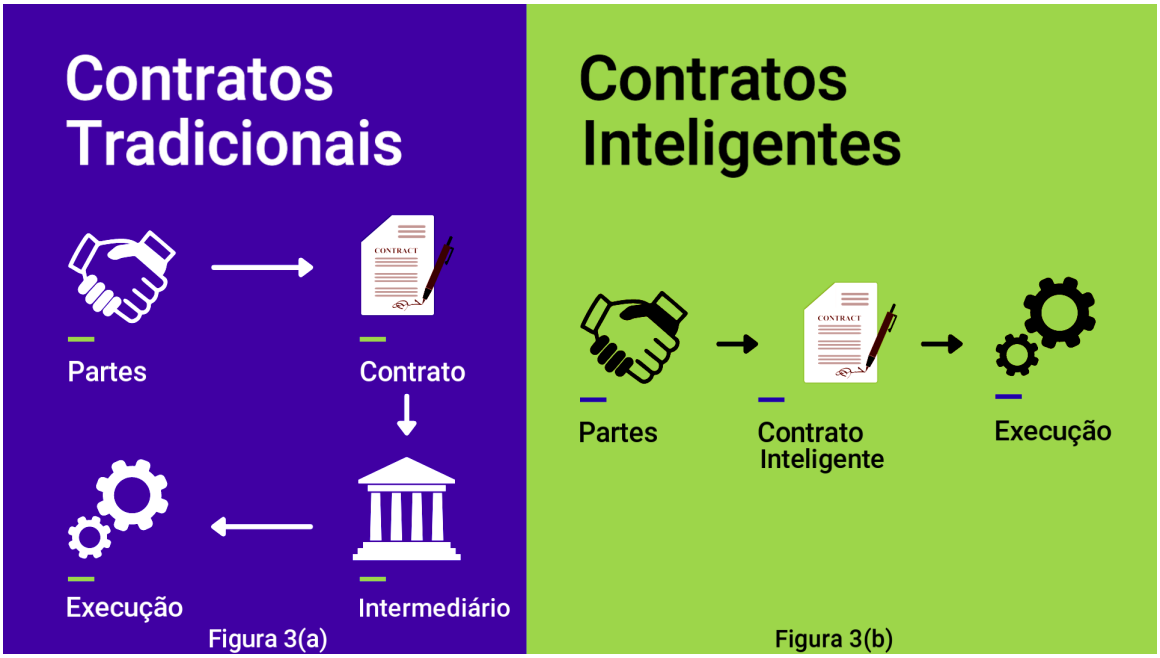

Figura 3: Contrato tradicional vs contrato inteligente. Adaptada de https://originstamp.com/blog/what-is-ethereum-and-what-are-its-use-cases/

2.3 Aplicações Descentralizadas

Comumente, quando adquirimos algum produto na Internet, seja pela compra de uma ação na bolsa de valores ou pela compra de comida por um aplicativo instalado no celular, estamos utilizando uma aplicação centralizada. Esse aplicativo corresponde a um sistema de uma empresa específica que determina suas taxas e políticas operacionais, além de servir como um terceiro de confiança que nos conecta com outros indivíduos e estabelecimentos.

Por outro lado, as aplicações descentralizadas, também conhecidas como *dapps*, são um novo modelo de aplicativos criados em uma rede descentralizada, que combina um contrato inteligente armazenado em uma blockchain com uma interface de usuário front-end [8], conforme mostra a Figura 4. Embora as aplicações descentralizadas se assemelhem às aplicações web em termos da experiência do usuário, a forma como o backend funciona é completamente diferente. Aplicativos e sites geralmente usam APIs (interfaces de programação de aplicativos) para se comunicar com o seu banco de dados, enquanto que, nas aplicações descentralizadas são utilizados contratos inteligentes para se comunicar com a blockchain.

Na Figura 4, também é possível observar que, ao contrário das aplicações centralizadas, os principais dados processados nas aplicações descentralizadas não são armazenados no servidor de uma empresa, mas são gravados na blockchain e preservados permanentemente, podendo ser visualizados por todos. Desse modo, essa característica torna as aplicações descentralizadas impossíveis de serem bloqueadas, tornando-as resistentes a qualquer tipo de censura e, ao mesmo tempo, garante que fiquem acessíveis 24 horas por dia, 7 dias por semana.

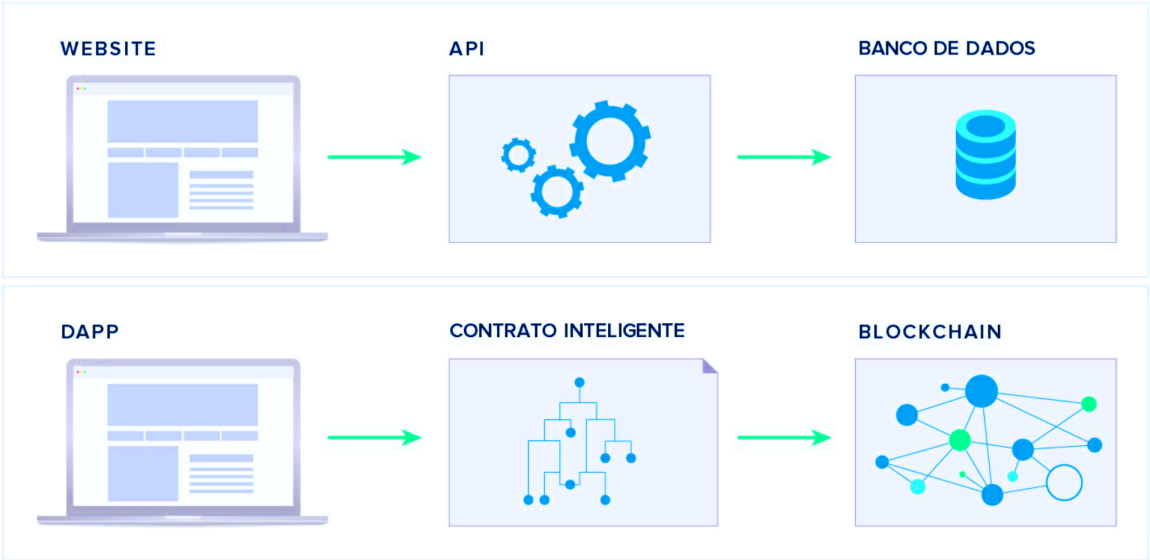

Figura 4: Aplicação centralizada vs aplicação descentralizada. Adaptada de https://academy.horizen.io/technology/advanced/guaranteed-execution-with-smart-contracts/

2.4 Finanças Descentralizadas

Finanças descentralizadas (*DeFi*) é um ecossistema financeiro que consiste em ativos digitais, contratos inteligentes e aplicativos descentralizados construídos em uma rede blockchain [8]. O objetivo da criação desse ecossistema é ter um sistema financeiro de código aberto e transparente que não seja governado por nenhuma autoridade central. Além disso, as finanças descentralizadas servem como uma alternativa para que as pessoas possam administrar e investir seu dinheiro sem terem que depender da infraestrutura financeira tradicional. As finanças descentralizadas permitem que os usuários tenham total controle sobre seus ativos e que possam interagir entre si por meio de redes ponto a ponto (P2P) ou através de aplicativos descentralizados (*dApps*).

Existem várias plataformas de blockchain que fornecem aplicativos de finanças descentralizadas, porém, a Ethereum é, de longe, a mais famosa e utilizada [9]. Alguns dos serviços mais populares ofertados pelas finanças descentralizadas são as corretoras descentralizadas, mercados de empréstimo e mineração de liquidez, tópicos que serão abordados no decorrer desse trabalho.

Na Figura 5, podem ser vistos os principais atores envolvidos em uma transação nas finanças centralizadas e nas finanças descentralizadas. Enquanto que na Figura 5(a) existem custos adicionais devido ao excesso de personagens, como as taxas cobradas por bancos e cartões de crédito, na Figura 5(b) existe a autonomia de enviar, receber e investir fundos sem a necessidade da autorização de terceiros.

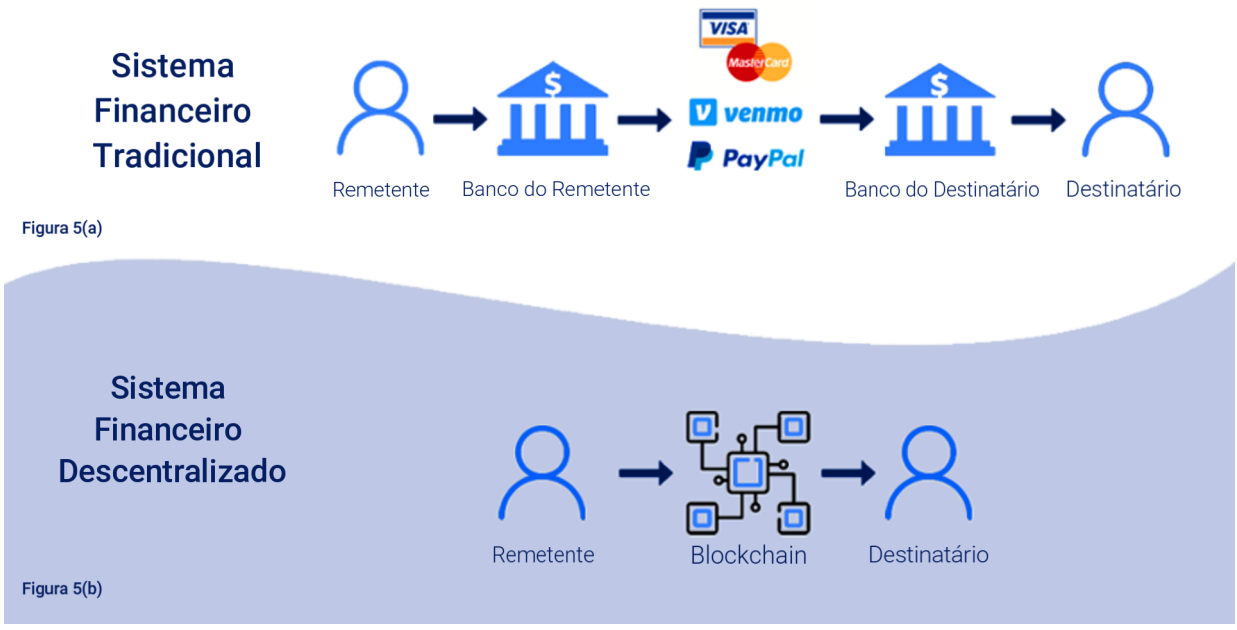

Figura 5: Finanças centralizada vs finanças descentralizada. Adaptada de https://www.stably.io/post/decentralized-finance-vs-traditional-finance-what-you-need-to-know/

2.5 Carteira de Criptomoeda, Chave Pública e Chave Privada

Para poder utilizar os serviços oferecidos por finanças descentralizadas ou qualquer outra aplicação descentralizada que use a tecnologia blockchain, é necessário a criação de uma carteira de criptomoedas [10]. Tal carteira, por sua vez, é um software que armazena duas chaves, sendo uma pública, usada para identificar uma conta na rede, e outra privada, que é usada como assinatura para comprovar o proprietário da chave pública, ou seja, o proprietário da conta [11].

Embora seja seguro compartilhar a chave pública, isto é, o endereço da carteira, nunca se deve compartilhar ou divulgar a chave privada a terceiros. A chave privada pode ser usada para acessar os fundos da conta e assinar novas transações. Isso significa que, se alguém conseguir a chave privada da conta, os fundos nela contidos podem ser roubados.

Por fim, as carteiras de criptomoedas costumam ser classificadas em dois tipos, como indicado a seguir:

- Carteiras quentes: São carteiras de criptomoedas que de alguma forma estão conectadas à Internet. Por exemplo:
  - Carteira de Desktop: São programas de software que podem ser baixados para um laptop ou PC.
  - Carteira móvel: As carteiras móveis são carteiras baseadas em aplicativos que podem ser usadas em celulares. Para ultilizá-la é preciso fazer o download e instalação no dispositivo móvel. Elas oferecem extrema conveniência, pois é possível fazer negociações com o uso de QR code, tornando-as a opção mais viável para gastar criptomoedas.
  - Carteira Web: As carteiras Web estão disponíveis online e podem ser acessadas por meio de um navegador, sem a necessidade de baixar nenhum aplicativo ou programa. Nesse tipo de carteira, alguns provedores mantêm e gerenciam as chaves privadas, como é o caso das carteiras Web das corretoras centralizadas. Embora possa parecer conveniente, usar uma carteira Web é bastante perigoso pelo fato de não se ter acesso às chaves privadas da carteira. Existem inúmeros casos famosos de corretoras hackeadas, alguns deles serão observados na análise SWOT discutida no Capítulo 5.
- Carteiras frias: São uma alternativa mais segura às carteiras quentes. Eles não estão conectados à Internet e armazenam fisicamente as chaves públicas e privadas offline. São elas:
  - Carteiras de hardware: São aquelas onde as criptomoedas são armazenadas offline em um dispositivo físico eletrônico.
  - Carteiras de papel: São carteiras que podem ser impressas. Eles contêm suas chaves públicas e privadas, que geralmente estão na forma de um QR code. É preciso escanear o QR code para acessar a carteira e para executar transações.

2.6 Stablecoins

Nas finanças descentralizadas, para que certos serviços financeiros ocorram, é necessário que o acordo esteja vinculado a uma moeda estável, visto que os riscos e as incertezas nos contratos aumentam quando a volatilidade do ativo é alta. As criptomoedas possuem alta volatilidade quando comparadas com moedas fiduciárias (emitidas pelos governos). Assim, com o objetivo de resolver esse problema, foram criadas as *stablecoins*, que, como o próprio nome sugere, são ativos com baixa volatilidade no preço [12]. Ademais, no mercado existe uma vasta gama de stablecoins disponíveis, contudo, aquelas que possuem paridade com o dólar americano são as mais utilizadas. Isso significa que, para cada emissão de uma stablecoin, um dólar será mantido em um custodiante central, como um banco [12].

2.7 Algoritmos de Consenso: Prova de Trabalho e Prova de Participação.

Conforme foi mencionado anteriormente, a blockchain do Bitcoin, do Ethereum e das outras criptomoedas descentralizadas prometem a possibilidade do envio do dinheiro digitalmente sem o envolvimento de qualquer autoridade central. Para que isso aconteça, são utilizados algoritmos de consenso, que são procedimentos através dos quais todos os nós na rede da blockchain chegam a um acordo sobre o estado atual do livro-razão. A priori, a solução proposta por Satoshi Nakamoto [1] para gerenciar uma blockchain, isto é, registrar e processar as transações em um livro-razão compartilhado, foi de utilizar um algoritmo de consenso chamado de prova de trabalho [1], que é conhecido como uma competição na qual computadores, também chamados de mineradores, tentam achar a solução para um problema matemático através de um processo de tentativa e erro. Sendo assim, quem encontrar a solução primeiro, ganha o direito de escrever o próximo bloco na blockchain, além de receber uma recompensa por isso. Então, quanto mais poder computacional uma máquina possuir, mais suposições por segundo ela poderá fazer, aumentando, desse modo, as suas chances de ganhar esse concurso. Ademais, o nome prova de trabalho advém do fato de que, para exibir a solução correta, os mineradores provam que "trabalharam" muito, uma vez que não há outra maneira de chegar à solução do problema matemático além de usar poder computacional para tentar, constantemente, achar a solução.

No entanto, embora o mecanismo de consenso de prova de trabalho seja uma solução confiável e segura para gerenciar um livro-razão descentralizado, executar todos esses computadores apenas para achar um número consome muita energia [13], entre outras desvantagens. Por isso, outros mecanismos de consenso foram sugeridos ao longo dos anos. Por conseguinte, uma alternativa muito popular é a prova de participação. Nesse algoritmo de consenso, é preciso que seja bloqueada uma certa quantia de fundos em um computador que está conectado à rede. Isto é, em termos técnicos, esse computador é chamado de nó e os fundos bloqueados são a participação. Assim que a participação for realizada, a pessoa se torna um validador e participa do concurso de qual nó irá forjar o próximo bloco. Dessa maneira, o vencedor é escolhido levando-se em consideração vários fatores, como quanto dinheiro e há quanto tempo ele está bloqueado, além de randomização para que nenhuma entidade com grande capital obtenha o monopólio da participação [14]. De modo geral, quem ganha o concurso consegue forjar o próximo bloco de transações e é recompensado em moedas por sua contribuição para a rede. No entanto, caso o validador tente forjar dados incorretos, será penalizado, perdendo parte da sua participação.

No Quadro 1, são descritas as principais diferenças entre os algoritmos de consenso de prova de trabalho e prova de participação. Como pode ser observado, mineradores e validadores são as nomenclaturas utilizadas para identificar, respectivamente, os nós da rede de uma blockchain que utiliza prova de trabalho e prova de participação. Conforme explicado anteriormente, na prova de trabalho, apenas o primeiro minerador que encontrar a solução será recompensado, enquanto que o restante apenas irá ter desperdiçado energia. Isso não ocorre na prova de participação visto que o próprio algoritmo seleciona quem irá forjar o próximo bloco, o que o torna mais eficiente.

Com relação às recompensas, essas costumam ser fornecidas aos mineradores mediante blocos minerados, enquanto que os validadores recebem recompensas nas taxas cobradas pelas transações forjadas na blockchain.

Por fim, quanto maior o número de nós na rede mais difícil de ela ser hackeada. Para hackear uma blockchain que utiliza prova de trabalho, é necessário ter mais de 50% do poder computacional da rede, enquanto que, para a prova de participação, é preciso mais de 50% na participação (fundos bloqueados). Como na prova de participação o hacker necessita de recursos financeiros investidos na rede, caso ele obtenha sucesso no ataque, os seus próprios ativos irão se desvalorizar, desincentivando a prática.

Quadro 1: Prova de trabalho vs prova de participação. Adaptada de https://www.wallstreetmojo.com/proof-of-stake-vs-proof-of-work/

2.8 Corretoras de Criptomoedas

Corretoras de criptomoedas são plataformas que permitem a compra e venda de criptomoedas. Elas costumam ser categorizadas em dois tipos: corretoras de criptomoedas centralizadas e corretoras de criptomoedas descentralizadas. As corretoras de criptomoedas centralizadas, como, por exemplo, a Binance, Coinbase, Mercado Bitcoin e BitcoinTrade, atuam como terceiros entre um comprador e um vendedor. Nessas plataformas, todos os usuários depositam na carteira da empresa e negociam criptomoedas sob o controle delas.

Já as corretoras descentralizadas são uma plataforma de negociação de criptomoedas baseada em contratos inteligentes, na qual não existe a necessidade de depositar qualquer confiança em terceiros. Nessas plataformas, os usuários negociam diretamente de suas carteiras, interagindo com os contratos inteligentes por meio da plataforma de negociação.

Além disso, nas corretoras de criptomoedas descentralizadas, não há a necessidade de se inscrever na plataforma ou fornecer informações pessoais, como ocorre nas corretoras centralizadas, visto que as transações são feitas apenas com o endereço da carteira.

A desvantagem das corretoras de criptomoedas descentralizadas é sua falta de liquidez quando comparada às corretoras de criptomoedas centralizadas que, por serem mais fáceis de usar, são mais populares e, consequentemente, possuem maior liquidez. Dessa forma, transações de corretoras descentralizadas podem demorar mais tempo para serem executadas.

Contudo, corretoras de criptomoedas descentralizadas não possuem riscos de serem hackeadas, visto que os próprios usuários estão com as posses de seus ativos, enquanto que, em corretoras de criptomoedas centralizadas, pelo fato de possuírem controles dos ativos de seus clientes, tornam-se alvos de hackers.

Figura 6 apresenta um gráfico com uma comparação entre o volume diário de negociação entre corretoras centralizadas e descentralizadas. Conforme pode ser observado, no dia 16 de março de 2021, por exemplo, o volume diário de negociações foi de 56,33 bilhões de dólares na corretora centralizada da Binance contra apenas 3,64 bilhões de dólares na corretora descentralizada da Uniswap, um valor 15 vezes menor [15]. Por fim, a Figura 7 resume o que foi explicado nesta seção.

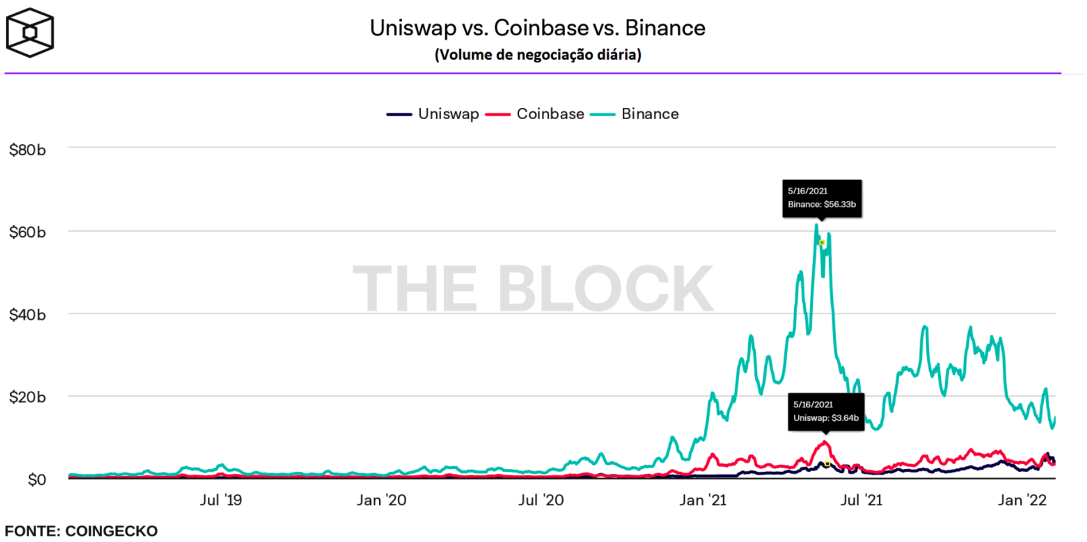

Figura 6: Comparação do volume diário de negociação entre a corretora descentralizada Uniswap e as corretoras centralizadas Coinbase e Binance. Adaptada de https://www.theblockcrypto.com/data/decentralized-finance/dex-non-custodial/uniswap-vs-coinbase-and-binance-trade-volume-7dma

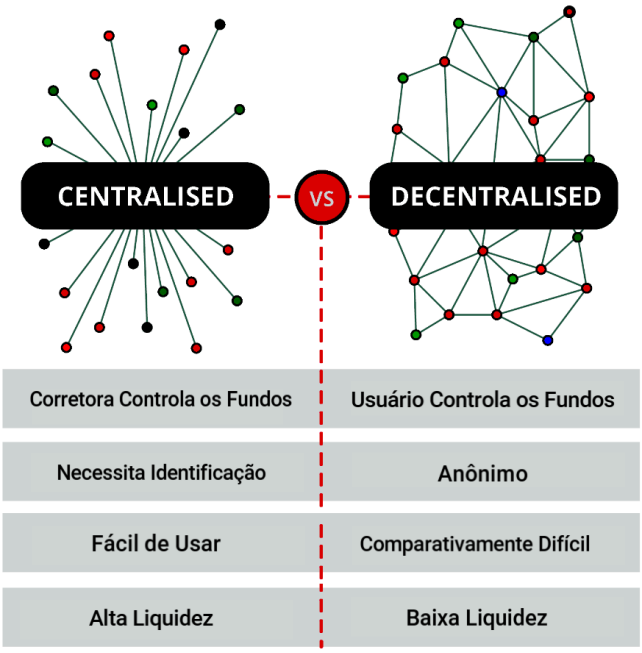

Figura 7: Corretora centralizada vs corretora descentralizada. Adaptada de https://coincasso.com/blockchain-academy/how-do-cryptocurrency-exchanges-work/

2.9 Formador de Mercado Automatizado e Piscinas de Liquidez

Sabe-se que, nas primeiras corretoras descentralizadas, quando um usuário registrava seu interesse de compra/venda em um livro de ofertas, que é o local onde o investidor consegue visualizar as ordens de compra e venda que estão em negociação no mercado, e um outro usuário aceitava a troca, a transação era feita por meio de um contrato inteligente, usando diretamente as carteiras pessoais dos envolvidos. Desse modo, o principal problema dessas trocas era a falta de liquidez nas corretoras descentralizadas. Como resultado, a diferença entre os preços de compra e venda mais próximos podiam divergir significativamente, especialmente em pares de criptoativos pouco conhecidos.

Por conseguinte, essa deficiência foi corrigida com o desenvolvimento da tecnologia de formador de mercado automatizado. Que é um tipo de protocolo que depende de uma fórmula matemática, para definir os preços dos ativos [6].

Dessa maneira, em corretoras descentralizadas baseadas em formador de mercado automatizado, o livro de ofertas tradicional é substituído por piscinas de liquidez. Uma piscina de liquidez é um contrato inteligente, que é responsável por bloquear criptoativos em uma corretora descentralizada, fornecendo, então, um fundo de reservas dos ativos que garante uma maior liquidez no mercado descentralizado da corretora.

2.10 Considerações Finais

Neste capítulo, foram apresentados os conceitos básicos que existem nas finanças descentralizadas e foram encontrados na revisão da literatura analisada. Eles são necessários para um melhor entendimento dos próximos capítulos. A seguir, serão discutidos os trabalhos relacionados a esse trabalho de conclusão de curso.

3 Trabalhos Relacionados

Neste capítulo, será exibido um resumo dos artigos acadêmicos relacionados ao tema do trabalho discutido nesse documento, com a finalidade de expor e de reunir informações relevantes que auxiliem no cumprimento do objetivo geral, ou seja, na verificação de se os serviços ofertados nas finanças descentralizadas proporcionam reais benefícios quando comparados com os serviços ofertados nas finanças centralizadas.

Na literatura analisada, não existem estudos com foco nos serviços ofertados em finanças descentralizadas. Como será observado a seguir, os trabalhos relacionados concentram-se nas terminologias, nas métricas, na tecnologia da blockchain e nos benefícios que se pode alcançar com o uso de *DeFi* em finanças.

3.1 Fabian Schär 2021

Em "Decentralized Finance: On Blockchain and Smart Contract-Based Financial Markets", o autor apresenta os conceitos básicos de finanças descentralizadas, como o conceito de aplicações descentralizadas, contratos inteligentes, stablecoins, entre outros termos já discutidos no capítulo anterior. O autor também aborda o valor total bloqueado (TVL) que, no contexto das criptomoedas, representa a soma de todos os ativos depositados em protocolos de finanças descentralizadas (*DeFi*). Figura 8 apresenta o histórico de valor total bloqueado até a data de 29 de dezembro de 2021. Conforme pode ser observado, em menos de 5 anos, o valor total bloqueado em finanças descentralizadas passou dos milhares para os milhões e, no momento da escrita desse trabalho, encontra-se em 99,65 bilhões de dólares.

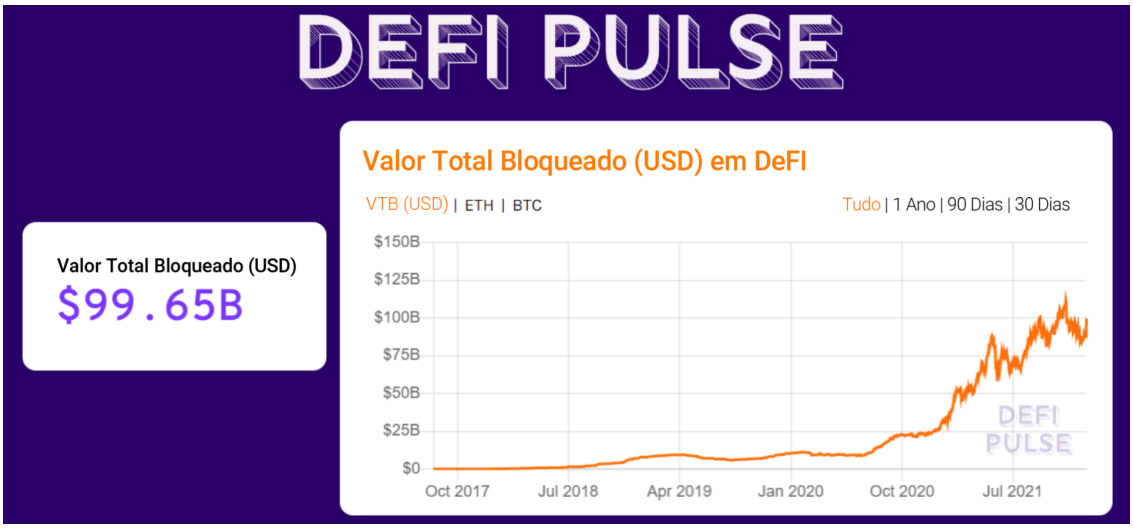

Figura 8: Total de valor bloqueado em Finanças descentralizadas. Adaptada de https://www.defipulse.com/

Em "Decentralized Finance: On Blockchain and Smart Contract-Based Financial Markets", são também discutidas as oportunidades e os riscos de se usar finanças descentralizadas, no entanto, o autor não faz comparações com os serviços das finanças centralizadas, tópicos que serão abordados no capítulo 5 (análise swot) . Por fim, é concluído que, embora finanças descentralizadas tenham um grande potencial, existem certos riscos envolvidos, como, por exemplo, os contratos inteligentes apresentarem problemas de segurança que podem permitir o uso deles de forma indevida. Contudo, as finanças descentralizadas podem levar a mudanças de paradigmas no setor financeiro, pois tem o potencial de criar uma infraestrutura financeira mais robusta, aberta, transparente e imutável [6].

3.2 Robert Donald Leonhard 2019

"Decentralized finance on the ethereum blockchain" mostra como as finanças descentralizadas podem ser uma alternativa contra a desvalorização do dinheiro estatal motivada por ações políticas insustentáveis, como também para a proteção de capital contra o confisco financeiro por parte de governos autoritários. O autor argumenta que as finanças descentralizadas podem garantir o poder de compra de cidadãos que vivem em países instáveis, como a Venezuela, e relata, através de dois casos hipotéticos, os possíveis instrumentos financeiros fornecidos pelas finanças descentralizadas, evidenciando os benefícios e vantagens do uso da tecnologia de blockchain.

Mesmo tendo sido escrito em 2019 com foco em narrativas ocorridas na Venezuela durante a hiperinflação, atualmente, também é possível evidenciar casos de uso das finanças descentralizadas além dos citados pelo autor, como, por exemplo, no bloqueio de saques em bancos durante a invasão do Talibã no Afeganistão, no congelamento de contas bancárias feito pelo governo do Canadá para os envolvidos em protestos anti vacina e na suspensão de saques em bancos da Ucrânia e da Rússia durante a invasão efetuada pelo presidente Vladimir Putin em 2022.

Para concluir, o autor relata que finanças descentralizadas podem ser uma opção de último recurso para refugiados que escapam do colapso político e social, sendo uma maneira viável de armazenar com segurança a riqueza de uma pessoa de forma que acumule juros, evitando que o governo e suas medidas se apropriem do seu dinheiro, mesmo que temporariamente, ou desvalorizem seu capital através da inflação.

3.3 Campbell R. Harvey, Ashwin Ramachandran & Joey Santoro 2021

"DeFi and the Future of Finance" relata como o sistema financeiro atual é excludente e fornece o número de pessoas sem contas bancárias ao redor do mundo, como também as porcentagens cobradas a pequenos negócios pelas empresas de cartão de crédito [16]. Os autores ainda argumentam que esse sistema gera menos investimentos e diminui o crescimento econômico e que as finanças descentralizadas possuem potencial para solucionar os problemas inerentes à infraestrutura das finanças tradicionais.

Os autores também relatam as formas de escambo existentes no passado e afirma que o sistema era altamente ineficiente, visto que um comprador e vendedor ou prestador de serviço necessitavam que suas necessidades fossem exatamente combinadas para que a troca ocorresse. Este problema foi resolvido com o surgimento do dinheiro como meio de troca e reserva de valor. Inicialmente, o dinheiro não era centralizado e inúmeros itens já foram utilizados para esse propósito, como pedras ou conchas, em troca de mercadorias. Eventualmente, surgiu o dinheiro em espécie da forma que conhecemos hoje, no qual seu controle é feito pelos bancos centrais. O autor alega que enquanto a forma do dinheiro mudou ao longo da história da humanidade, a infraestrutura básica das instituições financeiras permanece praticamente a mesma.

Diante desse cenário, os autores acreditam que finanças descentralizadas serão e já estão sendo uma disrupção da atual infraestrutura financeira, por se tratar de uma tecnologia que fornece ao usuário, produtos financeiros sofisticados com custos reduzidos. Eles também afirmam que esta é uma tecnologia de inclusão pela qual qualquer pessoa pode pagar uma taxa fixa para usar e se beneficiar das inovações do *DeFi*.

Os autores afirmam que um dos problemas das finanças centralizadas é seu controle centralizado, alegando que a maioria dos consumidores e empresas lidam com um único

banco que controla taxas e encargos. Outro problema nas finanças centralizadas é seu acesso limitado, visto que 1,7 bilhão de pessoas não têm conta bancária, o que torna difícil para esses indivíduos obterem empréstimos ou operarem comercialmente através da Internet. Esse tema será abordado na análise SWOT detalhada no Capítulo 5. Além disso, finanças centralizadas possuem ineficiências, como, por exemplo, a taxa do cartão de crédito de 2-3% cobrada a empresas que oferecem essa opção a seus clientes. Outros problemas incluem o tempo para "liquidar"uma transação de ação (transferir oficialmente a propriedade), além disso, existem outras ineficiências, como taxas de corretagem e transferências, que podem ser lentas. Muitas dessas ineficiências não são óbvias para os usuários. No sistema bancário atual, as taxas de juros dos depósitos permanecem muito baixas e as taxas de empréstimos são altas, porque os bancos precisam cobrir seus custos físicos.

Outro problema enfrentado nas finanças centralizadas é sua falta de transparência. Os clientes de bancos têm muito pouca informação sobre a sua saúde financeira e devem confiar na proteção limitada do governo, como o FGC (fundo garantidor de crédito) que permite recuperar créditos em instituições financeiras em caso de falência, intervenção ou liquidação, dentro dos limites definidos. Além disso, os clientes dos bancos que procuram um empréstimo também possuem dificuldade em determinar se a taxa oferecida é competitiva.

Por fim, serviços de *DeFi* oferecem potencial para resolver os problemas citados acima associados às finanças centralizadas, assunto que será abordado no Capítulo 4.

3.4 Estudo Comparativo

Como mencionado inicialmente, os trabalhos acadêmicos analisados focam seus estudos nas terminologias, nas métricas e na tecnologia da blockchain. Contudo, os trabalhos supramencionados fornecem estudos que contribuem para o objetivo principal desse TCC, o qual visa analisar se os serviços ofertados nas finanças descentralizadas proporcionam reais benefícios quando comparados com os serviços ofertados nas finanças centralizadas. Embora os trabalhos analisados abordem o tema de finanças descentralizadas, como seus conceitos básicos, casos de uso e benefícios, pouco é o estudo que se observa na comparação dos serviços ofertados pelo sistema financeiro tradicional com os serviços ofertados nas finanças descentralizadas, que é o foco central desse trabalho de graduação.

3.5 Considerações Finais

Conforme foi apresentado, os artigos científicos focam em apresentar as vantagens e desvantagens da tecnologia de finanças descentralizadas, mas pecam em elucidar as diferenças entre os serviços ofertados nas finanças centralizadas e nas finanças descentralizadas. Nesse trabalho, o objetivo principal é elucidar finanças descentralizadas, com o foco nos serviços disponíveis, comparando-os com os serviços ofertados nas finanças centralizadas.

4 Serviços de Finanças Descentralizadas

Este capítulo tem como objetivo elucidar os principais serviços ofertados atualmente nas finanças descentralizadas. Comparações com os serviços oferecidos em finanças centralizadas serão realizadas com o intuito de alcançar o objetivo principal desse trabalho de conclusão de curso.

4.1 Staking

Staking significa receber renda passiva ao bloquear criptomoedas de uma blockchain, que utiliza como algoritmo de consenso prova de participação. Conforme explicado anteriormente, o algoritmo de consenso é a forma como os nós de uma blockchain verificam se os dados inseridos no bloco estão corretos. No algoritmo de consenso, chamado prova de participação, os validadores precisam bloquear suas criptomoedas para se tornarem elegíveis a validar novos blocos. Atualmente, existem muitas blockchains que utilizam prova de participação como algoritmo de consenso e cada uma delas possui seu próprio mecanismo de recompensa. Por isso, será realizada uma apresentação da prova de participação da blockchain do Ethereum.

O Ethereum foi inicialmente desenvolvido baseado no mesmo algoritmo de consenso do Bitcoin, chamado de prova de trabalho. Contudo, visando torná-lo mais escalável, seguro e sustentável, os desenvolvedores optaram pela mudança do algoritmo de consenso da rede para prova de participação [17]. Até 2020, a blockchain do Ethereum era baseada puramente em prova de trabalho, mas em dezembro de 2020 foi criada uma nova blockchain chamada de "Beacon chain", popularmente conhecida como Ethereum 2.0, que utiliza como algoritmo de consenso a prova de participação, que é executada em paralelo à blockchain original (Ethereum 1.0).

Para participar como validador do Ethereum 2.0, é necessário bloquear trinta e dois Ether como garantia. Não há como bloquear mais de trinta e dois Ether em um único nó, e caso o usuário tenha interesse em aumentar sua recompensa, será necessário configurar vários nós com trinta e dois Ether cada. Após o usuário se tornar um validador, ele fica elegível a receber recompensas pela participação. De acordo com os desenvolvedores, o Ethereum 2.0 será implantado por completo e se fundirá com o Ethereum 1.0 em 2022, tornando sua blockchain 100% à prova de participação. Somente após o merge, os validadores poderão retirar seus Ether e recompensas da participação.

No Ethereum 2.0, cada validador que participa do forjamento de um bloco recebe uma porcentagem do Ether recém-cunhado, quando um novo bloco é criado. Quanto mais validadores a rede possuir, menor será a proporção da recompensa e sua recompensa anual varia de 2%-20%, de acordo com o número de validadores existentes na rede [18]. A cada dia, apenas 900 novos validadores são permitidos na blockchain do Ethereum. No momento da escrita desse TG, existem 13225 validadores pendentes esperando para participar [19], o que dá aproximadamente 15 dias de espera. Além disso, configurar seu próprio validador requer conhecimento técnico, um computador dedicado e trinta e dois Ether. Caso o usuário não configure seu validador corretamente, ou se ele ficar offline ou for prejudicial à rede de alguma forma, poderá estar sujeito a penalidades, como destruição de parte de sua participação ou até mesmo estar sujeito à remoção da rede como validador.

Devido aos riscos mencionados, alternativas adicionais de staking foram criadas buscando permitir que o usuário comum faça participação no Ethereum e ganhe recompensas, como um validador da rede sem ter que se preocupar com os esforços e riscos de executar

seu próprio nó. A maneira mais fácil de fazer staking para uma pessoa não experiente na tecnologia seria usar os serviços de participação fornecidos pelas corretoras centralizadas. Isso elimina completamente o incômodo de executar seu próprio validador e o usuário pode participar com valores menores do que trinta e dois Ether, contudo as taxas cobradas pelas corretoras para disponibilizar esse tipo de staking podem ser altas e o usuário não tem controle sobre suas criptomoedas, uma vez que elas ficam custodiadas pela corretora intermediária. Algumas corretoras também permitem que o usuário reivindique suas recompensas da participação sem a necessidade de espera até que o merge do Ethereum 2.0 seja concluído.

Outra opção é participar de uma piscina de staking, que significa juntar a liquidez de vários usuários até chegar no valor mínimo de trinta e dois Ether, que é o pré-requisito para a criação de um nó. Cada usuário que participa da piscina de staking recebe a recompensa proporcionalmente ao tamanho do aporte que foi deixado na piscina. Uma piscina de staking pode ser composta de vários nós para obter uma melhor chance de forjar o próximo bloco.

Se o usuário decidir optar por entrar em uma piscina de staking, é importante pesquisar certos aspectos da piscina; como confiabilidade de seus validadores, taxa de manutenção cobrada pela piscina, suporte ao cliente, tamanho da piscina, avaliações de usuários e se você é obrigado ou não a ceder suas chaves privadas à piscina.

Por fim, existe o validador como opção de serviço, que são empresas que permitem que o usuário execute seu próprio validador em seus computadores sem a necessidade de configurá-los ou mantê-los. Como esse é um validador pessoal, o usuário precisará depositar trinta e dois Ether e pagar uma certa taxa por esse serviço. O melhor dessa opção é que é relativamente fácil de configurar e você não precisa dar o controle de suas moedas para a empresa.

4.2 Empréstimo

Empréstimo é um dos serviços mais populares em finanças centralizadas [12], visto que permite que o tomador do empréstimo compre bens ou serviços e efetue o pagamento posteriormente. Nesse contexto, assim que o empréstimo é concedido, o tomador do empréstimo começa a acumular juros a uma taxa previamente acordada por ambas as partes e, no seu vencimento, o mutuário, isto é, o tomador do empréstimo, deve pagar a dívida acrescida dos juros vencidos.

Logo, nessa negociação sempre existe o risco do devedor deixar de pagar o empréstimo dentro do prazo. Então, para evitar que isso ocorra, o credor, por exemplo, um banco, costuma seguir uma rigorosa política de crédito antes de decidir se vai conceder um empréstimo a um mutuário. Além disso, em alguns casos específicos, também costuma-se aceitar garantias, como bens móveis, bens imóveis e entre outros ativos, para mitigar o risco de calote.

Ademais, é importante salientar que, nas finanças descentralizadas, não há requisito de pontuação de crédito, por isso, a maioria dos protocolos apenas permitem empréstimos colateralizados, isto é, exige-se garantias para que se possa liberar o crédito.

Portanto, o tomador é obrigado a fornecer uma garantia maior do que o valor em crédito que se deseja adquirir. Assim, a maioria das plataformas que permitem esse tipo de serviço concede como empréstimo até 50-80% da garantia. Então, tanto o credor quanto o tomador depositam os seus criptoativos em um contrato inteligente e este, por sua vez, se encarrega em administrá-los, com o intuito de que o empréstimo ocorra conforme

previamente acordado.

Diante do exposto, se o preço do criptoativo dado como garantia cair ou o preço do criptoativo emprestado aumentar próximo ao valor do empréstimo, a garantia é liquidada à força, de acordo com as regras do contrato inteligente, inviabilizando, desta forma, a possibilidade de calote. Portanto, a principal vantagem desse sistema, para aqueles que precisam de um empréstimo, são as baixas taxas de juros cobradas, quando comparadas com aquelas oferecidas no mercado tradicional e, para aqueles que efetuam o empréstimo, tem-se a oportunidade de atuar como verdadeiros banqueiros, recebendo, praticamente, todo o lucro obtido dos juros acumulados na transação.

Figura 9 elucida uma transação de empréstimo em finanças descentralizadas. Como pode ser observado no exemplo apresentado, o usuário que fornece o empréstimo deposita dinheiro fiduciário na plataforma e recebe após um período de tempo o empréstimo realizado acrescido de juros, enquanto que, o usuário que deseja realizar o empréstimo, deposita seus criptoativos como garantia, recebe o empréstimo e, após o seu pagamento acrescido dos juros, recebe sua garantia de volta.

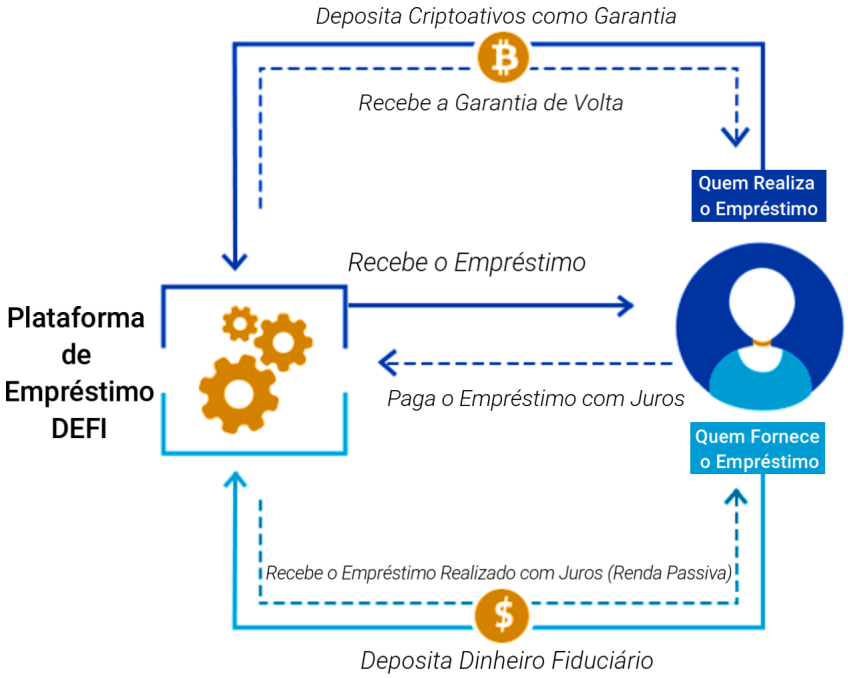

Figura 9: Funcionamento das plataformas de empréstimos em finanças descentralizadas.
Adaptada de https://www.leewayhertz.com/how-defi-lending-works/

4.3 Mineração de Liquidez

Mineração de liquidez significa obter lucros ao fornecer liquidez para uma corretora descentralizada, baseada em formador de mercado automatizado. Dessa maneira, quando ocorre uma troca em uma corretora descentralizada baseada em formador de mercado automatizado, uma taxa de transação é cobrada para cada troca efetuada e é, também, entregue para os provedores de liquidez da piscina, incentivando, portanto, os usuários, para que eles coloquem os seus criptoativos nessas piscinas em troca de rendimentos passivos.

Figura 10 apresenta como corretoras descentralizadas baseadas em formador de mercado automatizado funcionam. Conforme pode ser observado, os provedores de liquidez depositam dois pares de criptoativos (A & B) em uma piscina de liquidez, para formar a

base da transação, como, por exemplo, uma piscina de liquidez com a mesma quantidade de pares USDT e Ethereum. Os usuários que desejarem trocar esses ativos, poderão usar essa piscina de liquidez para negociar USDT e Ethereum a um preço automatizado.

Logo, se for assumido que o USDT é trocado por Ethereum, o USDT, na piscina de liquidez, aumenta e o Ethereum diminui após a troca, fazendo com que o preço do ativo mais escasso aumente. Por outro lado, se o preço do Ethereum aumentar devido à troca, pode haver uma diferença no preço do Ethereum quando comparado ao valor ofertado por outras corretoras. Nesse caso, detentores de Ethereum costumam vendê-los a um preço mais alto e recompram a um preço menor em outra corretora e esta operação é conhecida no mercado financeiro como arbitragem (Figura 11). Eventualmente, é formado, na corretora descentralizada baseada em formador de mercado automatizado, um preço próximo ao preço de mercado. Assim, as taxas de corretagem, que no mercado tradicional são absorvidas exclusivamente pelas corretoras, agora, são distribuídas de forma justa e proporcional aos provedores de liquidez.

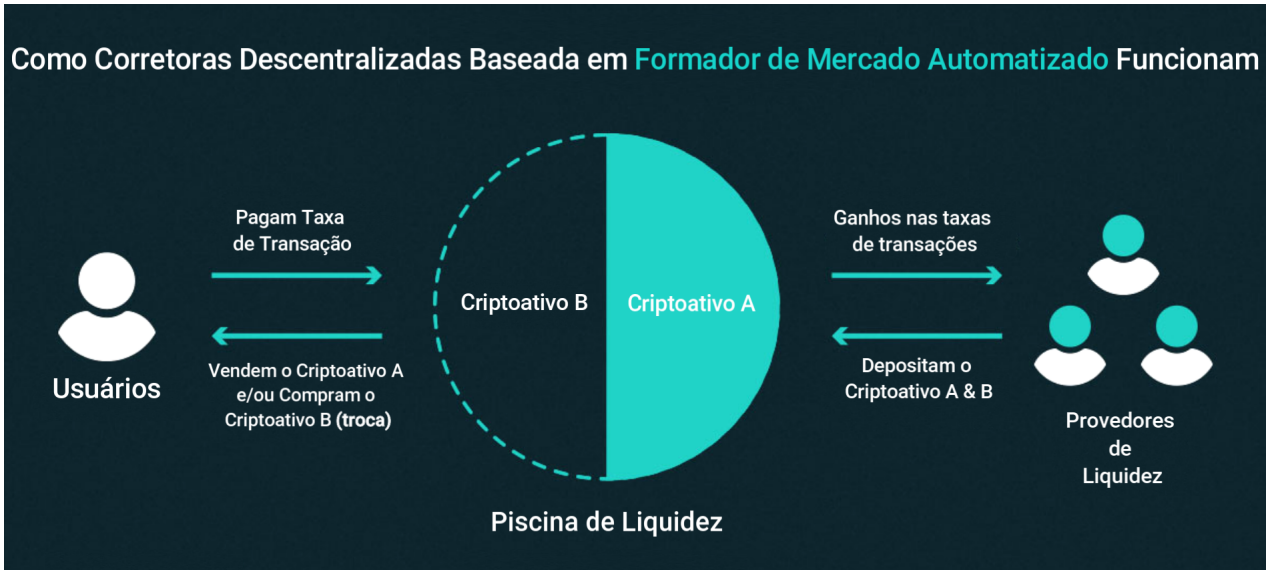

Figura 10: Corretoras descentralizadas baseada em Automated Market Maker (AMM). Adaptada de https://cryptorobin.com/what-are-automated-market-makers/

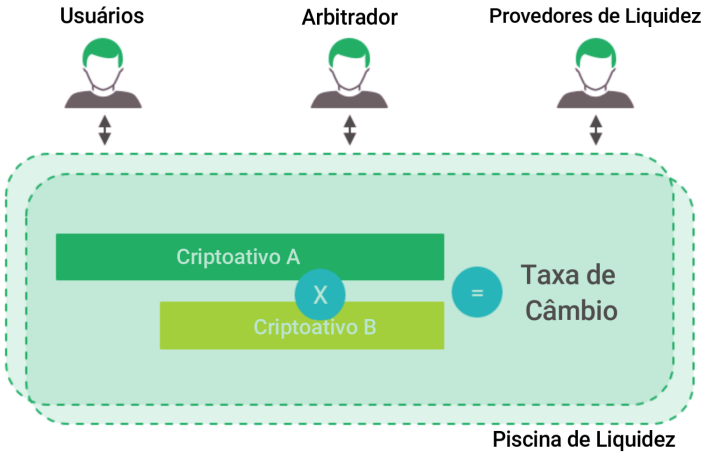

Figura 11: Arbitragem. Adaptada de https://medium.com/liquifiorg/liquifi-a-new-liquidity-pool-dex-that-is-a-golden-cut-for-the-price-slippage-and-front-running-2bbdc5cccfc5

4.4 Outras Aplicações

Conforme explicado no Capítulo 2, finanças descentralizadas caracterizam uma variedade de diferentes aplicações financeiras, com o objetivo de descentralizar serviços financeiros que atualmente são intermediados por instituições financeiras.

Por se encontrar em estágio de desenvolvimento, existem inúmeras aplicações sendo criadas, além das citadas nesse capítulo, que visam ampliar os serviços ofertados nas finanças descentralizadas.

Por exemplo, Synthetix é um protocolo de finanças descentralizadas que fornece exposições a uma ampla variedade de ativos de fora da blockchain, como ações e comódites, mediante ativos sintéticos (produtos que seguem o preço de outro ativo) [6]. Dessa forma, essa aplicação descentralizada visa ampliar o acesso das finanças descentralizadas aos mercados financeiros tradicionais.

Existem outras aplicações em desenvolvimento, como é o caso daquelas voltadas para a área de seguros. Os seguros descentralizados buscam mitigar e cobrir os riscos associados às plataformas de finanças descentralizadas. Essas plataformas de seguros visam proteger os usuários das finanças descentralizadas contra ataques de hackers, e de eventuais falhas ou bugs que possam ocorrer nas aplicações descentralizadas.

Ao contrário dos sistemas centralizados, no qual as pessoas buscam uma instituição como seguradoras, o seguro descentralizado permite que seus usuários forneçam seguro por um determinado período em troca de juros ou comprem seguro por um prazo específico para certos produtos financeiros.

Em suma, existem muitas aplicações em desenvolvimento nas mais diversas áreas, onde a maioria delas faz uso da blockchain da Ethereum. No momento da escrita desse trabalho de conclusão de curso existem 100 bilhões de dólares investidos nesses protocolos de finanças descentralizadas [13], onde a maioria está inserida em aplicações descentralizadas de empréstimos.

4.5 Considerações Finais

É possível notar, nos exemplos de serviços descentralizados apresentados, que certos investimentos, que antes apenas estavam disponíveis aos bancos, corretoras e seguradoras nas finanças centralizadas, podem ser acessados por qualquer pessoa nas finanças descentralizadas, democratizando, dessa forma, os serviços financeiros. A seguir, uma análise SWOT será discutida para melhor identificar os pontos fortes, pontos fracos, oportunidades e ameaças desses serviços.

5 Análise SWOT

A discussão apresentada nos capítulos anteriores fornece ao leitor uma visão geral da tecnologia blockchain e das aplicações no setor de finanças descentralizadas. A seguir, uma análise SWOT resumindo as vantagens e desvantagens dessa tecnologia é fornecida. A análise SWOT é um método que irá permitir identificar os pontos fortes e fracos nas finanças descentralizadas e ajudará a identificar oportunidades e ameaças, que surgem do ambiente considerado na análise. Desse modo, a análise SWOT foi realizada de forma colaborativa, ou seja, foi desenvolvida pelo autor do trabalho com base na bibliografia analisada, sendo cada um dos pontos catalogados entre forças, fraquezas, oportunidades e ameaças. Tabela 1 apresenta os principais artigos utilizados durante o desenvolvimento da análise SWOT.

Autor	Artigo
NAKAMOTO, Satoshi	Bitcoin: A Peer-to-Peer Electronic Cash System
BUTERIN, Vitalik	A Next Generation Smart Contract & Decentralized Application Platform
PAKENAITE, Simona; TAUJANSKAITE, Kamile	Investigation of the Blockchain's Influence on Traditional Banking: Challenges and Opportunities
ZHENG, Zibin	An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends
SCHAR, Fabian	Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets
BERENTSEN, Aleksander; SCHAR, Fabian	A Short Introduction to the World of Cryptocurrencies
SCHA, Fabian	Stablecoins: The quest for a low- volatility cryptocurrency
LEONHARD, Robert	Decentralized Finance on the Ethereum Blockchain

Tabela 1: Principais artigos utilizados durante o desenvolvimento da análise SWOT.

5.1 Forças

Os pontos fortes das finanças descentralizadas estão, principalmente, relacionados aos aspectos tecnológicos apresentados no Capítulo 2. A seguir, serão enumerados os pontos fortes mais frequentes encontrados na literatura analisada.

5.1.1 Desintermediação

A desintermediação é definida como a redução no uso de intermediários. No setor financeiro, isso ocorre, por exemplo, quando um investidor consegue comprar ações diretamente, em vez de adquiri-las por meio de uma corretora ou instituição financeira.

Atualmente, os contratos, as transações e outras operações da economia são administrados por autoridades públicas ou privadas, ou seja, instituições centrais. No entanto, a tecnologia da blockchain, dos contratos inteligentes e das finanças descentralizadas permitem que essas transações ocorram de forma segura e sem a necessidade de instituições centrais.

5.1.2 Redução dos Custos

Ao remover intermediários, os custos de certas operações podem ser reduzidos, por exemplo, nas finanças centralizadas, os bancos continuam com altos custos de transação e, dependendo da instituição financeira na qual se opere, ainda existem cobranças para realização de transferências bancárias utilizando o TED ou DOC. Vale mencionar que as

taxas cobradas só aumentam ao se expandir os horizontes para transferências internacionais. Milhões de trabalhadores em todo o mundo fazem transferências diárias de dinheiro para seus países de origem, tendo que arcar com altos custos de transferência que podem levar dias para serem concluídas [14].

Além disso, existem as taxas de corretagem cobradas por algumas corretoras no mercado financeiro, quando o cliente exerce o seu desejo de comprar ou vender um ativo financeiro. Então, tem-se que, por meio das finanças descentralizadas, muitas comissões exercidas por instituições financeiras centralizadas deixam de existir graças à desintermediação proporcionada pela tecnologia blockchain.

5.1.3 Transparência

Em finanças descentralizadas, todas as transações, dados e códigos na blockchain estão disponíveis publicamente. Para se ter acesso a essas informações, usa-se exploradores de blockchain que permitem a qualquer pessoa o acesso/pesquisa do conteúdo dos blocos [20]. Este grau de transparência nunca existiu dentro do sistema financeiro tradicional, visto que as instituições financeiras são livros fechados e, por exemplo, o usuário não pode pedir para ver seus históricos de transações ou empréstimos.

5.1.4 Anonimato

Para abrir uma conta bancária no Brasil, é necessário apresentar uma documentação adequada, como CPF, RG ou carteira de motorista às autoridades do banco. Processos similares de identificação são necessários para criação de contas bancárias em outros países.

Para abrir uma conta nas finanças descentralizadas, os usuários não precisam fornecer qualquer prova de suas identidades. Como explicado no Capítulo 2, basta gerar uma carteira de criptomoeda, isto é, um par de chaves e usar a chave pública como número da conta para receber fundos. Cada conta pode ser acessada usando a chave privada dessa conta e nenhuma identificação é necessária. Embora todas as transações sejam de conhecimento público, ou seja, qualquer pessoa pode acessar as transações e os respectivos valores transacionados, não há qualquer mapeamento público entre a identidade de um usuário e seu número de conta. Em finanças centralizadas, isso é o que acontece de forma semelhante, no histórico de negociações em bolsa de valores, em que a quantidade comprada ou vendida é de conhecimento público, mas os vendedores e compradores não são identificáveis.

5.1.5 Horário de Funcionamento

Para realizar uma transação ou comprar um ativo financeiro no mercado financeiro tradicional, é preciso ficar atento ao horário de funcionamento da instituição em questão. Por exemplo, bancos costumam operar nos dias úteis, em horários comerciais e a abertura das bolsas de valores também possuem horários específicos e, por serem localizadas em diferentes países, existe a possível inconveniência do fuso horário. Em finanças descentralizadas, isso não ocorre, isto é, todas as transações são realizadas o tempo todo (não há a restrição de adoção de um horário específico de trabalho).

5.1.6 Maior Automação

Contratos inteligentes garantem uma maior automação dos serviços financeiros descentralizados e, como foi exposto no Capítulo 2, um contrato inteligente é um pedaço de

código que, uma vez armazenado na blockchain, executa sua tarefa de forma autônoma.

Os contratos inteligentes podem substituir os contratos tradicionais devido ao fato de que o código do contrato é conhecido com antecedência e não pode ser alterado por agentes mal intencionados.

Por exemplo, um contrato inteligente pode ser usado para fazer um empréstimo de forma autônoma e segura, sem a necessidade de um intermediário e, além disso, criam-se as mais diversas possibilidades, como, por exemplo, pagar automaticamente um artista musical cada vez que sua música for tocada na rádio [14].

5.1.7 Segurança na Transação

Alterar as transações em um livro-razão compartilhado (blockchain) é quase impossível, visto que cada transação que ocorre na blockchain é espalhada e armazenada em cada um dos nós (computadores da rede). Além disso, cada novo bloco é validado pelos nós, ou seja, todas as transações são verificadas.

Como apresentado no Capítulo 2, para blockchains que utilizam prova de trabalho como algoritmo de consenso, é necessário deter mais de 50% de todo o poder de processamento da rede para alterar uma transação e continuar alterando transações mais rapidamente que o resto dos usuários da rede e para blockchains que utilizam prova de participação, é necessário mais de 50% dos fundos bloqueados da rede.

Já os livros centralizados enfatizam o alto controle institucional que podem ser destruídos, invadidos ou comprometidos, resultando na manipulação dos dados originais.

5.2 Fraquezas

Essa seção inclui a segunda parte de uma análise SWOT onde os pontos fracos das finanças descentralizadas, ou seja, suas limitações são elencadas.

5.2.1 Complexidade

Embora finanças descentralizadas possuam benefícios, os usuários podem achar sua usabilidade complexa e difícil de entender. No Capítulo 4, foram apresentados alguns dos serviços mais populares em finanças descentralizadas e, foi visto que exceto o serviço de empréstimos, todos os outros investimentos não estão no domínio do usuário comum, que apenas está acostumado aos serviços financeiros tradicionais ofertados nas finanças centralizadas.

Além disso, interagir com finanças descentralizadas requer algumas habilidades técnicas, como, por exemplo, saber instalar uma carteira de criptomoedas, habilitá-la a poder interagir com contratos inteligentes, aprender a conectar a carteira a uma aplicação descentralizada e entender como funciona cada um dos protocolos que se deseja usar.

5.2.2 Escalabilidade

Escalabilidade refere-se à capacidade de lidar com grandes volumes de transações. As transações em finanças descentralizadas exigem longos períodos de tempo para confirmação e, para a execução em massa ocorrer, as redes blockchains precisam ser capazes de lidar com milhões de usuários e um número elevado de transações por segundo.

Transação por segundo (TPS) refere-se ao número de transações que uma rede pode processar a cada segundo, quanto mais rápida for a rede, menor o seu congestionamento

e, como resultado, uma maior eficiência de pagamento é alcançada, portanto, uma maior chance de adoção.

Figura 12 ilustra o número máximo de transações por segundos que a blockchain do Bitcoin, do Ethereum e do serviço centralizado da Visa conseguem realizar. No geral, a Visa continua a ter uma das velocidades de transações por segundos mais rápidas, porém, a empresa foi fundada em 1958 e teve mais de 60 anos para melhorar e aumentar suas capacidades de rede de pagamento, além de ser centralizada, enquanto que a tecnologia da blockchain ainda está nos estágios iniciais. O Ethereum 2.0 está atualmente em desenvolvimento e promete alcançar até 100 mil transações por segundo.

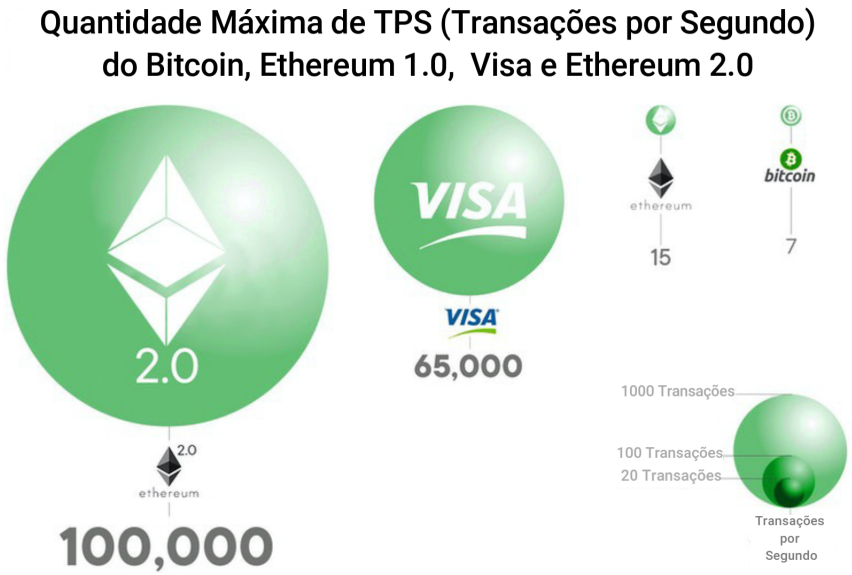

Figura 12: Transações por segundo da blockchain do Bitcoin, do Ethereum e do serviço centralizado da Visa. Adaptada de https://swissborg.com/blog/ethereum-2-0-what-is-it-why-price-booming

5.2.3 Custo de Transação

O custo de transação é outra desvantagem das finanças descentralizadas e, enquanto o problema da escalabilidade não for resolvido de forma eficiente, continuará existindo. Como explicado anteriormente, Ethereum é uma blockchain que processa transações e executa contratos inteligentes. Essas transações são confirmadas por nós, isto é, computadores da rede, que são operados por um grupo de usuários chamados mineradores. Para confirmar as transações e, portanto, apoiar a rede da Ethereum, mineradores têm que gastar muito poder computacional que incorre no aumento da conta de energia. Devido aos gastos com eletricidade, os mineradores não são incentivados a validar transações sem receber uma recompensa financeira, isto é, uma taxa, também chamada de gás, que refere-se ao valor necessário para realizar uma transação no Ethereum com sucesso.

Atualmente, a blockchain da Ethereum pode processar 15 transações por segundo e quanto maior a demanda para usar a rede, maior é a taxa cobrada. Naturalmente, tarefas complexas que demandam mais poder computacional exigem uma quantidade maior de gás para serem executadas, como, por exemplo, a execução de contratos inteligentes, enquanto que tarefas simples exigem menos. Se um usuário quiser concluir uma transação mais rapidamente, ele pode optar por pagar uma quantidade maior de gás, e ao fazer isso, a prioridade da transação é aumentada. Também é possível definir um limite de gás e decidir a quantidade máxima que o usuário está disposto a gastar para uma transação

específica, e se o limite for muito baixo, os mineradores ignorarão as taxas de gás da transação.

As taxas de gás flutuam com a oferta e demanda de poder de processamento. Se o Ethereum enfrentar um aumento na demanda, mas não tiver mineradores suficientes para executar mais transações, ele experimenta um efeito conhecido como congestionamento de rede. Congestionamento de rede torna as taxas de gás mais altas, já que alguns usuários estão dispostos a pagar mais unidades de gás para aumentar suas prioridades nas transações, como resultado, a taxa média de transação aumenta e os usuários devem pagar mais dinheiro do que o normal.

As taxas de gás voltam ao normal apenas quando a demanda cai, pois é improvável que haja um evento em que o número de mineradores aumente repentinamente. Para atender à nova demanda, as taxas podem manter-se com um preço alto por semanas, ou meses, e é comum encontrar o Ethereum com congestionamentos na rede.

A fórmula a seguir mostra como é calculada a taxa de gás e resume o que foi explicado nesta seção.

Taxa Total = Unidades de gás (limite) * (Taxa base + gorjeta) [21]

Onde:

- Unidades de gás (limite) é a quantidade mínima de gás que um usuário está disposto a pagar em uma transação.
- Taxa base é a quantidade mínima de gás necessária para incluir uma transação na blockchain Ethereum. O nível de congestionamento da rede geralmente determina a tarifa básica, e eles são ajustados dinamicamente de acordo com o número de usuários que interagem pela rede.
- Gorjeta são as taxas adicionais que os usuários pagam aos mineradores para priorizar suas transações. Consiste em dar um incentivo para que mineradores confirmem a transação de alguns usuários em detrimento de outras solicitações de outros usuários.

5.2.4 Colaterização

A garantia é algo de valor usado para garantir um empréstimo e consequentemente a liberação de crédito. Por exemplo, em finanças centralizadas é possível hipotecar um imóvel, isto é, colocá-lo como garantia para conseguir um empréstimo com juros baixos e prazos longos. Quase todas as transações de empréstimos em finanças descentralizadas exigem garantias iguais a pelo menos 100% do valor do empréstimo, ou ainda maiores. Esse requisito restringe amplamente quem é elegível para muitos tipos de empréstimos em finanças descentralizadas.

5.2.5 Moeda de Emissão Privada

Ao longo da história, os bancos centrais surgiram como as principais instituições que emitem e sustentam a confiança do dinheiro. Contudo, os investimentos disponíveis em finanças descentralizadas são realizados em moedas estáveis e criptomoedas que não são emitidas pelos bancos centrais, mas por código ou por empresas privadas de tecnologia que podem ter incentivos diferentes na emissão da moeda em comparação com as entidades públicas.

5.3 Oportunidades

Esta seção inclui a terceira parte de uma análise SWOT, chamada de oportunidades. Oportunidade consiste nos fatores favoráveis que podem dar às finanças descentralizadas, uma vantagem competitiva quando comparada às finanças centralizadas.

5.3.1 Inclusão Financeira

Inclusão financeira refere-se aos esforços para tornar os produtos e serviços financeiros acessíveis a todos os indivíduos, independentemente de sua renda ou do seu patrimônio. De acordo com o *Global Findex Database* [22], existem atualmente 1,7 bilhão de pessoas que não têm acesso a serviços financeiros básicos, e cerca de 1 bilhão desses indivíduos excluídos financeiramente não possuem documento de identificação mas possuem dispositivos móveis, e que metade deles possuem acesso à internet.

Para se ter acesso aos serviços financeiros tradicionais, tipicamente é necessário a apresentação de identidade emitida pelo governo, comprovante de residência, não ter dívidas para se ter direito a serviços de crédito, além de outras burocracias que apenas contribuem para exclusão de indivíduos. Por outro lado, ao se transferir as operações financeiras para a blockchain, as pessoas precisarão apenas de um smartphone ou computador e uma conexão estável à Internet para acessar o sistema financeiro global.

Portanto, as finanças descentralizadas (*DeFi*) possuem margem para crescimento e representam um grande passo para a inclusão financeira, especialmente para aqueles que não possuem identificação formal.

5.3.2 Democratização de Serviços Financeiros

Conforme visto no Capítulo 4, as finanças descentralizadas (*DeFi*) fornecem novas formas de investimentos que no mercado tradicional são restritos aos mais ricos, como bancos, corretoras e seguradoras. Além disso, o atual sistema de empréstimos das finanças centralizadas é excludente e evoluiu de tal forma que não consegue atender a um grande segmento da população mundial. Sendo assim, o *DeFi* possui uma vantagem quando comparado ao sistema financeiro tradicional, pois fornece uma gama completa de serviços financeiros que vão desde os serviços mais simples, como novos meios para ganhar juros, fazer empréstimos e realizar transações até relacionamentos contratuais complicados.

5.4 Ameaças

Esta seção inclui a quarta parte de uma análise SWOT, chamada de ameaças. As ameaças estão associadas a diferentes causas externas e, uma ameaça em finanças descentralizadas pode ser vista como uma situação ou barreira que aumenta o risco de o mercado associar *DeFi* como algo inseguro, devido a bugs, golpes e hacks, limitando o sucesso e adoção da tecnologia blockchain.

5.4.1 Regulamentação

Nas finanças descentralizadas, existe a ausência de proteção ao consumidor, então, práticas que são consideradas ilegais no mercado financeiro tradicional poderão ser realizadas sem punição. Desse modo, por exemplo, a manipulação do preço de um ativo, causada por um grupo de investidores com muito capital, é frequente nas finanças descentralizadas, sem condenação dos autores.

Sendo assim, essa ausência de regulamentação nas finanças descentralizadas pode ameaçar a adoção da blockchain pela população e instituições, uma vez que ainda há muitas dúvidas e deliberações acerca do uso dos contratos inteligentes. Portanto, podem haver situações em que um contrato inteligente seja considerado ilegal por um tribunal, de acordo com as leis existentes, como, por exemplo, um contrato inteligente contendo cláusulas abusivas ou regulando transações de bens ilegais.

Ademais, os erros cometidos pelos usuários são irreversíveis nas finanças descentralizadas, visto que as transações na blockchain não podem ser desfeitas. Logo, se um usuário, por exemplo, transferir criptomoedas para o destinatário incorreto, não será possível recuperar o valor já transferido.

Além de ter cuidado no momento de efetuar as transações, o usuário também precisa proteger a sua carteira de criptomoedas, uma vez que a carteira é protegida por uma chave privada, que é um código longo e exclusivo, conhecido apenas pelo proprietário da carteira. Então, se o usuário perder a sua chave privada, perderá, consequentemente, o acesso aos fundos associados a essa chave, pois ela é necessária para visualizar os fundos e para transferir os criptoativos de uma conta para outra. Logo, o usuário deve ter cuidado com a sua chave de acesso, visto que não há como recuperar uma chave privada perdida.

Por outro lado, nas finanças centralizadas, caso o usuário esqueça sua senha de acesso ou realize algum erro na transação, como transferir um valor errado ou enviar fundos para um destinatário incorreto, sempre existirá a possibilidade de recorrer à instituição financeira para recuperar a senha ou desfazer a transação incorreta. Além disso, outro ponto bastante atrativo das finanças centralizadas é o Fundo Garantidor de Crédito (FGC), cuja função é reembolsar certos investimentos da renda fixa, na hipótese de um banco falir. Desse modo, esse reembolso pode ser de até R$ 250.000,00 por CPF/CNPJ em cada conglomerado financeiro, com um limite de R$ 1.000.000,00 renovado a cada quatro anos. Nenhuma proteção semelhante existe nas finanças descentralizadas.

5.4.2 Golpes e Hackers

Crimes em finanças descentralizadas ocorrem principalmente de duas maneiras:

1. Quando hackers se infiltram na plataforma e roubam fundos.

2. Quando desenvolvedores maliciosos criam uma criptomoeda ou um projeto de finanças descentralizadas e atrai investidores para alocar capital no projeto, no qual, em seguida, eles o abandonam e sacam o dinheiro dos investidores.

Diante do exposto, é recomendado que o usuário pesquise acerca da credibilidade do projeto antes de alocar fundos nas finanças descentralizadas, uma vez que qualquer desenvolvedor pode criar plataformas sem a necessidade de uma auditoria ou fiscalização. Logo, essa ausência de supervisão dificulta a adoção das finanças descentralizadas, visto que o usuário comum precisa ter conhecimento técnico para reconhecer se determinado protocolo é fraudulento ou se é passível de ataque de hackers. Apesar dessas fragilidades, é possível que um usuário comum consiga identificar os projetos fraudulentos, uma vez que, na maioria das vezes, esses projetos possuem determinadas características que são fortes indícios de se tratarem de golpes. Então, o usuário deve desconfiar de projetos que surgem do dia para a noite, que tenham desenvolvedores anônimos e que tenham pouca liquidez no ativo. Nesse contexto, alguns dos casos mais famosos de Golpes e hackers são:

1. Mt. Gox foi uma corretora de criptomoedas que sofreu um dos maiores roubos financeiros da história. A corretora afirmou que 750 mil Bitcoins foram roubados dos usuários da empresa, juntamente com 100 mil Bitcoins pessoais da companhia [23]. Isso equivalia a cerca de 473 milhões de dólares na época e o valor pode chegar a quase US$50 bilhões quando ajustado ao preço de 56 mil dólares por Bitcoin no momento de escrita desse documento. Uma investigação realizada pela empresa WizSec, com sede em Tóquio, confirmou que quase todos os Bitcoins haviam sido roubados diretamente da Hot Wallet da empresa [23].

2. Em Outubro de 2021, uma criptomoeda criada por desenvolvedores anônimos inspirada no sucesso da série sul-coreana "round six" foi lançada. Aos detentores da moeda, foi prometido que eles poderiam participar de um jogo online inspirado na série da Netflix que estaria disponível na rede a partir de novembro. Infelizmente, em menos de duas semanas após seu lançamento, os desenvolvedores fugiram com cerca de 3 milhões de dólares, mostrando que o projeto era uma grande farsa. Golpes similares são frequentes no mundo das finanças descentralizadas, como, por exemplo, o caso do projeto "Defi100", no qual os desenvolvedores roubaram 32 milhões de dólares e anunciaram na página web principal do projeto que o mesmo se tratava de um golpe e que os investidores não poderiam fazer nada quanto ao roubo.

Existem outros tipos de golpes praticados que não foram mencionados acima, como sites maliciosos que solicitam de diversas maneiras as chaves privadas de uma carteira, golpistas se passando por pessoas famosas nas redes sociais tentando induzir investidores a depositarem criptomoedas em suas contas para que eles supostamente invistam o dinheiro pelo usuário com a promessa de multiplicação de capital. Alguns golpistas, inclusive, criam sites que são uma cópia exata de alguma aplicação descentralizada específica na qual o usuário deseja investir, porém, eles alteram o contrato inteligente usado no site falso para que, se o usuário interagir com ele, eles possam ter acesso aos fundos da carteira, levando o investidor a perder todo o seu dinheiro. Figura 13 apresenta os números de incidentes nos protocolos *DeFi* envolvendo hackers e os valores roubados em cada ano. Como pode ser observado, o número de casos envolvendo hackers como também a quantia total dos valores roubados só aumentam a cada ano que passa.

Por isso, pelo fato de existir pouca regulamentação no mercado, o usuário deve ficar atento quanto ao que está investindo e com quais contratos inteligentes está interagindo.

5.4.3 Falta de Padrões no Desenvolvimento das Aplicações

Finanças descentralizadas dependem muito da integridade dos contratos inteligentes e do protocolo blockchain subjacente. Qualquer falha no código pode levar a um hack e a perdas financeiras que, muitas vezes, não possuem reparação para os usuários de uma aplicação descentralizada.

É quase impossível codificar sem erros e uma falha de programação pode fazer com que um contrato inteligente deixe de funcionar conforme desejado, potencializando vulnerabilidades que costumam ser exploradas por invasores que buscam drenar os fundos do contrato inteligente.

Para minimizar esse problema, procedimentos padronizados de desenvolvimento em contratos inteligentes devem ser criados, visto que as ferramentas de desenvolvimento ainda estão em um estágio inicial e os padrões para desenvolver aplicativos baseados em blockchain ainda não foram definidos.

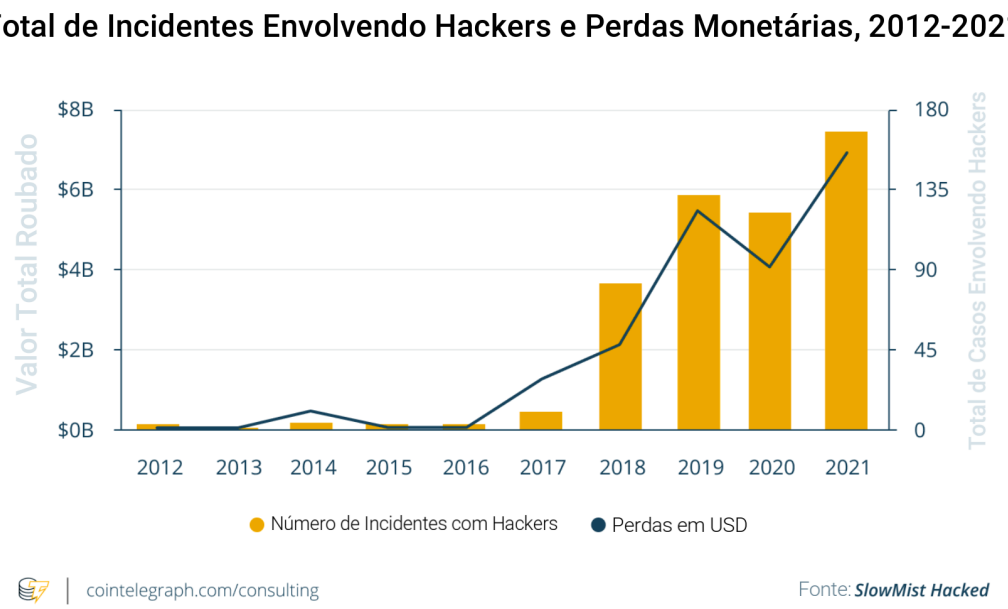

Figura 13: Número total de incidentes com hackers em DeFi e perdas monetárias, 2012-2021. Adaptada de https://cointelegraph.com/news/cointelegraph-consulting-recounting-2021-s-biggest-defi-hacking-incidents

A criação de uma padronização, incluindo auditorias, verificação formal e serviços de seguro podem proporcionar o desenvolvimento de softwares menos suscetíveis a ataques, o que melhora a segurança e aceitação do usuário. Na Figura 14, é possível observar que praticamente 80% dos protocolos de finanças descentralizadas que foram vítimas de hackers, erros e ataques em 2021 não passaram por qualquer tipo de auditoria, se mostrando uma medida importante para melhorar os protocolos de segurança do setor.

5.5 Considerações Finais

Nesta seção, as finanças descentralizadas foram analisadas através de uma análise SWOT que está resumida na figura 15.

Conforme a análise apresenta, os pontos fortes e oportunidades das finanças descentralizadas superam suas fraquezas e ameaças. Dessa forma, fica claro que as finanças descentralizadas oferecem potencial disruptivo e uma proposta de valor muito atraente, pela qual visa melhorar significativamente os serviços financeiros tradicionais, mediante a inclusão financeira e democratização dos serviços financeiros, fornecendo eficiência transacional, serviços automatizados e produtos de investimentos com rendimentos mais atrativos.

Contudo, para que a adoção em massa das finanças descentralizadas possam ocorrer, é preciso superar alguns obstáculos, como, por exemplo, os aspectos de segurança relacionados a contratos inteligentes e a usabilidade da maioria dos aplicativos DeFi que atualmente dificultam a adoção e o crescimento mais amplo dos usuários. Finalmente, considerações regulatórias que estão surgindo ao longo do desenvolvimento das finanças descentralizadas não podem ser desconsideradas pelos desenvolvedores, visto que as aplicações desentralizadas podem ter suas operações interrompidas em um determinado país caso o serviço não siga as leis vigentes da região na qual opere.

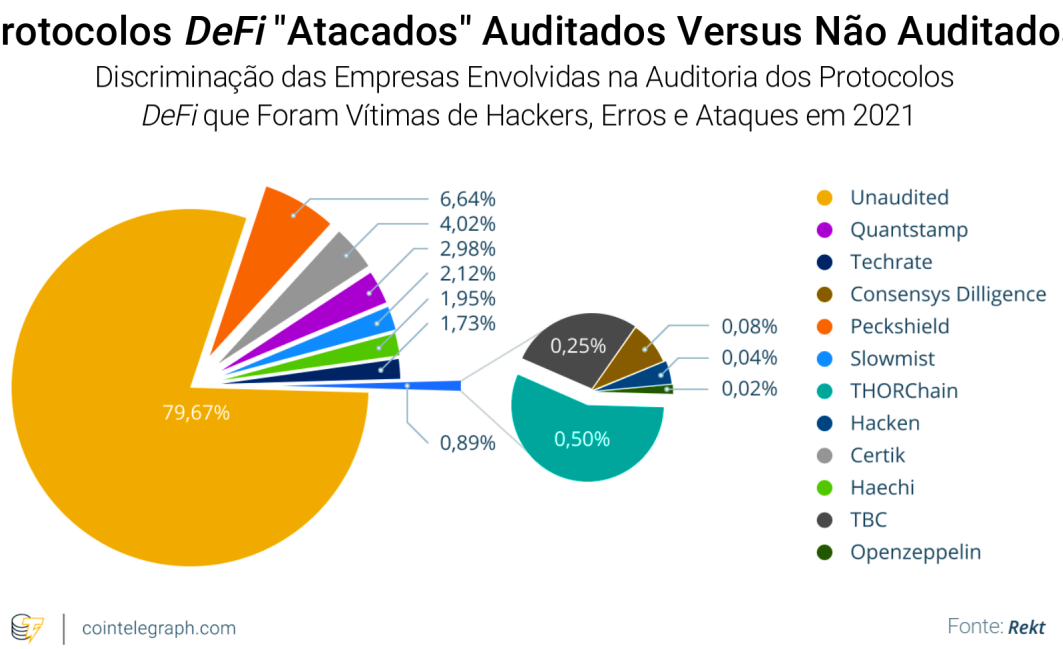

Figura 14: Detalhamento das empresas envolvidas em auditorias dos protocolos DeFi que foram vítimas de hackers, erros e ataques em 2021. Adaptada de https://cointelegraph.com/news/cointelegraph-consulting-recounting-2021-s-biggest-defi-hacking-incidents

Figura 15: Análise SWOT de Serviços Financeiros Descentralizados

6 Conclusão

Este capítulo resume as conclusões gerais do estudo realizado. Na Seção 5.1, as principais contribuições são apresentadas. Por fim, na Seção 5.2, os possíveis trabalhos futuros são listados.

6.1 Principais Contribuições

O presente trabalho de graduação fornece ao leitor um levantamento bibliográfico sobre os conceitos e serviços existentes, que são ofertados nas finanças descentralizadas. Além disso, foram destacadas as diferenças entre o sistema financeiro tradicional centralizado e as finanças descentralizadas. Tabela 2 resume as principais divergências entre as finanças centralizadas e as finanças descentralizadas com base no estudo realizado ao longo desse documento.

Destacados na cor verde estão os pontos nos quais as finanças descentralizadas se sobressaem perante às finanças centralizadas. Por conseguinte, destacados em azul estão os pontos nas quais as finanças centralizadas se sobressaem perante às finanças descentralizadas, contudo, de acordo com a Tabela 3, é possível notar que os pontos desfavoráveis ao DeFi em comparação às finanças centralizadas estão relacionados à baixa educação dos usuários sobre os sistemas descentralizados, aos problemas na escalabilidade e segurança, e às poucas regulamentações criadas, que, ao longo do tempo, esses pontos desfavoráveis podem ser contornados com o amadurecimento dos serviços financeiros descentralizados. Já destacados na cor vermelha estão os pontos nos quais, de acordo com o estudo realizado, não existem soluções que possam favorecer as finanças descentralizadas em relação às finanças centralizadas.

Diante do exposto, dos vinte pontos levantados, dez favorecem as finanças descentralizadas e dez favorecem as finanças centralizadas. Contudo, oito dos dez pontos que favorecem as finanças centralizadas podem, futuramente, se tornarem vantagens das finanças descentralizadas perante às finanças centralizadas, se os problemas destacados na Tabela 3 forem solucionados.

Por fim, o resultado da pesquisa realizada sugere que os serviços ofertados nas finanças descentralizadas proporcionam reais benefícios, quando comparados com os serviços ofertados nas finanças centralizadas, podendo ser uma ferramenta útil na luta contra os desafios socioeconômicos atuais, fomentando a inclusão de grupos desfavorecidos. No entanto, para desenvolver todo o seu potencial disruptivo, sérias ineficiências devem ser sanadas, como o seu uso intenso de energia e problemas com escalabilidade. Além disso, existem os desafios regulatórios e problemas com vulnerabilidade que precisam ser superados para romper as barreiras culturais à entrada nesse ecossistema.

Sendo assim, essa pesquisa apoia o argumento de que os serviços ofertados nas finanças descentralizadas serão amplamente utilizados em novos sistemas financeiros. No entanto, é provável que esses sistemas sejam, significativamente, mais avançados do que os existentes e sejam fortemente controlados por órgãos reguladores.

	Finanças Centralizadas	Finanças Descentralizadas
Existência de intermediários	Existe a presença dos intermediários	Ausência dos intermediários
Custódia dos ativos	Detido por um prestador de serviços regulamentado em nome dos proprietários dos ativos. Potencialmente problemático em colapso político e/ou social.	Mantido diretamente pelos usuários em carteiras de criptomoedas, sem a necessidade de custódia ou por meio de depósito baseado em contrato inteligente. Usuários possuem total controle dos seus ativos.
Como participar	Necessita de identificação e, na maioria dos casos, de comprovante de residência, o que gera menos inclusão financeira, principalmente em países pouco desenvolvidos com baixos índices de identificação formal, como é o caso do país El Salvador, onde 70% da população não possui conta bancária devido à falta de identificação formal da população [24].	Necessita apenas de uma carteira de criptomoedas e um dispositivo eletrônico, como um celular ou um computador com acesso à Internet.
Resistência à Censura	Passível de censura	Livre de censura
Automação dos processos	Menor automação	Maior automação dos processos, por causa dos contratos inteligentes.
Execução das transações	Os intermediários normalmente processam transações entre as partes.	Por meio de contratos inteligentes, operando nos ativos do usuário.
Restrição nos investimentos	Serviços limitados de acordo com a renda, com o patrimônio e com a identificação do usuário. Além disso, certos investimentos estão apenas disponíveis para as grandes instituições, como bancos, corretoras ou seguradoras.	Todos os investimentos ficam disponíveis aos usuários. Empréstimos, seguros, staking e mineração de liquidez são alguns dos produtos financeiros ofertados em finanças descentralizadas com custos reduzidos.
Horário de funcionamento	Apenas em horário comercial	24 horas por dia
Auditabilidade	Auditorias de terceiros contratadas em código proprietário e em código aberto verificado publicamente.	O código-fonte aberto e o livro-razão público permitem que os auditores verifiquem protocolos e atividades.
Transparência	Menor transparência, visto que as instituições financeiras não disponibilizam seu histórico de transações aos seus usuários.	Mais transparência, uma vez que todas as transações, dados e códigos da blockchain estão disponíveis publicamente.
Facilidade no uso	Mais intuitivo, fácil de usar.	Menos intuitivo, difícil de usar. É necessário o conhecimento técnico para saber como instalar uma carteira de criptomoedas, como habilitá-la para interagir com contratos inteligentes e como conectá-la com as aplicações descentralizadas. Necessita o desenvolvimento e aperfeiçoamento das interfaces gráficas e front-end.
Liquidez	Maior liquidez	Menor liquidez (em ambientes 100% descentralizados)
Taxas	Altas taxas devido ao custo dos intermediários.	Altas taxas devido aos problemas ligados à escalabilidade.
Compensação e Liquidação	Processada por prestadores de serviços, normalmente após um período de tempo. Exemplo: Cartões de créditos. Transações internacionais podem demorar longos períodos para serem finalizadas.	A gravação de transações na blockchain conclui o processo de liquidação. Transações instantâneas para qualquer lugar do mundo, caso o problema de escalabilidade seja resolvido.
Emissão da moeda (unidade de troca)	Normalmente, a moeda é fiduciária, ou seja, emitida por governos.	Ativos digitais ou moedas estáveis emitidos por empresas privadas.
Segurança	Vulnerável a hacks e violações de dados.	Vulnerável a hacks e a outros riscos (contratos inteligentes, aplicações descentralizadas...). Os danos causados tendem a diminuir com a maturação nos padrões de desenvolvimento das finanças descentralizadas e com o avanço no desenvolvimento de seguros descentralizados. Além disso, o fato das finanças descentralizadas serem de código aberto, facilita para que as vulnerabilidades sejam tratadas rapidamente. Inclusive, as plataformas descentralizadas oferecem recompensas aos hackers que reportam problemas de segurança, esses são popularmente conhecidos como "white hat hackers". Educação por parte dos usuários também precisa ser realizada para evitar cair em golpes, como os citados na análise SWOT.
Regulamentação	Ambiente altamente regulado.	Ambiente pouco regulado, o que facilita a manipulação do mercado e aumenta as questões regulatórias a respeito da legalidade das cláusulas dos contratos inteligentes.
Proteção ao investidor	Alta proteção ao consumidor, como fiscalização pelos órgãos competentes, a existência do FGC em alguns investimentos de renda fixa e punições aos autores que pratiquem manipulação no mercado.	Não existe proteção ao consumidor, os usuários assumem todos os riscos. Contudo, seguros descentralizados oferecem alguma proteção contra perdas.
Exigências de Garantias nos empréstimos	Sujeito a análise de crédito, sendo possível o empréstimo sem o envolvimento de garantias. Existe a possibilidade do empréstimo com garantia.	Empréstimos sobre-colateralizados* devido à volatilidade dos ativos digitais e à ausência de pontuação de crédito. *garantia maior do que o valor em crédito que se deseja adquirir
Erro causado pelo usuário	Pode-se recorrer ao custodiante sempre que necessário	Não tem a quem recorrer após uma transação concluída.

Tabela 2: Divergências entre as finanças centralizadas e as finanças descentralizadas

	Finanças Centralizadas	Finanças Descentralizadas
Facilidade no uso	Mais intuitivo, fácil de usar.	Menos intuitivo, difícil de usar. É necessário o conhecimento técnico para saber como instalar uma carteira de criptomoedas, como habilitá-la para interagir com contratos inteligentes e como conectá-la com as aplicações descentralizadas. Necessita o desenvolvimento e aperfeiçoamento das interfaces gráficas e front-end.
Liquidez	Maior liquidez	Menor liquidez (em ambientes 100% descentralizados)
Taxas	Altas taxas devido ao custo dos intermediários.	Altas taxas devido aos problemas ligados à escalabilidade.
Compensação e Liquidação	Processada por prestadores de serviços, normalmente após um período de tempo. Exemplo: Cartões de créditos. Transações internacionais podem demorar longos períodos para serem finalizadas.	A gravação de transações na blockchain conclui o processo de liquidação. Transações instantâneas para qualquer lugar do mundo, caso o problema de escalabilidade seja resolvido.
Emissão da moeda (unidade de troca)	Normalmente, a moeda é fiduciária, ou seja, emitida por governos.	Ativos digitais ou moedas estáveis emitidos por empresas privadas.
Segurança	Vulnerável a hacks e violações de dados.	Vulnerável a hacks e a outros riscos (contratos inteligentes, aplicações descentralizadas...). Os danos causados tendem a diminuir com a maturação nos padrões de desenvolvimento das finanças descentralizadas e com o avanço no desenvolvimento de seguros descentralizados. Além disso, o fato das finanças descentralizadas serem de código aberto, facilita para que as vulnerabilidades sejam tratadas rapidamente. Inclusive, as plataformas descentralizadas oferecem recompensas aos hackers que reportam problemas de segurança, esses são popularmente conhecidos como "white hat hackers". Educação por parte dos usuários também precisa ser realizada para evitar cair em golpes, como os citados na análise SWOT.
Regulamentação	Ambiente altamente regulado.	Ambiente pouco regulado, o que facilita a manipulação do mercado e aumenta as questões regulatórias a respeito da legalidade das cláusulas dos contratos inteligentes.
Proteção ao investidor	Alta proteção ao consumidor, como fiscalização pelos órgãos competentes, a existência do FGC em alguns investimentos de renda fixa e punições aos autores que pratiquem manipulação no mercado.	Não existe proteção ao consumidor, os usuários assumem todos os riscos. Contudo, seguros descentralizados oferecem alguma proteção contra perdas.

Tabela 3: Motivos que fazem as finanças centralizadas se sobressariem perante às finanças descentralizadas

6.2 Trabalhos Futuros

O presente trabalho visou responder se os serviços ofertados nas finanças descentralizadas proporcionam reais benefícios ou apenas as mesmas vantagens dos serviços ofertados nas finanças centralizadas. A esse respeito, mais pesquisas devem ser dedicadas para entender se os custos de uma possível descentralização das finanças centralizadas conduz a economias substanciais e a eficiências transacionais que justifiquem a mudança. Ademais, estudos devem ser realizados para determinar os efeitos econômicos em caso de adoção em massa do uso das finanças descentralizadas no desempenho das moedas fiduciárias, visto que, na maioria dos serviços, usam-se criptomoedas ou moedas estáveis lastreadas em dólar. Uma atenção especial deve ser dada à economia e à inclusão financeira dos países e cidades que adotam criptomoedas como moeda de curso legal, como é o caso dos países El Salvador e República Centro-Africana, que adotaram o bitcoin como moeda de curso legal, ou da cidade Lugano que, além de adotar o bitcoin como moeda de curso legal, adotou o "Tether", uma moeda estável lastreada em dólar.

Outro importante trabalho a ser feito são as pesquisas voltadas para a detecção precoce de possíveis ataques aos contratos inteligentes, com o intuito de contribuir para um aumento na confiança dos serviços ofertados nas finanças descentralizadas.

Por fim, conforme citado na seção anterior, estudos sobre questões regulatórias devem ser explorados, visando enquadrar os serviços das finanças descentralizadas dentro da lei de cada país, impulsionando a sua adoção por parte de grandes instituições, como, por exemplo, indústrias, empresas e bancos.

Referências

[1] NAKAMOTO, Satoshi. Bitcoin: A Peer-to-Peer Electronic Cash System. **Bitcoin**. Disponível em: https://bitcoin.org. Acesso em: 21 set. 2021.

[2] PAKENAITE, Simona; TAUJANSKAITE, Kamile. Investigation of the Blockchain's Influence on Traditional Banking: Challenges and Opportunities. **European Scientific Journal**, Lithuania, vol. 15, n. 10, p. 1 - 15, 2019. Acesso em: 22 set. 2021

[3] CHOI, Sujin; KO, Deokyoon; PARK, Sooyong; SMOLANDER, Kari; YLI-HUUMO, Jesse. Where Is Current Research on Blockchain Technology?—A Systematic Review. **Plos One**, Seul, 3 out. 2016. Disponível em: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0163477. Acesso em: 15 out. 2021.

[4] DAVIS, Joshuai. Peer to peer insurance on an Ethereum Blockchain: General consideration of the Fundamentals of Peer to Peer Insurance. **The Blockchain**. Disponível em: https://www.the-blockchain.com/docs/Peer%20to%20peer%20insurance%20on%20Blockchain.pdf . Acesso em: 04 out. 2021.

[5] VON HALLER, Martin. Blockchain 2.0, smart contracts and challenges. **Bird Bird**. Disponível em: https://www.twobirds.com/-/media/pdfs/in-focus/fintech/blockchain2_0_martinvonhallergroenbaek_08_06_16.pdf . Acesso em: 30 out. 2021.

[6] SCHAR, Fabian. Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets. **Economic Reasearch Federal Reserve Bank of St. Louis**, St. Louis, 05 fev., 2021. Disponível em: https://research.stlouisfed.org/publications/review/2021/02/05/decentralized-finance-on-blockchain-and-smart-contract-based-financial-markets . Acesso em: 09 nov 2021.

[7] CARDOSO, Bruno. Contratos inteligentes: descubra o que são e como funcionam. **Revista Jus Navigandi, ISSN 1518-4862**, Teresina, ano 23, n. 5479, 2 jul. 2018. Disponível em: https://jus.com.br/artigos/65596. Acesso em: 13 nov. 2021.

[8] BUTERIN, Vitalik. A Next Generation Smart Contract Decentralized Application Platform. **Ethereum White Paper**. Disponível em: https://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf . Acesso em: 13 nov. 2021.

[9] COIN MARKET CAP. **Gráficos Globais de Criptomoedas: Capitalização de Mercado Total de Criptomoedas.** Disponível em: https://coinmarketcap.com/pt-br/charts/ . Acesso em: 13 nov. 2021.

[10] BERENTSEN, Aleksander; SCHAR, Fabian. A Short Introduction to the World of Cryptocurrencies. **Federal Reserve Bank of St. Louis Review**, St. Louis, p. 1- 16, 2018. Disponível em: https://files.stlouisfed.org/files/htdocs/publications/review/2018/01/10/a-short-introduction-to-the-world-of-cryptocurrencies.pdf . Acesso em: 14 nov. 2021.

[11] LEONHARD, Robert. Decentralized Finance on the Ethereum Blockchain. **SSRN.** Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3359732 . Acesso em: 14 nov. 2021.

[12] SCHA, Fabian. Stablecoins: The quest for a low- volatility cryptocurrency. **The Economics of Fintech and Digital Currencies**. Disponível em: https://www.researchgate.net/pu_volatility_cryptocurrency . Acesso em: 14 nov. 2021.

[13] ZHENG, Zibin. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. **IEEE 6th International Congress on Big Data**, China, p. 557 - 564, 2017. Disponível em: https://www.henrylab.net/wp-content/uploads/2017/10/blockchain-conference-2017.pdf . Acesso em: 14 nov. 2021.

[14] QIJUN, Chen; A Review on Consensus Algorithm of Blockchain. **IEEE 6th**

International Congress on Big Data, Beijing, p. 2567 - 2572. Disponível em: https://blockhack.osive.com/_downloads/33a65d87de38eaf5b8d817681a3e4674/7.pdf . Acesso em: 24 nov. 2021.

[15] THE BLOCK. **Defi Exchange**. Disponível em: https://www.theblockcrypto.com/data/decentralized-finance/dex-non-custodial/uniswap-vs-coinbase-and . Acesso em: 25 nov. 2021.

[16] SANTORO, Joey. DeFi and the Future of Finance. **SSRN**. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3711777 . Acesso em: 02 dez. 2021.

[17] ETHEREUM ORG. **The Beacon Chain**. Disponível em: https://ethereum.org/en/upgrades/beacon-chain/ . Acesso em: 03 dez. 2021.

[18] ETHEREUM ORG. **How large are the rewards/penalties?.** Disponível em: https://launchpad.ethereum.org/en/faq

[19] BEACONCHAIN. **Validators Overview**. Disponível em: https://beaconcha.in/validators#pending . Acesso em: 26 jan. 2022

[20] BLOCKCHAIN EXPLORER. **Ethereum Explorer.** Disponível em: https://www.blockchain.com/pt/explorer . Acesso em: 02 fev. 2022

[21] ETHEREUM ORG. **Gas and fees**. Disponível em: https://ethereum.org/en/developers/docs/gas/ . Acesso em: 06 fev. 2022

[22] THE WORLD BANK. **The global findex database.** Disponível em: https://globalfindex.worldbank.org/ . Acesso em: 12 fev. 2022

[23] WIKIPEDIA. **Corretora Mt. Gox.** Disponível em: https://en.wikipedia.org/wiki/Mt._Gox . Acesso em: 16 fev. 2022

[24] THE WORLD BANK. **Porcentagem de bancarizados em El Salvador.** Disponível em: https://data.worldbank.org/indicator/FX.OWN.TOTL.ZS?locations=SV . Acesso em: 22 fev. 2022.