



# **COINVESTING**

**"DE CRIPTO INVESTIDOR  
PARA CRIPTO INVESTIDOR"**

**WHITEPAPER**  
**MARÇO 2021**

# **SUMÁRIO**

<b>Criptoeconomia</b>	<b>3</b>
<b>Coinvesting DeFi v2</b>	<b>16</b>
<b>Roadmap</b>	<b>27</b>

# **CRIPTOECONOMIA**

O ARTIGO SEGUINTE EXPÕE DE MANEIRA SIMPLES E OBJETIVA OS CONCEITOS, DEFINIÇÕES, HISTÓRICO E PROJEÇÕES DO MERCADO DE CRIPTOMOEDAS.

VALE SALIENTAR QUE O ARTIGO EM QUESTÃO FOI UTILIZADO PELO AUTOR COMO TRABALHO DE CONCLUSÃO DO CURSO DE PÓS-GRADUAÇÃO EM MERCADO FINANCEIRO & BANKING NO 1º SEMESTRE DE 2019, TENDO SIDO APROVADO E VALIDADO NO ÂMBITO ACADÊMICO.

O ARTIGO A SEGUIR TAMBÉM FOI DISPONIBILIZADO EM FORMATO DE LIVRO/E-BOOK, E AGORA ESTÁ SENDO UTILIZADO COMO BASE CIENTÍFICA PARA O DESENVOLVIMENTO DE UM NOVO ECOSISTEMA ECONÔMICO, DIGITAL E DESCENTRALIZADO A PARTIR DA IMPLEMENTAÇÃO DE CONTRATOS INTELIGENTES EM BLOCKCHAIN CONFORME VEREMOS A PARTIR DE AGORA.

# **CRIPTOECONOMIA: A TECNOLOGIA BLOCKCHAIN COMO MOTOR DE PROPULSÃO ECONÔMICA ATRAVÉS DAS CRYPTOTECHS**

CHRISTOPHER ANDERSEN MIRANDA DE OLIVEIRA<sup>1</sup>

ÉRICA APARECIDA RIBEIRO<sup>2</sup>

## **RESUMO**

Depreende que a crise de confiança no sistema econômico internacional, iniciada em 2008, não trouxe apenas a escassez de produtos e serviços, mas também uma inovação disruptiva de natureza tecnológico-econômica, a *blockchain*. Enfatiza que, conhecer as profundas transformações oriundas desta tecnologia é fundamental para todos os participantes da sociedade e em especial aos profissionais, estudantes, empresários e investidores, pois a tecnologia *blockchain* é um recurso que já permeia e inova as interações econômicas e sociais em todos os continentes amplamente habitados. Ressalta que, o franco desenvolvimento desta tecnologia expande os mercados tradicionais e eclode novas economias; que captar recursos através dos processos tradicionais somado às ofertas iniciais de criptomoedas, alavanca o mercado de *startups*, sob a forma de *cryptotechs*, e cria condições para o surgimento de inovações; e por conseqüário lógico, gera novo fator de crescimento econômico, tendo em vista que a criptoeconomia constrói novos padrões na ordem econômica, política, social, jurídica e tecnológica.

**Palavras-chave:** crise de confiança, inovação disruptiva, criptomoedas.

## **1 INTRODUÇÃO**

Corolário às crises, há uma tendência do surgimento de novas soluções tecnológicas, e com estas, novos mercados e economias, de maneira cíclica; e que neste momento histórico, a tecnologia *blockchain* se mostra como um importante trunfo para a retomada do crescimento econômico internacional, tendo em vista o seu contundente desenvolvimento nos últimos anos e suas potencialidades.

O presente estudo tem o objetivo de explorar, de maneira clara e objetiva, a evolução econômica e tecnológica, no contexto das interações humanas, assim

---

<sup>1</sup> Pós-graduando em Mercado Financeiro e Banking pelo Centro Universitário de Maringá – UniCesumar, graduado em Negócios Imobiliários pelo Centro Universitário de Maringá – UniCesumar, graduando em Análise e Desenvolvimento de Sistemas pelo Centro Universitário de Maringá – UniCesumar.

<sup>2</sup> Mestre em Teoria Econômica pela Universidade Estadual de Maringá (UEM) e bacharel em Ciências Econômicas pela Universidade Estadual de Maringá (UEM).

como, relacionar crises de capital ao fenômeno da desconfiança generalizada no Sistema Econômico Internacional e suas consequências.

Para alcançar tais objetivos, este artigo é baseado em uma revisão da literatura que é caracterizada, de forma inicial, pela coleta de referenciais teóricos para construção da literatura base, seguida da discussão das ideias apresentadas, relacionando-as com o objetivo de pesquisa.

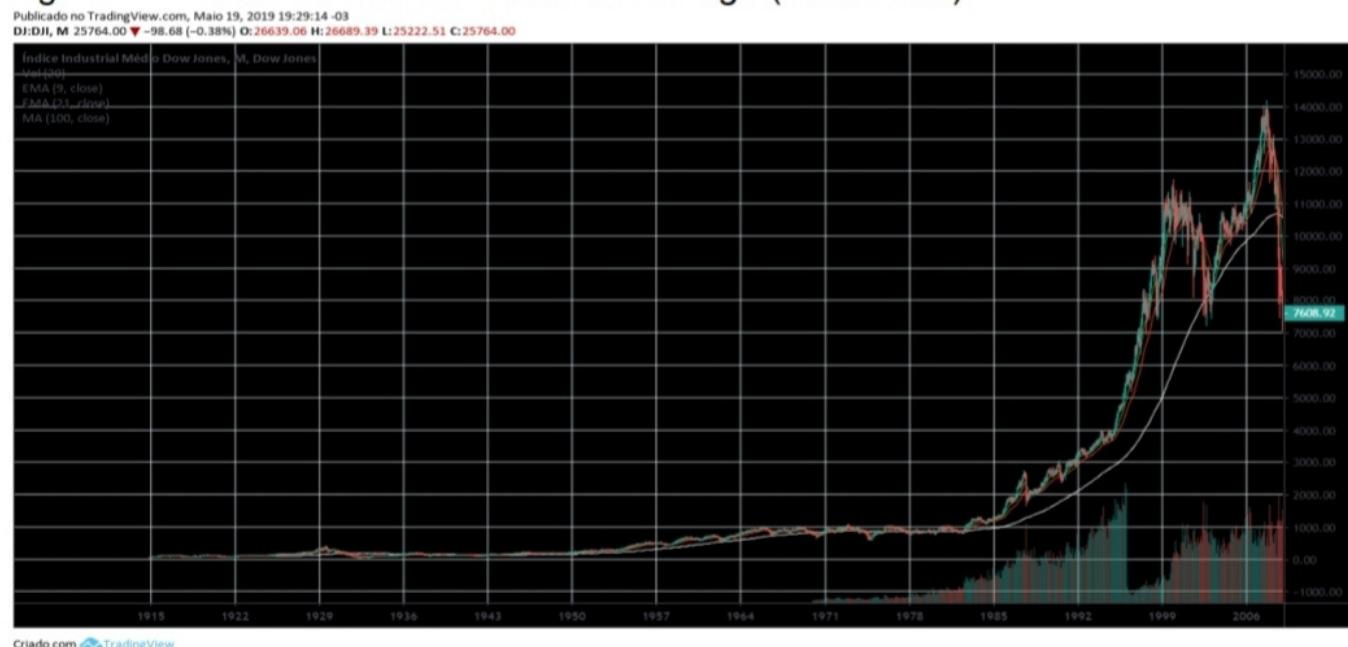
Neste sentido, o presente artigo está estruturado em seis tópicos, sendo o primeiro esta introdução. No segundo tópico será abordada a crise de confiança no Sistema Econômico Internacional; no terceiro tópico será categorizada a criptoeconomia; no quarto tópico será examinado o mercado de criptomoedas; no quinto tópico será tratado sobre inovações disruptivas, startups e os processos de captação de recursos de *cryptotechs*; em seguida serão apresentadas as considerações finais no sexto tópico; e ao término serão relacionadas as fundamentações teóricas da pesquisa.

## **2 A CRISE DE CONFIANÇA NO SISTEMA ECONÔMICO INTERNACIONAL**

Em setembro de 2008, o *Dow Jones Industrial Average*, o principal índice da indústria dos Estados Unidos da América, já demonstrava, a partir de análise gráfica da Figura 1, a imersão da economia norte-americana em uma profunda crise, e que dada a significância desta economia para o mundo, sistematicamente, comprometeria a economia internacional.

Embora a “Crise de 2008” tenha origens na “Depressão de 1929”, segundo Krugman (2009), o seu estopim se deu com à “Crise do Subprime” em 2006, que foi causada pelas concessões de empréstimos hipotecários de alto risco, por décadas, ao povo norte-americano através de instituições de crédito centenárias, e que devido à baixa qualidade do crédito, ocasionou uma inadimplência generalizada, levando vários bancos à insolvência, o que, por conseqüário lógico, fez com que não apenas o mercado imobiliário e financeiro norte-americanos, mas muitas outras economias mundiais, entrassem em recessão (KRUGMAN, 2009).

Figura 1 – Índice Dow Jones Industrial Average (1915-2008)



Fonte: Tradingview (2019).

No intuito de conter esta depressão e adaptar o sistema econômico como em outras oportunidades no passado, nações e organismos internacionais adotaram inúmeras medidas. Tais medidas, no entanto, não surtiram todos os efeitos almejados, fazendo com que a crise perdurasse até os dias atuais (KRUGMAN, 2009).

Criando um paralelo entre a “Crise de 2008” e as demais crises econômicas no decorrer da história, percebe-se que todas foram agravadas pela falta de confiança nos governos e instituições, que se converteram em escassez de produtos e serviços. E que essa desconfiança generalizada chega ao sistema de gerenciamento econômico, fazendo com que este seja posto em xeque, ciclicamente, durante as crises, pelo fato de não conseguir acompanhar, em tempo hábil, às evoluções tecnológicas e por não conseguir responder rapidamente às demandas do mercado (KRUGMAN, 2009).

Neste sentido, a evolução tecnológica das últimas décadas e a crescente interação humana com estas tecnologias, a globalização, fazem com que o atual sistema de gerenciamento econômico internacional precise se adaptar o mais breve possível, pois, caso contrário, sucessões de crises cada vez mais profundas surgirão como respostas a essas necessidades, o que indica para a possibilidade de que a internet do valor, no atual contexto global, seja a evolução natural da economia.

### **3 CRIPTOECONOMIA: O ADVENTO DA TECNOLOGIA BLOCKCHAIN**

Embora a internet já existisse desde a década de 1960, foi a *World Wide Web*, criada em 1989 pelo Cientista Tim Berners-Lee, com a publicação do estudo “*Information Management: A Proposal*”, que iniciou o processo de globalização da informação, tendo tal façanha completado 30 anos (BERNERS-LEE, 1989).

Desde então o mundo passou por profundas transformações, o número de pessoas que passaram a interagir a partir de seus computadores pessoais e, mais adiante, através de smartphones, em especial nas redes sociais, eboliu nos últimos 15 anos. É nesse contexto de grande interação tecnológica e de crise, da segunda metade dos anos 2000, que a internet passou a ter valor em si, com o advento da tecnologia *blockchain*, conforme veremos adiante.

#### **3.1 BITCOIN: O SURGIMENTO DA CRIPTOECONOMIA**

Disruptivamente, no dia 03 de janeiro de 2009, ocorre a primeira transação na *blockchain* do *bitcoin*, a “*Genesis of Bitcoin*”, que deu início, ao que conhecemos como “Criptoeconomia”, permitindo desde então que pessoas passassem a trocar criptomoedas (moedas digitais encriptadas) por produtos, serviços ou até mesmo por moedas fiduciárias, a partir de um software denominado *blockchain* (MOUGAYAR, 2017).

Mas o que vêm a ser a tecnologia *blockchain* do *bitcoin*? Ela é basicamente um software de código aberto (público), um sistema de contabilidade encriptado, onde é possível minerar ou transacionar valores financeiros (*bitcoins* ou frações de *bitcoins*), pessoa para pessoa (P2P), sem a necessidade de terceiros (casa da moeda ou bancos), por meio de registros, imutáveis, de transações em um livro-razão distribuído e digital (NAKAMOTO, 2008).

Satoshi Nakamoto, o criador da tecnologia *blockchain* do *bitcoin*, em seu *White Paper*, propõe um sistema para transações eletrônicas sem depender da confiança em intermediários (descentralização), através de uma rede (pública) ponto-a-ponto, usando a prova de trabalho computacional para os registros das transações e recompensas em *bitcoin* por esta prova de trabalho (mineração de *bitcoin*), limitadas em 21.000.000 (vinte e um milhões) de unidades de *bitcoin* (escassez) (NAKAMOTO, 2008).

### 3.2 ETHEREUM: A SEGUNDA GERAÇÃO DA CRIPTOECONOMIA

Ao final de 2013, Vitalik Buterin escreveu o *White Paper* da plataforma *Ethereum*, que consistia em uma plataforma de código aberto (pública), descentralizada, adaptável e flexível, criada para a implementação de contratos inteligentes (aplicações que funcionam exatamente como programadas), desde games descentralizados até bolsas de valores (BUTERIN, 2014).

Em meados de 2014, foi aberta uma captação de recursos online, *crowdfunding*, para financiar o Projeto *Ethereum*, em formato assemelhado ao que hoje conhecemos como ICO (*Initial Coin Offering*), onde *tokens* são criados e vendidos para financiamentos de projetos, como veremos mais adiante (TAPSCOTT; TAPSCOTT, 2016).

Dando continuidade ao projeto, a plataforma *Ethereum* foi lançada aos 30 dias do mês de julho de 2015, dando início de fato à “Segunda Geração da Tecnologia *Blockchain*” ou “Segunda Geração Criptoeconômica”, uma vez que o mercado de criptomoedas cresceu, significativamente, desde então, através de inúmeros projetos que utilizaram a *blockchain* do *Ethereum* para captar recursos e realizar lançamentos, tendo em vista que os custos das ICOs (Ofertas Iniciais de Criptomoedas) são muito inferiores aos das IPOs (Ofertas Públicas Iniciais) no mercado de capitais, o que viabiliza e fomenta a ascensão do mercado de startups (TAPSCOTT; TAPSCOTT, 2016).

### 3.3 TOKENS DE UTILIDADE: A TERCEIRA GERAÇÃO DA CRIPTOECONOMIA

Inúmeros projetos utilizaram a *blockchain* do *Ethereum* e outras *blockchains* lançadoras para a captação de recursos através de ICOs desde 2015, mas dentro de um contexto de interação humana através da tecnologia *blockchain* aliada a outras tecnologias disruptivas, as criptomoedas sob o padrão de *tokens* de utilidade, merecem grande atenção, pois a utilização simplificada da tecnologia *blockchain* parece ser o caminho mais promissor para a adoção generalizada de criptomoedas.

Neste momento, a tecnologia *blockchain* avança a passos largos, no sentido de cada vez mais ser utilizada por pessoas comuns através de mídias e redes sociais, e com o propósito de criar uma “Criptoeconomia Interativa”, onde marcas recompensam seus clientes conforme a interação digital do cliente com estas

marcas, criando um cenário retributivo, onde *tokens* de utilidade (criptomoedas), podem ser trocados por produtos, serviços, moeda fiduciária, ou até mesmo por outras criptomoedas em *exchanges* (plataformas de negociações de criptomoedas) (MOUGAYAR, 2017).

#### **4 O MERCADO DE CRIPTOMOEDAS: COMPOSIÇÃO, LIQUIDEZ, SEGURANÇA, EVOLUÇÃO, VOLUME, RENTABILIDADE E PROJEÇÕES**

Da primeira transação de *bitcoin* até os dias atuais, o mercado de criptomoedas passou por inúmeras transformações. Com a chegada das primeiras *exchanges*, casas de câmbio de criptomoedas, o volume de negociações aumentou fortemente, o que contribuiu para que o valor da unidade de *bitcoin* disparasse de US\$ 0,0025, valor da cotação de *bitcoin* para a compra de pizzas em 22 de maio de 2010 - *Bitcoin Pizza Day*<sup>3</sup>, para US\$ 1.175,00 (em 02 de dezembro de 2013), poucos meses antes do anúncio do *cracking* (subtração de 850 mil *bitcoins*) na *exchange* *MTGox*, que naquele momento era responsável por 70% das negociações de *bitcoins* de todo o mundo.

Após esse *cracking*, o mercado de criptomoedas passou por um período turbulento e de questionamentos sobre os riscos e a segurança no emprego da tecnologia *blockchain*, todavia, a capilaridade do *bitcoin* e da tecnologia *blockchain* continuou crescendo vertiginosamente, uma vez que muitas pessoas e setores de várias economias passaram a entender sobre as enormes possibilidades desta tecnologia; tendo sido criadas, desde então, várias empresas e plataformas, que fizeram com que o mercado ganhasse muito volume e atenção mundial nos últimos anos (TAPSCOTT; TAPSCOTT, 2016).

##### **4.1 COMPOSIÇÃO, LIQUIDEZ E SEGURANÇA DO MERCADO DE CRIPTOMOEDAS**

Na atualidade, o mercado de criptomoedas é composto por *exchanges* (plataformas de negociações de criptomoedas), onde compradores e vendedores (pessoas físicas ou jurídicas), negociam por meio de um livro digital de ofertas, o valor a ser pago por cada unidade de criptomoeda, compondo às cotações das criptomoedas.

---

<sup>3</sup> Disponível em: <<https://bitcointalk.org/index.php?topic=137.0>>. Acesso em: 15 de mai. 2019.

As *exchanges* propiciam maior liquidez ao mercado de criptomoedas, pois possibilitam negociações internas e envios de criptomoedas, em poucos minutos, para outras *exchanges*, ou *wallets* (carteiras de criptomoedas) de aproximadamente 35 milhões de usuários ao redor do mundo, segundo estudo do *Cambridge Center for Alternative Finance*, realizado em dezembro de 2018 (RAUCHS, 2018).

Em 22 de maio de 2019, segundo o *CoinMarketCap*<sup>4</sup>, existiam 2194 criptomoedas sendo negociadas em 18589 *exchanges*, em todos os continentes amplamente habitados do planeta, e por óbvio, cada criptomoeda e cada *exchange* representa uma empresa (pequena, média ou grande), sendo que cada criptomoeda está inserida em um setor tradicional ou até mesmo em novos mercados, dadas as potencialidades da tecnologia *blockchain* (TAPSCOTT; TAPSCOTT, 2016).

Quanto ao fator segurança, ele é inerente à própria tecnologia *blockchain*, dada a forte encriptação de dados. Não obstante, existem soluções e hábitos que influenciam, positivamente ou negativamente, os níveis de segurança quando das utilizações ou negociações de criptomoedas, a exemplo os fatores de segurança, como autenticadores, biometria, reconhecimento facial e chaves de segurança; mas o fator primordial de segurança em qualquer tecnologia está associado aos hábitos do próprio usuário, especialmente, no que se refere à utilização de suas informações nos vários ambientes virtuais (MOUGAYAR, 2017).

#### 4.2 EVOLUÇÃO, VOLUME, RENTABILIDADE E PROJEÇÕES DO MERCADO DE CRIPTOMOEDAS

No decorrer da história, muitas corporações e muitos investidores criaram enormes fortunas a partir de vários mercados que um dia se encontravam em fase de formação, mas que hoje são considerados tradicionais, como o caso do Mercado de Capitais, que em seu início era visto como uma aberração financeira. Desta forma, o mercado de criptomoedas também está quebrando paradigmas, pois graças à globalização da informação, a tecnologia *blockchain* também está globalizando economias, alinhadamente com os níveis de transformações que vivemos (TAPSCOTT; TAPSCOTT, 2016).

Como pode-se constatar na Figura 2 (Bitcoin/Dólar), o *bitcoin* (representando o mercado de criptomoedas, dada a sua precursão e predominância) evoluiu

---

<sup>4</sup> Disponível em: <<https://coinmarketcap.com/>>. Acesso em: 22 de mai. 2019.

bastante e de maneira diretamente proporcional ao seu nível de inovação; e isso fez com que muitos investidores e várias corporações obtivessem rentabilidades nunca vistas na história, seja por motivações de riscos técnicos, empíricos ou entusiásticos, no que tange aos investidores, seja pela criação de novos mercados por parte das corporações que desenvolveram seus negócios utilizando a tecnologia *blockchain*.

**Figura 2 – Bitcoin/Dólar (2013-2019)**



Fonte: Tradingview (2019).

Em 22 de maio de 2019, as 00 horas e 04 minutos, o mercado global de criptomoedas, possuía volume total na ordem de US\$ 249.722.365.917,00 e a unidade de *bitcoin* negociada a US\$ 7.953,20. Valendo frisar que, o topo histórico do volume do mercado de criptomoedas, ocorreu em 17 de dezembro de 2017, com a marca de US\$ 736.657.096.536,00, e o topo histórico da unidade de *bitcoin*, naquela data, em US\$19.891,00, o que significava uma alta de 7.956.000%, quase oito milhões percentuais, se comparada ao valor da unidade de *bitcoin* (US\$ 0,0025) utilizada para a compra de pizzas, no *Bitcoin Pizza Day*<sup>5</sup>.

Dentro de um contexto econômico e tecnológico, nunca se viu na história um crescimento percentual tão contundente como o do mercado de criptomoedas, que já se encontra no início da sua terceira geração, “A Geração da Utilidade”, através dos “*Utility Tokens*”, onde novas empresas e comportamentos já estão sendo criados, o que resultará em abundância de recursos nas próximas décadas.

<sup>5</sup> Cf. nota 3 deste tópico.

## **5 INOVAÇÕES DISRUPTIVAS, STARTUPS, CRYPTOTECHS, VENTURE CAPITAL E AS OFERTAS INICIAIS DE CRIPTOMOEDAS - ICOs**

Em 1997, Clayton M. Christensen, professor de Harvard, em “O Dilema do Inovador”, criou o conceito de “Inovação Disruptiva”, que de maneira bem sintética, diz respeito a transformação de uma tecnologia, produto, ou serviço em algo novo, mais simples, conveniente e acessível, e que torna o seu antecessor obsoleto (CHRISTENSEN, 1997). Neste mesmo sentido, Klaus Schwab, desenvolveu a terminologia “Quarta Revolução Industrial”, se referindo às profundas alterações nas formas como nos relacionamos e consumimos, como verdadeiras quebras de paradigmas, sob a forma digital (SCHWAB, 2016).

É nesse contexto de criatividade e inovação, que iremos abordar as *startups* e demonstrar como é possível captar recursos através do mercado tradicional cumulativamente com mercado de criptomoedas, com o propósito de transformar em realidade grandes ideias e projetos sob a forma de *cryptotechs*.

### **5.1 INOVAÇÕES DISRUPTIVAS, STARTUPS E A DECLARAÇÃO DOS DIREITOS DE LIBERDADE ECONÔMICA**

Provavelmente, muitos já ouviram falar do Vale do Silício e das gigantes corporações que ali nasceram. Elas possuem uma característica peculiar, surgiram sob a forma de *startup*, que em outras palavras significa que embora tivessem que passar por uma fase de incubação e depois de aceleração, graças ao modelo de negócios escalável, repetitivo ou disruptivo, conseguiram se desenvolver (MOUGAYAR, 2017). Sabe-se também que além do Vale do Silício, existem outros ecossistemas de *startups* pelo mundo e que eles estão em franco desenvolvimento.

Neste contexto, fica mais fácil compreender que além do desenvolvimento tecnológico, os ecossistemas de *startups* geram forte crescimento econômico, e é nesta conjectura que a “Declaração de Direitos de Liberdade Econômica”, instituída no dia 30 de abril de 2019, por meio da Medida Provisória Nº 881, é bem recepcionada pela economia brasileira, pois com esta medida, a criação e o desenvolvimento de novos ecossistemas de *startups* em território brasileiro será mais factível.

## 5.2 CRYPTOTECHS, VENTURE CAPITAL E AS OFERTAS INICIAIS DE CRIPTOMOEDAS - ICOS

O *Venture Capital* (capital de risco) é uma das opções para a captação de recursos para o desenvolvimento de *startups*. Nesse tipo de investimento, os investidores expõem um percentual de seu patrimônio ao risco do empreendimento empresarial, em fase emergente, e em troca detêm uma parte da empresa e seus possíveis lucros futuros (MOUGAYAR, 2017).

No mesmo sentido, o advento da tecnologia *blockchain* possibilita a captação de recursos para o desenvolvimento de *startups*, através de ICOs (ofertas iniciais de criptomoedas), onde projeto e *roadmap* são lançados ao público, por meio de um *White Paper* (memorial descritivo das informações técnicas); dando início à fase de captação de recursos em criptomoedas e moeda fiduciária; que é sucedida pela fase de emissão e distribuição de *tokens* (fichas que possuem o ativo em questão associado), nos exatos termos e condições previamente acordados no ambiente virtual (MOUGAYAR, 2017).

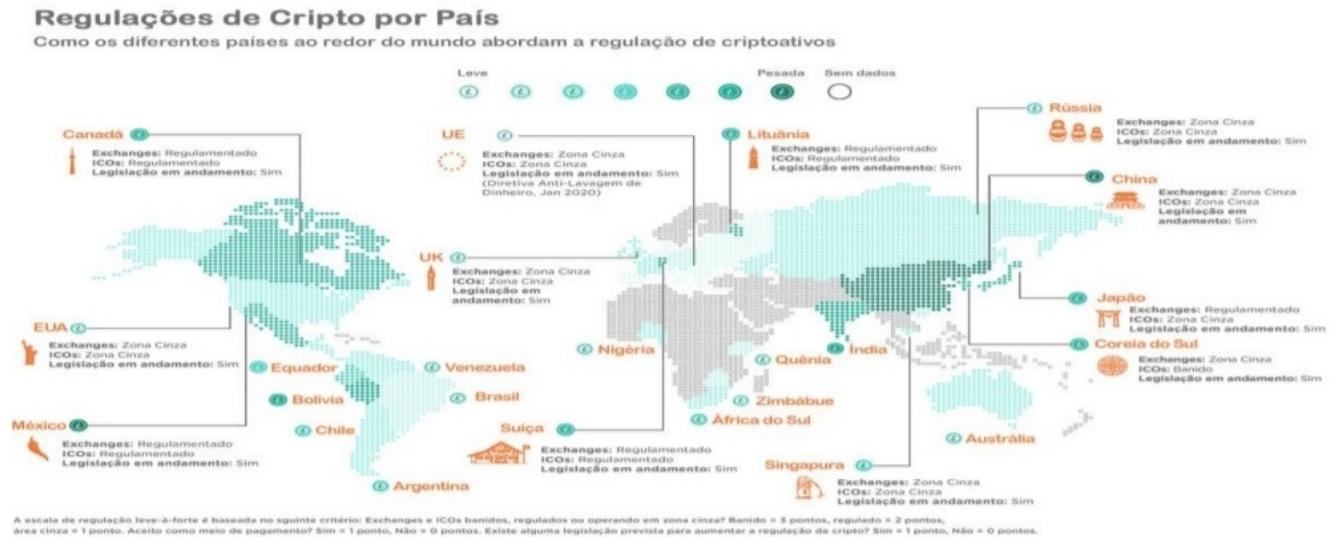
Analizando as projeções do mercado de criptomoedas, podemos conjugar *Venture Capital* e *Initial Coin Offering*, no intuito de acelerar *startups* e desenvolvê-las nos mercados sob a forma de *cryptotechs* (*startups* de tecnologia *blockchain*), uma vez que tanto a captação primária de recursos por meio de capital de risco de investidores quanto a captação secundária por meio de ofertas iniciais de criptomoedas, podem ser cumuladas, não havendo impeditivos ou solenidades no mercado financeiro em relação aos *tokens* de utilidade, pois no âmbito do direito privado, o que não é proibido é permitido, conforme examinaremos (MOUGAYAR, 2017).

## 5.3 ASPECTOS JURÍDICOS RELACIONADOS ÀS OFERTAS INICIAIS DE CRIPTOMOEDAS

Em vários países, tanto as criptomoedas quanto os processos de ofertas iniciais de criptomoedas já foram regulamentados, ou possuem projetos normativos em andamento, de forma mais ou menos intervencionista, conforme observa-se na Figura 3. No cenário brasileiro, a Comissão de Valores Mobiliários e a Receita Federal, tem tratado sobre criptomoedas nos termos dos seguintes atos normativos: Ofício-circular nº 1/2018/CVM/SIN de 12 de janeiro de 2018; Ofício-circular

CVM/SRE nº 01/2018 de 27 de fevereiro de 2018; Ofício-circular CVM/SRE nº 02/2019 de 27 de fevereiro de 2019; RFB/Instrução Normativa nº 1888 de maio de 2019.

Figura 3 - Regulações de criptomoedas por país



Fonte: Comply Advantage (2019).

Em andamento, tem-se ainda, o Projeto de Lei 2060/2019 que dispõe sobre o Regime Jurídico de Criptoativos, englobando criptomoedas utilizadas como meio de pagamento, reserva de valor, tokens de utilidade, tokens de valor mobiliário e sobre o aumento de pena para o crime de “pirâmide financeira”, bem como para os crimes relacionados ao uso fraudulento de criptomoedas.

## 6 CONSIDERAÇÕES FINAIS

Nesse diapasão, fica evidente que a solução às crises é o desenvolvimento tecnológico, e que em resposta à “Crise de 2008”, a tecnologia *blockchain* surgiu como uma inovação disruptiva frente ao Sistema Econômico Internacional, tendo evoluído de maneira constante em mercados tradicionais e ainda criado outras economias. Sendo que, para tal feito, a tecnologia foi evoluída ao ponto de popularizar plataformas de captação de recursos para lançamentos de projetos, que conseguiram impulsionar milhares de startups para o cenário internacional, fazendo com que o mercado de criptomoedas tivesse uma forte expansão nos últimos anos, e deixando claro que, de fato, se está no início de uma profunda transformação econômico-tecnológica.

## **REFERÊNCIAS**

BERNERS-LEE, Timothy J. **Information management: A proposal.** 1989.

BUTERIN, Vitalik et al. A next-generation smart contract and decentralized application platform. **white paper**, 2014.

CHRISTENSEN, C. **The innovator's dilemma: when new technologies cause great firms to fail.** New York: Harvard Business Review Press, 1997.

Comissão de Valores Mobiliários, Criptoativos, disponível em: <<http://www.cvm.gov.br/legislacao/index.html>>. Acesso em: 15 de mai. 2019.

COMPLY ADVANTAGE. Disponível em: <<https://complyadvantage.com>>. Acesso em: 19 de mai. 2019.

Declaração dos Direitos de Liberdade Econômica, Medida Provisória nº 881, disponível em: <[http://www.planalto.gov.br/ccivil\\_03/\\_ato2019-2022/2019/Mpv/mpv881.htm](http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/Mpv/mpv881.htm)>. Acesso em: 15 de mai. 2019.

KRUGMAN, Paul. **A crise de 2008 e a economia da depressão.** Rio de Janeiro: Elsevier, 2009.

MOUGAYAR, William. **Blockchain para negócios: promessa, prática e aplicação da nova tecnologia da internet.** 1. ed. Rio de Janeiro: Alta Books, 2017.

NAKAMOTO, Satoshi et al. **Bitcoin:** A peer-to-peer electronic cash system. 2008. Disponível em: <<https://bitcoin.org/bitcoin.pdf>>. Acesso em: 15 de mai. 2019.

SCHWAB, Klaus. **A quarta revolução industrial.** 1. ed. São Paulo: Edipro, 2016.

Projeto de Lei 2060/2019, Regime Jurídico de Criptoativos, disponível em:<<https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2196875>>. Acesso em: 15 de mai. 2019.

RAUCHS, Michel et al. **2nd Global Cryptoasset Benchmarking Study.** 2018. Disponível em: <<https://bit.ly/2Tw3z1A>>. Acesso em: 30 de maio 2019.

Receita Federal do Brasil, Instrução Normativa nº 1888, criptoativos, disponível em:<<http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?visao=anotado&idAto=100592>>. Acesso em: 15 de mai. 2019.

TAPSCOTT, Don; TAPSCOTT, Alex. **Blockchain revolution: como a tecnologia por trás do bitcoin está mudando o dinheiro, os negócios e o mundo.** 1. ed. São Paulo: SENAI-SP Editora, 2016.

TRADINGVIEW. Disponível em: <<https://www.tradingview.com>>. Acesso em: 19 de mai. 2019.

# **COINVESTING DEFI V2**

ANTE TODO O EXPOSTO NO ARTIGO ANTERIOR FICA EVIDENTE A NECESSIDADE DE MECANISMOS QUE FAVOREÇAM O DESENVOLVIMENTO TECNOLÓGICO E ECONÔMICO, QUE SE DARÁ A PARTIR DE PLATAFORMAS QUE FAVOREÇAM TANTO AS EMPRESAS(CRYPTOTECHS) QUANTO OS INVESTIDORES(TRADERS/LIQUID PROVIDERS).

DIANTE DISTO, O PROTOCOLO COINVESTING DEFI V2 NASCE COM O PROPÓSITO DE CRIAR CONDIÇÕES FAVORÁVEIS PARA QUE STARTUPS POSSAM INICIAR SEUS PROCESSOS DE TOKENIZAÇÃO E EM SEGUITA NEGOCIÁ-LOS NA NOSSA PLATAFORMA DESCENTRALIZADA COINVESTING DEX, UMA VEZ QUE OS PARES DE CRIPTOMOEDAS PODERÃO SER CRIADOS POR QUAISQUER DETENTORES DE TOKENS EM PADRÃO ERC-20 DE MANEIRA SIMPLES E AUTOMATIZADA, BASTANDO O SEU DETENTOR ADICIONAR LIQUIDEZ AOS CONTRATOS INTELIGENTES.

ALÉM DISTO, O PROTOCOLO COINVESTING DEFI V2 TAMBÉM JÁ NASCE COM O PROPÓSITO DE RESOLVER PROBLEMAS DE SEGURANÇA GERALMENTE RELACIONADOS ÀS EXCHANGES CENTRALIZADA, UMA VEZ QUE TODAS AS OPERAÇÕES ACONTECERÃO NA BLOKCHAIN A PARTIR DE CONTRATOS INTELIGENTES, CONFORME VEREMOS A SEGUIR NO WHITEPAPER TÉCNICO, QUE EXPLICA O FIEL FUNCIONAMENTO DOS CONTRATOS INTELIGENTES DO PROTOCOLO COINVESTING DEFI V2 QUE COMPREENDE OS CONTRATOS INTELIGENTES DA COINVESTING DEX(DECENTRALIZED EXCHANGE), O CONTRATO INTELIGENTE NÃO CUSTODIAL DE TOKENS E O CONTRATO INTELIGENTE DE CRIAÇÃO DOS TOKENS DE GOVERNANÇA DA COINVESTING DEX E COMO ELES SE COMUNICAM.

# Coinvesting DeFi v2

Christopher Miranda  
christopher@coinvesting.app

Tarcísio Santos  
tarcisio@coinvesting.app

Março 2021

## Abstract

Este *whitepaper* explica algumas das decisões de design por trás dos contratos Coinvesting DeFi v2. Ele cobre os novos recursos dos contratos - incluindo pares arbitrários entre ERC20s, um oráculo de preço endurecido que permite que outros contratos estimem o preço médio ponderado no tempo ao longo de um determinado intervalo, "swaps flash" que permitem que os negociantes recebam ativos e os utilizem em outro lugar antes de pagar por eles posteriormente na transação e uma taxa de protocolo que pode ser ativada no futuro. Ele também reconstrói os contratos para reduzir sua superfície de ataque. Este *whitepaper* descreve a mecânica dos contratos "*principais*" do Coinvesting v2, incluindo o contrato do par que armazena os fundos dos provedores de liquidez - e o contrato de fábrica usado para instanciar os contratos do par.

## 1 Introdução

Coinvesting DeFi v1 é um sistema on-chain de contratos inteligentes no "Ethereum blockchain", implementado por um protocolo de liquidez automatizado com base em uma "*fórmula de produto constante*". Cada par de Coinvesting DeFi v1 armazena reservas conjuntas de dois ativos e fornece liquidez para esses dois ativos, mantendo a invariante de que o produto das reservas não pode diminuir. Os comerciantes pagam uma taxa de 30 pontos-base sobre as negociações, que vai para os provedores de liquidez. Os contratos não podem ser atualizados.

Coinvesting DeFi v2 é uma nova implementação baseada na mesma fórmula, com vários novos recursos altamente desejáveis. Mais significativamente, permite a criação de pares ERC20 / ERC20 arbitrários, em vez de suportar apenas pares entre ERC20 e ETH. Ele também fornece um oráculo de preço endurecido que acumula o preço relativo dos dois ativos no início de cada bloco. Isso permite que outros contratos no Ethereum estimem o preço médio ponderado no tempo para os dois ativos em intervalos arbitrários. Por fim, permite "swaps flash" em que os usuários podem receber ativos gratuitamente e usá-los em outros lugares da cadeia, pagando (ou devolvendo) apenas esses ativos no final da transação.

Embora o contrato geralmente não seja atualizável, há uma chave privada que tem a capacidade de atualizar uma variável no contrato de fábrica para ativar uma taxa de 5 pontos-base na cadeia nas negociações. Essa taxa será inicialmente cancelada, mas poderá ser ativada no futuro, após o qual os provedores de liquidez ganhariam 25 pontos-base em cada negociação, em vez de 30 pontos-base.

Coinvesting DeFi v2 também corrige alguns problemas menores no Coinvesting DeFi v1, bem como a rearquitetura da implementação, reduzindo a superfície de ataque da Coinvesting e tornando o sistema mais facilmente atualizável, minimizando a lógica no contrato "*principal*" que mantém os fundos dos provedores de liquidez.

Este artigo descreve a mecânica desse contrato central, bem como o contrato de fábrica costumava ser usado para instanciar esses contratos. Na verdade, o uso do Coinvesting DeFi v2 exigirá a chamada do contrato do par por meio de um contrato de “roteador” que calcula o valor da transação ou do depósito e transfere fundos para o contrato do par.

## 2 Novas características

### 2.1 Pares ERC-20

Coinvesting DeFi v1 usou ETH como moeda-ponte. Cada par incluiu a ETH como um de seus ativos. Isso torna o roteamento mais simples - todas as negociações entre ABC e XYZ passam pelo par ETH / ABC e pelo par ETH / XYZ - e reduz a fragmentação da liquidez.

No entanto, essa regra impõe custos significativos aos provedores de liquidez. Todos os provedores de liquidez têm exposição à ETH e sofrem perdas impermanentes com base nas mudanças nos preços de outros ativos em relação à ETH. Quando dois ativos ABC e XYZ são correlacionados - por exemplo, se ambos são USD stablecoins - os provedores de liquidez em um par de Coinvesting DeFi v2 ABC / XYZ geralmente estariam sujeitos a menos perdas impermanentes do que os pares ABC / ETH ou XYZ / ETH.

Usar a ETH como moeda-ponte obrigatória também impõe custos aos “traders”. Os “traders” têm de pagar duas vezes mais em taxas do que pagariam em um par ABC/XYZ direto e sofrem duas vezes de “slippage”.

Coinvesting DeFi v2 permite que os provedores de liquidez criem contratos de pares para quaisquer ERC-20s.

Uma proliferação de pares entre ERC-20s arbitrários pode tornar um pouco mais difícil encontrar o melhor caminho para negociar um par específico, mas o roteamento pode ser tratado em uma camada superior (ou fora da cadeia ou por meio de um roteador ou agregador na cadeia).

### 2.2 Oráculo de preços

O preço marginal oferecido pelo Coinvesting DeFi v2 (não incluindo taxas) no tempo  $t$  pode ser calculado dividindo as reservas do ativo  $a$  pelas reservas do ativo  $b$ .

$$p_t = \frac{r_t^a}{r_t^b} \quad (1)$$

Uma vez que os arbitradores negociarão com Coinvesting DeFi se este preço estiver incorreto (por uma quantia suficiente para compensar a taxa), o preço oferecido por Coinvesting DeFi tende a rastrear o preço de mercado relativo dos ativos. Isso significa que pode ser usado como um oráculo de preço aproximado.

No entanto, o Coinvesting DeFi v1 não é seguro para usar como um oráculo de preços na rede, porque é muito fácil de manipular. Suponha que algum outro contrato use o preço ETH-DAI atual para liquidar uma derivada. Um invasor que deseja manipular o preço medido pode comprar ETH do par ETH-DAI, acionar a liquidação no contrato de derivativo (fazendo com que seja liquidado com base no preço inflacionado) e, em seguida, vender ETH de volta ao par para negociá-lo de volta o verdadeiro preço.<sup>(1)</sup> Isso pode até ser feito como uma transação atômica ou por um minerador que controla a ordem das transações dentro de um bloco.

Coinvesting DeFi v2 melhora esta funcionalidade do oráculo medindo e registrando o preço *antes* da primeira negociação de cada bloco (ou de forma equivalente, *após* a última negociação do bloco

anterior). Esse preço é mais difícil de manipular do que os preços durante um bloco. Se o invasor enviar uma transação que tenta manipular o preço no final de um bloco, algum outro仲裁ador poderá enviar outra transação para negociar imediatamente depois no mesmo bloco. Um minerador (ou um atacante que usa gás suficiente para preencher um bloco inteiro) poderia manipular o preço no final de um bloco, mas a menos que extraia também o próximo bloco, eles podem não ter uma vantagem particular em arbitrar a negociação de volta.

Especificamente, Coinvesting DeFi v2 *acumula* esse preço, acompanhando a soma acumulada dos preços no início de cada bloco em que alguém interage com o contrato. Cada preço é ponderado pelo tempo decorrido desde o último bloco em que foi atualizado, de acordo com a data e hora do bloco. Isso significa que o valor do acumulador a qualquer momento (após ser atualizado) deve ser a soma do preço à vista a cada segundo do histórico do contrato.

$$a_t = \sum_{i=1}^t p_i \quad (2)$$

Para estimar o *preço médio ponderado no tempo* de  $t_1$  a  $t_2$ , um chamador externo pode verificar o valor do acumulador em  $t_1$  e, em seguida, novamente em  $t_2$ , subtrair o primeiro valor do segundo e dividir pelo número de segundos decorridos. (Observe que o próprio contrato não armazena valores históricos para este acumulador - o chamador tem que chamar o contrato no início do período para ler e armazenar esse valor.)

$$p_{t_1, t_2} = \frac{\sum_{i=t_1}^{t_2} p_i}{t_2 - t_1} = \frac{\sum_{i=1}^{t_2} p_i - \sum_{i=1}^{t_1} p_i}{t_2 - t_1} = \frac{a_{t_2} - a_{t_1}}{t_2 - t_1} \quad (3)$$

Os usuários do oráculo podem escolher quando iniciar e terminar este período. Escolher um período mais longo torna mais caro para um invasor manipular o TWAP, embora resulte em um preço menos atualizado.

Uma complicação: devemos medir o preço do ativo A em termos do ativo B ou o preço do ativo B em termos do ativo A? Enquanto o preço à vista de A em termos de B é sempre o recíproco do preço à vista de B em termos de A, o preço médio do ativo A em termos do ativo B durante um determinado período de tempo *não* é igual ao recíproco do preço médio do ativo B em termos de ativo A.<sup>(2)</sup> Por exemplo, se o preço USD/ETH for 100 no bloco 1 e 300 no bloco 2, o preço médio USD/ETH será 200 USD/ETH, mas o preço médio ETH/USD será 1/150 ETH/USD. Uma vez que o contrato não pode saber qual dos dois ativos os usuários iriam desejar usar como unidade de conta, Coinvesting DeFi v2 rastreia ambos os preços.

Outra complicação é que é possível alguém enviar ativos para o contrato do par - e assim alterar seus saldos e preço marginal - sem interagir com ele e, portanto, sem acionar uma atualização do oráculo. Se o contrato simplesmente verificava seus próprios saldos e atualizava o oráculo com base no preço atual, um invasor poderia manipular o oráculo enviando um ativo para o contrato imediatamente antes de chamá-lo pela primeira vez em um bloco. Se a última negociação foi em um bloco cujo carimbo de data / hora foi X segundos atrás, o contrato multiplicaria incorretamente o novo preço por X antes de acumulá-lo, mesmo que ninguém

<sup>1</sup>Uma vez que os mineradores têm alguma liberdade para definir o carimbo de data/hora do bloco, os usuários do oráculo devem estar cientes de que esses valores podem não corresponder precisamente aos tempos do mundo real.

<sup>2</sup>O preço médio aritmético do ativo A em termos do ativo B durante um determinado período é igual ao recíproco do preço médio *harmônico* do ativo B em termos do ativo A durante esse período. Se o contrato medisse o preço médio *geométrico*, então os preços seriam os recíprocos um do outro. No entanto, o TWAP médio geométrico é menos comumente usado e é difícil de calcular no Ethereum.

tenha tido a oportunidade de negociar a esse preço. Para evitar isso, o contrato principal armazena em cache suas reservas após cada interação e atualiza o oráculo usando o preço derivado das reservas em cache em vez das reservas atuais. Além de proteger o oráculo de manipulação, esta mudança permite a re-arquitetura do contrato descrita abaixo na seção 3.2.

### 2.2.1 Precisão

Como o *Solidity* não tem suporte de primeira classe para tipos de dados numéricos não inteiros, o Coinvesting DeFi v2 usa um formato de ponto fixo binário simples para codificar e manipular preços. Especificamente, os preços em um determinado momento são armazenados como números UQ112.112, o que significa que 112 bits fracionários de precisão são especificados em cada lado da vírgula decimal, sem sinal. Esses números têm um intervalo de  $[0, 2^{112} - 1]$ <sup>(3)</sup> e uma precisão de  $\frac{1}{2^{112}}$ .

<sup>1</sup> O formato UQ112.112 foi escolhido por uma razão pragmática - porque esses números podem ser armazenados em um uint224, isso deixa livre 32 bits de um slot de armazenamento de 256 bits. Também acontece que as reservas, cada uma armazenada em um uint112, também deixam 32 bits livres em um slot de armazenamento de 256 bits (compactado). Esses espaços livres são usados para o processo de acumulação descrito acima. Especificamente, as reservas são armazenadas junto com o carimbo de data/hora do bloco mais recente com pelo menos uma negociação, modificada com 232 para que se encaixe em 32 bits. Além disso, embora o preço em qualquer momento (armazenado como um número UQ112.112) seja garantido para se ajustar em 224 bits, o acúmulo desse preço ao longo de um intervalo não o é. Os 32 bits extras no final dos slots de armazenamento para o preço acumulado de A/B e B/A são usados para armazenar bits de estouro resultantes de somas repetidas de preços. Este projeto significa que o oráculo de preços adiciona apenas três operações SSTORE adicionais (um custo atual de cerca de 15.000 gás) para a primeira negociação em cada bloco.

A principal desvantagem é que 32 bits não são suficientes para armazenar valores de carimbo de data/hora que razoavelmente nunca irão transbordar. Na verdade, a data em que o carimbo de data/hora Unix transborda um uint32 é 15/04/2021. Para garantir que este sistema continue a funcionar adequadamente após esta data, e a cada múltiplo de  $2^{32} - 1$  segundos daí em diante, os oráculos são simplesmente solicitados a verificar os preços pelo menos uma vez por intervalo (aproximadamente 136 anos). Isso ocorre porque o método central de acumulação (e modding de timestamp) é realmente seguro contra transbordamento, o que significa que as negociações entre intervalos de transbordamento podem ser contabilizadas de forma apropriada, dado que os oráculos estão usando a aritmética de transbordamento adequada (simples) para calcular deltas.

## 2.3 Flash Swaps

No Coinvesting DeFi v1, um usuário que compra ABC com XYZ precisa enviar o XYZ para o contrato antes de receber o ABC. Isso é inconveniente se o usuário precisar do ABC que está comprando para obter o XYZ com o qual está pagando. Por exemplo, o usuário pode estar usando esse ABC para comprar XYZ em algum outro contrato a fim de arbitrar uma diferença de preço do Coinvesting DeFi, ou pode estar revertendo uma posição no Maker ou Compound vendendo a garantia para reembolsar Coinvesting DeFi.

Coinvesting DeFi v2 adiciona um novo recurso que permite ao usuário receber e usar um ativo antes de pagá-lo, desde que faça o pagamento dentro da mesma transação atômica. A função **swap** faz uma chamada para um contrato de callback opcional especificado pelo usuário entre a transferência dos tokens solicitados pelo usuário e a aplicação do invariante. Assim que o retorno de chamada for concluído, o contrato verifica os novos saldos e confirma que o invariante está satisfeito

<sup>3</sup> O limite superior teórico de  $2^{112} - (\frac{1}{2^{112}})$  não se aplica a esta configuração, como números UQ112.112 em

Coinvesting são sempre gerados a partir da proporção de dois uint112s. A maior dessas proporções é  $\frac{2^{112}-1}{1} = 2^{112} - 1$ .

(após ajuste das taxas sobre os valores pagos). Se o contrato não tiver fundos suficientes, ele reverte toda a transação.

Um usuário também pode reembolsar o pool de Coinvesting DeFi usando o mesmo token, em vez de completar a troca. Isso é efetivamente o mesmo que deixar qualquer um pegar emprestado qualquer um dos ativos armazenados em um pool de Coinvesting DeFi (pela mesma taxa de 0,30% dos encargos de Coinvesting DeFi para negociação).<sup>(4)</sup>

## 2.4 Taxa de protocolo

Coinvesting DeFi v2 inclui uma taxa de protocolo de 0,05% que pode ser ligada e desligada. Se ativada, essa taxa seria enviada para um endereço de `feeTo` especificado no contrato de fábrica.

Inicialmente, `feeTo` não é definido e nenhuma taxa é cobrada. Um endereço pré-especificado `feeToSetter` pode chamar a função `setFeeTo` no contrato de fábrica do Coinvesting DeFi v2, definindo `feeTo` para um valor diferente. `feeToSetter` também pode chamar `setFeeToSetter` para alterar o próprio endereço `feeToSetter`.

Se o endereço `feeTo` for definido, o protocolo começará a cobrar uma taxa de 5 pontos-base, que é considerada como um corte de  $\frac{1}{6}$  das taxas de 30 pontos-base ganhas pelos provedores de liquidez. Ou seja, os traders continuarão a pagar uma taxa de 0,30% em todas as negociações; 83,3% dessa taxa (0,25% do valor negociado) irá para os provedores de liquidez, e 16,6% dessa taxa (0,05% do valor negociado) irá para o endereço `feeTo`.

A cobrança dessa taxa de 0,05% no momento da negociação imporia um custo adicional do gás a todas as negociações. Para evitar isso, as taxas acumuladas são cobradas apenas quando a liquidez é depositada ou retirada. O contrato calcula as taxas acumuladas e cria novos tokens de liquidez para o beneficiário da taxa, imediatamente antes de quaisquer tokens serem cunhados ou onerados.

O total das taxas cobradas pode ser calculado medindo o crescimento em  $\sqrt{k}$  (isso é,  $\sqrt{x \cdot y}$ ) desde a última vez que as taxas foram cobradas.<sup>(5)</sup> Esta fórmula fornece as taxas acumuladas entre  $t_1$  e  $t_2$  como uma porcentagem da liquidez na carteira em  $t_2$ :

$$f_{1,2} = 1 - \frac{\sqrt{k_1}}{\sqrt{k_2}} \quad (4)$$

Se a taxa foi ativada antes de  $t_1$ , o endereço `feeTo` deve capturar capture  $\frac{1}{6}$  das taxas que foram acumuladas entre  $t_1$  e  $t_2$ . Portanto, queremos cunhar novos tokens de liquidez para o endereço `feeTo` que representa  $\phi \cdot f_{1,2}$  da carteira, onde  $\phi$  é  $\frac{1}{6}$ .

Ou seja, queremos escolher  $s_m$  para satisfazer a seguinte relação, onde  $s_1$  é a quantidade total de ações em circulação no momento  $t_1$ :

$$\frac{s_m}{s_m + s_1} = \phi \cdot f_{1,2} \quad (5)$$

Depois de alguma manipulação, incluindo a substituição de  $1 - \frac{\sqrt{k_1}}{\sqrt{k_2}}$  por  $f_{1,2}$  e a resolução de  $s_m$ , nós podemos reescrever isso como:

$$s_m = \frac{\sqrt{k_2} - \sqrt{k_1}}{\left(\frac{1}{\phi} - 1\right) \cdot \sqrt{k_2} + \sqrt{k_1}} \cdot s_1 \quad (6)$$

Definir  $\phi$  como  $\frac{1}{6}$  nos dá a seguinte fórmula:

<sup>4</sup>Como Coinvesting DeFi v2 cobra taxas sobre os valores de entrada, a taxa relativa ao valor *retirado* é, na verdade, um pouco maior:  $\frac{1}{1-0.003} - 1 = \frac{3}{997} \approx 0.3009203\%$ .

<sup>5</sup>Podemos usar esta invariante, que não leva em conta os tokens de liquidez que foram cunhados ou queimados, porque sabemos que as taxas são cobradas toda vez que a liquidez é depositada ou retirada.

$$s_m = \frac{\sqrt{k_2} - \sqrt{k_1}}{5 \cdot \sqrt{k_2} + \sqrt{k_1}} \cdot s_1 \quad (7)$$

Suponha que o depositante inicial coloque 100 DAI e 1 ETH em um par, recebendo 10 ações. Algum tempo depois (sem que nenhum outro depositante tenha participado daquele par), eles tentam retirá-lo, num momento em que o par tem 96 DAI e 1,5 ETH. Conectar esses valores à fórmula acima nos dá o seguinte:

$$s_m = \frac{\sqrt{1.5 \cdot 96} - \sqrt{1 \cdot 100}}{5 \cdot \sqrt{1.5 \cdot 96} + \sqrt{1 \cdot 100}} \cdot 10 \approx 0.0286 \quad (8)$$

## 2.5 Meta transações para ações do pool

As ações do pool cunhadas pelos pares Coinvesting DeFi v2 suportam nativamente meta transações. Isso significa que os usuários podem autorizar uma transferência de suas ações do pool com uma assinatura<sup>(6)</sup>, em vez de uma transação em cadeia de seu endereço. Qualquer pessoa pode enviar esta assinatura em nome do usuário, chamando a função de permissão, pagando taxas de gás e possivelmente realizando outras ações na mesma transação.

## 3 Outras mudanças

### 3.1 Solidity

Coinvesting v1 é implementado em Vyper, uma linguagem de contrato inteligente semelhante ao Python. Coinvesting v2 é implementado no Solidity 8.0 mais amplamente utilizado, uma vez que requer alguns recursos que ainda não estavam disponíveis no Vyper (como a capacidade de interpretar os valores de retorno de tokens ERC-20 não padrão, bem como acesso a novos opcodes como `chainid` via montagem em linha) no momento em que estava sendo desenvolvido.

### 3.2 Re-arquitetura de contrato

Uma prioridade de projeto para Coinvesting v2 é minimizar a área de superfície e a complexidade do contrato do par principal - o contrato que armazena os ativos dos provedores de liquidez. Qualquer bug neste contrato pode ser desastroso, já que milhões de dólares de liquidez podem ser roubados ou congelados.

Ao avaliar a segurança desse contrato central, a questão mais importante é se ele protege os *provedores de liquidez* de terem seus ativos roubados ou bloqueados. Qualquer recurso destinado a apoiar ou proteger os *negociantes* - além da funcionalidade básica de permitir que um ativo do pool seja trocado por outro - pode ser tratado em um contrato de “*roteador*”.

Na verdade, até mesmo parte da funcionalidade de troca pode ser incluída no contrato do roteador. Como mencionado acima, o Coinvesting v2 armazena o último saldo registrado de cada ativo (a fim de evitar uma exploração manipuladora específica do mecanismo do oráculo). A nova arquitetura aproveita isso para simplificar ainda mais o contrato do Coinvesting v1.

Em Coinvesting DeFi v2, o vendedor envia o ativo para o contrato *principal* antes de chamar a função de swap. Em seguida, o contrato mede quanto do ativo ele recebeu, comparando o último saldo registrado com seu saldo atual. Isso significa que o contrato central é agnóstico

---

<sup>6</sup>A mensagem assinada segue o padrão EIP-712, o mesmo usado por meta transações para tokens como CHAI e DAI.

à forma como o trader transfere o ativo. Em vez de transferFrom, pode ser uma meta-transação ou qualquer outro mecanismo futuro para autorizar a transferência de ERC-20s.

### 3.2.1 Ajuste de taxa

A taxa de negociação do coinvesting v1 é aplicada reduzindo o valor pago no contrato em 0,3% antes de aplicar a invariante de produto constante. O contrato impõe implicitamente a seguinte fórmula:

$$(x_1 - 0.003 \cdot x_{in}) \cdot y_1 \geq x_0 \cdot y_0 \quad (9)$$

Com os flash swaps, o Coinvesting v2 introduz a possibilidade de que  $x_{in}$  e  $y_{in}$  possam ser diferentes de zero (quando um usuário deseja pagar o par usando o mesmo ativo, em vez de trocar). Para lidar com esses casos enquanto aplica as taxas de maneira adequada, o contrato foi escrito para fazer cumprir a seguinte invariante:<sup>(7)</sup>

$$(x_1 - 0.003 \cdot x_{in}) \cdot (y_1 - 0.003 \cdot y_{in}) \geq x_0 \cdot y_0 \quad (10)$$

Para simplificar esse cálculo na cadeia, podemos multiplicar cada lado da desigualdade por 1.000.000:

$$(1000 \cdot x_1 - 3 \cdot x_{in}) \cdot (1000 \cdot y_1 - 3 \cdot y_{in}) \geq 1000000 \cdot x_0 \cdot y_0 \quad (11)$$

### 3.2.2 sync() e skim()

Para se proteger contra implementações de tokens sob medida que podem atualizar o saldo do contrato do par, e para lidar com tokens mais graciosamente cujo suprimento total pode ser maior que  $2^{112}$ , Coinvesting v2 tem duas funções de resgate: sync() and skim().

sync() funciona como um mecanismo de recuperação no caso de um token diminuir de forma assíncrona o equilíbrio de um par. Nesse caso, as negociações receberão taxas abaixo do ideal e, se nenhum provedor de liquidez estiver disposto a retificar a situação, o par está preso. sync() existe para definir as reservas do contrato para os saldos atuais, proporcionando uma recuperação um tanto elegante desta situação.

skim() funciona como um mecanismo de recuperação no caso de tokens suficientes serem enviados a um par para transbordar os dois slots de armazenamento uint112 para reservas, o que poderia causar falha nas negociações. skim() permite que um usuário retire a diferença entre o saldo atual do par e  $2^{112} - 1$  para o chamador, se essa diferença for maior que 0.

## 3.3 Tratamento de tokens não padrão e incomuns

O padrão ERC-20 requer que transfer() e transferFrom() retornem um booleano indicando o sucesso ou falha da chamada [2]. As implementações de uma ou ambas as funções em alguns tokens - incluindo os populares como Tether (USDT) e Binance Coin (BNB) - em vez disso, não tem valor de retorno. Coinvesting v1 interpreta o valor de retorno ausente dessas funções definidas indevidamente como falsos - ou seja, como uma indicação de que a transferência não foi bem-sucedida - e reverte a transação, causando o fracasso da tentativa de transferência.

---

<sup>7</sup>Observe que usando a nova arquitetura, o  $x_{in}$  não é fornecido pelo usuário; em vez disso, é calculado medindo o saldo do contrato após o retorno de chamada,  $x_1$ , e subtraindo  $(x_0 - x_{out})$  dele. Essa lógica não distingue entre ativos enviados para o contrato antes de ser chamado e ativos enviados para o contrato durante o retorno de chamada.  $y_{in}$  é calculado da mesma maneira, com base em  $y_0$ ,  $y_1$ , e  $y_{out}$ .

Coinvesting v2 lida com implementações fora do padrão de forma diferente. Especificamente, se uma chamada<sup>(8)</sup> `transfer()` não tem valor de retorno, o Coinvesting v2 a interpreta como um sucesso ao invés de um fracasso. Essa alteração não deve afetar nenhum token ERC-20 que esteja em conformidade com o padrão (porque nesses tokens, `transfer()` sempre tem um valor de retorno).

Coinvesting v1 também pressupõe que as chamadas para `transfer()` e `transferFrom()` não podem acionar uma chamada reentrante para o contrato do par Coinvesting. Esta suposição é violada por certos tokens ERC-20, incluindo aqueles que suportam ERC-777's "hooks" [3]. Para apoiar totalmente tais tokens, o Coinvesting v2 inclui um " *bloqueio*" que impede diretamente a reentrada em todas as funções públicas de mudança de estado. Isso também protege contra a reentrada do retorno de chamada especificado pelo usuário em um flash swap, conforme descrito na seção 2.3.

### 3.4 Inicialização do fornecimento de token de liquidez

Quando um novo provedor de liquidez deposita tokens em um par de Coinvesting existente, o número de tokens de liquidez cunhados é calculado com base na quantidade existente de tokens:

$$s_{minted} = \frac{x_{deposited}}{x_{starting}} \cdot s_{starting} \quad (12)$$

Mas e se eles forem o primeiro depositante? Nesse caso,  $x_{starting}$  é 0, portanto, esta fórmula não funcionará.

Coinvesting v1 define a oferta inicial de ações como sendo igual à quantidade de ETH depositada (em wei). Esse foi um valor um tanto razoável, porque se a liquidez inicial fosse depositada ao preço correto, então 1 ação do pool de liquidez (que, como a ETH, é um token de 18 casas decimais) valeria aproximadamente 2 ETH.

No entanto, isso significava que o valor de uma ação da carteira de liquidez dependia do índice pelo qual a liquidez foi inicialmente depositada, o que era bastante arbitrário, especialmente porque não havia garantia de que esse índice refletisse o preço real. Além disso, o Coinvesting v2 oferece suporte a pares arbitrários, portanto, muitos pares não incluirão ETH de forma alguma.

Em vez disso, o Coinvesting v2 inicialmente produz ações iguais à média geométrica dos valores depositados:

$$s_{minted} = \sqrt{x_{deposited} \cdot y_{deposited}} \quad (13)$$

Essa fórmula garante que o valor de uma ação da carteira de liquidez a qualquer momento seja essencialmente independente do índice pelo qual a liquidez foi inicialmente depositada. Por exemplo, suponha que o preço de 1 ABC seja atualmente 100 XYZ. Se o depósito inicial tivesse sido 2 ABC e 200 XYZ (uma proporção de 1: 100), o depositante teria recebido  $\sqrt{2 \cdot 200} = 20$  ações. Essas ações agora ainda devem valer 2 ABC e 200 XYZ, mais as taxas acumuladas.

Se o depósito inicial fosse 2 ABC e 800 XYZ (uma proporção de 1: 400), o depositante teria recebido  $\sqrt{2 \cdot 800} = 40$  ações do pool<sup>(9)</sup>.

A fórmula acima garante que uma ação da carteira de liquidez nunca valerá menos do que a média geométrica das reservas dessa carteira. No entanto, é possível para o valor de

<sup>8</sup>Conforme descrito acima na seção 3.2, Coinvesting v2 não usa `transferFrom()`.

<sup>9</sup>Isso também reduz a probabilidade de erros de arredondamento, uma vez que o número de bits na quantidade de ações será aproximadamente a média do número de bits na quantidade de ativo X nas reservas, e o número de bits na quantidade de ativo Y nas reservas:

$$\log_2 \sqrt{x \cdot y} = \frac{\log_2 x + \log_2 y}{2} \quad (14)$$

uma parcela do pool de liquidez deve crescer ao longo do tempo, seja pelo acúmulo de taxas de negociação ou por meio de “doações” para o pool de liquidez. Em teoria, isso poderia resultar em uma situação em que o valor da quantidade mínima de ações da carteira de liquidez (ações da carteira 1e-18) vale tanto que se torna inviável para pequenos provedores de liquidez fornecer qualquer liquidez.

Para mitigar isso, o Coinvesting v2 queima as primeiras ações do pool 1e-15 (0,0000000000000001) que são cunhadas (1000 vezes a quantidade mínima de ações do pool), enviando-os para o endereço zero em vez de para o apostador. Este deve ser um custo insignificante para quase qualquer par de tokens.<sup>(10)</sup> Mas aumenta drasticamente o custo do ataque acima. Para aumentar o valor de uma ação do pool de liquidez para \$ 100, o invasor precisaria doar \$ 100.000 para o pool, que ficaria permanentemente bloqueado como liquidez.

### 3.5 Wrapping ETH

A interface para fazer transações com o ativo nativo da Ethereum, ETH, é diferente da interface padrão para interagir com tokens ERC-20. Como resultado, muitos outros protocolos no Ethereum não suportam ETH, em vez de usar um token canônico ”wrapped ETH”, WETH [4].

Coinvesting v1 é uma exceção. Como cada par v1 da Coinvesting incluía o ETH como um ativo, fazia sentido lidar diretamente com o ETH, que era um pouco mais eficiente em termos de gás.

Como o Coinvesting v2 oferece suporte a pares ERC-20 arbitrários, agora não faz mais sentido oferecer suporte a ETH desembrulhado. Adicionar tal suporte dobraria o tamanho da base de código principal e arrisca a fragmentação de liquidez entre os pares ETH e WETH<sup>(11)</sup>. O ETH nativo precisa ser agrupado no WETH antes de ser negociado no Coinvesting v2.

### 3.6 Endereços de pares determinísticos

Como em Coinvesting v1, todos os contratos de pares do Coinvesting v2 são instanciados por um único contrato de fábrica. No Coinvesting v1, esses contratos de pares foram criados usando o opcode CREATE, o que significa que o endereço de tal contrato depende da ordem em que o par foi criado. Coinvesting v2 usa o novo opcode CREATE2 da Ethereum [5] para gerar um contrato de par com um endereço determinístico. Isso significa que é possível calcular o endereço de um par (se houver) da cadeia, sem ter que olhar para o estado da cadeia.

### 3.7 Saldo máximo de tokens

Para implementar com eficiência o mecanismo do oráculo, o Coinvesting v2 suporta apenas saldos de reserva de até  $2^{112} - 1$ . Esse número é alto o suficiente para suportar tokens de 18 casas decimais com um totalSupply acima de 1 quadrilhão.

Se o saldo da reserva ficar acima de  $2^{112} - 1$ , qualquer chamada para a função swap começará a falhar (devido a uma verificação na função `_update()`). Para se recuperar dessa situação, qualquer usuário pode chamar a função `skim()` para remover o excesso de ativos do pool de liquidez.

---

<sup>10</sup>Em teoria, há alguns casos em que essa queima não pode ser desprezível, como pares entre tokens decimais zero de alto valor. No entanto, esses pares são inadequados para Coinvesting de qualquer maneira, uma vez que erros de arredondamento tornariam a negociação inviável.

<sup>11</sup>No momento em que este livro foi escrito, um dos pares de maior liquidez no Coinvesting v1 é o par entre ETH e WETH.

## Referências

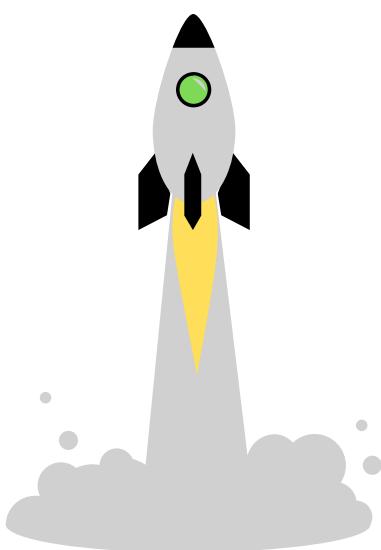
- [1] Christopher Miranda. 2019. url: <https://coinvesting.io/CriptoconomiaATecnologiaBlockchainComoMotorDePropulsãoEconômicaAtravésDasCryptotechs>
- [2] Fabian Vogelsteller and Vitalik Buterin. Nov. 2015. URL: <https://eips.ethereum.org/EIPS/eip-20>.
- [3] Jordi Baylina Jacques Dafflon and Thomas Shababi. *EIP 777: ERC777 Token Standard*. Nov. 2017. URL: <https://eips.ethereum.org/EIPS/eip-777>.
- [4] Radar. *WTF is WETH?* URL: <https://weth.io/>.
- [5] Vitalik Buterin. *EIP 1014: Skinny CREATE2*. Apr. 2018. URL: <https://eips.ethereum.org/EIPS/eip-1014>.

## 4 Disclaimer

Este artigo é apenas para fins de informação geral. Não constitui um conselho de investimento ou uma recomendação ou solicitação de compra ou venda de qualquer investimento e não deve ser usado na avaliação do mérito da tomada de qualquer decisão de investimento. Não deve ser invocado para aconselhamento contábil, jurídico ou tributário ou recomendações de investimento. Este artigo reflete as opiniões atuais dos autores. As opiniões aqui refletidas estão sujeitas a alterações sem serem atualizadas.

# **ROADMAP**

**"FIQUE ATENTO ÀS  
DATAS E INFORMAÇÕES A  
SEGUIR E NÃO PERCA O  
*TIME.*"**



# **COINVESTING DEX**

## **ROADMAP**

**1**

**ICO(OFERTA INICIAL DE CRIPTOMOEDAS)  
COINVEX TOKEN 0,01 USD**

AS 00h00min do dia 15 de abril de 2021.



**2**

**TÉRMINO DA OFERTA INICIAL DE  
CRIPTOMOEDAS(COINVEX TOKEN 0,05 USD)**

AS 23h59min do dia 15 de agosto de 2021.

**3**

**LISTAGEM DO COINVEX TOKEN NA COINVESTING  
DEX A 0,10 USDT E INÍCIO DAS OPERAÇÕES DA  
PLATAFORMA**

As 06h00min do dia 16 de agosto de 2021.

**4**

**LISTAGEM DO COINVEX TOKEN EM OUTRAS  
EXCHANGES**

Segundo semestre de 2021.



# **COINVEX É O TOKEN OFICIAL DA COINVESTING DEX DECENTRALIZED EXCHANGE**

A **Coinvesting DEX permitirá a negociação de tokens padrão ERC-20 de forma não custodial** por meio de uma conexão com uma carteira de software(Metamask e outras) ou de hardware.

A Coinvesting DEX lançará o seu token de governança(**COINVEX TOKEN**) através de uma distribuição de **280.000.000** tokens de um **total de 1.000.000.000** unidades por meio de sua **ICO “Oferta Inicial de Criptomoedas”**, que **começará as 00h00min do dia 15 de abril de 2021** com **valor do token a 0,01 USD** e se **encerrará as 23h59 do dia 15 de agosto de 2021** com **valor do token a 0,05 USD**, quando logo em seguida, **as 06h00min do dia 16 de agosto de 2021**, a **Coinvesting DEX dará início às operações em sua plataforma descentralizada** de negocações através do protocolo Coinvesting DeFi v2 na rede Ethereum e o **COINVEX TOKEN** **será listado oficialmente na Coinvesting DEX** com o **valor inicial de 0,10 USDT**.

Para **adquirir seus COINVEX TOKENS** durante a "**Oferta Inicial de Criptomoedas**" bastará **acessar sua carteira(Metamask)**, **alimentá-la com ETH (ETHEREUM)**, **conectar sua carteira** com a nossa interface gráfica/contrato inteligente COINVEX TOKEN e **em seguida realizar a compra/transferência do COINVEX TOKEN para sua carteira Metamask**.

**PRONTO! VOCÊ JÁ AQUIRIU OS SEUS**

# **COINVEX TOKENS**

**E PODERÁ ARMAZENÁ-LOS/UTILIZÁ-LOS  
QUANDO E COMO QUISER!**

**O COINVEX TOKEN** será listado oficialmente na **Coinvesting DEX** as 06h00min do dia **16 de agosto de 2021** sob o par **COINVEX/USDT** no valor de **1 COINVEX TOKEN para 0,10 USDT**, momento em que o protocolo Coinvesting DeFi v2 iniciará a negociação de tokens padrão ERC-20 de forma não custodial por meio de uma conexão com uma carteira de software(Metamask) ou de hardware.

**Os volumes negociados em DEXs(Decentralized Exchanges) aumentaram consideravelmente nos últimos meses.** A líder global no segmento de DEXs liderou esse volume, com mais de **US\$ 25 bilhões apenas em janeiro de 2021**, além do volume de negociações de tokens padrão ERC-20 apenas no mercado brasileiro registrar a incrível marca de **50 milhões de reais diários** em março de 2021, em um universo de apenas **2 milhões de Cripto investidores brasileiros**, neste momento.

Por isso **limitamos o suprimento total do COINVEX TOKEN para 1.000.000.000**(um bilhão de tokens padrão ERC-20) de modo que ele se torne cada vez mais escasso em um **segmento que vêm aumentando cada vez mais** seus os **volumes negociados nos últimos meses**.

**NA PRÁTICA!**

# **COINVESTING DEX**

## **NOVO ECOSSISTEMA DE NEGOCIAÇÕES**

**Você precisará apenas conectar sua carteira(Metamask ou outras) na interface da Coinvesting Dex, que automaticamente você irá interagir com os smart contracts Coinvesting DeFi v2 e poderá trocar suas criptomoedas padrão ERC-20 por outras criptomoedas padrão ERC-20.**

**Você poderá ainda criar novos pares de trocas de tokens ERC-20.** Para criar novos pares bastará **adicionar liquidez aos pools da Coinvesting DEX**(interagir seus tokens com o protocolo Coinvesting DeFi v2 smart contract através da sua carteira Metamask ou outras) e quando **houver alguma negociação dos seus pares de tokens você será recompensado**(partição automatizada e proporcional ao pool das taxas de corretagem geradas na Coinvesting DEX através do mesmo smart contract Coinvesting DeFi v2), **podendo ainda desvincular seus tokens quando quiser através do respectiva interface/smart contract.**

**As negociações na Coinvesting DEX funcionarão por meio de um formador automático de mercado (AMM), que usa uma fórmula  $x * y = k$ , em que x representa a quantidade de um token em um pool de liquidez, y é a quantidade de outro ativo e k é uma constante fixa.**

**O valor de ambos os ativos nos AMMs da Coinvesting DEX é de 50:50. Quando um token do par do AMM aprecia ou deprecia, o outro token será comprado ou vendido para compensar a diferença.**

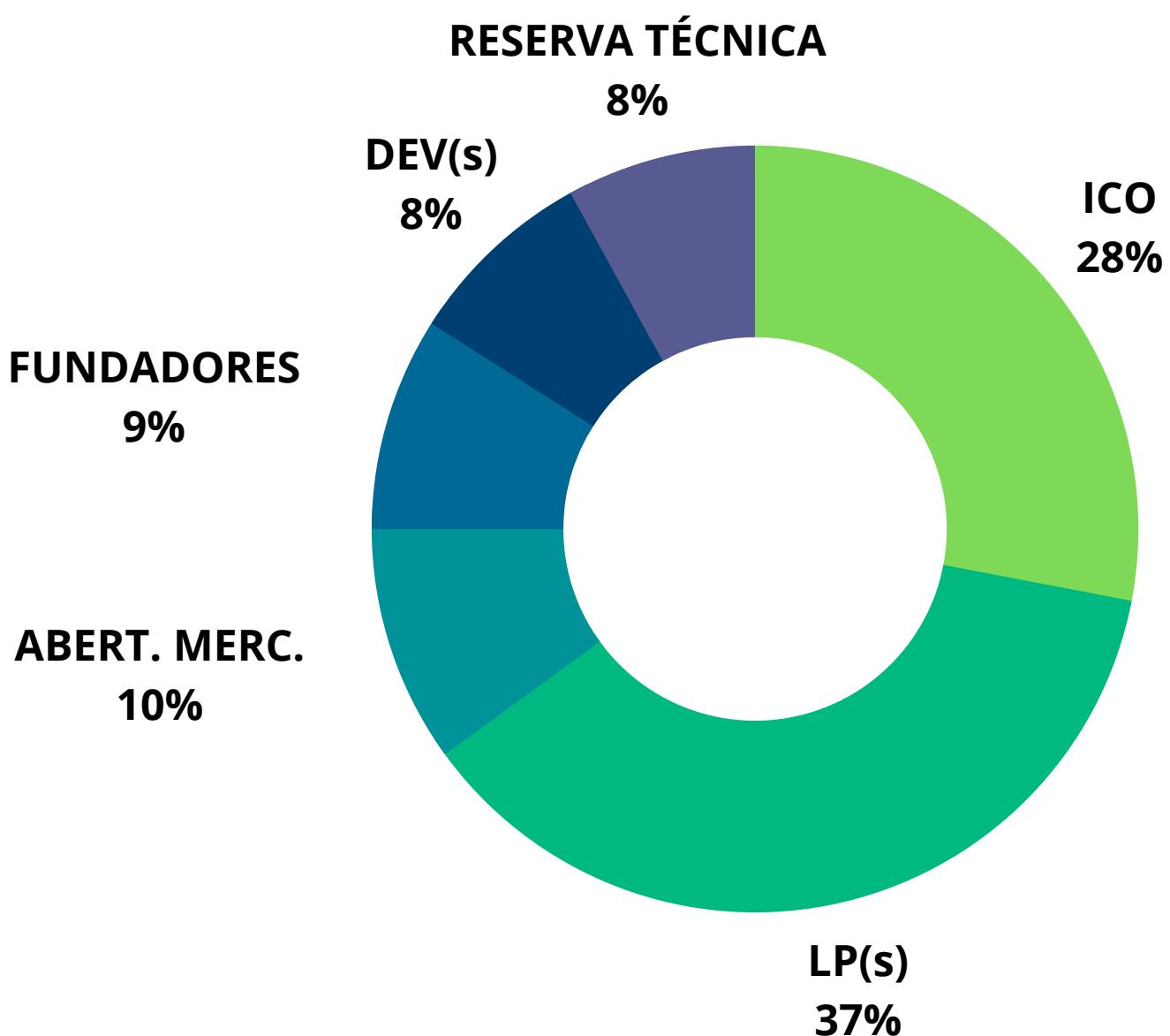
**Fornecedores de liquidez ou Liquid Providers (LPs) fornecem seus tokens a um pool específico de liquidez.** LPs substituem os livros de oferta tradicionais de corretoras centralizadas. Assim, **LPs recebem 0,3% das taxas negociadas e geradas por negociações no pool.**

Outros incentivos, como “**yield farming**” — empréstimo de fundos a outros usuários em troca de taxa de juros — e “**liquidity mining**” — recompensa a um pool de formadores de mercado pelo incentivo de liquidez para um token específico — **também encorajam LPs a fornecer liquidez.**

CAPILARIDADE

# COINVEX TOKEN

GRÁFICO DE DISTRIBUIÇÃO



- 28% do total de tokens criados estará disponível para venda aos consumidores durante os eventos de venda privada e ICO(Oferta Inicial de Criptomoedas). Caso o montante total de tokens não seja vendido neste processo, a quantidade remanescente será destruída;
- 37% do total de tokens será destinado às recompensas aos LPs (provedores de liquidez) a fim de gerar engajamento digital com seus usuários e fortalecer a usabilidade da moeda no ecossistema Coinvesting DEX. Esses tokens poderão ser utilizados exclusivamente para ações dentro da plataforma Coinvesting DEX, sem a possibilidade de troca em outras exchanges no primeiro uso;
- 10% do total de tokens será destinado à abertura de mercado, com o objetivo de firmar parcerias estratégicas. Esses tokens poderão ser utilizados tanto para ações dentro da plataforma Coinvesting DEX como em outras exchanges;
- 9% do total de tokens será destinado aos sócios fundadores (sujeitos às regras de realização);
- 8% do total de tokens será destinado à equipe de desenvolvedores (sujeitos às regras de realização);
- 8% do total de tokens será destinado a um fundo de reserva interno. Estes tokens serão liquidados apenas caso haja necessidade de recursos para expansão internacional das atividades da empresa;

Os tokens destinados aos fundadores e equipe de desenvolvedores estão sujeitos à seguinte regra de realização: 20% após o lançamento do token em outras exchanges e 10% a cada bimestre.

### **Percentuais de alocação dos recursos captados:**

- 40% Desenvolvimento do Negócio/MKT
- 25% Desenvolvimento de Software
- 20% Pessoal/Profissionais
- 10% G&A
- 5% Outros

