UNIVERSIDADE FEDERAL DO ESTADO DO RIO DE JANEIRO
CENTRO DE CIÊNCIAS EXATAS E TECNOLOGIA
CURSO DE PÓS-GRADUAÇÃO EM MATEMÁTICA

Uma Aplicação em Finanças Descentralizadas Via Piscinas de Liquidez na Uniswap

Paulo Cesar Silva de Araújo

Rio de Janeiro
2023

Paulo Cesar Silva de Araújo

Uma Aplicação em Finanças Descentralizadas Via Piscinas de Liquidez na Uniswap

Trabalho de Conclusão de Curso apresentado ao Programa de Pós-Graduação em Matemática PROFMAT da UNIRIO, como requisito para a obtenção do grau de MESTRE em Matemática.

Orientador: Silas Fantin
Doutor em Matemática - USP

Rio de Janeiro
2023

Catalogação informatizada pelo(a) autor(a)

A658 Araújo, Paulo Cesar Silva de
Uma Aplicação em Finanças Descentralizadas Via Piscinas de Liquidez na Uniswap / Paulo Cesar Silva de Araújo. -- Rio de Janeiro, 2023.
127 p

Orientador: Silas Fantin.
Dissertação (Mestrado) - Universidade Federal do Estado do Rio de Janeiro, Programa de Pós-Graduação em Matemática, 2023.

1. Piscinas de liquidez. 2. Finanças descentralizadas. 3. Uniswap. I. Fantin, Silas, orient. II. Título.

Paulo Cesar Silva de Araújo

Uma Aplicação em Finanças Descentralizadas Via Piscinas de Liquidez na Uniswap

Trabalho de Conclusão de Curso apresentado ao Programa de Pós-Graduação em Matemática PROFMAT da UNIRIO, como requisito para a obtenção do grau de MESTRE em Matemática.

Aprovado em 15 de setembro de 2023

Banca Examinadora

Prof. Dr. Silas Fantin – Orientador
UNIRIO

Prof. Dr. Helisson Ricardo Rufo Coutinho
UNIRIO

Prof. Dr. Marcelo Leonardo dos Santos Rainha
UNIRIO

Prof. Dr. Sérgio José Xavier de Mendonça
UFF

Rio de Janeiro
2023

Resumo

Esta pesquisa trata sobre um tipo de aplicação em finanças descentralizadas, que se tornou possível com o advento das blockchains e criptomoedas. Mais especificamente, o objetivo geral é analisar matematicamente o funcionamento de uma piscina de liquidez na Uniswap. Mas o que são criptomoedas? O que são blockchains? O que são finanças descentralizadas? O que são piscinas de liquidez? O que é Uniswap? Responder, de maneira introdutória, essas perguntas sobre alguns dos elementos envolvidos no processo de montagem e no funcionamento de uma piscina de liquidez é um dos objetivos específicos deste trabalho. Por fim, serão apresentados alguns roteiros com a expectativa de permitir ao leitor acessar e, minimamente, interagir com ambientes cripto, com foco na montagem de uma piscina de liquidez na Uniswap.

Palavras-chaves: Piscinas de Liquidez, Finanças Descentralizadas, Uniswap

Abstract

This research deals with a type of application in decentralized finance, which became possible with the advent of blockchains and cryptocurrencies. More specifically, the overall objective is to mathematically analyze the operation of a liquidity pool at Uniswap. But what are cryptocurrencies? What are blockchains? What is decentralized finance? What are liquidity pools? What is Uniswap? Responding, in an introductory manner, to these questions about some of the elements involved in the process of setting up and operating a liquidity pool is one of the specific objectives of this work. Finally, some scripts are going to be presented with the expectation of allowing the reader to access and, at least, interact with crypto environments, focusing on setting up a pool of liquidity at Uniswap.

Keywords: Liquidity Pools, Decentralized Finance, Uniswap

Agradecimentos

Agradeço à minha esposa por todo apoio recebido ao longo do curso e por compreender em diversas oportunidades os momentos em família que tive que me ausentar para me dedicar ao mestrado. Esse processo começou lá em 2012, ano em que entrei pela primeira vez num programa de mestrado e se encerra nesse programa, após três tentativas frustradas em outros programas.

Agradeço à toda minha família, em especial, minha mãe, que não mediu esforços para que eu pudesse me concentrar somente nos meus estudos até o fim da minha graduação. A minha busca incessante pelo título de mestre foi também uma forma de valorizar ainda mais todos os sacrifícios que minha família fez por mim.

Agradeço aos meus amigos de turma por toda parceria que tivemos ao longo do curso na UNIRIO.

Agradeço aos professores do programa por toda dedicação e paciência para que eu e meus colegas de turma tivéssemos a melhor formação possível. O primeiro ano de curso aconteceu com aulas 100% remotas devido à pandemia de COVID-19 e o desafio foi grande para alunos e professores.

Por fim, não posso deixar de agradecer ao professor Silas Fantin que aceitou me orientar e resistiu comigo até o final. Tivemos encontros semanais por um ano e aprendi bastante nesse período, não só sobre o tema dessa pesquisa, mas também sobre outros assuntos que envolvem análise matemática.

Sumário

INTRODUÇÃO

A quantidade excessiva de moeda em circulação em um país impacta, de forma significativa, no seu valor, quando comparado com o de outras moedas. Além disso, ela gera uma disparada de preços dos bens de consumo e, consequentemente, diminui o poder de compra das pessoas que não têm sua renda reajustada. Esse efeito é conhecido como inflação.

Países que sofrem com os impactos da inflação por vezes optam por mudanças em sua moeda oficial corrente para tentar estabilizar sua situação econômica. Como exemplo, líderes políticos na Argentina cogitam trocar a moeda oficial em seu país pelo dólar, como uma tentativa de frear os efeitos da alta inflação pela qual o país está passando, segundo (Elias, 2023).

Para se ter uma ideia, o Brasil já teve oito moedas oficiais desde o Cruzeiro (Cr$), moeda criada em novembro de 1942, conforme podemos ver na Figura 1 - Moedas brasileiras. abaixo.

Figura 1 - Moedas brasileiras. Fonte: (Hinsching, 2020)

O Real (R$), moeda oficial brasileira desde julho de 1994, já perdeu quase 90% do seu valor, como mostra a Figura 2 abaixo.

Figura 2 - Desvalorização do real ao longo do tempo.

O dólar americano, por exemplo, que é uma moeda bastante utilizada em transações comerciais em todo o mundo e, por isso, é considerada uma das mais seguras, também possui um histórico de desvalorização ao longo do tempo, como podemos ver em (Marinho, 2021).

A bitcoin, primeira e principal criptomoeda do mercado, juntamente com outras criptomoedas que surgiram posteriormente, descontinuam um sistema financeiro já estabelecido pelos governos por serem moedas que não são controladas pelos governos. A bitcoin, por exemplo, possui em seu código-fonte uma quantidade de produção de moedas limitada. Essa quantidade não pode ser alterada por nenhum indivíduo ou governo.

Com o surgimento das criptomoedas e das blockchains, ambiente virtual onde as criptomoedas ficam hospedadas, abriu-se caminho para o surgimento das corretoras de criptomoedas. As corretoras facilitam aos seus usuários o acesso, a negociação e a utilização das criptomoedas. Existem dois tipos de corretoras de criptomoedas:

- as centralizadas, que são mais populares e possuem maior controle dos dados e ativos dos usuários;
- e as descentralizadas, que priorizam uma maior privacidade e autonomia dos usuários quanto aos seus ativos.

Além disso, as corretoras descentralizadas (DEX's) dão a possibilidade de seus usuários atuarem como bancos. Nelas, os usuários podem disponibilizar suas criptomoedas, num ambiente chamado piscina de liquidez, para que outros usuários realizem trocas do seu interesse. Ao fornecerem as criptos para serem trocadas, os provedores de liquidez, aqueles que formam a piscina, ganham taxas por cada negociação realizada na sua piscina.

O fato de negociar ativos financeiros em ambiente descentralizado fez surgir o termo *finanças descentralizadas*. O objetivo geral desse trabalho é avaliar aspectos matemáticos envolvidos em piscinas de liquidez numa corretora descentralizada chamada Uniswap.

Para alcançar o objetivo geral, o autor deste trabalho elencou alguns pré-requisitos para desenvolver ao longo do texto, que dizem respeito ao processo de montagem de uma piscina de liquidez na Uniswap. Com isso, tem-se dois objetivos específicos, que são:

1) apresentar de forma introdutória os elementos cruciais envolvidos na montagem de uma piscina de liquidez na Uniswap;
2) apresentar um roteiro para a criação de uma piscina de liquidez na Uniswap.

A motivação para a realização desta pesquisa veio do grande potencial que as moedas digitais possuem de mudar completamente a forma como se faz política monetária no mundo. Além disso, há uma disponibilidade reduzida de materiais científicos abordando piscinas de liquidez, com detalhes matemáticos. Isso foi constatado ao utilizar as seguintes palavras-chaves no campo de busca de sites específicos, como Scielo, Capes, Google Acadêmico e o portal de dissertações do PROFMAT:

- piscina de liquidez;
- finanças descentralizadas;

- Uniswap

Essa pesquisa foi estruturada em cinco capítulos. No capítulo 1 faz-se um breve recorte da história da moeda. Historicamente, produtos que tinham maior demanda no mercado se tornavam uma moeda de troca. Atualmente, as moedas fiduciárias vigoram globalmente e são controladas pelos seus respectivos governos. As criptomoedas surgiram recentemente como uma alternativa ao sistema financeiro tradicional e possuem uma crescente quantidade de adeptos e de valor de mercado. Surfando no embalo das criptos, os governos estudam a implementação de moedas digitais, que podem aumentar ainda mais o seu controle sobre a população. Dá-se como exemplo o projeto do real digital.

No capítulo 2 será abordado de forma introdutória as características e o funcionamento das blockchains, que são onde as criptomoedas ficam hospedadas. As principais blockchains, que são a Bitcoin e a Ethereum, serão mais detalhadas. Além disso, será discutido a interoperacionalidade entre as blockchains através das pontes (bridges).

No capítulo 3 o leitor verá com mais detalhes o que é uma carteira de criptomoedas. Além disso, será visto o que são e quais as diferenças entre as corretoras centralizadas e descentralizadas. Por fim, detalha-se o funcionamento da Uniswap, corretora escolhida para montagem da piscina de liquidez.

No capítulo 4 dar-se-á destaque aos aspectos matemáticos envolvidos nas piscinas de liquidez da Uniswap. O intuito é analisar as vantagens e desvantagens de se montar uma piscina de liquidez, de maneira que o provedor de liquidez entenda o risco que a perda impermanente (impermanente loss) pode causar, além de conseguir dimensioná-lo.

No capítulo 5 será oferecido ao leitor dois roteiros: um para interação com a carteira MetaMask e outro com foco na montagem de uma piscina de liquidez na Uniswap.

1. UM BREVE RECORTE DA HISTÓRIA DAS MOEDAS

A comercialização de bens e serviços foi, e ainda é, fundamental para o desenvolvimento da economia. As diferentes habilidades e necessidades das pessoas, juntamente com diferentes concentrações de recursos naturais ao redor do globo terrestre, propiciam a troca de bens, serviços e produtos.

As primeiras trocas aconteciam por meio de produtos disponibilizados pelas próprias pessoas envolvidas no negócio. Ou seja, se uma pessoa possui um produto A, uma outra pessoa possui um produto B, e essas duas pessoas têm interesse no produto uma da outra, então a troca é realizada. Esse tipo troca também é conhecido como troca direta ou escambo.

Porém, nem sempre os interessados em trocar seus produtos encontravam um ponto em comum. Um mercador poderia ter um produto muito desejado por outro, mas a recíproca poderia não ser verdadeira. Outro fator que influenciava a decisão de um mercador em realizar uma troca era que um produto poderia ter grande demanda numa determinada região, mas em outra não.

Por muito tempo a troca direta foi a forma que as pessoas encontraram para conseguirem adquirir os produtos ou serviços que elas não conseguiam produzir ou realizar sozinhas. Segundo (Rothbard, 2013), ela mantém a economia num nível primitivo, sendo impossível haver qualquer tipo de economia civilizada sob um arranjo formado exclusivamente por esse formato de troca.

Todavia, passou-se a adotar um método de troca mais sofisticado, conhecido como troca indireta. Neste caso, se duas pessoas desejam trocar produtos que não são de interesse de ambos, busca-se um produto alternativo para ser utilizado como meio de troca e satisfazer o interesse de todos os envolvidos no negócio.

Por exemplo, imagine que João, um produtor de arroz, tenha interesse em trocar seu produto com José, um produtor de pães. Porém, José não tem interesse no arroz de João e, sim, no produto de Maria, uma produtora de trigo. Então, João troca seu produto com Maria e, posteriormente, troca o trigo que obteve de Maria pelos pães de José. Se a demanda pelo trigo de Maria cresce

por ser um produto de maior aceitação para realização de trocas, automaticamente esse produto se valoriza e passa a ser utilizado como meio de troca.

Diversos produtos ao longo da história foram utilizados como meio de troca, como, por exemplo, o tabaco, o açúcar, o sal, o cacau, as conchas marinhas, etc.

> Alguns bens são mais demandados que outros, alguns são plenamente divisíveis em unidades menores sem que haja perda de valor, alguns são mais duráveis, e outros são mais transportáveis por longas distâncias. Todas essas vantagens aumentam a comerciabilidade de um bem. Sendo assim, em cada sociedade, os bens mais comerciáveis serão, com o tempo, escolhidos para representar a função de meio de troca. (Rothbard, 2013)

No entanto, tais produtos quando demandados em grandes quantidades geravam uma maior dificuldade para transportá-los.

O aumento da procura por metais preciosos como ouro e prata foi importante para o surgimento das primeiras moedas. Esses metais eram moldados no formato de disco e marcados, além de serem leves e duráveis. Era muito mais conveniente utilizar moedas de metal como meio de troca.

O metal utilizado nas moedas podia ser desde ouro puro até o bronze, passando por ligação com misturas dependendo de cada lugar em cada período. A ampliação das redes comerciais, especialmente a partir das grandes navegações, causou mais encontros de povos de regiões diferentes que adotavam diferentes sistemas de moedas.

Um exemplo mais comum disso é que quando os espanhóis chegam na América Central, os astecas e outros povos viam o ouro como base para ornamentos e objetos, não como uma riqueza como os espanhóis. Ou seja, a integração do comércio pelo mundo é que, progressivamente, padroniza as moedas como meio de troca.

Quanto mais ampla uma rede comercial, mais ampla e verificável precisa ser a confiança da moeda utilizada. Isso quer dizer que com o surgimento de cada vez mais cidades e o consequente aumento das negociações entre elas,

foi necessário padronizar as moedas utilizadas como meio de troca. Desta forma, adotou-se a moeda com maior influência comercial até então. Esse é o início do dinheiro.

Uma vez que tínhamos uma moeda consolidada como meio de troca, estocá-la para realizar trocas a qualquer momento era importante e ao mesmo tempo perigoso, pois era necessário guardá-la com segurança, visto que as moedas passaram a ser bastante desejada pelas pessoas.

> Os negociantes de ouro e prata, por terem cofres e guardas a seu serviço, passaram a aceitar a responsabilidade de cuidar do dinheiro dos seus clientes e a dar recibos escritos das quantias guardadas. Esses recibos (então conhecidos como “goldsmith’s notes”) passaram, com o tempo, a servir como meio de pagamento por seus possuidores, por serem mais seguros de portar do que dinheiro vivo. (Casa da Moeda do Brasil, 2023)

Os recibos dados aos clientes eram lastreados em ouro, ou seja, não eram gerados recibos sem que houvesse a custódia de ouro por parte dos negociantes. Assim, segundo (Rothbard, 2013), “surgiram as primeiras cédulas de “papel moeda”, ou cédulas de banco, ao mesmo tempo em que a guarda dos valores em espécie dava origem a instituições bancárias”.

Dinheiro e moeda parecem sinônimos ou referências aos meios, mas significam coisas diferentes. Moeda é qualquer coisa com características que garantem seu uso em transações. O dinheiro é a moeda em um formato padronizado e com origem atestada. Por isso que as moedas metálicas ou cédulas possuem símbolos nacionais e são assinadas.

Com a expansão da revolução industrial, a integração comercial mundial cresceu, com moedas de países influentes sendo adotadas internacionalmente, como o dólar ou a libra esterlina, além de serem conversíveis em ouro até a década de 1970, quando se tornaram moedas fiduciárias. Isto é, as moedas deixaram de ser lastreadas em ouro e seu valor passou a vir da confiança que as pessoas têm em quem as emite, ou seja, na circunstância atual, nos governos.

O desenvolvimento tecnológico e as operações em tempo real aumentaram novamente a relação comercial mundial, como o uso de cartões de crédito e as transferências bancárias. Hoje, a maior parte da moeda mundial existe de forma não física, e na última década surge uma nova rede de confiança, motivada pela tecnologia, com uma proposta de ser uma alternativa ao sistema financeiro corrente. As criptomoedas! Em especial, a bitcoin!

No fim das contas, uma moeda é confiança, uma maneira de possibilitar que você confie em alguém que não conhece para que possam fazer comércio.

1.1 CRIPTOMOEDAS

As criptomoedas surgiram no mercado financeiro de forma revolucionária, principalmente impulsionadas pela proposta da primeira e mais importante delas, que é a bitcoin.

A bitcoin surge como uma alternativa às moedas controladas pelos governos. Isso se deve ao fato de ela ser, na sua essência, independente de políticas econômicas ou órgãos governamentais. Ela vive em uma rede onde todos os participantes possuem o mesmo nível de controle sobre ela.

Não demorou muito para que outras redes e criptomoedas fossem criadas, e atualmente existem diversas delas, cada uma com sua proposta. No entanto, a única criptomoeda que é reconhecidamente descentralizada pelo mercado cripto é a bitcoin.

O que impressiona é a velocidade de adesão da população a esses ativos e o volume financeiro empregado neles. Segundo (Bertolucci, 2023), o mercado de criptomoedas tem mais de 420 milhões de usuários e 10 mil empresas que aderiram a essa classe de ativos.

Figura 3 - Gráfico de capitalização do mercado de cripto. Fonte: (CoinGecko, 2023)

O gráfico na Figura 3 acima, retirado de (CoinGecko, 2023), nos mostra um recorte temporal, 01 de janeiro de 2017 a 01 de outubro de 2023, do valor de mercado das criptomoedas, numa escala que vai de 0 a 4 trilhões de dólares, com incremento de 1 trilhão de dólares. O valor de mercado das criptos ultrapassou 3 trilhões de dólares em novembro de 2021. Em julho de 2023, ele estava em cerca de 1,154 trilhões de dólares.

Ao comparar o valor de mercado das criptomoedas em julho de 2023 com o PIB das principais economias do mundo em 2022, é possível dimensionar a relevância do valor empregado nas criptomoedas. O valor de mercado das criptomoedas estaria entre as posições 17° e 18° na lista da Figura 4 abaixo.

Posição	País	PIB em US$ trilhões
1.º	Estados Unidos	22,998
2.º	China	17,458
3.º	Japão	4,937
4.º	Alemanha	4,226
5.º	Reino Unido	3,188
6.º	Índia	3,042
7.º	França	2,935
8.º	Itália	2,101
9.º	Canadá	1,991
10.º	Coreia do Sul	1,799
11.º	Rússia	1,776
12.º	Austrália	1,633
13.º	Brasil	1,608
14.º	Irã	1,4263
15.º	Espanha	1,4262
16.º	México	1,295
17.º	Indonésia	1,186
18.º	Países Baixos	1,019
19.º	Arábia Saudita	0,834
20.º	Suíça	0,813

Figura 4 - Ranking das 20 maiores economias do mundo em 2022. Fonte: (Pereira, 2023)

A Figura 5 abaixo nos mostra as dez principais criptomoedas, em valor de mercado, em 02 de outubro de 2023, segundo (CoinGecko, 2023). Observe que a bitcoin possui cerca de 551 bilhões de dólares em valor de mercado. Ela sozinha corresponde a quase 50% do valor de mercado de todas as criptomoedas juntas, uma parcela bastante significativa.

#	Moeda	Preço	1 h	24 h	7 d	Volume em 24 h	Capitalização de Mercado	Últimos 7 dias
1	Bitcoin BTC	US$ 28.262,67	-0.2%	4.1%	8.4%	US$ 14.773.188.597	US$ 551.175.972.653	
2	Ethereum ETH	US$ 1.728,19	-0.2%	2.5%	10.1%	US$ 12.019.662.800	US$ 207.886.714.851	
3	Tether USDT	US$ 1,00	0.1%	0.0%	0.0%	US$ 23.810.979.879	US$ 83.368.307.298	
4	BNB BNB	US$ 219,14	-0.1%	1.5%	5.3%	US$ 553.390.162	US$ 33.739.436.155	
5	XRP XRP	US$ 0,521885	0.1%	0.4%	5.3%	US$ 796.601.960	US$ 27.838.508.828	
6	USDC USDC	US$ 1,00	0.0%	0.1%	-0.0%	US$ 6.070.926.973	US$ 25.297.886.408	
7	Lido Staked Ether STETH	US$ 1.730,38	-0.0%	2.7%	10.1%	US$ 6.312.724	US$ 15.231.420.470	
8	Solana SOL	US$ 23,88	-1.1%	4.1%	22.4%	US$ 746.812.480	US$ 9.855.239.059	
9	Cardano ADA	US$ 0,267397	-0.1%	2.4%	10.0%	US$ 219.760.610	US$ 9.372.674.793	
10	Dogecoin DOGE	US$ 0,063691	0.0%	1.7%	5.0%	US$ 300.508.269	US$ 8.995.277.935	

Figura 5 - Top 10 das criptomoedas em valor de mercado em setembro de 2023. Fonte: (CoinGecko, 2023)

O mercado de criptos, dificilmente será deixado de lado. Os próprios governos de vários países estão lançando projetos de moedas digitais que, para os menos informados, podem parecer criptomoedas, mas não são. É importante que as pessoas entendam o que são as moedas digitais (seja uma criptomoeda ou não), conheçam suas características e saibam transacioná-las de maneira segura, porque essa será, provavelmente, a forma dominante de moeda num futuro próximo.

Altcoins

Com a exceção da bitcoin, todas as criptomoedas são consideradas altcoins. A palavra altcoin significa moeda alternativa. Segundo (Altcoins, 2022), elas são criadas para resolver problemas de outras redes, como lentidão ou altas taxas.

As altcoins podem ser criadas de três maneiras:

1) através de blockchains próprias como Ethereum, Cardano e Solana que possuem suas criptomoedas nativas;
2) através de um fork, que é uma bifurcação em uma blockchain devido a algum problema. Quando acontece uma bifurcação, a rede original se divide em duas outras. Uma delas mantém o token anterior e a outra passa a funcionar com uma altcoin criada a partir do fork.
3) através de uma blockchain criada a partir de outra já existente.

Como exemplo, a ether, moeda da blockchian da Ethereum, que é a segunda maior blockchain do mercado cripto em volume de capitalização, também é considerada uma altcoin.

Stablecoins

As stablecoins são um tipo de altcoins. Stablecoin significa moeda estável em tradução direta, ou seja, são moedas com baixa volatilidade. Elas são moedas lastreadas em outros ativos e são criadas em blockchains que possuem código fonte mais flexível, como é o caso da blockchain da Ethereum.

O emissor de uma stablecoin, que normalmente é uma empresa, precisa ter a mesma quantidade do ativo atrelado em caixa, da mesma forma que acontecia com as moedas lastreadas em ouro.

De acordo com (Stablecoins, 2022), há pelo menos quatro tipos de stablecoins no mercado, que são:

1) stablecoins lastreadas em moeda fiduciária, como o dólar, na proporção 1 por 1;
2) stablecoins lastreadas em outra criptomoeda, como, por exemplo, a criptomoeda DAI que para ser criada se faz necessário depositar a criptomoeda ETH num contrato inteligente;
3) stablecoins lastreadas em commodities, como o ouro.
4) stablecoins algorítmicas, que fogem um pouco à regra. Em vez de ser baseada em um ativo, sua estabilidade é alcançada com base no uso de algoritmos e contratos inteligentes.

Em julho de 2023 a terceira criptomoeda com maior volume de capitalização no mercado era a Tether (USDT), uma stablecoin lastreada em dólar.

1.2 REAL DIGITAL (Drex)

Em março de 2023, o Banco Central do Brasil anunciou que deu início ao projeto-piloto do real digital, a futura moeda virtual oficial do país e que se chamará Drex, conforme visto em (Sant'Ana, 2023) e (Sadi, 2023). Naturalmente, surgem alguns questionamentos sobre essa moeda, que tem previsão de ser lançada ao público em geral em 2024. Por exemplo:

- Como que essa moeda digital vai funcionar?
- Que diferença ela vai fazer para os cidadãos, principalmente na questão da segurança e da privacidade?
- Qual que é o perigo do real digital?

Antes do surgimento das criptomoedas, os governos detinham o monopólio do uso da moeda e cabia às pessoas a obrigação de aceitar. Quando a bitcoin foi criada, uma de suas propostas era que as pessoas passassem a ter o controle total de suas moedas. Surgia uma moeda descentralizada, que se mostra segura desde sua criação, transparente e protegida contra as arbitrariedades dos governos.

Os governos logo perceberam que as criptomoedas eram uma revolução sem volta. Com o surgimento delas, as suas moedas fiduciárias sofrerão forte concorrência. Se eles as proibirem, as chances de surgir um mercado paralelo para que a população possa comprar criptomoedas ilegalmente será grande.

Como exemplo, o governo argentino, diante da forte crise inflacionária que enfrentam atualmente, não quer que a população use o dólar americano. Para isso, ele criou o dólar Coldplay, com o objetivo de auxiliar o setor cultural e controlar a circulação de divisas no país. O dólar Coldplay é só uma das quinze cotações diferentes para a moeda americana na Argentina, como podemos ver em (InfoMoney, 2022).

Desta forma, os bancos centrais de alguns países, incluindo o Brasil, iniciaram projetos com moedas digitais, as chamadas CBDC's (Central Bank Digital Currencies), que utilizam a tecnologia blockchain. Essas moedas digitais podem até parecer um novo tipo de criptomoeda, porém, elas não possuem as mesmas características revolucionárias das criptomoedas, que são descentralização e privacidade.

Além disso, uma cripto está sujeita a volatilidade, ou seja, a cotação dela sobe e desce o tempo todo, com exceção, é claro, das stablecoins que tem uma cotação atrelada à outra moeda, que é justamente o caso do real digital. Um real digital sempre vai valer um real, ou seja, não vai estar sujeito à volatilidade.

Em contrapartida, com as CBDC's os governos terão ainda mais controle sobre o dinheiro da população, pois ele será centralizado e muito mais controlável, uma vez que ele estará sob custódia de órgãos governamentais ou controlados pelo governo. Diferentemente do dinheiro físico que fica sob custódia da população.

Por outro lado, o real digital também vai solucionar questões que já causam preocupação e problemas há tempos. Por exemplo, vamos supor que uma pessoa queira vender o seu carro. O que precisa acontecer primeiro, a transferência do veículo ou o pagamento? Na verdade, o ideal é que as coisas acontecessem simultaneamente, porque se a transferência do veículo acontece antes, o proprietário do veículo fica com o risco de não receber o dinheiro. Se o pagamento acontece antes, o comprador fica com o risco de não receber o carro.

De forma similar ocorre no processo de compra e venda de um imóvel. Quem faz o pagamento primeiro corre o risco de o vendedor não fazer a transferência de propriedade do imóvel, e quem faz a transferência de propriedade do imóvel primeiro corre o risco de não receber o dinheiro.

O uso do real digital, que será baseado na tecnologia blockchain, poderá inovar e acabar com os problemas de transações mencionados anteriormente, pois ele vai poder ser associado aos contratos inteligentes (smart contracts), como pode ser visto em (Sérvio, 2023).

Um contrato inteligente traz como benefício a possibilidade de executar simultaneamente as condições de uma transação financeira. Com esse tipo de inovação as compras e vendas de veículos, imóveis e muitos outros bens, vão poder ser feitas sem esses riscos que existem hoje.

Assim como uma pessoa não consegue sacar bitcoin em espécie e carregar ele na sua carteira de couro, com o real digital também não terá como fazer saque em espécie. A ideia é justamente que as transações aconteçam só no ambiente digital. Se alguém te sequestrar para pegar seu dinheiro, os criminosos não vão ter como fazer o saque em espécie. Eles vão ter que fazer uma transferência e, com isso, ficará fácil fazer o rastreamento do dinheiro e encontrá-los.

Capturar o criminoso é claro que é coisa boa. Esses avanços tecnológicos mencionados anteriormente, como o uso dos contratos inteligentes nas negociações ou o rastreamento do dinheiro digital, são muito interessantes e promissores, mas juntamente com eles abre-se a possibilidade de o governo ter ainda mais controle sobre a população, e isso vai de encontro com uma das propostas iniciais das criptomoedas, em especial, a bitcoin.

Na China, por exemplo, inspecionar os cidadãos ficou ainda mais fácil com o yuan digital, que é a moeda digital chinesa. Na verdade, a moeda digital deles cria possibilidades que merecem bastante reflexão.

> O governo chinês pretende implementar o sistema de crédito social no país com intuito de avaliar cada cidadão de acordo com seu comportamento social para então definir uma pontuação que estabeleça uma série de punições ou recompensas. (Schwingel, 2020)

Imagine um governo dizendo o que a população deve fazer com o seu dinheiro ou até quando o cidadão precisa gastar suas moedas, usando justamente esse mecanismo como um instrumento de política monetária. Se ele quiser que a população invista, basta ele criar um mecanismo para incentivá-la investir, inclusive punindo as pessoas que não cumprirem tal determinação. Se ele quiser que a população compre coisas é só ele forçá-la gastar e punir as pessoas que não acatarem.

Desta forma, se um governo quiser aumentar a atividade econômica para fazer o país crescer, basta ele, por exemplo, determinar que a população tem trinta dias para gastar todo o seu salário. Do contrário, o seu dinheiro perde a validade depois desse tempo. Como o dinheiro é digital, as preciosas moedas poderiam ser queimadas pelo governo, canceladas, confiscadas ou movidas forçadamente para outra pessoa, como podemos ver em (Barbosa, 2023). Essas são só algumas das possibilidades que uma moeda digital emitida por um banco central pode criar.

As lideranças políticas de um país não são eternas. Por mais que em determinado período possa existir um cenário de equilíbrio político e econômico, com as CBDC’s será criado um poder que vai estar disponível por tempo indeterminado para todo o governo que entrar no poder. Assim, o real digital trará benefícios, mas dará ao governo a possibilidade de ter ainda mais controle sobre a população.

2. BLOCKCHAINS

Neste capítulo, tem-se a intenção de fazer uma discussão introdutória sobre blockchain. O objetivo é que o leitor tome ciência sobre o que é e quais são as principais características e aplicações de uma blockchain. Para isso, será debatido alguns aspectos separados em tópicos como, por exemplo:

- o que é uma blockchain;
- como funciona uma blockchain;
- a função hash SHA-256;
- o trilema da blockchain;
- aplicações das blockhains.

Feito isso, será dado mais detalhes sobre as duas principais blockchains do mercado cripto, que são a Bitcoin e a Ethereum, além de ser introduzido o conceito de pontes entre blockchains.

A tecnologia blockchain resulta da soma de avanços tecnológicos que começaram a ser desenvolvidos desde 1991, quando o interesse inicial dos cientistas da computação era armazenar e proteger criptograficamente documentos digitais, conforme é possível verificar em (A História da Blockchain, 2018).

Antes de nos aprofundarmos mais sobre blockchains, é importante ressaltar que existem blockchains públicas e privadas.

Nas blockchains públicas, qualquer pessoa pode entrar. Além disso, todos podem ver as movimentações, e não há uma entidade central, como empresa, banco ou governo controlando as informações e ditando as regras. As redes Bitcoin e Ethereum se enquadram nessa categoria.

Com o *boom* das criptomoedas, empresas e governos se interessaram pela tecnologia. Eles criaram blockchains privadas, que têm uma entidade central controlando quem pode participar, bem como as informações e as regras. Esse modelo, portanto, faz mais sentido para aqueles que querem utilizar parte dos benefícios da tecnologia, mas precisam de privacidade. De acordo com (O que é Blockchain, 2022), empresas como a IBM e JBS, e entidades públicas como a Receita Federal do Brasil, utilizam o sistema em seus projetos.

As blockchains de interesse desse trabalho são as blockchains públicas. Não será discutido nesse texto as blockchains privadas. Sendo assim, daqui por diante, quando se usar o termo blockchain, automaticamente estará sendo falado sobre às blockchains públicas.

O que é a blockchain?

Uma blockchain é um sistema exclusivamente digital e online que funciona como um banco de dados de forma que as informações são adicionadas ao sistema, ao longo do tempo, em blocos que estão vinculados cronologicamente uns aos outros.

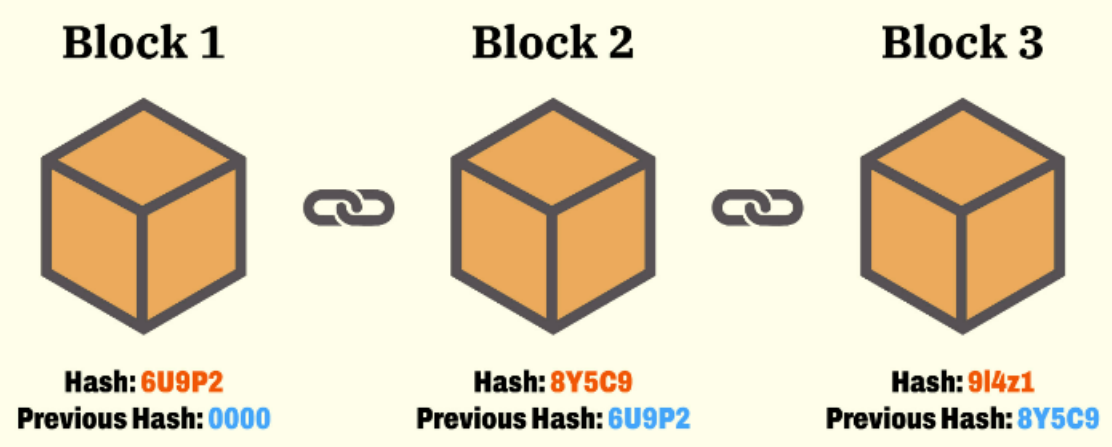


Figura 6 – Uma tentativa de representação visual de uma blockchain.

Assim como é possível verificar se alguma página foi adulterada ou excluída em um livro de registro com páginas numeradas, o vínculo entre os blocos da blockchain permite que se faça a verificação da veracidade da sequência de informações na cadeia de blocos.

> A Blockchain é uma cadeia linear de vários blocos conectados e protegidos por provas criptográficas. A tecnologia também pode ser aplicada em outras atividades que não requerem necessariamente operações financeiras, mas no contexto das criptomoedas, ela é responsável por manter um registro permanente de todas as transações confirmadas dentro da rede. (Blockchain vs Bitcoin, 2018)

No entanto, uma blockchain não é simplesmente um livro de registro em formato digital e online. Num livro de registro físico tradicional, normalmente existe uma pessoa, ou um grupo restrito de pessoas, que possuem acesso às

informações do livro. Desta forma, essa pessoa, ou grupo de pessoas, fica responsável pela segurança e veracidade de tais informações.

O controle das informações de um sistema por parte de uma quantidade restrita de pessoas caracteriza um sistema centralizado. As informações contidas numa blockchain são de livre acesso a todos os usuários da rede. Qualquer pessoa pode se conectar à rede e ter acesso às informações contidas nela. Isso faz com que a blockchain seja um sistema que não necessita de permissão para acessá-lo (a blockchain é permissionless) e essa característica a torna um sistema descentralizado.

A descentralização da blockchain requer cuidados com a segurança e veracidade dos dados contidos nela. Afinal, como qualquer pessoa pode se conectar à blockchain, pode haver alguém mal-intencionado com intuito de alterar ou excluir dados contidos nela.

Como funciona uma blockchain?

Uma blockchain tem certas propriedades únicas. Existem regras de como os blocos são adicionados ao longo do tempo. Uma vez armazenados, é praticamente impossível modificá-los ou excluí-los.

Cada novo bloco adicionado inclui informação que o vincula ao bloco adicionado anteriormente. Dessa maneira, é possível verificar se ele realmente foi criado após o último, e assim sucessivamente, até chegar ao primeiro bloco, chamado de bloco gênese.

Para tentar simplificar e visualizar como ocorre o vínculo entre os blocos, será utilizado uma situação retirada de (O que é uma Blockchain, 2023).

Considere uma planilha com duas colunas. Na primeira célula da primeira linha, coloca-se os dados que deseja armazenar. Os dados da primeira célula são convertidos em um identificador de duas letras, que será usado como parte da próxima entrada. Veja a Figura 7 abaixo.

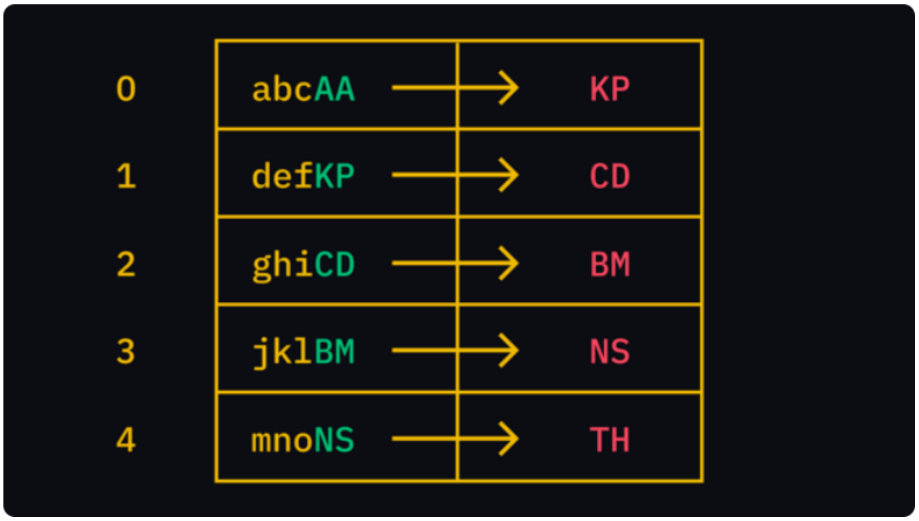


Figura 7 – Base de dados onde cada entrada está ligada à anterior. Fonte: (O que é uma Blockchain, 2023)

Observe que o identificador de duas letras KP é usado para preencher a próxima célula da linha seguinte (defKP). Ou seja, caso se altere os primeiros dados de input / entrada (abcAA), será recebido uma combinação diferente de letras na célula seguinte e, por consequência, em todas as outras células.

Desta forma, na planilha acima o identificador mais recente é o TH, localizado na segunda célula da linha 4. Ele é essencialmente o produto de todas as informações que vem antes dele. Se alguém tentar remover ou alterar os dados de alguma célula anterior, será fácil para qualquer usuário perceber tal tentativa. Assim, basta ignorá-la.

A função hash SHA-256

O caso citado anteriormente é uma analogia simplificada de como uma blockchain usa as funções hash criptográfica SHA-256. A função hash é o que mantém os blocos vinculados uns aos outros, fazendo com que o sistema alcance níveis significativos de segurança.

> "Essa função recebe uma entrada de tamanho aleatório (uma sequência de caracteres, um documento de texto, uma imagem ou até mesmo um vídeo) e a converte, através de transformações matemáticas combinadas, em uma sequência de saída de tamanho fixo de 256 bits escrita na base hexadecimal que conecta ao bloco atual toda a informação contida no bloco anterior". (Gonzaga, 2021)

Ainda de acordo com (Gonzaga, 2021), a função hash criptográfica SHA-256 cifra o conteúdo de um bloco de maneira que a partir do hash obtido não se consegue chegar na mensagem original.

A sequência obtida após a aplicação da função hash criptográfica SHA-256 possui sempre 64 caracteres, independentemente do tamanho da informação no bloco de entrada. Além disso, essa função é sensível à alteração dos dados de entrada a ponto de gerar outra sequência com resultado totalmente diferente da primeira, caso um caractere de entrada seja alterado de minúsculo para maiúsculo ou vice-versa. Veja o exemplo na Figura 8 abaixo.

Dados de input	Output do SHA256
Binance Academy	886c5fd21b403a139d24f2ea1554ff5c0df42d5f873a56d04dc480808c155af3
Binance academy	4733a0602ade574551bf6d977d94e091d571dc2fcfd8e39767d38301d2c459a7
binance academy	a780cd8a625deb767e999c6bec34bc86e883acc3cf8b7971138f5b25682ab181

Figura 8 – Sensibilidade da função hash. Fonte: (O que é uma Blockchain, 2023)

Como a saída da função hash é escrita na base hexadecimal, tem-se que a quantidade máxima de saídas diferentes que ela pode gerar é dada por:

$$\underbrace{16 \cdot 16 \cdot 16 \cdot \ldots \cdot 16}_{64\ fatores\ iguais\ a\ 16} = 16^{64} = 2^{256} \ .$$

Para se ter uma ideia do tamanho dessa quantidade de saídas, (Gonzaga, 2021) diz que “para calcular apenas os hash de 2^{128} entradas (quantidade muito menor) com um PC comercial, levaria-se mais do que 10^{27} anos”.

Mesmo com esse tamanho exorbitante de saídas possíveis da função hash, o tamanho do conjunto de todas as entradas é maior que o tamanho do conjunto de todas as saídas. Basta considerarmos $2^{256} + 1$ entradas que com certeza haverá duas delas com o mesmo hash de saída. Por isso, apesar de ser inviável, não é impossível obter dois hash iguais.

Segundo (Gonzaga, 2021), “até o presente momento ninguém foi capaz de encontrar uma colisão nessa função”, ou seja, nunca se encontrou o mesmo hash de saída para duas entradas diferentes. Devido a isso, diz-se que a função hash é resistente à colisão. Matematicamente falando, ela não é injetiva e, consequentemente, não possui inversa.

Trilema da blockchain

O trilema da blockchain, popularizado pelo cofundador da Ethereum, Vitalik Buterin, refere-se à ideia de que é difícil atingir, de forma simultânea, níveis ideais a três elementos desejáveis em uma blockchain: descentralização**,** segurança e escalabilidade. O foco em uma delas geralmente causa o enfraquecimento de outra.

Figura 9 – Trilema da blockchain. Fonte: (Goetze, 2022)

O termo escalabilidade refere-se ao objetivo de construir uma blockchain que possa suportar mais transações por segundo, mas é nesse ponto que muitas blockchains ainda enfrentam dificuldades. Isso ocorre porque os elementos de descentralização e segurança são tão fundamentais para a blockchain que tendem a receber mais atenção.

De acordo com (O'Neal, 2019), a Bitcoin não é capaz de lidar com mais de 7 transações por segundo e a Ethereum, a segunda rede mais popular, tem um limite de cerca de 20 transações por segundo. Por outro lado, um sistema de pagamento centralizado, como o da Visa, afirma ser capaz de processar 24.000

transações por segundo, apesar de possuir uma média de até 4.000 transações por segundo nos horários de pico. Isso ocorre porque a rede é fechada e não depende de consenso e de validadores públicos.

Desta forma, uma blockchain apresenta como vantagens ser um sistema descentralizado, sem permissão, resistente à ataques. Por outro lado, apresenta como desvantagens baixa escalabilidade e dificuldades para atualização.

Aplicações da blockchain

A blockchain nasceu junto com a Bitcoin e, portanto, possui intrinsecamente uma aplicação em finanças. Como a blockchain é um sistema descentralizado, abre-se um novo campo em finanças chamado de finanças descentralizadas (DeFi).

É comum algumas pessoas confundirem a tecnologia blockchain e a rede Bitcoin. Elas não são a mesma coisa. A rede Bitcoin é essencialmente um código computacional que determina o seu funcionamento e utiliza a tecnologia blockchain para garantir propriedades desejáveis.

Conforme pode ser visto em (O que é uma Blockchain, 2023) e (Blockchain: Casos de Uso, 2019), ao longo dos anos, outras aplicações da blockchain foram surgindo, como, por exemplo, em cadeia de suprimentos, sistemas de saúde, identidade digital, sistemas de governança, sistemas financeiros, etc. Contudo, o foco de investigação de aplicação da blockchain, nesse trabalho, é em finanças descentralizadas.

2.1 BITCOIN

Nesta seção será discutido superficialmente aspectos da rede Bitcoin e da criptomoeda bitcoin, também conhecida pela sigla BTC. Para isso, além de uma introdução sobre o funcionamento dessa rede, serão apresentados outros dois tópicos, que são: mineração e halving.

A bitcoin é a primeira moeda digital criada, a mais valiosa e considerada a principal criptomoeda até então.

É importante destacar que, conforme verifica-se em (Ulrich, 2014), “quando se refere ao sistema, à rede ou ao projeto Bitcoin, usa-se sempre inicial maiúscula. No entanto, quando se fizer referência às unidades monetárias bitcoins, utiliza-se a palavra em caixa baixa”.

A bitcoin é uma moeda digital que foi anunciada em 2008 e lançada em 2009 com a proposta de substituir o dinheiro físico sem a necessidade de ser controlada por uma instituição financeira, como um Banco Central, para intervir no valor de mercado desse ativo ou para validar as transações.

Para se ter uma ideia de como acontece tradicionalmente uma transferência bancária, será reproduzido abaixo um exemplo retirado de (Gonzaga, 2021).

Exemplo 1: Uma transferência bancária de R$ 100,00 de João no banco A para Maria no banco B, funciona da seguinte forma:

1. João, faz a transferência no banco A;
2. O banco A cobraria um percentual como comissão para processar a transação;
3. O banco A verifica se tem R$ 100,00 na conta do João;
4. O banco A pergunta ao banco B se a conta de Maria é válida e se está aberta para depósitos;
5. O banco A atualizaria seu livro de contabilidade para subtrair R$ 100,00 da conta de João;
6. O banco B atualizaria seu livro de contabilidade para adicionar R$ 100,00 na conta de Maria.

O exemplo 1 acima é um caso padrão de uma transação financeira controlada por um banco. Esse tipo de transação onde existe uma instituição que controla as operações bancárias é considerado um caso de finança centralizada. No caso da rede Bitcoin, não existe nenhuma instituição financeira ou órgão governamental que controle operações com bitcoins. Esse fato faz com que a rede Bitcoin seja considerada descentralizada. Segundo (Leão, 2019):

> “A descentralização tem o intuito de permitir que todos tenham o controle, enquanto, com a centralização, todo o controle está com os bancos centrais e isso implica que em termos da quantidade de dinheiro criado ou seu valor, nenhuma pessoa possui controle. Assim, os bancos centrais podem estipular o valor de moedas tradicionais, mediante a impressão de mais moeda.”

A Bitcoin é controlada pelos seus usuários, pois ela é uma rede ponto-a-ponto (peer-to-peer) que permite pagamentos online enviados diretamente de uma parte para outra sem passar por uma instituição financeira.

A seguir será reproduzido a mesma transferência do exemplo anterior, em que João transfere um valor para Maria, mas agora numa rede ponto-a-ponto (peer-to-peer), conforme visto em (Gonzaga, 2021).

Exemplo 2: Uma transferência de R$ 100,00 em rede Peer-to-peer com um ledger (carteira) de João para Maria, funciona da seguinte forma:

1. João envia a solicitação de transferência para a rede;
2. Em seguida, os computadores mais próximos a João na rede comprovam que João tem criptomoeda suficiente em sua conta;
3. Uma vez que verificam a transação, transmitem a transação para todos os computadores próximos a João e Maria na rede;
4. Por sua vez, esses computadores voltam a confirmar a transação e a transmitem, o que gera um efeito cascata até que a transação seja adicionada a todos os livros da rede Peer-to-peer.

O sistema ponto-a-ponto (peer-to-peer ou P2P) é o que está por trás da descentralização da rede Bitcoin. A Figura 10 abaixo ilustra seu efeito no funcionamento da rede.

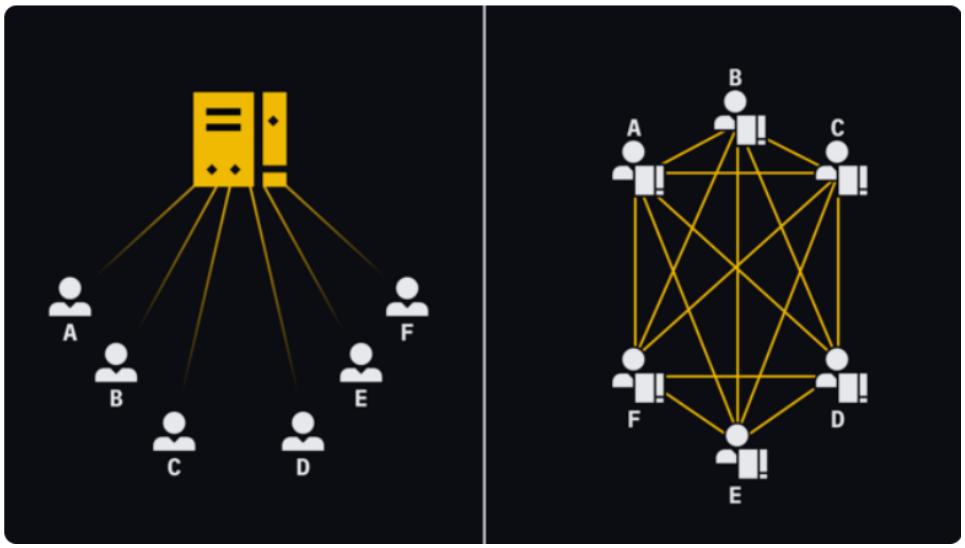


Figura 10 – Uma rede centralizada (esquerda) vs. Uma rede descentralizada (direita). Fonte: (O que é uma Blockchain, 2023)

Na imagem acima à esquerda, o usuário A precisa encaminhar sua mensagem através do servidor para que ela chegue ao usuário F. No lado direito, os usuários A e F estão diretamente conectados. Não existe um intermediário.

Note que no exemplo 2 acima são os próprios usuários da rede que validam a transação. Com a Bitcoin acontece algo análogo, pois ela é uma rede ponto-a-ponto (peer-to-peer).

A dinâmica de transação num sistema ponto-a-ponto não será detalhada nessa pesquisa. O sistema ponto-a-ponto foi destacado apenas para o leitor dimensionar a revolução trazida pela rede Bitcoin. Esse trabalho explora uma aplicação do uso de criptomoedas numa corretora descentralizada.

Mineração

Os participantes da rede Bitcoin que adicionam informações na rede são chamados de mineradores. Os mineradores recebem recompensas por cada problema resolvido e, consequentemente, por cada informação adicionada à rede.

No entanto, minerar bitcoins é algo que exige um grande esforço computacional para resolver problemas criptográficos. Segundo (Amaro, 2023), o custo energético para minerar 1 bitcoin no Brasil equivale a 45,5 mil dólares, ou seja, mais que a cotação atual de 1 bitcoin no mercado.

> A recompensa – geralmente chamada de recompensa de bloco – é composta de dois componentes: comissões associadas às transações e o subsídio por bloco. O subsídio por bloco é a única fonte de “novas” bitcoins. A cada bloco minerado, uma quantidade definida de moedas é adicionada ao fornecimento total. (O que é Bitcoin, 2020)

Os mineradores recebem novas bitcoins como prêmio após adicionarem um novo bloco de informações a rede Bitcoin e, assim, novas moedas entram em circulação na rede. Contudo, uma característica da rede Bitcoin que faz com que seus participantes atribuam valor às bitcoins é o fato de a quantidade de bitcoins ser finita.

A quantidade finita de bitcoins, que corresponde a 21 milhões de moedas, é estabelecida em seu protocolo e sua dificuldade de produção faz com que essa criptomoeda seja considerada uma reserva de valor e apelidada de ouro digital.

O fato de novas bitcoins serem adicionados à rede após a mineração de um bloco de informações ocorre porque nem todas as bitcoins estão disponíveis no mercado. Em 2020 a produção de moedas alcançou quase 90% do total de moedas estabelecido inicialmente no protocolo Bitcoin.

O halving

O acréscimo de bitcoins a rede Bitcoin é reduzido gradualmente em eventos periódicos conhecidos como halvings.

> O Halving de Bitcoin (também chamado de Bitcoin halvening) é simplesmente um evento que reduz a recompensa do bloco. Quando ocorre um Halving, a recompensa dada aos mineradores pela validação de novos blocos cai pela metade. No entanto, esse evento não causa impacto nas taxas de transação. (O que é Bitcoin, 2020)

Quando a Bitcoin foi lançada, os mineradores recebiam 50 BTC para cada bloco válido. Cada bloco demora cerca de 10 minutos para ser minerado e, por padrão do protocolo, o halving ocorre a cada 210.000 blocos minerados. Segundo, (Jenkinson, 2023), em julho de 2023 foi minerado o bloco de número 800 mil. Isso significa que restam 40 mil blocos para serem minerados até o próximo halving, que será o quarto da rede Bitcoin. Como podemos ver abaixo,

imediatamente após o primeiro Halving já havia 10,5 milhões de BTC adicionados à rede Bitcoin.

$$50\ BTC\ por\ bloco\ \times\ 210.000\ blocos = 10{,}5\ milhões\ de\ BTC\ .$$

Como cada bloco demora cerca de 10 minutos para ser minerado e cada halving ocorre após 210.000 blocos minerados, tem-se que o halving ocorre, aproximadamente, de 4 em 4 anos, como podemos ver abaixo:

$$210.000\ blocos\ \times\ 10\ \text{min}\ por\ bloco = 2.100.000\ minutos \approx 4\ anos\ .$$

O primeiro halving aconteceu no dia 28 de novembro de 2012. Naquele momento, o protocolo reduziu o subsídio por bloco de 50 BTC para 25 BTC. O segundo halving aconteceu em 9 de julho de 2016, reduzindo o subsídio por bloco de 25 BTC para 12,5 BTC. O terceiro halving ocorreu em 11 de maio de 2020 e reduziu o subsídio por bloco para 6,25 BTC.

Com isso, estima-se que o valor de subsídio aos mineradores chegue a zero por volta de o ano de 2140, quando todas as moedas estarão mineradas e, consequentemente, disponíveis no mercado.

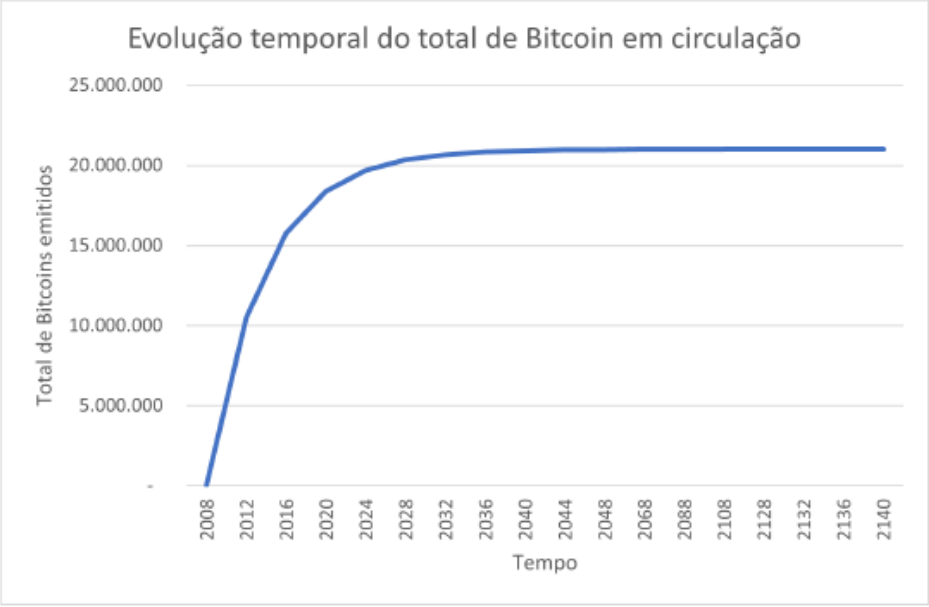


Figura 11 – Evolução temporal do total de bitcoin em circulação. Fonte: (Gonzaga, 2021)

A Figura 11 acima ilustra a evolução temporal do número total de bitcoins minerados.

2.2 ETHEREUM

Nessa seção será abordado de maneira inicial a blockchain da Ethereum. Será destacado em uma subseção os contratos inteligentes, onde será discutido suas principais características, além de mencionar o padrão ERC20.

A rede Ethereum surgiu após divergência entre Vitalik Buterin, um programador e co-fundador da Bitcoin Magazine, e a comunidade da rede Bitcoin em 2013, como pode ser visto em (O que é Ethereum, 2020). Vitalik Buterin queria implementar uma linguagem de programação que possibilitasse a criação de aplicativos descentralizados na rede Bitcoin. Como não foi possível chegar a um acordo com a comunidade, ele iniciou o desenvolvimento de uma nova rede baseada em blockchain que passou a ser chamada de Ethereum, que possui como moeda a ether, também conhecida pela sigla ETH.

> A Ethereum foi lançada em 2015 com um fornecimento inicial de 72 milhões de ether. Mais de 50 milhões desses tokens foram distribuídos em uma venda pública de tokens chamada de Initial Coin Offering (ICO) , onde aqueles que desejavam participar podiam comprar tokens ether em troca de bitcoins ou moeda fiduciária. (O que é Ethereum, 2020).

A rede Ethereum apresentou como nova funcionalidade os contratos inteligentes (smart-contracts), que são programas que são implementados e executados na blockchain da Ethereum e que podem ser usados para, por exemplo, fazer uma transação se determinadas condições forem atendidas.

> “Simplificando, a principal ideia por trás da Ethereum é que os desenvolvedores podem criar e lançar códigos que são executados em uma rede distribuída e não em um servidor centralizado. Isso significa que, em tese, esses aplicativos não podem ser desativados ou censurados”. (O que é Ethereum, 2020)

A liberdade que os desenvolvedores possuem para implementar e executar seus programas na blockchain da Ethereum é um fator importante que diferencia essa rede da rede Bitcoin.

A Bitcoin é considerada uma rede da primeira geração, que não possui um sistema extremamente complexo e que isso é um ponto positivo quando se trata de segurança. Além disso, a linguagem de contrato inteligente da Bitcoin é

extremamente restrita e não acomoda bem as aplicações que estão fora das transações.

Por outro lado, a Ethereum é a primeira blockchain da segunda geração e continua sendo a mais proeminente até hoje. Essa blockchain permite, além das transações financeiras, um grau de programação de maior complexidade. Desta forma, ela oferece aos desenvolvedores muito mais liberdade para experimentar seus próprios códigos e criar o que chamamos de Aplicações Descentralizadas (Dapps).

Assim como na rede Bitcoin, a ether, que é a moeda nativa da rede Ethereum, é criado após o processo de mineração.

> Ao contrário da Bitcoin, o cronograma de emissão de tokens da Ethereum, intencionalmente, não foi decidido no lançamento. A Bitcoin se propôs a preservar o valor, limitando sua oferta e diminuindo lentamente a criação de novas moedas. A Ethereum, por outro lado, visa fornecer uma base para aplicativos descentralizados (Dapps). Como ainda não está claro qual o tipo de programação de emissão de tokens se encaixa melhor nesse objetivo, essa questão permanece em aberto. (O que é Ethereum, 2020).

Portanto, percebe-se que a quantidade de ether's no mercado cripto ainda é algo controlável, pois o seu programa de emissão ainda está em aberto.

2.2.1 Contratos Inteligentes

Os contratos inteligentes aumentaram consideravelmente as possibilidades de aplicações da blockchain da Ethereum. Todavia, eles também foram baseados em tecnologias que já existiam e que estão disponíveis para o uso da população em geral.

Como exemplo, as máquinas de vendas automáticas existem desde 1920 e podem ser vistas como os ancestrais dos aplicativos e contratos inteligentes agora em execução na blockchain Ethereum, permitindo o surgimento das finanças descentralizadas, ou DeFi. Veja a Figura 12 abaixo, que ilustra uma máquina de venda automática.

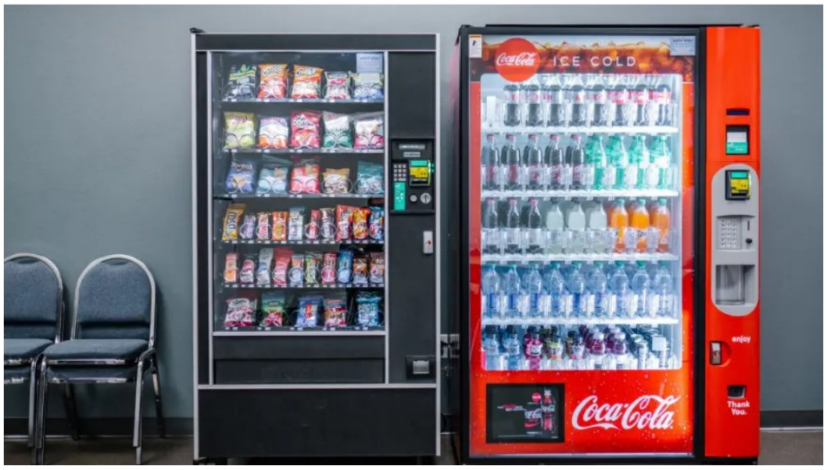


Figura 12 – Máquinas de venda automática

Desta forma, em vez de ir até um estabelecimento comercial para comprar uma bebida, o cliente pode interagir diretamente com uma dessas máquinas de venda automática para adquirir o produto desejado. Para isso o cliente precisa cumprir certos requisitos, como introduzir uma moeda ou cédula na máquina. Feito isso, a máquina, que possui uma programação de antemão, verifica se o dinheiro que o cliente colocou está de acordo com o valor do produto escolhido e, caso positivo, libera o produto ao cliente. Com isso, encerra-se a compra.

Se por algum motivo a máquina não conseguir identificar a quantia inserida pelo cliente ela retorna o valor inserido e, desse modo, a negociação não se concretiza.

Nick Szabo introduziu os contratos inteligentes na década de 1990. Na época, ele definiu um contrato inteligente como uma ferramenta que formaliza e protege redes de computadores combinando protocolos com interfaces de usuário.

> No mundo das criptomoedas, podemos definir um contrato inteligente como um aplicativo ou programa que é executado em uma blockchain. Normalmente, eles funcionam como um contrato digital que é aplicado com um conjunto específico de regras. Essas regras são predefinidas por código de computador, que é replicado e executado por todos os nodes da rede. (O que são Contratos Inteligentes, 2019).

Desta forma, (Prates, 2022) afirma que “o DeFi é como um setor completo onde várias máquinas automatizadas, agora digitais, podem ser usadas para

entregar não refrigerantes, mas serviços e produtos financeiros". Assim, é possível realizar, por exemplo, um empréstimo num ambiente DeFi, de forma semelhante como se faz numa agência bancária.

Normalmente, para se efetuar um empréstimo num banco a instituição bancária faz toda uma análise do negócio, como perfil do cliente, prazo do empréstimo, taxa de juros para liberar o empréstimo, além de ser utilizado moeda fiduciária no negócio. No caso de um empréstimo feito num ambiente DeFi, basta que o interessado aceite as condições de um contrato inteligente para realizar o negócio. Neste caso, o empréstimo é realizado com tokens (criptomoedas).

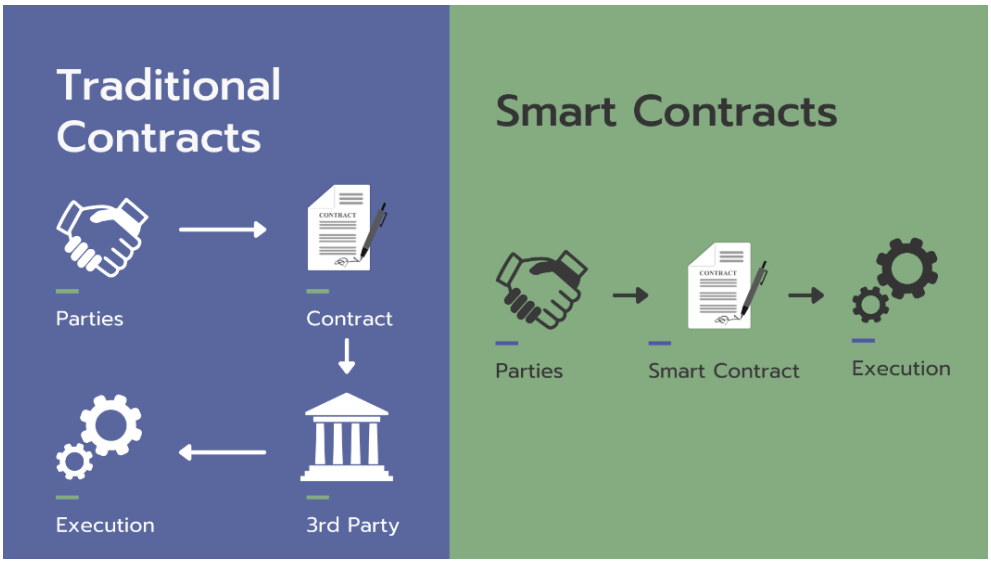


Figura 13 – Contrato Tradicional x Contrato Inteligente. Fonte: https://originstamp.com/blog/what-is-ethereum-and-what-are-its-use-cases/

A Figura 13 acima ilustra a diferença nas etapas seguidas em um contrato tradicional e em um contrato inteligente. Considere o exemplo 3 a seguir, adaptado de (Prates, 2022).

Exemplo 3: Digamos que José queira comprar um token não-fungível (NFT) de US$ 5.000 que acredita que aumentará de valor, mas não tem dinheiro suficiente para fazer a compra. Um empréstimo bancário de alguns milhares de dólares gera custos de transação consideráveis. Em vez disso, José poderia ir a uma das máquinas de venda automática no DeFi e usar alguns criptoativos que já possui como garantia para obter um empréstimo em criptoativos que melhor atenda às suas necessidades. A quantia emprestada seria então imediatamente entregue em sua carteira digital e, no período acordado, automaticamente

retirada da mesma carteira digital, acrescida de juros, tudo configurado pela máquina de venda automática digital de sua escolha.

Principais características dos contratos inteligentes

As principais características dos contratos inteligentes, geralmente, são:

- *distribuído*, ou seja, são replicados e distribuídos em todos os validadores da rede Ethereum;
- *determinísticos*, isto é, executam apenas as ações para as quais foram projetados, levando em conta os requisitos a serem cumpridos;
- *autônomos*;
- *imutáveis*;
- pesonalizáveis;
- trustless, ou seja, duas ou mais partes podem interagir através de contratos inteligentes sem a necessidade de se conhecerem ou de confiar uns nos outros;
- *transparentes*.

Essas características podem ser vistas como vantajosas ou desvantajosas, dependendo da análise que se faz.

- Vantagens: ser imutável e autônomo pode ser muito positivo a partir do momento que o contrato inteligente funciona bem e de acordo com o esperado.
- Desvantagens: se alguma funcionalidade não executar o esperado, essas características podem gerar um problema grave, como veremos no caso a seguir.

Em 2016, milhões de ether (ETH) foram roubados devido a falhas no código de um contrato inteligente, segundo (O que são Contratos Inteligentes, 2019). Como o contrato inteligente era imutável, não foi possível corrigir o código e a rede Ethereum sofreu um hard fork (bifurcação), ou seja, ela acabou sendo

dividida em duas outras cadeias. Isso, no entanto, foi uma medida extrema para um evento excepcional, que não ocorre normalmente.

Em uma dessas cadeias as transações ilegais foram efetivamente revertidas e essa cadeia deu origem a segunda blockchain da rede Ethereum. A outra cadeia decidiu não interferir nas consequências do ataque, afirmando que o que acontece numa blockchain nunca deve ser alterado. Essa cadeia passou a ser conhecida como blockchain da Ethereum Classic.

O roubo citado acima não teve origem na blockchain Ethereum. Ele foi causado por uma implementação defeituosa de contrato inteligente. Com isso, é sempre bom lembrar que:

> Contratos inteligentes são feitos por códigos de computador criados por humanos. Isso acaba trazendo alguns riscos, uma vez que o código está sujeito a vulnerabilidades e bugs. Em um cenário ideal, eles devem ser escritos e usados por programadores experientes, especialmente quando envolvem informações confidenciais ou muito dinheiro. (O que são Contratos Inteligentes, 2019)

Portanto, as principais características dos contratos inteligentes revolucionam certos tipos de negócios, principalmente nas transações de fundos entre partes, assim como apresentam limitações, como no exemplo acima do roubo de milhões de ether (ETH).

Tokens ERC20

A rede Ethereum, por ser mais flexível, permite que muitos desenvolvedores executem seus aplicativos descentralizados (Dapps) nela. Para garantir compatibilidade e interoperabilidade entre esses Dapps, foi desenvolvido um padrão para criação de projetos conhecido pela sigla ERC20, que significa Ethereum Request Comments. Esse padrão de criação é composto por documentos técnicos que normalizam a programação utilizada na rede Ethereum. O número 20 é o identificador dessa documentação.

Desta forma, os contratos inteligentes implementados na rede Ethereum seguem o padrão ERC20. Existem contratos inteligentes que desempenham as

mais diversas tarefas na rede Ethereum. Com isso, abriu-se a possibilidade de criação de tokens ERC20, e atualmente existem muitos deles. Há, inclusive, tokens desenvolvidos no padrão ERC20 de redes secundárias da Ethereum.

Os tokens ERC20 são executados na blockchain da Ethereum, mas existem apenas dentro de um contrato inteligente que determina as regras para o seu funcionamento, diferentemente da ether (ETH), que é a criptomoeda nativa da Ethereum.

De acordo com (Coinext, 2022), para serem criados, os tokens ERC20 precisam atender ao seguinte conjunto de parâmetros obrigatórios:

- TotalSupply, que retorno o fornecimento total de tokens;
- BalanceOf, que retorna o saldo de um endereço;
- Transfer, que transfere tokens de um endereço para outro;
- TransferFrom, que também é usado para transferência, porém para permitir que um terceiro mova fundos do seu endereço. Ou seja, Alice pode autorizar Bob a transferir fundos que pertence a ela;
- Approve, que limita a quantidade de tokens que um contrato pode retirar de um endereço;
- Allowance, que verifica se o endereço tem saldo suficiente para enviar tokens para outro endereço.

Além desses parâmetros obrigatórios, existem três funções opcionais que podem ser incluídas para aperfeiçoar o contrato:

- Name, que adiciona um nome legível ao token;
- Symbol, que associa um símbolo ao token;
- Decimal, que define até quantas casas decimais o token pode ser dividido.

Os tokens ERC20 não podem ser minerados, diferentemente da ether. Eles possuem um protocolo e cronograma de distribuição estabelecidos em seus projetos e implementados nos contatos inteligentes.

2.3 PONTES ENTRE BLOCKCHAINS

Nessa seção será introduzido o processo de interação entre duas blockchains, que possui considerável importância para o desenvolvimento do mercado cripto.

Quando uma pessoa envia um arquivo de um computador para outro, seja usando algum drive ou até mesmo a internet, essa informação não é de fato enviada, ela é copiada de um computador para o outro. Isso, antes da invenção da blockchain junto com a bitcoin, impossibilitava a criação de uma moeda digital sem intermediários.

Perceba que, em tais condições de envio, se o dinheiro fosse enviado de um computador para outro, ele seria copiado. Neste caso, o que impediria que ele fosse utilizado mais de uma vez, uma vez que ele agora está sob posse do remetente e do destinatário? Esse problema era chamado de gasto duplo. As blockchains resolveram o problema do gasto duplo, pois eram capazes de registrar de maneira descentralizada, e sem intermediários, a posse de um ativo digital de uma conta que apenas a pessoa com acesso à sua chave privada teria o seu controle.

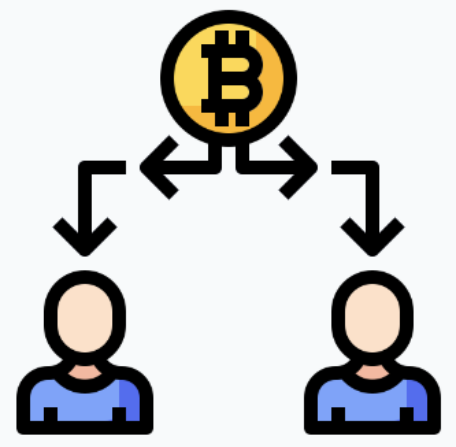


Figura 14 – Problema do gasto duplo.

Não demorou para que as pessoas entendessem que além do dinheiro, outras informações poderiam ser registradas em formas de ativos digitais e pudessem ser transferidas de um ponto para outro. Conforme as aplicações foram sendo desenvolvidas diferentes tipos de blockchain também surgiram para dar conta dessa demanda.

Qualquer certificado digital, também chamados de tokens, que pudessem dar acesso às votações, representar algum valor, ou ter a utilidade em jogos, fazer o papel de tickets para acessos às experiências virtuais ou reais, entre outros exemplos, poderiam ser registrados em blockchain e mantidos em posse, vendidos ou transferidos por qualquer pessoa que tivesse uma conta nessa blockchain.

Com o passar do tempo, apesar de algumas atualizações, a comunidade da bitcoin foi a que mais resistiu às mudanças, tentando deixar o projeto mais simples e parecido com a proposta inicial. A resistência à mudança da bitcoin fez com que muitas outras blockchains fossem surgindo com diferentes funções.

As blockchains de contratos inteligentes, sendo a Ethereum a primeira e a maior delas até hoje, surgiram com a função de ser um pouco menos simples e poder ser mais uma blockchain programável que executa tarefas automaticamente através dos contratos inteligentes.

A partir do desenvolvimento dessa segunda geração de blockchain, uma série de outras blockchain foram surgindo, visando atuar em nichos específicos ou tentando resolver o que entendiam ser problemas nessas outras blockchains originais. Muitas delas buscam soluções de escalabilidade, como as soluções de segunda camada das blockchain principais.

No caso da bitcoin, temos a Lightning Network, e da Ethereum, uma grande diversidade de soluções e projetos diferentes já foram criados, como a Polygon. O universo das blockchains ficou tão grande que hoje temos blockchains formadas ou interligadas com outras blockchains, como no caso da Polkadot, Avalanche e Cosmos, que permitem que outras blockchains personalizadas para diferentes funções sejam instaladas nelas, servindo como uma camada de base.

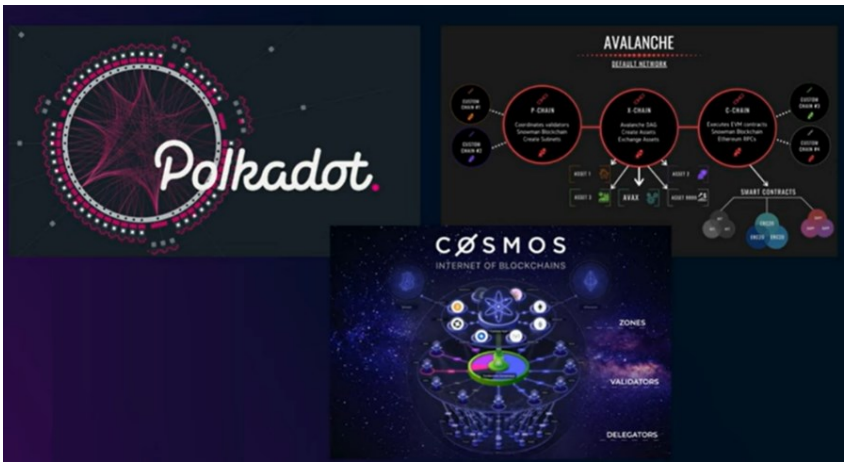


Figura 15 – Blockchains interligadas.

De forma geral, a vantagem dessa estrutura é poder oferecer uma camada de base ligada à segurança e criar blockchains personalizadas e específicas para certas aplicações que potencializam o desempenho para o qual elas foram projetadas, como as blockchains específicas para DeFi ou jogos, por exemplo.

Por outro lado, ainda temos muitas blockchains que não se comunicam, e com o surgimento de tantas blockchains isoladas umas das outras, foram desenvolvidas uma série de soluções para integrá-las e facilitar a transferência de valor de uma rede para outra. As pontes (bridges) são uma dessas soluções que permitem enviar token de uma blockchain para outra. Os tokens enviados são travados em um contrato inteligente na blockchain de origem e liberados na blockchain de destino por outro contrato inteligente nessa outra blockchain.

> A blockchain bridge é um protocolo que conecta duas blockchains separadas, econômica e tecnologicamente, para permitir interações entre elas. Esses protocolos funcionam como uma ponte que liga uma ilha a outra, sendo que as ilhas, neste caso, são ecossistemas blockchain separados. (Blockchain Bridge, 2022)

Existem diferentes tipos de pontes e transações possíveis. Esse processo pode ser automatizado e transparente, sem a necessidade de confiança. Porém, em alguns casos, isso não é tão fácil e pode exigir um tempo maior e até mesmo certo nível de confiança em uma empresa centralizada. Mesmo em caso de redes muito compatíveis, esse processo não é instantâneo, pois depende de uma série de confirmações em ambas as blockchains para aumentar a

segurança do processo. Por isso, normalmente se leva alguns minutos, até mesmo algumas horas, para uma transação poder ser completada.

Quando um token que se deseja enviar não é compatível na blockchain de destino, ele pode ser entregue na forma de um token sintético, ou seja, um outro token diferente do enviado, mas que representa o original, e que é registrado na blockchain de destino. Como exemplo, tem-se o WBTC que representa a bitcoin na rede da Ethereum, e o WETH que representa a ether em diferentes redes como a Polygon.

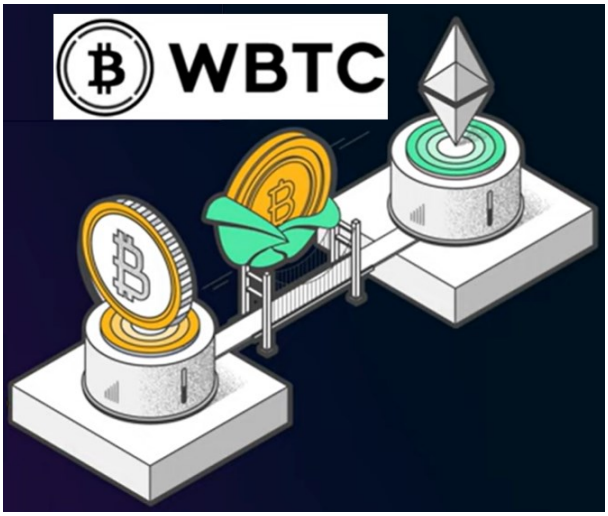


Figura 16 – Token sintético da bitcoin na rede Ethereum.

Se o protocolo for honesto e seguro esse token estará lastreado pelo valor travado na ponte do outro lado e pode ser resgatado a qualquer momento. Porém as pontes sempre foram uma estrutura mais frágeis no ecossistema das blockchains. Diversos ataques que causaram grandes prejuízos aconteceram nelas. Segundo (CoinDesk, 2023), em 2022 foram mais de 3,7 bilhões de dólares perdidos e boa parte desse montante foi roubado em ataques às pontes entre blockchains.

Apesar de muitas blockchains estarem num processo de desenvolvimento e testes, muitos apostam que o futuro do nosso sistema será multichain, com diferentes blockchains para diferentes funções. Um iniciante muitas vezes utiliza uma rede ou poucas delas, porém com o tempo é interessante que procure estudar outras redes onde poderá encontrar boas oportunidades. Para isso é importante que aprenda a transferir seus fundos entre blockchains.

3. CARTEIRAS E CORRETORAS DE CRIPTOMOEDAS

Este capítulo será dividido em três seções. A seção 3.1 tratará sobre carteiras de modo geral, sem aprofundar a discussão em algum caso particular. O intuito é realçar as principais características de uma carteira e, principalmente, aspectos sobre sua segurança. Quanto às corretoras, pretende diferenciar as corretoras centralizadas (CEX's) das corretoras descentralizadas (DEX's), destacando suas principais características.

No caso das corretoras centralizadas, tema visto na seção 3.2, não será discutido mais profundamente nenhum caso particular, pois esse tipo de corretora não está diretamente ligado com o foco deste trabalho, apesar de ser um caminho possível para se alcançar um dos objetivos específicos que é a montagem de uma piscina de liquidez.

Para as corretoras descentralizadas, na seção 3.3, será realçado suas principais características e nos aprofundaremos no funcionamento da Uniswap, que é a DEX utilizada como exemplo para montar uma piscina de liquidez, além de ser utilizada para discutir matematicamente a dinâmica de funcionamento das piscinas de liquidez.

3.1 CARTEIRAS DE CRIPTOS

Qualquer pessoa que deseja adquirir criptomoedas inevitavelmente vai precisar interagir com uma carteira de criptomoedas. Isso porque uma carteira de criptomoedas é uma ferramenta que permite que o usuário interaja com as redes blockchains, acessando e transferindo as suas moedas de forma segura. Nessa seção será mostrado os principais aspectos da transição do mundo físico, onde as pessoas usam carteiras de couro, para o mundo digital, onde as carteiras são dispositivos (hardware ou software).

Mas, afinal, o que é uma carteira de criptomoedas? Uma carteira de criptomoedas é um dispositivo físico (hardware) ou um programa de computador (software) que serve para você acessar, enviar e receber criptomoedas e ativos digitais. Esses dispositivos têm foco total em segurança, afinal, são responsáveis pelo acesso aos fundos em cripto e, por isso, utilizam tecnologia criptográfica.

O usuário pode imaginar uma carteira cripto como uma conta bancária por onde ele consegue acessar os produtos e serviços de sua instituição financeira. Porém, ao contrário das contas bancárias onde o banco fica com a posse do seu dinheiro, algumas das carteiras criptografadas permite que o usuário mantenha o controle total sobre os seus fundos.

Talvez seja intuitivo achar que as criptomoedas fiquem guardadas dentro de uma carteira de criptomoedas, assim como as moedas fiduciárias ficam guardadas dentro da carteira de couro, por exemplo. Contudo, na verdade não é assim que funciona. As criptomoedas ficam armazenadas na blockchain e a carteira de criptomoedas guardam e protegem suas senhas que dão acesso às suas criptomoedas na blockchain. Por isso que as criptomoedas de todos os detentores oscilam de preço conforme a variação do mercado, independentemente se elas forem negociadas por algum proprietário ou não.

Carteiras não custodiantes x Carteiras custodiantes

Ao interagir com uma carteira de criptomoedas o usuário terá acesso há, no mínimo, duas chaves, que são a chave pública e a chave privada. A chave pública é aquela que o usuário utiliza para receber criptomoedas. Ela pode ser disponibilizada para outras pessoas com tranquilidade. A chave privada é aquela que o usuário utiliza para acessar à sua carteira e movimentar as suas criptomoedas. A chave privada, como o próprio nome já diz, deve ser mantida sob sigilo.

Dependendo da carteira que o usuário escolher para interagir, além das chaves pública e privada, ainda há a possibilidade de o usuário ter sob sua posse a chave de recuperação da sua carteira, que também é conhecida como *seed* (semente). A seed é composta por 12 ou 24 palavras e é utilizada para recuperar o acesso à carteira do usuário que, por exemplo, esqueceu a chave privada. A seed também deve ser mantida em sigilo.

As carteiras que disponibilizam a seed para o usuário são chamadas de carteiras não custodiantes. Ao optar por esse tipo de carteira, o usuário é o único responsável pelo armazenamento e segurança das chaves de acesso aos seus

fundos. Por outro lado, as carteiras que não disponibilizam a seed para os usuários são chamadas de carteiras custodiantes. Essas carteiras são disponibilizadas por empresas que detêm as chaves privadas e tem o controle e o acesso sobre os fundos dos usuários. As corretoras centralizadas, que serão apresentadas na próxima seção, prestam serviço com carteiras custodiantes.

Perceba que ao abrir uma conta numa corretora centralizada, não há as 12 ou 24 palavras para serem anotadas. Por isso se fala tanto em escolher uma corretora centralizada segura, porque deixando suas criptos sob os cuidados da corretora, o usuário tem que confiar que estão gerenciando seus fundos da maneira adequada, sem risco de perder os seus ativos devido a fraudes, falência, ou até mesmo ataque hacker. Já as carteiras não custodiantes oferecem ao usuário controle total sobre as suas chaves privadas e seus fundos.

Quando uma pessoa escolhe interagir com uma carteira não custodiante, uma das primeiras coisas que ocorre no processo de configuração da carteira é a criação da seed. A partir da criação da seed são geradas uma chave privada e uma chave pública. Veja um exemplo fictício de uma seed na Figura 17 abaixo.

Figura 17 – Exemplo fictício de uma seed.

Caso você perca o acesso à carteira, ou ao dispositivo, ou celular onde você instalou a sua carteira, você pode fazer o backup usando essas palavras, na sequência correta, em outro dispositivo e recuperar toda a sua conta, os endereços e saldos.

Desta forma, é extremamente importante que o usuário tenha a seed em segurança, porque qualquer pessoa com a sua *seed* pode acessar seu saldo e

roubar seus fundos sem sequer precisar do seu celular ou dispositivo. Se o usuário, por acidente, cometer um pequeno erro ortográfico ou tiver com dificuldade de entender uma ou mais letras de alguma(s) palavra(s) da seed, ainda é possível reaver a escrita correta. A página dada no link abaixo

https://github.com/bitcoin/bips/blob/master/bip-0039/english.txt

disponibiliza, em ordem alfabética, todas as 2048 palavras possíveis que podem estar presentes na formação de uma seed. Veja a Tabela 1 abaixo que mostra as três primeiras e três últimas palavras.

Posição	Palavra
1°	abandon
2°	ability
3°	able
⋮	⋮
2046°	zero
2047°	zone
2048°	zoo

Tabela 1 – Lista das palavras que podem compor uma seed.

Se por acaso o usuário se descuidar e perder essas palavras de recuperação, vai perder também a possibilidade de fazer backup da sua carteira. É dessa forma que cerca de 30% das bitcoins mineradas podem estar perdidas para sempre, segundo (Barbosa, 2023).

No caso de optar por aderir a uma carteira não custodiante, o usuário se torna a única pessoa responsável pelos seus fundos, pois só ele possui acesso aos seus ativos. Nenhuma pessoa sem a chave privada e sem a seed conseguirá mexer em suas criptomoedas.

Além disso, algumas carteiras permitem que os usuários interajam com apenas uma criptomoeda, já outras tem soluções completas que oferecem suporte multimoedas e a vários aplicativos descentralizados. Os principais usos das carteiras são:

- manter ativos digitais em segurança;
- receber criptomoeda de outras pessoas;
- enviar criptomoedas para outras pessoas;

- pagar por produtos e serviços em estabelecimentos usando criptomoedas direto da própria carteira.

Além disso, algumas carteiras de criptomoedas mais avançadas fornecem recursos adicionais, como:

- conversões integradas ou swaps entre ativos digitais;
- conexão com soluções de terceiros baseadas em blockchain, como, por exemplo, os aplicativos de finanças descentralizadas;
- compra e venda de criptomoedas direto do aplicativo;
- opção de usar os ativos digitais em sua carteira com cartões pré-pagos;
- serviços de empréstimos e *stacking* de ativos digitais.

Existem dois tipos de carteiras no mercado cripto: as hot wallets (carteiras quentes) e as cold wallets (carteiras frias). Veja exemplos na Figura 18 abaixo.

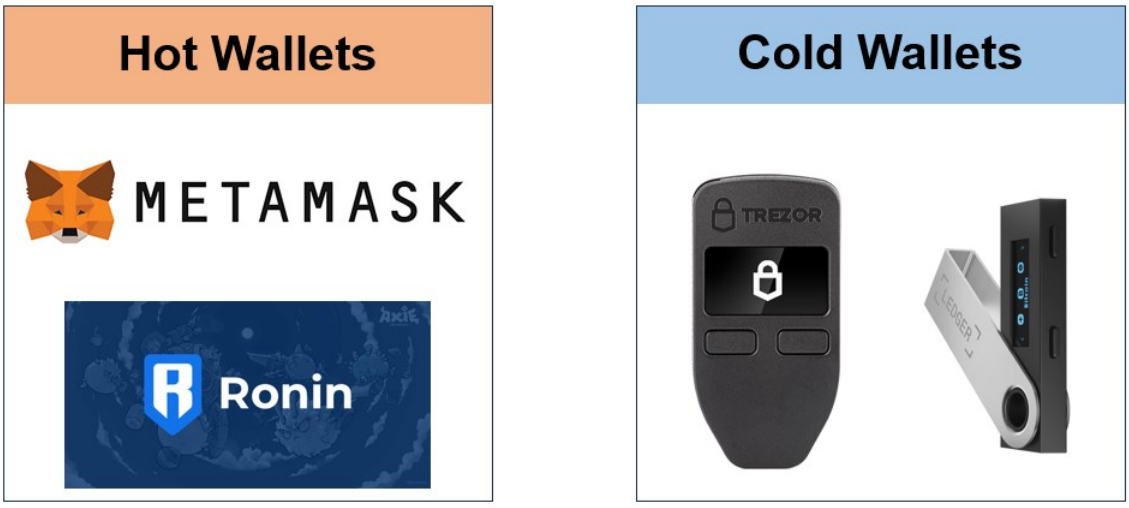


Figura 18 – Tipos de carteiras: hot wallets (carteiras quentes) e cold wallets (carteiras frias)

As carteiras hot wallets são conhecidas por ficarem sempre conectadas à internet. São incluídas nesse grupo as carteiras de desktop e as de celular. Na Figura 18 acima tem-se a MetaMask e a Ronin como exemplos de hot wallets. Já as cold wallets são as que ficam offline, como é o caso das hardware wallets, exemplificadas pela Trezor e pela Ledger na Figura 18.

Existem várias carteiras hot wallets à disposição do usuário. É importante os usuários analisarem minuciosamente aspectos como segurança, suporte para várias moedas, experiência de usuário, integração com outros aplicativos, reputação e privacidade para escolherem uma dessas carteiras.

De modo geral, as pessoas estão acostumadas a deixarem seu dinheiro na custódia de empresas bancárias, mas com a bitcoin e as outras criptomoedas existe a possibilidade de estar 100% no controle do próprio dinheiro. Guardar as chaves de acesso à sua própria carteira, sabendo que só você tem acesso a elas é libertador, porém, requer cuidados!

3.2 CORRETORAS CENTRALIZADAS (CEX's)

As corretoras de criptomoedas centralizadas, também conhecidas pela sigla CEX (Centralized Exchange), são corretoras dedicadas ao mercado de criptomoedas e seus usuários precisam realizar um cadastro nelas para terem acesso a uma variedade de ativos.

Essas corretoras funcionam como grandes mercados onde ficam vários produtos à disposição dos clientes. Contudo, nas corretoras são disponibilizadas várias criptomoedas que se encontram, cada uma, numa determinada rede, assim como no mercado os produtos ficam organizados em seções. Há redes que suportam somente uma criptomoeda, caso da rede Bitcoin, e há redes que suportam várias criptomoedas, caso da rede Ethereum.

Outra característica importante é que o preço de um ativo (criptomoeda) pode variar de CEX para CEX, da mesma forma que o preço de um produto pode variar de mercado para mercado. Cada CEX determina os ativos (criptomoedas) que quer negociar, assim como os mercados escolhem os produtos que querem vender. Isso significa que um mesmo ativo pode ser negociado numa CEX e em outra não, da mesma forma como um produto pode ser negociado num mercado e em outro não.

Quando o usuário opta por interagir com uma corretora centralizada (CEX), ele escolhe qual criptomoeda quer negociar, dentre as disponíveis naquela corretora. O acesso à rede onde se encontra a criptomoeda desejada pelo usuário é feito de forma automática pela corretora.

Para interagir pela primeira vez com uma corretora centralizada (CEX) o usuário precisa transferir moeda fiduciária para a corretora e depois adquirir as

criptomoedas do seu interesse, ou transferir/receber criptomoedas de outra carteira para a sua conta da corretora.

Algumas características marcantes das CEX's são:

- obrigatoriedade do KYC (Know Your Customer);
- livro de ofertas para as transações;
- maior credibilidade das moedas oferecidas;
- custódia das chaves de acesso aos ativos.

O KYC

O usuário interessado em interagir com uma CEX precisa realizar um cadastro conhecido pela sigla KYC (Know Your Customer). Essa identificação inicial do usuário é uma importante característica das CEX's. Como é possível ver em (O que é KYC, 2021), o KYC é um instrumento de combate a fraudes financeiras, como lavagem de dinheiro, e que garante a legalidade do usuário.

O livro de ofertas

O livro de ofertas é o local onde constam os valores de compra e de venda das criptomoedas que os usuários desejam negociar. Ou seja, o usuário que possui uma criptomoeda e deseja vendê-la, estipula um valor de venda que fica registrado no livro de ofertas. De forma análoga, o usuário que deseja comprar uma criptomoeda estipula um valor de compra que fica registrado no livro de ofertas.

Para que ocorra a negociação é necessário que se tenha um usuário interessado em vender uma criptomoeda por um preço X e outro usuário interessado em comprar a mesma criptomoeda pelo mesmo preço X. Enquanto o valor de venda e de compra não convergirem, a negociação não ocorre.

Criptomoedas com mais credibilidade

Nas CEX's, normalmente há um número considerável de criptomoedas para serem negociadas. Porém, nem todas as criptomoedas ficam disponíveis em todas as CEX's. Isso porque cada CEX possui seus próprios critérios de inclusão de uma criptomoeda em sua plataforma.

Antes de serem incluídas nas principais CEX's do mercado, as criptomoedas costumam passar por auditorias que avaliam os seus projetos e aprovam, ou não, sua listagem na corretora. Dentre os critérios avaliados está a liquidez de uma criptomoeda. Essa liquidez indica o quão rápido (fácil) é, ou não, negociar uma criptomoeda. Considera-se que quanto mais rápido (fácil) for para negociar uma criptomoeda, maior será a liquidez dela.

Custódia das chaves de acesso às criptomoedas

A chaves de acesso às criptomoedas negociadas numa CEX fica sob custódia da própria corretora. Essa é uma característica marcante das CEX's. Essas corretoras investem bastante em segurança, até porque o acesso a todos os ativos dos seus usuários ficam sob custódia delas.

Entretanto, é exatamente o fato de as corretoras terem a custódia das chaves de acesso dos ativos negociados pelos seus usuários que as torna mais propensas à ataques cibernéticos. Afinal, uma pessoa que conseguir invadir o sistema de uma dessas corretoras, terá acesso aos saldos dos usuários e, provavelmente, causará um dano financeiro irreversível.

3.3 CORRETORAS DESCENTRALIZADAS (DEX's)

As corretoras de criptomoedas descentralizadas, também conhecidas pela sigla DEX (Descentralized Exchange), surgiram a partir do advento das blockchains.

A falta de flexibilidade de interação com o código da rede Bitcoin foi um fator importante para o surgimento da rede Ethereum, que, por sua vez, é altamente flexível para interagir com outros códigos (contratos inteligentes)

desenvolvidos pelos seus usuários. À medida que a rede Ethereum foi crescendo, muitas aplicações foram surgindo. Dentre elas, estão as corretoras descentralizadas (DEX's).

Quando o usuário opta por interagir com uma corretora descentralizada (DEX), ele escolhe a rede na qual quer se conectar e, então, busca a criptomoeda desejada na rede escolhida. Essa busca pelo ativo desejado pelo usuário não acontece de forma automática como nas corretoras centralizadas (CEX's).

Para interagir pela primeira vez com uma corretora descentralizada (DEX) o usuário precisa possuir uma carteira de criptomoedas e conectá-la a uma DEX que a suporte. Assim, os usuários podem optar pelos seguintes caminhos:

- adquirir criptomoedas numa corretora centralizada e transferi-las para uma carteira que seja suportada pela DEX de sua escolha;
- comprar criptomoedas diretamente de uma carteira e conectá-la a uma DEX de sua escolha que suporte tal carteira;
- receber criptomoedas de outro usuário, em uma carteira, e conectá-la a uma DEX de sua escolha que suporte tal carteira.

De forma semelhante como ocorre nas corretoras centralizadas (CEX's), nas corretoras descentralizadas (DEX's) os usuários também podem realizar trocas entre tokens (criptomoedas). Mas por que alguém usaria uma corretora descentralizada (DEX) ao invés de usar corretora centralizada (CEX)?

As corretoras descentralizadas dão a possibilidade de os usuários terem acesso à serviços como empréstimo de criptomoedas, ou até mesmo de atuarem como o próprio banco tradicional ao formarem ambientes de trocas de criptomoedas e receberem taxas por isso. Além disso, as DEX's trazem consigo características atraentes, como:

- maior privacidade;
- acesso a um maior número de criptomoedas;
- ausência do livro de ofertas;
- não custodiantes.

Maior privacidade

Os usuários das corretoras descentralizadas (DEX's) não precisam informar nenhum dado pessoal para interagir com essas plataformas, diferentemente daqueles que optam por utilizar as corretoras centralizadas (CEX's). Desta forma, o dinheiro dos usuários é muito menos rastreável e suas identidades são preservadas.

Para que haja a interação do usuário com uma DEX, basta que ele conecte uma carteira de criptomoedas à DEX e, assim, estará apto para utilizar suas funcionalidades.

Acesso a mais criptomoedas

As criptomoedas para serem listadas numa DEX não passam pelo mesmo critério de seleção que acontece numa CEX. Desta forma, o usuário das DEX's tem mais opções de moedas e não ficam restritos às criptomoedas oferecidas pelas CEX's.

Todavia, o usuário assume uma maior responsabilidade ao negociar criptomoedas com projetos em estágio inicial ou com menor liquidez, que ainda não foram listadas nas CEX's. Apesar de a listagem de uma criptomoeda nas CEX's não ser garantia de que ela será bem-sucedida, essa listagem pode servir como um parâmetro para usuários menos experientes.

Ausência do livro de ofertas

O tradicional livro de ofertas das corretoras centralizadas (CEX's) não aparece nas corretoras descentralizadas (DEX's). No caso das DEX's, os usuários realizam trocas de criptomoedas acessando indiretamente as piscinas de liquidez, que são ambientes específicos para troca de criptomoedas nas DEX's. Essas piscinas de liquidez são disponibilizadas por outros usuários da DEX que agem como bancos e recebem taxas por isso. O valor de troca é estipulado automaticamente e respeita a fórmula matemática estipulada pela DEX utilizada.

Não custodiantes

As corretoras descentralizadas (DEX's) não fazem custódia das chaves de acesso aos ativos dos usuários. Os usuários são os únicos responsáveis pelas suas criptomoedas e precisam de uma carteira para interagir com as DEX's.

3.3.1 Formador de Mercado Automatizado (AMM)

O Formador de Mercado Automatizado, também conhecido pela sigla AMM (Automated Market Maker), é um algoritmo de precificação utilizado pelas corretoras descentralizadas (DEX's).

Como já visto anteriormente, as DEX's não possuem livro de ofertas. Isso significa que seus usuários não estipulam valores de compra e de venda. Cada DEX utiliza uma função matemática que determina automaticamente o valor de troca entre criptomoedas.

As criptomoedas disponibilizadas para troca são fornecidas pelos próprios usuários que optam por bloquear seus ativos numa DEX, formando piscinas de liquidez, a fim de receber taxas à medida que outros usuários utilizam essas piscinas para realizarem trocas.

Por exemplo, a Uniswap, uma DEX que será mais detalhada na seção 3.3.2, utiliza nas suas duas primeiras versões, a fórmula $x \cdot y = k$, como pode ser visto em (Adams, 2018), sendo:

- x a quantidade de criptomoedas do ativo X;
- y a quantidade de criptomoedas do ativo Y;
- k uma constante.

Ou seja, o produto entre as quantidades dos ativos X e Y é igual a uma constante k. Além disso, segundo (Adams, 2018), tem-se que os $v_X \cdot x = v_Y \cdot y$, sendo:

- v_X o valor do ativo X;
- v_Y o valor do ativo Y.

Isto é, o valor depositado em ativo X na piscina é igual ao valor depositado em ativo Y na piscina. Veja o exemplo 4 abaixo simulando uma troca entre tokens por um usuário da Uniswap V2. Será utilizado o critério de arredondamento para duas casas decimais quando necessário.

Exemplo 4: Considere uma piscina de liquidez com os tokens (criptomoedas) ETH e SOL. Se cada ETH vale $80\ SOL$ e a piscina possuir $10\ ETH$, responda:

a) Quantos tokens SOL deve haver na piscina e qual é o valor de k inicialmente na piscina?
b) Se um usuário desejar trocar $1\ ETH$ por tokens SOL nessa piscina, quantos tokens SOL ele irá receber? Considere que o protocolo Uniswap cobre uma taxa de $0{,}25\%$ por transação como bonificação aos provedores de liquidez.
c) Qual o valor de k após a troca realizada no item anterior?

Solução (a): Como condição da DEX escolhida (Uniswap), a piscina precisa ter quantidades de tokens ETH e SOL de forma que o valor dessas quantidades seja equivalente. Se cada token ETH vale $80\ SOL$ e a piscina possui $10\ ETH$, então:

$$\frac{1\ ETH}{10\ ETH} = \frac{80\ SOL}{Quant.de\ SOL} \implies Quant.de\ SOL = \frac{10\ ETH \cdot 80\ SOL}{1\ ETH} = 800\ Sol\ .$$

Dessa forma, a piscina é composta inicialmente por:

$$10\ ETH \quad \text{e} \quad 800\ SOL\ .$$

Assim, tem-se que:

$$k = \underbrace{10}_{n°\ de\ ETH} \cdot \underbrace{800}_{n°\ de\ SOL} = 8.000\ \blacksquare$$

Solução (b): Como um usuário deseja trocar $1\ ETH$ por SOL nessa piscina e a DEX escolhida (Uniswap) cobra uma taxa de $0{,}25\%$ por transação como bonificação aos provedores de liquidez, tem-se que:

$$0{,}25\%\ de\ 1\ ETH = 0{,}0025\ ETH\ .$$

Os outros $0{,}9975\ ETH$ são imediatamente adicionados à piscina. Desta forma, a piscina passa a ter $10{,}9975\ ETH$. Com isso, precisa-se calcular a nova quantidade de tokens SOL na piscina, pois:

$$(Quant.de\ token\ ETH)\ \cdot (Quant.de\ token\ SOL) = k = 8.000\ .$$

Portanto,

$$Quant.de\ token\ SOL = \frac{8.000}{10{,}9975} \approx 727{,}44\ .$$

Logo, o comprador de token SOL receberá:

$$800\ SOL - 727{,}44\ SOL = 72{,}56\ SOL\ \blacksquare$$

Solução (c): A taxa de $0{,}0025\ ETH$ é adicionada à piscina de liquidez como bonificação ao provedor de liquidez após a transação do item (b). Dessa forma, o valor de k aumenta ligeiramente, visto que, após a troca realizada anteriormente, a piscina passa a ser composta por:

$$11\ ETH \quad \text{e} \quad 727{,}44\ SOL.$$

Consequentemente,

$$k = 11 * 454{,}65 = 5.001{,}15\ \blacksquare$$

Note que no exemplo 4 o comprador recebeu $72{,}56\ SOL$ por $1\ ETH$, mas, inicialmente, tinha-se na piscina a relação de $1\ ETH$ para cada $80\ SOL$. Isso significa que qualquer alteração das quantidades de tokens na piscina, altera a relação de valor entre os tokens. Isto é, quantos mais tokens ETH na piscina, menor será a quantidade de tokens SOL na piscina, e menor será o valor do token ETH em relação aos tokens SOL.

De modo geral, quanto maior for a variação das quantidades de tokens na piscina, maior será o impacto na relação entre os preços desses tokens na piscina.

Se ocorrer uma outra negociação nessa piscina, com um usuário desejando comprar tokens SOL com $1\ ETH$, ele receberá uma quantidade menor de SOL em relação ao primeiro comprador.

Em contrapartida, se o novo comprador desejar adquirir tokens ETH com tokens SOL, receberá uma quantidade maior de ETH caso tivesse feito essa negociação antes do primeiro comprador.

Desta forma, tem-se que numa corretora centralizada (CEX) os preços dos ativos flutuam à medida que os usuários colocam ordem de compra e de venda no livro de ofertas. Já nas corretoras descentralizadas (DEX'S) é o formador de mercado automatizado (AMM) que regula os preços dos ativos.

3.3.2 Uniswap

A Uniswap é uma corretora descentralizada que surgiu em novembro de 2018 e que foi ganhando cada vez mais destaque, ao longo do tempo, no mercado de criptos. A disponibilidade de listagem de novas moedas, o volume de dinheiro movimentado e uma maior segurança contra ataques hackers são alguns dos fatores que fizeram a Uniswap se tornar uma das principais corretoras de criptomoedas.

A Uniswap possui uma estrutura dividida em quatro áreas que se distinguem umas das outras, que são: Uniswap Labs, protocolo Uniswap, a interface Uniswap e governança Uniswap.

> "Uniswap Labs é a empresa que desenvolveu o protocolo Uniswap, juntamente com a interface web; O protocolo Uniswap é um conjunto de contratos inteligentes persistentes e não atualizáveis que, juntos, criam um criador de mercado automatizado, um protocolo que facilita a criação de mercado ponto a ponto e a troca de tokens ERC-20 no blockchain Ethereum; A interface Uniswap é uma interface web que permite fácil interação com o protocolo Uniswap. A interface é apenas uma das muitas maneiras de interagir com o protocolo Uniswap; Governança Uniswap é um sistema de governança para governar o protocolo Uniswap, habilitado pelo token UNI". (Visão geral do Uniswap, 2022)

Dentre as áreas da Uniswap citadas acima, será mais explorado nessa seção o protocolo Uniswap, mais especificamente seu funcionamento. Ao interagir com a Uniswap o usuário pode atuar basicamente de duas maneiras:

a) realizar troca entre tokens, mediante pagamento de taxa aos provedores de liquidez, isto é, àqueles usuários que atuam como o banco ao montarem as piscinas de liquidez.

b) fornecer liquidez e, consequentemente, ganhar taxas dos usuários que realizam trocas entre tokens.

No caso (a) é como se o usuário estivesse indo até um banco para trocar moedas, pagando taxa ao banco por isso. No caso (b) é como se o usuário fosse o próprio banco, recebendo taxa de outros usuários que realizam trocas entre tokens (criptomoedas) por fornecer liquidez à plataforma.

O protocolo Uniswap foi sendo atualizado desde o surgimento da plataforma e atualmente está na sua terceira versão. A seguir será apresentado os principais aspectos e avanços de cada uma dessas versões.

O Protocolo Uniswap V1

A Uniswap V1 é a primeira versão do protocolo, lançado em novembro de 2018, e sempre existirá enquanto o Ethereum existir, devido à sua natureza sem permissão, conforme pode ser visto em (Os Contratos Inteligentes Uniswap V1, 2022). A natureza sem permissão significa que:

> Os serviços do protocolo são totalmente abertos para o público, sem capacidade de restringir seletivamente quem pode ou não usá-los. Qualquer um pode trocar, fornecer liquidez ou criar novos mercados à vontade. Isso é diferente dos serviços financeiros tradicionais que normalmente restringem o acesso com base na geografia, status de riqueza e idade. (O Protocolo Uniswap, 2022)

Neste protocolo o usuário pode realizar trocas entre pares de tokens ETH – ERC20, ou fornecer liquidez depositando uma quantidade de ETH e um token ERC20 cujos valores sejam equivalentes, ou seja, 50% do valor da reserva em ETH e os outros 50% em ERC20, conforme visto na seção 3.3.1. Cada par de tokens ETH – ERC20 possui um contrato que determina a quantidade de cada token ao final de cada negociação solicitada pelos usuários da plataforma.

Desta forma, nesse protocolo o token ETH também funciona como token intermediário para realizar trocas, visto que não há contrato próprio para pares

de tokens que sejam exclusivamente ERC20 nesse protocolo. Conforme visto em (Adams, 2018), os usuários que desejam realizar troca entre tokens ERC20 precisam trocar o token ERC20, que já está sob sua posse, pelo token ETH, através do par de troca ERC20 – ETH, e depois trocar os tokens ETH pelos tokens ERC20 desejado inicialmente, através do par de trocas ETH – ERC20.

Sobre cada transação realizada nesse protocolo é cobrada uma taxa de 0,30%, que é adicionada à reserva de tokens, fazendo com que ela cresça a cada transação. Se o usuário realiza troca entre tokens exclusivamente ERC20, ele é taxado duas vezes, o que totaliza 0,60% da transação. Tais taxas são bonificações aos provedores de liquidez que passam a ser detentores delas de forma proporcional a liquidez fornecida por eles.

Assim, um usuário que deseja trocar o token DAI pelo token USDC precisa, necessariamente, trocar seus tokens DAI por tokens ETH e, posteriormente, solicitar nova troca dos tokens ETH, recebidos da negociação anterior, por tokens USDC. Note que nesse protocolo os provedores de liquidez necessariamente precisam se expor ao token ETH.

Como exemplo, considere os tokens ERC20 DAI e USDC, e suponha que um usuário que deseja trocar tokens DAI por tokens USDC. A Figura 19 abaixo ilustra a dinâmica dessa troca no protocolo Uniswap V1.

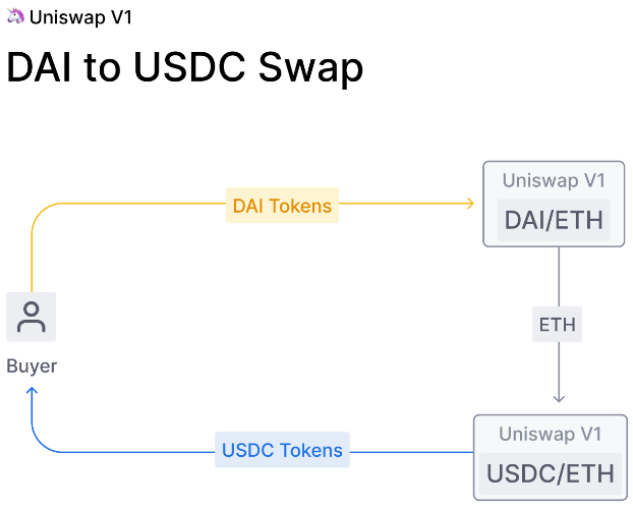


Figura 19 – Troca de tokens em Uniswap V1. Fonte: (Visão geral do Uniswap V2, 2020)

Outra característica desse protocolo é que não há privilégio entre tokens ou favorecimento a determinados investidores ou desenvolvedores. Tudo é regido pelos contratos que são públicos e iguais para todos.

> "Não há token central ou taxa de plataforma. Nenhum tratamento especial é dado aos primeiros investidores, adotantes ou desenvolvedores. A listagem de tokens é aberta e gratuita. Todas as funções do contrato inteligente são públicas e todas as atualizações são opcionais". (Os Contratos Inteligentes Uniswap V1, 2022)

A ausência de privilégios dos usuários ou ativos é uma característica necessária em um ambiente descentralizado, porém não suficiente. A Uniswap possui uma governança que pode, em algum momento, alterar as regras do seu protocolo.

O Protocolo Uniswap V2

O Uniswap V2, segunda versão do protocolo Uniswap, foi lançado em maio de 2020 com novos recursos e melhorias técnicas em comparação com o Uniswap V1, incluindo contratos para pares de tokens ERC20 – ERC20, oráculo de preços, flash swaps, etc. Tais melhorias proporcionaram ao protocolo Uniswap V2 se tornar uma das maiores corretoras de criptomoedas do mundo com um volume de negociação que alcançou mais de $135 bilhões, segundo (Uniswap, 2021).

Do ponto de vista dos provedores de liquidez, ter a possibilidade de fornecer liquidez diretamente para pares de tokens ERC20 – ERC20 elimina a exposição obrigatória ao token ETH e reduz a perda com base na mudança dos preços de outros ativos em relação ao ETH.

Para os usuários que desejam realizar trocas entre tokens, a possibilidade de ter os contratos para pares de tokens ERC20 – ERC20 pode melhorar os preços de negociação, visto que a troca entre dois tokens ERC20, passando necessariamente pelo token ETH como um token intermediário, envolve o pagamento de duas taxas de negociação, enquanto a troca entre tokens ERC20, sem usar o token ETH como intermediário, pode envolver apenas uma taxa de negociação.

Caso não haja um contrato para um par de tokens ERC20 – ERC20 específico, o protocolo Unisawp V2 ainda consegue realizar a troca desde que exista um caminho entre os tokens envolvidos. Os contratos de roteador podem ser usados para otimizar trocas diretas e de várias etapas. A Figura 20 abaixo ilustra as dinâmicas das possibilidades de trocas entre tokens no protocolo Uniswap V2.

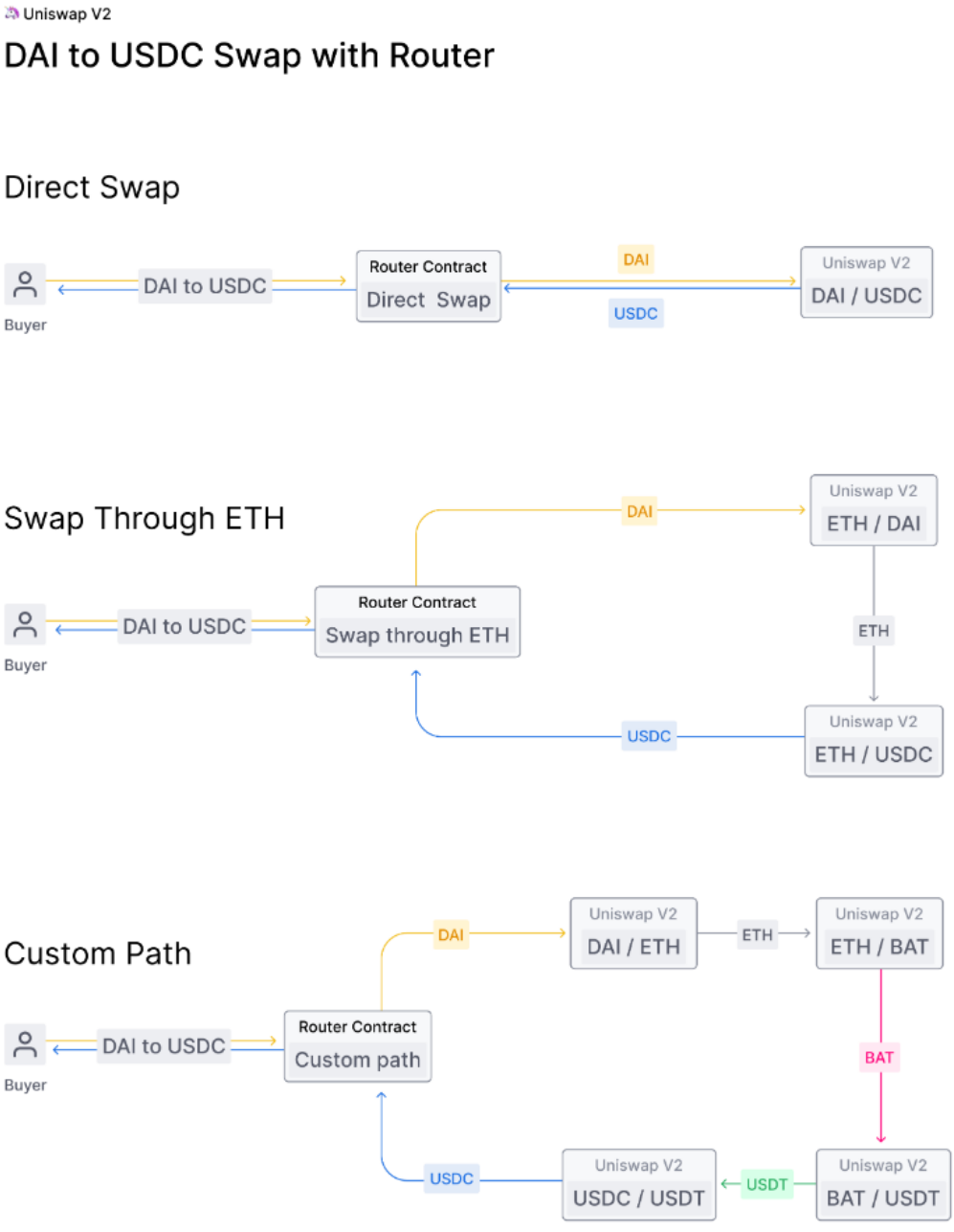


Figura 20 – Troca de tokens em Uniswap V2. Fonte: (Visão geral do Uniswap V2, 2020)

Como verifica-se acima, na troca direta entre tokens ERC20 temos os custos com taxas de negociação otimizados. Já nos casos de trocas envolvendo

o token ETH como intermediário ou trocas com caminho personalizado, o usuário consegue realizar trocas entre tokens ERC20 com apenas uma solicitação, ainda que as taxas de negociação não sejam reduzidas como na troca direta. Isso reduz a quantidade de interações do usuário com a plataforma.

O oráculo de preços e flash swaps, citados como melhorias do protocolo Uniswap V2, são novas funcionalidades que possibilitam resistência à manipulação de preços e "empréstimo" de tokens, respectivamente. Essas "ferramentas" e outras não citadas aqui, fogem do objetivo desse trabalho e por isso não serão detalhadas. Ao leitor mais interessado, indica-se a referência (Adams, Zinsmeister, & Robinson, 2023).

O Protocolo Uniswap V3

O Uniswap V3, lançado em março de 2021, foi idealizado imediatamente após o lançamento do protocolo V2, que teve recursos limitados e, consequentemente, sua infraestrutura de suporte ficou aquém do desejável. Para o protocolo V3, houve um planejamento para se gastar mais tempo criando ferramentas e produtos, melhorando a estrutura, conforme visto em (Uniswap V3 vs V2, 2023).

Essa nova versão do protocolo trouxe novidades em relação à versão anterior, como liquidez concentrada, taxas flexíveis, oráculo de preço aprimorado, etc.

Nos protocolos V1 e V2, a liquidez fornecida pelos provedores de liquidez era distribuída uniformemente ao longo da curva de reservas ($x \cdot y = k$), onde x representa a quantidade de um token X, y representa a quantidade de um token Y e k é uma constante.

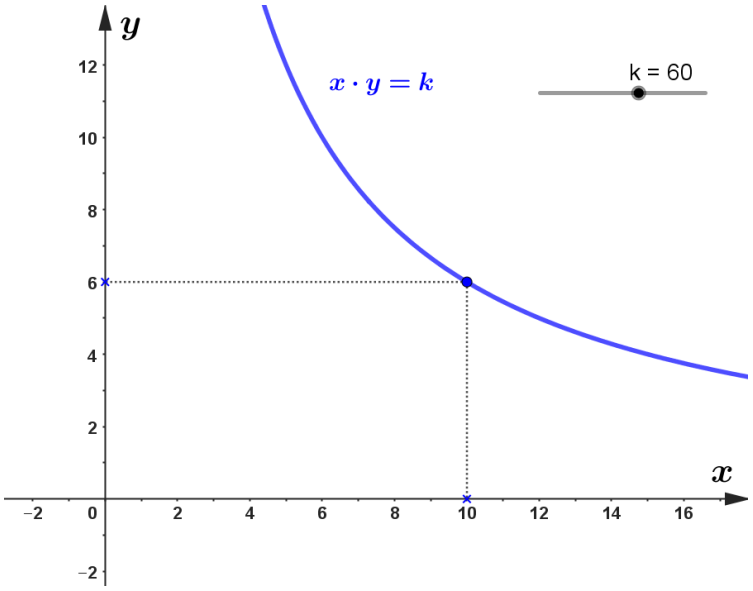


*Figura 21 – Exemplo da curva x*y=k utilizada nos protocolos Uniswap V1 e V2.*

A Figura 21 acima ilustra, graficamente, o comportamento da curva $x \cdot y = k$ utilizada nos protocolos Uniswap V1 e V2. Note que as quantidades de tokens X e Y podem variar no intervalo $(0, \infty)$.

> Em outras palavras, as versões anteriores foram projetadas para fornecer liquidez em toda a faixa de preço (0, ∞). Isso é simples de implementar e permite que a liquidez seja agregada de forma eficiente, mas significa que muitos dos ativos mantidos em um pool nunca são tocados. (Adams, Zinsmeister, & Salem, 2021)

Os idealizadores do protocolo Uniswap V3 questionam o fato do fornecimento de liquidez ocorrer ao longo de todo o intervalo $(0, \infty)$, como nos protocolos Uniswap V1 e V2. Como inovação, eles propõem um fornecimento de liquidez concentrado.

> Tendo considerado isso, parece razoável permitir que os LPs concentrem sua liquidez em faixas de preço menores que (0, ∞). Chamamos de posição a liquidez concentrada em um intervalo finito. Uma posição só precisa manter reservas suficientes para suportar a negociação dentro de sua faixa e, portanto, pode atuar como um pool de produtos constante com reservas maiores (chamamos de reservas virtuais) dentro dessa faixa. (Adams, Zinsmeister, & Salem, 2021)

Como exemplo, tem-se o caso particular do par de tokens, em Uniswap V2, DAI – USDC, cujos preços variam numa faixa entre \$0,99 e \$1,01. Neste caso, segundo (Uniswap, 2021), apenas $\approx 0{,}50\%$ da liquidez fornecida é

utilizada. Assim, não é vantajoso fornecer liquidez ao longo de toda a curva, se existe a possibilidade de concentrar a liquidez na faixa onde existe o maior volume de negociação entre os tokens, que é a proposta inovadora do protocolo V3.

No caso da liquidez concentrada, observamos em (Adams, Zinsmeister, & Salem, 2021) que o fornecimento de liquidez passa a ocorrer sobre a curva

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

sendo $L = \sqrt{k}$ e, p_a e p_b, os extremos do intervalo de preço $[p_a, p_b]$ onde a liquidez é fornecida. Veja abaixo os gráficos da curva com liquidez concentrada e da curva ao longo de todo intervalo $(0, \infty)$.

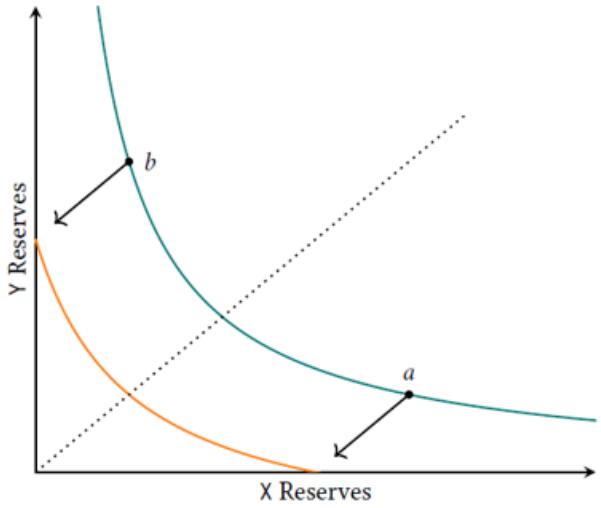


Figura 22 – Liquidez concentrada em Uniswap V3. Fonte: (Adams, Zinsmeister, & Salem, 2021)

Como podemos ver na Figura 22, a curva com liquidez concentrada, em laranja, é uma translação da curva $x \cdot y = k$, com liquidez ao longo do intervalo $(0, \infty)$, em verde.

Assim, considerando a curva de liquidez concentrada, se a razão entre o preço dos tokens variar para além do intervalo onde a liquidez é fornecida, seja para mais ou para menos, o provedor de liquidez passará a ter somente um dos tokens na piscina e deixará de receber taxas de negociação na plataforma enquanto a razão do preço dos tokens não retornar para a faixa de preço estipulada ao fornecer liquidez.

4. ASPECTOS MATEMÁTICOS EM PISCINAS DE LIQUIDEZ

Dentre alguns órgãos ou instituições que sofrem influência direta das regulamentações impostas pelo governo, estão as Casas de Câmbio. A atividade de uma Casa de Câmbio é, essencialmente, disponibilizar moedas para serem negociadas.

Para fins de exemplo, considere uma Casa de Câmbio que disponibiliza, além do real, algumas moedas internacionais, como dólar ou euro, para negociar com seus clientes. Assim, os turistas que chegam no Brasil podem trocar seus dólares ou euros por reais e, assim, realizarem suas atividades turísticas. Da mesma forma, os brasileiros que desejam viajar para os EUA ou Europa, podem trocar seus reais por dólar ou euro para utilizarem no país de destino. Assim, a Casa de Câmbio ganha taxas em cada negociação realizada.

A Piscina de Liquidez funciona de forma bem similar à uma Casa de Câmbio dada no exemplo anterior, porém, ela é um ambiente de troca de moedas digitais (criptomoedas) que se situa numa plataforma descentralizada que, por sua vez, dita as regras de transações via contrato inteligente.

Assim como numa Casa de Câmbio é possível negociar algumas moedas fiduciárias, nas piscinas de liquidez pode-se negociar diversas criptomoedas. No entanto, cada corretora descentralizada (DEX) possui um documento norteador (whitepapper) estabelecendo como ocorrem essas negociações. Na Uniswap, por exemplo, em cada piscina de liquidez existe somente um par de criptomoedas (tokens) disponíveis para serem negociadas. Em outras DEX's, como a Balancer ou GMX, é possível montar uma piscina de liquidez com mais de duas criptomoedas (tokens).

4.1 A PISCINA DE LIQUIDEZ DO UNISWAP V2

O protocolo Uniswap V2 é uma atualização do primeiro protocolo Uniswap. As equações do contrato inteligente que regem as negociações nas piscinas, no protocolo V2, são as mesmas utilizadas no primeiro protocolo Uniswap, e que foram apresentadas na seção 3.3.1. Ou seja, ao considerarmos

uma piscina de liquidez, na Uniswap V2, composta pelos tokens X e Y, tem-se duas equações que respeitam as seguintes condições:

I. O produto entre as quantidades dos tokens X e Y na piscina é sempre constante;
II. O valor total de tokens X na piscina é igual ao valor total de tokens Y na piscina, ou seja, cada token possui 50% do valor da piscina.

Tais condições estão representadas no sistema abaixo:

$$\begin{cases} x_t \cdot y_t = k & (1) \\ v_{X_t} \cdot x_t = v_{Y_t} \cdot y_t & (2) \end{cases},$$

sendo que, para cada instante t:

- x_t é a quantidade do token X;
- y_t é a quantidade do token Y;
- v_{X_t} é o valor de uma unidade do token X;
- v_{Y_t} é o valor de uma unidade do token Y.

Da equação (2), define-se:

$$V_t = v_{X_t} \cdot x_t + v_{Y_t} \cdot y_t \quad (3),$$

sendo V_t o valor total dos tokens na piscina num instante t.

Como x e y representam quantidades tais que $x \cdot y = k$, temos que $x \geq 0$, $y \geq 0$ e, consequentemente, $k \geq 0$. Os casos em que $x = 0$ ou $y = 0$ fazem a curva degenerar para os eixos y ou x, respectivamente. Se $x = 0$ e $y = 0$ a curva degenera para a origem $(0, 0)$ do plano cartesiano.

Nesse trabalho, será considerado o caso em que $x > 0$ e $y > 0$. Veja o gráfico da equação $x \cdot y = k$, na Figura 23 abaixo, para $k = 60$:

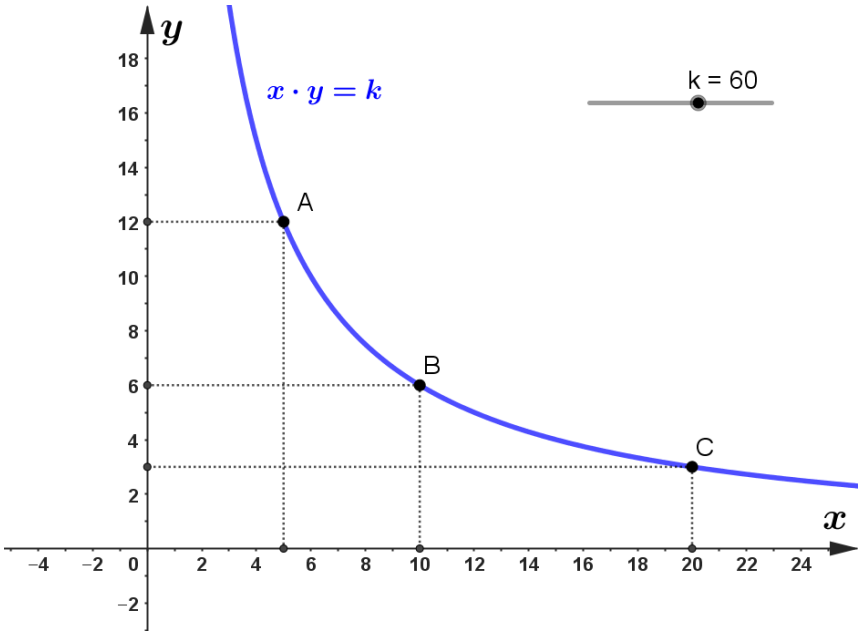


Figura 23 – Gráfico da relação entre as quantidades de tokens nas piscinas do Uniswap V2

Note que, na Figura 23, os valores e as quantidades dos tokens X e Y na piscina podem mudar ao longo do tempo t, mas sempre satisfazem a equação $x \cdot y = k$.

- No ponto A, tem-se 5 tokens X e 12 tokens Y. Logo, $k = 5 \cdot 12 = 60$.
- No ponto B, tem-se 10 tokens X e 6 tokens Y. Logo, $k = 10 \cdot 6 = 60$.
- No ponto C, tem-se 20 tokens X e 3 tokens Y. Logo, $k = 20 \cdot 3 = 60$.

No exemplo 4 da seção 3.3.1, foi visto como a interação dos usuários da Uniswap interfere nas quantidades e na relação de preço dos tokens na piscina à medida que eles realizam trocas.

É importante observar que as piscinas na Uniswap V2 sempre ficam disponíveis para o acesso dos usuários que desejam realizar trocas entre tokens nesse protocolo, independentemente da quantidade de tokens ou da relação de preço entre os tokens na piscina. No entanto, os usuários não escolhem qual ou quais piscinas desejam acessar. Eles apenas solicitam a troca na plataforma da Uniswap V2 e a própria Uniswap se encarrega de acessar as piscinas contidas nela, de maneira a onerar minimamente os usuários.

Na seção seguinte, analisaremos, matematicamente, o comportamento das quantidades e valores dos tokens na piscina sob uma outra ótica, que é a influência das condições de mercado na piscina. Para isso, consideraremos os

valores dos tokens variando e, a partir disso, será determinado a quantidade de cada token na piscina.

4.1.1 Influência das condições de mercado na piscina

Quando os valores dos tokens se alteram devido às condições de mercado, precisamos recalcular a quantidade de cada token na piscina. Para isso, considere:

$$P_t = \frac{v_{X_t}}{v_{Y_t}} \ .$$

Isso significa que para cada instante t, P_t pode ser calculado dividindo o valor do ativo X pelo valor do ativo Y na piscina de liquidez. Segue da equação (2) que:

$$v_{X_t} \cdot x_t = v_{Y_t} \cdot y_t \quad \Longrightarrow \quad P_t = \frac{v_{X_t}}{v_{Y_t}} = \frac{y_t}{x_t} \quad (4) \ .$$

Assim, P_t também pode ser interpretado como a razão entre a quantidade de tokens Y e a quantidade de tokens X, num instante t, na piscina de liquidez. Desta forma, combinando as equações (2) e (4), tem-se:

$$v_{X_t} \cdot x_t = v_{Y_t} \cdot y_t \quad \Longrightarrow \quad y_t = x_t \cdot \frac{v_{X_t}}{v_{Y_t}} \overset{(4)}{\Longrightarrow} \quad y_t = x_t \cdot P_t \quad (5) \ ;$$

$$v_{X_t} \cdot x_t = v_{Y_t} \cdot y_t \quad \Longrightarrow \quad x_t = y_t \cdot \frac{v_{y_t}}{v_{x_t}} \overset{(4)}{\Longrightarrow} \quad x_t = y_t \cdot \frac{1}{P_t} \quad (6) \ .$$

Substituindo a equação (5) na equação (1), tem-se que:

$$x_t \cdot y_t = k \overset{(5)}{\Longrightarrow} x_t \cdot (x_t \cdot P_t) = k \quad \Longrightarrow \quad (x_t)^2 = \frac{k}{P_t}$$

$$\Longrightarrow \quad x_t = \sqrt{k \cdot \frac{v_{Y_t}}{v_{X_t}}} \quad \Longrightarrow \quad x_t = \sqrt{\frac{k}{P_t}} \quad (7) \ .$$

Substituindo a equação (7) na equação (5), tem-se que:

$$y_t = x_t \cdot P_t \overset{(7)}{\Rightarrow} y_t = \sqrt{\frac{k}{P_t}} \cdot P_t \implies y_t = \sqrt{\frac{k}{P_t}} \cdot \sqrt{(P_t)^2}$$

$$\implies y_t = \sqrt{\frac{k \cdot (P_t)^2}{P_t}} \implies y_t = \sqrt{k \cdot P_t} \quad (8)\,.$$

Para melhorar o entendimento desse caso, veja o exemplo 5 abaixo com várias etapas, onde em cada uma delas será determinada a variação de preço dos tokens. Essas etapas serão usadas para fins de comparação na seção 4.1.2.

Exemplo 5: Suponha que um provedor de liquidez deseje montar uma piscina com um investimento inicial de $\$3.600{,}00$. Para isso, ele escolhe os tokens X e Y, tais que:

- o valor da unidade do token X é $\$300{,}00$;
- o valor da unidade do token Y é $\$1{,}00$.

Deseja-se determinar a quantidade inicial de cada um dos tokens e a constante k.

Solução: Das equações (2) e (3),

$$v_{X_t} \cdot x_t = v_{Y_t} \cdot y_t \quad (2) \quad \text{e} \quad V_t = v_{X_t} \cdot x_t + v_{Y_t} \cdot y_t \quad (3)\,,$$

conclui-se que cada um dos tokens contribui com 50% do valor da piscina.

$$V_t = v_{X_t} \cdot x_t + v_{Y_t} \cdot y_t \overset{(2)}{\Rightarrow} V_t = v_{X_t} \cdot x_t + v_{X_t} \cdot x_t \implies V_t = 2 \cdot v_{X_t} \cdot x_t \;;$$

$$V_t = v_{X_t} \cdot x_t + v_{Y_t} \cdot y_t \overset{(2)}{\Rightarrow} V_t = v_{Y_t} \cdot y_t + v_{Y_t} \cdot y_t \implies V_t = 2 \cdot v_{Y_t} \cdot y_t \;.$$

Assim, substituindo $v_{X_0} = \$300{,}00$, $v_{Y_0} = \$1{,}00$ e $V_0 = \$3.600{,}00$, nas equações anteriores, tem-se que:

$$2 \cdot \$300{,}00 \cdot x_0 = \$3.600{,}00 \implies x_0 = \frac{\$3.600{,}00}{\$600{,}00} \implies x_0 = 6 \;;$$

$$2 \cdot \$1{,}00 \cdot y_0 = \$3.600{,}00 \implies y_0 = \frac{\$3.600{,}00}{\$2{,}00} \implies y_0 = 1.800 \;.$$

Substituindo $x_0 = 6$ e $y_0 = 1.800$ na equação $x \cdot y = k$, tem-se que:

$$x_t \cdot y_t = k \implies 6 \cdot 1.800 = k \implies k = 10.800 \ .$$

Desta forma, a piscina é inicialmente constituída, conforme a Tabela 2 abaixo.

t	V_0	v_{X_0}	v_{Y_0}	x_0	y_0	k
0	$ 3.600,00	$ 300,00	$ 1,00	6	1800	10.800

Tabela 2 - Configuração inicial da piscina no exemplo 5.

A partir de agora, vamos simular algumas variações de preços dos tokens X e Y em diferentes etapas.

- Etapa 1: Suponha que o valor do token X valorizou 50% em relação ao seu valor inicial, ou seja, passou a ser $v_{X_1} = \$450{,}00$ e que o valor do token Y se manteve o mesmo, ou seja, $v_{Y_1} = \$1{,}00$. Deseja-se determinar a quantidade de cada um dos tokens nesta etapa.

Solução: Da equação (4), temos que:

$$P_t = \frac{v_{X_t}}{v_{Y_t}} = \frac{y_t}{x_t} \quad \implies \quad P_1 = \frac{\$450{,}00}{\$1{,}00} = 450 \ .$$

Das equações (7) e (8), temos que:

$$x_t = \sqrt{\frac{k}{P_t}} \quad \implies \quad x_1 = \sqrt{\frac{10.800}{450}} = \sqrt{24} \cong 4{,}90 \ ;$$

$$y_t = \sqrt{k \cdot P_t} \quad \implies \quad y_1 = \sqrt{10.800 \cdot 450} = \sqrt{4.860.000} \cong 2.204{,}54 \ .$$

Da equação (3), temos que:

$$V_t = v_{X_t} \cdot x_t + v_{Y_t} \cdot y_t \implies V_1 \cong \$450{,}00 \cdot 4{,}90 + \$1{,}00 \cdot 2.204{,}54 \cong \$4.409{,}54 \ .$$

Ao final da etapa 1 temos a seguinte configuração na piscina:

t	V_1	v_{X_1}	v_{Y_1}	x_1	y_1	k
1	$ 4.409,54	$ 450,00	$ 1,00	4,9	2.204,54	10.800

Tabela 3 - Configuração da piscina após a etapa 1 do exemplo 5.

- Etapa 2: Suponha que o valor do token X desvalorizou 50% em relação ao seu valor inicial, ou seja, passou a ser $v_{X_2} = \$150{,}00$ e que o valor do token Y se manteve o mesmo, ou seja, $v_{Y_2} = \$1{,}00$. Deseja-se determinar a quantidade de cada um dos tokens nesta etapa.

Solução: Da equação (4), temos que:

$$P_t = \frac{v_{X_t}}{v_{Y_t}} = \frac{y_t}{x_t} \quad \Longrightarrow \quad P_2 = \frac{\$150{,}00}{\$1{,}00} = 150 \ .$$

Das equações (7) e (8), temos que:

$$x_t = \sqrt{\frac{k}{P_t}} \quad \Longrightarrow \quad x_2 = \sqrt{\frac{10.800}{150}} = \sqrt{72} \cong 8{,}49 \ ;$$

$$y_t = \sqrt{k \cdot P_t} \quad \Longrightarrow \quad y_2 = \sqrt{10.800 \cdot 150} = \sqrt{1.620.000} \cong 1.272{,}79 \ .$$

Da equação (3), temos que:

$$V_t = v_{X_t} \cdot x_t + v_{Y_t} \cdot y_t \quad \Longrightarrow \quad V_2 \cong \$150{,}00 \cdot 8{,}49 + \$1{,}00 \cdot 1.272{,}79 \cong \$2.546{,}29 \ .$$

Ao final da etapa 2 temos a seguinte configuração na piscina:

t	V_2	v_{X_2}	v_{Y_2}	x_2	y_2	k
2	$ 2.546,29	$ 150,00	$ 1,00	8,49	1.272,79	10.800

Tabela 4 - Configuração da piscina após a etapa 2 do exemplo 5.

Considere mais algumas etapas de variação dos tokens, sempre em relação aos seus valores iniciais, a fim de realizar na seção 4.1.2 uma comparação do saldo dos tokens na piscina com o saldo dos tokens na carteira:

- Etapa 3: O token X valorizando 100% e o token Y se mantendo constante;
- Etapa 4: O token X valorizando 20% e o token Y se mantendo constante;
- Etapa 5: O token X valorizando 50% e o token Y valorizando 25%;
- Etapa 6: O token X valorizando 50% e o token Y desvalorizando 25%;
- Etapa 7: Os tokens X e Y valorizando 30%;
- Etapa 8: Os tokens X e Y desvalorizando 50%.

Efetuando cálculos análogos aos das etapas 1 e 2 para as etapas de 3 a 8, tem-se a situação da piscina em cada etapa na tabela abaixo.

t	V_t	V_{X_t}	V_{Y_t}	x_t	y_t	k	P_t
0	\$ 3.600,00	\$ 300,00	\$ 1,00	6	1.800	10.800	300
1	\$ 4.409,54	\$ 450,00	\$ 1,00	4,9	2.204,54	10.800	450
2	\$ 2.546,29	\$ 150,00	\$ 1,00	8,49	1.272,79	10.800	150
3	\$ 5.089,58	\$ 600	\$ 1	4,24	2.545,58	10.800	600
4	\$ 4.930,60	\$ 360	\$ 1	5,48	1.971,80	10.800	360
5	\$ 4.930,75	\$ 450	\$ 1,25	5,48	1.971,80	10.800	360
6	\$ 3.817,19	\$ 450	\$ 0,75	4,24	2.545,58	10.800	600
7	\$ 4.680,00	\$ 390	\$ 1,30	6	1.800	10.800	300
8	\$ 1.800,00	\$ 150	\$ 0,5	6	1.800	10.800	300

Tabela 5 - Configuração da piscina em cada etapa do exemplo 5.

Desta forma, pode-se calcular as quantidades de tokens X e Y após qualquer variação de preços deles e em qualquer instante t, assim como nas etapas do exemplo anterior.

4.1.2 O Impermanent Loss na piscina de liquidez Uniswap V2

Uma vez que o investidor entendeu o funcionamento de uma piscina de liquidez é natural surgir a seguinte pergunta: é mais vantajoso deixar as moedas na carteira ou montar uma piscina de liquidez?

Para responder a essa pergunta precisa-se calcular o saldo dos tokens em uma piscina de liquidez e comparar com o saldo que o investidor alcançaria se deixasse as moedas na carteira.

Para fins de comparação, é necessário considerar o valor inicial dos tokens, ao montar uma piscina de liquidez, igual o valor inicial deles ao deixá-los em carteira. Isto é, se uma piscina possui inicialmente 10 tokens X e 12 tokens Y, sendo $v_X = \$1{,}20$ e $v_Y = \$1{,}00$, faz-se necessário uma carteira com 10 tokens X e 12 tokens Y, sendo $v_X = \$1{,}20$ e $v_Y = \$1{,}00$, para comparar o comportamento de ambos.

Considere S_t o saldo do investidor que mantém seus tokens em carteira após um tempo t da compra dos tokens. Assim, S_t é dado por:

$$S_t = v_{X_t} \cdot x_0 + v_{Y_t} \cdot y_0 \quad (9) .$$

Com isso, a razão $\frac{V_t}{S_t}$ indica o saldo que o investidor alcança mantendo os tokens numa piscina de liquidez em relação ao saldo que o investidor alcançaria mantendo os mesmos tokens, com os mesmos valores iniciais, em carteira.

O Impermanent Loss (I_L), que em tradução livre significa perda impermanente, é a perda que um investidor pode ter ao optar por colocar seus tokens em uma piscina de liquidez ao invés de mantê-los em carteira. O cálculo do Impermanent Loss (I_L) é dado pela seguinte expressão:

$$I_L = \frac{V_t}{S_t} - 1 \quad (10) .$$

Para ilustrar o cálculo do Impermanent Loss (I_L), veja o exemplo 6 abaixo.

Exemplo 6: Considere uma piscina com as mesmas condições iniciais do exemplo 5 na seção 4.1.1, conforme exibido na tabela abaixo.

t	V_0	v_{X_0}	v_{Y_0}	x_0	y_0	k	P_t
0	\$ 3.600,00	\$ 300,00	\$ 1,00	6	1800	10.800	300

Tabela 6 - Configuração inicial da piscina no exemplo 5.

Calcule o Impermanent Loss (I_L) de cada caso abaixo. Os casos a seguir tomam como base as etapas do exemplo 5 na seção 4.1.1.

- Caso 1: Suponha que o valor do token X valorizou 50% em relação ao seu valor inicial, ou seja, passou a ser $v_{X_1} = \$450{,}00$ e que o valor do token Y se manteve o mesmo, ou seja, $v_{Y_1} = \$1{,}00$. Verificou-se que a piscina ficou com a seguinte configuração após essa etapa:

t	V_1	v_{X_1}	v_{Y_1}	x_1	y_1	k	P_t
1	\$ 4.409,54	\$ 450,00	\$ 1,00	4,9	2.204,54	10.800	450

Tabela 7 - Configuração da piscina após o caso 1 do exemplo 6.

Qual é o valor do Impermanent Loss (I_L) ao final desta etapa?

Solução: Se o investidor mantivesse os 6 tokens X e 1.800 tokens Y na carteira, seu saldo após a variação de preço dos tokens seria dado por:

$$S_1 = v_{X_1} \cdot x_0 + v_{Y_1} \cdot y_0 \implies S_1 = \$450{,}00 \cdot 6 + \$1{,}00 \cdot 1.800$$

$$\implies S_1 = \$4.500{,}00 \ .$$

Observe que $S_1 > V_1$. Portanto, seria mais vantajoso manter os tokens em carteira. Nesse caso, o I_L é dado por:

$$I_L = \frac{V_1}{S_1} - 1 \implies I_L = \frac{\$4.409{,}54}{\$4.500{,}00} - 1 \implies I_L \cong -0{,}02 \implies I_L \cong -2\% \ .$$

Isso significa que o investidor terá um saldo 2% menor alocando os tokens numa piscina, se comparado com a manutenção dos tokens em carteira.

- Caso 2: Suponha que o valor do token X desvalorizou 50% em relação ao seu valor inicial, ou seja, passou a ser $v_{X_2} = \$150{,}00$ e que o valor do token Y se manteve o mesmo, ou seja, $v_{Y_2} = \$1{,}00$. Verificou-se que a piscina ficou com a seguinte configuração após essa etapa:

t	V_2	v_{X_2}	v_{Y_2}	x_2	y_2	k	P_t
2	$ 2.546,29	$ 150,00	$ 1,00	8,49	1.272,79	10.800	150

Tabela 8 - Configuração da piscina após o caso 2 do exemplo 6.

Qual é o valor do Impermanent Loss (I_L) ao final desta etapa?

Solução: Se o investidor mantivesse os 6 tokens X e 1.800 tokens Y na carteira, seu saldo após a variação de preço dos tokens seria dado por:

$$S_2 = v_{X_2} \cdot x_0 + v_{Y_2} \cdot y_0 \implies S_2 = \$150{,}00 \cdot 6 + \$1{,}00 \cdot 1.800$$

$$\implies S_2 = \$2.700{,}00 \ .$$

Observe que $S_2 > V_2$. Portanto, seria mais vantajoso manter os tokens em carteira. Nesse caso, o I_L é dado por:

$$I_L = \frac{V_2}{S_2} - 1 \implies I_L = \frac{\$2.546{,}29}{\$2.700{,}00} - 1 \implies I_L \cong -0{,}0569 \implies I_L \cong -5{,}69\% \ .$$

Isso significa que o investidor terá um saldo $5{,}69\%$ menor alocando os tokens numa piscina, se comparado com a manutenção dos tokens em carteira.

Considere as etapas de 3 a 8 do exemplo 5 da seção 4.1.1, descritas abaixo, para dar continuidade ao cálculo do Impermanent Loss (I_L).

- Etapa 3: O token X valorizando 100% e o token Y se mantendo constante;
- Etapa 4: O token X valorizando 20% e o token Y se mantendo constante;
- Etapa 5: O token X valorizando 50% e o token Y valorizando 25%;
- Etapa 6: O token X valorizando 50% e o token Y desvalorizando 25%;
- Etapa 7: Os tokens X e Y valorizando 30%;
- Etapa 8: Os tokens X e Y desvalorizando 50%.

A configuração da piscina ao final de cada etapa acima foi dada na tabela abaixo:

t	V_t	V_{X_t}	V_{Y_t}	x_t	y_t	k	P_t
0	\$ 3.600,00	\$ 300,00	\$ 1,00	6	1.800	10.800	300
1	\$ 4.409,54	\$ 450,00	\$ 1,00	4,9	2.204,54	10.800	450
2	\$ 2.546,29	\$ 150,00	\$ 1,00	8,49	1.272,79	10.800	150
3	\$ 5.089,58	\$ 600,00	\$ 1,00	4,24	2.545,58	10.800	600
4	\$ 4.930,60	\$ 360,00	\$ 1,00	5,48	1.971,80	10.800	360
5	\$ 4.930,75	\$ 450,00	\$ 1,25	5,48	1.971,80	10.800	360
6	\$ 3.817,19	\$ 450,00	\$ 0,75	4,24	2.545,58	10.800	600
7	\$ 4.680,00	\$ 390,00	\$ 1,30	6	1.800	10.800	300
8	\$ 1.800,00	\$ 150,00	\$ 0,50	6	1.800	10.800	300

Tabela 9 - Configuração da piscina em cada caso do exemplo 5.

Seguindo cálculos análogos aos dos casos 1 e 2 para as etapas de 3 a 8 do exemplo 5 da seção 4.1.1, e adaptando a tabela anterior para o valor do Impermanent Loss (I_L) em cada caso, obtém-se a Tabela 10 a seguir.

t	V_t	V_{X_t}	V_{Y_t}	x_t	y_t	P_t	S_t	I_L (%)
0	$ 3.600,00	$ 300,00	$ 1,00	6	1.800	300	$ 3.600,00	0
1	$ 4.409,54	$ 450,00	$ 1,00	4,9	2.204,54	450	$ 4.500,00	−2
2	$ 2.546,29	$ 150,00	$ 1,00	8,49	1.272,79	150	$ 2.700,00	−5,69
3	$ 5.089,58	$ 600,00	$ 1,00	4,24	2.545,58	600	$ 5.400,00	−5,75
4	$ 4.930,60	$ 360,00	$ 1,00	5,48	1.971,80	360	$ 3.960,00	−0,39
5	$ 4.930,75	$ 450,00	$ 1,25	5,48	1.971,80	360	$4.950,00	−0,39
6	$ 3.817,19	$ 450,00	$ 0,75	4,24	2.545,58	600	$ 4.050,00	−5,75
7	$ 4.680,00	$ 390,00	$ 1,30	6	1.800	300	$ 4.680,00	0
8	$ 1.800,00	$ 150,00	$ 0,50	6	1.800	300	$ 1.800,00	0

Tabela 10 - Configuração da piscina com o IL em cada caso do exemplo 6.

É possível calcular o Impermanent Loss (I_L) em cada caso nos sites indicados nos links abaixo, conforme mostra a Figura 24:

- https://dailydefi.org/tools/impermanent-loss-calculator/ ;
- https://impermanentloss.github.io/calculator/ .

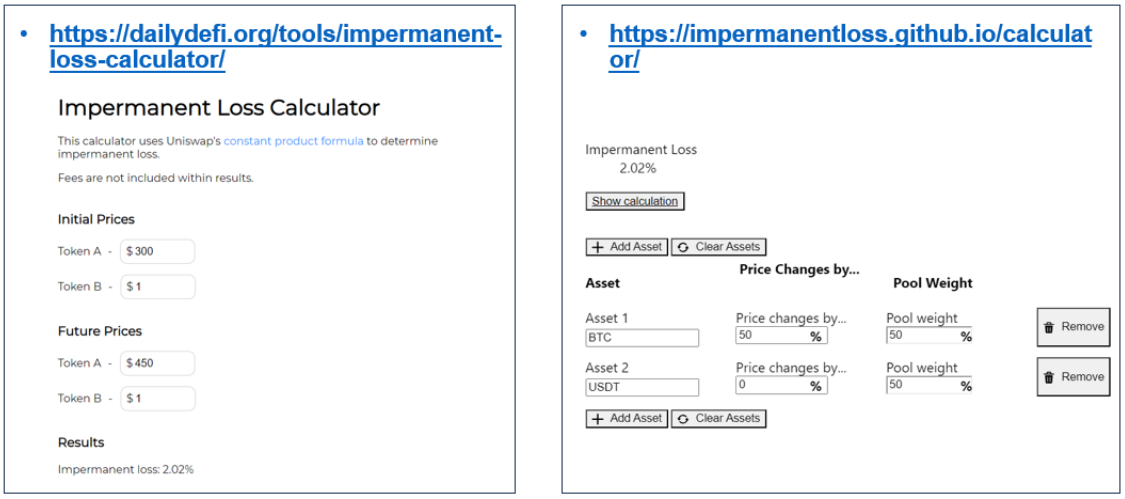


Figura 24 - Cálculo online do Impermanent Loss

Em ambos os casos da Figura 24 o cálculo do Impermanent Loss (I_L) para o caso 1 da Tabela 10 resultou em 2,02%.

Observe que os *casos 1 e 2* geram I_L diferentes. Nesses casos, o valor do token X varia em 50% e -50%, respectivamente, e o token Y se mantém com

valor inicial em ambos. Ou seja, ao fixar o valor de um dos tokens e variar o valor do outro token de forma simétrica, obtém-se I_L diferentes.

$$\overbrace{\left\{\begin{matrix} X\ valoriza\ 50\%\ ; \\ Y\ se\ matém\ constante. \end{matrix}\right.}^{caso\ 1} e \overbrace{\left\{\begin{matrix} X\ desvaloriza\ 50\%\ ; \\ Y\ se\ matém\ constante. \end{matrix}\right.}^{caso\ 2} \Longrightarrow I_L\ diferentes\ .$$

Em contrapartida, os *casos 2 e 3* geram o mesmo I_L (há uma pequena diferença na tabela devido a arredondamentos), sendo o preço do token X variando em -50% e 100% , respectivamente, e o token Y se mantendo com valor inicial.

$$\overbrace{\left\{\begin{matrix} X\ desvaloriza\ 50\%\ ; \\ Y\ se\ matém\ constante. \end{matrix}\right.}^{caso\ 2} e \overbrace{\left\{\begin{matrix} X\ valoriza\ 100\%\ ; \\ Y\ se\ matém\ constante. \end{matrix}\right.}^{caso\ 3} \Longrightarrow I_L\ iguais\ .$$

No *caso 4* temos o preço do token X variando em 20% e o token Y se mantendo com valor inicial, enquanto no *caso 5* temos os preços dos tokens X e Y variando em 50% e 25%, respectivamente. Ainda assim, ambos os *casos* geram o mesmo I_L.

Ou seja, se considerarmos dois casos diferentes, onde a variação dos preços dos tokens não é a mesma nos dois casos, mas a razão entre os novos preços dos tokens, em cada caso, se mantém igual, então o I_L , em ambos os casos, também será igual.

$$\frac{\overbrace{360}^{\substack{valor\ do\ token\ X \\ no\ caso\ 4}}}{\underbrace{1}_{\substack{valor\ do\ token\ Y \\ no\ caso\ 4}}} = \frac{\overbrace{450}^{\substack{valor\ do\ token\ X \\ no\ caso\ 5}}}{\underbrace{1{,}25}_{\substack{valor\ do\ token\ Y \\ no\ caso\ 5}}} \quad \Longrightarrow \quad I_L\ igual\ nos\ dois\ casos\ .$$

Analogamente, temos o caso 3, onde o preço do token X varia em 100% e o token Y se mantém com valor inicial, enquanto no caso 6 o preço do token X varia em 50% e o preço do token Y varia em -25%. Os casos 3 e 6 também geram o mesmo I_L.

$$\frac{\overbrace{600}^{\substack{valor\ do\ token\ X \\ no\ caso\ 3}}}{\underbrace{1}_{\substack{valor\ do\ token\ Y \\ no\ caso\ 3}}} = \frac{\overbrace{450}^{\substack{valor\ do\ token\ X \\ no\ caso\ 6}}}{\underbrace{0{,}75}_{\substack{valor\ do\ token\ Y \\ no\ caso\ 6}}} \quad \Longrightarrow \quad I_L\ igual\ nos\ dois\ casos\ .$$

O caso 7 tem os preços dos tokens X e Y variando em *30%*, enquanto o caso 8 tem os preços dos tokens X e Y variando em -50%. Ainda assim, ambos os casos geram o mesmo valor de I_L.

$$\frac{\overbrace{390}^{\substack{valor\ do\ token\ X\\ no\ caso\ 7}}}{\underbrace{1{,}30}_{\substack{valor\ do\ token\ Y\\ no\ caso\ 7}}} = \frac{\overbrace{150}^{\substack{valor\ do\ token\ X\\ no\ caso\ 8}}}{\underbrace{0{,}50}_{\substack{valor\ do\ token\ Y\\ no\ caso\ 8}}} \quad \Longrightarrow \quad I_L\ igual\ nos\ dois\ casos\ .$$

Para generalizar o cálculo do Impermanent Loss (I_L), será seguido os mesmos passos dos casos do exemplo 6 acima, mas agora não mais de forma numérica e, sim, de forma literal. A equação (3) abaixo

$$V_t = v_{X_t} \cdot x_t + v_{Y_t} \cdot y_t \quad (3)\ ,$$

nos dá o valor total dos tokens na piscina após um tempo t da formação da piscina. A equação (9) abaixo

$$S_t = v_{X_t} \cdot x_0 + v_{Y_t} \cdot y_0 \quad (9)\ ,$$

nos dá o valor total dos tokens em carteira após um tempo t da compra dos tokens. Substituindo as equações

$$P_t = \frac{v_{X_t}}{v_{Y_t}} = \frac{y_t}{x_t} \quad (4)\ , \quad x_t = \sqrt{\frac{k}{P_t}} \quad (7) \quad e \quad y_t = \sqrt{k \cdot P_t} \quad (8)\ ,$$

na equação (3), tem-se que:

$$V_t = v_{X_t} \cdot \sqrt{\frac{k}{\frac{v_{X_t}}{v_{Y_t}}}} + v_{Y_t} \cdot \sqrt{k \cdot \frac{v_{X_t}}{v_{Y_t}}} = \sqrt{k \cdot (v_{X_t})^2 \cdot \frac{v_{Y_t}}{v_{X_t}}} + \sqrt{k \cdot (v_{Y_t})^2 \cdot \frac{v_{X_t}}{v_{Y_t}}}$$

$$= \sqrt{k \cdot v_{X_t} \cdot v_{Y_t}} + \sqrt{k \cdot v_{X_t} \cdot v_{Y_t}} = 2 \cdot \sqrt{k \cdot v_{X_t} \cdot v_{Y_t}}\ .$$

Substituindo as equações

$$P_t = \frac{v_{X_t}}{v_{Y_t}} = \frac{y_t}{x_t} \quad (4)\ , \quad x_t = \sqrt{\frac{k}{P_t}} \quad (7) \quad e \quad y_t = \sqrt{k \cdot P_t} \quad (8)\ ,$$

na equação (9), tem-se que:

$$S_t = v_{X_t} \cdot \sqrt{\frac{k}{\frac{v_{X_0}}{v_{Y_0}}}} + v_{Y_t} \cdot \sqrt{k \cdot \frac{v_{X_0}}{v_{Y_0}}} = v_{X_t} \cdot \sqrt{k \cdot \frac{v_{Y_0}}{v_{X_0}}} + v_{Y_t} \cdot \sqrt{k \cdot \frac{v_{X_0}}{v_{Y_0}}}$$

$$= v_{X_t} \cdot \sqrt{k \cdot \frac{v_{X_0} \cdot v_{Y_0}}{(v_{X_0})^2}} + v_{Y_t} \cdot \sqrt{k \cdot \frac{v_{X_0} \cdot v_{Y_0}}{(v_{Y_0})^2}}$$

$$= \frac{v_{X_t}}{v_{X_0}} \cdot \sqrt{k \cdot v_{X_0} \cdot v_{Y_0}} + \frac{v_{Y_t}}{v_{Y_0}} \cdot \sqrt{k \cdot v_{X_0} \cdot v_{Y_0}}$$

$$= \left(\frac{v_{X_t}}{v_{X_0}} + \frac{v_{Y_t}}{v_{Y_0}}\right) \cdot \sqrt{k \cdot v_{X_0} \cdot v_{Y_0}} \ .$$

Desta forma, tem-se que:

$$\frac{V_t}{S_t} = \frac{2 \cdot \sqrt{k \cdot v_{X_t} \cdot v_{Y_t}}}{\left(\frac{v_{X_t}}{v_{X_0}} + \frac{v_{Y_t}}{v_{Y_0}}\right) \cdot \sqrt{k \cdot v_{X_0} \cdot v_{Y_0}}} = \frac{2 \cdot \sqrt{\frac{v_{X_t}}{v_{X_0}} \cdot \frac{v_{Y_t}}{v_{Y_0}}}}{\frac{v_{X_t}}{v_{X_0}} + \frac{v_{Y_t}}{v_{Y_0}}}$$

$$\Longrightarrow \qquad \frac{V_t}{S_t} = \frac{2 \cdot \sqrt{q \cdot s}}{q + s} \ , \qquad sendo \ \ q = \frac{v_{X_t}}{v_{X_0}} \ \text{ e } \ s = \frac{v_{Y_t}}{v_{Y_0}} \ . \qquad (11)$$

Substituindo a equação (11) na equação (10), o cálculo do Impermanent Loss (I_L) será dado por:

$$\underbrace{I_L = \frac{V_t}{S_t} - 1}_{equação\ (10)} \quad \Longrightarrow \quad I_L = \frac{2 \cdot \sqrt{q \cdot s}}{q + s} - 1 \quad (12) \ .$$

Observe que

$$\frac{2 \cdot \sqrt{q \cdot s}}{q + s} = \frac{\sqrt{q \cdot s}}{\frac{q + s}{2}} \ .$$

Assim, nota-se que na razão encontrada acima o numerador é dado pela média geométrica entre q e s, e o denominador é dado pela média aritmética entre q e s. Será verificado que essa razão será sempre menor ou igual a 1.

Tem-se que q e s são sempre maiores ou iguais a zero, visto que representam razões entre os preços de moedas e não faz sentido termos moedas com valores negativos. Sendo assim,

$$\left(\sqrt{q}-\sqrt{s}\right)^2 \geq 0 \quad \Longrightarrow \quad q-2\cdot\sqrt{q}\cdot\sqrt{s}+s \geq 0$$

$$\Longrightarrow \quad q+s \geq 2\cdot\sqrt{q\cdot s}$$

$$\Longrightarrow \quad \frac{q+s}{2} \geq \sqrt{q\cdot s}\ .$$

Com isso, desconsiderando o ganho de taxas por negociação, investir na piscina se mostra quase sempre um cenário menos vantajoso do que deixar as moedas na carteira. O máximo que pode acontecer é o rendimento da piscina igualar o rendimento da carteira. Esse cenário ocorre quando $q = s$ na equação (12).

$$I_L = \frac{2\cdot\sqrt{q\cdot s}}{q+s} - 1 \quad (12)\ .$$

Isso significa que sempre que o valor dos tokens variarem na mesma proporção, o saldo final deles na piscina será equivalente ao saldo final deles caso estejam na carteira. Se os tokens variarem em proporções diferentes, o valor final dos tokens na piscina será inferior ao valor final dos tokens na carteira.

Abaixo segue alguns gráficos do I_L em ângulos diferentes, sendo os eixos x e y, representando uma variação positiva de preços dos tokens X e Y, e o eixo z representando o I_L.

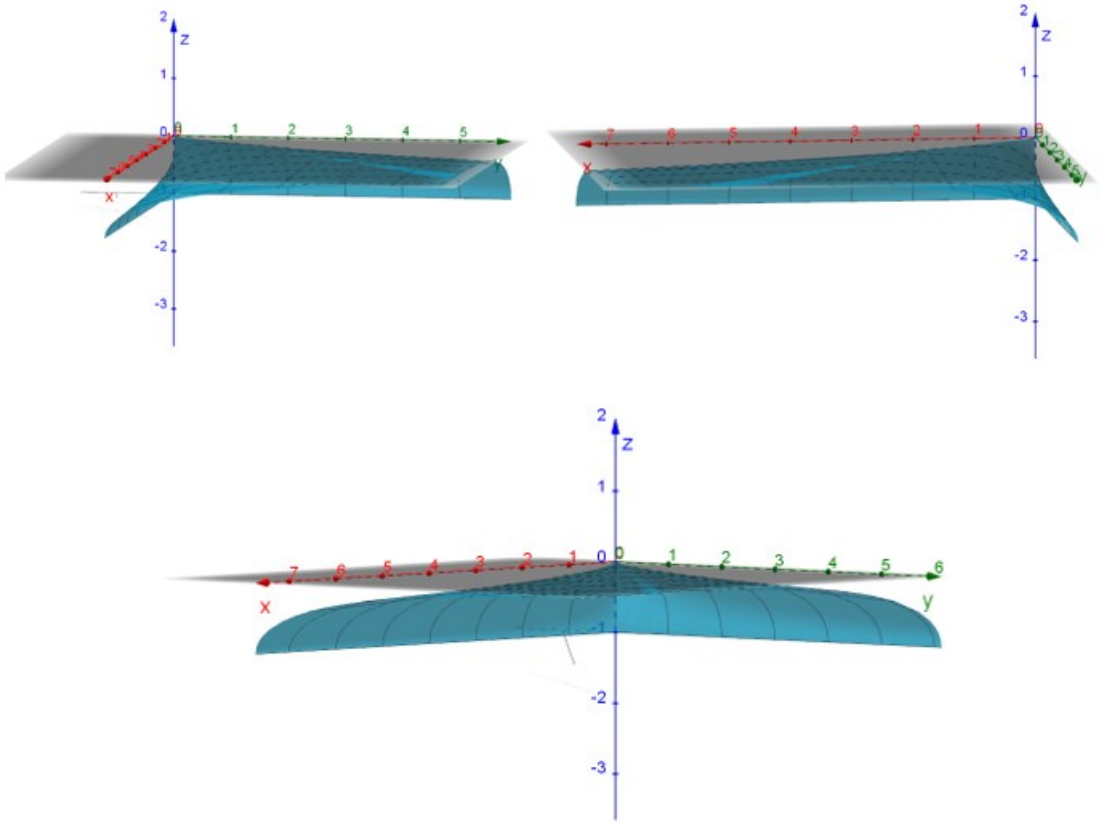


Figura 25 - Gráficos do Impermanent Loss

Nos gráficos da Figura 25 acima, considera-se que a piscina está nas suas condições iniciais no ponto $(0,0,0)$, ou seja, não há variação de preço dos tokens X e Y e, consequentemente, não existe I_L.

O ponto $(1;\ 1;\ 0)$, indica que houve uma variação de 100% nos preços dos tokens X e Y. Essa variação nos dá um $I_L = 0$.

O ponto $(1;\ 0;\ -5{,}75)$ indica que o preço do token X variou 100% enquanto o preço do token Y se manteve constante. Essa variação nos leva a um $I_L = -5{,}75\%$. E assim por diante.

Note que os gráficos da Figura 25 acima não contemplam variações negativas de preço dos tokens X e Y. Eles tangenciam o plano $z = 0$ nos pontos dados por $(x, x, 0)$, $x \in \mathbb{R}_+$, ou seja, tangenciam o plano $z = 0$ ao longo da semirreta $y = x$, com $x \geq 0$. Para os demais pontos do plano $z = 0$, tais que $x, y \geq 0$, tem-se sempre que $I_L < 0$.

A equação (12) abaixo,

$$I_L = \frac{2 \cdot \sqrt{q \cdot s}}{q + s} - 1 \quad (12)$$

possui o I_L em função das variáveis q e s. Logo, é uma função de duas variáveis. Nela considera-se que os tokens X e Y possuem seus valores medidos em uma terceira moeda. Contudo, pode-se medir o valor de um token em relação ao outro token. É dessa forma que se determina as quantidades dos tokens ao montar uma piscina.

Para o caso em que um token, por exemplo, o token X, tiver seu valor medido em relação ao outro token da piscina, o token Y, tem-se que $v_{Y_t} = 1, \forall t$. Assim, $s = 1, \forall t$. Portanto, o I_L é dado por:

$$I_L = \frac{2 \cdot \sqrt{q}}{q + 1} - 1 \quad , \quad onde\ q = \frac{v_{X_t}}{v_{X_0}} \quad (13) \ .$$

Abaixo, na Figura 26, segue o gráfico do caso em que o valor de s, na equação (12), não varia, ou seja, o valor do token Y é constante.

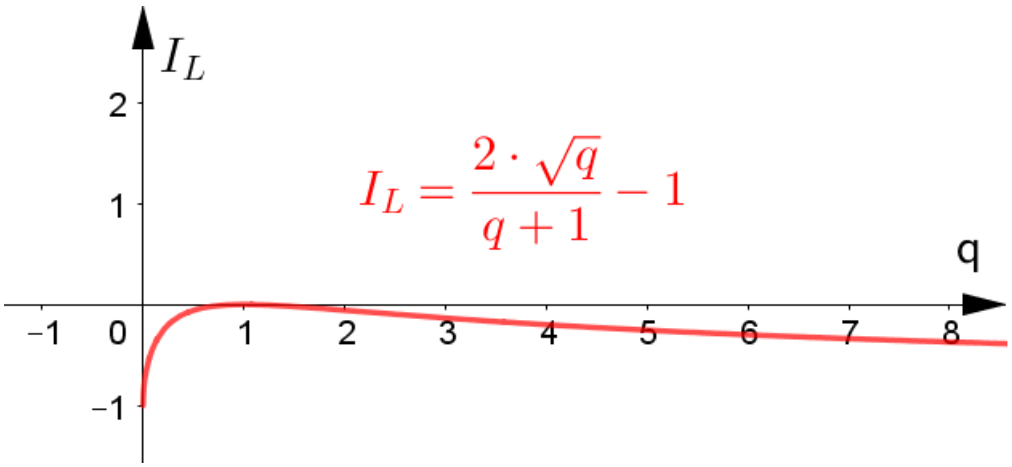


Figura 26 - Gráfico do Impermanent Loss

Note que na Figura 26, o gráfico tangencia o eixo q, que representa a variação percentual do token X, quando $q = 1$. Para os demais valores de q, tem-se sempre que $I_L < 0$.

A graduação do eixo q na figura Figura 26 acima indica a razão entre o preço do token X em um instante qualquer pelo preço inicial do token X ao montar a piscina, sempre medidos em relação ao token Y, diferentemente da graduação dos eixos x e y nos gráficos da Figura 25.

Quanto a utilização do termo “perda impermanente”, (Pintail, 2019) diz que:

> “Este artigo originalmente usou o termo “perda impermanente” para descrever as perdas que os provedores de liquidez experimentam devido à divergência de preços. A palavra “impermanente” foi escolhida porque a perda devido à divergência de preços pode ser revertida se a divergência de preços também for revertida. Entretanto, a utilização desse termo poderia criar a expectativa de que as perdas são garantidas de serem revertidas, o que não é o caso. Para refletir melhor isso, o artigo foi atualizado para usar o termo “perda divergente”.

Desta forma, o provedor de liquidez só terá perdas caso encerre a piscina num momento em que o valor dos tokens estejam com uma variação proporcionalmente diferentes. Como os preços dos tokens flutuam de acordo com o mercado, enquanto a piscina estiver ativa, as perdas podem aumentar indefinidamente, assim como podem ser zeradas em um determinado momento. Uma vez que a piscina é encerrada, o provedor assume a possível perda dada pela variação de preço dos tokens. Esta perda passa a ser irreversível, porém pode ser compensada com o ganho de taxas pelo provedor.

4.2 A LIQUIDEZ CONCENTRADA NAS PISCINAS DO UNISWAP V3

Como já visto na seção 3.3.2, a Uniswap V3 trouxe como uma de suas inovações a liquidez concentrada. Neste caso, o usuário deixa de fornecer liquidez ao longo de toda a curva $x \cdot y = k$, com $x > 0$, $y > 0$ e k constante, e passa a fornecer liquidez num pedaço da curva limitado pelos pontos B e A, conforme ilustrado na Figura 27 abaixo:

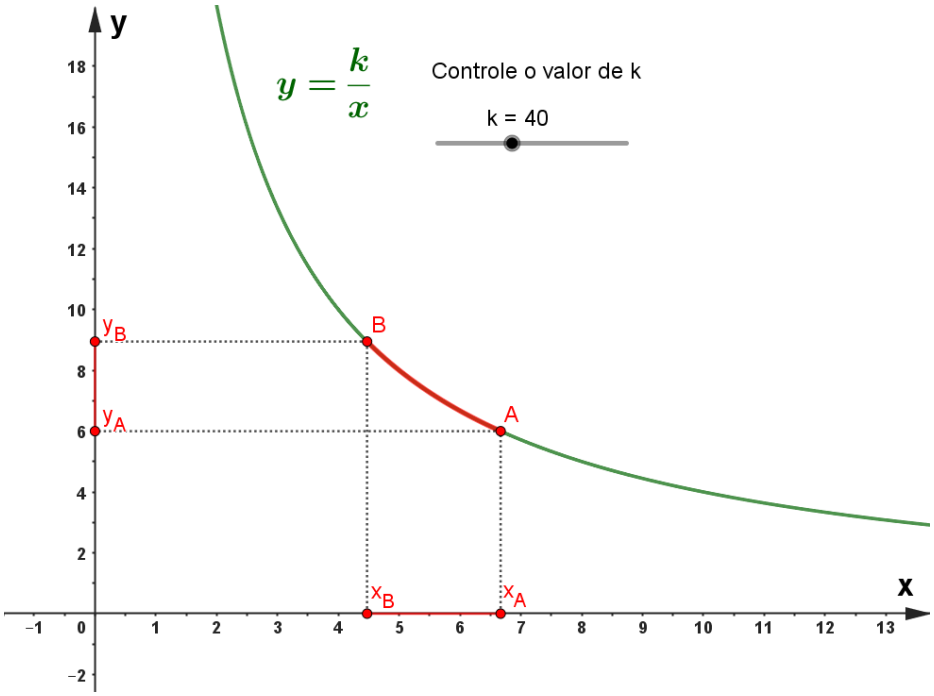


Figura 27 - Liquidez concentrada em Uniswap V3.

Observe na Figura 27 que o pedaço da curva $x \cdot y = k$ entre os pontos B e A determina os intervalos $[x_B, x_A]$ e $[y_A, y_B]$ no eixo x e no eixo y, respectivamente, sendo:

- x_B a quantidade de tokens X no ponto B da curva $x \cdot y = k$;
- x_A a quantidade de tokens X no ponto A da curva $x \cdot y = k$;
- y_A a quantidade de tokens Y no ponto A da curva $x \cdot y = k$;
- y_B a quantidade de tokens Y no ponto B da curva $x \cdot y = k$.

Note que os intervalos $[x_B, x_A]$ e $[y_A, y_B]$ são totalmente dependentes um do outro. À medida que um deles varia, o outro também varia, e vice-versa, visto que a curva $x \cdot y = k$, com $x > 0$, $y > 0$ e k constante é bijetiva.

Verifica-se em (Aigner & Dhaliwal, 2021) e (Adams, Zinsmeister, & Salem, 2021) que para fornecer liquidez concentrada, faz-se uma translação da curva $x \cdot y = k$ movimentando-a horizontalmente, no sentido negativo, em um valor igual a x_B, e verticalmente, no sentido negativo, em um valor igual a y_A. Assim, obtém-se uma nova curva dada por $x' \cdot y' = k$, sendo

$$x' = x + x_B \quad \text{e} \quad y' = y + y_A$$

com $x' > 0$, $y' > 0$ e k constante. Com essa translação, passamos a ter o ponto A sobre o eixo y, representado por A' e o ponto B sobre o eixo x, representado por B'. Veja a Figura 28 abaixo.

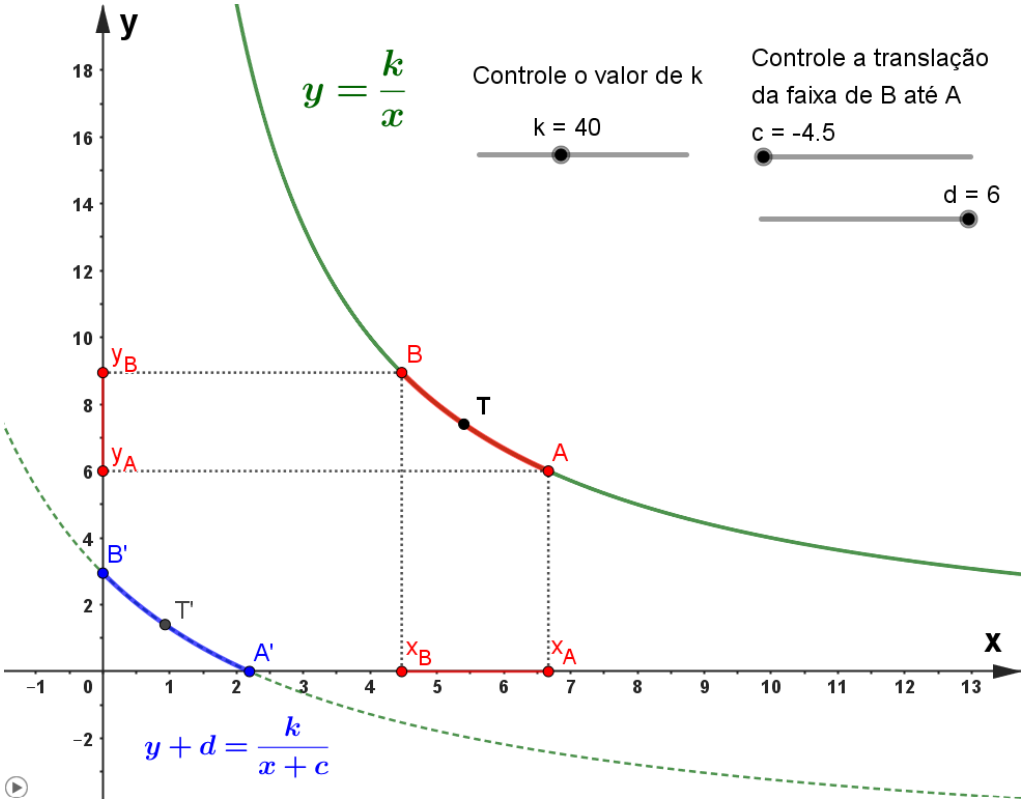


Figura 28 - Liquidez concentrada em Uniswap V3.

A partir de agora, temos que buscar os valores de x_A e y_B para concluir a translação e concentrar a liquidez.

A translação

Ao montar uma piscina de liquidez no Uniswap V3, entramos com dois valores que delimitam a curva $x \cdot y = k$ entre os pontos B e A, onde desejamos fornecer liquidez. Esses dois valores formam uma faixa de preço e são determinados através da razão entre os preços dos tokens X e Y.

Ou seja, o provedor de liquidez escolhe um menor valor aceitável para o preço do token X em relação ao token Y, e um maior valor aceitável para o preço do token X em relação ao token Y. O provedor de liquidez somente estará apto a receber taxas de negociação enquanto a relação de preços entre os tokens estiver entre os valores estipulados inicialmente por ele.

Na prática, os intervalos $[x_B, x_A]$ e $[y_A, y_B]$ que delimitam a curva $x \cdot y = k$ entre os pontos B e A não aparecem de forma explícita no momento de formação de uma piscina. Eles ficam implicitamente determinados pelos valores de entrada, que desejamos encontrar. A Figura 29 abaixo ilustra a tela de formação de uma piscina.

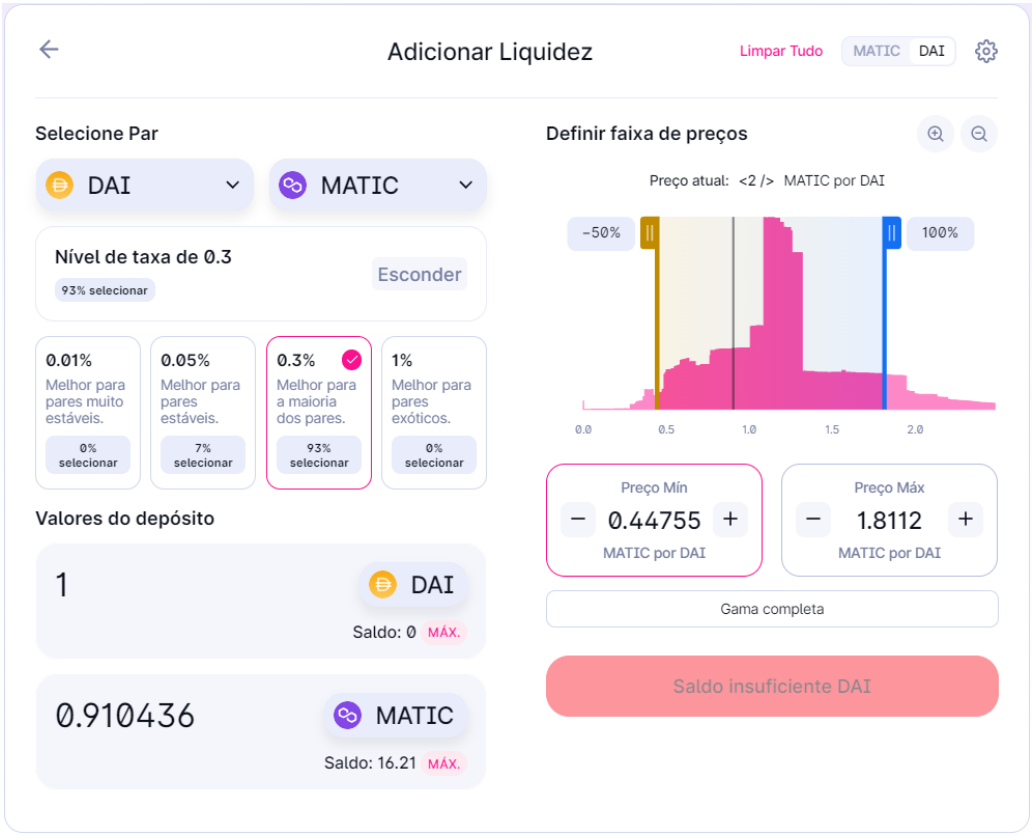


Figura 29 - Formação de uma piscina de liquidez com os tokens em Uniswap V3

Na Figura 29 acima temos a tela onde se adiciona liquidez no protocolo Uniswap V3. Nela, está sendo simulado a montagem de uma piscina com os tokens DAI e $MATIC$. O nível de taxa escolhido foi de $0{,}3\%$. Os saldos de $MATIC$ e DAI disponíveis em carteira pelo provedor de liquidez são $16{,}21$ e 0, respectivamente.

A faixa de preços, que está sendo medida pela razão entre as quantidades de tokens $MATIC$ e DAI, nessa ordem, varia do preço mínimo, igual a $0{,}45296$, ao preço máximo, igual a 1.8112. Com essa faixa, são necessários $0{,}910436$ $MATIC$ por cada unidade de DAI para formar a piscina.

Note que o preço mínimo de $MATIC$ por DAI estipulado na faixa é aproximadamente 50% menor que o valor de mercado de $MATIC$ em relação ao

DAI, assim como o preço máximo de $MATIC$ por DAI estipulado na faixa é aproximadamente 100% maior que o valor de mercado de $MATIC$ em relação ao DAI. O valor de mercado do $MATIC$ por DAI pode ser visto na Figura 30 abaixo.

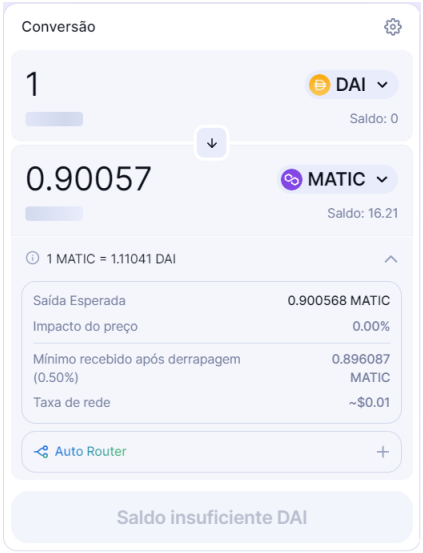


Figura 30 - Preço do MATIC por DAI no Uniswap

Para fins de comparação, a Figura 30 acima nos mostra a relação de preços entre os tokens $MATIC$ e DAI caso um usuário deseje trocar um deles pelo outro. Ela é a tela de trocas de tokens do Uniswap e foi simulada instantes após a simulação ilustrada na Figura 29.

Repare que há uma pequena diferença na relação entre o preço de $MATIC$ por DAI quando comparamos as Figura 29 e Figura 30. O espaço de tempo entre a retirada das imagens na Uniswap pode influenciar nessa diferença de preço de $MATIC$ por DAI. Aproximações de valores feitos pela própria plataforma também pode influenciar na diferença observada.

O fato é que a relação entre as quantidades dos tokens para efetuar a troca de um pelo outro (preço de mercado), visto na Figura 30, é muito próxima da relação entre as quantidades dos tokens necessária para fazer o depósito no momento de montar a piscina, visto na Figura 29. Isso ocorre particularmente devido a faixa de preços variar de -50% a 100% em relação ao valor de mercado de $MATIC$ por DAI, visto na Figura 29. Se modificarmos a faixa, em termos percentuais, da variação de preços dos tokens, a relação entre as quantidades de tokens a serem depositados na piscina se altera em relação ao preço de mercado dos tokens.

Com isso, visto que para montar uma piscina no Uniswap V3 se faz necessário estipular os valores mínimo e máximo de um dos tokens em relação ao outro, precisamos escrever x_B e y_A , presentes na equação de translação

$$x' \cdot y' = k \text{ , tal que } x' = x + x_B \quad \text{e} \quad y' = y + y_A \text{ ,}$$

em função do preço de entrada mínimo e do preço de entrada máximo de um token em relação ao outro. Para isso, nos apoiaremos nas equações que regem as negociações na plataforma Uniswap V2 via contrato inteligente.

A regra de negociação nesse protocolo é dada pelas equações abaixo:

$$\begin{cases} x \cdot y = k & (1) \\ v_X \cdot x = v_Y \cdot y & (2) \end{cases} .$$

Analisando a equação (1), que possui gráfico ilustrado na Figura 23, exibida na seção 4.1, e a equação (2), pode-se alterar qualquer uma das variáveis x , y , v_X ou v_Y, que as outras três se modificam de modo a satisfazer as equações (1) e (2). Em particular:

(i) diminuindo a quantidade de tokens X, conclui-se que a quantidade de tokens Y aumenta, que v_X aumenta e que v_Y diminui;

(ii) aumentando a quantidade de tokens X, conclui-se que a quantidade de tokens Y diminui, que v_X diminui e que v_Y aumenta.

Pode-se notar das equações (7) e (8), que:

$$x = \sqrt{\frac{k}{P}} \quad (7) \quad \text{e} \quad y = \sqrt{k \cdot P} \quad (8)$$

(j) quando P diminui, x aumenta, e quando P aumenta, x diminui;

(jj) quando P diminui, y diminui, e quando P aumenta, y aumenta.

As conclusões anteriores podem ser observadas na Figura 31 abaixo, que exibe o gráfico dado pela equação $x = \sqrt{\frac{k}{P}}$.

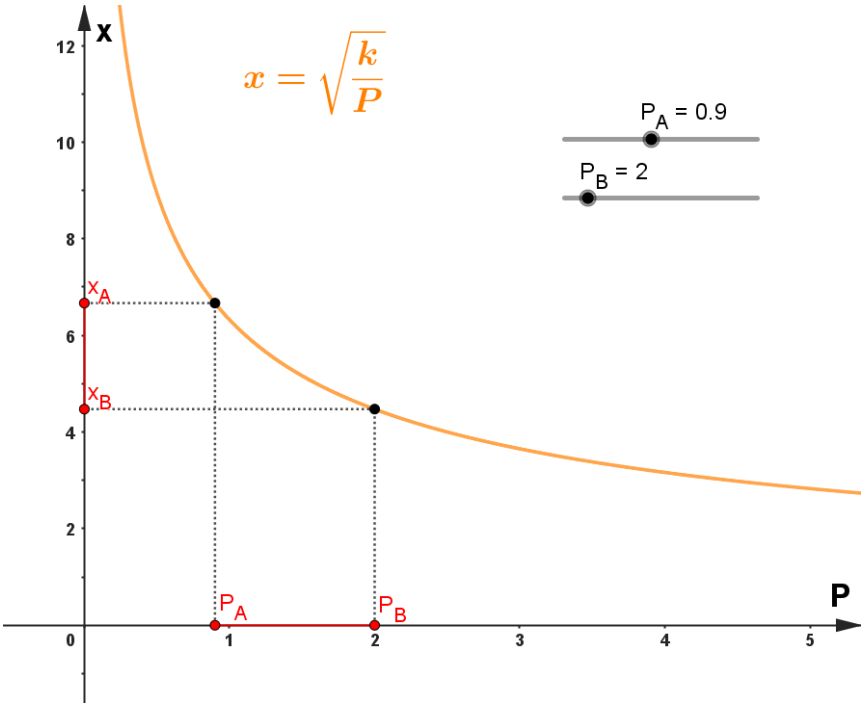


Figura 31 - Liquidez concentrada em Uniswap V3.

Desta forma, à medida que se estipula um intervalo para variável x, por exemplo $[x_B, x_A]$, automaticamente se obtém um intervalo para variável P, dado por $[P_A, P_B]$, e vice-versa, visto que a curva $x = \sqrt{\frac{k}{P}}$ é bijetiva, para $x, P \in \mathbb{R}_+^*$.

Com isso, podemos perceber da Figura 31 que, uma vez fixado o intervalo $[x_B, x_A]$, determina-se indiretamente o intervalo $[P_A, P_B]$ associado a ele, onde P_A é o menor valor do intervalo e P_B é o maior valor do intervalo. Chamando P_A de $P_{mín}$ e P_B de $P_{máx}$ temos que o intervalo $[P_A, P_B]$ coincide com o intervalo $[P_{mín}, P_{máx}]$.

Porém, nada impede que o intervalo $[P_A, P_B] = [P_{mín}, P_{máx}]$ seja conhecido de antemão e, a partir dele, os intervalos $[x_B, x_A]$ e $[y_A, y_B]$, ficam indiretamente determinados.

A Figura 32 abaixo ilustra a relação de dependência entre os intervalos $[P_A, P_B] = [P_{mín}, P_{máx}]$, $[x_B, x_A]$ e $[y_A, y_B]$.

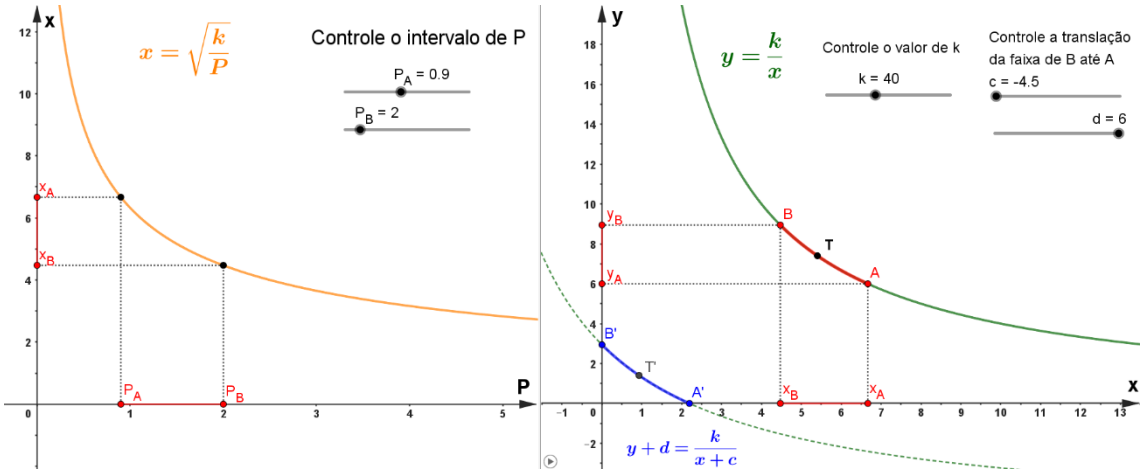


Figura 32 - Liquidez concentrada em Uniswap V3.

Das equações (7) e (8), temos que:

$$\underbrace{x_B = \sqrt{\frac{k}{P_B}}}_{equação\ (7)} = \sqrt{\frac{k}{P_{máx}}} \quad \text{e} \quad \underbrace{y_A = \sqrt{k \cdot P_A}}_{equação\ (8)} = \sqrt{k \cdot P_{mín}} \quad .$$

Portanto,

$$x' = x + x_B \implies x' = x + \sqrt{\frac{k}{P_{máx}}} \quad (14) \quad ;$$

$$y' = y + y_A \implies y' = y + \sqrt{k \cdot P_{mín}} \quad (15) \quad .$$

Uma vez determinados os valores de x_B e y_A, a translação da curva $x \cdot y = k$ fica concluída. Assim, obtém-se a curva

$$x' \cdot y' = k \quad ,$$

que pode ser reescrita como:

$$\left(x + \sqrt{\frac{k}{P_{máx}}}\right) \cdot \left(y + \sqrt{k \cdot P_{mín}}\right) = k \quad (16) \, .$$

A curva $x' \cdot y' = k$, representada em termos de x e y na equação (16), está parcialmente representada em azul nas Figura 28 e Figura 32 nesta seção. Ela é a equação que que relaciona a quantidade de tokens X e Y, a faixa de preço escolhida pelo provedor de liquidez e o valor de k, no protocolo Uniswap V3.

Faixa de preços x Quantidade de tokens na piscina

A faixa de preço estipulada pelo provedor de liquidez no momento de formação da piscina pode ser vista tanto relacionando as quantidades de tokens X e Y, escolhendo-se o $P_{mín}$ e o $P_{máx}$, conforme visto na equação (16), como em variação percentual do valor de mercado de um token em relação ao outro.

Na Figura 29, nessa seção, tem-se que $P_{mín}$ equivale a $0{,}4529\ MATIC$ por DAI e $P_{máx}$ equivale a $1.8112\ MATIC$ por DAI . Em termos percentuais, tem-se uma variação de -50% a 100% em relação ao valor de mercado de $MATIC$ por DAI, que é dado por $0{,}90057$, conforme visto na Figura 30, nessa seção. Desta forma, pode-se reescrever a equação (16) como

$$\left(x + \sqrt{\frac{k}{(1+q)\cdot P}}\right)\cdot\left(y + \sqrt{k\cdot(1+s)\cdot P}\right) = k \quad (17)\ ,$$

sendo:

- $P_{máx} = (1+q)\cdot P$;
- $P_{mín} = (1+s)\cdot P$;
- q é a variação percentual do limite superior da faixa de entrada;
- s é a variação percentual do limite inferior da faixa de entrada.

Pode-se reescrever a equação (17) da seguinte forma:

$$\left(x + \left[\frac{1}{\sqrt{1+q}}\right]\cdot\sqrt{\frac{k}{P}}\right)\cdot\left(y + \left[\sqrt{(1+s)}\right]\cdot\sqrt{k\cdot P}\right) = k\ .$$

Utilizando o caso particular da Figura 29, onde $q = 100\%$ e $s = -50\%$, tem-se que:

$$\frac{1}{\sqrt{1+q}} = \sqrt{(1+s)} \implies \frac{1}{1+q} = 1+s \implies (1+q)\cdot(1+s) = 1 \quad (18).$$

Empiricamente, tem-se que quaisquer valores de q e s que satisfaçam a condição dada pela equação (18), geram piscinas cuja relação entre as quantidades de depósito dos tokens envolvidos, no caso X e Y, empata com o

valor de mercado entre os tokens. Se escolhermos q e s que não satisfaçam a condição dada pela equação (18), a relação de depósito entre os tokens na piscina não será igual ao valor de mercado de um token pelo outro.

Quantidades máximas e mínimas dos tokens em uma piscina Uniswap V3

Observando o gráfico da curva dada pela equação (16) abaixo

$$\left(x + \sqrt{\frac{k}{P_{máx}}}\right) \cdot \left(y + \sqrt{k \cdot P_{mín}}\right) = k \quad (16)\,,$$

que corresponde a Figura 28 nessa seção, faz sentido falar em x e y máximo (o valor mínimo de ambos é zero), ao contrário da curva $x \cdot y = k$ que não possui valor máximo nem mínimo para x ou y.

Observe que quando $x \longrightarrow 0$ na equação (16), temos que y tende a sua quantidade máxima e pode-se determiná-lo da seguinte maneira:

$$\left(x + \sqrt{\frac{k}{P_{máx}}}\right) \cdot \left(y + \sqrt{k \cdot P_{mín}}\right) = k \overset{x \longrightarrow 0}{\Longrightarrow} \sqrt{\frac{k}{P_{máx}}} \cdot \left(y_{máx} + \sqrt{k \cdot P_{mín}}\right) = k$$

$$\Longrightarrow \quad y_{máx} + \sqrt{k \cdot P_{mín}} = \frac{k}{\sqrt{\frac{k}{P_{máx}}}} \quad \Longrightarrow \quad y_{máx} = \frac{k}{\sqrt{\frac{k}{P_{máx}}}} - \sqrt{k \cdot P_{mín}}$$

$$\Longrightarrow \quad y_{máx} = \sqrt{k \cdot P_{máx}} - \sqrt{k \cdot P_{mín}} \quad \Longrightarrow \quad y_{máx} = \sqrt{k} \cdot \left(\sqrt{P_{máx}} - \sqrt{P_{mín}}\right) \quad (19)\,.$$

Isso significa que, após a montagem da piscina, quando o valor de P for maior que $P_{máx}$, então a piscina só terá tokens Y, cuja quantidade será dada pelo $y_{máx}$ calculado acima. Na Figura 29, nessa seção, se a quantidade de $MATIC$ por DAI ultrapassar 1.8112 , então a piscina passará a ter somente tokens $MATIC$.

De forma análoga, quando $y \longrightarrow 0$ na equação (16), temos que x tende ao seu valor máximo e pode-se determiná-lo da seguinte maneira:

$$\left(x + \sqrt{\frac{k}{P_{máx}}}\right) \cdot \left(y + \sqrt{k \cdot P_{mín}}\right) = k \overset{y \longrightarrow 0}{\Longrightarrow} \left(x_{máx} + \sqrt{\frac{k}{P_{máx}}}\right) \cdot \sqrt{k \cdot P_{mín}} = k$$

$$\Longrightarrow \quad x_{máx} + \sqrt{\frac{k}{P_{máx}}} = \frac{k}{\sqrt{k \cdot P_{mín}}} \quad \Longrightarrow \quad x_{máx} = \frac{k}{\sqrt{k \cdot P_{mín}}} - \sqrt{\frac{k}{P_{máx}}}$$

$$\Longrightarrow \quad x_{máx} = \sqrt{\frac{k}{P_{mín}}} - \sqrt{\frac{k}{P_{máx}}} \quad \Longrightarrow \quad x_{máx} = \sqrt{k} \cdot \left(\frac{1}{\sqrt{P_{mín}}} - \frac{1}{\sqrt{P_{máx}}} \right) \quad (20) \, .$$

Isso significa que, após a montagem da piscina, quando o valor de P for menor que $P_{mín}$, então a piscina só terá tokens X, cuja quantidade será dada pelo $x_{máx}$ calculado acima. Na Figura 29, nessa seção, se a quantidade de $MATIC$ por DAI se tornar menor que $0{,}44755$, então a piscina passará a ter somente tokens DAI. Veja a seguir um exemplo.

Exemplo 7: Considere uma piscina com 10 tokens LDO e 12 tokens $USDC$, sendo $1\ LDO = \$1{,}20$ e $1\ USDC = \$1$. Determine a quantidade máxima de tokens LDO e $USDC$ que pode haver nessa piscina.

Solução: Da equação (1), tem-se que:

$$(Quant.de\ LDO) \cdot (Quant.de\ USDC) = k \quad \Longrightarrow \quad k = 10 \cdot 12 \quad \Longrightarrow \quad k = 120 \ .$$

Da equação (3), tem-se que:

$$P = \frac{v_X}{v_Y} = \frac{y}{x} \ \Longrightarrow \ P = \frac{\$1{,}20}{\$1} = \frac{12\ USDC}{10\ LDO} \ \Longrightarrow \ P = 1{,}2 \ .$$

Tomando $P \in [1\,;\,1{,}44]$, ou seja, $P_{mín} = 1$ e $P_{máx} = 1{,}44$, temos das equações (19) e (20) que:

$$LDO_{máx} = \sqrt{120} \cdot \left(\frac{1}{\sqrt{1}} - \frac{1}{\sqrt{1{,}44}} \right) \ \Longrightarrow \ LDO_{máx} \approx 1{,}83 \ ;$$

$$USDC_{máx} = \sqrt{120} \cdot \left(\sqrt{1{,}44} - \sqrt{1} \right) \ \Longrightarrow \ USDC_{máx} \approx 2{,}19 \ \blacksquare$$

Desta forma, se P for menor que 1, teremos somente tokens LDO na piscina, que corresponderá à $1{,}83\ LDO$. Por outro lado, se P for maior que $1{,}44$, teremos somente tokens $USDC$ na piscina, que corresponderá à $2{,}19\ USDC$.

Para fins de desenvolvimento das contas, optou-se por definir inicialmente

$$P = \frac{v_X}{v_Y} = \frac{y}{x} \ ,$$

como é feito em (Adams, Zinsmeister, & Salem, 2021), que é a principal fonte do protocolo Uniswap V3 para os autores dessa pesquisa. Contudo, nada impede que P seja definido como $P = \frac{v_Y}{v_X} = \frac{x}{y}$, conforme é feito em (Aigner & Dhaliwal, 2021).

Caso P tivesse sido definido como

$$P = \frac{v_Y}{v_X} = \frac{x}{y} ,$$

ao fazer manipulações análogas às que foram apresentadas anteriormente, chegar-se-ia em:

$$x = \sqrt{k \cdot P} \quad \text{e} \quad y = \sqrt{\frac{k}{P}} \quad .$$

Assim,

$$x' = x + \sqrt{k \cdot P_{máx}} \qquad \text{e} \qquad y' = y + \sqrt{\frac{k}{P_{mín}}} \, .$$

Consequentemente,

$$x_{máx} = \sqrt{k} \cdot \left(\sqrt{P_{máx}} - \sqrt{P_{mín}}\right) \qquad \text{e} \qquad y_{máx} = \sqrt{k} \cdot \left(\frac{1}{\sqrt{P_{mín}}} - \frac{1}{\sqrt{P_{máx}}}\right) ,$$

que converge com os resultados apresentados em (Aigner & Dhaliwal, 2021).

5. INTERAGINDO COM A METAMASK E A UNISWAP

Neste capítulo será abordado de forma prática um possível caminho para se montar uma piscina de liquidez, passando pela MetaMask e pela Uniswap.

Será detalhado o processo de instalação, configuração e segurança da MetaMask, que é uma carteira de criptomoedas não custodiante e considerada uma das maiores hot wallets do mercado. É crucial que o usuário saiba interagir com uma carteira porque inevitavelmente ele precisará passar por uma delas para montar uma piscina de liquidez na Uniswap.

Finalmente, será feito o passo-a-passo de como montar uma piscina de liquidez em Uniswap V2 e Uniswap V3.

5.1 MetaMask: instalação, segurança e configuração

A MetaMask é um tipo de hot wallet (carteira quente) que foi criada em 2016 pela Consensys, uma empresa focada em tecnologia em blockchain e que foi fundada por Joseph Lubin, cofundador da Ethereum. Nela é possível guardar criptomoedas e tokens não fungíveis (NFT) criados na blockchain da Ethereum.

Atualmente, a MetaMask possui mais de 30 milhões de usuários em todo mundo, segundo (Introdução à MetaMask, 2023). Essa carteira já foi auditada algumas vezes desde sua criação, como pode ser visto em (MetaMask, 2023). Esses fatores fizeram com que escolhêssemos essa carteira para a realização deste trabalho.

A carteira MetaMask é compatível com os navegadores Chrome, Firefox, Brave e Edge, para o caso de uso em computadores, e com os sistemas Android e IOS, no caso de uso em smartphones.

Figura 33 - Navegadores compatíveis com a MetaMask.

Independente do navegador web que o usuário escolher, não há necessidade de baixar nenhum programa no computador. A MetaMask é instalada como extensão do navegador escolhido.

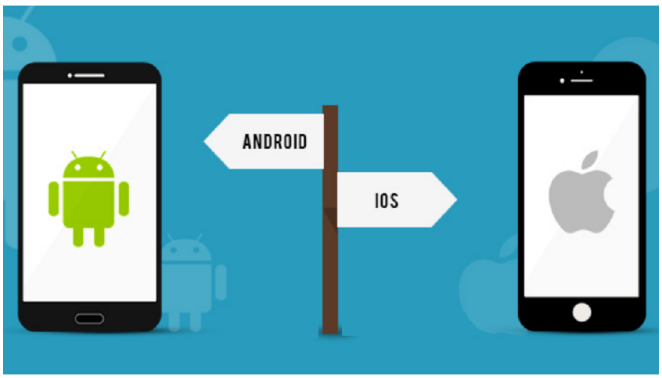


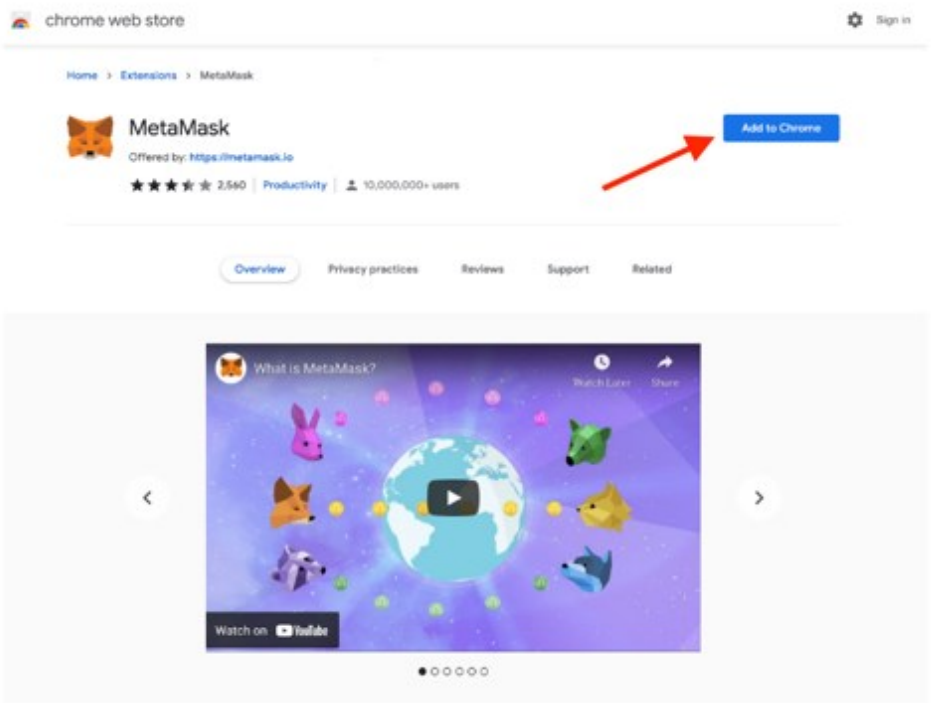
Figura 34 - Sistemas de smartphones compatíveis com a MetaMask

No caso de uso da MetaMask em smartphones, é necessário a instalação do aplicativo.

Instalação da MetaMask

Para fins de exemplo, neste trabalho a MetaMask será utilizada no navegador Chrome. A seguir, tem-se um passo-a-passo, disponibilizado em (Introdução à MetaMask, 2023), de como instalar a carteira MetaMask no navegador Chrome.

1. Acesse https://metamask.io/
2. Clique em "Download" (Baixar) na barra de menus.
3. Clique em "Install MetaMask for Chrome" (Instalar a MetaMask para o Chrome). Você será direcionado para o Chrome Web Store.



4. Clique em "Add to Chrome" (Adicionar ao Chrome).
5. Na janela pop-up, clique em "Add extension" (Adicionar extensão).

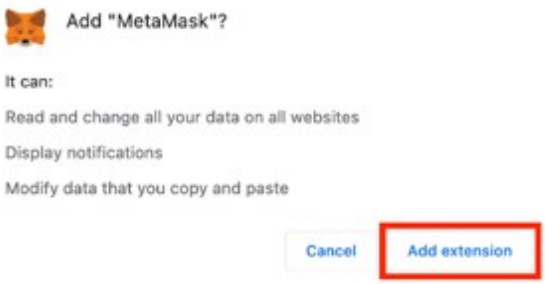


Figura 35 - Passo-a-passo para instalação da carteira MetaMask.

Depois de adicionar a extensão ao navegador, o usuário pode optar por adicionar um atalho da MetaMask na barra de ferramentas do navegador, clicando no ícone de quebra-cabeça, no canto superior direito do navegador e, depois, no ícone de pino. Veja a Figura 36 a seguir.

Figura 36 - Fixando a MetaMask na barra e ferramentas do navegador.

Caso contrário, basta acessar as extensões do navegador e procurar por MetaMask.

Criação e Segurança da MetaMask

O primeiro acesso à carteira é dedicado à criação e segurança da carteira. O usuário irá se deparar com a tela ilustrada na Figura 37 abaixo, retirada de (Alexandre, 2022).

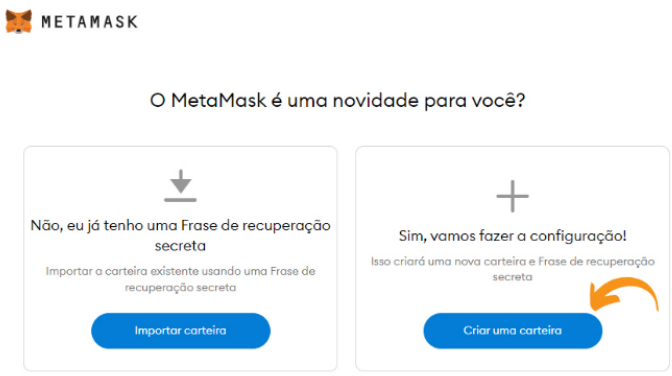


Figura 37 - Tela de primeiro acesso à MetaMask.

Note que existem duas opções: uma para o usuário que já tem uma carteira MetaMask e deseja recuperá-la, e outra para o usuário que está acessando-a pela primeira vez e que deseja configurá-la.

Devido a atualizações da MetaMask, pode haver pequenas variações nas telas apresentadas nesse trabalho. A fase de configuração mostrada na imagem anterior também pode ser exibida como na Figura 38 a seguir.

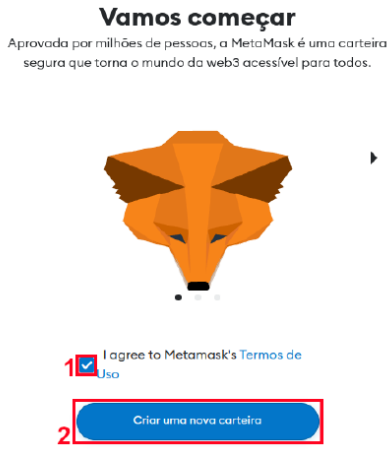


Figura 38 - Tela de acesso à criação da MetaMask.

Figura 39 - Tela de solicitação de compartilhamento de dados.

Após clicar na opção *criar uma carteira*, como na Figura 37, ou em *criar uma nova carteira*, como na Figura 38, a MetaMask perguntará se o usuário deseja compartilhar dados para melhorar a plataforma, conforme mostrado na Figura 39 acima, retirada de (Alexandre, 2022). Esse compartilhamento é opcional e cada usuário decide se aceita ou não.

Após esse momento, inicia-se uma fase importante da configuração da carteira, que diz respeito às senhas. A primeira senha a ser cadastrada é a de acesso à carteira MetaMask e será pedida sempre que o usuário desejar utilizá-la. Veja a Figura 40 a seguir, retirada de (Alexandre, 2022), que ilustra o cadastro dessa senha.

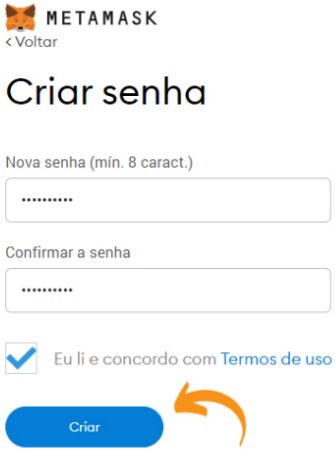


Figura 40 - Tela de cadastro da senha de acesso à carteiro MetaMask.

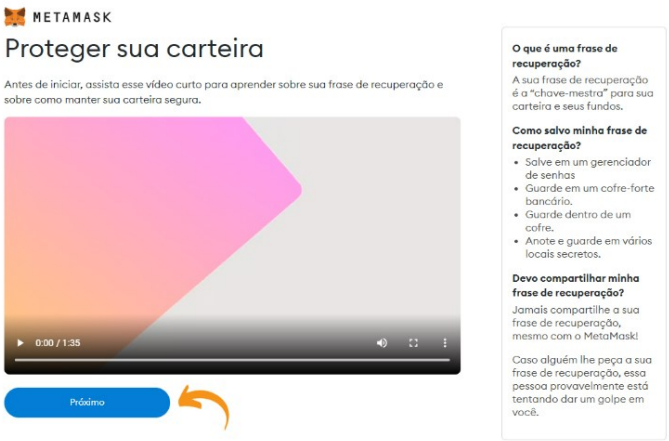


Figura 41 - Vídeo explicativo sobre a frase de recuperação.

É importante o usuário ter pleno conhecimento de que a MetaMask não é capaz de recuperar essa senha de acesso futuramente. Repare que o usuário não cadastra nenhum e-mail de recuperação ao instalar e configurar a MetaMask.

Feito isso, a MetaMask apresentará um vídeo explicando o que é a frase de recuperação, como exibido na Figura 41 acima.

É extremamente importante que o usuário assista ao vídeo e tome os devidos cuidados para armazenar suas senhas. Muitas criptomoedas se perdem pelo fato de os usuários perderem acesso às suas carteiras e, consequentemente, aos seus fundos. Em carteiras não custodiantes como a MetaMask, o usuário é o único responsável pelas suas criptomoedas.

Na tela seguinte, a MetaMask exibirá a seed, ou seja, a frase de recuperação, que é um conjunto e palavras que os usuários utilizam para se conectar às suas carteiras, independente dos dispositivos que estejam usando. Ao contrário da senha de acesso que serve apenas para desbloquear o acesso à carteira. Veja na Figura 42 abaixo um exemplo de exibição de seed na MetaMask.

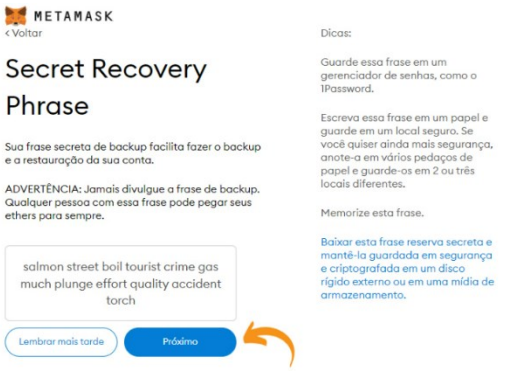


Figura 42 - Exemplo de uma seed na MetaMask.

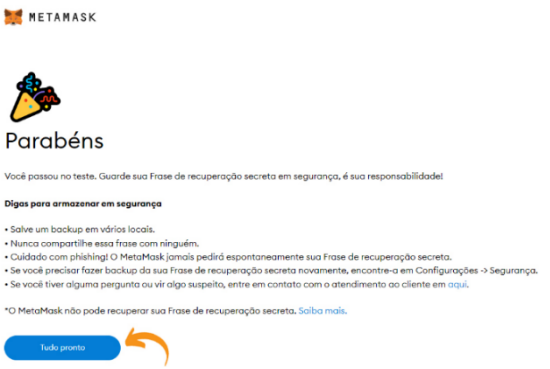


Figura 43 - Finalização do processo de criação da carteira MetaMask.

Os usuários devem guardar essa frase de maneira offline para, caso seus aparelhos sejam roubados ou invadidos, eles não sejam vítimas de hackers que podem querer roubar suas criptomoedas. A comunidade cripto recomenda que o usuário guarde sua frase de recuperação em um ou mais locais que só o próprio tenha acesso.

A ordem das palavras que compõem a *seed* é de grande relevância para recuperar a carteira futuramente. Com a *seed*, qualquer pessoa em qualquer lugar do mundo pode acessar novamente sua carteira a partir de um dispositivo com conexão à internet, mesmo que não tenha mais a senha de acesso. Ao recuperar uma carteira com a *seed*, o usuário cadastra uma nova senha de acesso à carteira.

Essa é a última etapa de criação da carteira. O processo é finalizado exibindo a Figura 43 acima.

O usuário que porventura perder a *seed*, mas que ainda possua acesso a carteira, consegue recuperar a seed acessando as configurações da carteira e, depois, escolhendo o menu *segurança e privacidade*. A seguir será visto como acessar essa opção.

Funcionalidades e Configuração da MetaMask

Uma vez que a MetaMask está instalada no navegador, inicia-se o processo de configuração da carteira. Ao clicar no ícone da MetaMask adicionado a barra de ferramentas do navegador, a MetaMask abre como um pop-up, conforme a Figura 44 a seguir.

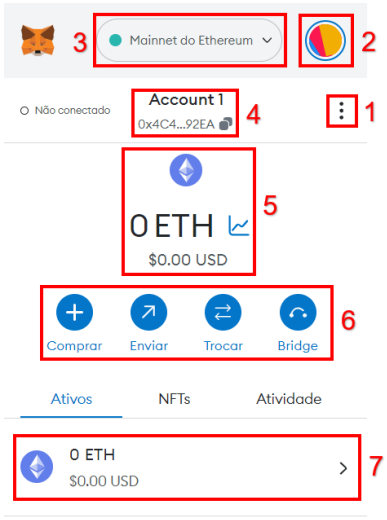


Figura 44 - Tela inicial da Metamask.

A seguir, será descrito cada funcionalidade destacada na imagem anterior.

1) Nesse item o usuário tem quatro opções, que são: ver conta no explore; expandir exibição; detalhes da conta; sites conectados.
2) Local onde o usuário pode criar mais contas, importar uma conta, conectar uma carteira de hardware, acessar a página de suporte da MetaMask e acessar as configurações. Inicialmente, o usuário possui apenas uma conta cadastrada.
3) Indica a rede na qual a carteira está conectada e é onde o usuário pode adicionar e acessar outras redes à carteira.
4) Este item exibe o nome da conta que o usuário está utilizando (no caso, Account 1) e, logo abaixo, o endereço da conta utilizado para receber tokens (criptomoedas).
5) Indica o símbolo da blockchain utilizada pela rede que está sendo exibida e, abaixo, o valor dos tokens nativos que o usuário possui na blockchain utilizada. Na imagem acima, temos a rede Ethereum que usa a blockchain da própria Ethereum e uma quantidade de 0 ETH, que é o token nativo da blockchain da Ethereum.
6) Local onde o usuário pode comprar criptomoedas com moeda fiduciária, enviar criptomoedas para outras carteiras, realizar troca entre criptomoedas e fazer pontes entre redes.

7) Indica a quantidade e o valor dos tokens (criptomoedas) que o usuário possui na rede exibida. Também é onde o usuário pode adicionar novos tokens à rede. Se o usuário receber tokens que ainda não foram adicionados por ele à carteira, eles não serão exibidos a menos que o usuário o faça.

Como é possível verificar, são muitas as funcionalidades e não é o foco deste trabalho mostrar uma a uma. Iremos focar na adição de rede e de tokens que será crucial para as seções futuras.

A MetaMask possui a rede da Ethereum como padrão. Como a rede Ethereum prioriza a segurança e ainda mantém um grau considerável de descentralização, a escalabilidade dessa rede (capacidade de negociações por segundo) fica aquém do desejável se comparada com bancos centralizados. Um outro fator que pesa contra a rede Ethereum são as taxas de transação consideradas elevadas.

Como alternativa, outras redes baseadas na rede Ethereum surgiram com um menor grau de segurança, porém com uma maior escalabilidade e custos de operação menores. Como exemplo, temos as redes da Polygon, Arbitrum, Optimism. Essas redes, apesar de serem consideradas menos seguras que a rede Ethereum, ainda possuem um considerável grau de segurança. Tanto é que movimentam uma alta quantidade de dinheiro. Sendo assim, essas redes são boas opções aos usuários que não desejam pagar as taxas mais elevadas que atualmente são praticadas na rede Ethereum.

Um outro fator que favorece a utilização das redes que surgem como uma alternativa ao uso da rede Ethereum é que a carteira MetaMask se conecta com essas e algumas outras redes. Basta o usuário adicioná-las à carteira para começar a interagir com elas. Como exemplo, será mostrado como adicionar a rede da Binance Smart Chain (BSC) à MetaMask. Veja as imagens a seguir.

Figura 46 - Processo para adicionar uma rede à MetaMask.

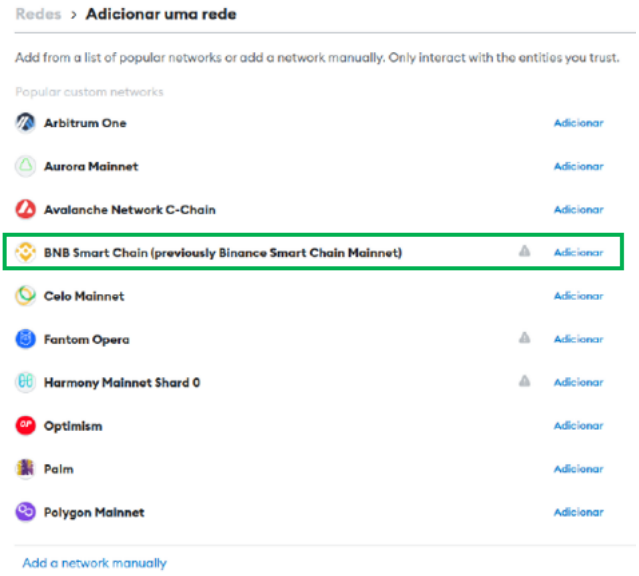


Figura 47 - Algumas redes compatíveis com a MetaMask.

Ao acessar a MetaMask, o usuário deve clicar no botão que indica a rede em que a carteira está conectada, no caso, Mainnet do Ethereum, e, depois, clicar no botão adicionar rede, conforme indicado na Figura acima. Feito isso, o usuário será direcionado à tela ilustrada pela Figura 47 acima.

Agora, basta clicar em adicionar para seguir o procedimento de adição da rede pretendida. Veja a Figura 8 a seguir.

Figura 48 - Tela de aprovação para inserção da rede BSC à MetaMask.

Figura 459 - Tela exibida pela MetaMask após mudança da rede Ethereum para rede BSC.

Ao clicar em Aprovar, o processo de adição da rede BSC à MetaMask será finalizado. A Figura 459 acima mostra a mensagem de adição realizada com sucesso.

Pronto! Agora a rede BSC aparecerá como opção para o usuário quando ele clicar no botão que indica a rede conectada à carteira. Caso ele deseje mudar para a rede BSC, basta clicar sobre BNB Smart Chain, conforme a Figura 504650 abaixo.

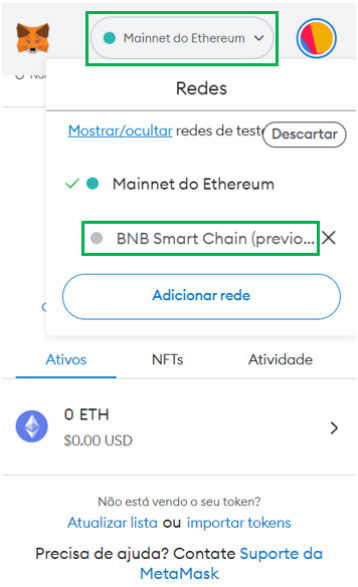


Figura 5046 - Tela com passo-a-passo para selecionar a rede Polygon.

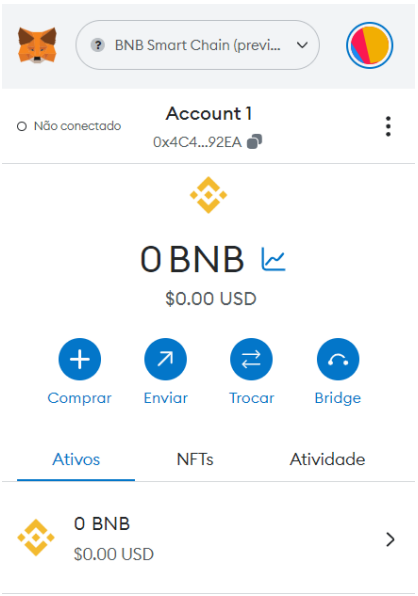


Figura 5147 - Adição da rede Polygon à MetaMask realizada com sucesso.

Assim, encerra-se o procedimento para adicionar e conectar uma rede à MetaMask. O procedimento é análogo para a adição de qualquer uma das outras redes disponíveis. A tela exibida pela MetaMask após a mudança de rede é mostrada abaixo.

A partir de agora será mostrado como adicionar um token (criptomoeda) à uma rede da carteira MetaMask. É extremamente importante que os usuários tenham ciência de que uma rede não suporta qualquer tipo de token. Como exemplo, o BTC não é suportado em nenhuma das redes compatíveis com a MetaMask. Se um usuário enviar token BTC para uma das redes conectadas à MetaMask, ele perderá as moedas.

O processo de adição de tokens à uma das redes compatíveis com a MetaMask serve para deixar o saldo referente a tais tokens visível na carteira.

Ou seja, será visto que o token MATIC, nativo da rede Polygon, é compatível na rede Ethereum. Porém, se ele for enviado para a MetaMask do usuário na rede Ethereum sem que ele tenha sido adicionado em tal rede, o usuário não conseguirá visualizar seu saldo aplicado nesse token. Contudo, os tokens não estarão perdidos! Basta adicioná-los à rede de interesse, no caso, a Ethereum, que o usuário conseguirá visualizar seu saldo de tokens MATIC em tal rede. Veja a Figura 52482 abaixo.

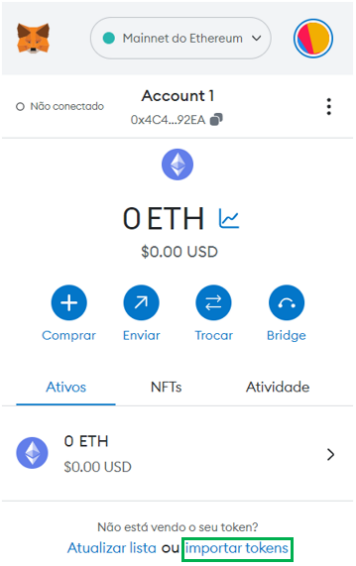


Figura 5248 - Token nativo dessa rede.

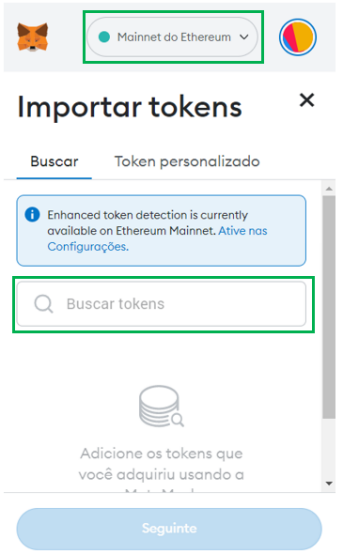


Figura 53 - Tela de busca do token a ser adicionado.

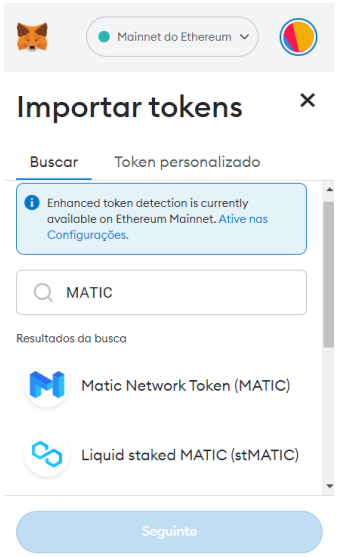


Figura 54 - Busca do token MATIC através de digitação no campo de busca.

Observe que o único token cadastrado na rede Ethereum é o token ETH, que é nativo dessa rede. Clicando no link importar tokens, como indicado na Figura 524852 acima, podemos adicionar outros tokens compatíveis com a rede Ethereum, por exemplo, o token MATIC. Veja a Figura acima.

É importante observar que a MetaMask já está conectada à rede Ethereum, que é a rede onde desejamos adicionar o token MATIC. Para cada rede em que o token MATIC se conecta existe um contrato específico para que se possa realizar tal conexão.

Agora podemos buscar pelo token escrevendo MATIC no campo de busca ou colar o contrato do token MATIC com a rede Ethereum no campo de busca. Ao digitar MATIC no campo de busca, chega-se na Figura 4 acima.

Feito isso, basta selecionar o token MATIC dentre as opções que aparecerão. Entretanto, também é possível colar no campo de entrada o contrato do token MATIC com a rede Ethereum. Nesse caso, aparecerá como opção de seleção apenas o token desejado.

O contrato do token MATIC com a rede Ethereum pode ser encontrado em sites como:

- CoinMarketCap: https://coinmarketcap.com/pt-br/
- CoinGecko: https://www.coingecko.com/pt

que são considerados sites confiáveis, segundo (Alexandre, 2022).

Acessando o site CoinGecko, tem-se a sua tela inicial ilustrada pela Figura 495 abaixo.

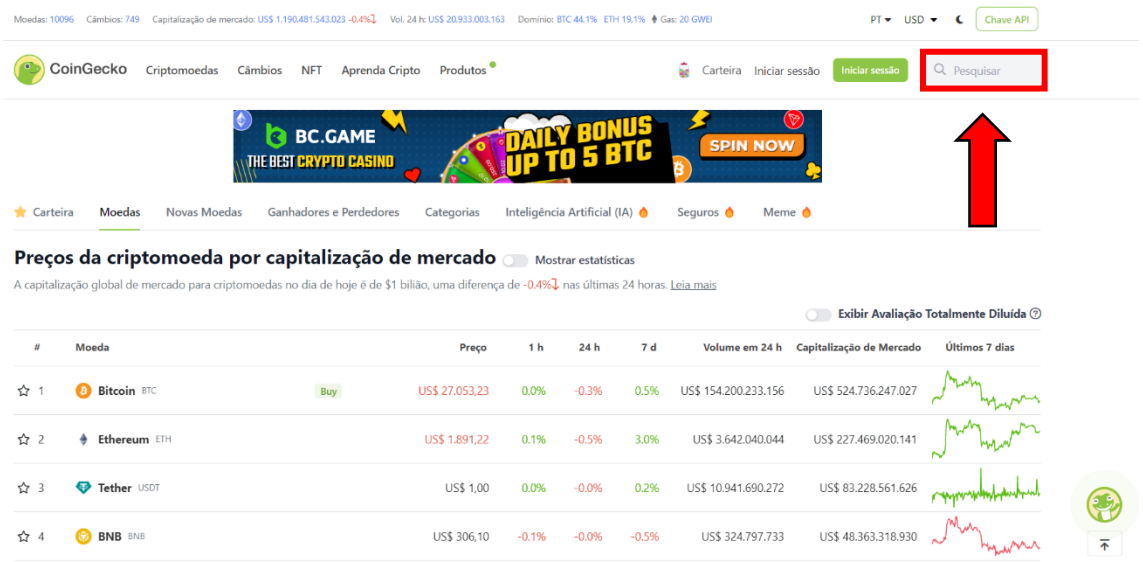


Figura 495 - Tela inicial do site CoinGecko.

Ao digitar MATIC no campo de busca, indicado na Figura 495 acima, encontra-se os resultados exibidos na Figura 506 abaixo.

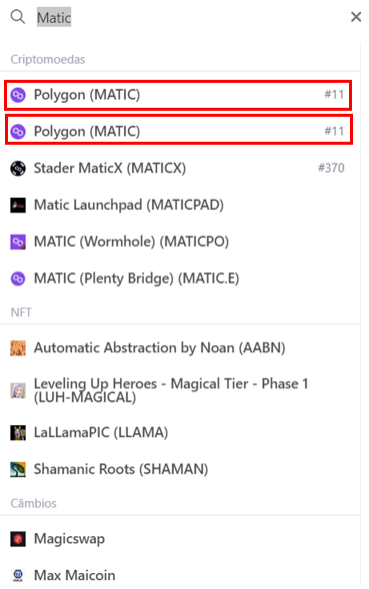


Figura 506 - Resultados da busca do token MATIC no CoinGecko.

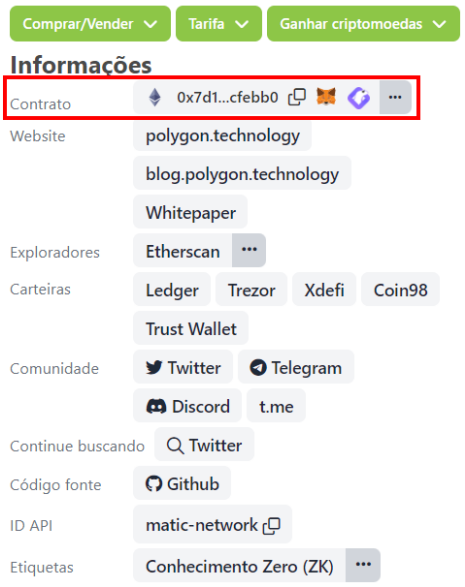


Figura 517 - Contratos do token MATIC com outras redes.

Ao selecionar qualquer uma das opções indicadas na imagem acima, somos encaminhados a uma outra tela onde encontra-se o contrato do token MATIC com a rede Ethereum. Veja um recorte da tela na Figura 517 acima.

O primeiro contrato que aparece é o do token MATIC com a rede Ethereum. É sabido que esse contrato do token MATIC é com a rede Ethereum, pois aparece o símbolo da rede Ethereum antes do início da chave do contrato. Basta copiar essa chave do contrato e colar no campo de busca de token na carteira MetaMask conectada à rede Ethereum. Caso o usuário queira o contrato do token MATIC com outras redes, basta clicar nos “três pontinhos”, ao final do campo destacado na imagem acima, que aparecerá outros contratos do token MATIC com outras redes.

Colocando a chave do contrato do token MATIC com a rede Ethereum na carteira MetaMask vinculada a rede Etehreum, chega-se na tela ilustrada pela Figura 8 abaixo.

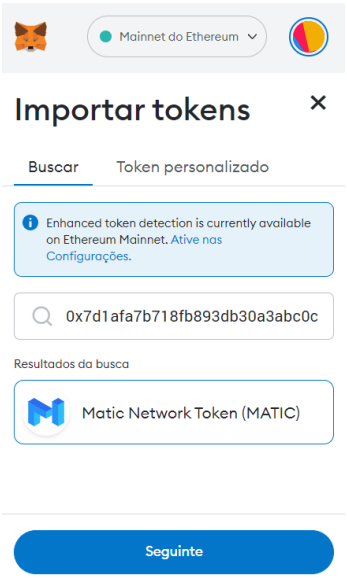


Figura 58 - Busca do token MATIC na rede Ethereum através do contrato.

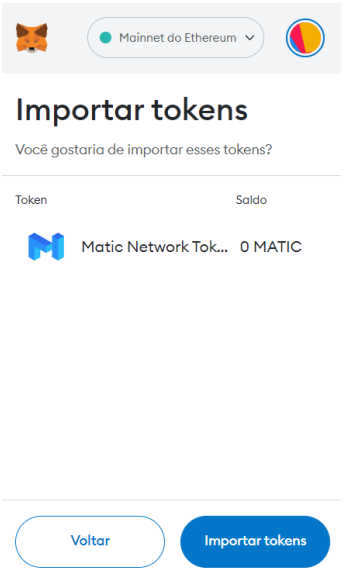


Figura 529 - Tela de confirmação da adição do token MATIC à rede Ethereum.

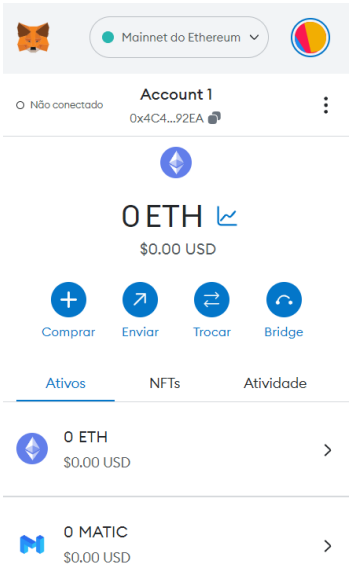


Figura 60 - Token MATIC visível na carteira MetaMask vinculada à rede Ethereum.

Agora é só selecionar o token MATIC e clicar no botão *seguinte*. O usuário será direcionado para uma tela de confirmação, conforme a Figura 529 acima.

Clica-se em *importar tokens* e pronto! Ao retornar a tela inicial da MetaMask vinculada à rede MATIC é possível visualizar a quantidade e o saldo do token MATIC nessa rede. Veja a Figura 60 acima.

5.2 Montando uma Piscina de Liquidez na Uniswap

Antes de efetivamente iniciar o processo de montagem de uma piscina de liquidez, é pudente que o termo Piscina de Liquidez seja mais explorado para que ele fique mais claro e, assim, faça sentido criar uma piscina.

Uma piscina de liquidez (liquid pool) funciona de forma semelhante a uma Casa de Cambio. No caso da Casa de Câmbio, ela disponibiliza algumas moedas fiduciárias para pessoas interessadas em fazer trocas e, como consequência, ganha taxas com isso. A piscina de liquidez disponibiliza tokens (criptomoedas) para pessoas interessadas em fazer trocas e, também como consequência, ganha taxas com isso.

O inovador no caso das piscinas de liquidez é que qualquer pessoa pode prover liquidez através de uma corretora descentralizada e receber taxas por isso, ou seja, a pessoa passa a fazer o papel do banco. Isso rompe com uma estrutura financeira tradicional, eliminando intermediários e reduzindo taxas.

Segundo (O que é um pool de liquidez, 2022), “um pool de liquidez é um grupo de tokens que são bloqueados em um contrato inteligente e usados para negociação entre ativos em uma corretora descentralizada (DEX) como a Uniswap”.

Desta forma, qualquer pessoa que possui, por exemplo, ether (ETH) e dólar (USDT) pode assumir o papel de provedor de liquidez, buscar uma corretora descentralizada (DEX) e criar uma piscina de liquidez com esses tokens. Ao formar a piscina, os tokens ficam bloqueados pela corretora até que o provedor de liquidez decida desfazer a piscina.

Na Uniswap uma piscina de liquidez pode ser desfeita a qualquer momento, basta que o provedor queira desfazê-la. Enquanto a piscina estiver formada e outros usuários, indiretamente, acessarem ela para realizar trocas, o provedor ganhará taxas.

Quando é dito que os usuários acessam indiretamente uma piscina, é porque, de fato, o usuário não escolhe qual piscina deve acessar para realizar uma troca. Ele apenas indica quais tokens deseja trocar e a própria corretora (DEX) se encarrega de buscar a piscina que gere menor taxa ao usuário.

Montando uma piscina na Uniswap V2

Para montar uma piscina de liquidez em Uniswap V2 o usuário precisa acessar a Uniswap através do endereço https://app.uniswap.org/. A Figura 61 mostra a tela inicial da Uniswap.

Figura 61 - Tela inicial da Uniswap.

A seguir, será descrito cada funcionalidade destacada na Figura 1.

1) Local onde o usuário acessa o ambiente de troca entre tokens.
2) Local onde o usuário cria e acessa as suas piscinas.
3) Indica a rede na qual a Uniswap está conectada. Nesse mesmo local é possível acessar outras redes compatíveis com a Uniswap, como Polygon, Arbitrum, etc. Na imagem acima, tem-se a Uniswap conectada à rede Ethereum.
4) Local destinado para o usuário conectar uma das carteiras compatíveis com a Uniswap.

Ao clicar sobre o link *piscinas*, indicado no campo 2, o usuário é direcionado para a tela a seguir.

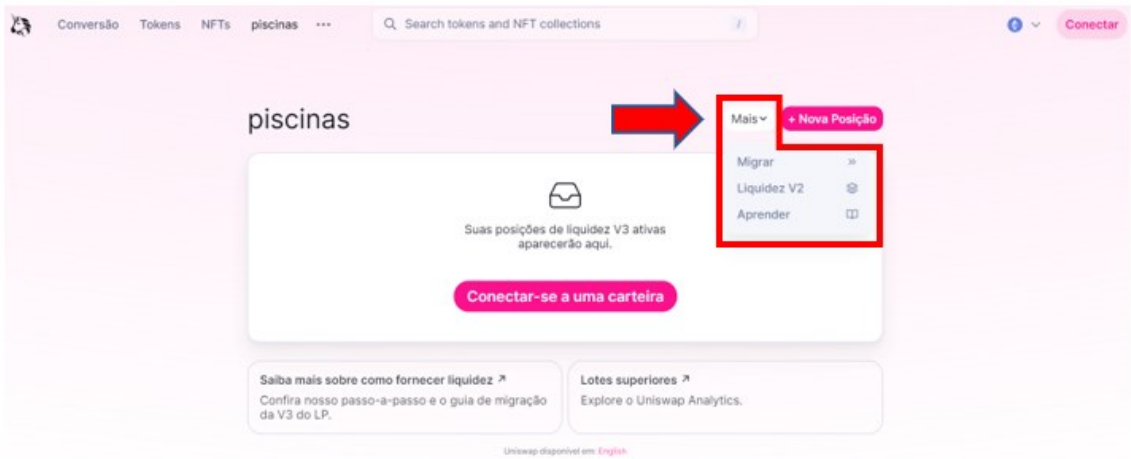


Figura 62 - Tela para formação de piscinas na rede Ethereum.

Quando se está conectado à rede Ethereum fica disponível um campo escrito *Mais*, indicado acima na Figura 2, que, ao clicá-lo, nos dá a possibilidade de formar uma piscina em Uniswap V2. Essa opção não aparece quando a Uniswap está conectada às outras redes disponíveis.

Observe que na parte central da Figura 2 existe a opção de conectar a sua carteira à Uniswap. Se o usuário conectar sua carteira e já tiver alguma piscina montada na rede Ethereum, a piscina aparecerá na parte central da tela, no espaço onde aparece escrito *Conectar-se a uma carteira*.

Ao clicar em Liquidez V2, o usuário é direcionado a uma tela, conforme Figura 3 abaixo.

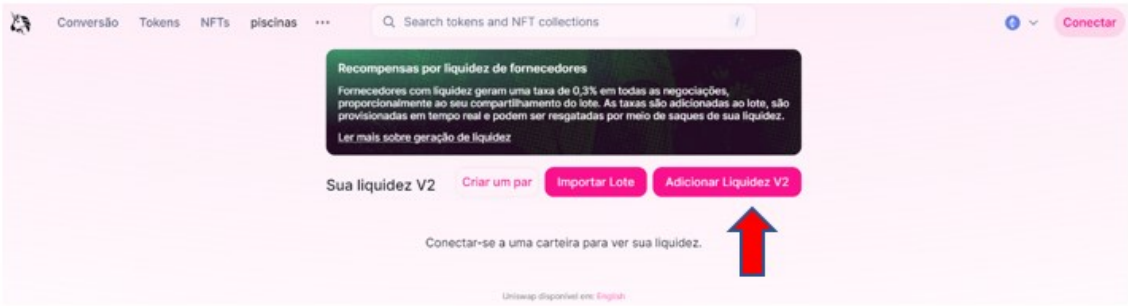


Figura 63 - Tela de acesso às piscinas em Uniswap V2.

Clicando em *Adicionar Liquidez V2*, indicado acima na Figura 3, o usuário é levado a uma tela onde vai escolher os tokens a serem disponibilizados na piscina e determinar as quantidades deles dentro dos limites do seu saldo em carteira e respeitando a proporção de 50% do valor da piscina em cada token. Veja a Figura 4 a seguir.

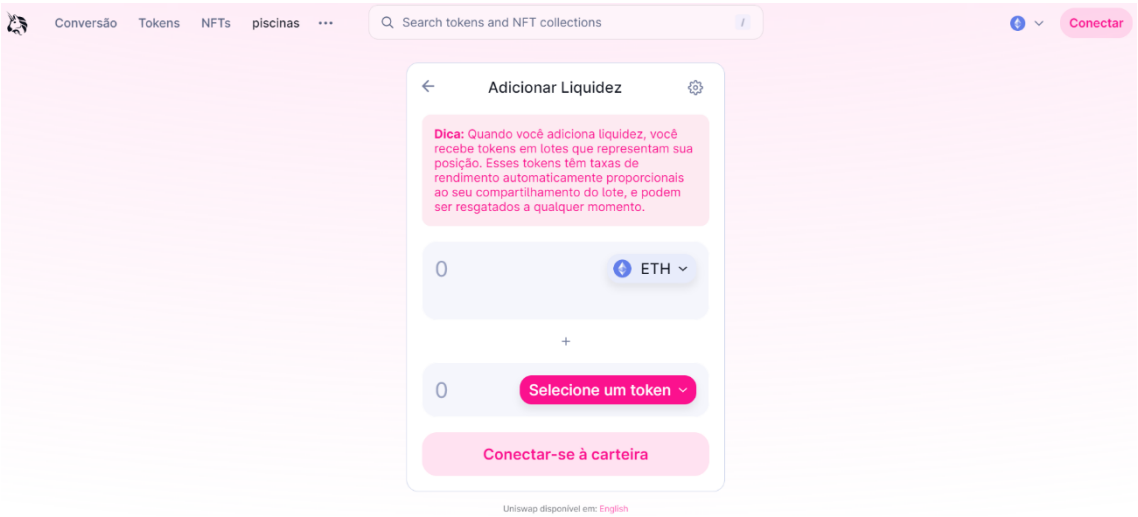


Figura 64 - Tela de montagem de uma piscina em Uniswap V2.

A partir desta etapa é necessário ter saldo em carteira e conectá-la a Uniswap para concretizar a formação da piscina. Para não ser redundante, optou-se por mostrar a conexão da carteira apenas uma vez. Essa conexão será exibida durante a montagem de uma piscina na Uniswap V3.

Montando uma piscina na Uniswap V3

Após acessar o link que dá acesso as piscinas, na página inicial da Uniswap, o usuário deve clicar no botão + *Nova Formação*, indicado na Figura 5 abaixo.

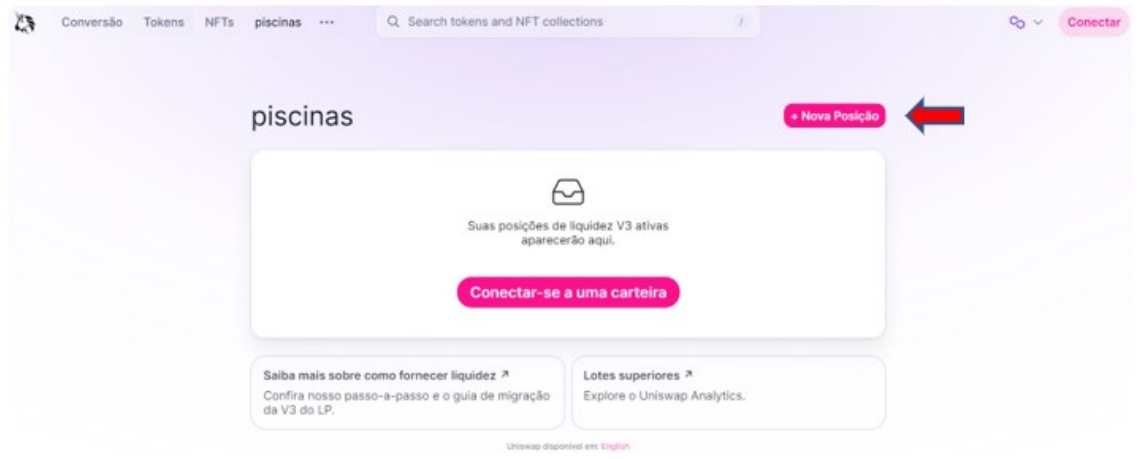


Figura 65 - Tela de acesso às piscinas na Uniswap V3.

Note que na figura 51 não aparece o botão *Mais*, como visto anteriormente na imagem 48. Isso ocorre porque na Figura 5 a Uniswap está conectada à rede

Polygon. A criação de piscinas na Uniswap V3 é análoga para todas as redes disponíveis na Uniswap.

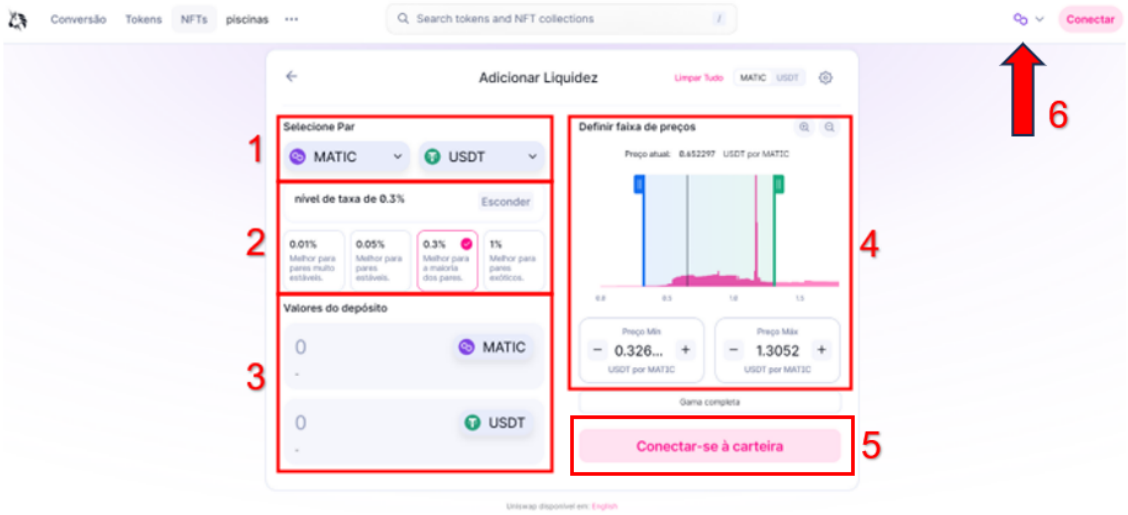


Figura 66 - Tela de formação de uma piscina em Uniswap V3.

A seguir, detalharemos cada campo indicado na Figura 6.

1) Local onde o usuário escolher o par de tokens que deseja disponibilizar.
2) Local onde o usuário escolhe a taxa que deseja receber referente às negociações na piscina. É importante observar que cada taxa disponível possui uma recomendação para determinados pares de tokens disponibilizados.
3) Local onde o usuário determina as quantidades de cada token que deseja disponibilizar de acordo com seu saldo em carteira. Essas quantidades influenciam diretamente no intervalo do campo 4 e, no caso das piscinas em V3, não precisam, necessariamente, seguir a proporção de 50% do valor da piscina para cada token.
4) Local onde o usuário determina o intervalo de preços de um token em relação ao outro que deseja fornecer liquidez. Esse intervalo influencia diretamente nas quantidades de tokens escolhidas no campo 3.
5) Local onde o usuário conecta-se à carteira.
6) Local que indica a rede onde a piscina está sendo montada. O símbolo na imagem Figura remete à rede Polygon.

Uma vez que essas informações forem preenchidas, basta conectar-se à uma carteira, clicando no campo 5. Feito isso, o usuário será direcionado à tela representada pela Figura 537 abaixo.

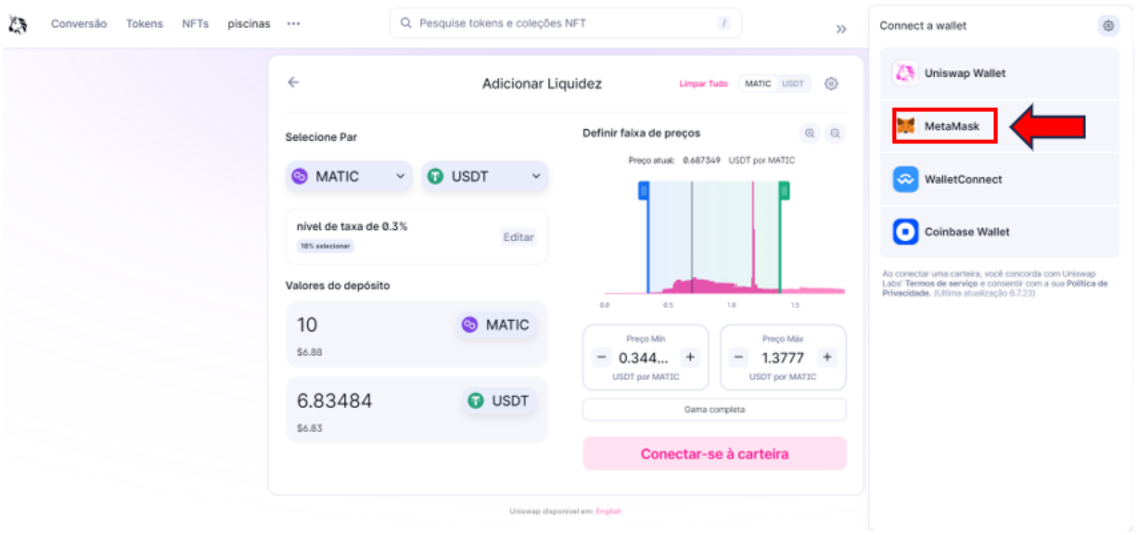


Figura 537 - Conectando à carteira.

Note que foi selecionado uma taxa de 0,3%, além de $10\ MATIC$ para formar a piscina. Automaticamente, foi preenchido a quantidade de $6{,}83484\ USDT$. A faixa de preço entre os dois tokens escolhidos não foi alterada. Ao clicar na MetaMask, chega-se na Figura 548 abaixo.

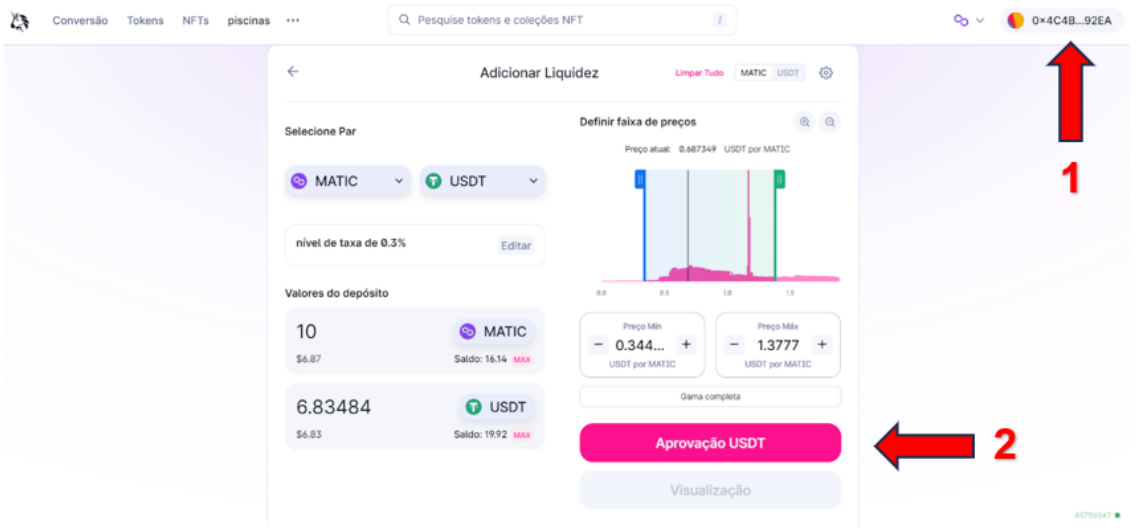


Figura 548 - Tela de aprovação da montagem da piscina.

Observe que a carteira já está conectada, como se vê na seta 1 na Figura 548 acima. Para prosseguir, clica-se no campo *Aprovação USDT* indicado pela seta 2. Assim, chega-se na Figura abaixo.

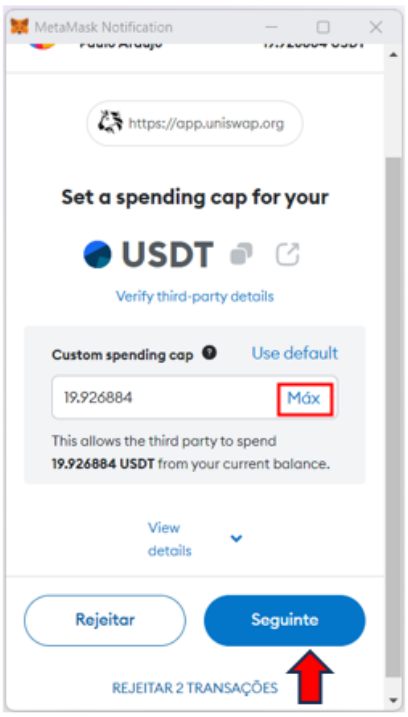


Figura 69 – limite de gasto personalizado.

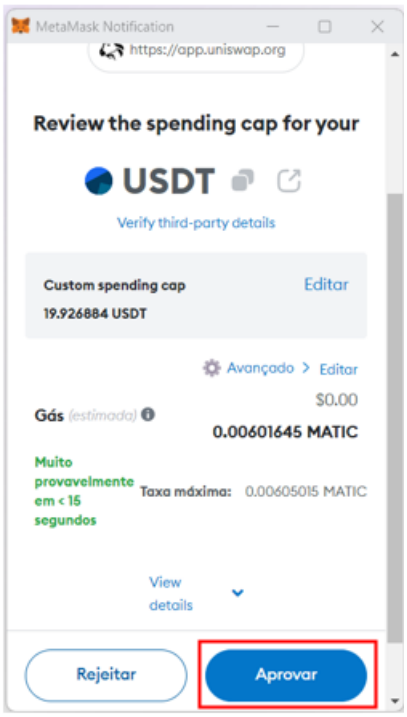


Figura 70 - Revisão do limite de gastos.

Define-se o limite de gastos selecionando a opção *Máx* e depois clica-se no campo *Seguinte*, conforme destacado na Figura acima, para revisar e aprovar, como destacado na Figura 70 acima. Assim, o usuário é direcionado para a Figura 1 abaixo.

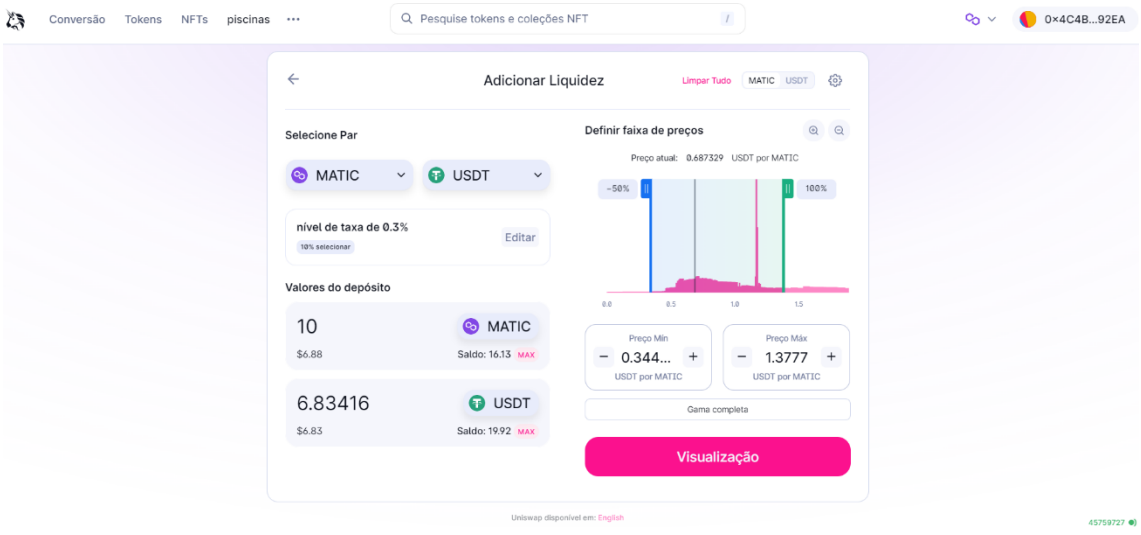


Figura 71 – Tela de visualização.

Nessa etapa o usuário deve clicar na opção *Visualização* conforme pode ser vista na Figura 1 acima.

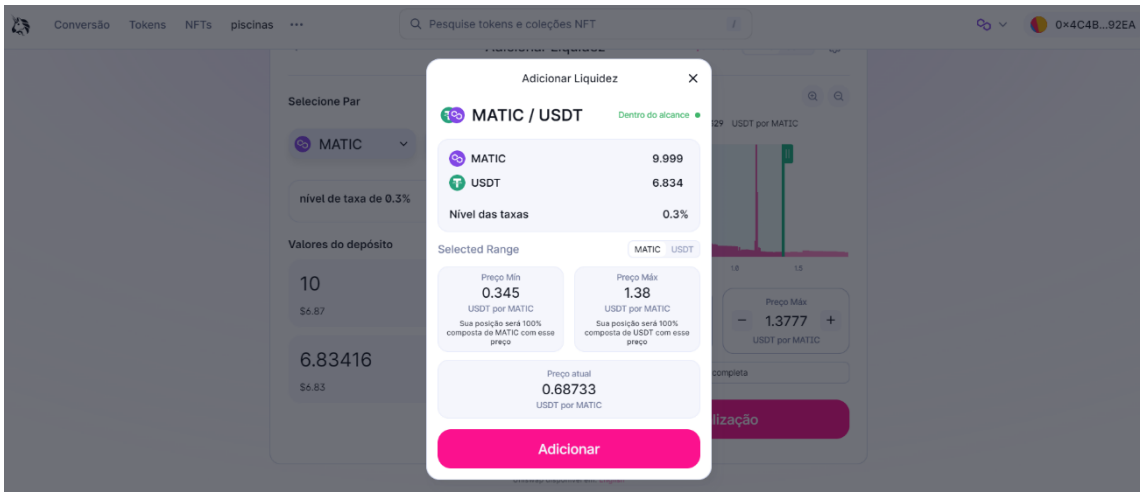


Figura 72 - Tela de visualização da configuração da piscina.

A Figura 2 mostra a configuração da piscina e, se o usuário estiver de acordo, basta clicar em *Adicionar*.

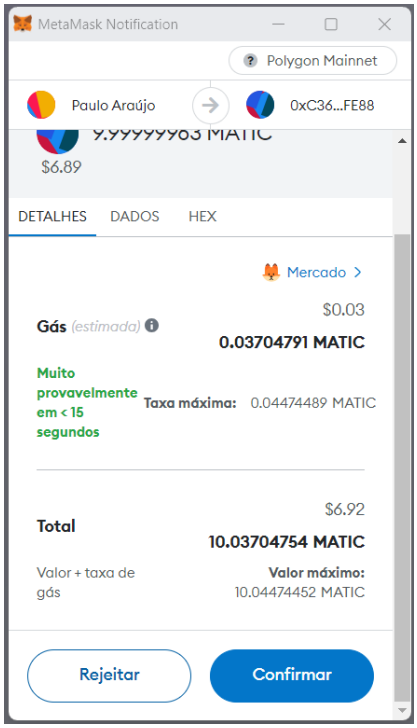


Figura 73 - Confirmação da montagem da piscina na MetaMask.

Na Figura 3 acima o usuário visualiza as taxas cobradas e conclui a montagem da piscina clicando em *Confirmar*. Pronto! A piscina está criada.

Para visualizar a piscina, basta clicar no campo *Piscinas* na tela inicial da Uniswap, conforme visto na Figura 1 nessa seção. Feito isso, o usuário será direcionado à Figura 4 abaixo.

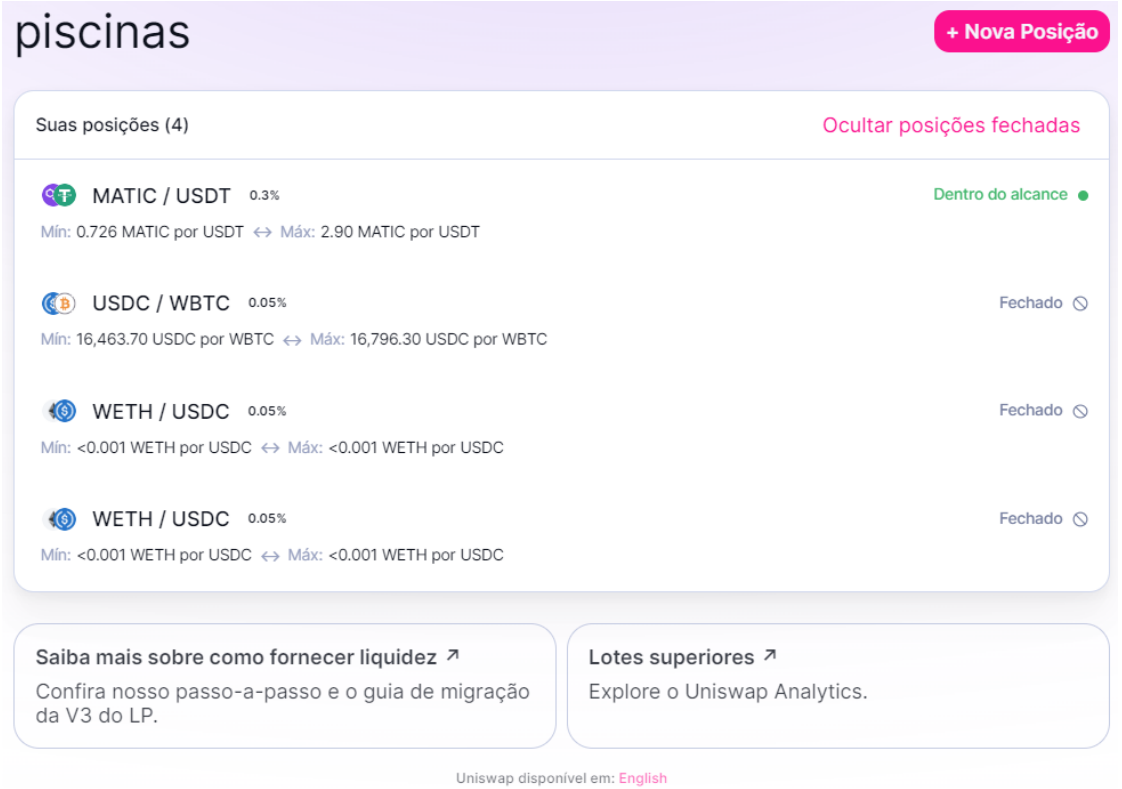


Figura 74 - Tela de exibição das piscinas.

Note que há quatro piscinas: a primeira, que acabou de ser criada, está em aberto e dentro da faixa, e as três últimas que já foram fechadas. Ao clicar nas piscinas fechadas o usuário consegue visualizar algumas informações de montagem dessas piscinas. Porém, uma vez fechada, não há mais o que fazer.

Para as piscinas abertas, o usuário pode clicar sobre elas, e checar informações do andamento da piscina. A Figura 5 a seguir mostra a primeira piscina da Figura 4 acima, que acabou de ser criada.

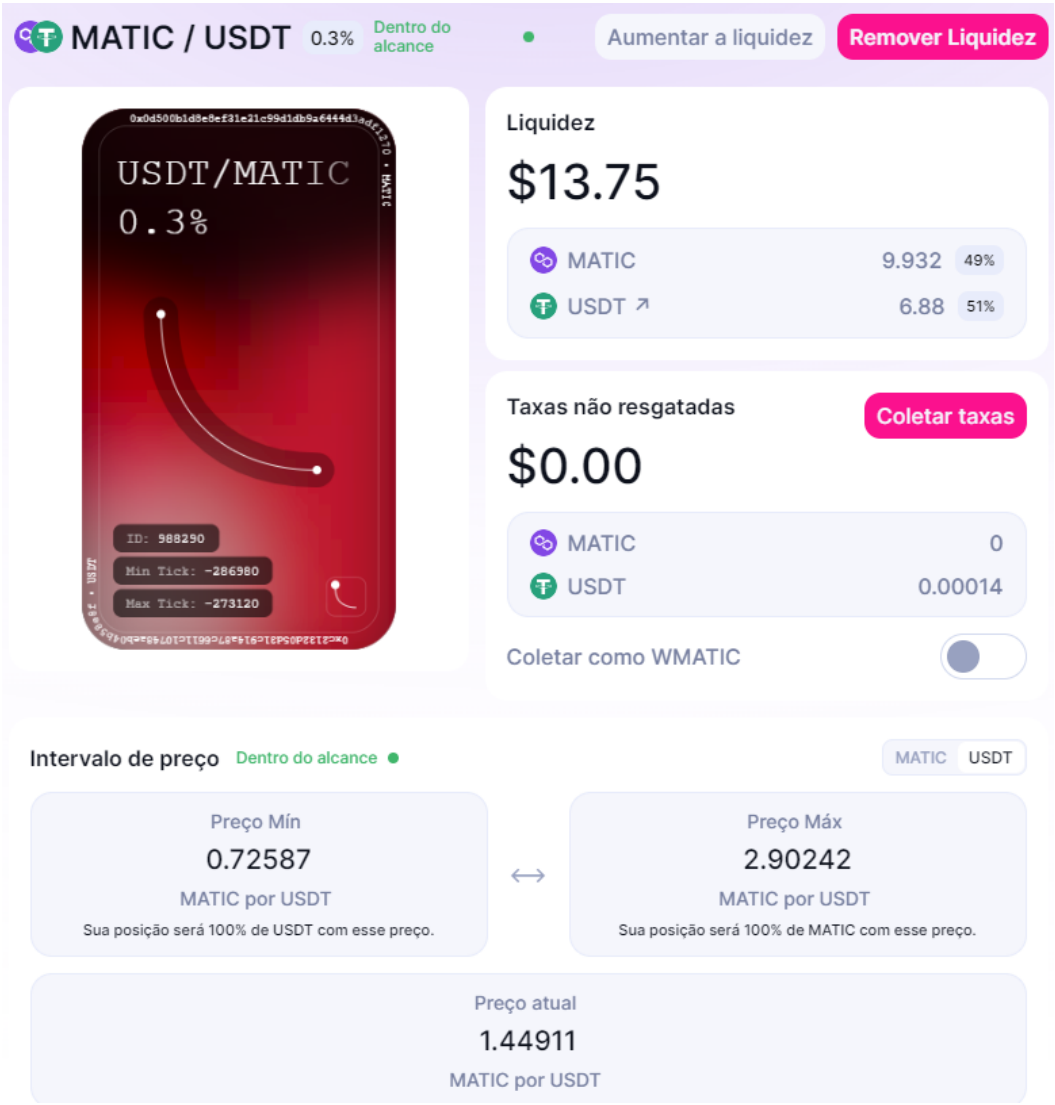


Figura 75 - Piscina de liquidez.

Finalmente, tem-se a piscina de liquidez que acabou de ser criada. Nela aparecem informações como:

- o valor investido ($13,75);
- taxas não resgatadas ($0,00);
- faixa de preços entre os tokens (0,72587 à 2,90242 $MATIC$ por $USDT$);
- opção para remover liquidez (fechar a piscina);
- opção para coletar as taxas recebidas.
- o valor atual de $MATIC$ por $USDT$ (1,44911);
- taxa que o provedor ganhará por negociação na piscina
- opção para aumentar liquidez.

CONCLUSÃO

Apesar de esse trabalho abordar um tipo de aplicação financeira, em momento nenhum existe a intenção por parte do autor de indicar essa aplicação ou fazer propaganda de alguma criptomoeda específica. Todas as criptomoedas citadas ao longo do texto foram escolhidas para fins de exemplo. Privilegiou-se aquelas com maior volume de negociação ou ligadas a alguma rede citada no texto por se acreditar que elas possam ser mais reconhecidas pelas pessoas.

Como pode ser visto na seção 4.1.2, as piscinas de liquidez podem ser rentáveis ou gerar prejuízos para os provedores. As criptomoedas, em geral, são consideradas ativos muito voláteis, ou seja, com grande variação em seus preços. Assim, a perda impermanente (impermanent loss) de um uma piscina de liquidez pode ser significativamente impactada pela volatilidade das criptomoedas escolhidas ao montar a piscina.

Outro ponto a se destacar é que o provedor de liquidez na Uniswap V2 só ganha taxas quando sua piscina é acessada para negociação. No caso da Uniswap V3, o provedor só ganha taxas quando a relação de preços entre as criptomoedas escolhidas estiver dentro da faixa de preços estipulada inicialmente por ele e quando houver negociação na piscina.

A perda impermanente (impermanent loss), de fato, só ocorre quando o provedor decide encerrar a piscina e caso a relação de preços entre as criptomoedas escolhidas seja diferente se comparada com o momento de montagem da piscina. O fato de o mercado cripto ser bastante volátil faz com que o autor considere esse tipo de aplicação arriscada.

É possível explorar o estudo de piscinas de liquidez em outras corretoras descentralizadas, como a Balancer ou GMX. Cada uma delas possuem leis matemáticas que regem as negociações em suas piscinas e isso gera variações na expressão do cálculo da perda impermanente (impermanent loss).

Outro ponto que pode ser explorado é a análise técnica, que diz respeito ao estudo do comportamento de preços de determinada criptomoeda. Essa é uma tentativa de prever a flutuabilidade de preços de uma moeda e, com isso,

ter maior embasamento no momento de criar uma piscina, estipular uma faixa de preços, ou encerrar a piscina.

Além disso, a forma como a Uniswap direciona as negociações nas piscinas também não foi esclarecido nessa pesquisa. Os critérios de acesso a uma determinada piscina e o volume financeiro movimentado nela não foram expostos. Essas informações dão mais transparência aos provedores de liquidez, no que diz respeito ao cálculo de taxas recebidas por eles.

Ainda como lacuna dessa pesquisa, tem-se a relação entre a faixa de preços entre os tokens da piscina e a quantidade de cada token a ser depositada numa piscina em Uniswap V3. Só foi possível prever a quantidade de cada token a ser depositada na piscina para condições bem específicas de faixas de preços, conforme visto na equação 18 da seção 4.2.

Refletindo sobre o conceito de descentralização, por vezes o próprio autor dessa pesquisa se viu em dúvida sobre o que de fato pode ser considerado um ambiente, ou projeto, descentralizado. Ser descentralizado não pode ser reduzido a retirar o controle de um ambiente, ou projeto, do governo. Se um ambiente ou projeto se diz descentralizado, mas possui um grupo de pessoas ou empresa em condições privilegiadas em sua tomada de decisão, tal descentralização já está posta em xeque.

Desta forma, considerando o conhecimento do autor dessa pesquisa em estágio inicial, ao classificar um ambiente ou projeto como descentralizado de forma binária, tem-se somente a Bitcoin como rede descentralizada. Diante disso, talvez faça mais sentido classificar um ambiente ou projeto como descentralizado, ou não, segundo uma escala, grau ou nível de descentralização.

Por fim, espera-se que o leitor consiga compreender o desenvolvimento e as implicações matemáticas envolvidas numa piscina de liquidez na Uniswap após a leitura desse texto, e que ele consiga acessar, interagir minimamente com a MetaMask e montar uma piscina de liquidez na Uniswap.

BIBLIOGRAFIA

A História da Blockchain. (06 de Dezembro de 2018). Fonte: Binance Academy: https://academy.binance.com/pt/articles/history-of-blockchain. Acesso em: 01 mai. 2023

Adams, H. (2018). *Whitepaper Uniswap*. Fonte: hackmd.io: https://hackmd.io/@HaydenAdams/HJ9jLsfTz?type=view. Acesso em: 31 dez. 2022

Adams, H., Zinsmeister, N., & Robinson, D. (Março de 2023). *Uniswap V2 Core.* Fonte: Uniswap.org: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://uniswap.org/whitepaper.pdf. Acesso em: 01 jan. 2023

Adams, H., Zinsmeister, N., & Salem, M. (Março de 2021). *Uniswap v3 Core.* Fonte: Uniswap.org/whitepaper: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://uniswap.org/whitepaper-v3.pdf. Acesso em: 02 jan. 2023

Aigner, A. A., & Dhaliwal, G. (25 de Junho de 2021). UNISWAP: Impermanent Loss and Risk Profile of a Liquidity Provider.

Alexandre, P. (25 de Janeiro de 2022). *O passo a passo para criar e usar uma carteira Metamask*. Fonte: Portal do Bitcoin: https://portaldobitcoin.uol.com.br/o-passo-a-passo-para-criar-e-usar-uma-carteira-metamask/. Acesso em: 01 jul. 2023

Altcoins. (14 de Outubro de 2022). Fonte: InfoMoney: https://www.infomoney.com.br/guias/altcoins/. Acesso em: 27 jul. 2023.

Amaro, L. (20 de Agosto de 2023). *Veja quanto custa minerar 1 Bitcoin em casa no Brasil*. Fonte: Criptofacil: https://www.criptofacil.com/veja-quanto-custa-minerar-1-bitcoin-em-casa-no-brasil-e-em-outros-paises/amp/. Acesso em: 25 set. 2023

Barbosa, V. (17 de Julho de 2023). Fonte: Portal do Bitcoin: https://portaldobitcoin.uol.com.br/quase-30-de-todos-os-bitcoins-nao-se-movem-ha-cinco-anos-e-podem-estar-perdidos-para-sempre/. Acesso em: 01/10/2023

Barbosa, V. (13 de Julho de 2023). *BC poderá congelar contas e apreender ativos até a nova versão final do Real Digital*. Fonte: Portal do Bitcoin: https://portaldobitcoin.uol.com.br/bc-podera-congelar-contas-e-apreender-ativos-ate-na-versao-final-do-real-digital/. Acesso em 25 jul. 2023

Bertolucci, G. (11 de Julho de 2023). Fonte: Livecoins: https://livecoins.com.br/mercado-de-criptomoedas-tem-420-milhoes-de-investidores/. Acesso em: 27 jul. 2023.

Blockchain Bridge. (22 de Junho de 2022). Fonte: Binance Academy: https://academy.binance.com/pt/articles/what-s-a-blockchain-bridge. Acesso em: 09 jul. 2023.

Blockchain vs Bitcoin. (28 de Novembro de 2018). Fonte: Binance Academy: https://academy.binance.com/pt/articles/difference-between-blockchain-and-bitcoin. Acesso em: 07 jul. 2023.

Blockchain: Casos de Uso. (27 de Fevereiro de 2019). Fonte: Binance Academy: https://academy.binance.com/pt/articles/blockchain-use-cases. Acesso em: 27 mai. 2023

Casa da Moeda do Brasil. (2023). Fonte: Origem do dinheiro: https://www.casadamoeda.gov.br/portal/socioambiental/cultural/origem-do-dinheiro.html. Acesso em: 20 dez. 2022.

CoinDesk. (03 de Janeiro de 2023). *InfoMoney*. Fonte: https://www.infomoney.com.br/mercados/hacks-em-projetos-cripto-batem-recorde-e-desviam-valor-bilionario-em-2022/. Acesso em: 20 jul. 2023

Coinext, E. (02 de Junho de 2022). *ERC-20: O que é e como funciona esse tipo de token?* Fonte: Coinext: https://coinext.com.br/blog/erc-20. Acesso em: 27 jul. 2023.

CoinGecko. (02 de outubro de 2023). Fonte: https://www.coingecko.com/pt. Acesso em: 02 out. 2023

CoinGecko. (02 de Outubro de 2023). Fonte: CoinGecko: https://www.coingecko.com/pt/global-charts. Acesso em: 02 out. 2023

Elias, J. (23 de 08 de 2023). *CNN Brasil*. Fonte: https://www.cnnbrasil.com.br/economia/com-dolarizacao-e-fim-do-bc-argentina-perderia-o-poder-de-controlar-sua-economia/. Acesso em: 28 set. 2023

Goetze, C. (17 de Outubro de 2022). *Hub do Investidor*. Fonte: Trilema das Blockchains: o que é e como resolver?: https://hubdoinvestidor.com.br/trilema-das-blockchains-o-que-e-e-como-resolver/. Acesso em: 10 jul. 2023

Gonzaga, R. d. (2021). Bitcoin: uma introdução à matemática das transações. 15.

Hinsching, F. G. (20 de 06 de 2020). *Costina do Passado*. Fonte: https://cortinadopassado.com.br/2020/06/20/moedas-brasileiras-historias/. Acesso em: 28 set. 2023

InfoMoney, E. (12 de Outubro de 2022). *Argentina anuncia criação do "dólar Coldplay" e do "dólar Qatar" para controlar divisas em meio à crise*. Fonte: InfoMoney: https://www.infomoney.com.br/mercados/argentina-anuncia-criacao-do-dolar-coldplay-e-do-dolar-qatar-para-controlar-divisas-em-meio-a-crise/. Acesso em: 27 jul. 2023.

Introdução à MetaMask. (2023). Fonte: support.metamask.io: https://support.metamask.io/hc/pt-br/articles/360015489531-Introdu%C3%A7%C3%A3o-%C3%A0-MetaMask. Acesso em: 01 jul. 2023

Jenkinson, G. (24 de Julho de 2023). *Bloco 800.00 do Bitcoin foi minerado - O que vem a seguir?* Fonte: Cointelegraph: https://br.cointelegraph.com/news/bitcoin-800000-block-mined. Acesso em 26 jul. 2023.

Leão, L. (08 de Abril de 2019). Uma introdução ao estudo de bitcoins e blockchains. p. 17.

Marinho, G. (27 de fevereiro de 2021). *Cointimes*. Fonte: https://cointimes.com.br/do-ouro-ao-papel-a-historia-da-desvalorizacao-do-dolar-americano/. Acesso em: 30 set. 2023

MetaMask. (2023). Fonte: https://metamask.io/security/. Acesso em: 02 out. 2023

O Protocolo Uniswap. (2022). Fonte: Uniswap Docs: https://docs.uniswap.org/concepts/uniswap-protocol. Acesso em: 26 dez. 2022.

O que é Bitcoin. (23 de Fevereiro de 2020). Fonte: Binance Academy: https://academy.binance.com/pt/articles/what-is-bitcoin. Acesso em: 11 abr. 2023

O que é Blockchain. (14 de Outubro de 2022). Fonte: InfoMoney: https://www.infomoney.com.br/guias/blockchain/. Acesso em: 10 mai. 2023

O que é Ethereum. (17 de Março de 2020). Fonte: Binance Academy: https://academy.binance.com/pt/articles/what-is-ethereum#participating-in-the-ethereum-network. Acesso em: 10 mai. 2023

O que é KYC. (19 de Agosto de 2021). Fonte: Binance Academy: https://academy.binance.com/pt/articles/what-is-kyc-know-your-customer. Acesso em: 08 jun. 2023.

O que é um pool de liquidez. (2022). Fonte: Uniswap Help Center: https://support.uniswap.org/hc/en-us/articles/8829880740109-What-is-a-liquidity-pool-. Acesso em: 03 dez. 2022.

O que é uma Blockchain. (15 de Maio de 2023). Fonte: Binance Academy: https://academy.binance.com/pt/articles/what-is-blockchain-technology-a-comprehensive-guide-for-beginners. Acesso em: 27 mai. 2023

O que são Contratos Inteligentes. (15 de Setembro de 2019). Fonte: Binace Academy: https://academy.binance.com/pt/articles/what-are-smart-contracts. Acesso em: 15 mai. 2023.

O'Neal, S. (22 de Janeiro de 2019). Fonte: Cointelegraph: https://br.cointelegraph.com/news/who-scales-it-best-inside-blockchains-ongoing-transactions-per-second-race. Acesso em: 03 out. 2023

Os Contratos Inteligentes Uniswap V1. (2022). Fonte: Uniswap Docs: https://docs.uniswap.org/contracts/v1/overview. Acesso em: 26 dez. 2022

Pereira, L. (2023). Fonte: Dicionário Financeiro: https://www.dicionariofinanceiro.com/maiores-economias-do-mundo/. Acesso em: 05 set. 2023

Pintail. (11 de Janeiro de 2019). *Uniswap: um bom negócio para provedores de liquidez?* Fonte: Medium: https://pintail.medium.com/uniswap-a-good-deal-for-liquidity-providers-104c0b6816f2. Acesso em: 22 dez. 2022

Prates, M. M. (15 de Janeiro de 2022). *Por dentro das máquinas de venda automática do DeFi*. Fonte: InfoMoney: https://www.infomoney.com.br/mercados/por-dentro-das-maquinas-de-venda-automatica-do-defi/. Acesso em: 12 mai. 2023

Rothbard, M. N. (2013). *O que o governo fez com o nosso dinheiro?* São Paulo: Mises Brasil.

Sadi, A. (07 de Julho de 2023). Fonte: G1: https://g1.globo.com/politica/blog/andreia-sadi/post/2023/08/07/banco-central-define-nome-da-nova-moeda-digital-do-pais-drex.ghtml. Acesso em: 20 jul. 2023

Sant'Ana, J. (06 de março de 2023). Fonte: G1: https://g1.globo.com/economia/noticia/2023/03/06/banco-central-da-inicio-a-projeto-piloto-do-real-digital.ghtml. Acesso em: 20 jul. 2023

Schwingel, S. (27 de Janeiro de 2020). *Poder 360*. Fonte: https://www.poder360.com.br/internacional/entenda-o-sistema-de-credito-social-planejado-pela-china/. Acesso em 30 set. 2023

Sérvio, G. (23 de Setembro de 2023). *Olhar Digital*. Fonte: https://olhardigital.com.br/2023/09/25/pro/moeda-digital-drex-facilitara-a-compra-de-imoveis/amp/. Acesso em: 25 set. 2023

Stablecoins. (07 de Novembro de 2022). Fonte: InfoMoney: https://www.infomoney.com.br/guias/stablecoins/. Acesso em: 27 jul. 2023.

Ulrich, F. (2014). *BITCOIN - A Moeda na Era Virtual.* LVM EDITORA.

Uniswap V3 vs V2. (2023). Fonte: support.uniswap.org: https://support.uniswap.org/hc/en-us/articles/7425482965517-Uniswap-V3-vs-V2. Acesso em: 02 jan. 2023

Uniswap, E. (23 de Março de 2021). *Apresentando o Uniswap V3.* Fonte: Uniswap.org: https://uniswap.org/blog/uniswap-v3. Acesso em 02 jan. 2023.

Visão geral do Uniswap. (2022). Fonte: Uniswap Docs: https://docs.uniswap.org/concepts/overview#protocol-interface-labs. Acesso em: 26 dez. 2022

Visão geral do Uniswap V2. (23 de Março de 2020). Fonte: Iniswap.org: https://uniswap.org/blog/uniswap-v2. Acesso em 01 jan. 2023