FACULDADE DE TECNOLOGIA DE TAUBATÉ

GABRIEL MENDES FIGUEIRA

# *Finanças Descentralizadas (DeFi) em Blockchain de segunda geração: Um estudo de caso sobre Corretoras Descentralizadas (DEXs) na rede Ethereum*

TAUBATÉ

2022

**FACULDADE DE TECNOLOGIA DE TAUBATÉ**

**GABRIEL FIGUEIRA**

# *Finanças Descentralizadas (DeFi) em Blockchain de segunda geração: Um estudo de caso sobre Corretoras Descentralizadas (DEXs) na rede Ethereum*

Trabalho de Graduação apresentado à Coordenação do Curso Superior de Tecnologia em Análise e Desenvolvimento de Sistemas do Centro Estadual de Educação Tecnológica Paula Souza para a obtenção do diploma de Tecnólogo em Análise e Desenvolvimento de Sistemas.

**Orientadora: Profa. Phd. Divani Carvalho Barbosa**

**Coorientador: Prof. Ms. Luiz Eduardo Souza Evangelista**

**TAUBATÉ**

**2022**

**GABRIEL MENDES FIGUEIRA**

# *Finanças Descentralizadas (DeFi) em Blockchain de segunda geração: Um estudo de caso sobre Corretoras Descentralizadas (DEXs) na rede Ethereum*

Trabalho de Graduação apresentado à Faculdade de Tecnologia de Taubaté, como parte das exigências para a obtenção do diploma de Tecnólogo em Análise e Desenvolvimento de Sistemas.

**Orientadora: Profa. Phd. Divani Carvalho Barbosa**

**Coorientador: Prof. Ms. Luiz Eduardo Souza Evangelista**

Taubaté, _____ de _____ de 2022.

**BANCA EXAMINADORA**

_____

Prof. Titulação e Nome

Instituição

_____

Prof. Titulação e Nome

Instituição

_____

Prof. Titulação e Nome

Instituição

Dedico este trabalho aos “doidões da internet”, que há mais de 14 anos sonham, planejam, executam e compartilham um mundo mais descentralizado, e às futuras gerações, que terão o discernimento e paciência para dedicar seu tempo aos estudos.

# AGRADECIMENTOS

A todes que, direta ou indiretamente, contribuíram para a realização deste trabalho.
Aos meus pais Solonardo e Sneide, pela vida e ensinamentos. Ao meu irmãozinho, Guinnes, pela amizade. À minha bela esposa, Doniluin, pela bacanice, paciência e apoio antes, durante e depois da realização deste estudo. Ao Berino, pelo suporte emocional.
Aos professores, todos, pela inestimável força de seguir educando.
Aos colegas de classe, Álvaro, Maria, Renato e Laura com quem tive a felicidade de conviver do início ao fim da faculdade.
Aos criadores de conteúdo cripto em língua portuguesa no youtube e à comunidade Mercurius Crypto pela dedicação em compartilhar conhecimento.
Ao desconhecido, que é instigado a ser descoberto.

“Chanceler à beira do segundo resgate aos bancos.”

(S. Nakamoto)

# RESUMO

Criptoativos como o Bitcoin vem sendo cada vez mais utilizados e apreciados graças aos avanços tecnológicos das primeiras décadas do século XXI e às limitações do sistema financeiro tradicional. Com a tecnologia blockchain e o desenvolvimento de aplicações descentralizadas *(Dapps)*, novas formas de investimento surgem, eliminando intermediários como bancos centrais e instituições financeiras, e abrindo as portas para uma nova maneira de intercambiar dinheiro. O presente estudo tem como objetivo apresentar o contexto de Corretoras Descentralizadas (DEX) na rede de blockchain da Ethereum, inseridas no conceito de Finanças Descentralizadas (DeFi). Tem como metodologia a pesquisa bibliográfica, fundamentada em conteúdo disponível na web como livros, artigos, vídeos, blogs, investigações e notícias, além de realizar uma pesquisa quantitativa com usuários brasileiros. Por fim, conclui-se apresentando o cenário desta inovação tecnológica, seus riscos e oportunidades, além dos seus desafios para as próximas décadas.



**Palavras-Chave**: Blockchain. Ethereum. Criptoativos. Finanças Descentralizadas (DeFi). Corretoras Descentralizadas (DEXs).

# ABSTRACT

Cryptoassets like Bitcoin are being increasingly used and valued thanks to connectivity technologies and trust between peers. With blockchain protocols, new forms of investment emerge, eliminating intermediaries such as banks and brokers, and opening the door to a revolution in the financial sector. This study aims to analyze the main Decentralized Exchanges (DEX) of the Ethereum blockchain, inserted in the Decentralized Finance (DeFi) scenario. Its methodology is the analysis of content available on the web such as books, articles, videos, websites, investigations and news, in addition to conducting quantitative research with Brazilian users. Finally, it concludes by presenting the scenario of this market, its risks and opportunities, in addition to its challenges for the coming decades.



**Keywords**: Blockchain. Ethereum. Cryptoassets. Decentralized finance (DeFi). Decentralized exchange (DEX).

# LISTA DE FIGURAS

# LISTA DE TABELAS

# LISTA DE ABREVIATURAS E SIGLAS

| | |
|---|---|
| **BTC** | Bitcoin |
| **CBDC** | Central Bank Digital Currency |
| **CEFI** | Centralized Finance |
| **DAO** | Decentralized Autonomous Organization |
| **DAPPS** | Decentralized Apps |
| **DEFI** | Decentralized Finance |
| **DEX** | Decentralized Exchange |
| **DLT** | Distributed Ledger |
| **ETH** | Ethereum |
| **KYC** | Know-your-customer |
| **LPS** | Liquidity Provider |
| **P2P** | Peer-to-Peer |
| **TRADFI** | Traditional Finance |

**SUMÁRIO**

## INTRODUÇÃO

A tecnologia de blockchain transcendeu as fronteiras acadêmicas pela primeira vez durante a crise econômica de 2007-2008 com a criação do bitcoin, o primeiro ativo financeiro criptografado e descentralizado do mundo. Em oposição às moedas fiduciárias como o dólar e o real, inflacionárias e emitidas por bancos centrais, o advento tecnológico das criptomoedas permitiu a criação de representações digitais de valor de modo deflacionário, na qual pessoas de todo o globo pudessem trocar sua moeda fiduciária em corretoras de criptomoedas, e guardar esse patrimônio de maneira digital, segura e de forma não custodiante em redes distribuídas, de maneira mais soberana a estados e bancos centrais. Em 2014, uma segunda geração de blockchains foi criada, denominada Ethereum. Esta plataforma permitiu a execução de contratos inteligentes (*smart contracts*), que são protocolos de computador imutáveis e autoexecutáveis, e a execução de aplicativos descentralizados (*DApps*).

Os aplicativos descentralizados da blockchain da Ethereum são de código aberto (*open-source)*, e têm seu código de back-end em uma rede ponto-a-ponto (*peer-to-peer* ou *p2p*) descentralizada, sem a necessidade de execução em servidores centralizados. Com essa tecnologia, surgiu uma forma experimental de financiamento que não depende de intermediários financeiros centrais como corretoras tradicionais, bolsas ou bancos, denominada Finanças Descentralizadas (DeFi). As aplicações DeFi na blockchain da Ethereum permitem que as pessoas emprestem ou tomem emprestado fundos de terceiros (*lending*), especulem sobre os movimentos de preços de ativos usando derivativos, comprem seguros descentralizados contra riscos, ganhem juros em uma conta tipo poupança (*pool*) e negociem criptomoedas em corretoras descentralizadas (DEXs).

Corretoras descentralizadas da rede Ethereum permitem que transações de criptomoedas sejam realizadas de pessoa para pessoa sem a necessidade de um intermediário que supervisione a segurança e a transferência dos ativos, sendo realizado pelos algoritmos dos contratos inteligentes da blockchain, e são auditáveis publicamente por qualquer pessoa. Como os usuários não precisam renunciar à custódia de seus ativos para realizar as operações nas corretoras, tampouco é possível que os fundos sejam confiscado. Além disso, as DEXs garantem maior privacidade pois são mais anônimas do que as corretoras tradicionais que

implementam os requisitos de *know your customer* (KYC), como a solicitação de documentos de identificação, por exemplo.

Os conceitos derivados da tecnologia blockchain podem ser considerados relativamente novos e de complexo entendimento para a maioria das pessoas, incluindo os profissionais de tecnologia da informação como desenvolvedores de software. Portanto, o escopo do presente estudo se delimita a apresentar as funcionalidades e a conceitualização das Corretoras Descentralizadas apenas da rede blockchain da Ethereum, inseridas no contexto das Finanças Descentralizadas. Como funciona essa tecnologia? Quais são as características principais dessa blockchain? Quais são os riscos inerentes à utilização de Corretoras Descentralizadas? Por que cresce tanto a adesão por esse tipo de tecnologia? Quais as perspectivas de futuro dessa tecnologia? O desconhecimento sobre essa tecnologia pode ser considerado como um problema a ser resolvido, democratizando assim o acesso a este novo saber.

As tecnologias de modo geral, incluindo a própria tecnologia da informação com o surgimento de computadores pessoais, sofreram muita resistência por parte da sociedade até serem aceitas e fazerem parte do cotidiano das pessoas. Por se tratar de uma inovação disruptiva, que provoca uma ruptura com os padrões e modelos já estabelecidos pela sociedade, é de se esperar que haja receio por parte da população frente às mudanças propostas pela adoção de tecnologias como a blockchain. Toda mudança gera resistência, ainda mais quando se fala de dinheiro. É comum que haja estranhamento de diversas parcelas da sociedade, principalmente às mais privilegiadas, quanto à alteração de um sistema financeiro global centralizado que existe há séculos, para um sistema descentralizado e autogerido pelos algoritmos presentes em contratos inteligentes.  A ausência de uma autoridade centralizadora que garanta confiança no sistema, assim como a ausência de um metal precioso como o ouro que lastreie o valor de uma moeda, geram medo por serem desconhecidos, e pode parecer uma utopia do universo *geek*. Tal resistência pode ser comparada, em diferente grau, com a revolução que os dispositivos móveis conectados à internet geraram na virada do século passado, transformando por completo modelos de negócios e o comportamento humano.

O presente estudo tem como objetivo geral apresentar o conceito de Corretora Descentralizada (DEX) da rede de blockchain da Ethereum, inserida no contexto das Finanças Descentralizadas (DeFi) e dos Aplicativos Descentralizados (DApps). Para o atingimento de tal propósito, este trabalho acadêmico tem como objetivos

específicos contextualizar o funcionamento da blockchain da Ethereum, apresentar casos de uso, oportunidade e riscos de aplicativos de DeFi, e, por fim, apresentar um exemplo de DEX. Por outro lado, o estudo não pretende contemplar todas as problemáticas do mundo da blockchain e dos demais temas propostos, tão pouco busca incentivar a alocação de recursos em plataformas de finanças descentralizadas, não servindo de nenhuma maneira como uma indicação de investimento.

Por se tratar de uma tecnologia nova, disruptiva, distribuída e descentralizada, com real potencial de gerar mudanças peremptórias na sociedade e nos alicerces de instituições financeiras tradicionais, bancos centrais e do setor financeiro como um todo, o presente estudo se mostra pertinente do ponto de vista social, econômico e tecnológico. Para que se possa acompanhar a evolução histórica de tal movimento, é fundamental que haja a documentação do processo de descentralização financeira iniciado na década de 10 do século XXI. Ademais, a ausência de uma regulamentação destas práticas, e o pouco conteúdo acadêmico em língua portuguesa, são fatores que justificam a relevância do presente estudo, apoiando assim futuras tomadas de decisão de órgãos públicos, privados e de organizações autônomas descentralizadas (DAO), além de apresentar às futuras gerações um recorte histórico desse movimento.

A metodologia empregada para o atingimento dos objetivos propostos foi a pesquisa bibliográfica, fundamentada em conteúdo disponível na internet como livros, artigos, vídeos, blogs, investigações e notícias, além de realizar uma pesquisa quantitativa sobre o tema com estudantes da Faculdade de Tecnologia do Estado de São Paulo em Taubaté (Fatec Taubaté).

O primeiro capítulo do estudo se dedica a apresentar o conceito de blockchain, seu surgimento, funcionalidades primárias e principais características. Em seguida é apresentado o conceito de Ethereum, sua tecnologia, aplicações, atributos e linguagem de programação. No terceiro capítulo, os conceitos de Aplicativos, Finanças e Corretoras Descentralizadas são abordados juntamente com exemplos reais na rede Ethereum. Logo após, no quarto capítulo, são apresentados os resultados da pesquisa com estudantes da Fatec Taubaté. Por fim, no quinto e último capítulo, são apresentadas as conclusões do estudo e sugestões para futuras investigações.

# 1. BLOCKCHAIN

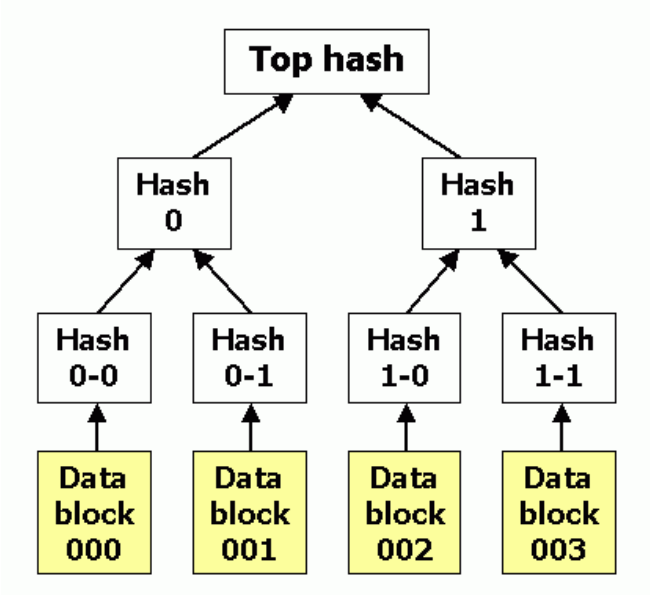
A blockchain, ou cadeia de blocos, é um tipo de banco de dados distribuído e descentralizado, onde cada participante da rede detém uma réplica de todos os dados e todas as atualizações são executadas em conjunto e em consenso. A Blockchain é uma lista crescente de registros, chamados blocos, que são vinculados através da criptografia (NARAYANAN *et al*., 2016). Cada bloco contém um indicador, *hash* criptográfico, do bloco anterior, ou seja, contém geralmente uma marcação de data e horário, dados de transação e outras informações que confirmam sua validade. Através do registro distribuído, essa tecnologia visa a descentralização como forma de segurança (SCHUEFFEL *et al*., 2019). Assim, é resistente às modificações de seus dados pois, uma vez registrados, os dados em um bloco não podem ser alterados sem alteração de todos os blocos subsequentes. Esta tecnologia é normalmente gerenciada por uma rede *peer-to-peer*, aderindo coletivamente a um protocolo para comunicação entre *nodes* (nós) e validação de novos blocos. Podemos definir o blockchain como um livro razão aberto e distribuído que pode registrar transações entre duas partes de forma eficiente, verificável e permanente (IANSITI, LAKHANI, 2017). O blockchain é considerado um tipo de ferrovia de pagamento (LUNN, 2018).

> [...] Um blockchain é um livro-razão digital descentralizado, distribuído e, muitas vezes, público, que consiste em registros chamados de blocos, usados para registrar transações em muitos computadores, de forma que nenhum bloco envolvido possa ser alterado retroativamente, sem a alteração de todos os blocos subsequentes. (ARMSTRONG, 2016)

O criptógrafo David Chaum propôs pela primeira vez um sistema do tipo blockchain em sua dissertação "*Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups",* publicado em 1982 (SHERMAN *et al*., 2019). Em 1991 Stuart Haber e W Scott Stornetta desenvolveram trabalhos adicionais sobre o tema. Eles queriam implementar um sistema em que as marcações de data e hora de documentos não pudessem ser alteradas. Em 1992, os estudiosos em companhia de Dave Bayer incorporaram árvores Merkle, ou árvores de dispersão, ao projeto, o

que melhorou sua eficiência ao permitir que vários documentos fossem coletados em um único bloco. Tais árvores são um tipo de estrutura de dados que contém uma árvore de informações resumidas sobre um pedaço maior de dados usado para verificar seu conteúdo, conforme imagem a seguir.

**Figura 1** - Árvores de Merkle.




Fonte: Wikipédia - Árvores de Merkle. Acessado em 18 de junho de 2022. https://pt.wikipedia.org/wiki/%C3%81rvores_de_Merkle

No ano de 2004 o estudioso Hal Finney deu o primeiro passo para a história das moedas digitais. Ele implementou no sistema de blockchain o conceito de RPoW – *Reusable Proof os Work* (Prova de Trabalho Reutilizável), do qual recebia um token (chave eletrônica), e em troca criava um novo token que poderia ser transmitido de uma pessoa para outra. Com isso, segundo o Academy Binance (2020), Finney:

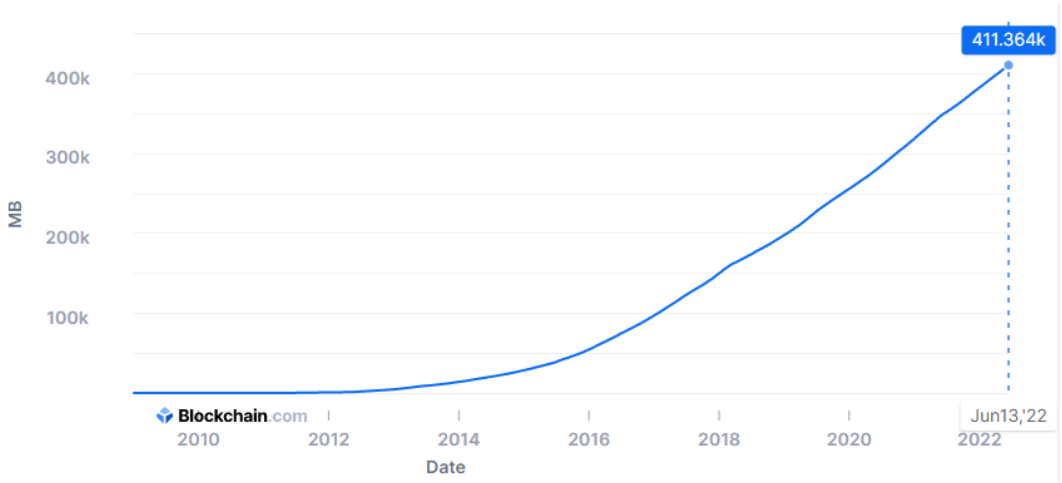
> [...] solucionou o problema do gasto duplo mantendo a propriedade dos tokens registrados em um servidor confiável e projetado para permitir que usuários em todo o mundo verificassem em tempo real os dados com exatidão e integridade.

A primeira blockchain pública foi propriamente lançada em 2008 pelo pseudônimo Satoshi Nakamoto, cuja identidade continua sendo um mistério nos dias

de hoje. Através da publicação intitulada "*Bitcoin: A Peer-to-Peer Electronic Cash System*[1]", Nakamoto pretendia criar um livro razão para transações públicas da criptomoeda bitcoin, a primeira moeda digital independente de autoridades governamentais ou bancos centrais. O *design* do bitcoin inspirou outras aplicações e blockchains (POPPER, 2016).

Depois de 6 anos, em agosto de 2014, o tamanho do arquivo blockchain do bitcoin, contendo registros de todas as transações que ocorreram na rede, atingiu 20 GB (gigabytes) (NIAN *et al*., 2015). Em 2015, o tamanho cresceu para quase 30 GB e, de 2016 a 2017, a blockchain do bitcoin cresceu de 50 para 100 GB. O tamanho do livro-razão do bitcoin ultrapassou 400 GB em 2022.

**Figura 2:** Tamanho da blockchain do bitcoin em megabytes em escala linear.




Fonte: Blockchain.com, acessado em 18 de junho de 2022.
https://www.blockchain.com/pt/charts/blocks-size

## 1.1 Estrutura de Blockchain

Por ser um livro-razão digital descentralizado e distribuído, a maioria dos blockchains permitem que os participantes da rede verifiquem e auditem as informações de forma independente e simultânea. Os dados de um blockchain é gerenciado de forma autônoma usando, na maioria das vezes, uma rede *peer-to-peer*. Os dados das transações são autenticados pela colaboração em massa alimentada

[1] Nakamoto, 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf Acessado em 30/06/2022.

por interesses próprios coletivos (TAPSCOTT, 2016). O uso de um blockchain remove a característica de reprodutibilidade infinita de um ativo digital, confirmando que cada unidade de valor foi transferida uma só vez, resolvendo o problema de gasto duplo.

A participação em uma blockchain só pode ser realizada através de softwares específicos de cada blockchain. Uma vez instalado na máquina, este software interage com outros computadores para realizar o download das informações contidas na rede, assim executando e verificando o estado de uma blockchain. Ao baixar um bloco da blockchain, por exemplo, a máquina verifica se este foi desenvolvido seguindo as regras do protocolo do sistema, e, em seguida, transmite essa informação para outros pares do ecossistema. Tal ambiente pode conter dezenas, centenas, milhares e até milhões de máquinas (nós) que sincronizam uma cópia idêntica das informações da rede durante 24 horas por dia, todos os dias.

Porém a tecnologia blockchain avança sendo impactada pelo Trilema da Escalabilidade. Isso significa que uma blockchain só pode ter duas das três propriedades, ou que precisa abrir mão de uma das três propriedades, sendo elas: segurança, descentralização e escalabilidade.

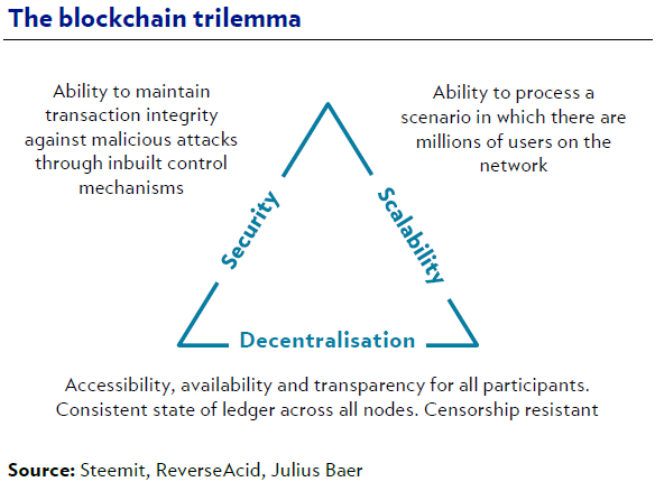
O conceito foi criado por Vitalik Buterin, criador do Ethereum, em discussões sobre os desafios para a adoção de tecnologias blockchain, estabelecendo que uma blockchain deve equilibrar as três variáveis, dependendo da função da aplicação (HAFID, 2020).

- **Segurança**: Uma blockchain precisa ter capacidade de se defender e ter segurança suficiente contra ataques e entidades mal intencionadas, é a proteção de toda a criptografia que permite com que a rede esteja protegida. A *layer* 0, ou camada zero, base de uma blockchain, precisa garantir que a segurança das informações seja inviolável.
- **Descentralização**: Uma blockchain não pode ser manipulada por um único ponto da rede *p2p*, sendo fundamental que a rede esteja distribuída no maior número de nós possíveis, compartilhadas igualmente entre todos os participantes, nós da rede.
- **Escalabilidade**: Uma blockchain precisa ter velocidade e estabilidade suportando uma imensa quantidade de informações, de modo que a rede não seja comprometida devido ao congestionamento de informações, impactando no tempo de espera e custos de transação

com a rede, assim como no tempo para criação de um novo bloco. A *layer* 2, protocolos com soluções de *sidechains* e , como a *Lightning Network* na rede do Bitcoin, a Polygon na blockchain da Ethereum e os sistemas de parachains da rede da Polkadot.

Isso significa que, ao prezar por segurança e escalabilidade, uma rede perde em descentralização, havendo poucos nós de validação e deixando a rede mais centralizada. Por outro lado, ao ter uma rede distribuída em muitos nós, descentralizada, e segura devido à qualidade de validadores da rede, perde-se em escalabilidade, tornando a rede mais lenta e cara. Fica claro que para que o avanço do desenvolvimento da tecnologia blockchain siga prosperando, um equilíbrio entre estes três fatores é inevitável.

**Figura 3 -** O trilema da blockchain.




Fonte: Trilema da Blockchain, Bar, 2021.

### 1.1.1 Blocos

Uma rede blockchain é um grande banco de dados distribuído e descentralizado que se autorreplica caso um nó desapareça ou adentre na rede. Isso significa que, caso um nó saia da rede, outros nós já têm dentro de si uma cópia exata de todas as informações contidas no nó ausente. Na via oposta, caso um novo nó

entre na rede, automaticamente é realizada uma cópia com as informações para o novo nó. Nós estes, que registram nos blocos todas as informações da transação.

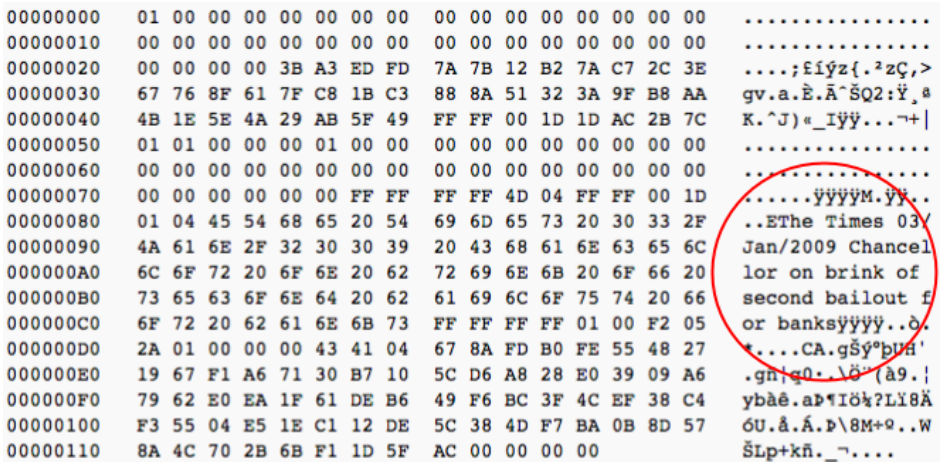
Os blocos contêm lotes de transações válidas, denominados *hash*. Cada bloco inclui o *hash* criptográfico do bloco anterior no blockchain, interligando os dois e vinculando-os em forma de cadeia. Esse processo iterativo confirma a integridade do bloco anterior, de volta ao bloco inicial, que é conhecido como bloco de gênese (BHASKAR, *et al.,* 2015).

**Figura 4** - Interdependência entre blocos.


Fonte: Desenvolvido pelo autor.

O bloco gênese de uma blockchain, ou bloco 0, serve como um estado inicial do sistema. Lançado tal bloco, novos blocos são adicionados à cadeia de blocos. O bloco gênesis do bitcoin, por exemplo, além das informações citadas acima, também contém a seguinte frase, traduzida para o português: “Chanceler à beira do segundo resgate para bancos”. Tal alusão ao jornal britânico *The Times* demonstra a descrença de Satoshi Nakamoto com o sistema bancário e a instabilidade do sistema financeiro, gerado por moedas inflacionárias como o real e o dólar.

**Figura 5** - Retrato do bloco gênesis do Bitcoin




Fonte: Wikipedia. Bloco Gênesis https://en.bitcoin.it/wiki/Genesis_block

A criação de novos blocos, assim como a validação das informações contidas na blockchain é chamada de *data hashing*, ou mineração. Isso significa que, de um dado *output* (saída), é praticamente impossível adivinhar qual foi o *input* (entrada). Assim, qualquer participante da rede pode validar se o bloco gerado na blockchain estava correto, sem violações. Graças a criptografia de chave pública e privada existe tal segurança na rede. Apenas o proprietário conhece sua chave privada, esta vinculada a chave pública na rede, assim como apenas uma assinatura válida pode certificar uma movimentação, permite que as moedas sejam movimentadas.

Às vezes, blocos separados podem ser produzidos simultaneamente, criando uma bifurcação temporária. Além de um histórico baseado em *hash* seguro, qualquer blockchain tem um algoritmo específico para pontuar diferentes versões do histórico, de forma que uma com uma pontuação mais alta possa ser selecionada em detrimento de outras. Os blocos não selecionados para inclusão na cadeia são chamados de blocos órfãos (BHASKAR, *et al.*, 2015). Os pares que dão suporte ao banco de dados têm diferentes versões do histórico de tempos em tempos. Eles mantêm apenas a versão de maior pontuação do banco de dados. Sempre que um par recebe uma versão de pontuação mais alta (geralmente a versão antiga com um único bloco novo adicionado), ele amplia ou sobrescreve seu próprio banco de dados e retransmite a melhoria para seus pares. Nunca há uma garantia absoluta de que qualquer entrada em particular permanecerá na melhor versão da história para sempre. As blockchains são normalmente construídas para adicionar a pontuação de novos blocos à blocos antigos, e recebem incentivos para estender novos blocos em vez de substituir blocos antigos. Portanto, a probabilidade de uma entrada ser substituída diminui exponencialmente à medida que mais blocos são construídos em cima dela, tornando-

se eventualmente muito baixa (ANTONOPOULOS, Andreas, 2014). Por exemplo, o bitcoin usa um sistema de prova de trabalho (*Proof-of-Work*), onde a cadeia com a prova de trabalho mais cumulativa é considerada válida pela rede. Existem vários métodos, também conhecidos como algoritmos de consenso, que podem ser usados para demonstrar um nível suficiente de computação. Dentro de uma blockchain, a computação é realizada de forma redundante, em vez da forma tradicional segregada e paralela.

### 1.1.2 Algoritmo de consenso

Um algoritmo de consenso em um blockchain é uma regra que garante que novos dados inseridos em um bloco não possam ser modificados, pois as informações contidas em um novo bloco precisam ser verificadas por todos os demais blocos, gerando assim confiança na rede sem a necessidade de uma terceira parte centralizadora. A criação, ou mineração, de um novo bloco só virá a ser realidade quando o bloco passar pelas regras do algoritmo de consenso e se tornar público para auditoria de todos os usuários da rede. Segundo artigo da Binance Academy[2]:

> "Um algoritmo de consenso é um mecanismo que permite que usuários ou máquinas se coordenem em uma configuração distribuída. Ele deve garantir que todos os membros de um sistema possam concordar com uma única fonte de verdade, mesmo que alguns dos membros falhem. Em outras palavras, o sistema deve ser tolerante a falhas."

Dessa forma, com o consenso distribuído não existe a necessidade dos usuários da rede confiarem em ninguém, senão que no próprio algoritmo. Existem diversos tipos de algoritmos de consenso para resolver o problema de confiança em sistemas de processamento distribuído, como é o caso da blockchain. Os três principais são:

---

[2] Binance Academy: https://academy.binance.com/pt/articles/what-is-a-blockchain-consensus-algorithm Acessado em 18/06/2022

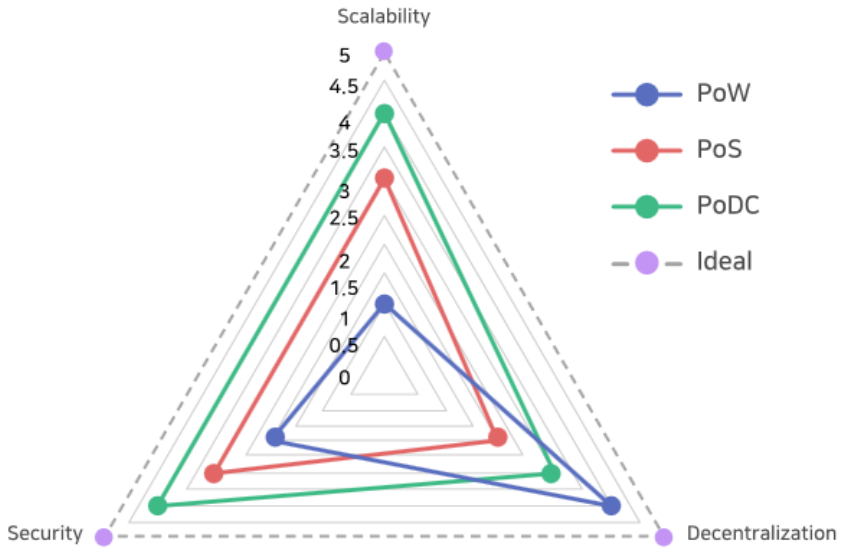
- **PoW – *Proof-of-Work* (prova de trabalho)**: O Proof-of-Work é um dos primeiros algoritmos de consenso para uso da tecnologia blockchain. A primeira vez que este algoritmo foi utilizado foi para combater *junk e-mails* em correspondências eletrônicas, fruto de um artigo publicado por Cynthia Dwork e Moni Naor em 1992 como um mecanismo para combater *junk mails*. Por outro lado, o conceito de *proof-of-work* foi popularizado com a criação do Bitcoin. Através da competição de computadores ligados à blockchain, este algoritmo identifica aquele que primeiro encontrar o *hash* respectivo ao novo bloco. Assim, computadores com maior poder computacional, e maior consumo energético, têm maior probabilidade de minerar o novo bloco. Em troca, este nó da rede (computador) ganha uma recompensa em forma de moeda digital. A blockchain do bitcoin utiliza este algoritmo de consenso.

- **PoS – *Proof-of-Stake* (prova de participação)**: A primeira implementação funcional de uma criptomoeda de prova de participação foi a Peercoin, introduzida em 2012 (SALEH, Fahad 2021). No entanto, foi a partir de 2017 que o uso de algoritmos de consenso de prova de participação começou a ser amplamente utilizado. (Li, Wenting, *et al*. 2017). Este tipo de algoritmo de consenso surgiu para resolver o problema do alto gasto energético dos algoritmos que usam da prova de trabalho. Em vez de priorizar o nó com a forma de trabalho mais rápida, ou seja, com maior velocidade computacional para encontrar o *hash*, no algoritmo PoS é necessário que o nó tenha acesso à uma grande parte das moedas digitais aceitas na blockchain para que possa realizar a mineração do novo bloco. A validação do nó para a mineração de um novo bloco consiste no depósito das moedas digitais na própria blockchain, provando assim a posse do ativo e diminuindo a possibilidade de ataques maliciosos que apenas poderiam depreciar o valor do ativo. Os participantes do blockchain com maior número de moedas votam para a escolha do nó validador, e o peso do voto está diretamente relacionado com a quantidade de moedas em caixa. O desenvolvimento desse tipo algoritmo surgiu para minimizar a dependência energética de grandes computadores, fazendo com que

uma máquina mineradora seja ao mesmo tempo uma carteira virtual onde o poder é diretamente proporcional ao saldo em conta.

- **DPoS – Delegated-Proof-of-Stake** (prova de participação delegada): Este tipo de algoritmo de consenso surgiu para resolver o problema do alto gasto energético dos algoritmos que usam da prova de trabalho e inserir uma camada extra de democracia ao algoritmo de prova de trabalho. Similar ao PoS, o DPoS também leva em consideração a quantidade de ativos digitais dos participantes, porém de uma maneira mais colaborativa, pois a escolha não é de participantes em si, mas de delegados que combina um sistema social de reputação para alcançar o consenso. Ou seja, todo usuário que possui um ativo digital na rede exerce certo grau de influência sobre o que acontece na rede. Este tipo de algoritmo de consenso usa um sistema de votação combinada a um sistema social de reputação para que o consenso seja alcançado. Pode ser considerado como o protocolo de consenso menos centralizado quando comparado com os algoritmos anteriores. As críticas desse algoritmo são referentes aos grandes proprietários de moedas que podem exercer poder centralizado na blockchain.

**Figura 6** - Comparação da solução do trilema da blockchain baseado em diferentes algoritmos de consenso



Fonte: Medium CMReap, 2021 https://medium.com/reapchain/solutions-for-trilemma-61ace7d717cc

Cada nó em um sistema descentralizado tem uma cópia do blockchain. A qualidade dos dados é mantida por replicação massiva de banco de dados (RAVAL, 2013) e confiança computacional. Não existe nenhuma cópia oficial centralizada e nenhum usuário é mais confiável do que qualquer outro (BRITO, *el al.*, 2013). As transações são transmitidas para a rede usando software. As mensagens são entregues com base no melhor esforço. Os nós de mineração validam as transações (BHASKAR, *et al.*, 2015), adicionam-nas ao bloco que estão construindo e, em seguida, transmitem o bloco completo para outros nós (ANTONOPOULOS, Andreas, 2014). Blockchains usam vários esquemas de marcação de data e hora, como prova de trabalho, para serializar as alterações (KOPFSTEIN, Janus, 2013). Métodos alternativos de consenso incluem prova de aposta (BHASKAR, *et al.*, 2015). O crescimento de uma blockchain descentralizada é acompanhada pelo risco de centralização porque os recursos de computador necessários para processar grandes quantidades de dados se tornam mais caros (GERVAIS, *et al.*, 2016).

### 1.1.3 Rede P2P e Descentralização

A maioria dos blockchains utilizam uma arquitetura de redes de computador *p2p*, onde cada um dos nós da rede funcionam tanto como servidor como cliente, possibilitando o compartilhamento de dados sem a necessidade de um sistema de administração centralizado. Ao armazenar dados em sua rede *p2p*, a blockchain elimina uma série de riscos que vêm com o armazenamento de dados de maneira centralizada. A blockchain descentralizada pode usar passagem de mensagens *ad hoc* e rede distribuída. Redes de blockchain *peer-to-peer* carecem de pontos centralizados de vulnerabilidade que hackers possam explorar. Os métodos de segurança da blockchain incluem o uso de criptografia de chave pública (BRITO *et al.,* 2013). Uma chave pública é um endereço no blockchain, representado por uma longa sequência de números de aparência aleatória. Os tokens de valor enviados pela rede são registrados como pertencentes a esse endereço. Uma chave privada é como uma senha que dá ao seu proprietário acesso aos seus ativos digitais ou os meios para interagir de outra forma com os vários recursos que o blockchains suporta.

### 1.1.4 Interoperabilidade

Com o crescente número de sistemas de blockchain surgindo, a interoperabilidade de blockchain se torna um tópico de grande relevância. O objetivo da interoperabilidade é dar suporte à transferência de ativos de um sistema blockchain para outro. Para Wegner (1996) "interoperabilidade é a habilidade de dois ou mais componentes de software cooperarem apesar das diferenças de linguagem, interface e plataforma de execução". O objetivo da interoperabilidade de blockchain é, portanto, apoiar tal cooperação entre sistemas de blockchain, apesar de suas diferenças.

Já existem várias soluções de interoperabilidade de blockchain disponíveis (BELCHIOR *et al*., 2020). Eles podem ser classificados em três categorias: abordagens de interoperabilidade de criptomoeda, motores de blockchain e conectores de blockchain. A *Internet Engineering Task Force* (IETF) tem um grupo de trabalho de interoperabilidade Blockchain que já produziu o rascunho de uma arquitetura de interoperabilidade de blockchain (HARDJONO, T *et al*., 2020).

## 1.2 Tipos de Blockchain

Existem diversos tipos de blockchains quanto às suas principais características relacionadas ao problema do trilema das blockchain, apresentadas a seguir. Este capítulo tem como objetivo apresentar alguns dos principais tipos de blockchains existentes.

### 1.2.1 Blockchains públicas

Uma blockchain pública não tem absolutamente nenhuma restrição de acesso. Qualquer pessoa com uma conexão à Internet pode enviar transações para ela, bem como se tornar um validador através do processo de mineração[3]. Normalmente, essas

[3] How Companies Can Leverage Private Blockchains to Improve Efficiency and Streamline Business Processes" Perfectial. https://perfectial.com/blog/leveraging-private-blockchains-improve-efficiency-streamline-business-processes/ Acessado em 18/06/2022.

redes oferecem incentivos econômicos para aqueles que protegem e utilizam algum tipo de algoritmo de prova de participação ou prova de trabalho. Alguns dos maiores e mais conhecidos blockchain públicos são o blockchain bitcoin e o blockchain Ethereum.

### 1.2.2 Blockchains privadas ou permissionadas

Em uma blockchain privada não se pode entrar, a menos que seja convidado pelos administradores da rede. O acesso do participante e do validador é restrito. Para distinguir entre blockchains abertos e outros aplicativos de banco de dados descentralizados *p2p* que não são *clusters* de computação *ad-hoc* abertos, a terminologia *Distributed Ledger* (DLT) é normalmente usada para blockchains privados.

### 1.2.3 Blockchains híbridas

Um blockchain híbrido tem uma combinação de recursos centralizados e descentralizados (WALKER, 2018). O funcionamento exato da cadeia pode variar com base em quais partes da descentralização de centralização são usadas.

### 1.2.4 *Sidechain*

*Sidechain* ou cadeira paralela é uma blockchain que valida dados de outras blockchains, permitindo a troca de informações de duas ou mais blockchains, muitas vezes funcionando nas segundas camadas das blockchains. Uma *sidechain* é a designação para um livro-razão de blockchain que é executado em paralelo a um blockchain primário (RAVAL, Siraj, 2016). As entradas da blockchain primária, onde as referidas entradas normalmente representam ativos digitais, podem ser vinculadas de e para a *sidechain*. Isto permite que a cadeia lateral opere de outra forma independentemente da blockchain primária, como por exemplo, usando um meio alternativo de manutenção de registros, algoritmo de consenso alternativo. (BELCHIOR *et al.*, 2020).

## 1.3 Usos de Blockchain

Muitas são as aplicações possíveis da tecnologia blockchain. Essa tecnologia pode ser usada para resolver diversos problemas contemporâneos, de diversas indústrias e mercados que vão muito além do setor de criptomoedas. Por outro lado, este é o principal segmento de mercado onde a tecnologia blockchain é recordada. Este capítulo tem como objetivo apresentar algumas das aplicações da tecnologia blockchain.

### 1.3.1 Criptomoedas

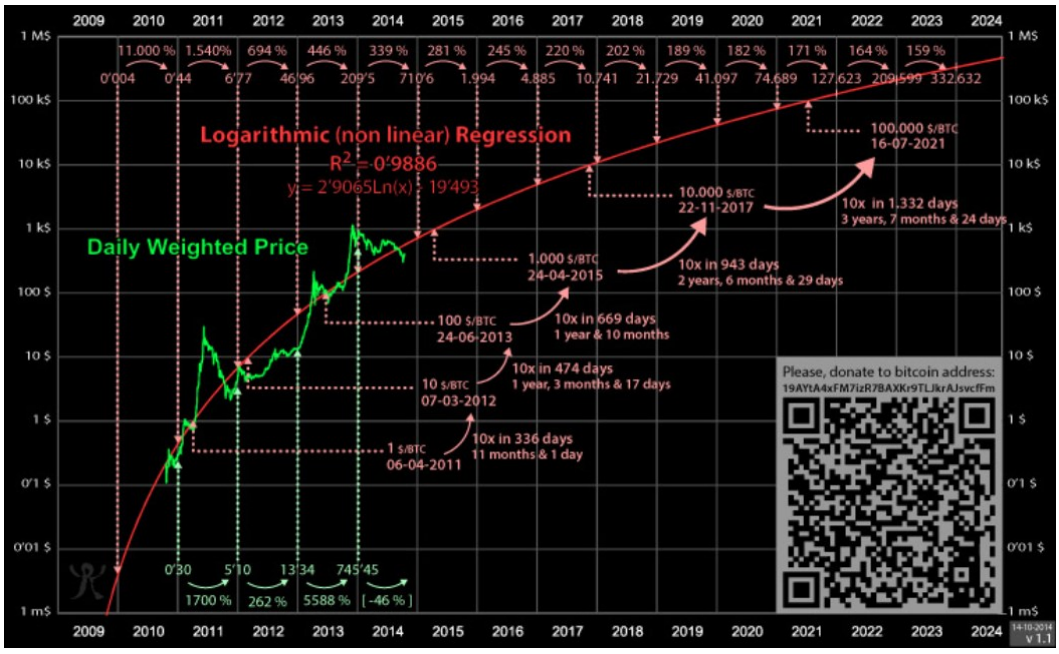
A maioria das criptomoedas usa tecnologia blockchain para registrar transações, como o BTC da rede bitcoin e o ETH da rede Ethereum, por exemplo. Uma criptomoeda é um ativo digital projetado para funcionar como um meio de troca em que os registros de propriedade de moedas individuais são armazenados na blockchain. Normalmente não existe na forma física, como papel-moeda, e normalmente não é emitido por uma autoridade central. As criptomoedas geralmente usam controle descentralizado em oposição à moeda digital centralizada (ALLISON, Ian, 2015) ou *CBDCs - Central Bank Digital Currency*, como o Real Digital no caso do Brasil. Quando uma criptomoeda é cunhada ou criada antes da emissão ou emitida por um único emissor, geralmente é considerada centralizada. Quando implementado com controle descentralizado, cada criptomoeda funciona por meio da tecnologia blockchain.

Como o Bitcoin ainda é uma classe de ativo relativamente jovem, seus movimentos de preços são altamente voláteis. Embora em uma macro linha do tempo o Bitcoin esteja sendo adotado, o movimento geral de preços leva em consideração ciclos de mercado. Durante esses ciclos de mercado, o preço do Bitcoin, principal ativo do mercado de criptomoedas, pode aumentar parabólicamente e também cair muito rapidamente. O primeiro exemplo de uma curva de regressão logarítmica do preço para o Bitcoin foi criado em 2014 pelo usuário do Bitcoin Talk “Trolololo”[4]. A imagem

[4] Bitcointalk, 2014. https://bitcointalk.org/index.php?topic=831547.0 Acessado em 18/06/2022.

a seguir mostra como o preço do BTC poderia evoluir ao longo do tempo usando a análise de regressão de crescimento de log:

**Figura 7** - Regressão logarítmica (não linear) para valor estimado do Bitcoin



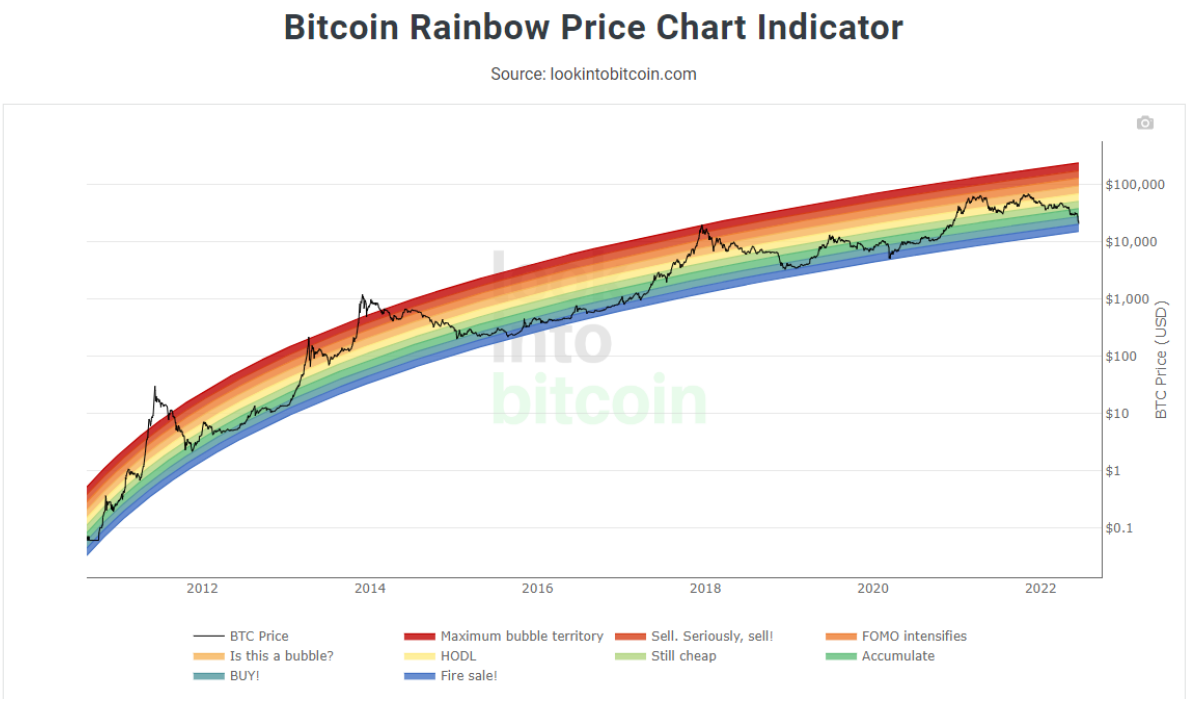

Fonte: Bitcoin Talks (2014) https://bitcointalk.org/index.php?topic=831547.0

Anos depois a plataforma *Look into Bitcoin* desenvolveu o *Rainbow Chart*[5] (gráfico arco-íris) baseado nos estudos de Trolololo, sendo o gráfico uma ferramenta de avaliação de longo prazo do preço do Bitcoin. Ele usa uma curva de crescimento logarítmica para prever a possível direção futura do preço do Bitcoin. Ele sobrepõe bandas de cores do arco-íris no topo do canal da curva de crescimento logarítmica em uma tentativa de destacar o sentimento do mercado em cada estágio de cores do

[5] Rainbow Chart – Look Into Bitcoin. https://www.lookintobitcoin.com/charts/bitcoin-rainbow-chart/ Acessado em 18/06/2022.

arco-íris à medida que o preço se move por ele. Até o momento, o preço do bitcoin continuou dentro das faixas de cores do arco-íris do canal de crescimento logarítmico.

**Figura 8** - Indicador de gráfico de preços Bitcoin Rainbow




Fonte: Lookintobitcoin, acessado em https://www.lookintobitcoin.com/charts/bitcoin-rainbow-chart/ 17/06/2022

As cores superiores mais quentes do gráfico do arco-íris mostram quando o mercado provavelmente está superaquecido. Esses períodos historicamente provaram ser bons momentos para o investidor estratégico começar a obter alguns lucros, assim como o posicionamento das bandas inferiores, em azul, indicam um bom momento para compra visando o longo prazo.

### 1.3.2 Contratos Inteligentes

Um *smart contract* ou contrato inteligente é um programa de computador ou um protocolo de transação que se destina a executar, controlar ou documentar automaticamente eventos e ações legalmente relevantes de acordo com os termos de um contrato ou acordo (TAPSCOTT, 2016). Os objetivos dos contratos inteligentes são a redução da necessidade de intermediários confiáveis, custos de arbitragem e execução, perdas por fraude, bem como a redução de exceções maliciosas e acidentais (SZABO, Nick, 2016).

*Smart contracts* baseados em blockchain são contratos que podem ser executados parcial ou totalmente, ou executados sem interação humana (FRANCO, 2014). Uma característica importante dos contratos inteligentes é que eles não precisam de um terceiro para atuar como intermediário entre as entidades contratantes. Isso pode reduzir o atrito entre as entidades ao transferir valor e, subsequentemente, pode abrir a porta para um nível mais alto de automação de transações (CASEY, 2018).

### 1.3.3 Anti-falsificação

A Blockchain pode ser usada na detecção de falsificações associando identificadores únicos a produtos, documentos e remessas, e armazenando registros associados a transações que não podem ser falsificadas ou adulteradas (MA *et al*., 2020). No entanto, é argumentado que a tecnologia blockchain precisa ser suplementada com tecnologias que forneçam uma forte ligação entre objetos físicos e sistemas blockchain (BALAGURUSAMY, 2019). Duas dessas tecnologias são o uso de âncoras criptográficas e a inserção de gráficos seguros em códigos QR (MORRIS, Nick, 2018).

### 1.3.4 Setor da Saúde

Em resposta à pandemia COVID-19 de 2020, o *The Wall Street Journal*[6] relatou que a Ernst & Young estava trabalhando em uma blockchain para ajudar

[6] A cryptocurrency technology finds new use tackling coronavirus. WSJ https://www.wsj.com/articles/a-

empregadores, governos, companhias aéreas e outros a rastrear pessoas que fizeram testes de anticorpos e poderiam ser imunes ao vírus. Além disso, a tecnologia blockchain estava sendo usada na China para acelerar o tempo que leva para os pagamentos de seguro saúde serem pagos a prestadores de cuidados de saúde e pacientes (CASTELLANOS, 2020).

### 1.3.5 Nomes de domínio

Ao contrário dos nomes de domínio regulares, nomes de domínio blockchain são inteiramente um ativo do proprietário do domínio e só podem ser controlados pelo proprietário através de uma chave privada (BEYERS, 2020). Os domínios blockchain abrem caminho para sites que são mais resistentes à censura e, portanto, permitem a liberdade de expressão, visto que não há autoridades ou indivíduos que possam intervir no controle de um domínio, exceto o detentor da chave privada (THIBODEAU, 2019) Eles poderiam ser uma opção melhor para substituir os endereços de carteira de criptomoeda tradicionais, pois é possível memorizar facilmente o domínio e usá-lo para receber pagamentos (ALLEMANN, 2020).

### 1.3.6 Cadeia de suprimentos

Há uma série de esforços e organizações da indústria trabalhando para empregar blockchain no gerenciamento da cadeia de suprimentos. No setor de mineração, por exemplo, a tecnologia Blockchain permite que atacadistas, varejistas e clientes rastreiem as origens das gemas e de outras mercadorias preciosas. A DTC, Diamond *Trading Company*, está envolvida na construção de um produto da cadeia de fornecimento de comércio de diamantes chamado *Tracr* (GSTETTNER, Stefan, 2019). A tecnologia Blockchain também está sendo usada para permitir que varejistas e consumidores rastreiem a procedência da carne e de outros produtos alimentícios, desde suas origens até as lojas e restaurantes (LEONG *et al*, 2018). O Walmart e a IBM estão executando um teste para usar um sistema apoiado por blockchain para

---

cryptocurrency-technology-finds-new-use-tackling-coronavirus-11587675966 Acessado em 18/06/2022

monitoramento da cadeia de suprimentos de alface e espinafre - todos os nós do blockchain são administrados pelo Walmart e estão localizados na nuvem da IBM (CORKERY *et al.,* 2018). A Fogo de Chão, rede de restaurantes temáticos brasileiros que oferece carnes grelhadas, anunciou parceria com a HerdX, empresa de tecnologia blockchain voltada para a indústria de alimentos, que permitirá a fornecedores, atacadistas e lanchonetes rastrear a carne servida nos restaurantes Fogo de Chão de volta à fazenda onde foi criado (BANDOIM, 2019).

### 1.3.7 Serviços financeiros

Grande parte da indústria financeira está implementando blockchains distribuídas para uso bancário (SHAH, 2018), e isso está ocorrendo mais rápido do que o esperado (KELLY, 2016). Os bancos estão interessados nesta tecnologia porque ela tem potencial para acelerar os sistemas de liquidação de *back office* (ARNOLD, 2013). Bancos como o UBS estão abrindo novos laboratórios de pesquisa dedicados à tecnologia de blockchain para explorar como o blockchain pode ser usado em serviços financeiros para aumentar a eficiência e reduzir custos (KELLY, 2016).

Em dezembro de 2018, a Bitwala lançou a primeira solução bancária de blockchain regulamentada da Europa que permite aos usuários gerenciar seus depósitos em bitcoin e em euros em um só lugar com a segurança e a conveniência de uma conta bancária alemã (KOLN, 2018).

### 1.3.8 Eleições

As eleições também podem acontecer através da aplicação do blockchain (CHANDRA, 2018). Nos últimos anos, estados estadunidenses de West Virginia, Denver e Utah usaram aplicativos móveis baseados em blockchain para permitir que militares e suas famílias que vivem no exterior pudessem votar por meio de um telefone[7].

[7] Computer World. Why blockchain cloud be a threat to democracy.

## 1.4 Blockchain na academia

Em outubro de 2014, o *MIT Bitcoin Club*, com financiamento de ex-alunos do do *Massachusetts Institute of Technology* (MIT), forneceu aos alunos de graduação acesso a 100 dólares em bitcoins. As taxas de adoção, conforme estudado por Catalini e Tucker (2016), revelaram que quando as pessoas que normalmente adotam tecnologias precocemente têm acesso atrasado à tecnologia, elas tendem a rejeitá-la.

As motivações para a adoção da tecnologia blockchain foram investigadas por diversos pesquisadores. Janssen *et al*. (2020) forneceu uma estrutura para análise. Koens e Poll (2019) apontaram que a adoção pela tecnologia blockchain pode ser fortemente impulsionada por fatores não técnicos. Com base em modelos comportamentais, Li (2020) discutiu as diferenças entre a adoção em nível individual e em nível de organização.

Acadêmicos da área de negócios e gestão começaram a estudar a função de blockchains para apoiar a colaboração (HSIEH *et al*., 2019). Graças à confiabilidade, transparência, rastreabilidade de registros e imutabilidade de informações, as blockchains facilitam a colaboração de uma forma que difere tanto do uso tradicional de contratos quanto das normas relacionais (LUMINEAU, 2020). Ao contrário dos contratos, as blockchains não dependem diretamente do sistema jurídico para fazer cumprir os acordos. Além disso, ao contrário do uso de normas relacionais, as blockchains não exigem confiança ou conexões diretas entre os colaboradores.

Em setembro de 2015, foi anunciado o primeiro jornal acadêmico revisado por pares dedicado à pesquisa de criptomoeda e tecnologia de blockchain, a *Ledger*. A edição inaugural foi publicada em dezembro de 2016 (EXTANCE, 2015). A revista cobre aspectos de matemática, ciência da computação, engenharia, direito, economia e filosofia que se relacionam a criptomoedas e a tecnologia de blockchain (HERTIG, 2015). A revista incentiva os autores a assinarem digitalmente um *hash* de arquivo de artigos submetidos, que são então carimbados no blockchain do bitcoin. Os autores

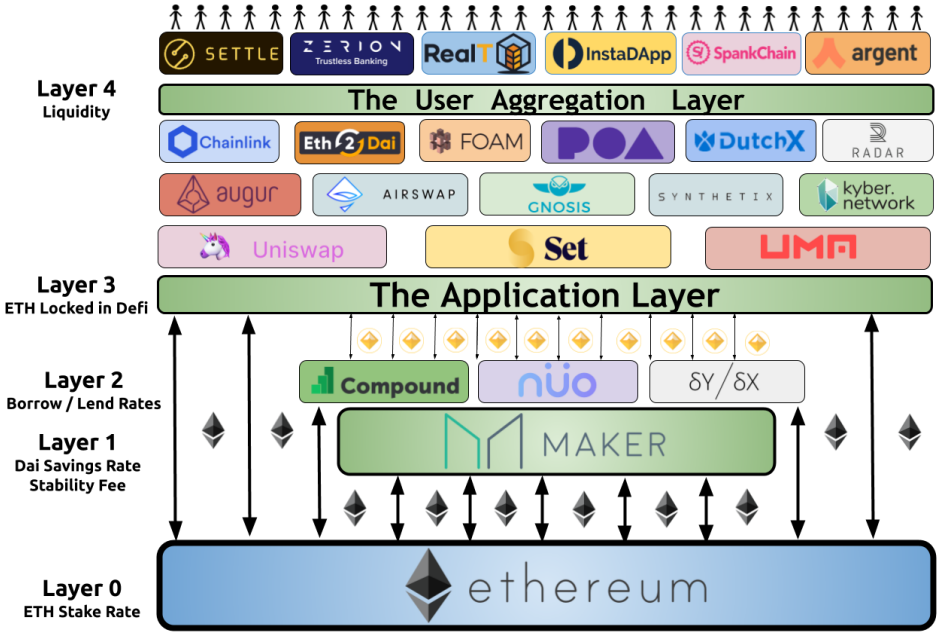
---

https://www.computerworld.com/article/3430697/why-blockchain-could-be-a-threat-to-democracy.html Acessado em 18/06/2022.

também são solicitados a incluir um endereço bitcoin pessoal na primeira página de seus artigos para fins de não repúdio (RIZUN, 2015).

Percebe-se até aqui que a tecnologia blockchain é relativamente nova e fundamental para a resolução de problemas presentes e futuros. No capítulo a seguir é apresentada a Ethereum, uma blockchain de segunda geração que abre a possibilidade para que distintos aplicativos descentralizados usem sua camada base para funcionar, como um software que precisa de um sistema operacional para ser utilizado.

**Figura 9** - Camadas da rede da Ethereum




Fonte: Medium. Hoffman, 2019. https://medium.com/pov-crypto/ethereum-the-digital-finance-stack-4ba988c6c14b

## 2. ETHEREUM

Ethereum é uma blockchain descentralizada de código aberto com funcionalidade de contrato inteligente. Ether (ETH) é a criptomoeda nativa da rede (VENKATARAMAKRISHNAN, 2021). O Ethereum foi concebido em 2013 através da publicação de um artigo do programador russo-canadense Vitalik Buterin, cofundador da *Bitcoin Magazine*. Porém, a Ethereum teve outros fundadores, como: Gavin Wood, Charles Hoskinson, Anthony Di Iorio e Joseph Lubin (PAUMGARTEN, 2018). Através de uma campanha de *crowdfunding* ou financiamento coletivo o projeto conseguiu arrecadar fundos para o desenvolvimento inicial da rede, em 2014, e já em 30 de julho de 2015 a rede entrou em operação (Ethereum Foundation, 2015).

Em um estudo de Camila Russo, de 2020, "*The infinite machine : how an army of crypto-hackers is building the next internet with Ethereum"*, é apresentado que Buterin argumentou com os desenvolvedores que mantém o *Bitcoin Core* código fonte do bitcoin, que a tecnologia Bitcoin e blockchain poderiam se beneficiar de outros aplicativos além do dinheiro digital, precisando de uma linguagem mais robusta para o desenvolvimento de aplicativos que pudessem anexar ativos do mundo real, como ações e propriedades físicas como imóveis, para a blockchain (RUSSO, 2020).

**Figura 10** - Símbolo da Ethereum

Fonte: Wikipedia. Logo da Ethereum
https://pt.m.wikipedia.org/wiki/Ficheiro:Ethereum_logo_2014.svg

## 2.1 ROADMAP DA ETHEREUM

A Ethereum foi anunciada na *North American Bitcoin Conference* em Miami, em janeiro de 2014 (PAUMGARTEN, 2018). A origem do nome “Ethereum” se deu através de Buterin, pois a palavra éter se refere a um hipotético meio invisível que permeia o universo e permite que a luz viaje. Buterin sonhava que sua plataforma fosse como um sistema operacional descentralizado onde aplicativos pudessem rodar em seu sistema de maneira imperceptível (RUSSO, 2020).

Desde o lançamento inicial, o Ethereum passou por várias atualizações de protocolo planejadas, que são mudanças importantes que afetam a funcionalidade subjacente e/ou estruturas de incentivo da plataforma (Ethereum Foundation, 2015).

Em 2016, uma organização autônoma descentralizada chamada *The DAO*, responsável pela governança de contratos inteligentes desenvolvidos na plataforma, foi explorada, quando 50 milhões de dólares em tokens DAO foram roubados por um hacker desconhecido. O evento provocou um debate na comunidade de criptomoedas sobre se o Ethereum deveria realizar um *hard fork* contencioso para reapropriar os fundos afetados. Isso resultou na divisão da rede em duas blockchains: Ethereum com o roubo revertido e Ethereum Classic que continuou na cadeia original.

O objetivo de impulsionar o uso da tecnologia blockchain da rede, em 2017 várias startups de blockchain e grupos de pesquisa criaram a *Enterprise Ethereum Alliance* (EEA)[8], que também contava com membros corporativos como a *ConsenSys, CME Group*, grupo de pesquisa da *Cornell University, Toyota Research Institute, Samsung SDS, Microsoft, Intel, JP Morgan, Cooley LLP, Merck KGaA, DTCC, Deloitte, Accenture, Banco Santander, BNY Mellon*, entre outros.

Em janeiro de 2018, a Ethereum era a segunda maior criptomoeda em termos de capitalização de mercado, atrás apenas do Bitcoin[9].

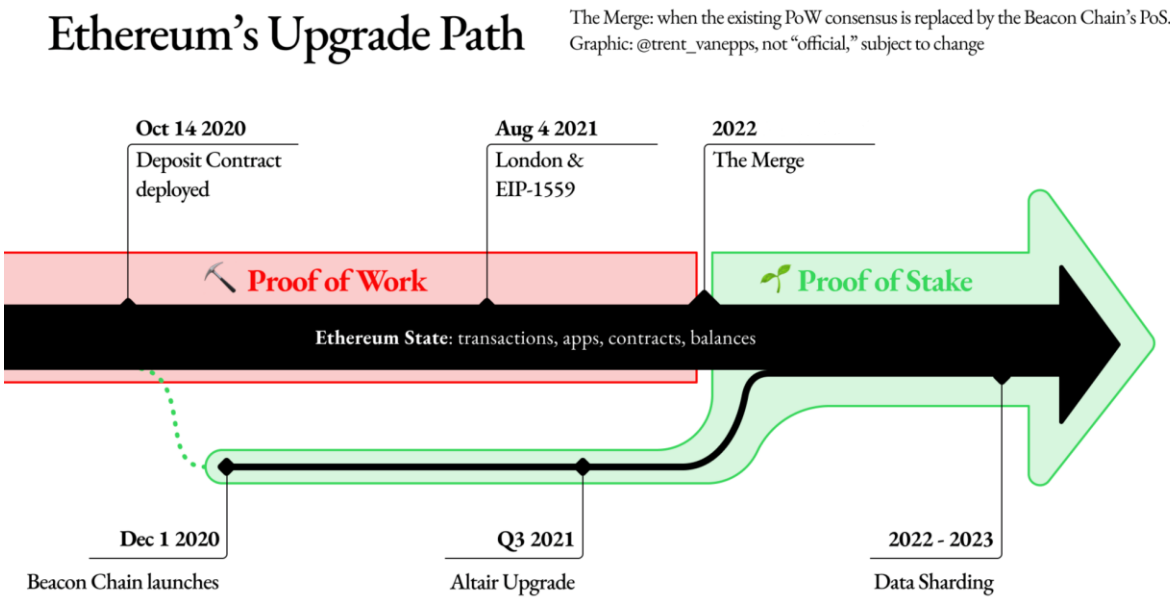
Durante os anos subsequentes, a rede passou por diversas atualizações de para garantir sua evolução alinhada aos desafios do trilema das blockchains, como a atualização de Constantinopla (2019), Berlin (2021) e London (2021), que incluiu a *EIP - Ethereum Improvement Proposal*[10] ou Proposta de Melhoria da Ethereum 1559, introduzindo um mecanismo para reduzir a volatilidade das taxas de transação através

[8] Enterprise Ethereum Alliance (EEA). https://entethalliance.org/ Acessado em 18/06/2022.
[9] Coinmarketcap. www.coinmarketcap.com Acessado em 18/06/2022.
[10] Ethereum Improvement Proposal. https://eips.ethereum.org/ Acessado em 18/06/2022.

da queima de tokens. O mecanismo faz com que uma parte do Éter paga em taxas de transação de cada bloco seja destruída em vez de entregue ao minerador, reduzindo a taxa de inflação do ETH e potencialmente resultando em períodos de deflação.

O roadmap da Ethereum inclui a mudança do seu algoritmo de consenso do *proof-of-work* para o *proof-of-stake*, inaugurando o Ethereum 2.0[11], expandindo a rede de maneira descentralizada.

**Figura 11** - Roadmap de curto prazo da Ethereum




Fonte: Ethereum Foundation, 2022. https://blog.ethereum.org/2022/01/24/the-great-eth2-renaming/

## 2.2 Ethereum Virtual Machine

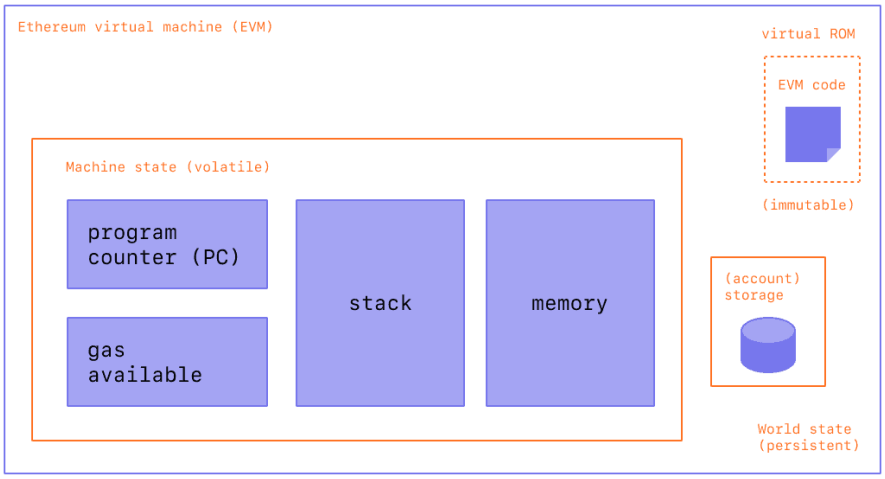
A Ethereum Virtual Machine (EVM) ou Máquina Virtual da Ethereum é o ambiente que contém uma pilha de transação, memória, balanço de gás, contador de programa e código de contratos inteligentes. Quando uma transação chama a função de um contrato, os argumentos na chamada são adicionados à pilha e o EVM traduz o *bytecode* do contrato em operações de pilha. A definição formal do EVM é

[11] Blog Ethereum. The great eth2 renaming. https://blog.ethereum.org/2022/01/24/the-great-eth2-renaming/ Acessado em 18/06/2022.

especificada no *Ethereum Yellow Paper*[12]. Sendo a própria Ethereum Foundation, EVMs foram implementados em C++, C#, Go, Haskell, Java, JavaScript, Python, Ruby, Rust, Elixir e Erlang[13].

O próprio protocolo Ethereum existe apenas com o propósito de manter a operação contínua, ininterrupta e imutável dessa máquina, sendo o ambiente em que todas as contas e contratos inteligentes coexistem. Em qualquer bloco da cadeia, a Ethereum tem um e apenas um estado canônico, e o EVM é o que define as regras para calcular um novo estado válido de bloco a bloco.

**Figura 12** - Ethereum Virtual Machine (EVM)




Fonte: Ethereum Foundation, 2022. https://ethereum.org/en/developers/docs/evm/

O conjunto de instruções do EVM é Turing-completo (Ethereum Foundation, 2020). Na teoria da computação, um sistema de regras de manipulação de dados é dito Turing-completo ou computacionalmente universal se e somente se puder ser usado para manipular qualquer máquina de Turing de única fita e assim, a princípio, qualquer computador[14].

[12] Ethereum Yellow Paper. *https://ethereum.github.io/yellowpaper/paper.pdf* Acessado em 18/06/2022.
[13] Ethereum Foundation. https://ethereum.org/en/developers/docs/evm/ Acessado em 18/06/2022.
[14] Wikipedia. Turing completo. https://pt.wikipedia.org/wiki/Turing_completude) Acessado em 18/06/2022.

## 2.3 CONTRATOS INTELIGENTES E LINGUAGEM DE PROGRAMAÇÃO

Os contratos inteligentes da Ethereum são escritos em linguagens de programação de alto nível e, em seguida, compilados para *bytecode* EVM e implantados na blockchain Ethereum. Segundo a Ethereum Foundation, o código fonte e as informações do compilador são geralmente publicados junto com o lançamento do contrato para que os usuários possam ver o código e verificar se ele compila para o *bytecode* que está na cadeia.

Os contratos inteligentes da rede podem ser programados em diversas linguagens de programação como Serpent, Yul, LLL e Mutan (Ethereum Foundation, 2020). Porém a maioria dos contratos são escritos em Solidity, uma linguagem de programação orientada a objetos, muito semelhante a JavaScript, Python, e C++, conforme pode ser visto a seguir.

```
// SPDX-License-Identifier: GPL-3.0
pragma solidity ^0.8.4;

contract Coin {
    // The keyword "public" makes variables
    // accessible from other contracts
    address public minter;
    mapping (address => uint) public balances;

    // Events allow clients to react to specific
    // contract changes you declare
    event Sent(address from, address to, uint amount);

    // Constructor code is only run when the contract
    // is created
    constructor() {
        minter = msg.sender;
    }

    // Sends an amount of newly created coins to an address
    // Can only be called by the contract creator
    function mint(address receiver, uint amount) public {
        require(msg.sender == minter);
        balances[receiver] += amount;
```

```
    }

    // Errors allow you to provide information about
    // why an operation failed. They are returned
    // to the caller of the function.
    error InsufficientBalance(uint requested, uint available);

    // Sends an amount of existing coins
    // from any caller to an address
    function send(address receiver, uint amount) public {
        if (amount > balances[msg.sender])
            revert InsufficientBalance({
                requested: amount,
                available: balances[msg.sender]
            });

        balances[msg.sender] -= amount;
        balances[receiver] += amount;
        emit Sent(msg.sender, receiver, amount);
    }
}
```

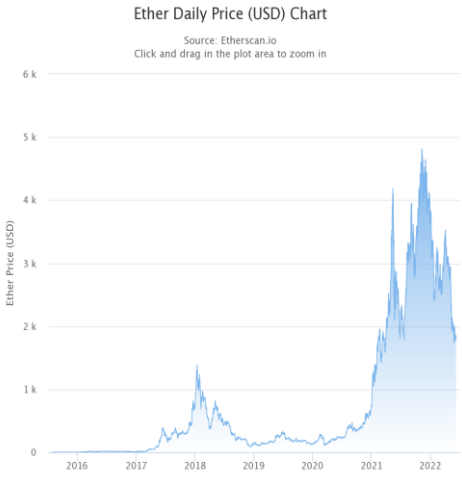
## 2.4 ÉTER (ETH)

Éter (ETH) é a criptomoeda gerada pelo protocolo Ethereum como recompensa aos mineradores em um sistema de prova de trabalho para adicionar blocos à blockchain. É a única moeda aceita no pagamento das taxas de transação, que também vão para os mineradores. A recompensa do bloco junto com as taxas de transação fornece o incentivo aos mineradores para manter a blockchain processando novas transações.

Portanto, ETH é fundamental para o funcionamento da rede. Cada conta Ethereum tem um saldo ETH e pode enviar ETH para qualquer outra conta. A menor subunidade de ETH é conhecida como *Wei*, em homenagem ao pioneiro da criptomoeda Wei Dai[15], e é igual a 10 −18 ETH.

[15] Wikipedia. Wei Dai. https://en.wikipedia.org/wiki/Wei_Dai Acessado em 18/06/2022.

**Figura 13** - Valor do ETH em dólares



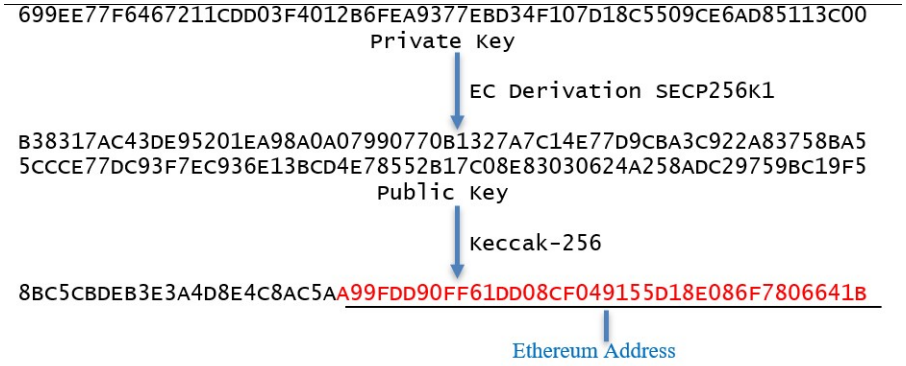

Fonte: Etherscan, acessado em 18 de junho de 2022. https://etherscan.io/charts

## 2.5 CONTAS

Existem dois tipos de contas no Ethereum: contas de usuário (também conhecidas como contas de propriedade externa) e contratos. Ambos os tipos possuem saldo de ETH, podem enviar ETH para qualquer conta, podem chamar qualquer função pública de um contrato ou criar um novo contrato.

As contas de usuário são o único tipo que pode criar transações. Para que uma transação seja válida, ela deve ser assinada usando a chave privada da conta de envio, a *string* hexadecimal de 64 caracteres da qual o endereço da conta é derivado. O algoritmo usado para produzir a assinatura é o ECDSA, Algoritmo de assinatura digital de curva elíptica. É importante ressaltar que esse algoritmo permite derivar o endereço do assinante da assinatura sem conhecer a chave privada.

**Figura 14** - Criação de um endereço público através de uma chave privada na Ethereum




Fonte: Stack Overflow. Acessado em 18 de junho de 2022. https://stackoverflow.com/questions/60697592/create-an-ethereum-public-address-from-a-private-key

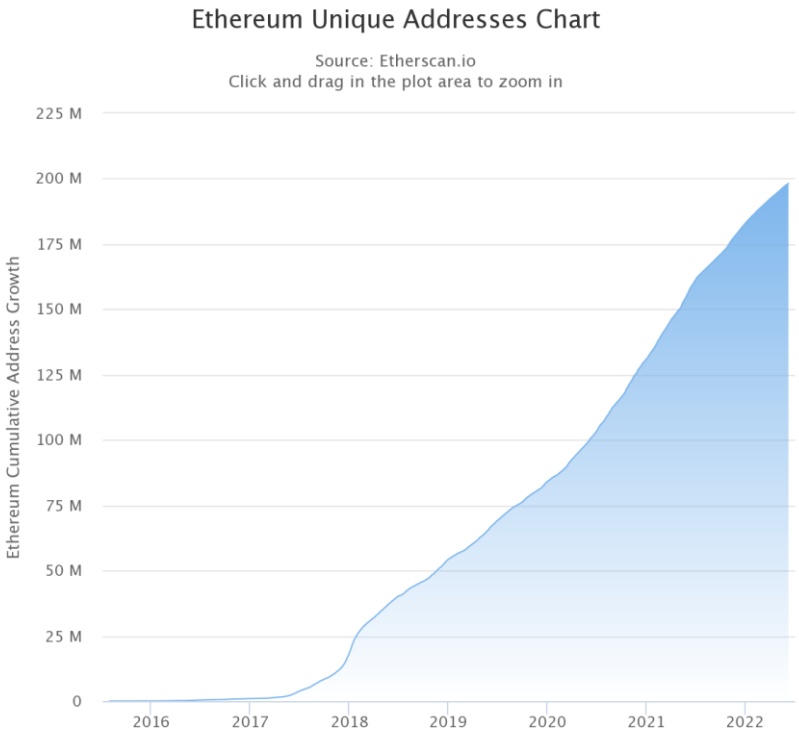
Os contratos são o único tipo de conta que possui código associado (um conjunto de funções e declarações de variáveis) e armazenamento de contrato (os valores das variáveis em um determinado momento). Uma função de contrato pode receber argumentos e valores de retorno. Dentro do corpo de uma função, além de instruções de fluxo de controle, o código de um contrato pode incluir instruções para enviar ETH, ler e gravar em seu armazenamento, criar armazenamento temporário que morre no final da função, realizar operações aritméticas e hashing operações, chamar suas próprias funções, chamar funções públicas de outros contratos, criar contratos e consultar informações sobre a transação atual ou o blockchain.[16]

## 2.6 ENDEREÇOS

Os endereços Ethereum são compostos pelo prefixo "0x", um identificador comum para hexadecimal, concatenado com os 20 bytes mais à direita do hash Keccak-256 da chave pública ECDSA. Em hexadecimal, dois dígitos representam um byte, o que significa que os endereços contêm 40 dígitos hexadecimais, por exemplo, 0x7a5ec603665C4E4Ea79791914Cf3a950A44a8F14. Os endereços de contrato estão no mesmo formato, no entanto, são determinados pelo remetente e pela transação de criação.

[16] Solidity. Introduction to Smart Contracts https://docs.soliditylang.org/en/v0.4.24/introduction-to-smart-contracts.html Acessado em 18/06/2022.

**Figura 15** - Número de endereços na rede Ethereum



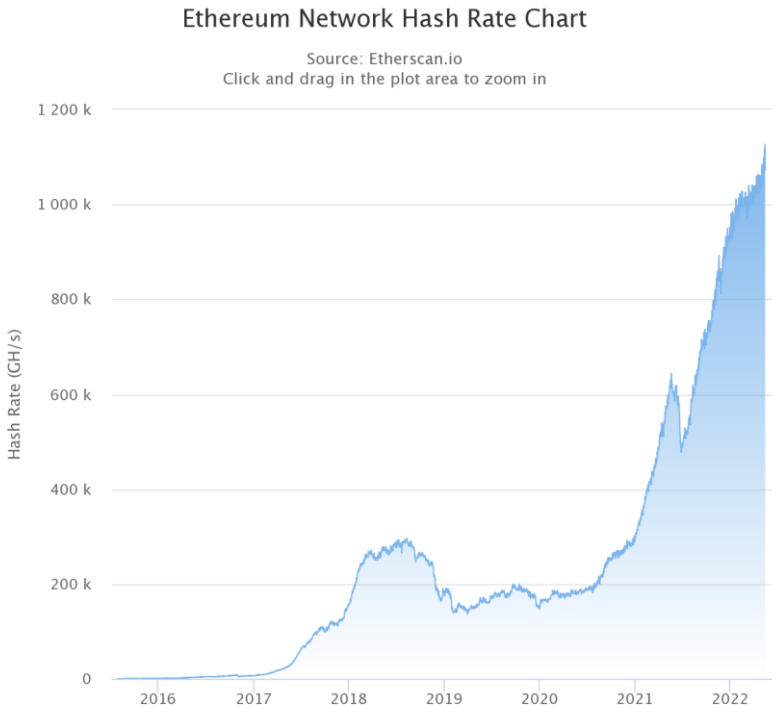

Fonte: Etherscan, acessado em 18 de junho de 2022.

## 2.7 GÁS

Gás é uma unidade de conta dentro do EVM usada no cálculo de uma taxa de transação, que é o valor de ETH que o remetente de uma transação deve pagar ao minerador que inclui a transação na blockchain. A taxa de *hash* da rede Ethereum é a medida do poder de processamento da rede, que desde sua origem cresce de modo exponencial, conforme gráfico abaixo, do Etherscan[17].

**Figura 16** - Taxa de hash na rede da Ethereum.

[17] Etherscan. https://etherscan.io Acessado em 18/06/2022.




Fonte: Etherscan, acessado em 18 de junho de 2022.

Cada tipo de operação que pode ser realizada pela EVM é codificada com um determinado custo de gás, que se destina a ser aproximadamente proporcional à quantidade de recursos computação e de armazenamento que um nó deve gastar para realizar uma operação. Ao criar uma transação, o remetente deve especificar um limite de gás e um preço de gás . O limite de gás é a quantidade máxima de taxa que o remetente está disposto a pagar na transação, e o preço do gás é a quantidade de ETH que o remetente deseja pagar ao minerador por unidade de gás utilizada. Quanto maior o preço do gás, mais incentivo um minerador tem para incluir a transação em seu bloco e, portanto, mais rápido a transação será incluída na blockchain. O remetente compra a quantidade total de gás antecipadamente, no início da execução da transação, e é reembolsado no final por qualquer gás não utilizado.

## 2.8 BOMBA DE DIFICULDADE

A bomba de dificuldade é um recurso do protocolo Ethereum que faz com que a dificuldade de mineração de um bloco aumente exponencialmente ao longo do tempo após um determinado bloco ser alcançado, com o objetivo de incentivar

atualizações no protocolo e impedir que os mineradores tenham muito controle sobre as atualizações (Ethereum Foundation, 2020).

À medida que o protocolo é atualizado, a bomba de dificuldade geralmente é empurrada para mais longe no tempo. Ele foi originalmente colocado lá principalmente para garantir uma atualização bem-sucedida de prova de trabalho para prova de participação.

## 2.9 TIPOS DE TOKENS NA ETHEREUM

Um dos muitos padrões de desenvolvimento do Ethereum se concentra em interfaces de token (BUTERIN, 2015). Esses padrões ajudam a garantir que os contratos inteligentes permaneçam compostos, por exemplo, quando um novo projeto emite um token, ele permanece compatível com as *exchanges* descentralizadas existentes.

Aqui estão alguns dos padrões de token mais populares no Ethereum, sendo os dois primeiros a maior parte dos tokens existentes na rede[18]:

- ERC-20: Uma interface padrão para tokens fungíveis (intercambiáveis), como tokens de votação, tokens de *staking* ou moedas virtuais.
- ERC-721: Uma interface padrão para tokens não fungíveis (NFTs), como uma escritura de arte ou uma música.
- ERC-777: permite que as pessoas criem funcionalidades extras em cima de tokens, como um contrato de mixagem para melhorar a privacidade das transações ou uma função de recuperação de emergência para salvá-la caso haja a perda das chaves privadas.
- ERC-1155: permite negociações mais eficientes e agrupamento de transações, economizando custos. Esse padrão de token permite a criação de tokens utilitários como o $BNB ou $BAT.

O padrão de token ERC-20 (*Ethereum Request for Comments 20*) permite tokens fungíveis na blockchain da Ethereum. O padrão, proposto por Fabian

[18] Ethereum Foundation. https://ethereum.org/en/developers/docs/standards/tokens/ Acessado em 18/06/2022.

Vogelsteller em novembro de 2015[19], implementa uma API para tokens dentro de contratos inteligentes.

O padrão fornece funções que incluem a transferência de tokens de uma conta para outra, obtendo o saldo atual do token de uma conta e obtendo o fornecimento total do token disponível na rede. Contratos inteligentes que implementam corretamente os processos ERC-20 são chamados de contratos de token ERC-20 e ajudam a acompanhar os tokens criados no Ethereum.

O Ethereum também permite a criação de tokens únicos e indivisíveis, chamados tokens não fungíveis (NFTs). Como os tokens desse tipo são únicos, eles têm sido usados para representar propriedades físicas (tokenização de imóveis por exemplo) e virtuais, como colecionáveis, arte digital, imóveis virtuais e itens dentro de jogos são exemplos de NFTs de propriedade digital.

Os NFTs fornecem um certificado público de autenticidade ou prova de propriedade baseado na confiança da rede blockchain, garantindo direitos autorais e direitos de propriedade intelectual para quem cunha ou minta, neologismo do inglês *mint*, o arquivo digital pela primeira vez. Um NFT não restringe o compartilhamento ou cópia de seu arquivo digital associado e não impede a criação de NFTs que fazem referência a arquivos idênticos.

Os NFTs têm sido usados como investimentos especulativos e atraíram críticas crescentes pelo custo de energia, bem como seu uso frequente em golpes de arte, comparado a uma bolha econômica ou a um esquema Ponzi[20].

## 2.10 ETHEREUM 2.0

O desenvolvimento de código aberto está em andamento para uma grande atualização para o Ethereum conhecido como Ethereum 2.0. O principal objetivo da atualização é aumentar a taxa de transferência de transações para a rede do atual de cerca de 15 transações por segundo para até dezenas de milhares de transações por segundo[21].

O objetivo declarado é aumentar a taxa de transferência dividindo a carga de trabalho em muitos blockchains executadas em paralelo, referido pela Ethereum

[19] Ethereum Improvement Proposal. https://eips.ethereum.org/ Acessado em 18/06/2022.
[20] Wikipedia. Ponzi. https://eips.ethereum.org/ Acessado em 18/06/2022.
[21] Ethereum. www.Ethereum.org Acessado em 18/06/2022.

Foundation como *sharding*[22] e, em seguida, fazendo com que todos compartilhem um blockchain de prova de participação de consenso comum, de modo que adulterar maliciosamente qualquer cadeia singular exigir que alguém adultere o consenso comum, o que custaria ao invasor muito mais do que ele poderia ganhar com um ataque.

Segundo o roadmap do Ethereum 2.0, o projeto foi projetado para ser lançado em três fases:

- A "Fase 0", também conhecida como "*The Beacon Chain*", foi lançada em 1º de dezembro de 2020 e criou a *Beacon Chain*, uma blockchain de prova de participação (PoS) que atuará como a coordenação central e o *hub* de consenso do Ethereum 2.0.
- A "Fase 1", também conhecida como "*The Merge*", fundirá a *Beacon Chain* com a atual rede Ethereum, fazendo a transição de seu mecanismo de consenso de *proof-of-work* para *proof-of-stake*, previsto para 2022.
- A "Fase 2", também conhecida como "cadeias de fragmentos", irá implementar a execução de estado nas cadeias de fragmentos com a atual cadeia Ethereum 1.0 prevista para se tornar um dos fragmentos do Ethereum 2.0 em 2023, segundo a Ethereum Foundation.

Por fim, atualmente a rede da Ethereum permite que sejam compilados aplicativos descentralizados (*Dapps*) de maneira permanente e imutável na blockchain, uma vez que a plataforma funciona com contratos inteligentes. Parte destes aplicativos são aplicativos de finanças descentralizadas (DeFi), fornecendo uma ampla gama de serviços financeiros sem a necessidade de intermediários financeiros, como corretoras, bolsas ou bancos. A plataforma também permite que usuários peguem empréstimos em criptomoedas ou emprestem suas moedas digitais ganhando juros (VIGNA, 2021).

[22] Ethereum Foundation. Shard Chains https://ethereum.org/en/upgrades/shard-chains/ Acessado em 18/06/2022.

# 3. FINANÇAS DESCENTRALIZADAS (DEFI) E CORRETORAS DESCENTRALIZADAS (DEX)

Finanças Descentralizadas é um conceito contemporâneo que está diretamente relacionado à existência da tecnologia blockchain. Uma de suas aplicações se dá através de corretoras descentralizadas de criptomoedas. Neste capítulo são abordados ambos os conceitos, além de suas aplicações, riscos e oportunidades, concluindo com a apresentação do caso de uso da aplicação Uniswap e o conceito de liquidez descentralizada.

## 3.1 FINANÇAS DESCENTRALIZADAS (DEFI)

Segundo a Ethereum Foundation[23] o DeFi é um sistema financeiro aberto e global construído para a era da internet, uma alternativa a um sistema centralizado e opaco, rigidamente controlado e mantido por infraestrutura e processos oligopólicos. As aplicações DeFi dão acesso a distintos serviços financeiros para qualquer pessoa com uma conexão com a internet e conhecimento para interagir com a Web3.

Para Schär (2021), o termo DeFi geralmente se refere a uma pilha de protocolos abertos, sem permissão e altamente interoperáveis, construída em plataformas públicas de contratos inteligentes. O DeFi replica os serviços financeiros tradicionais de uma forma mais aberta e transparente, não dependendo de intermediários e instituições centralizadas. Em vez disso, é baseado em protocolos abertos e aplicativos descentralizados (*DApps*). A confiança necessária para firmar um acordo financeiro entre as partes é aplicada pelas regras escritas no código dos contratos inteligentes. As transações são executadas de maneira segura e verificável. Assim, essa arquitetura das aplicações DeFi podem criar um sistema financeiro imutável e altamente interoperável com transparência sem precedentes, direitos de acesso iguais e pouca necessidade de custodiantes, câmaras centrais de compensação ou serviços de custódia, pois a maioria dessas funções pode ser assumida pelos contratos inteligentes das aplicações DeFi.

Schueffel (2021) desenvolveu em seu estudo "*DeFi: Decentralized Finance - An Introduction and Overview*" uma tabela que compara as principais características

[23] Defi. Ethereum https://ethereum.org/en/defi/ Acessado em 18/06/2022.

das finanças tradicionais (TradFi) ou finanças centralizadas (CeFi), com as finanças descentralizadas (DeFi), disponível abaixo.

**Tabela 1 - Características dos serviços financeiros tradicionais e descentralizados**

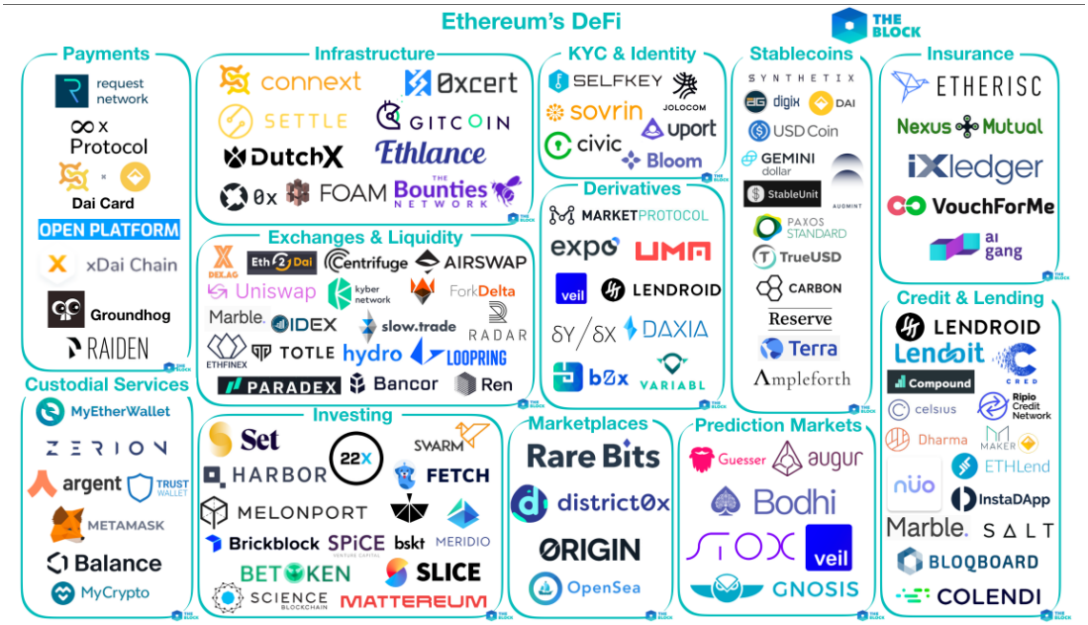
| **Característica** | **Serviços Financeiros Tradicionais (TradFi)** | **Finanças Descentralizadas (DeFi)** |
|---|---|---|
| Grau de automação | Baixo | Alto |
| Estrutura de rede | Centralizado | Descentralizado |
| Auto-custódia | Não | Sim |
| Sem confiança | Não | Sim |
| Importância da tecnologia | Baixa | Alta |
| Importância do intermediário | Alta | Baixa |
| Custos do serviço | Alto | Baixo |
| Foco do produto | Alto | Baixo |
| Transparente | Não | Sim |
| Código aberto | Não | Sim |
| Sem permissão | Não | Sim |
| Flexibilidade | Baixa | Alta |
| Segurança | Baixa | Alta |
| Regulamentado | Sim | Não |

Fonte: Schueffel (2021) *DeFi: Decentralized Finance - An Introduction and Overview*”

As finanças descentralizadas, em vez de um único serviço, representam todo um ecossistema de serviços financeiros prestados por meio de contratos inteligentes implantados na blockchain (AMMOUYS, S. 2015). Essa nova abordagem visa descentralizar o atual sistema financeiro fornecendo serviços sem intermediários, que são acompanhados por altos custos de transações, processos morosos e falta de transparência. Por outro lado, o DeFi permite que as transações sejam realizadas pela confiança *p2p*, de modo transparente e mais barato do que nas finanças tradicionais. Desta forma, aplicações como empréstimos, derivativos e negociação são automatizadas e executadas de forma confiável, transparente e com segurança (HOLOTIUK *et al*, 2017).

Por meio de recursos públicos de protocolos de código aberto, como aplicativos descentralizados e contratos inteligentes, o DeFi permite que os indivíduos joguem nos dois lados das transações financeiras (quem empresta e quem pega emprestado), consumindo e prestando serviços, e assim democratizando o acesso a instrumentos financeiros (JANASHIA, 2019).

**Figura 17** - Ecossistema de DeFi na rede Ethereum

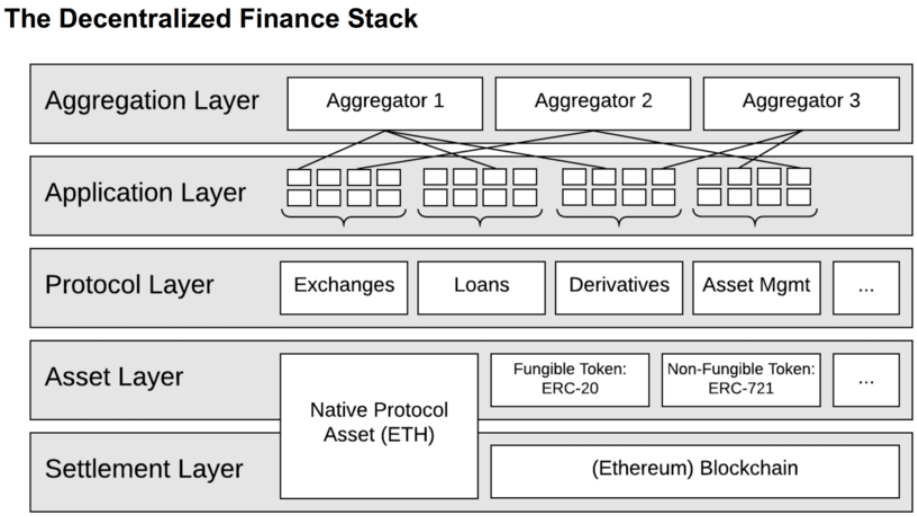



Fonte: The Block, acessado em 18 de junho de 2022.
https://www.theblockcrypto.com/

### 3.1.1 Camadas do DeFi

Segundo a Ethereum Foundation as aplicações de DeFi da rede Ethereum são projetadas em 5 camadas base: Camada de liquidação, camada de ativo, camada de protocolo, camada de aplicações a camada de agregadores.[24]

**Figura 18 -** As cinco camadas das Finanças Descentralizadas




Fonte: Loop Markets - xuanling11. https://www.loop.markets/defi-a-rainbow-5-layers-cake/ Acessado em 18/06/2022.

Segundo a publicação "*Fundamentals of DeFi*" da Applicature[25] (, a camada de liquidação é a base da própria blockchain. Sem essa base, não haveria um ambiente para que se possa criar aplicativos descentralizados. É uma base que funciona de modo bem diferente quando comparado às finanças centralizadas: as transações são confirmadas pelos mineradores e registradas de modo distribuído na blockchain. Essa funcionalidade exclusiva, no entanto, tem várias desvantagens em potencial relacionadas aos custos de transação e ao tempo necessário para realizar uma transação.

[24] Loop Markets. https://www.loop.markets/defi-a-rainbow-5-layers-cake/ Acessado em 18/06/2022.
[25]Applicature. Fundamentals of DeFi. https://applicature.com/blog/blockchain-technology/the-fundamentals-of-defi Acessado em 18/06/2022.

- **Camada de ativos:** É onde os tokens criptográficos utilizados nos aplicativos DeFi são geridos, incluindo ativos nativos do protocolo, como é o caso do ETH para o protocolo da Ethereum.
- **Camada de protocolo**: É responsável pelo funcionamento interno dos aplicativos descentralizados em si, assim como a gestão das atividades e tarefas específicas de cada aplicação. Geralmente compreende uma série de contratos inteligentes que gerenciam automaticamente o comportamento dos ativos utilizados no ambiente DeFi. Vale pontuar que, embora todos os contratos inteligentes sejam regidos por sua própria lógica e sempre funcionem com base nessa lógica, eles foram originalmente escritos por humanos, e é possível que seu código contenha bugs ou brechas que possam ser exploradas.
- **Camada de aplicação:** É uma interface de usuário que facilita a interação das pessoas com as plataformas DeFi. Sem essa camada, seria muito mais difícil para as pessoas interagirem com os DeFi. Ao contrário da camada de protocolo, usada por desenvolvedores, um aplicativo contém a interface para os usuários. Podemos fazer a comparação de que a camada de protocolo está para o back-end assim como a camada de aplicação, os Dapps, estão para o front-end.
- **Camada de agregação:** É uma extensão da camada de aplicação. Os agregadores reúnem vários aplicativos para que os usuários possam usar um único painel para executar vários tipos de transações no DeFi. Um agregador normalmente é composto por diversas funcionalidades de distintos aplicativos descentralizados, permitindo que as pessoas escolham quais aplicativos descentralizados desejam agregar para construir seu conjunto de produtos DeFi. O nível de agregação permite que o DeFi como um todo se torne mais do que a soma de suas partes individuais.

Quando um usuário deseja interagir na Web3 com um aplicativos descentralizados, ele pode começar plugando um agregador como a 1inch[26] ou a Metamask[27], que também tem a funcionalidade de carteira de ativos digitais. Esse

[26] 1inch. https://1inch.io/ Acessado em 18/06/2022.
[27] Metamask. https://metamask.io Acessado em 18/06/2022.

painel dá a ele acesso a algumas ou todas as plataformas DeFi que estão sendo usadas no momento.

### 3.1.2 Casos de Uso do DeFi

Como mencionado acima, os protocolos DeFi são representados por aplicativos descentralizados de fácil utilização que fornecem acesso a serviços financeiros permitindo que vários participantes do mercado estejam envolvidos ao mesmo tempo em condições *p2p*. A seguir vemos alguns dos principais tipos de aplicações dos protocolos DeFi, segundo publicação da 1inch[28], principal agregador de serviços DeFi.

#### 3.1.2.1 Empréstimo descentralizado

Os usuários podem emprestar um ativo criptográfico fornecendo outro como garantia, e os protocolos DeFi ajudam a tornar o processo de empréstimo transparente e fácil. Entre os maiores projetos de crédito do mercado DeFi estão Aave[29], Compound[30] e MakerDAO[31].

A Aave permite que os usuários emprestem e tomem emprestado ativos criptográficos sem interferência de terceiros. Um usuário pode tomar um empréstimo de outros usuários em vez de bancos. No entanto, o usuário ainda precisa colocar garantias em outros ativos criptográficos.

Normalmente os protocolos de empréstimo exigem garantias excessivas, e isso significa que, para obter um empréstimo criptográfico equivalente a 1.000 dólares na Aave, por exemplo, o usuário precisa colocar um valor maior em outra criptomoeda. Se o preço da última moeda cair e o valor da garantia não cobrir mais a quantia emprestada, o valor de garantia pode ser liquidado. O protocolo pode basicamente confiscar a garantia para cobrir o custo do seu empréstimo.

---

[28] Types of DeFi, their pros and cons. 1inch. https://blog.1inch.io/types-of-defi-their-pros-and-cons-c5ec2f18ff11 Acessado em 18/06/2022.
[29] Aave. https://aave.com Acessado em 18/06/2022.
[30] Compound https://compound.finance Acessado em 18/06/2022.
[31] MakerDAO. https://makerdao.com Acessado em 18/06/2022.

### 3.1.2.2 Derivativos

Os derivativos podem variar de tokens lastreados, quando se há uma garantia de valor que lastreia o token, a ativos de oráculos descentralizados, responsáveis por trazer informações do mundo real para dentro da blockchain. Como exemplo lastreável, temos a Synthetix[32], uma plataforma descentralizada que permite a construção de Synths, ativos baseados em moeda fiduciária, *commodities* e outros ativos criptográficos tokenizados na blockchain. Como exemplos de oráculos temos a Chainlink[33], uma rede que se destina a facilitar a transferência de dados invioláveis de fontes fora da cadeia para contratos inteligentes na blockchain. A aplicação pode ser usada para verificar se os parâmetros de um contrato inteligente são atendidos de maneira independente de qualquer uma das partes interessadas do contrato, conectando o contrato diretamente a dados, eventos, pagamentos e outras entradas do mundo real (NIKBAKHT et al., 2021)

### 3.1.2.3 Seguro

O Nexus Mutual[34], baseado em Ethereum, oferece a seus clientes a capacidade de agrupar e compartilhar riscos por meio de uma alternativa de seguro de propriedade da comunidade conhecida como mútuo discricionário. A plataforma destaca que se apresenta como uma alternativa às seguradoras e é administrada integralmente por seus membros que decidem quais sinistros são válidos. Todas as decisões dos membros são registradas e aplicadas por contratos inteligentes na blockchain Ethereum.

### 3.1.2.4 Soluções de pagamento

As plataformas DeFi tentam facilitar os pagamentos, oferecendo também aos usuários taxas mais baixas do que as que as instituições financeiras tradicionais cobram. A *Lightning Network*[35] é um produto com foco no blockchain do Bitcoin, que induz eficiência em transferências menores, tirando-as da blockchain. Na *Lightning*

[32] Synthetix. https://synthetix.io Acessado em 18/06/2022.
[33] Chainlink. https://chain.link Acessado em 18/06/2022.
[34] Nexus Mutual https://nexusmutual.io Acessado em 18/06/2022.
[35] Lighting Network *https://lightning.network* Acessado em 18/06/2022.

*Network*, dois ou mais participantes da rede que planejam fazer uma transferência podem abrir um canal depositando tokens bitcoin. Eles podem realizar quantas transferências quiserem sem exceder a soma total dos fundos carregados. Todas as transferências serão mantidas fora da blockchain e, quando o canal for fechado, o estado mais recente do ledger fora da cadeia será renovado na blockchain.

#### 3.1.2.5 Corretoras descentralizadas

Segundo Heimbach et al (2022), as corretoras descentralizadas (DEXs) ou *decentralized exchanges*, facilitam transações diretas *p2p* de maneira segura e sem a necessidade de um intermediário. A Uniswap é um exemplo de DEX que permite que qualquer pessoa crie um mercado ou um pool de liquidez fornecendo um valor igual de ETH e um token ERC-20. A taxa de corretagem é inicialmente definida pelo criador do mercado, mas muda à medida que a negociação ocorre e a liquidez de um ativo em comparação com o outro é reduzida.

### 3.1.3 Oportunidades no DeFi

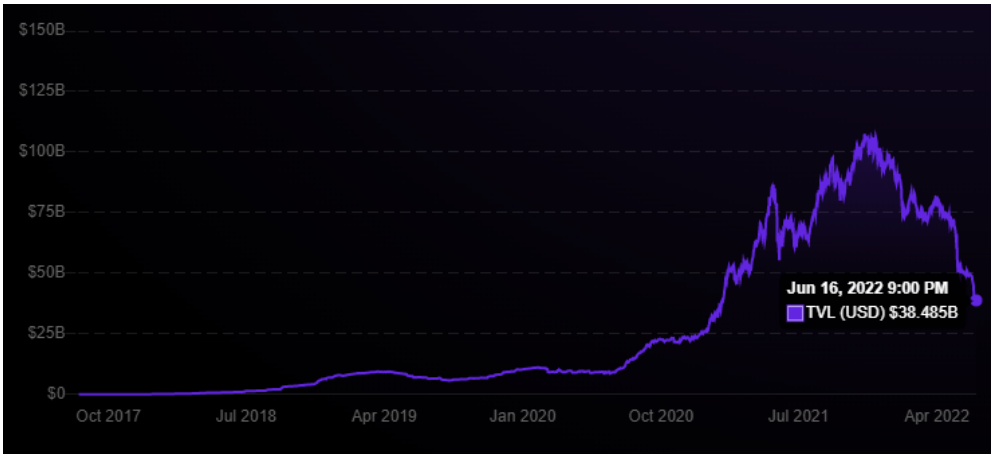
Segundo Schär (2021), o DeFi pode aumentar a eficiência, transparência e acessibilidade da infraestrutura financeira. Além disso, a capacidade de compossibilidade do sistema permite que qualquer pessoa combine vários aplicativos e protocolos, criando assim serviços novos e modularizados, como um lego. Tais fatores são comentados a seguir:

- **Eficiência**: Embora grande parte do sistema financeiro tradicional seja baseado em confiança e dependa de instituições centralizadas, o DeFi substitui alguns desses requisitos de confiança por contratos inteligentes. Se duas partes desejam trocar ativos digitais na forma de tokens, não há necessidade de garantias de um banco ou ente estatal. Em vez disso, as duas transações podem ser realizadas pelo próprio contrato, o que significa que ambas ou nenhuma das transferências serão executadas. Além disso, as transferências de tokens são muito mais rápidas do que qualquer uma das transferências no sistema financeiro tradicional. A velocidade de transferência e a taxa de

transferência de transações podem ser aumentadas ainda mais com soluções de 2ª camada, ou *layer* 2.

- **Transparência**: Os aplicativos DeFi são transparentes. Todas as transações em aplicativos DeFi são observáveis publicamente e o código do contrato inteligente pode ser auditado na blockchain. Os dados das transações estão disponíveis publicamente e podem potencialmente ser usados por pesquisadores e usuários. No caso de uma crise, a disponibilidade de dados históricos é um grande benefício em relação aos sistemas financeiros tradicionais, onde grande parte da informação está espalhada por muitos bancos de dados proprietários. Como tal, a transparência dos aplicativos DeFi pode permitir a mitigação de eventos indesejáveis antes que eles ocorram e ajudar a fornecer uma compreensão muito mais rápida de sua origem e possíveis consequências quando eles surgem.
- **Acessibilidade**: Por padrão, os protocolos DeFi podem ser usados por qualquer pessoa. Como tal, o DeFi pode potencialmente criar um sistema financeiro genuinamente aberto e acessível. Em particular, os requisitos de infraestrutura são relativamente baixos e o risco de discriminação é quase inexistente devido à falta de identidades. Se a regulamentação exigir restrições de acesso, por exemplo, para tokens de segurança, tais restrições podem ser implementadas nos contratos de token sem comprometer a integridade da camada de liquidação e as propriedades de descentralização.
- **Composabilidade:** Os protocolos DeFi são frequentemente comparados com peças de Lego. A camada de liquidação compartilhada permite a interconexão desses protocolos e aplicativos. Os protocolos de fundos *on-chain* podem fazer uso de protocolos de corretoras descentralizadas ou alcançar posições alavancadas por meio de protocolos de empréstimo. Quaisquer duas ou mais peças podem ser integradas, bifurcadas ou refeitas para criar algo totalmente novo. Qualquer coisa que tenha sido criada antes pode ser usada por um indivíduo ou por outros contratos inteligentes. Essa flexibilidade permite uma gama cada vez maior de possibilidades e um interesse sem precedentes na engenharia financeira aberta.

**Figura 19** - Valor total travado em protocolos DeFi, em dólares.




Fonte: Defi Pulse, acessado em 16 de junho de 2022. https://www.defipulse.com/

Segundo Amler *et al* (2021), existem 6 vantagens dos serviços DeFi em comparação com os sistemas financeiros tradicionais: (1) sem necessidade de permissão, (2) sem necessidade de confiança em terceiros, (3) transparência, (4) interconectividade, (5) governança descentralizada e (6) possibilita a auto soberania para seus usuários.

- **Sem necessidade de permissão:** serviços DeFi em blockchains públicas são projetados para serem abertos, significando que eles não especificam regras de acesso, onde qualquer pessoa com acesso à internet tem a capacidade de utilizar serviços financeiros tradicionais.
- **Sem necessidade de confiança em terceiros:** Os sistemas financeiros descentralizados são baseados na confiança nos algoritmos de consenso de uma blockchain, sua descentralização e no código imutável dos contratos inteligentes de cada *Dapp*, e não em pessoas ou instituições centralizadas. O consenso na rede garante que o sistema seja imutável, não possibilitando que as transações possam ser alteradas, adicionadas, excluídas ou censuradas.
- **Transparência:** A maioria das blockchains fornece transparência por padrão, pois todas as transações armazenadas são publicamente visíveis, como o caso da Etherscan para a rede da Ethereum. Sendo assim toda interação com os protocolos DeFi de redes públicas podem ser auditados, evitando censuras ou edições de informações de transações.

- **Interconectividade:** Ecossistemas de blockchain como Ethereum fornece ferramentas de programação poderosas que são usadas para serviços DeFi. Aplicações complexas, incluindo leilões, votação e negociação, podem ser construídas com contratos inteligentes[36]. Seus recursos permitem conectar, empilhar ou combinar facilmente aplicativos existentes sem esforços de programação adicionais. Combinar contratos para criar novos tipos de serviços é muitas vezes considerado como propriedade Lego dos protocolos DeFi.
- **Governança Descentralizada:** Não restrito ao espaço DeFi mas altamente prevalente nele é o aspecto de transformar contratos inteligentes em organizações autônomas descentralizadas *(DAOs)*[37]. Ao permitir que a comunidade sugira legislação e vote com base em sua participação no projeto, a governança é distribuída. Os três principais aspectos de governança, compatibilidade de incentivos, prestação de contas e transparência são realizados tornando os usuários e investidores responsáveis pelo bem-estar do ecossistema.
- **Possibilita a auto soberania:** Como nenhuma autoridade central controla e organiza o acesso ao ambiente financeiro descentralizado, os usuários são os responsáveis por gerenciar seus próprios dados pessoais e cuidar da segurança e custódia de seus fundos, sendo assim, os sistemas financeiros descentralizado garantem maior auto soberania.

### 3.1.4 Riscos do DeFi

Para o pesquisador Migan (2020), existem doze principais riscos dos protocolos DeFi na blockchain Ethereum: risco de escalabilidade, risco de vulnerabilidade de contrato inteligente, risco de oráculo, risco de design, risco de compossibilidade, risco de centralidade, risco de incentivo econômico, risco financeiro, risco de analfabetismo financeiro, risco regulatório, risco de finalidade, risco de divulgação e risco de mais riscos.

---

[36] Cointelegraph. https://cointelegraph.com.br/explained/smart-contracts-explained Acessado em 18/06/2022.
[37] Wikipedia. DAOs. *https://en.wikipedia.org/wiki/Decentralized_autonomous_organization* Acessado em 18/06/2022.

- **Risco de escalabilidade:** É o risco de que o Ethereum possa sofrer um congestionamento de rede causado pelo aumento de seu uso. O risco se origina do núcleo do Ethereum, pelo qual as taxas de transação são mais altas quanto maior a demanda para usar a blockchain. Quando há menos demanda e menos transações sendo feitas na Ethereum, o risco é menor. Quando há alta demanda e uso de mais transações sendo feitas na Ethereum, o risco é maior. O maior componente do risco de escalabilidade é o quão imprevisível é saber quando a rede blockchain Ethereum ficará congestionada de usuários enviando mais transações do que o normal. Soluções de segunda camada como a Polygon[38] e Optimism[39] são alternativas para resolver o problema de escalabilidade.
- **Risco de vulnerabilidade de contrato inteligente:** É o risco de um invasor encontrar uma maneira de drenar fundos de um contrato inteligente devido ao código ser escrito incorretamente ou de um invasor usar vetores de ataque conhecidos para explorar a funcionalidade de um contrato inteligente. Somente em abril de 2020, no ecossistema DeFi, houve 5 incidentes de segurança relacionados a vulnerabilidades de contratos inteligentes[40].
- **Risco de oráculo:** É o risco de um contrato inteligente receber informações desonestas sobre valores *off-chain* devido à manipulação de informações do provedor ou um oráculo não atualizar um contrato inteligente com informações *off-chain* tão rápido quanto um aplicativo espera, relacionado ao risco de escalabilidade. Os protocolos DeFi são extremamente dependentes de oráculos, que são terceiros que relatam informações de fontes do mundo real. Os oráculos são necessários porque as blockchains são sistemas de dados únicos e determinísticos, inerentemente incapazes de registrar ou considerar qualquer informação que não seja transações dentro da blockchain: um conceito referido como o problema do oráculo[41].

---

[38] Polygon. https://polygon.technology Acessado em 18/06/2022.
[39] Optimism. https://www.optimism.io Acessado em 18/06/2022.
[40]Consensys. https://consensys.net/blog/codefi/security-risks-in-ethereum-defi/ Acessado em 18/06/2022.
[41] Smith and Crown. https://smithandcrown.com/research/the-oracle-problem-and-mixicles/ Acessado em 18/06/2022.

- **Risco de design:** É o risco de que uma pequena falha de desenho de um protocolo leve ao não funcionamento dele conforme foi pretendido. Um protocolo DeFi pode ter muita segurança e ter altos níveis de mitigação de risco, mas se adicionar um novo contrato inteligente ou token ao seu protocolo que tenha níveis menores ou diferentes de segurança ou mitigação de risco sem um exame completo do que está adicionando, ele pode potencialmente levar à anulação de todo o protocolo.
- **Risco de compossibilidade:** É o risco de uma plataforma DeFi depender de outra plataforma DeFi operando corretamente para que sua própria plataforma funcione corretamente. O risco de compossibilidade está relacionado ao risco de design. Compossibilidade é um princípio de design de sistema que permite que aplicativos sejam criados a partir de partes componentes. A capacidade de composição é muitas vezes referida como legos de dinheiro no ecossistema DeFi, pois o código pode ser selecionado e montado em várias combinações[42].
- **Risco de centralidade:** É o risco de um ponto central de falha no DeFi poder ser a ruína de todo o ecossistema DeFi. Um tipo de risco de centralidade no DeFi está relacionado a contratos inteligentes atualizáveis, pois esse tipo de risco tem um administrador controlando as funções de uma plataforma. Se alguém pode controlar a funcionalidade de uma plataforma, os usuários do DeFi confiam no administrador para não alterar como eles acham que a plataforma funcionará quando investirem.
- **Risco de incentivo econômico:** É o risco que os incentivos econômicos que incentivam os participantes da rede a realizar determinadas ações podem falhar em incentivar o comportamento correto ou não ser suficientes, levando outros usuários a serem afetados negativamente[43].

---

[42] Consensys. https://consensys.net/blog/news/2019-was-the-year-of-defi-and-why-2020-will-be-too/ Acessado em 18/06/2022.

[43] Medium. Nexus Mutual. https://medium.com/nexus-mutual/understanding-risks-in-defi-eth-cc-presentation-4db9c7aedbb1 Acessado em 18/06/2022.

- **Risco de analfabetismo financeiro:** É o risco de que uma plataforma seja desenvolvida por alguém sem experiência financeira. DeFi é a transformação de produtos financeiros tradicionais em produtos que operam sem intermediário por meio de contratos inteligentes na blockchain da Ethereum. Os programadores que transformam produtos financeiros tradicionais em código em contratos inteligentes geralmente não têm nenhum histórico financeiro. Isso contrasta com as finanças tradicionais, onde os produtos financeiros tradicionais são negociados por instituições e criados por engenheiros financeiros com certificação.
- **Risco regulatório:** É o risco de que qualquer protocolo DeFi possa ser afetado pelo governo com leis que afetam o funcionamento de um protocolo DeFi ou leis que desativam efetivamente os protocolos DeFi.
- **Risco de finalidade:** É o risco de que a blockchain Ethereum seja bifurcada (*hard fork*), resultando na criação de duas cadeias diferentes, resultando em ativos DeFi disponíveis em duas ou mais cadeias, não em uma.
- **Risco de divulgação:** É o risco de um protocolo DeFi não divulgar uma lista completa de riscos que um usuário DeFi pode enfrentar ao usar a plataforma. Há sempre um risco para um usuário DeFi de que a plataforma escolhida pelo usuário não tenha divulgado adequadamente os resultados dos relatórios de auditoria de seus produtos. Não apenas isso, mas mesmo que uma plataforma DeFi tenha sido auditada, ela pode ter sido auditada antes de uma atualização de protocolo, onde novas vulnerabilidades poderiam ter sido introduzidas.

Isto posto, percebe-se que as aplicações de DeFi apresentam oportunidade e riscos inerentes ao desenvolvimento de uma nova tecnologia, porém com peculiaridades únicas de nossos tempos. Assim como a internet nos anos 2000 sofreu com sua superestimação, o mercado das finanças descentralizadas também enfrenta suas dores do crescimento. A seguir é apresentada um dos tipos de aplicações relacionadas às DeFi, o caso das DEXs.

## 3.2 CORRETORAS DESCENTRALIZADAS (DEXS)

DEXes representam uma tecnologia fundamental do DeFi. Elas permitem que os usuários troquem criptomoedas sem abrir mão da custódia de seus ativos. Os usuários interagem diretamente com os contratos inteligentes que constroem as DEXs. A negociação é habilitada pela liquidez reservada para cada par de criptomoedas negociáveis, reservadas em um respectivo contrato inteligente conhecido como pool de liquidez (HEIMBACH et al, 2022).

As DEXs como ecossistemas alternativos de pagamento com novos protocolos para transações financeiras surgiram no âmbito das finanças descentralizadas (SHAR, 2021). Ao contrário das *exchanges* de criptomoedas centralizadas (CEXs), como a Binance[44] e a Mercado Bitcoin[45], que usam livros de pedidos para combinar compradores e vendedores no mercado aberto e manter ativos criptográficos em uma carteira baseada em exchange, as DEXs não são custodiantes e tem sua funcionalidade baseado em contratos inteligentes auto-executáveis para negociação *p2p*, enquanto os usuários mantêm o controle de suas chaves privadas e fundos[46].

### 3.2.1 Agregadores de DEX

Mais recentemente, os agregadores DEX começaram a desempenhar um papel mais distinto no segmento DEX. Os agregadores DEX, como a 1inch formam hubs centrados no usuário que compõem vários aplicativos e protocolos, fornecendo também ferramentas para comparar e classificar serviços, permitindo que os usuários executem tarefas complexas conectando-se a vários protocolos simultaneamente.

DEXs e agregadores DEX são todos construídos na arquitetura ou componentes DeFi multicamadas, onde cada camada serve a um propósito bem definido (SHAR, 2021).

Embora compartilhem componentes comuns das quatro primeiras camadas, como camada de liquidação, camada de ativos, camada de protocolo e camada de aplicativo, os agregadores DEX têm um componente adicional ou camada de

---

[44] Binance: https://www.binance.com Acessado em 18/06/2022.
[45] Mercado Bitcoin. https://www.mercadobitcoin.com.br Acessado em 18/06/2022.
[46] Gemini. https://www.gemini.com/cryptopedia/decentralized-exchange-crypto-dex#section-exchanges-of-the-future Acessado em 18/06/2022.

agregador, que permite que eles se conectem e interajam com outros DEXs por meio de contratos inteligentes.

**Figura 20:** Agregador 1inch comparando taxas entre diferentes DEXs


Fonte: Blog 1inch, acessado em 18 de junho de 2022. https://blog.1inch.io/introducing-the-1inch-aggregation-protocol-v3-b02890986547

### 3.2.2 Piscinas de liquidez

Uma piscina de liquidez ou *liquidity pool* em DEXs da rede Ethereum é um local de negociação para um par de tokens ERC-20. Assim, quando um usuário deseja trocar o token x pelo token y, por exemplo, o usuário interage com a respectiva piscina de liquidez, depositando o token x na *pool* e recebendo o token y. Provedores de liquidez individuais fornecem a liquidez da *pool* depositando ambos os ativos no contrato inteligente. Por seu serviço, os provedores de liquidez recebem taxas de transação dos negócios suportados por sua liquidez.

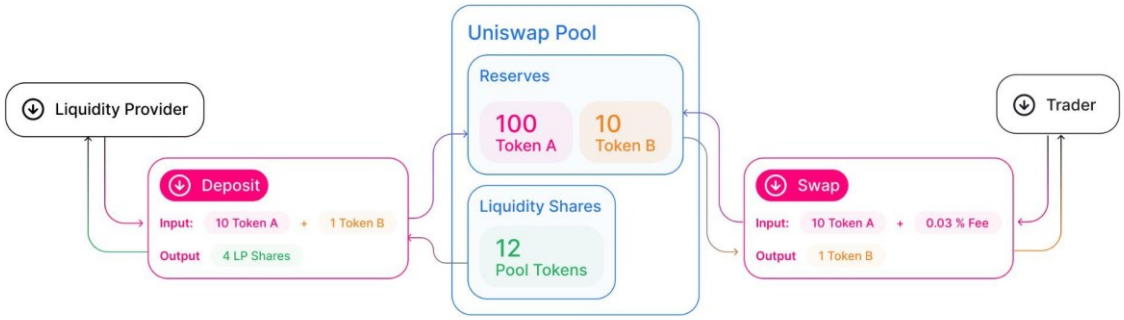
Segundo artigo de Antolin para a CoinDesk[47] uma *pool* de liquidez é uma pilha digital de criptomoedas bloqueadas em um contrato inteligente. Isso resulta na criação

[47] CoinDesk. https://www.coindesk.com/learn/what-are-liquidity-

de liquidez para transações mais rápidas. Um componente importante de um *pool* de liquidez são os criadores de mercado automatizados ou *Automated Market Makers (AMM)*. Um AMM é um protocolo que usa *pools* de liquidez para permitir que ativos digitais sejam negociados de maneira automatizada, e não por meio de um mercado tradicional de compradores e vendedores. Em outras palavras, os usuários de uma plataforma AMM fornecem *pools* de liquidez com tokens, e o preço dos tokens na *pool* é determinado por uma fórmula matemática do próprio AMM.

As *pools* de liquidez são projetadas para incentivar que usuários de diferentes blockchains provenham liquidez aos protocolos. Após um certo período, os provedores de liquidez, ou *Liquidity Providers (LPs)* são recompensados com uma fração de taxas e incentivos, equivalente à quantidade de liquidez que eles forneceram, chamados de tokens de provedor de liquidez. Tais tokens podem ser usados de diferentes maneiras em uma rede DeFi.

**Figura 21** - Exemplo de *pool* de liquidez na Uniswap




Fonte: Uniswap, acessado em 18 de junho de 2022.
https://docs.uniswap.org/protocol/V2/concepts/core-concepts/pools

### 3.2.3 Oportunidades e riscos nas DEXes

Ainda segundo Antolin (2022), existem prós e contras, oportunidade e ameaças referente ao uso de *pools* de liquidez em corretoras descentralizadas. Como pontos positivos podemos destacar:

pools/#:~:text=What%20is%20a%20liquidity%20pool,automated%20market%20makers%20(AMMs)
Acessado em 18/06/2022.

- Simplifica a negociação de DEX realizando transações a preços de mercado em tempo real;
- Permite que as pessoas forneçam liquidez e recebam recompensas, juros ou um rendimento percentual anual em suas criptomoedas;
- Utiliza contratos inteligentes visíveis publicamente para manter as informações de auditoria de segurança transparentes.

Por outro lado, alguns pontos de atenção mais relevantes são:

- O conjunto de fundos está sob o controle de um pequeno grupo, o que é contrário ao conceito de descentralização;
- Existe o risco de exploração de hackers devido a protocolos de segurança inadequados, causando perdas para os provedores de liquidez;
- Risco de fraudes, como puxões de tapete ou *rug pull*, na qual os desenvolvedores de determinado projeto fogem com os fundos dos investidores, o que leva a uma queda vertiginosa no preço da criptomoeda em questão;
- Exposição à perda impermanente. Isso acontece quando o preço dos ativos bloqueados em um *pool* de liquidez muda e cria uma perda não realizada, versus o valor dos ativos parados em uma carteira.

Erros de codificação e hacks são comuns no DEXs. As transações em blockchains são irreversíveis, o que significa que uma transação incorreta ou fraudulenta não pode ser corrigida facilmente. Além disso, o código para os contratos inteligentes geralmente é um software de código aberto que pode ser copiado para configurar plataformas concorrentes, o que cria instabilidades à medida que os fundos mudam de plataforma para plataforma[48].

Também existe a possibilidade da pessoa ou entidade por trás de um protocolo desaparecer com o dinheiro dos investidores, caracterizados como esquemas Ponzi. Em 2021, metade do crime de criptomoeda estava relacionado a DEXs[49]. Esse aumento foi atribuído a uma combinação de incompetência do desenvolvedor e regulamentos inexistentes ou mal aplicados. O roubo do DeFi pode vir de hackers

---

[48] Bloomberg. https://www.bloomberg.com/news/articles/2020-09-11/-come-to-jesus-moment-for-crypto-finance-apps-rocks-valuations#xj4y7vzkg Acessado em 18/06/2022.

[49] Insurance Journal. https://www.insurancejournal.com/news/national/2021/05/14/613928.htm Acessado em 18/06/2022.

externos roubando projetos vulneráveis, onde os desenvolvedores e influenciadores promovem um projeto e depois pegam o dinheiro[50].

### 3.2.4 Caso Uniswap

Fornecer liquidez nos mercados financeiros tradicionais é geralmente uma forma de investimento reservada a traders e instituições profissionais. A natureza descentralizada da blockchain, por outro lado, permite que muitos provedores de liquidez individuais se unam para facilitar trocas de criptomoedas em blockchain enquanto ganham taxas, como é o caso da Uniswap[51]. Trabalhos anteriores mostraram que fornecer liquidez em DEXs pode ser um investimento lucrativo, acessível a comerciantes de varejo e requer apenas algumas considerações simples de seu lado (ANTOLIN, 2022).

Baseado na segmentação entre as 5 camadas das finanças descentralizadas, podemos considerar as seguintes características para a Uniswap:

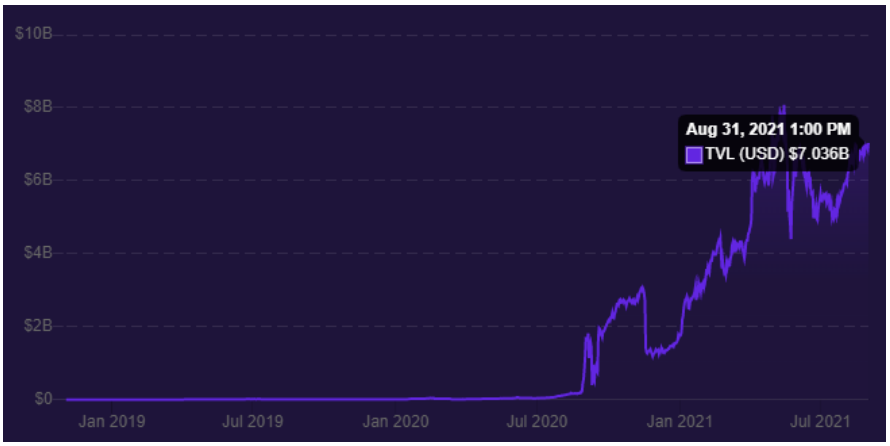
- **Camada de liquidação:** Blockchain da Ethereum;
- **Camada de ativos:** tokens ERC-20 e token Uniswap;
- **Camada de protocolo:** Corretora descentralizada (DEX);
- **Camada de aplicação:** Provedores de liquidez (LPs), formador de mercado automatizado (AMM);
- **Camada de agregação:** Uniswap v3 com recurso de liquidez distribuída.

Uniswap é atualmente a maior DEX na Ethereum em termos de volume de ativos travados no protocolo. Os provedores de liquidez neste protocolo são os usuários que depositam token em *pools* de liquidez para ganhar taxas, enquanto que os formadores de mercado automatizado são os criadores das *pools*. Existem duas versões do Uniswap usadas ativamente: V2 e V3. Enquanto o Uniswap V2 implementa um Formador de Mercado de Produto Constante ou *Constant Product Market Maker (CPMM)*, onde a liquidez fornecida por qualquer provedor de liquidez suporta negociação em toda a faixa de preço, o Uniswap V3 utiliza um novo design CPMM destinado a otimizar a eficiência do capital.

---

[50] Techrepublic. https://www.techrepublic.com/article/dont-get-rugged-defi-scams-go-from-zero-to-129-million-in-a-year-to-become-top-financial-hack/ Acessado em 18/06/2022.
[51] Uniswap. https://uniswap.org Acessado em 18/06/2022.

**Figura 22** - Valor total travado na Uniswap, em dólares.




Fonte: Defi Pulse, acessado em 18 de junho de 2022.

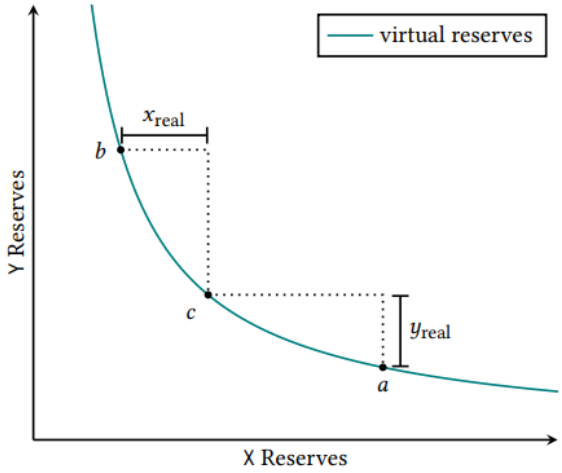
Diferente da maioria das *pools* de liquidez, na Uniswap v3 a liquidez é limitada a uma faixa de preço especificada pelo usuário. Já na Uniswap v2, e na maioria das DEXs da rede Ethereum, a liquidez é distribuída uniformemente ao longo da curva de reservas:

$$x * y = k$$

Neste caso, $x$ e $y$ são as respectivas reservas de dois ativos X e Y e $k$ é uma constante[52]. Em outras palavras, as versões anteriores foram projetadas para fornecer liquidez em toda a faixa de preço (0, ∞). Já na v3, uma posição só precisa manter reservas suficientes para suportar a negociação dentro de sua faixa, denominada pela Uniswap como uma reserva virtual.

[52] Uniswap Whitepaper. https://uniswap.org/whitepaper.pdf

**Figura 23** - Simulação de reservas virtuais em *pools* de liquidez da Uniswap V3.



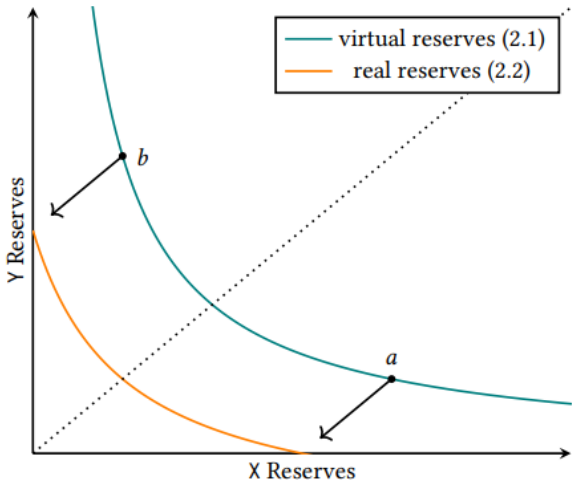

Fonte: Whitepaper Uniswap v3 https://startcy.io/whitepaper-v3.pdf

Especificamente, uma posição só precisa manter o ativo X suficiente para cobrir o movimento de preço até seu limite superior, porque o movimento de preço ascendente corresponde ao esgotamento das reservas X. Da mesma forma, ele só precisa manter o ativo Y suficiente para cobrir o movimento de preços até seu limite inferior. A figura anterior mostra essa relação para uma posição em um intervalo [$pa$, $pb$] e um preço atual $pc \in [pa, pb]$. $x$ real e $y$ real denotam as reservas reais da posição. Quando o preço sai do intervalo de uma posição, a liquidez da posição não está mais ativa e não gera mais taxas. Nesse ponto, sua liquidez é composta inteiramente por um único ativo, pois as reservas do outro ativo devem estar totalmente esgotadas. Se o preço entrar novamente no intervalo, a liquidez se tornará ativa novamente. A quantidade de liquidez fornecida pode ser medida pelo valor $L$, que é igual a $\sqrt{k}$. As reservas reais de uma posição são descritas pela curva:

$$(x + \frac{L}{\sqrt{p_b}})(y + L\sqrt{p_a}) = L^2$$

Esta curva é uma tradução da fórmula $x * y = k$ tal que a posição é solvente exatamente dentro de sua faixa.

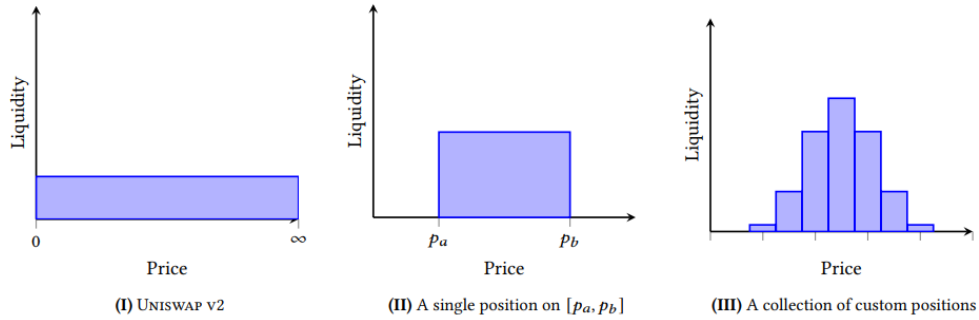
**Figura 24** - Simulação de reservas reais na Uniswap V3.




Fonte: Whitepaper Uniswap v3 https://startcy.io/whitepaper-v3.pdf

Os provedores de liquidez são livres para criar quantas posições acharem adequadas, cada uma em sua própria faixa de preço. Desta forma, as piscinas de liquidez podem aproximar qualquer distribuição desejada de liquidez no espaço de preços, conforme demonstrado na figura a seguir.

**Figura 25** - Exemplos de liquidez distribuída na Uniswap V3.




Fonte: Whitepaper Uniswap v3 https://startcy.io/whitepaper-v3.pdf

Fica claro que obter altos retornos como provedor de liquidez no Uniswap V3 é uma tarefa altamente complicada que exige uma gestão ativa e um conhecimento profundo no funcionamento do protocolo. A introdução do Uniswap V3 transformou o fornecimento de liquidez em um campo de jogo para investidores sofisticados, onde os comerciantes de varejo devem ser cautelosos para evitar o risco de perdas significativas.

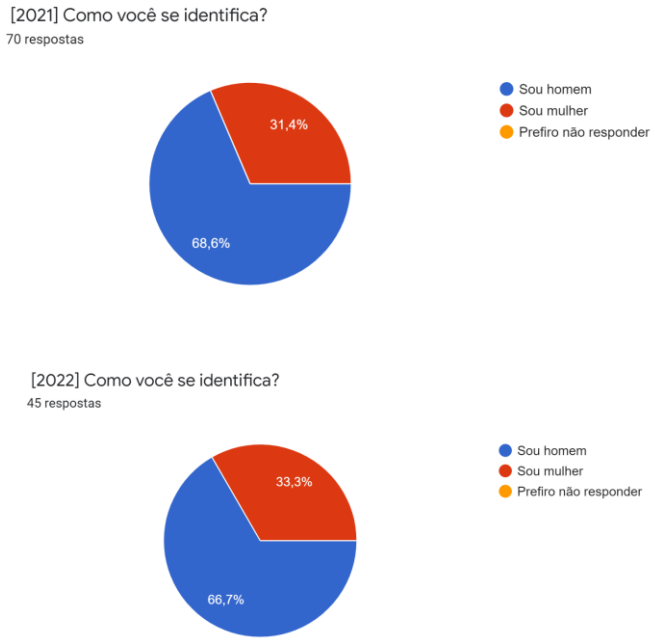
## 4. PESQUISA ACADÊMICA

Durante o primeiro semestre de 2021 foi realizada uma pesquisa através da plataforma Forms do Google com estudantes de Análise e Desenvolvimento de Sistemas da Fatec Taubaté para identificar o nível de conhecimento dos alunos com os temas abordados no presente trabalho. O questionário desenvolvido pode ser encontrado no anexo deste estudo.

Um ano depois, no primeiro semestre de 2022 a pesquisa foi novamente realizada com o mesmo público para verificar se houve alguma grande alteração nos resultados. O objetivo desta segunda rodada de pesquisa foi avaliar se durante o último ano houve aumento sobre o entendimento da tecnologia por trás desta inovação, o que validaria a tese de que a adoção ao mercado de criptomoedas vem aumentando localmente entre os estudantes de Análise e Desenvolvimento de Sistemas da Fatec, na cidade de Taubaté.

A pesquisa de 2021 registrou 70 respondentes, enquanto que a de 2022 registrou 45 respondentes. A seguir apresentamos os resultados obtidos nas pesquisas:

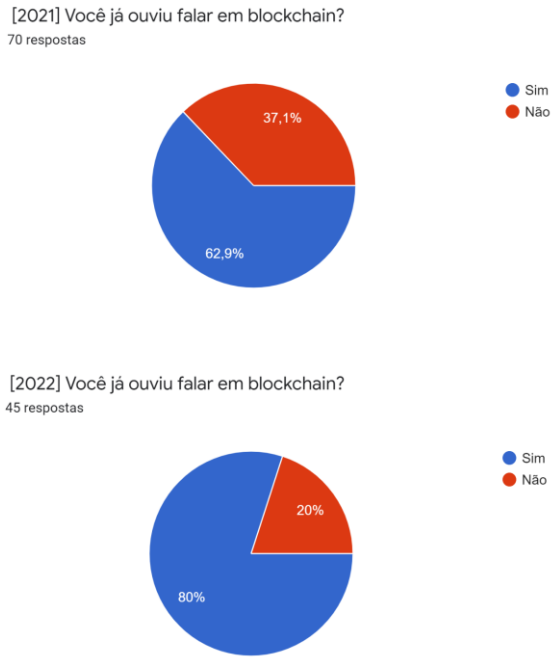
**Figura 26** - Comparativo do resultado das pesquisas de 2021 e 2022 quanto ao gênero que o público se identifica.




Fonte: Desenvolvido pelo autor.

Quando perguntados sobre como o respondente se identifica em termos de gênero, percebemos um aumento percentual de 1,9% do público feminino na comparação com a pesquisa realizada em 2022.

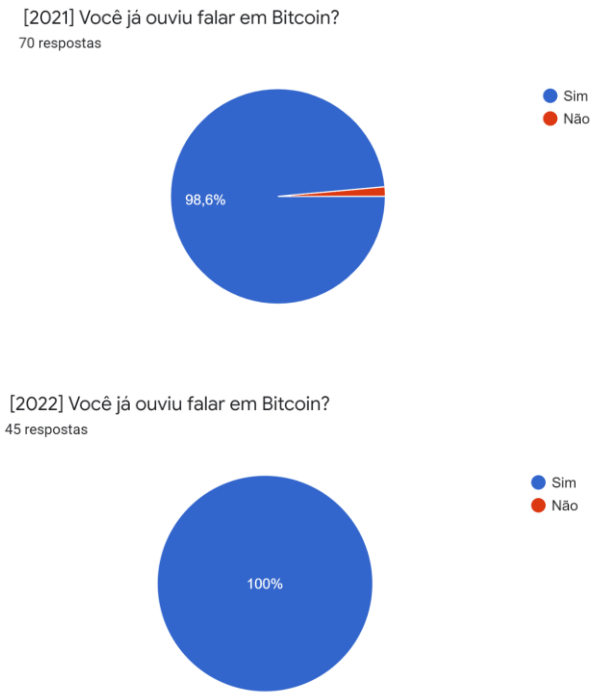
**Figura 27 -** Comparativo do resultado das pesquisas de 2021 e 2022 quanto ao conhecimento sobre blockchain.




Fonte: Desenvolvido pelo autor.

Ao perguntar sobre se os respondentes já haviam ouvido falar em blockchain, a segunda pesquisa registrou um resultado positivo quando comparado à primeira, registrando um aumento de 17,1 pontos percentuais, totalizando 80% dos respondentes.

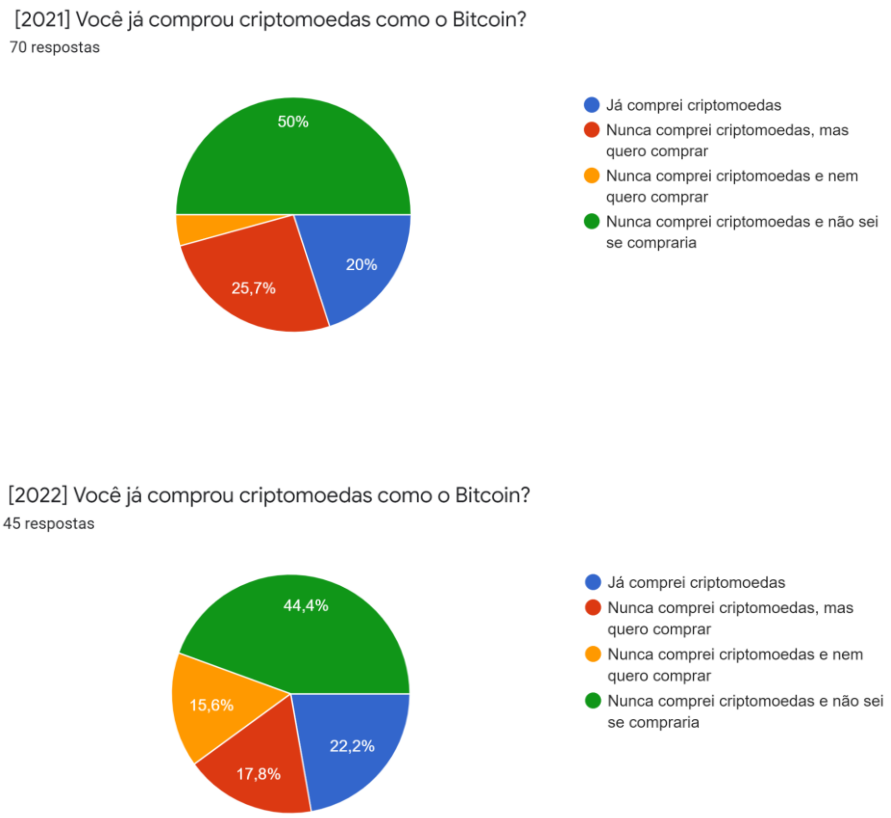
**Figura 28 -** Comparativo do resultado das pesquisas de 2021 e 2022 quanto ao conhecimento sobre Bitcoin.




Fonte: Desenvolvido pelo autor.

Quando questionados sobre se já ouviram falar sobre Bitcoin, a principal e primeira criptomoeda do mercado, em 2022 a totalidade dos respondentes sinalizou que sim, enquanto que na primeira pesquisa apenas 1 pessoa sinalizou que não ouviu falar.

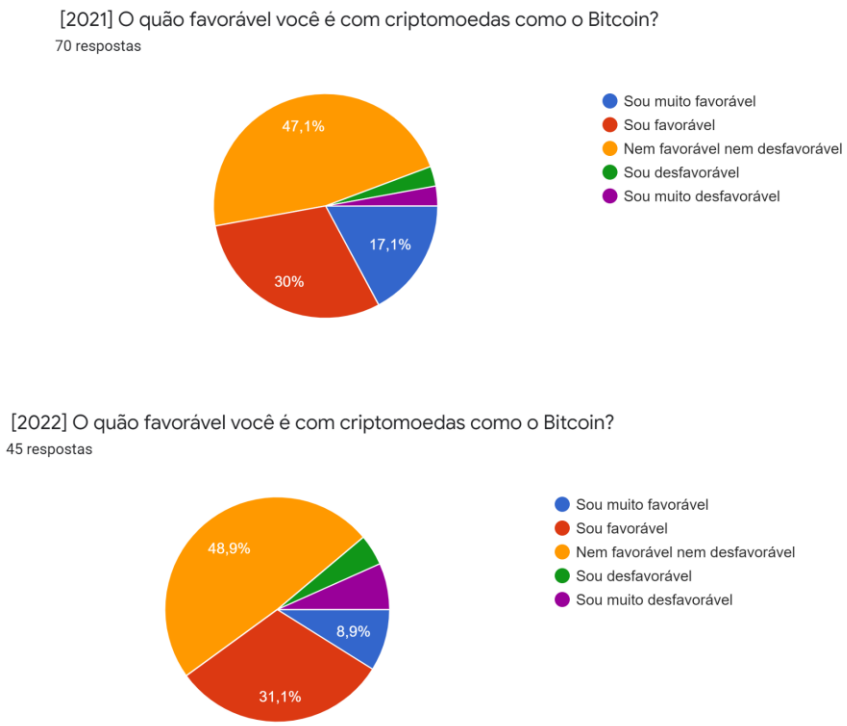
**Figura 29 -** Comparativo do resultado das pesquisas de 2021 e 2022 quanto à compra de criptomoedas como o Bitcoin.




Fonte: Desenvolvido pelo autor.

Ao serem perguntados se já compraram criptomoedas como o bitcoin, em 2022 os que já compraram tiveram um ganho percentual de 2,2% quando comparado com a pesquisa de 2021, totalizando 22,2% dos entrevistados. O número de respondentes que sinalizaram que “nunca comprei criptomoedas, mas quero comprar”, reduziu de 25,7% para 17,8% dos respondentes. Isto pode ser justificado pelo preço atual de um bitcoin que caiu cerca de 70% entre as duas pesquisas Convergente ao último resultado, 4,3% dos respondentes da primeira pesquisa sinalizaram que “nunca comprei criptomoedas e nem quero comprar”, enquanto que na segunda pesquisa o resultado foi de 15,6%. Por fim, metade dos respondentes da primeira pesquisa sinalizaram que “nunca comprei criptomoedas e não sei se compraria”, enquanto que na segunda pesquisa o resultado foi de 44,4%, sinalizando um decréscimo quanto à dúvida de comprar ou não criptomoedas.

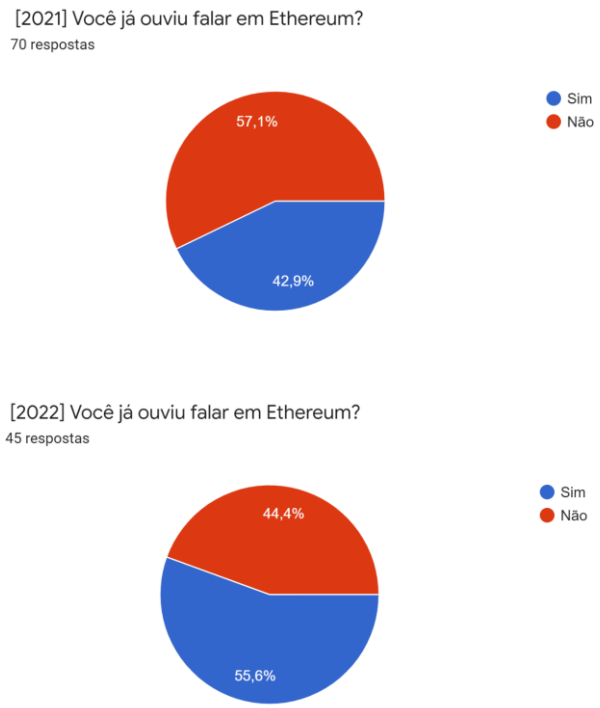
**Figura 30 -** Comparativo do resultado das pesquisas de 2021 e 2022 quanto ao nível de favorabilidade com criptomoedas.




Fonte: Desenvolvido pelo autor.

Avaliando o nível de favorabilidade dos entrevistados com criptomoedas como o Bitcoin, os “muito favoráveis” caíram de 17,1% para 8,9%, enquanto os “muito desfavoráveis” cresceram de 2,9% para 6,7%. Os “favoráveis” aumentaram de 30% para 31,1%, enquanto os “desfavoráveis” também aumentaram de 2,9% para 4,4%. A maioria dos respondentes não é favorável nem desfavorável, representando 47,1% na pesquisa de 2021 contra 48,9% na pesquisa de 2022.

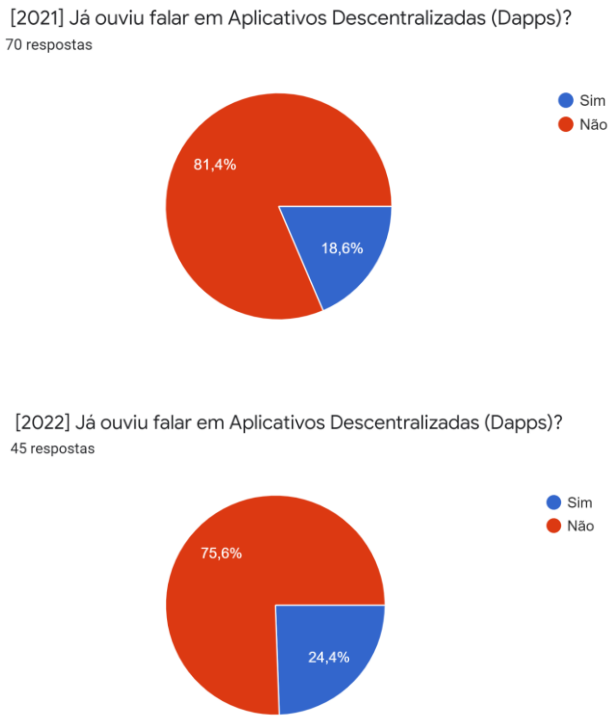
**Figura 31 -** Comparativo do resultado das pesquisas de 2021 e 2022 quanto ao conhecimento sobre Ethereum.




Fonte: Desenvolvido pelo autor.

Quando perguntados se já haviam ouvido falar sobre Ethereum, a pesquisa de 2022 teve um acréscimo de 12,7% quando comparado com a pesquisa de 2021, totalizando 55,8% do público. Esse resultado demonstra que o segundo maior ativo do mercado de criptomoedas vem sendo cada vez mais conhecido para o público estudado.

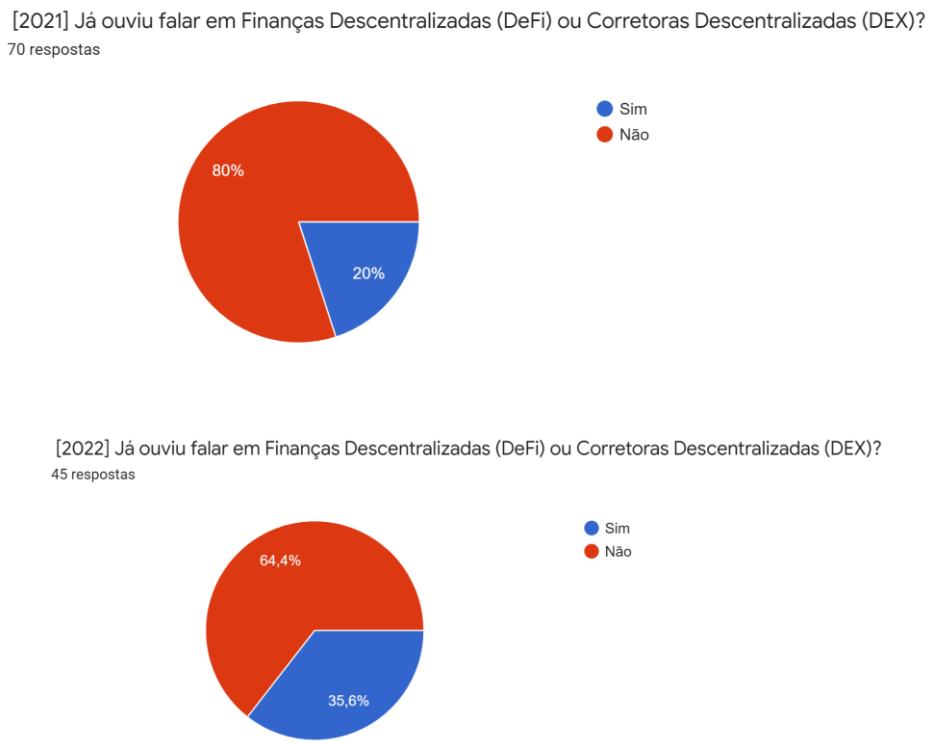
**Figura 32 -** Comparativo do resultado das pesquisas de 2021 e 2022 quanto ao conhecimento sobre *Dapps*.




Fonte: Desenvolvido pelo autor.

Na primeira pesquisa, apenas 18,6% dos respondentes já haviam ouvido falar em aplicativos descentralizados, enquanto em 2022 o resultado representou 24,4% do público, praticamente um quarto dos entrevistados.

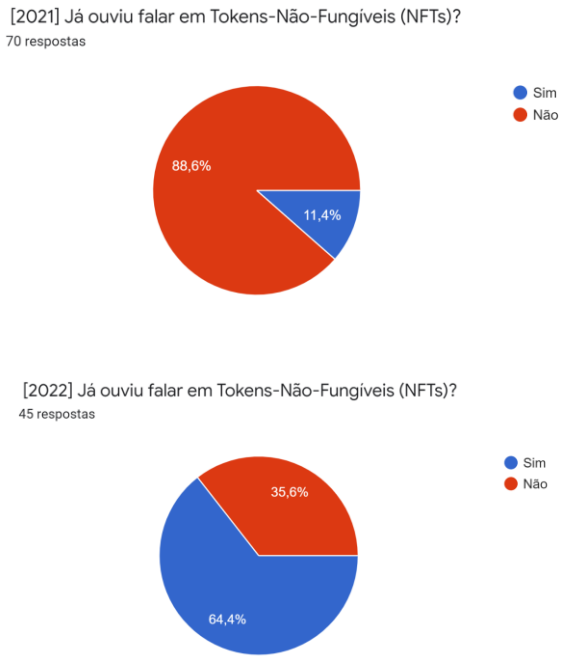
**Figura 33 -** Comparativo do resultado das pesquisas de 2021 e 2022 quanto ao conhecimento sobre DeFi e DEX.




Fonte: Desenvolvido pelo autor.

Assim como na questão referente ao conhecimento sobre aplicativos descentralizados, a pergunta referente ao conhecimento de DeFi e DEX também teve um incremento quando comparados os resultados das pesquisas. O incremento de pessoas que já ouviram falar de DeFi e DEX aumentou de 20% para 35,6% quando comparadas às pesquisas de 2021 e 2022.

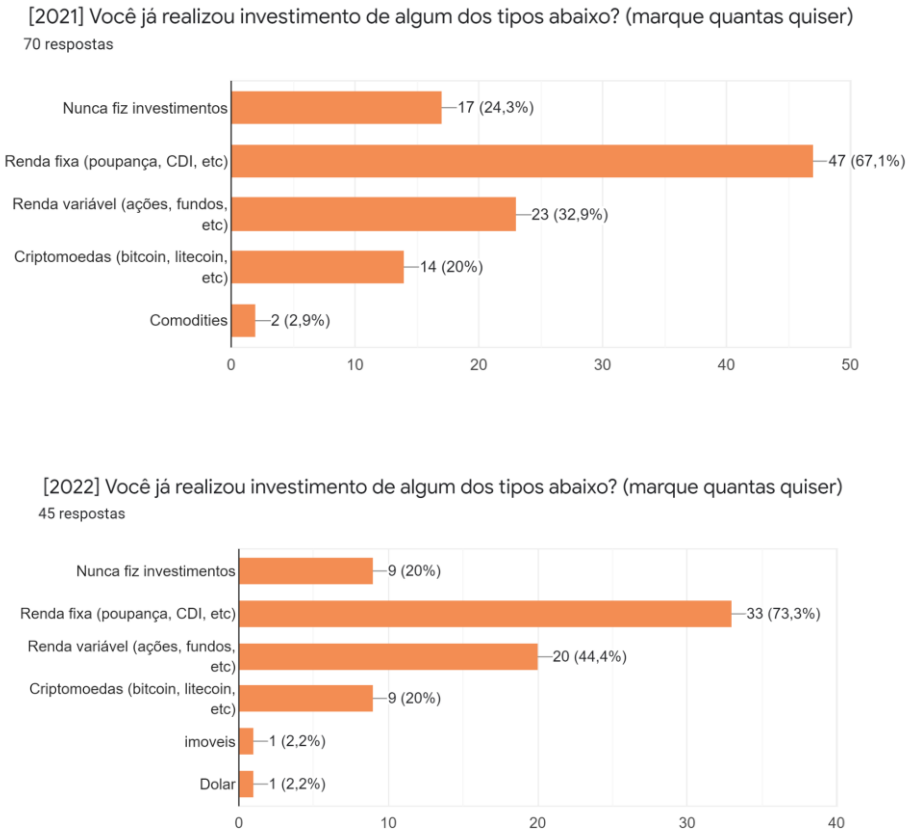
**Figura 34 -** Comparativo do resultado das pesquisas de 2021 e 2022 quanto ao conhecimento sobre NFTs.




Fonte: Desenvolvido pelo autor.

O mesmo incremento pode ser visto na questão relacionada à NFTs, que teve um aumento superior às demais tecnologias perguntadas no questionário. A maior variação entre as pesquisas foi verificada na pergunta sobre se os respondentes já haviam ouvido falar em NFTs, saltando de 11,4% para 64,4%, representando um incremento de 53%.

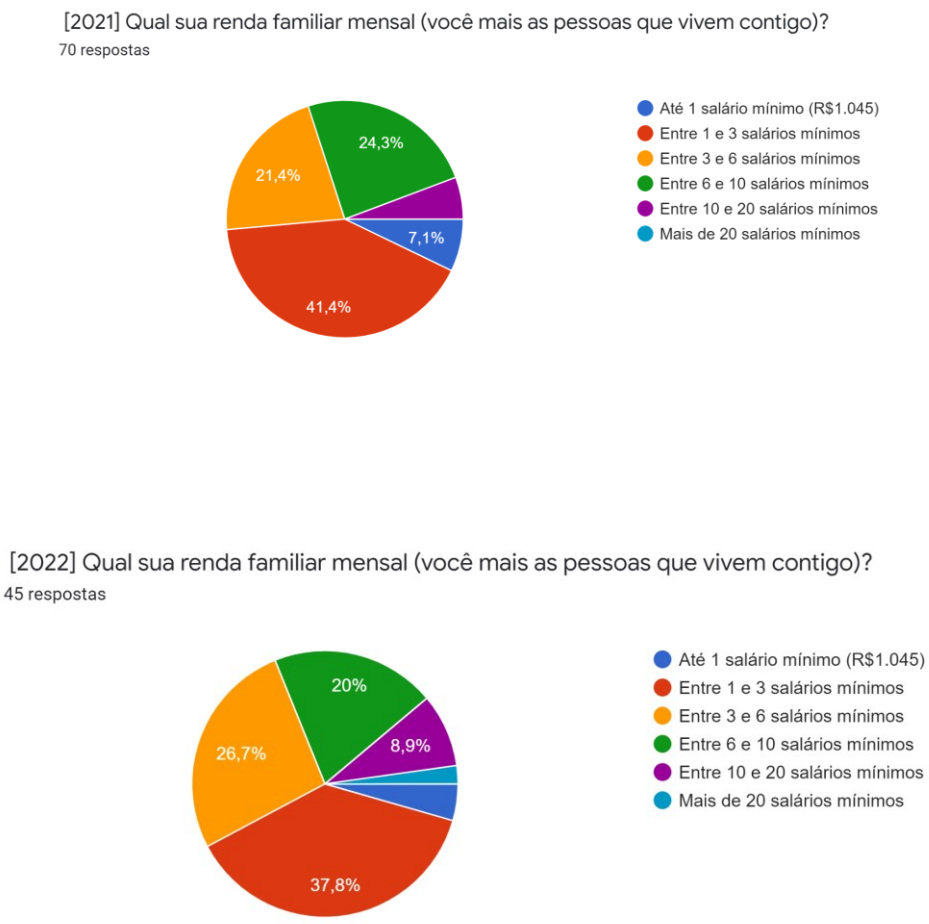
**Figura 35 -** Comparativo do resultado das pesquisas de 2021 e 2022 quanto à realização de investimentos.




Fonte: Desenvolvido pelo autor.

Quando perguntados se já realizou investimento de algum tipo, a maioria já investiu em renda fixa, representando 67,1% na primeira pesquisa e 73,3% na segunda pesquisa. Um oitavo dos respondentes já investiu em criptomoedas, segundo ambas as pesquisas.

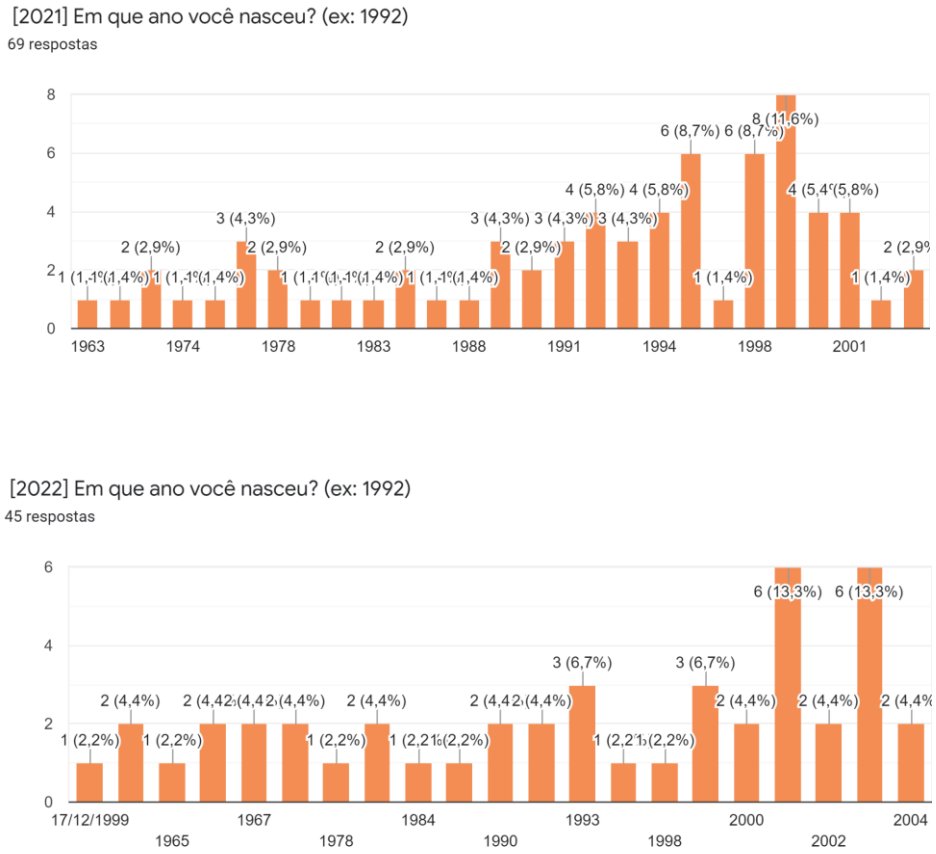
**Figura 36 -** Comparativo do resultado das pesquisas de 2021 e 2022 quanto à renda familiar mensal dos entrevistados.




Fonte: Desenvolvido pelo autor.

Quando questionados sobre a renda familiar mensal, os entrevistados em uma maioria recebem até 3 salários mínimos (R$3.636), e aqueles com renda familiar mensal superior a 6 salários mínimos (R$7.272) representam aproximadamente 25% dos entrevistados. Os entrevistados com renda familiar mensal acima de 10 salários mínimos (R$12.120) representam 5,8% dos respondentes da primeira pesquisa, enquanto que na pesquisa de 2022 representaram aproximadamente 12% dos entrevistados.

**Figura 37 -** Comparativo do resultado das pesquisas de 2021 e 2022 quanto ao ano de nascimento dos entrevistados.




Fonte: Desenvolvido pelo autor.

Em seguida, quando questionados sobre o ano de nascimento, vemos que na primeira pesquisa a maioria do público nasceu entre 1995 e 1997, enquanto que na segunda pesquisa prevaleceram os resultados do público com nascimento entre 2001 e 2003.

Por fim, fica claro que as mudanças de resultados entre a pesquisa realizada em 2021 e 2022 foram sutis mas perceptíveis. Os entrevistados apresentaram muitos conhecimento sobre as temáticas apresentadas no presente estudo, validando a tese, já comprovada através de dados neste estudo, de que a adoção ao mercado de criptomoedas vem avançando a grandes passos.

## 5. Conclusão

A tecnologia blockchain possibilita a resolução de diferentes problemas através da descentralização da rede *p2p* e da maneira como a informação é armazenada e distribuída, possibilitando sua auditoria de modo transparente. Diversas aplicações podem ser construídas em sua infraestrutura, possibilitando novas formas de troca de ativos reais, em forma de tokenização ou digitalmente, como é o caso das criptomoedas.

Blockchains como da Ethereum possibilitam que contratos inteligentes sejam desenvolvidos e executados de forma automatizada, dando acesso aos usuários à distintos serviços financeiros, tradicionalmente inacessíveis para o investidor do varejo. Através das finanças descentralizadas é possível desenvolver soluções como as corretoras descentralizadas, que além de funcionarem como uma *marketplace* para troca de tokens entre os usuários, também possibilita a participação em *pools* de liquidez, ganhando taxas e ajudando na descentralização do protocolo.

Desde 2017, o DeFi experimentou um aumento parabólico na sua relevância acadêmica e no seu valor apreciado, sendo usado principalmente em DEXs da blockchain da Ethereum. Não houve apenas um aumento exponencial no valor usado nos protocolos, fruto da possibilidade de renda passiva através da participação no protocolo, mas também os tokens DeFi deram acesso à governança e participação nas decisões do futuro dos Dapps. As aplicações no DeFi são basicamente as versões descentralizadas de instituições financeiras tradicionais existentes, como casas de câmbio, empréstimos, companhias de seguros, mercados de previsão e gerenciamento de ativos, entre outras.

Através de protocolos como a Uniswap, usuários tem acesso à distintos serviços financeiros tradicionais, além de possibilitar a geração de renda passiva através dos algoritmos do protocolo. Tal inovação traz consigo diversas oportunidades e pontos positivos, mas por outro lado também apresenta riscos e pontos de atenção. Do ponto de vista positivo, temos principalmente o aumento da eficiência, transparência e acessibilidade da infraestrutura financeira. Ademais, podemos citar algumas vantagens destes serviços, em comparação com sistemas tradicionais: sem necessidade de permissão, sem necessidade de confiança em terceiros, transparência, interconectividade, governança descentralizada e (possibilita a auto soberania.

Além disso, a capacidade de composabilidade do DeFi permite que qualquer pessoa combine vários aplicativos e protocolos, criando assim serviços novos e modularizados, como um lego.

Porém, do outro lado da moeda, os protocolos têm suas vulnerabilidades e podem colocar o usuário em risco, como por exemplo: risco de escalabilidade, de vulnerabilidade de contrato inteligente, de oráculo, de design, de compossibilidade, de centralidade, de incentivo econômico, financeiro, de analfabetismo financeiro, regulatório, de finalidade, de divulgação e risco de mais riscos, segundo estudo desenvolvido. Além deste, existem outros riscos, como a exploração de hackers devido a protocolos de segurança inadequados, risco de fraudes, como *rug pull*, e risco de perda impermanente de liquidez.

Provedores de liquidez de protocolos de DEXs na rede Ethereum, como é o caso da Uniswap, tem a possibilidade de arbitrar como formadores de mercado em diferentes pools de liquidez. Diferente da maioria dos protocolos DeFi, a Uniswap V3 permite que o usuário configure sua faixa de negociação dentro de uma *pool*, conceito denominado liquidez distribuída. Diferente da maioria das *pools* de liquidez, na Uniswap v3 a liquidez é limitada a uma faixa de preço especificada pelo usuário, diferente da maioria das DEXs da rede Ethereum, onde a liquidez é distribuída uniformemente ao longo de toda a curva de reservas, e não em uma zona específica.

Através da pesquisa desenvolvida pelo autor, aplicada duas vezes entre os anos de 2021 e 2022 com alunos da Fatec Taubaté, foi possível identificar que os temas relacionados ao presente estudo vem sendo cada vez mais compreendidos por parte do público. Isso demonstra um aumento na adoção de ativos digitais descentralizados, visto que na segunda pesquisa praticamente todos os temas tiveram respostas positivas quando comparados com a pesquisa de 2021, como: Dapps, DeFi, DEXs, e com um crescimento acima da média, NFT e Ethereum.

Finalmente, é possível concluir que o presente estudo cumpriu seu objetivo de conceitualizar as finanças descentralizadas e corretoras descentralizadas, trazendo suas oportunidade e riscos do ponto de vista tecnológico. Ademais, fica claro que a complexidade do tema, em especial na interação com *pools* de liquidez em corretoras descentralizadas na rede da Ethereum, como o caso Uniswap, acaba sendo de difícil usabilidade para a maioria dos usuários de internet. De certo com o passar dos anos será possível evidenciar com mais dados o nível de adoção da tecnologia blockchain, e suas implicações na economia e sociedade em termos de serviços financeiros

digitalizados. Para futuras pesquisas, sugere-se o aprofundamento no tema, abordando as etapas e processos relacionados ao front-end de aplicativos de finanças descentralizadas, de modo a ajudar futuros usuários em sua usabilidade.

## REFERÊNCIAS

1INCH. Disponível em: https://1inch.io/ Acessado em 18/06/2022.

1INCH. **Introducing the 1inch aggregation protocol v3.** 2022. Disponível em: https://blog.1inch.io/introducing-the-1inch-aggregation-protocol-v3-b02890986547 Acessado em 18 de junho de 2022.

1INCH. **Types of DeFi, their pros and cons**. Disponível em: https://blog.1inch.io/types-of-defi-their-pros-and-cons-c5ec2f18ff11 Acessado em 18/06/2022.

AAVE. Disponível em: https://aave.com Acessado em 18/06/2022.

ALLEMANN, Andrew. **Kred launches as dual DNS and ENS domain**. Domain Name Wire, 2020.

ALLISON, Ian. **If Banks Want Benefits of Blockchains, They Must Go Permissionless**. International Business Times, 2015.

AMLER et al. **DeFi-ning DeFi: Challenges & Pathway.** 2021. Disponível em: https://arxiv.org/pdf/2101.05589.pdf Acessado em 18/06/2022.

AMMOUS, S. **Economics beyond financial intermediation: Digitalcurrencies' potential for growth, poverty alleviation and international development.** Disponível em: https://ssrn.com/abstract=2832738. Acessado em 18/06/2022.

ANTONOPOULOS, Andreas. **Bitcoin security model: trust by computation**. Radar O'Reilly, 2014.

APPLICATURE. **Fundamentals of DeFi**. Disponível em: https://applicature.com/blog/blockchain-technology/the-fundamentals-of-defi Acessado em 18/06/2022.

ARMSTRONG, Stephen. **Move over Bitcoin, the blockchain is only just getting started**. Wired, 2016.

ARNOLD, Martin. **IBM in blockchain project with China UnionPay**. Financial Times, 2013.

BALAGURUSAMY, V. S. K. et al. **Crypto anchors**. IBM Journal of Research and Development, 2019.

BANDOIM, Lana. **Can Blockchain And Chip Technology Improve Beef Sourcing Transparency?** Forbes, 2019.

BAR, Julian. **Blockchain & cryptocurrencies is this the future of money and data?** Disponível em: https://theblockchaintest.com/uploads/resources/Julius%20Bar%20-%20Blockchain%20&%20cryptocurrencies-is%20this%20the%20future%20of%20money%20and%20data%20-%202021%20-%20may.pdf Acessado em 18/06/2022.

BELCHIOR, Rafael et al. **A Survey on Blockchain Interoperability: Past, Present, and Future Trends**. Cornell University, 2020.

BEYERS, Julia. **Blockchain Domains: What Are They and How Are They Implemented?** Hacker Noon, 2020.

BHASKAR, Nirupama Devi; CHUEN, David Lee Kuo. **Bitcoin Mining Technology**. Handbook of Digital Currency, 2015.

BINANCE ACADEMY. **What is a blockchain consensus algorithm.** Disponível em: https://academy.binance.com/pt/articles/what-is-a-blockchain-consensus-algorithm Acessado em 18/06/2022

BINANCE, **History of Blockchain (2020).** Disponível em: https://academy.binance.com/pt/articles/history-of-blockchainAcessado em 18/02/2022.

BINANCE. Disponível em: https://www.binance.com Acessado em 18/06/2022.

BITCOIN TALKS **Trolololo**. Disponível em: https://bitcointalk.org/index.php?topic=831547.0 Acessado em 18/06/2022.

BLOCKCHAIN.COM, **Block charts**. Disponível em: https://www.blockchain.com/pt/charts/blocks-size Acessado em 18/06/2022.

BLOOMBERG. **Come to Jesus moment for crypto finance apps rocks valuation.** Disponível em: https://www.bloomberg.com/news/articles/2020-09-11/-come-to-jesus-moment-for-crypto-finance-apps-rocks-valuations#xj4y7vzkg Acessado em 18/06/2022.

BLOOMBERG. **Crypto Exchange Gets Millions After Copy-Paste of a Rival's Code**. 2020 Disponível em: https://www.bloomberg.com/news/articles/2020-09-11/-come-to-jesus-moment-for-crypto-finance-apps-rocks-valuations#xj4y7vzkg Acessado em 18/06/2022.

CASEY, Michael. **The impact of blockchain technology on finance: a catalyst for change.** London, UK, 2018.

CASTELLANOS, Sara. **A Cryptocurrency Technology Finds New Use Tackling Coronavirus.** The Wall Street Journal, 2020.

CATALINI, Christian et al., **Seeding the S-Curve? The Role of Early Adopters in Diffusion**. SSRN Electronic Journal, 2016.

CATALINI, Christian; GANS, Joshua S. **Some Simple Economics of the Blockchain.**

CHAINLINK. Disponível em: https://chain.link Acessado em 18/06/2022.

CHANDRA, Prabhul. **Reimagining Democracy: What if votes were a crypto-currency?** Blog Democracy Without Borders, 2018. Disponível em: https://www.democracywithoutborders.org/4625/reimagining-democracy-what-if-votes-were-a-crypto-currency/ Acesso em 19/01/2021.

CHUEN, David Lee Kuo. **Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data**. Academic Press.

CMREAP. **Solutions for the Trilemma.** 2021. Disponível em: https://medium.com/reapchain/solutions-for-trilemma-61ace7d717cc Acessado em 18/06/2022.

COINDESK. **What are liquidity pool?** Disponível em: https://www.coindesk.com/learn/what-are-liquidity-pools/#:~:text=What%20is%20a%20liquidity%20pool,automated%20market%20makers%20(AMMs) Acessado em 18/06/2022.

COINMARKETCAP. Disponível em: www.coinmarketcap.com Acessado em 18/06/2022.

COINTELEGRAPH. **Smart Contracts Explained.** Disponível em: https://cointelegraph.com.br/explained/smart-contracts-explained Acessado em 18/06/2022.

COMPOUND Disponível em: https://compound.finance Acessado em 18/06/2022.

COMPUTER WORLD. **Why blockchain cloud be a threat to democracy**. Disponível em: https://www.computerworld.com/article/3430697/why-blockchain-could-be-a-threat-to-democracy.html Acessado em 18/06/2022.

CONSENSYS. **2019 was the year od DeFi and why 200 will be too**. Disponível em: https://consensys.net/blog/news/2019-was-the-year-of-defi-and-why-2020-will-be-too/ Acessado em 18/06/2022.

CONSENSYS. **Security Risk in Ethereum DeFi.** Disponível em: https://consensys.net/blog/codefi/security-risks-in-ethereum-defi/ Acessado em 18/06/2022.

CORKERY, Michael et al., **From Farm to Blockchain: Walmart Tracks Its Lettuce**. The New York Times, 2018.

CRYPTOPEDIA. **What Is a Decentralized Exchange (DEX)?**. Disponível em: https://www.gemini.com/cryptopedia/decentralized-exchange-crypto-dex#section-exchanges-of-the-future Acessado em 18/06/2022.

DEFI PULSE. **Defi Pulse Charts.** Disponível em: https://www.defipulse.com/ Acessado em 16 de junho de 2022.

DWORK, et al., **Pricing via Processing or Combating Junk Mail**. Disponível em: https://link.springer.com/chapter/10.1007/3-540-48071-4_10 Acessado em 18/02/2022.

ENTERPRISE ETHEREUM ALLIANCE. **EEA**. Disponível em: https://entethalliance.org/ Acessado em 18/06/2022.

ETHEREUM FOUNDATION, **Developers Documents.** 2022. Disponível em: https://ethereum.org/en/developers/docs/evm/ Acessado em 18/06/2022.

ETHEREUM FOUNDATION. **Defi.** Disponível em: https://ethereum.org/en/defi Acessado em 18/06/2022.

ETHEREUM FOUNDATION. Disponível em: www.ethereum.org Acessado em 18/06/2022.

ETHEREUM FOUNDATION. **Ethereum Improvement Proposal**. Disponível em: https://eips.ethereum.org/ Acessado em 18/06/2022.

ETHEREUM FOUNDATION. **Ethereum Launches**. 2015. Disponível em: www.blog.ethereum.org Acessado em 18 de junho de 2022

ETHEREUM FOUNDATION. **Ethereum Token Standards.** Disponível em: https://ethereum.org/en/developers/docs/standards/tokens/ Acessado em 18/06/2022.

ETHEREUM FOUNDATION. **Ethereum Yellow Paper**. Disponível em: https://ethereum.github.io/yellowpaper/paper.pdf Acessado em 18/06/2022.

ETHEREUM FOUNDATION. **Shard Chains**. Disponível em: https://ethereum.org/en/upgrades/shard-chains/ Acessado em 18/06/2022.

ETHEREUM FOUNDATION. **The great eth2 renaming.** 2022. Disponível em: https://blog.ethereum.org/2022/01/24/the-great-eth2-renaming/ Acessado em 18/06/2022.

ETHEREUM FOUNDATION.. **The great eth2 renaming**. Disponível em: https://blog.ethereum.org/2022/01/24/the-great-eth2-renaming/ Acessado em 18/06/2022.

ETHERSCAN. Disponível em: https://etherscan.io/charts Acessado em 18/06/2022.

EVA Venkataramakrishnan. **O que são criptomoedas e stablecoins e como elas funcionam?**. 2021

EXTANCE, Andy. **The future of cryptocurrencies: Bitcoin and beyond**. Nature, 2015.

FRANCO, Pedro. **Understanding Bitcoin: Cryptography, Engineering and Economics**. John Wiley & Sons, 2014.

GEMINI. **Decentralized Exchanges of the future.** Disponível em: https://www.gemini.com/cryptopedia/decentralized-exchange-crypto-dex#section-exchanges-of-the-future Acessado em 18/06/2022

GERTRUDE, Chavez-Dreyfuss,. **Cryptocurrency Crime Declines But 'DeFi' Fraud Soars: CipherTrace**. Reuters. 2019.

GERVAIS, Arthur et al. **Is Bitcoin a Decentralized Currency?** InfoQ & IEEE Computer Society, 2014.

GSTETTNER, Stefan. **How Blockchain Will Redefine Supply Chain Management**. The Wharton School of the University of Pennsylvania, 2019.

HAFID, Abdelatif. **Scaling Blockchains: A Comprehensive Survey**. 2020. Disponível em: https://www.researchgate.net/publication/342639281_Scaling_Blockchains_A_Comprehensive_Survey Acessado em 18/06/2022.

HARDJONO, et al., **An Interoperability Architecture for Blockchain Gateways**. IETF Tecnical report, 2020.

HEIMBACH, Lioba et al. **Risks and Returns of Uniswap V3 Liquidity Providers.** Disponível em: https://arxiv.org/pdf/2205.08904.pdf Acessado em 18/06/2022.

HERTIG, Alyssa. **Introducing Ledger, the First Bitcoin-Only Academic Journal**. Motherboard, 2015.

HOFFMAN, 2019. **Ethereum the digital finance stack.** Disponível em: https://medium.com/pov-crypto/ethereum-the-digital-finance-stack-4ba988c6c14b Acessado em 18/06/2022.

HOLOTIUK, F et al. **The impact of blockchain technology on business models in the payments industry**. 2017

HSIEH, Ying-Ying et al. **Correction to: Bitcoin and the rise of decentralized autonomous organizations**. Journal of Organization Design 8, 2019.

INSURANCE JOURNAL. **Cryptocurrency Crime Declines But 'DeFi' Fraud Soars: CipherTrace**. Disponível em: https://www.insurancejournal.com/news/national/2021/05/14/613928.htm 2021. Acessado em 18/06/2022.

JANASHIA, N. **Introduction to decentralized finance aka 'defi'.** 2019. Disponível em: https://medium.com/@Nodar/introduction-to-decentralized-financeaka-defiea4f12e6256d. Acessado em 18/06/2022

JANSSEN, Marijn et al. **A framework for analysing blockchain technology adoption: Integrating institutional, market and technical factors**. International Journal of Information Management, 2020.

KELLY, Jemima. **UBS leads team of banks working on blockchain settlement system**. Reuters, 2019

KELLY, Jemima. **Banks adopting blockchain 'dramatically faster' than expected: IBM**. Reuters, 2016.

KOENS, Tommy; et al. **The Drivers Behind Blockchain Adoption: The Rationality of Irrational Choices**, Concurrency and Computation Practice and Experience, 2020.

KOLN, Nils. **Bank mit Kette**. Sueddeutsche Zeitung, 2018.

KOPFSTEIN, Janus. **The Mission to Decentralize the Internet**. The New Yorker, 2013.

KUMAR, Randhir; TRIPATHI, Rakesh. **Implementation of Distributed File Storage and Access Framework using IPFS and Blockchain**. Fifth International Conference on Image Information Processing (ICIIP), 2019.

LEE, Timothy. **Major glitch in Bitcoin network sparks sell-off; price temporarily falls 23%**. Arstechnica, 2013.

LI et al. **Securing Proof-of-Stake Blockchain Protocols**. Springer International Publishing, 2017.

LI, Jerry. **Blockchain technology adoption: Examining the Fundamental Drivers**. ACM Publication, 2020.

LIGHTING NETWORK Disponível em: https://lightning.network Acessado em 18/06/2022

LOOKINTOBITCOIN. **Bitcoin Rainbow Chart.** Disponível em: https://www.lookintobitcoin.com/charts/bitcoin-rainbow-chart/ Acessado em 18/06/2022.

LOOP MARKETS - xuanling11. **Defi a Rainbow 5 layers cake.** Disponível em: https://www.loop.markets/defi-a-rainbow-5-layers-cake/ Acessado em 18/06/2022.

LUMINEAU, Fabrice; et al. **Blockchain Governance -A New Way of Organizing Collaborations?** Organization Science, 2020.

MA, Jinhua et al. **A Blockchain-Based Application System for Product Anti-Counterfeiting**. IEEE, 2020.

MAKERDAO. Disponível em: https://makerdao.com Acessado em 18/06/2022.

MEDIUM. **Nexus Mutual**. Disponível em: https://medium.com/nexus-mutual/understanding-risks-in-defi-eth-cc-presentation-4db9c7aedbb1 Acessado em 18/06/2022.

MERCADO BITCOIN. Disponível em: https://www.mercadobitcoin.com.br Acessado em 18/06/2022.

METAMASK. Disponível em: https://metamask.io Acessado em 18/06/2022.

MIGAN, Xavier. **Identifying Key Non-Financial Risks in Decentralised Finance on Ethereum Blockchain.** 2020. Disponível em: https://www.researchgate.net/profile/Xavier-Meegan-2/publication/344689196_Identifying_Key_Non-Financial_Risks_in_Decentralised_Finance_on_Ethereum_Blockchain/links/5f8985c9458515b7cf8507e6/Identifying-Key-Non-Financial-Risks-in-Decentralised-Finance-on-Ethereum-Blockchain.pdf Acessado em 18/06/2022.

MORRIS, Nicky. **ScanTrust's anti-counterfeit solution isn't just about blockchain**. Ledger Insights - enterprise blockchain, 2018.

NARAYANAN, Arvind et al. **Bitcoin and cryptocurrency technologies**: a comprehensive introduction. Princeton: Princeton University Press, 2016.

NEXUS MUTUAL Disponível em: https://nexusmutual.io Acessado em 18/06/2022.

NIKBAKHT, et al., **The Emerald Handbook of Blockchain for Business**. 2021

OPTIMISM. Disponível em: https://www.optimism.io Acessado em 18/06/2022.

PAUMGARTEN, Nick. **The Prophets of Cryptocurrency Survey the Boom and Bust**. The New Yorker. 2021

PERFECTIAL. **How Companies Can Leverage Private Blockchains to Improve Efficiency and Streamline Business Processes**. Disponível em: https://perfectial.com/blog/leveraging-private-blockchains-improve-efficiency-streamline-business-processes / Acessado em 18/06/2022.

POLYGON. Disponível em: https://polygon.technology Acessado em 18/06/2022.

POPPER, Nathan. **A Venture Fund With Plenty of Virtual Capital, but No Capitalist**. The New York Times, 2016

RAVAL, Siraj. **Decentralized Applications: Harnessing Bitcoin's Blockchain Technology**. O'Reilly, 2016.

RIZUN, Peter R. et al. **How to Write and Format an Article for Ledger"** Ledger, 2015.

RUSSO, Camila. **The infinite machine: how an army of crypto hackers is building the next internet with Ethereum.** 2020

SALEH et al., **Blockchain without Waste: Proof-of-Stake**. The Review of Financial Studies.

SCHUEFFEL, Patrick. **DeFi: Finanças Descentralizadas - Uma Introdução e Visão Geral.** 2021

SCHUEFFEL, Patrick; GROENEWEG, Nikolaj; BALDEGGER, Rico. **The Crypto Encyclopedia: Coins, Tokens and Digital Assets from A to Z**. Bern: School of Management Fribourg / Switzerland, 2019.

SHAH, Rakesh. **How Can The Banking Sector Leverage Blockchain Technology?** PostBox Communications Blog, 2018.

SHAR, Fabian. **Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets**. 2021. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3843844 Acessado em 18/06/2022

SMITH AND CROWN. **The Oracle problem and mixicles.** Disponível em: https://smithandcrown.com/research/the-oracle-problem-and-mixicles/ Acessado em 18/06/2022.

SOLIDITY. **Introduction to Smart Contracts**. Disponível em: https://docs.soliditylang.org/en/v0.4.24/introduction-to-smart-contracts.html Acessado em 18/06/2022.

SOLIDITYLANG. **Introduction to Smart Contracts**. 2021 Disponível em: www.SolidityLang.org. Acessado em 18/06/2022.

STACK OVERFLOW. **Create Ethereum public address from a private key.** Disponível em: https://stackoverflow.com/questions/60697592/create-an-ethereum-public-address-from-a-private-key Acessado em 18/06/2022.

STRYDOM, Moses; BUCKLEY, Sheryl. **AI and Big Data's Potential for Disruptive Innovation**. IGI Global, 2019.

SYNTHETIX. Disponível em: https://synthetix.io Acessado em 18/06/2022.

SZABO, Nick. **View of Formalizing and Securing Relationships on Public Networks.** 2017.

TAPSCOTT, Don; TAPSCOTT, Alex. **Here's Why Blockchains Will Change the World**. Fortune, 2016.

TAPSCOTT, Don; TAPSCOTT, Alex. **The Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World**. Portfolio/Penguin, 2016.

TECH CRUNCH. **Vapor No More: Ethereum Has Launched**. 2020.

TECHREPUBLIC. **Don't get rugged DeDi Scams go from zero to 129 million in a year to became top financial hack.** Disponível em: https://www.techrepublic.com/article/dont-get-rugged-defi-scams-go-from-zero-to-129-million-in-a-year-to-become-top-financial-hack/ Acessado em 18/06/2022.

THE BLOCK. **The Block Blog.** Disponível em: https://www.theblockcrypto.com/ , acessado em 18 de junho de 2022.

THIBODEAU, Mary. **Unstoppable Domains and the End of Internet Censorship**. HedgeTrade Blog, 2019.

UNISWAP. Disponível em: https://uniswap.org Acessado em 18/06/2022.

UNISWAP. **Uniswap Whitepaper.** Disponível em: https://uniswap.org/whitepaper.pdf Acessado em 18/06/2022.

UNISWAP. **Whitepaper Uniswap v3.** Disponível em: https://startcy.io/whitepaper-v3.pdf acessado em 16 de junho de 2022.

VIGNA, Paul. **Ethereum Is Booming in the NFT Frenzy—So Is Network Congestion**. The Wall Street Journal. 2021.

WALKER, Martin. **Distributed Ledger Technology: Hybrid Approach, Front-to-Back Designing and Changing Trade Processing Infrastructure**. 2018

WEGNER, Peter. **Interoperability**. ACM Computing Surveys, 1996.

WIKIPÉDIA. **Árvores de Merkle**. Disponível em: https://pt.wikipedia.org/wiki/%C3%81rvores_de_Merkle Acessado em 18 de junho de 2022.

WIKIPEDIA. **Bloco Gênesis**. Disponível em: https://en.bitcoin.it/wiki/Genesis_block Acessado em 18/06/2022.

WIKIPEDIA. **DAOs**. Disponível em: https://en.wikipedia.org/wiki/Decentralized_autonomous_organization Acessado em 18/06/2022.

WIKIPEDIA. **Logo da Ethereum**. Disponível em: https://pt.m.wikipedia.org/wiki/Ficheiro:Ethereum_logo_2014.svg Acessado em 18/06/2022.

WIKIPEDIA. **Ponzi**. Disponível em: https://en.wikipedia.org/wiki/Ponzi_scheme Acessado em 18/06/2022.

WIKIPEDIA. **Turing completo**. Disponível em: https://pt.wikipedia.org/wiki/Turing_completude Acessado em 18/06/2022.

WIKIPEDIA. **Wei Dai**. Disponível em: https://en.wikipedia.org/wiki/Wei_Dai Acessado em 18/06/2022.

WSJ. **A cryptocurrency technology finds new use tackling coronavirus**. Disponível em: https://www.wsj.com/articles/a-cryptocurrency-technology-finds-new-use-tackling-coronavirus-11587675966 Acessado em 18/06/2022

**ANEXOS E APÊNDICES**

ANEXO A – QUESTIONÁRIO DA PESQUISA REALIZADA EM 2021 E 2022 PELO AUTOR


# Pesquisa acadêmica

As informações coletadas na presente pesquisa não serão compartilhadas com terceiros. Ao responder a pesquisa você concorda que os dados coletados sejam utilizados para a realização de um trabalho acadêmico de conclusão de curso da Fatec Taubaté.

Faça login no Google para salvar o que você já preencheu. Saiba mais

*Obrigatório

Como você se identifica? *

- ◯ Sou homem
- ◯ Sou mulher
- ◯ Prefiro não responder

Você já ouviu falar em blockchain? *

- ◯ Sim
- ◯ Não

Você já ouviu falar em Bitcoin? *

- ◯ Sim
- ◯ Não

[2022] Você já comprou criptomoedas como o Bitcoin? *

- ◯ Já comprei criptomoedas
- ◯ Nunca comprei criptomoedas, mas quero comprar
- ◯ Nunca comprei criptomoedas e nem quero comprar
- ◯ Nunca comprei criptomoedas e não sei se compraria

O quão favorável você é com criptomoedas como o Bitcoin? *

- ◯ Sou muito favorável
- ◯ Sou favorável
- ◯ Nem favorável nem desfavorável
- ◯ Sou desfavorável
- ◯ Sou muito desfavorável

[2022] Você já ouviu falar em Ethereum? *

- ◯ Sim
- ◯ Não

Já ouviu falar em Aplicativos Descentralizadas (Dapps)? *

- ◯ Sim
- ◯ Não

Já ouviu falar em Finanças Descentralizadas (DeFi) ou Corretoras Descentralizadas (DEX)? *

- ◯ Sim
- ◯ Não

Já ouviu falar em Tokens-Não-Fungíveis (NFTs)? *

- ◯ Sim
- ◯ Não

Você já realizou investimento de algum dos tipos abaixo? (marque quantas quiser) *

- [ ] Nunca fiz investimentos
- [ ] Renda fixa (poupança, CDI, etc)
- [ ] Renda variável (ações, fundos, etc)
- [ ] Criptomoedas (bitcoin, litecoin, etc)
- [ ] Outro: _____

[2022] Qual sua renda familiar mensal (você mais as pessoas que vivem contigo)? *

- ◯ Até 1 salário mínimo (R$1.045)
- ◯ Entre 1 e 3 salários mínimos
- ◯ Entre 3 e 6 salários mínimos
- ◯ Entre 6 e 10 salários mínimos
- ◯ Entre 10 e 20 salários mínimos
- ◯ Mais de 20 salários mínimos

Em que ano você nasceu? (ex: 1992) *

Sua resposta