Dedicamos esse livro a você.

Obrigado pela curiosidade e por decidir ler esse livro.

Agradecemos também por você estar interessado em aprender sobre tópicos fundamentais que serão cruciais para a construção de nosso futuro próximo.

Índice

[Parte 1: ECONOMIA DA ENGENHARIA DE TOKENS 1](#_Toc127108682)

[Capítulo 1: Introdução aos Fundamentos da Economia de Tokens 2](#_Toc127108683)

[1.1 Camada 1 vs. Protocolos DApp 2](#_Toc127108684)

[1.2 Economia em Três Palavras 4](#_Toc127108685)

[1.3 10 Perguntas Frequentes Sobre a Economia da Construção de Tokens 8](#_Toc127108686)

[1.4 Conclusão 14](#_Toc127108687)

[Capítulo: 2 Evolução da Economia 16](#_Toc127108688)

[2.1 Economia definida de forma simples 16](#_Toc127108689)

[2.2 Fatores de Produção 16](#_Toc127108690)

[2.3 Economia e a Evolução Tecnológica 21](#_Toc127108691)

[2.4 Tabela de Resumo 23](#_Toc127108692)

[Capítulo: 3 Coordenação e Incentivos 24](#_Toc127108693)

[3.1 Evolução Geral da Coordenação 24](#_Toc127108694)

[3.2 Coordenação a Nível de Mercado 25](#_Toc127108695)

[3.3 Cooperação 27](#_Toc127108696)

[3.4 [Estudo de Caso] Coordenação e Economia de Token: MolochDAO 28](#_Toc127108697)

[3.5 Externalidades de Incentivos 29](#_Toc127108698)

[Capítulo: 4 Objetivos e Restrições 34](#_Toc127108699)

[4.1 Objetivo 34](#_Toc127108700)

[4.2 Restrições 35](#_Toc127108701)

[4.3 Processo de Design 35](#_Toc127108702)

[Capítulo: 5 As Sete Maravilhas da Economia de Token 37](#_Toc127108703)

[5.1 Efeitos de Rede (Network Effects) 37](#_Toc127108704)

[5.2 Sinalização 39](#_Toc127108705)

[5.3 Políticas Monetárias 40](#_Toc127108706)

[5.4 Direito de Propriedade 42](#_Toc127108707)

[5.5 Lock-In 43](#_Toc127108708)

[5.6 Problema do Principal-Agente, Risco Moral, e Informação Assimétrica 44](#_Toc127108709)

[5.7 Ponto Focal ou Ponto de Schelling 47](#_Toc127108710)

[Capítulo: 6 Design de Mercado 49](#_Toc127108711)

[6.1 Design de Mercado: Parte 1 – Introdução 49](#_Toc127108712)

[6.2 Por que Design de Mercado é Importante para Ecossistemas de Token? 50](#_Toc127108713)

[6.3 Design de Mercado: Parte 2 – Definindo Design 50](#_Toc127108714)

[6.4 Design de Mercado: Parte 3 – Por Que Estudar Design de Mercado? 51](#_Toc127108715)

[6.5 Fatores no Design de Mercado 54](#_Toc127108716)

[6.6 Robustez (ou Densidade) 55](#_Toc127108717)

[6.7 Congestionamento Reduzido 55](#_Toc127108718)

[6.8 Segurança & Facilidade de Uso 55](#_Toc127108719)

[6.9 Design de Mercado e Economia de Token 56](#_Toc127108720)

[Capítulo: 7 [Estudo de Caso] Nexus Mutual 59](#_Toc127108721)

[7.1 O que é o Nexus Mutual 59](#_Toc127108722)

[7.2 Primeiros Passos com $NXM 59](#_Toc127108723)

[7.3 Como a Nexus Mutual Funciona? 60](#_Toc127108724)

[7.4 Aplicando Design de Mercado na Nexus Mutual 61](#_Toc127108725)

[7.5 Robustez do Mercado 62](#_Toc127108726)

[7.6 Congestionamento Reduzido 63](#_Toc127108727)

[7.7 Segurança & Facilidade de Uso 63](#_Toc127108728)

[Capítulo: 8 Design de Mecanismo 65](#_Toc127108729)

[8.1 Design de Mecanismo: Parte 1 - Introdução 65](#_Toc127108730)

[8.2 Por que Precisamos de Design de Mecanismo? 65](#_Toc127108731)

[8.3 Por que é Importante para Ecossistemas de Token? 66](#_Toc127108732)

[8.4 Design de Mecanismo: Parte 2 – O Que é? 66](#_Toc127108733)

[8.5 Design de Mecanismo: Parte 3 – Por que estudar? 67](#_Toc127108734)

[8.6 Primeiros Passos 69](#_Toc127108735)

[8.7 Fatores no Design de Mecanismo 69](#_Toc127108736)

[8.8 Governança 72](#_Toc127108737)

[8.9 Incentivos Não-Financeiros 72](#_Toc127108738)

[8.10 Estrutura 74](#_Toc127108739)

[8.11 Design de Mecanismo e Economia de Token 75](#_Toc127108740)

[Capítulo: 9 [Estudo de Caso] MakerDAO 81](#_Toc127108741)

[9.1 Plataforma baseada em DAO 81](#_Toc127108742)

[9.2 Governança 84](#_Toc127108743)

[9.3 Incentivos Não-Financeiros 88](#_Toc127108744)

[9.4 Estrutura 90](#_Toc127108745)

[9.5 Conclusão 93](#_Toc127108746)

[Capítulo: 10 Design de Token 94](#_Toc127108747)

[10.1 Token Design: Parte 1 - Introdução 94](#_Toc127108748)

[10.2 Por que precisamos de Design de Token? 94](#_Toc127108749)

[10.3 Por que é Importante para um Ecossistema? 94](#_Toc127108750)

[10.4 Design de Token: Parte 2 – O que é? 94](#_Toc127108751)

[10.5 Token Design: Parte 3 – Por Que se Aprofundar? 95](#_Toc127108752)

[10.6 Fatores no Design de Token 96](#_Toc127108753)

[10.7 Design e Economia de Tokens 106](#_Toc127108754)

[Capítulo: 11 “Curvas de Ligação”, ou *Bonding Curves* 111](#_Toc127108755)

[11.1 Definindo Curvas de Ligação 111](#_Toc127108756)

[11.2 Quatro Propriedades de Bonding Curves (“Curvas de ligação”) 113](#_Toc127108757)

[11.3 Considerações Sobre Bonding Curves 114](#_Toc127108758)

[11.4 Perguntas Práticas para Começar 116](#_Toc127108759)

[11.5 Duas Variações de Curvas de Ligação (Bonding Curves) 116](#_Toc127108760)

[Capítulo: 12 [Estudo de Caso] Bancor 118](#_Toc127108761)

[12.1 Introdução ao Protocolo Bancor 118](#_Toc127108762)

[12.2 Objetivos da Bancor 120](#_Toc127108763)

[12.3 Tokens no Protocolo Bancor 121](#_Toc127108764)

[12.4 Bancor e DeFi 124](#_Toc127108765)

[12.5 Aplicações de Design de Token no protocolo Bancor 126](#_Toc127108766)

[12.6 Política de Token 127](#_Toc127108767)

[12.7 Incentivos Financeiros 128](#_Toc127108768)

[12.8 Arquitetura 130](#_Toc127108769)

[12.9 Conclusão 135](#_Toc127108770)

[Capítulo: 13 Outros Princípios Econômicos 136](#_Toc127108771)

[13.1 Tokens de Desconto 136](#_Toc127108772)

[13.2 Direto de Propriedade 139](#_Toc127108773)

[13.3 Financiamento Inflacionário por Convicção de Stake 141](#_Toc127108774)

[13.4 Teoria Geral dos Contratos 142](#_Toc127108775)

[13.5 Registros Curados de Tokens (TCRs) 143](#_Toc127108776)

[Parte II: FINANÇAS DESCENTRALIZADAS 145](#_Toc127108777)

[Capítulo: 14 Economia em Finanças Descentralizadas (DeFi) 146](#_Toc127108778)

[14.1 Introdução ao DeFi 146](#_Toc127108779)

[14.2 Nove Perguntas Frequentes Sobre DeFi 151](#_Toc127108780)

[14.3 Economia vs. Valor Monetário 157](#_Toc127108781)

[14.4 Como DeFi Cria Valor Econômico Agregado? 157](#_Toc127108782)

[14.5 Nove Setores de DeFi 159](#_Toc127108783)

[Capítulo: 15 Ponzinomics 165](#_Toc127108784)

[15.1 Economia (Economics) vs. Ponzinomics 165](#_Toc127108785)

[15.2 Fundamentos de Ponzinomics 166](#_Toc127108786)

[15.3 Estudo de Caso: Ponzinomics Sete Passos 166](#_Toc127108787)

[15.4 Dez Mecanismos de Ponzinomics 167](#_Toc127108788)

[Capítulo: 16 Matemática de Tokens Estáveis 168](#_Toc127108789)

[16.1 Conceitos Matemáticos de DeFi 168](#_Toc127108790)

[16.2 Moedas Como Meio de Pagamento 168](#_Toc127108791)

[Capítulo: 17 Matemática dos Mecanismos de AMMs Descentralizados 170](#_Toc127108792)

[17.1 CeFi vs. DeFi 170](#_Toc127108793)

[17.2 Formadores de Mercado Automatizados (AMMs) 171](#_Toc127108794)

[17.3 Gráfico Geral 172](#_Toc127108795)

[Capítulo: 18 Curvas de Ligação para Captação de Recursos (*Fundraising*) 174](#_Toc127108796)

[18.1 Aplicações para Fundraising 174](#_Toc127108797)

[18.2 Captação para Tokens com Função de Utilidade 174](#_Toc127108798)

[18.3 Captação para Tokens Classificados como Securities 181](#_Toc127108799)

[Capítulo: 19 Seguros em Cripto 183](#_Toc127108800)

[19.1 Seguros de Contratos Inteligentes 183](#_Toc127108801)

[19.2 Seguros de Impermanent Loss (“Perdas Impermanentes”) 183](#_Toc127108802)

[Capítulo: 20 Derivativos em Cripto 185](#_Toc127108803)

[20.1 Ativos Sintéticos 185](#_Toc127108804)

[20.2 Tokens Alavancados 187](#_Toc127108805)

[20.3 Tokenização de Títulos de Cripto 188](#_Toc127108806)

[Capítulo: 21 Riscos Financeiros de DeFi 191](#_Toc127108807)

[21.1 Custo de Oportunidade 191](#_Toc127108808)

[21.2 Reduções de Liquidez 191](#_Toc127108809)

[21.3 Slippage de Preço 192](#_Toc127108810)

[21.4 Perdas Impermanentes, ou Impermanent Loss 193](#_Toc127108811)

[Capítulo: 22 DAO, O Futuro da Governança 197](#_Toc127108812)

[22.1 Potenciais Melhorias para o Sistema Atual 197](#_Toc127108813)

[22.2 Definição básica: Contratos inteligentes 198](#_Toc127108814)

[22.3 Exemplo: Como Alocar Fundos 198](#_Toc127108815)

[22.4 Economia de DAOs 199](#_Toc127108816)

[22.5 Outros Tipos de DAO 201](#_Toc127108817)

[Capítulo: 23 Economia de Yield Farming 203](#_Toc127108818)

[23.1 Projetos Utilizando Yield Farming 203](#_Toc127108819)

[23.2 O Bom, Ruim, e Pior 204](#_Toc127108820)

[23.3 Economia de Yield Farming 205](#_Toc127108821)

[23.4 Valor do Yield Farming 205](#_Toc127108822)

[23.5 Resumo 206](#_Toc127108823)

[Capítulo: 24 [Estudo de Caso] Binance 207](#_Toc127108824)

[24.1 Design de Mercado 207](#_Toc127108825)

[24.2 Estrutura do Token 208](#_Toc127108826)

[24.3 Incentivos Financeiros 211](#_Toc127108827)

[24.4 Conclusões 212](#_Toc127108828)

[Capítulo: 25 [Estudo de Caso] Esse Livro 214](#_Toc127108829)

[25.1 Pensamentos Por Trás Dessa Ideia 214](#_Toc127108830)

[25.2 Direitos de Distribuição como NFT 214](#_Toc127108831)

[25.3 Design Econômico desse NFT - $EDBK 215](#_Toc127108832)

[Capítulo: 26 O Futuro de Ecossistemas Tokenizados 218](#_Toc127108833)

[26.1 O Que Esperar Para o Futuro da Engenharia de Tokens e DeFi 218](#_Toc127108834)

[26.2 Setores Para Ficar de Olho 218](#_Toc127108835)

[26.3 Futuro Ideal 219](#_Toc127108836)

Introdução

Disclaimer: Esse livro menciona vários projetos e protocolos. Não há nenhum tipo de endosso para tais projetos. Projetos referenciados foram selecionados de acordo com o *Market Cap* dentro de cada categoria ou pelo fato de ser o mais relevante para certos mecanismos. No momento de escrita desse livro, projetos e protocolos mencionados estavam vivos e com comunidades ativas.

Nada nesse material pode ser considerado aconselhamento financeiro.

*Em resumo: Esse é um livro de referência. A maioria dos capítulos faz sentido individualmente. Leitura sequencial não é necessária para entender cada capítulo.*

Esse livro é a culminação de três anos de pesquisa. Todas as informações eram atuais no momento de escrito. Porém, dada velocidade em que o setor se move, muita coisa pode ter mudado até o momento em que você está lendo essa obra. Não se esqueça disso!

Iremos abordar tópicos diversos, desde economia e finanças, até matemática e tecnologia. Por mais que nossa intenção seja de que você leia todos os capítulos e páginas, o livro foi escrito de forma que cada capítulo é independente dos outros. Com isso, você pode pular para capítulos ou tópicos específicos conforme necessário. Quando contexto adicional for requerido, você encontrará referências para demais capítulos.

Use esse livro como um manual/guia para te ajudar no entendimento do setor e principais fundamentos. Você encontrará recomendações de como navegar esse material nas próximas páginas, de acordo com seu contexto pessoal.

Criei também um glossário com explicações básicas dos principais termos explorados no final do livro. Rodapés contém referências, comentários adicionais e links para reports mais longos.

Boa leitura!

**Lisa JY Tan**

Como ler esse livro: Guia de Navegação

Esse livro cobre fundamentos da economia de tokens. Use esse guia de navegação para mapear capítulos mais relevantes para você.

Esse livro foi organizado em duas grandes partes. Capítulos 1 ao 13 focam na Economia. Capítulos 14 ao 25 focam em mecanismos e matemática de Finanças Descentralizadas (DeFi).

Para desenvolvedores de protocolos

Você possui uma ideia, e deseja transformá-la em um contrato inteligente na blockchain:

* Entendendo os fundamentos: Cáp. 4, Cáp. 6 , Cáp. 8, Cáp. 10, Cáp. 13
* Introdução a Bonding Curve: Cáp. 11
* Introdução a DeFi: Cáp. 14
* Matemática para aplicações de DeFi: Cáp. 16 ao 20
* Governança: Cáp. 22

Para investidores de varejo

Você busca entender mais sobre análise fundamentalista antes de investir nesses protocolos a longo prazo. O ideal é que você estude os fundamentos ao invés de *apenas* análises de mercado.

* Estudos de casos: Cáp. 7, Cáp. 9, Cáp. 12, Cáp. 25, Cáp. 26
* Introdução a DeFi: Cáp. 14
* Matemática para aplicações de DeFi: Cáp. 16 ao 20
* Governança: Cáp. 22

Para os que apenas querem se educar mais sobre o setor:

Caso você esteja buscando um emprego no setor, aprender mais antes de investir, oferecer consultoria para projetos, ou começar seu próprio negócio. Todos essas são metas incríveis!

* Economia da engenharia de tokens: Cáp. 1 ao 13
* DeFi e Matemática: Cáp. 14 ao 25

Para os reguladores e legisladores

Obrigado por não forçar um sistema novo a se encaixar nos moldes do antigo. Regulamentação anda de mãos dadas com inovação, apoiando novos sistemas e formas de resolver os problemas.

* Princípios econômicos desses ecossistemas: Cáp. 6, Cáp. 8, Cáp. 10, Cáp. 13
* Estudos de casos: Cáp. 7, Cáp. 9, Cáp. 12, Cáp. 25, Cáp. 26

# Parte 1: ECONOMIA DA ENGENHARIA DE TOKENS

## Capítulo 1: Introdução aos Fundamentos da Economia de Tokens

### Camada 1 vs. Protocolos DApp

Em blockchain e outras tecnologias, podemos dividir o sistema em três camadas: Camada 1, Camada 2, e a Camada de Aplicações (Camada de DApps).

O conjunto de regras de formatação e processamento de dados que cada sistema segue é chamado de protocolo[[1]](#footnote-2). Possibilita a comunicação entre os mais variados sistemas das camadas 1 e 2, assim como a camada de aplicações.

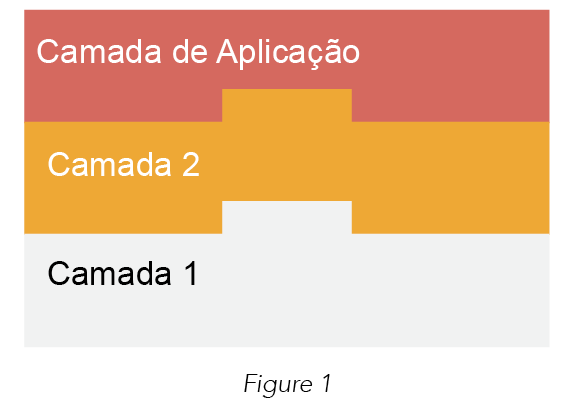


Figura 1

Protocolos de Camada 1 formam a camada base de tecnologia. Protocolos de Camada 2 geralmente são focados em resolver problemas de escalabilidade da Camada 1. DApps (termo usado para “Aplicativos Descentralizados”) são desenvolvidos e utilizados na Camada de Aplicação. DApps são os ambientes da rede em que tokens habitam. Protocolos de Camada 1 e 2 são como os sistemas operacionais do seu celular, como iOS ou Android. Protocolos da Camada de Aplicação são análogos aos diversos aplicativos que você acessa por meio da App Store ou Google Play, como Twitter, LinkedIn ou WhatsApp.

**L1 Analogia do mundo físico:** Inglês, espanhol, francês.

**L1 Exemplos do mundo digital:** Solidity[[2]](#footnote-3) da Ethereum, Glow[[3]](#footnote-4) da Cardano, Rust[[4]](#footnote-5) da Polkadot, e Motoko[[5]](#footnote-6) da Internet Computer.

**L2 Analogia do mundo físico:** Inglês jamaicano, inglês escocês, inglês australiano, inglês americano.

**L2 Exemplos do mundo digital:** ZK-rollup, Rollup Otimista, ou Sidechains na Ethereum

**DApp Analogia do mundo físico:** Inglaterra, Índia, Estados Unidos, Singapura, Escócia, Nova Zelândia

**DApp Exemplos do mundo digital:** Aave, Maker, Nexus Mutual

Assim como os idiomas inglês e espanhol podem ser traduzidos de um para o outro com esforço e a ajuda de um dicionário, protocolos que possuem *interoperabilidade* podem se comunicar entre suas próprias linguagens.

*Interoperabilidade* é necessária visto que o mundo digital possui muito mais do que apenas dois idiomas. Há um oceano de linguagens de Camada 1 e Camada 2, e precisamos de soluções de interoperabilidade se desejamos enviar e receber informações ou dados entre os protocolos e suas diferentes camadas. Ou seja, encontrar um Sistema para traduzir esses idiomas de um para o outro. Geralmente chamamos essa função de *cross-chain*. Exemplos incluem Starkware, Tendermint, e Cosmos.

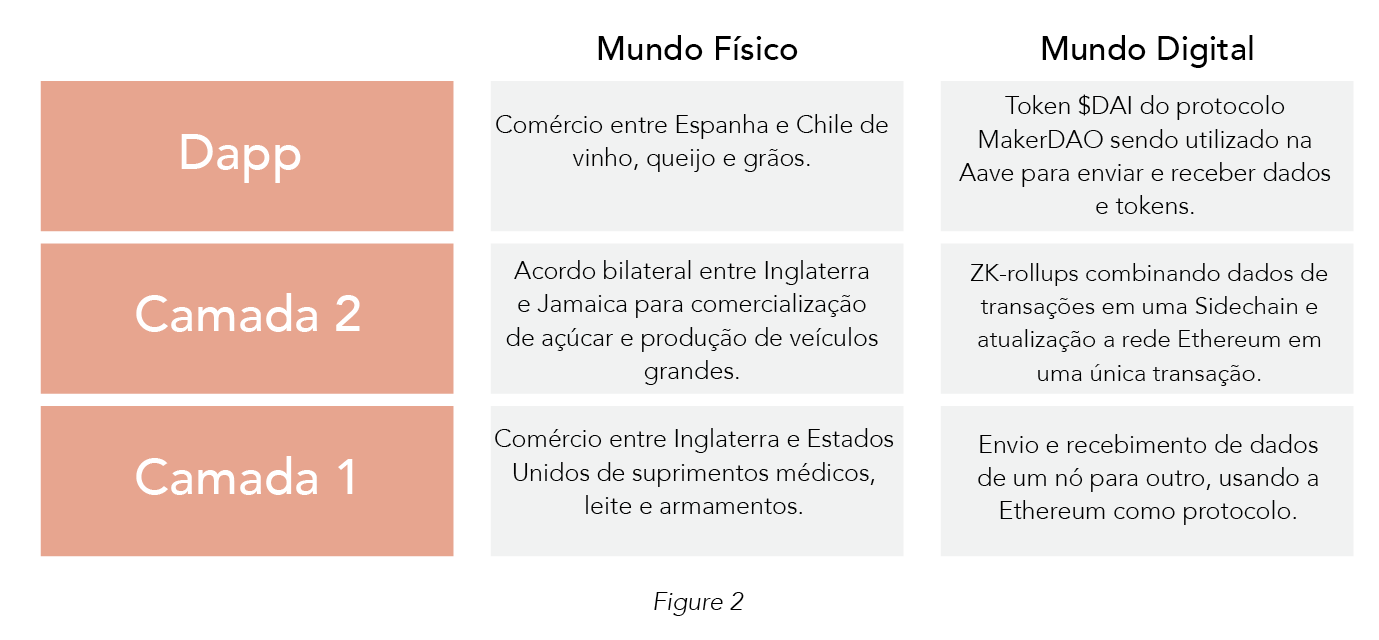


Figura 2

No contexto de sistemas de blockchain, interoperabilidade é chamada de “funcionalidade cross-chain”. Cada protocolo de Camada 1 funciona de forma independente e isolada. Por isso, a habilidade de “cruzar” (*cross*) as mais variadas “cadeias” (*chains*) se torna crucial. Essa funcionalidade cross-chain entre protocolos de Camada 1 são um grande tópico de discussão por si só. Para protocolos de Camada 2, soluções de escalabilidade e arquiteturas tecnológicas são fundamentais. Nesse livro, porém, vamos focar nos protocolos de DApp e os fundamentos matemáticos e econômicos que os regem.

Isso significa que vamos focar menos em protocolos de Camada 1, seus problemas (como tolerância a falhas Bizantinas, ataques Sybil, impactos na mudança de incentivos de validadores de acordo com a Teoria dos Jogos etc.), e modelos de consenso[[6]](#footnote-7). O foco será nos modelos matemáticos necessários para desenvolver diversos mecanismos de incentivo e outras considerações econômicas que impactam o comportamento dos agentes econômicos em um ecossistema fechado (por exemplo, um DApp)[[7]](#footnote-8).

### Economia em Três Palavras

Economia pode ser dividida em dois grandes domínios: Macroeconomia e Microeconomia. Nos últimos anos, o campo de Economia Comportamental vem ganhando muita relevância. Existem, também, outras vertentes de pensamento que influenciam a forma como cada um interpreta políticas e conceitos econômicos. Na sua essência, economia pode ser descrita em três simples conceitos:

* Incentivos
* Punições (Desincentivos)
* Comportamentos[[8]](#footnote-9)

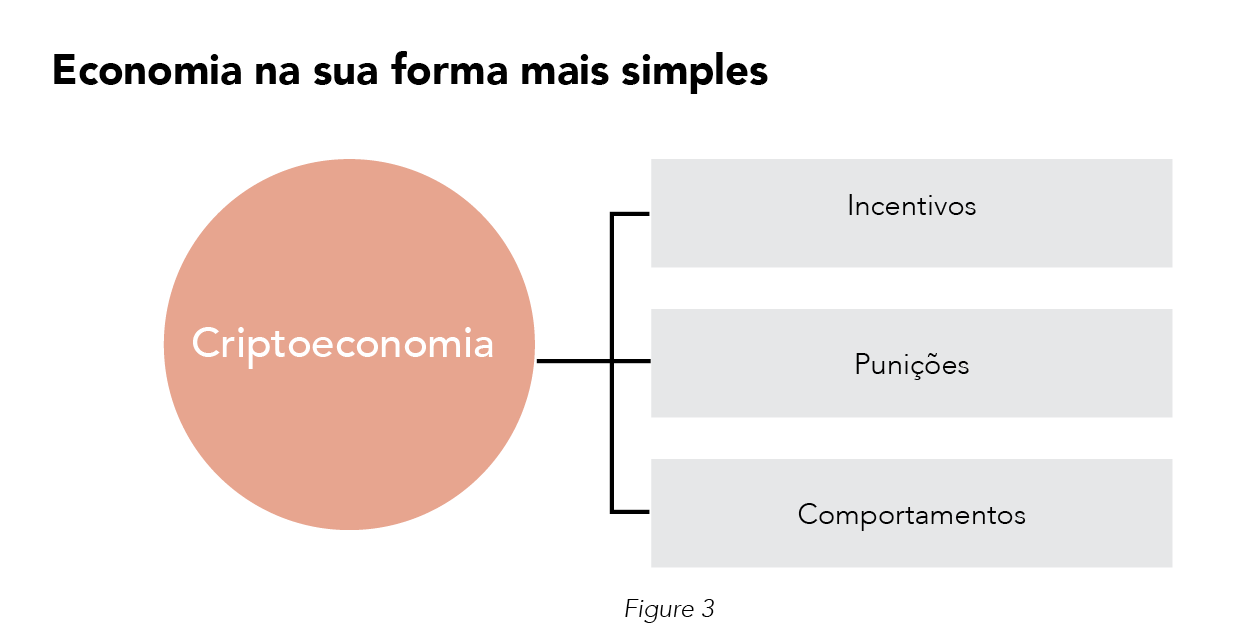


Figura 3

As duas principais escolas de pensamento são a Keynesiana[[9]](#footnote-10) e austríaca[[10]](#footnote-11). Por mais que discordem em muitas coisas, **concordam que Economia pode ser resumida nos incentivos que resultam em comportamentos desejados dentro do sistema.** Políticas econômicas tem o objetivo de intensificar incentivos e punições para guiar o comportamento racional (ou irracional) dos participantes do ecossistema.

#### Economias Baseadas em Tokens

Podemos aplicar esses mesmos princípios para economias baseadas em tokens. A principal diferença entre o mundo físico tradicional e o mundo descentralizado digital (isto é, economias baseadas em tokens) é o estado da economia. Agentes econômicos usam tokens para incentivar estratégias de utilidade, seja com incentivos financeiros (tokens fungíveis e alguns tipos de tokens não-fungíveis[[11]](#footnote-12)) ou incentivos não-financeiros. (outros tipos de tokens não-fungíveis).

Uma Nota Sobre Tokens Fungíveis vs. Não-Fungíveis (NFTs)

“Fungibilidade” é a característica de um item que pode ser mutuamente trocado por outro sem qualquer alteração de valor. “Não-fungibilidade” é a característica de um item único, e por isso não pode ser mutuamente trocado por nenhum outro.

Por exemplo, qualquer nota de R$100 (100 reais) pode ser mutuamente trocada por outra nota de R$100 sem alteração de valor – fungível. Já uma nota de R$100 autografada por Pelé (rei do futebol) é única, e não pode ser trocada por qualquer outra nota sem alteração de valor – ou seja, não-fungível.

Todos os tokens fungíveis dentro de um protocolo são iguais. Podem ser trocados por outro sem nenhuma alteração de valor (por exemplo, qualquer bitcoin pode ser trocado por outro sem problema algum). Tokens não-fungíveis são únicos e não podem ser trocados por outro, mesmo se fizerem parte de um mesmo padrão de token ou coleção (por exemplo, artes ou ativos digitais).

Um NFT pode representar um ativo no mundo físico, como uma pintura do Banksy, ou a posse de um ativo financeiro. NFTs são ferramentas que podem traduzir[[12]](#footnote-13) um ativo para o mundo digital. Eles contêm metadados, acordos e contratos inteligentes relacionados ao ativo que ficam armazenados na blockchain. Dado que uma pintura física do Banksy possui valor percebido, sua posse pode ser dividida em 100 partes idênticas (sub-tokens fungíveis referentes ao NFT da pintura) e co-detidos por 100 indivíduos diferentes. No future, esses sub-tokens fungíveis podem até serem utilizados como colateral, possibilitando os proprietários a adquirirem empréstimos com base no valor de mercado do ativo.

##### Circuito Aberto (Open-loop) vs. Circuito Fechado (Closed-Loop)

O mundo físico é geralmente regido por sistemas de circuito aberto. O sistema – isto é, a Economia – não é diretamente influenciado por seu “controlador” (feedback do estado, ou *state feedback*)[[13]](#footnote-14). Isso limita a habilidade de atualizar o sistema atual por parte dos reguladores, para que eventualmente pudessem incentivar ações desejáveis e otimizar a coordenação entre os agentes econômicos[[14]](#footnote-15).

Banco Central, por exemplo, altera a taxa de juros de acordo com o estado da Economia. Porém, ele não possui nenhum controle sobre a forma que a Economia reage de acordo com essas mudanças. Outro exemplo é o período de pandemia do COVID-19, e a alta inflação que se sucedeu e por último o risco de recessão em 2022. Existe um limite para o quanto o Banco Central consegue influenciar, estimular, estabilizar a economia, por meio da taxa de juros, políticas de reservas bancárias mínimas, e outras ferramentas discutidas no Capítulo 5.3. Mas, dada interconexão das mais diversas economias por conta da globalização, o poder de um único Banco Central tem impacto real limitado na Economia. Não é um sistema de circuito fechado, portanto influenciado por políticas econômicas de outros parceiros comerciais diretamente na sua Economia interna.

Por outro lado, o mundo digital descentralizado consiste em sistemas de circuito fechado, que pode ser dinamicamente definido de acordo com o feedback do sistema. Isso dá ao desenvolvedor (i.e. Designers Econômicos e Engenheiros de Software[[15]](#footnote-16)) a possibilidade de alcançar a estabilidade dos resultados e comportamentos desejados dentro do ambiente. Sistemas digitais descentralizados de circuito fechado são caracterizados por possibilitar novas formas para executar Governança, alinhar Incentivos, e atingir Estabilidade.

Por exemplo, moedas digitais de bancos centrais – as chamadas CBDCs, uma forma de dinheiro digital emitido por bancos centrais, pode introduzir mecanismos de incentivos mais criativos, como por exemplo taxas de juros negativas, moedas com data de validade, e muitos outros[[16]](#footnote-17). Esses mecanismos podem ajudar o engenheiro ou economista do token a incentivar certos comportamentos no sistema.

##### Função Primária de um Token

Um token é qualquer coisa que representa valor. Valor pode ser intrínseco[[17]](#footnote-18) ou extrínseco. Valor intrínseco é o valor de uso no mercado primário. Valor extrínseco é o valor de troca, geralmente exercido no mercado secundário. Ambos são importantes, e a chave para o balanceamento no design do token.

Existem dois tipos de tokens: tokens como uma ferramenta de coordenação para incentivar certas ações dos usuários do sistema e tokens como a representação de ativo(s) financeiros. O primeiro é tipicamente estruturado com utilidade para capturar o valor da atividade econômica, enquanto o segundo geralmente possui funções de títulos tokenizados (*security token*), com valor baseado no ativo real referente. Como tokens são uma nova classe de ativo, ainda não há regulamentação bem definida sobre essas classificações. Vale reforçar que discussões sobre design econômico não são conselhos sobre o que é melhor em termos jurídicos, mas discutir a estrutura do token.

A principal função do primeiro token introduzido é capturar o valor econômico gerado internamente no ecossistema, e não para ganhar valor no mercado secundário – ou seja, não existir apenas para ser negociado em corretoras (*exchanges*). Isso é possível pois ecossistemas digitais descentralizados podem ser baseados em plataformas com diversas frentes e gerar valor econômico. Tokens desse sistema capturam esse valor. Mercados secundários facilitam a descoberta de preço (*price discovery*) quando tokens são negociados – e capturam o valor gerado pelo token no longo prazo, descontado ao valor presente para chegar nos preços que vemos nas corretoras.

Dentro do ecossistema de um token, o objetivo central é agir como a principal mecânica de incentivo da rede. Cada ecossistema tem seu objetivo, e tokens incentivam participantes a atingirem esse objetivo em comum. Por isso, design e estrutura econômica de um token se torna um critério-chave para o sucesso dele[[18]](#footnote-19).

Por mais que esse livro seja sobre tokenização de valor criado, nem todos os ecossistemas necessitam de um token, e nem todo token precisa ser negociado no mercado secundário.

A principal função do segundo token é representar o valor econômico referente ao ativo real que ele representa. Isso está muito relacionado a estruturas de derivativos, títulos, engenharia financeira etc. Os fundamentos de um token como esse não seriam muito diferentes de como o sistema financeiro tradicional funciona.

##### Razões práticas para se criar um token

* Tokens podem ajudar a executar estratégias financeiras específicas. Designers de token tokenizam essas estratégias para representar valor acumulado.
* Tokens representam ativos reais. Designers de token tokenizam esse ativo real para que o ativo digital possa interagir com novas capacidades tecnológicas.
* Tokens criam auxílios em termos de contabilidade. Designers de token tokenizam meios de pagamento para fazer o balanceamento e atualização de contas de usuários a todo momento.
* Tokens ajudam com a distribuição. Designers de token distribuem ativos (lucros obtidos, dividendos, retornos acumulados) facilmente com tokens.
* Tokens alinham incentivos de vários agentes econômicos. Dinheiro pode até fazer isso, mas existem participantes demais nesse sistema. Um token específico de certo ecossistema pode, por outro lado, atingir esse alinhamento de incentivo.

### 10 Perguntas Frequentes Sobre a Economia da Construção de Tokens

Antes de nos aprofundarmos mais nos tópicos acima, vamos responder algumas perguntas frequentes sobre a Economia da Construção de Tokens (*Economics of Token Engineering*). Esclarecer essas dúvidas irá facilitar no entendimento do restante do livro.

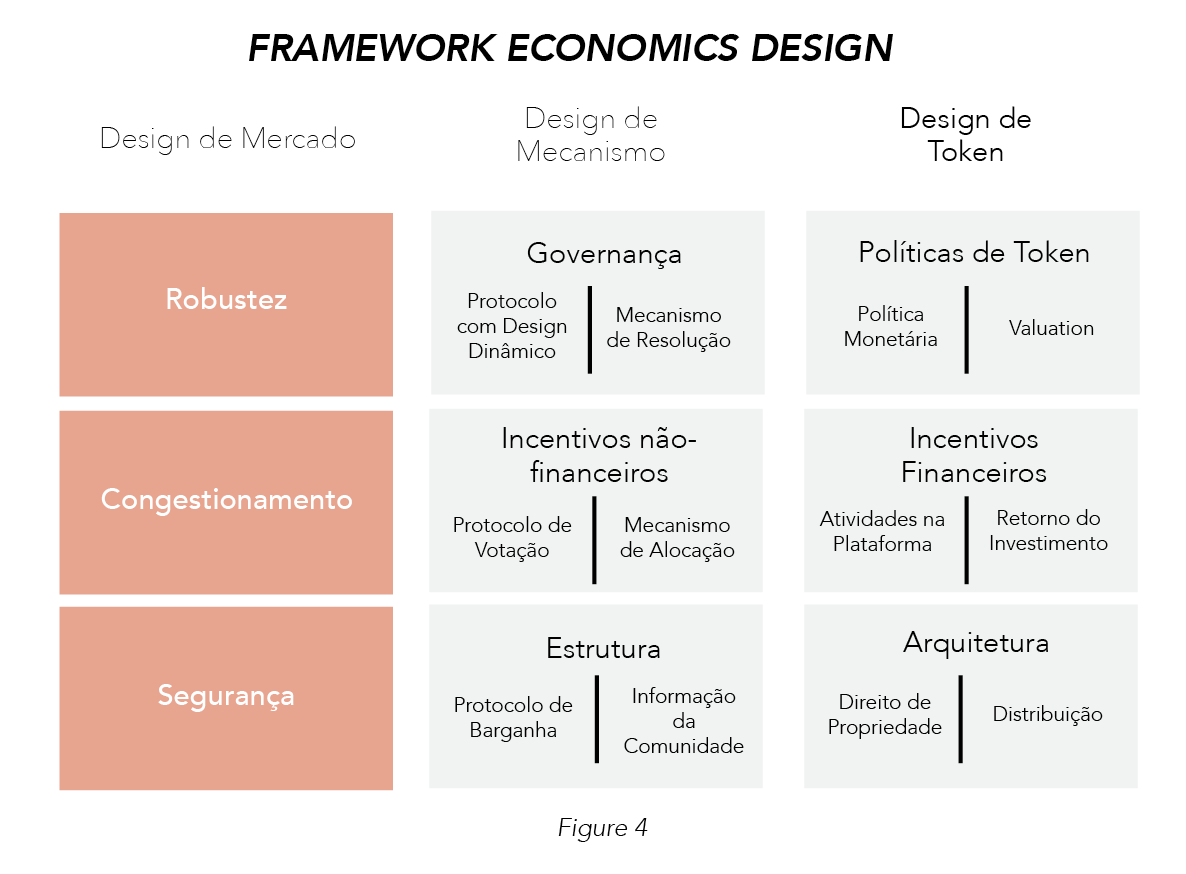
1. Qual é o Framework Economics DesignTM? 

Figura 4

O Framework Economics Design considera as variáveis acima na construção da economia de ecossistemas. Usamos esse framework quando executamos consultoria para outros projetos, e em pesquisas acadêmicas sobre protocolos existentes.

Design de mercado é o primeiro pilar no Framework Economics Design. O mercado é o ambiente em que negociações acontecem. Design de mercado define esse ambiente por meio da estrutura e design. Isso garante que usuários do ecossistema negociem dentro do próprio ambiente. Negociações, nesse contexto, pode significar movimentação de tokens ou dados.

Design de mecanismo é o segundo pilar. Design de mecanismo desenvolve as regras que os participantes devem seguir no mercado, incluindo governança, incentivos não-financeiros, e estruturas para atualizar essas regras conforme necessário.

Design de token é o terceiro, e último pilar. Design de token determina as regras específicas do token em si. Essas regras podem ser definidas por meio de códigos em contratos inteligentes. Pode mudar conforme o sistema se desenvolve e integra novas formas de transacionar.

1. O que tokens fazem?

Tokens representam valor. Há muitas formas de categorizá-los. Por exemplo, podemos categorizar por **tipo de token**: tokens fungíveis e não-fungíveis.

Outra forma de categorizar tokens é por sua função. Existem quatro funções principais de tokens – **SUMS. S**egurança, **U**tilidade, Dinheiro (***M****oney*), e Estabilidade (***S****tability*).



Figura 5

Existem outras formas de definir funções específicas de token, principalmente em termos legais. Regulamentação e legislação podem ditar até o que tokens podem ou não fazer. Porém, isso está for a do escopo dessa discussão. A tabela acima explora uma análise geral das funções que um token pode ter.

Títulos Tokenizados (***S****ecurity Token*)

Títulos tokenizados representam ativos reais. A classificação de token de “garantidor” – ou *security* – é tradicionalmente determinado por meio do Howey Test[[19]](#footnote-20) (referenciar Glossário), mas uma regra básica é que se um token digital representa o valor de um ativo real, e a razão primária de sua emissão é a especulação de ganhos futuros, muito provavelmente é uma *security*. Pode ser uma ação tokenizada, que representa o *equity* em uma empresa; ou pode ser um imóvel tokenizado, representando a posse total ou parcial da propriedade. A parte interessante é que você pode negociá-lo!

Token de Utilidade (***U****tility Token*)

Tokens de utilidade são usados para **acessar plataformas digitais ou redes.** Isso é análogo às fichas que usávamos nos antigos Arcades para jogar fliperamas e outros videogames, ou milhas de companhias aéreas que dão acesso à hotéis, aluguéis de carros, e descontos em passagens. Tokens de utilidade dão acesso à plataforma (Arcade) ou rede (companhia aérea e parceiros). Detentores do token (*holders*) o utilizam para interagir com os outros em um ecossistema digital.

Dinheiro (***M****oney*)

Dinheiro é **moeda**, e é quase universalmente aceito em troca de produtos e serviços. É um ativo líquido, usado pela maioria das pessoas para realizar pagamentos.

Dinheiro tem três principais propósitos: reserva de valor, unidade de medida, e meio de troca (ou pagamento). Pense no USD (dólar), GBP (libra), ou EUR (euro). Dinheiro também possui subcategorias:

* Moeda física corrente (*Fiat*) emitida pelo Banco Central do país.
* Dinheiro digital[[20]](#footnote-21): criptomoedas como o bitcoin[[21]](#footnote-22), dinheiro virtual como “ouro” no World of Warcraft, e até mesmo CBDCs.

Estabilidade (***S****tability*)

Alguns tokens têm elementos de *security*, utilidade, e moeda corrente, mas seu principal propósito é garantir a estabilidade contra volatilidade externa – as chamadas *Stablecoins*. Elas são estáveis pois são atreladas a outro ativo que é estável (geralmente moedas como dólar). A ideia é que o valor não flutue **relativo ao valor do ativo que a stablecoin está atrelada**.

1. O que é Consenso, Alocação e Resolução?

**Consenso**

Consenso é a tomada de decisão geral que depende da aprovação do grupo.

ELI5[[22]](#footnote-23): Nós cinco concordamos em comer sushi no jantar.

**Resolução**

Resolução compreende várias formas de governança de DeFi, como contratos inteligentes e contingências manuais para resolver problemas não endereçados pelos contratos inteligentes.

ELI5: Nós cinco concordamos em comer pizza porque o restaurante japonês estava fechado.

**Alocação**

Alocação descreve como ativos são distribuídos para usuários por meio de mercados de leilão, votação, mecanismos de preço, distribuição de renda e como o acesso à recursos de produção afetam distribuição dessa renda, retornos e participação no sistema, e várias formas de direito de propriedade.

1. Qual é a diferença entre Valuation e Precificação de Tokens?

**Valuation**

Valuation é o valor econômico objetivo. Geralmente é utilizado no contexto de um ecossistema. Um exemplo do mundo real é o cálculo baseado nos custos (i.e. quanto você de fato pagou) para definir o valor de uma conta de energia – como R$100 – no contexto atual da economia que você está vivendo.

No contexto de design econômico de tokens, isso refere-se à de onde tokens derivam seu valor, que holisticamente considera uma variedade de fatores do ecossistema. Valuation pode considerar o valor capturado por meio de taxas, arbitragem em um mercado de derivativos, e outros métodos criativos.

ELI5: O casaco que a minha avó teceu tem um valor inestimável para mim.

ELI-finanças: O valor de uma opção considera muitas outras variáveis, como a volatilidade, tempo de maturidade e métricas históricas.

**Precificação**

Preço é o montante a se pagar em uma transação. Precificação inclui incentivos e desincentivos como reembolsos, crédito, e cupons. No exemplo da conta de energia, após incentivos de reembolso e cupons, o preço da conta poderia cair para R$83. O **valor** era R$100, mas o **preço** real é R$83.

No contexto de preço, o montante é determinado por meio do descobrimento de preço no mercado secundário. Esse é o preço que as pessoas estão dispostas a pagar em troca do token.

ELI5: O casaco que a minha avó teceu tem um preço de R$30 se eu vender para outra pessoa.

ELI-finanças: O preço da opção é o que o mercado está disposto a pagar por ela, geralmente considerando o valuation da opção com base no modelo de Black-Scholes.

1. Onde entra a “mineração de liquidez” ou “*yield farming*” no Framework Economics Design?

Mineração de liquidez e *yield farming* são usados mutuamente para dizer o mesmo. São mecanismos de incentivo para encorajar participação por meio de recompensas na forma de tokens nativos para usuários. Esses mecanismos são criados durante o processo de design do token.

Mineração de liquidez e *yield farming* se entram na caixa de Incentivos Financeiros no Framework Economics Design. Mineração de recompensas de liquidez em protocolos da Camada de Aplicação são tokens nativos emitidos pelo protocolo quando transações são feitas (ex: $UNI emitido para usuários da Uniswap). Mineração de liquidez em protocolos de Camadas 1 recompensam validadores com tokens do ecossistema (ex: $BTC emitido para validadores do Bitcoin).

Tudo que tem relacionado a tokens e seu valor monetário entra na parte de design do token. Design de mercado e mecanismos não endereçam os aspectos monetários do token.

1. Onde entra “teoria dos jogos” no Framework Economics Design?

Design de mecanismo define as regras do sistema. Teoria dos jogos é a análise das ações baseadas nas regras, e por isso entra na coluna de design de mecanismo.

Teoria dos jogos analisa *como* as pessoas se comportam no sistema. As regras criadas para o token e seu design de mecanismo são as variáveis cruciais para entender como será o comportamento em resposta às regras.

Por exemplo, o aumento do requerimento de capital mínimo (MCR) do Nexus Mutual é parte do mecanismo e design do token. O estudo sobre como usuários reagem a esse aumento é parte da análise da teoria dos jogos.

1. Que políticas monetárias devo usar quando estiver definindo o design do ecossistema do meu token?

A seleção de políticas monetárias depende no caso de uso do token, função, e modelo de negócios.

Exemplos:

1. Se o seu token é uma **moeda para facilitar transações** dentro do ecossistema, teoria monetária econômica tradicional irá te ajudar a entender as considerações importantes e implementações de políticas para seu token. Um ótimo lugar para começar seria pesquisar sobre “instrumentos de política monetária” relacionados à forma que o dinheiro é governado.
2. Se o seu token é uma **moeda** que é **muito vulnerável a forças externas** (ex: stablecoins estão sujeitas ao câmbio entre o token em si e o ativo referente, como o dólar) você deveria estudar tipos de políticas monetárias que bancos centrais usam para governar a moeda.
3. Se o seu token representa **a posse sobre certos ativos** dentro ou for a da blockchain, estude *bonding curves* que definem o preço do token como função do *supply.* Isso requer alguns novos conceitos na economia monetária como a proporção de reservas e considera o impacto da inflação.
4. Se o seu token tem como **utilidade o acesso à rede,** políticas monetárias vão depender no caso de uso e propósito. Por exemplo, se funcionar como programa de milhas de companhias aéreas, políticas monetárias tem pouca relevância; talvez medidas deflacionárias sejam ocasionalmente necessárias.

Em qualquer um dos casos, uma inflação de três porcento[[23]](#footnote-24) é geralmente tida como ideal pelos bancos centrais. Na economia de tokens, porém, não é necessário se limitar a isso.

1. O modelo econômico[[24]](#footnote-25) de MV=PQ[[25]](#footnote-26) (i.e. Teoria Quantitativa da Moeda) é bom o suficiente para definir o valuation do meu token?

Resposta curta: Não necessariamente.

1. pretende determinar o preço da moeda.

Seu token pode não ter a função de “moeda”. Usar para tokens que não são moeda é como usar uma faca de manteiga para cortar uma carne; é ineficiente. Enquanto é apropriado para análise de tokens de moeda, não é universalmente útil para valuation de todo tipo de token.

é usado para encontrar a velocidade da moeda[[26]](#footnote-27), que é um sinal do valor da mesma. Definir o V (velocidade) na equação, porém, não nos permite encontrar as demais variáveis na fórmula.

1. O modelo foca nas variáveis exógenas (externas).

Ecossistemas com tokens possibilitam a inclusão no design de muitas variáveis endógenas (internas), mas a maioria falha no design das variáveis externas. Por isso, o valor do token deve ser definido com relação às variáveis endógenas, não exógenas. Isso é uma **forma diferente de ecossistemas TradFi** (mercado financeiro tradicional). Ecossistemas com tokens tem mais controle sobre o resultado (*output*) dadas as entradas (*inputs*) em comparação ao TradFi[[27]](#footnote-28). E isso faz com que seja um método ineficiente para o valuation de muitos tokens.

1. Quais são alguns conceitos econômicos fundamentais na economia de token?

Conceitos da teoria do ajuste, teoria de leilões, economia monetária, economia de rede, teoria do principal-agente, e teoria dos jogos podem ajudar a construir incentivos melhores e mais fortes para os participantes. Esses modelos podem produzir resultados estáveis e robustos, melhorar alocações ineficientes e transações dentro do ecossistema.

1. Por que governança é tão importante na economia de token?

O governo se reúne para tomar decisões políticas em nosso país. Isso acontece pois, por mais que os países existam há séculos, políticas do passado podem não ser relevantes para a economia de hoje. Por isso, o governo se reúne para fazer alterações nas regras (mecanismos, leis) da sociedade. Economias baseadas em token não são diferentes! Funcionam como um país, onde os mecanismos regentes iniciais podem não ser relevantes conforme a economia muda.

Em um ecossistema descentralizado, governança é uma consideração crucial no design do mecanismo.

Governança ajuda na organização de transações no ecossistema por meio de mecanismos endógenos, tornando segura a participação e prevenindo atritos quando problemas aparecerem. Isso pode se dar em várias formas, incluindo legislação e design de contratos inteligentes.

Governança pode limitar o ecossistema em diversas formas, dependendo da função do token, no caso de uso, e seus objetivos.

Certos mecanismos de governança podem causar uma maior centralização, como contratos inteligentes inflexíveis[[28]](#footnote-29), e leis nas várias jurisdições em que o protocolo atua. Mas governança não deveria ser limitada apenas a contratos inteligentes. Pode incluir também outros mecanismos de resolução, protocolos de consenso, e outras camadas de governança. Uma governança bem-pensada pode equilibrar os prós e contras entre centralização e descentralização, para possibilitar tomadas de decisão sem concentração de poder na principal entidade.

### Conclusão

Economia de token é o novo campo na economia que estuda os mecanismos de incentivo e design de ecossistemas baseados em token. Pode ser definido conforme o framework geral usado para o design de incentivo.

Um token representa o valor **intrínseco** de seu ecossistema. Quando é negociado em mercados secundários, passa pela fase de descobrimento de preço para determinar seu valor **extrínseco**. O objetivo da economia de token é definir, elaborar o design, e construir o valor intrínseco.

Por mais que seja possível utilizar o Framework Economics Design em protocolos de Camadas 1 e 2, focamos seu uso principalmente para a Camada de Aplicação. Design econômico de tokens foca no ambiente e as regras pelas quais agentes econômicos, tokens, e instituições estarão sujeitos.

## Evolução da Economia

### Economia definida de forma simples

Economia é uma ciência. Examina principalmente como decisões são tomadas e quais alternativas oferecem os melhores benefícios para cada participante. Economia é, e sempre foi, o estudo da alocação de recursos escassos (comportamentos).

Uma das principais diferenças na economia de tokens é a criação de regras para alocação de recursos escassos para influenciar no comportamento dos agentes. Podemos forçar essas regras por meio de incentivos e desincentivos (punições).

### Fatores de Produção

Os quatro fatores econômicos de produção são trabalho, capital, recursos naturais, e empreendedorismo. Esses são ativos *tangíveis* (até mesmo empreendedorismo).

Um novo fator surgiu com o advento da economia digital: informação/dados. Informação é um ativo *intangível*.

#### Novo Fator: Informação, o ativo intangível

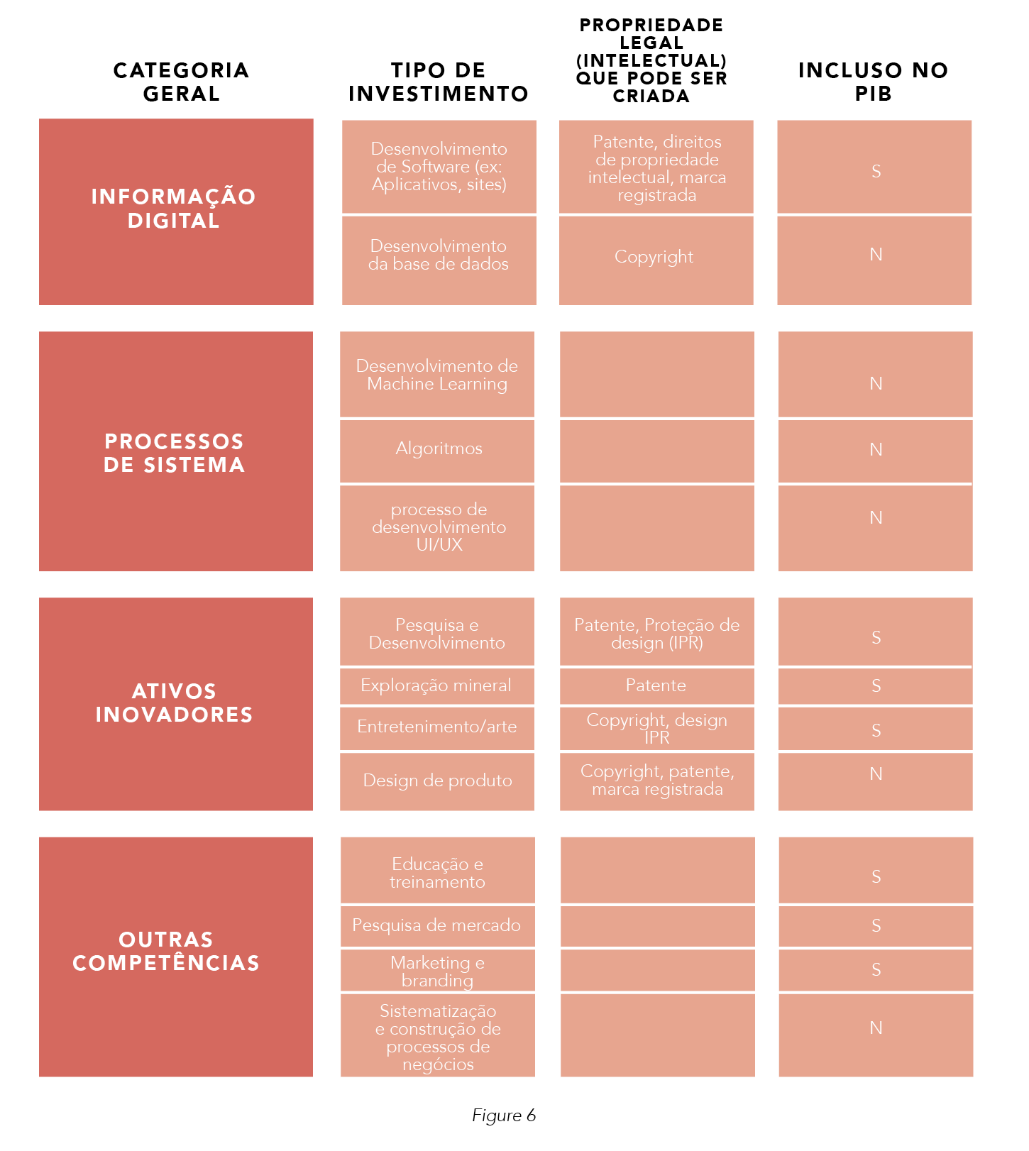


Figura 6

Essas são propriedade e características a se considerar quando ao nos aprofundarmos e explorarmos essa nova variável na economia.



Figura 7

#### Evolução dos Mercados

##### Mercado econômico clássico

No mercado econômico clássico, construímos o modelo baseado na oferta e demanda para entender como o mercado se comporta. Determinação da oferta e demanda é feita de forma independente em modelos clássicos. O custo afeta o preço, que afeta a predisposição à venda do fornecedor. Consumidores são afetados pelo preço, e pela demanda em qualquer nível de preço. Oferta não determina a demanda, nem a demanda determina a oferta. São variáveis relativamente independentes – “lei da oferta e procura” é um termo errôneo, visto que são leis separadas: lei da oferta e lei da procura (demanda).

##### Mercado de informação

Em mercados de informação, as coisas funcionam de uma forma diferente. Agentes econômicos têm outras formas de sinalizar e entender como os mercados se comportam, como por exemplo analisar as propriedades dos bens públicos, externalidades, monopólios e intervenções governamentais.

Além disso, conforme mercados de informação se desenvolvem para economias de rede (*network economy*), oferta e demanda se tornam independentes. Demanda por um ativo existe por causa da oferta existente, não apenas por causa do preço desse ativo. Isso se dá pois, em uma economia de mercados multifacetados, o mercado em si fornece apenas informações sobre a curva de oferta e de demanda.

**Mercados multifacetados como mercados de informação**

Como simples exemplo, temos aplicativos de transporte. Por mais que a Uber não seja dona de nenhum carro, possui as informações de alguém procurando uma carona e de quem está disponível para provê-la. Eles dividem essa informação com usuários nesse mercado (clientes e motoristas) e fazem a correspondência da demanda com a oferta.

**Mercados unilaterais como mercados de informação**

Economias de mercado não são dependentes de mercados que não controlam os ativos (como no exemplo do Uber). A economia também existe para mercados em que a oferta é centralizada. Vamos olhar a Netflix, por exemplo.

Imagine que um novo filme exclusivo da Netflix é lançado. Demanda pelo filme existe **simplesmente porque** a oferta (o filme) existe. Estatisticamente, antes disso acontecer e ver a obra listada na categoria de “Novos Lançamentos”, ninguém estava clamando por um novo filme a ser lançado na Netflix. Mesmo assim, você quis assistir a partir do momento em que o filme foi disponibilizado na plataforma. Netflix[[29]](#footnote-30) agrega e fornece o conteúdo para **criar a demanda** em categorias diferentes de filmes e séries.

Dentro da plataforma da Netflix, consumo de uma série específica (demanda) é inextricavelmente ligado à disponibilidade (oferta). Essas plataformas jogam o jogo com novas regras:

* Acesso restrito: assinaturas diferentes determinam a qualidade do *streaming*.
* Congestão reduzida: aprendizado de máquina (*machine learning)* prevê os tipos de filme mais adequados para cada base de usuários de acordo com o histórico e recomenda os filmes mais apropriados, reduzindo o atrito do processo de busca.
* Forma massa crítica e subsidia crescimento da base de usuários: possibilita que vários usuários acessem a mesma conta e são menos rigorosas com políticas de contas compartilhadas.
* Forçam regras para punir comportamentos indesejados: Gravação de tela não é permitido no aplicativo da Netflix.
* Lucram por meio da interdependência da oferta e demanda: Netflix ajuda pessoas a encontrarem o melhor filme para assistir, baseado no perfil de consumo de cada um. Ao te ajudar a reduzir o tempo de procura por um novo filme que você gostaria, a empresa lucra – por meio dessa pequena troca.

Isso irá mudar a forma que economia básica é ensinada nas escolas. Esse novo modelo de negócios traz uma mudança de paradigma econômico com uma estrutura econômica totalmente nova.

###### Informação como bem público

Informação é diferente de bens físicos em vários aspectos. Informação pode ser consumida por duas ou mais pessoas ao mesmo tempo, e eles não são competidores nesse consumo. Isso significa que não existe escassez natural quando falamos de consumo.

Por exemplo, você pode ler um artigo no Wall Street Journal enquanto outra pessoa faz o mesmo simultaneamente. Caso você vá para uma livraria, porém, e deseja ler o jornal do dia, você terá que aguardar a outra pessoa terminar a leitura para então fazê-la.

Por causa dessa natureza “não-competitiva”, torna-se difícil estimar a demanda por bens de informação. Mas também não é impossível. Podemos estimar a demanda usando proxies de dados agregados.

Wall Street Journal, por exemplo, pode monitorar quantas pessoas estão acessando uma página em seu site para entender a demanda por um assunto específico abordado por uma matéria. WSJ pode também usar outros proxies de referência, como os tópicos em alta no Twitter, Google, ou Facebook. Isso pode ser usado como estimativa da demanda por tópicos específicos.

Exemplos de mercados de informação: seguros, educação, mercado de casamentos.

#### Diferenças entre Ativos Tangíveis e Ativos Intangíveis da Web3

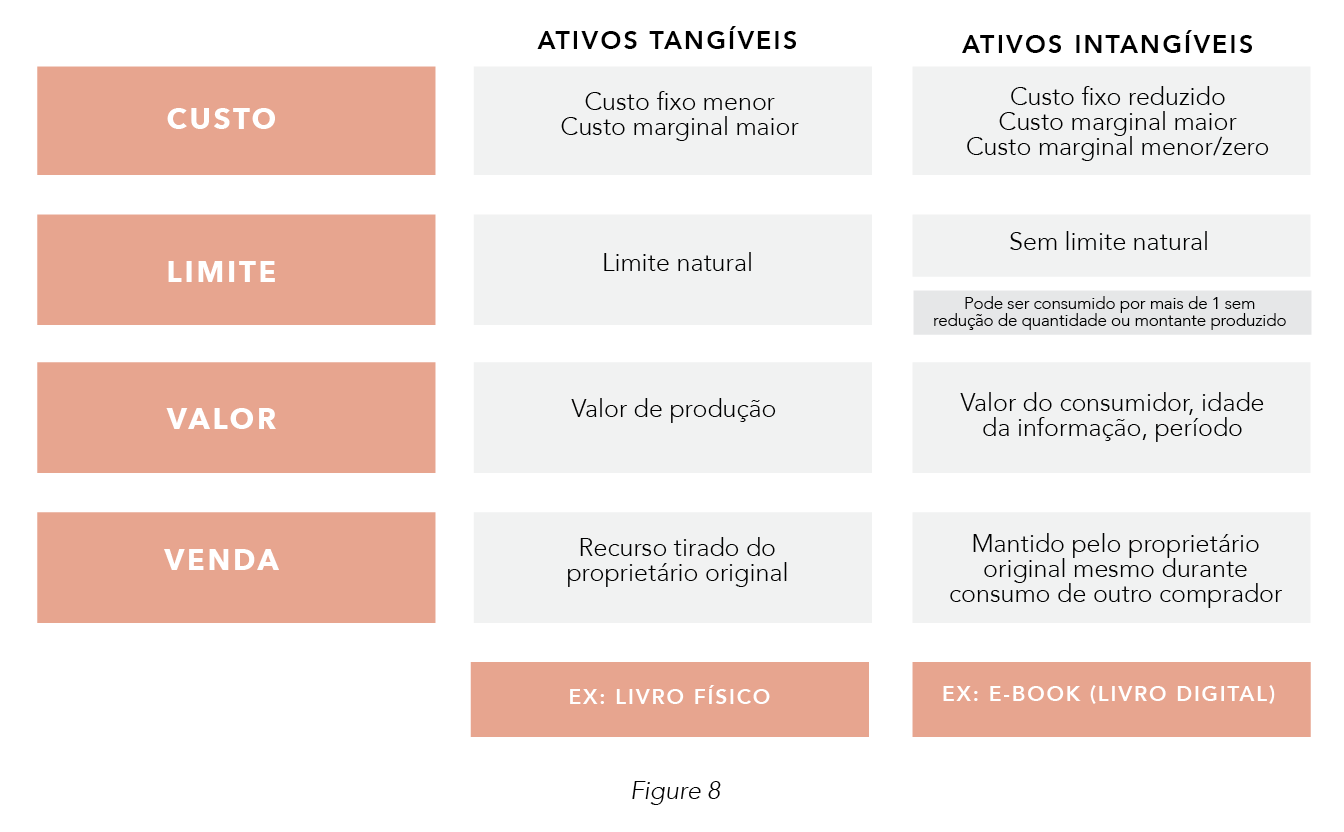


Figura 8

##### Características de recursos intangíveis da Web3

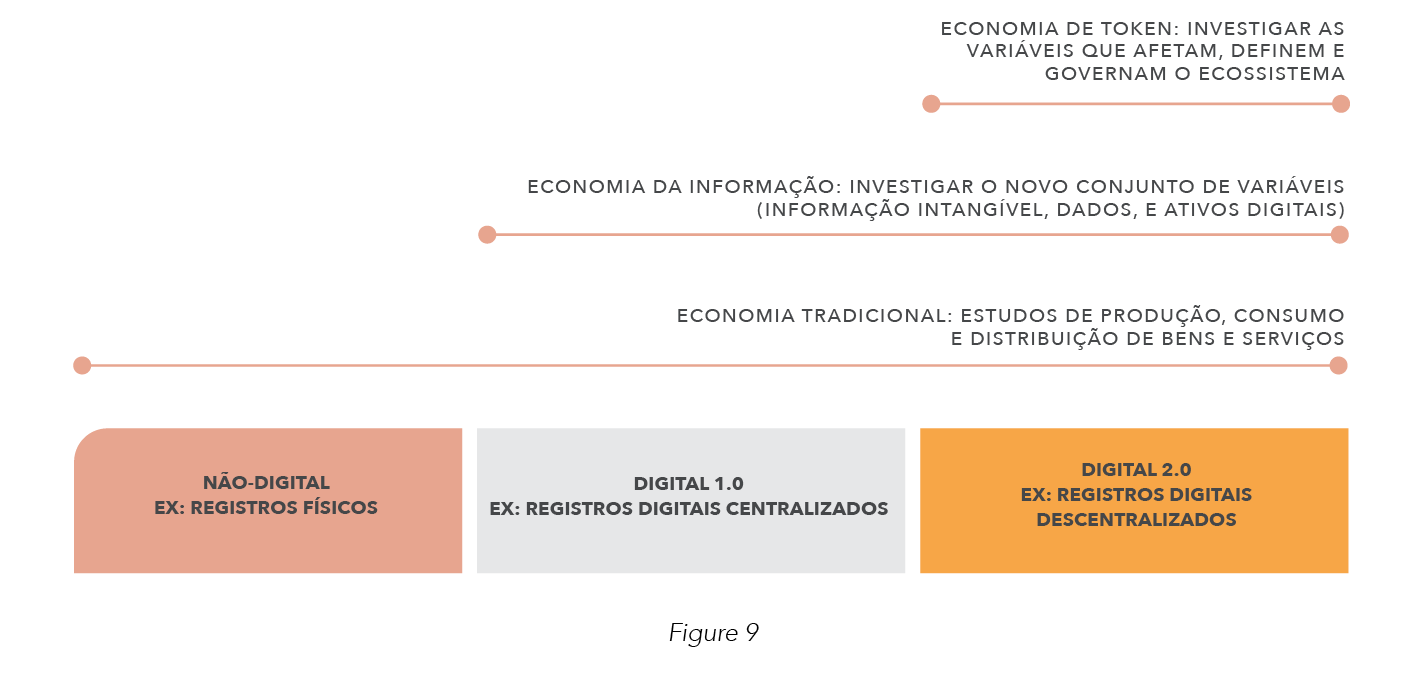
Para recursos intangíveis como informação, dados e protocolos *open-source*, há um alto custo fixo para se produzir a primeira unidade e baixo custo marginal para qualquer unidade adicional. Provavelmente, veremos num futuro próximo um custo marginal zero para produção dessas novas unidades. Atividades de custo marginal zero que existem hoje são executar um *fork* em um protocolo open-source na blockchain, ou copiar e colar as anotações de seu colega de classe da faculdade.

Por conta dessa nova estrutura de recursos, basicamente não existe limite na quantidade de ativos intangíveis ofertados ou produzidos na Web3. Podem ser consumidos por mais de uma pessoa, sem a redução da quantidade disponível. Além disso, mercados de informação interconectados se traduzem em mais consumidores engajando com o mercado (*network effects*) e consequentemente maior valor entregue a cada cliente. Esse benefício pode até ser tokenizado.

Valor de recursos intangíveis é interpretado de outra forma. Não é mais baseado nos custos de produção. O valor da informação depende do momento de venda, da idade da informação, e do benefício para o consumidor.

Quando a informação é vendida, o vendedor continua em posse da mesma. Por exemplo, o fato de te vender esse livro não apaga do meu cérebro as informações aqui contidas, nem a versão digital que possuo no meu computador. Por outro lado, informação pode ser comprada mas não facilmente devolvida. As informações contidas nesse livro são suas quando você as consome, e não há como eu pegar de volta ou você mesmo me devolver.

### Economia e a Evolução Tecnológica

**

*Figura 9*

#### Passado: Economia Tradicional

Economia tradicional[[30]](#footnote-31) estuda a produção, distribuição e consumo de bens e serviços. Analisa o equilíbrio e determina quando deve parar de produzir novos itens para não diminuir os retornos. Economia tradicional calcula o custo de produção de um item em comparação com a receita gerada por ele. Produção é interrompida quando o custo marginal é igual à receita marginal.

Caso o custo marginal seja maior que a receita marginal, isso cria um cenário de prejuízo – o que geralmente[[31]](#footnote-32) é ruim. Ao produzir um hambúrguer, por exemplo, caso o custo marginal seja R$10 e a receita marginal gerada por vendê-lo também seja R$10, não há porque continuar produzindo.

#### Presente: Economia da Informação

A evolução atual da economia (economia da informação) estuda como informação, sistemas de informação e dados afetam a economia e eventuais decisões econômicas. Custo da informação possui uma nova estrutura; é caro de produzir, mas barato de *re*produzir.

Pegue esse livro como exemplo: um projeto de mais de três anos, e que foi muito custoso para produzir. Porém, precisamos apenas imprimir mais uma unidade ou duplicar a versão digital para reproduzi-lo.

Consequentemente, precificação com base no custo não é mais eficiente. Economia da informação determina o preço de acordo com o valor para o consumidor, não apenas o custo de produção. Precificação de valor é dependente do valor da rede, externalidades, e parcerias.

#### Futuro: Economia Digital Descentralizada

Economias digitais descentralizadas são o futuro. Economia digital descentralizada estuda os fatores que afetam, definem e governam ecossistemas digitais descentralizados. Conforme os mercados se movem em direção à descentralização e digitalização, economia da informação, e propriedade intelectual (ideias, conhecimento, pesquisa, protocolos *open-source*, algoritmos, dados etc.), estão mudando a forma que a economia funciona.

A economia da informação irá continuar crescendo e florescendo. Economias digitais descentralizadas **não estão** **substituindo** a economia da informação, mas introduzindo uma nova forma de interação com ela. Com ambientes digitais migrando para ecossistemas descentralizados, novos desafios, variáveis e problemas surgem, resultando em economias digitais descentralizadas.

Um dos principais desafios é a coordenação de ecossistemas descentralizados. Todos têm incentivos, objetivos e preferências diferentes, o que torna a coordenação muito difícil. Como podemos alinhá-los? Como podemos coordenar acordos entre organizações desse tipo? Economia e tokens podem solucionar esses problemas.

Tecnologia mudou a **forma** que princípios econômicos são aplicados. A boa notícia é que princípios econômicos fundamentais **não mudam**.

### Tabela de Resumo



Figura 10

## Coordenação e Incentivos

Em mercados livres, empresas facilitam e diminuem custos de coordenação entre compradores e vendedores. Sem empresas, indivíduos precisam:

1. Descobrir preços de mercado
2. Negociar contratos para qualquer transação
3. Determinar a confiança de compradores e vendedores

O que faz um ecossistema ser bom? Coordenação, visto que mais coordenação significa maior eficiência.

Empresas e indivíduos podem operar em mercados livres. Isso funciona bem quando os incentivos estão alinhados entre todos os participantes (empresas e indivíduos). Quando incentivos estão desalinhados, o governo impõe novas regulamentações. Lei Dodd-Frank, por exemplo, é uma lei que foi criada após a crise de 2008. Essa regulamentação tem o objetivo de impedir empresas de financiamento (hipoteca) e credores de tirarem vantagem dos consumidores. Isso é relevante no mundo centralizado. No mundo descentralizado, coordenar essas normas de regulamentação é muito desafiador.

Ao invés de regulamentações, normas podem auxiliar comunidades de DeFi a aliviarem a dificuldade de coordenação entre os diversos agentes econômicos. Por outro lado, a auto coordenação pode ser custosa em termos de tempo e custo de oportunidade.

### Evolução Geral da Coordenação

Passado

Indivíduos viviam suas vidas em **comunidades pequenas e fechadas**.

Impulsos morais, exclusão social, fofoca e empatia eram os incentivos/punições primárias para indivíduos em conformidade com o bem comum. Essas comunidades fechadas se tornaram um **registro informal de contabilidade e confiança**.

Comportamento individual era também controlado de diversas maneiras por meio da governança da comunidade. Isso geralmente se manifestava como normas culturais ou religiosas.

Presente

Comunidades fechadas foram desfeitas conforme a **escala e escopo do comércio se expandiu** para além das cidades e registros informais de contabilidade e confiança. 0

Produção em massa gerou preços mais baixos. Bilhões de pessoas consomem bens produzidos em massa. É difícil, ou impraticável, boicotar produtos produzidos em massa que perpetuam práticas antiéticas ou imorais. Seria difícil, ou impossível, coordenar comunidades fechadas manualmente. Ao invés disso, comerciantes negociam produtos com desconhecidos localizados do outro lado do mundo. O registro informal de contabilidade e confiança evoluiu para **contratos e regulamentações formais/legais**. O governo apoia o comércio e protege as comunidades contra abusos por meio das leis de comércio.

A economia de mercado moderna gera significativamente mais valor do que a economia antiga (moral). Economias morais têm a vantagem de poderem punir e recompensar ações individuais que afetam o resto da comunidade. Mercados modernos geralmente não têm esse poder. Porém, economias morais não conseguem incluir participantes que estão em outras localizações (fora da jurisdição local).  
  
Em comparação com as tentativas de coordenação em massa dos sistemas acima, coordenação é uma questão central para ecossistemas e mercados da Web3, e boicotar empresas e organizações inadequadas será cada vez mais fácil com essas novas ferramentas.

#### Economia Moral e Economia de Token

Governança tem o objetivo de impor e administrar economias morais por meio de regulamentações e incentivos. Porém, sua aplicação é complicada em grandes populações e nunca a opção mais eficiente em comunidades pequenas e fechadas. Como então podemos melhorar a economia moral em ecossistemas de token? Podemos fazer isso por meio de design de mecanismos?

Duas soluções possíveis:

1. Adicionar uma camada de identidade do participante, como reputação, para garantir que existe um impacto de suas ações no longo prazo. Por exemplo, uma ação indesejada que afeta o ecossistema será punida por um bom tempo.
2. Criar uma definição universal de ‘reputação’ e estabelecer uma estrutura de referência para conhecer ou confiar em alguém sem realmente conhecer o indivíduo. Por outro lado, podemos limitar a motivação intrínseca de ações individuais quando começamos a comoditizar todas as atividades, incluindo as desejáveis. Por exemplo, um indivíduo pode contratar alguém para fazer boas ações em seu lugar para melhorar sua reputação.

### Coordenação a Nível de Mercado

**Permuta: C2C, consumidor para consumidor**

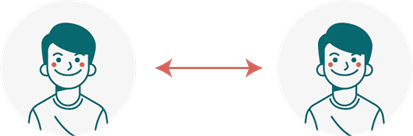


Figura 11

Essa era a forma de comércio mais comum nas comunidades pré-moeda (antes do dinheiro como conhecemos hoje ser inventado) – conforme tópico 3.1, um sistema de comércio. Membros da comunidade confiavam um no outro em comunidades fechadas e coordenavam entre si as negociações (ex: maçãs no verão por vegetais no inverno).

**Grandes corporações: B2C, empresa para consumidor (Walmart, Pão de Açúcar, Extra)**

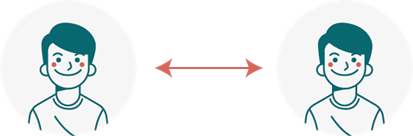


Figura 12

Coordenação em modelos B2C é mais difícil de implementar pois (1) o comércio com desconhecidos requer custos com KYC (conheça seu cliente) e (2) produção em massa é mais eficiente por conta das economias de escala. Isso beneficia grandes corporações pois elas são mais eficientes na coordenação de muitos participantes.

**Plataformas: C2C, consumidor para consumidor (Marketplaces centralizados)**

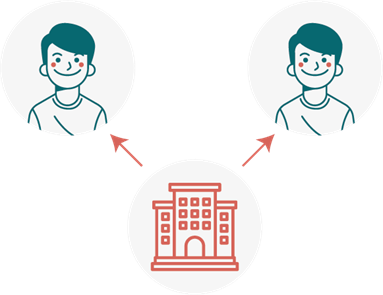
****

Figura 13

Muitos comerciantes desenvolvem produtos de nicho para vender aos consumidores por meio de plataformas como Amazon, Mercado Livre, Alibaba, ou Etsy. Esse modelo de plataforma pode ser entendido como um híbrido C2C (consumidor para consumidor) e B2C (empresa para consumidor), em que marketplaces centralizados coordenam o fluxo de movimento e informações dos indivíduos, produtos e serviços.

**Tecnologia de registro distribuído (*Distributed* *ledger*): C2C, P2P**

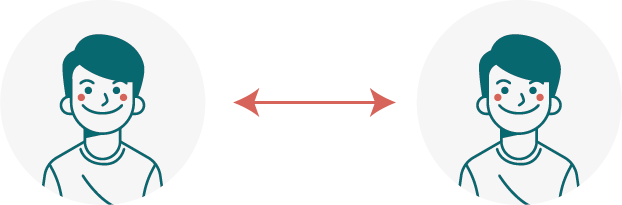


Figura 14

No início do modelo C2C, indivíduos precisavam confiar em todos os envolvidos no negócio para seguir em frente. Com o modelo de plataforma, participantes precisam confiar apenas nela, o que se mostra muito mais conveniente para o cliente dado que fazem todo o trabalho de coordenação de informação e intermediação. Facilita também pois consumidores precisam confiar em um número reduzido de agentes (plataformas) ao invés de cada indivíduo presente no ecossistema.

E podemos ir além. O que podemos fazer se não confiamos na Meta (antigo Facebook) por causa de seus algoritmos que utilizam nossos dados para recomendar conteúdo específico e problemas de privacidade (ex: vazamento de dados Cambridge Analytica[[32]](#footnote-33)), ou se não confiamos na Amazon (foram acusados de roubarem ideias[[33]](#footnote-34)), mas ainda assim queremos nos beneficiar da coordenação e conveniência das plataformas e ecossistemas? Introduzimos a descentralização, que possibilita coordenação C2C eficiente em uma plataforma confiável sem a necessidade de grandes corporações centralizadas.

### Cooperação

A grande questão é: se conseguimos coordenar as atividades, como garantir que as pessoas irão cooperar?

Pessoas não cooperam entre si naturalmente, a não ser que exista um incentivo para tal. É nesse ponto que a Teoria dos Jogos se torna crucial (consultar Cáp: 6 ).

Primeiramente, como facilitamos cooperação? Idealmente por meio de escolhas genuínas dos participantes da economia.

*Exemplos onde a cooperação existe em ecossistema de tokens: oráculos em protocolos descentralizados de aposta, acordo de consenso, votação, e tomada de decisão.*

#### Compatibilidade de Incentivos

Agentes econômicos podem incentivar pessoas a revelarem suas preferências de consumo por meio de:

1. Garantir que ser honesto é consistente com premissas racionais e inteligentes. Por exemplo, usuários cooperam e concordam em aumentar certas taxas de protocolo pois é uma boa opção alinhada com o propósito do ecossistema.

*Caso em questão: Holders do token $MKR, da MakerDao concordam em aumentar a taxa de estabilidade (stability fee) para manter a paridade (peg) com o dólar (USD).*

1. Oferecer incentivos corretos para revelar preferências e tipos de consumidor de forma sincera. Chamamos de “compatibilidade de incentivos”. Por exemplo, podemos ter um requerimento de *staking* de tokens para ter poder de voto e o incentivo de redistribuição dos tokens caso você vença a votação.

*Caso em questão: Token de governança $KNC, da Kyber Network, com requerimento de staking para votar em como os tokens de transação serão utilizados.*

Existem dois tipos de compatibilidade de incentivos:

1. Sinceridade dos participantes é a melhor opção, independente do que outros participantes façam ou digam. Essa é a Compatibilidade de Incentivos da Estratégia Dominante (DSIC).
2. Sinceridade dos participantes é a melhor opção, com base na expectativa deles sobre as escolhas dos demais participantes. Essa é a Compatibilidade de Incentivos Bayesiana (BIC).

Mecanismo de compatibilidade DSIC é o ideal, mas nem sempre simples de se estruturar. Por isso, BIC é a segunda melhor alternativa.

BIC pode ser usado, por exemplo, em propostas de melhoria e votações de governança. Nesse exemplo, participantes votantes de uma governança podem se comunicar por meio do mecanismo de *staking* e necessidade de atingir o quórum mínimo para a votação. A decisão de votar é pública, mas o voto em si é privado. Participantes da economia não têm como comunicar perfeitamente sua escolha de voto, mas eles **podem** comprometer-se com o resultado da votação por meio do *staking* de uma quantia maior de tokens para atingir o quórum mínimo. BIC entra nessa dinâmica pois, visto que participantes fazem suas escolhas previamente e não podem mudar após verem os resultados, faz com que os votantes não tenham incentivos para enganar os demais sobre seu voto.

### [Estudo de Caso] Coordenação e Economia de Token: MolochDAO

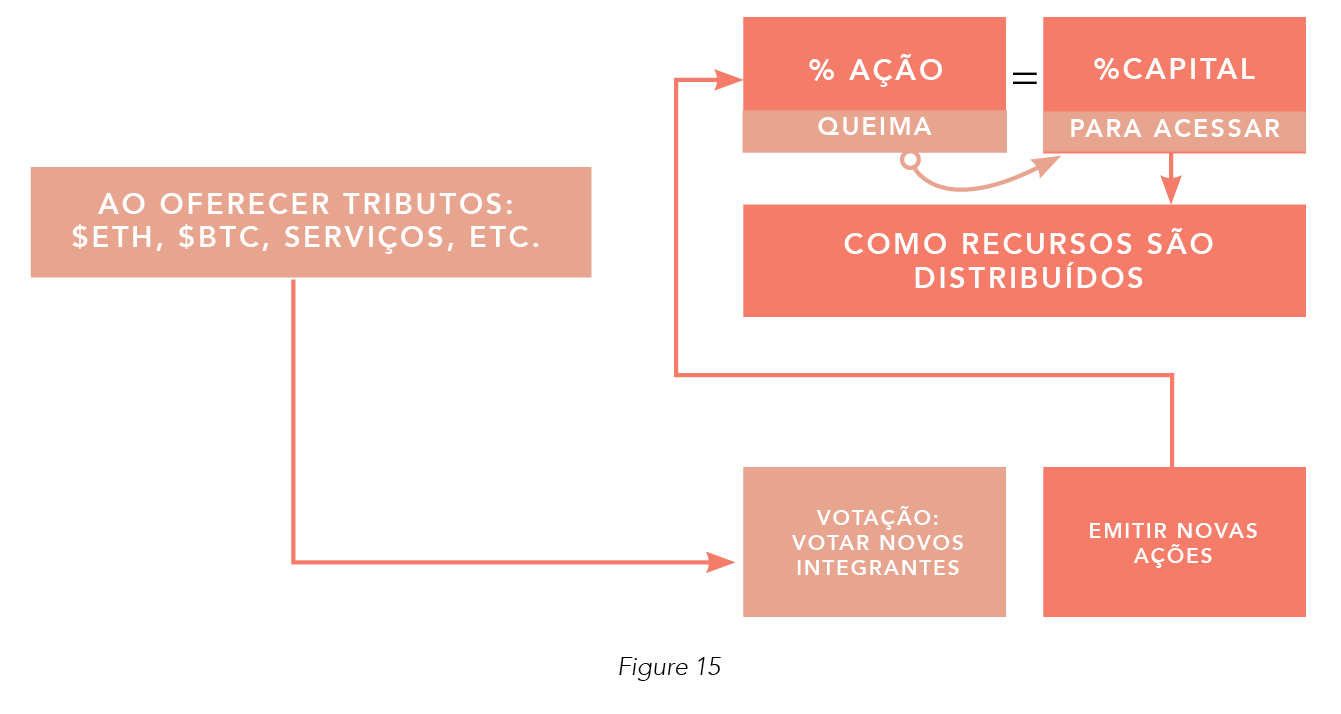


Figura 15

Na sua essência, MolochDAO busca coordenar e administrar recursos para distribuição de subsídios a projetos desenvolvidos na rede Ethereum. A única forma de acessar o capital da MolockDAO é por meio da queima (*burn*) de ações, junto com o direito proporcional de votar sobre a emissão de novas ações. Em outras palavras, um desenvolvedor que está desenvolvendo um projeto na rede Ethereum e possui 10% das ações da MolochDAO pode optar por queimar essas ações e receber 10% do capital detido pelo protocolo naquele momento.

As únicas votações na MolochDAO são para entrada de novas pessoas e emissão de novas ações para eles. Para entrar na MolochDAO, aplicantes precisam que acionistas votem e criem ações para eles. Caso participantes que já queimaram suas ações queiram retornar para a MolochDAO, acionistas atuais votam novamente sobre sua admissão (ou não) de volta ao ecossistema.

Esse mecanismo facilita a entrada e saída de participantes. Membros que não querem mais fazer parte da DAO podem queimar sua participação, receber capital referente ao total, e seguir a vida. Isso incentiva honestidade e transparência, além de ajudar a garantir cooperação. Membros que não pretendem cooperar sairão do ecossistema e serão pagos para isso, deixando apenas participantes que querem cooperar uns com os outros.

### Externalidades de Incentivos

*“Não é da benevolência do açougueiro, do cervejeiro ou do padeiro que esperamos nosso jantar, mas da consideração que eles têm pelos próprios interesses.”*

*- Adam Smith*

Pessoas se comportam com base em seus próprios interesses. A solução é alinhar seus interesses pessoas com os interesses da comunidade (*online* ou *offline*). Mas primeiro precisamos entender no porquê de as pessoas tomarem decisões de interesse próprio. Isso se dá pois o custo das decisões é arcado por outra pessoa[[34]](#footnote-35).

Por exemplo, suponhamos que um profissional sênior possui cargo estável e não pode ser imediatamente substituído. Isso remove a preocupação sobre a segurança de seu trabalho, e garante o foco no crescimento do negócio no longo prazo. Por outro lado, esse incentivo cria uma externalidade negativa, visto que o profissional se sente protegido das consequências de decisões ruins. Ele pode focar em resultados de curto prazo às custas de resultados de longo prazo. O custo de abrir mão de resultados futuros será arcado por acionistas e profissionais futuros, assumindo que o time atual já não esteja mais presente.

A solução é alinhar os interesses dos agentes (profissionais) e do principal (empresa) para que um indivíduo não possa se beneficiar às custas dos outros (consultar 5.6).

Duas externalidades são Risco Moral e Seleção Adversa.

#### Risco Moral

Essa é a situação em que **ações ocultas** ocorrem. Por exemplo, o **agente** possui mais informação do que o **principal** e assina o contrato com base nessa **informação secreta.** Isso significa que o principal irá arcar com esse **custo** (consultar 5.6).

Exemplo 1: Fumantes (agentes) têm maior interesse por planos de saúde pois sabem que vão precisar no futuro (ação oculta/informação secreta). Isso é ruim pois a empresa de seguros (principal) se torna responsável por pagar os gastos médicos (custo).

Exemplo 2: Uma pessoa (agente) com seguro contra roubos de carro será menos cautelosa (ação oculta) sobre onde estacionar seu carro pois as consequências negativas (custo) são transferidas para a empresa de seguros (principal).

Risco moral ocorre quando um indivíduo aumenta sua exposição ao risco por possuir alguma forma de proteção e porque outro agente irá arcar com o custo do mesmo. O agente protegido decide quanto tomar de risco, enquanto o outro agente arca com os custos se as coisas derem errado. A existência de seguros ou proteções pode mudar a forma como alguém se comporta quando comparado à exposição completa ao risco. Uma possível solução é que o principal crie desincentivos para prevenir agentes de “se aproveitarem”.

#### Risco Moral e Economias de Token

Há muitos exemplos de risco moral no mundo cripto e blockchain no geral. Ótimos exemplos são as agências de classificação de tokens (rating). As agências são os principais, e investidores são os agentes. Investidores usam as informações de rating para suas decisões de investimento.

Agências de classificação deveriam considerar todos os riscos de forma honesta. As informações são usadas para benefício dos investidores como parte de sua pesquisa e diligência. Porém, incentivos não estão sempre alinhados. As agências são pagas pelos emissores de tokens e portanto são mais inclinadas a darem boas avaliações para os tokens e manter relação saudável com seus clientes. Essa informação oculta não é revelada para os investidores.

Investidores tomam mais risco ao seguirem classificações imprecisas por parte das agências. Eles pagam o preço (consequências do risco aumentado) por não saberem das informações ocultas (classificações imprecisas).

Esse risco moral é comum em TradFi e agências de crédito, por mais que seja um pouco diferente em Economias de Token.

##### Rug Pull como Risco Moral

*Um rug pull, de forma genérica, é a remoção inesperada da ajuda de alguém, deixando o outro em uma situação complicada. Rug pull em DeFi é quando o provedor de liquidez remove a liquidez do sistema, deixando usuários com tokens sem valor algum. Isso é chamado de “tomar um rug”.*

Rug pulls são causados pelo risco moral em finanças descentralizadas (DeFi), principalmente nas corretoras descentralizadas (DEXs). Qualquer um pode criar uma piscina de liquidez adicionando $ETH e outro token aleatório à essa piscina. Isso provém liquidez para usuários negociarem os tokens em questão. Ao injetar grandes quantias desse token aleatório na piscina, um indivíduo pode automaticamente remover todo ou quase todo o $ETH restante.

*Lembrete: Essa é a situação em que* ***ações ocultas*** *acontecem. Um partido possui mais informação do que outro (sobre o plano de dar executar um rug pull) e ambos entram em um acordo. Após o contrato ser acordado, apenas um dos partidos irá arcar com os custos da ação oculta (injeção relevante de tokens aleatórios).*

Rug pulls podem ser ações ocultas tomadas pelo designer do protocolo, sendo que seu custo é suportado pelos usuários. O designer pode intencionalmente deixar uma “porta dos fundos” (*backdoor*) no código para possibilitar o roubo de fundos num momento futuro.

Como exemplo temos o caso da UniCat, um projeto de rug pull com vários riscos morais. UniCat possibilitava usuários de ganharem tokens $MEOW (*farming*). Ao interagir com o protocolo, aprovação de transações na carteira era requerida, e o limite era automaticamente configurado para “Permissão ilimitada de fundos”.

UniCat, dono do projeto fraudulento, é um ator malicioso[[35]](#footnote-36). Planejaram algumas ações ocultadas mesmo antes do token $MEOW ser lançado.

1. Puxaram o tapete dos usuários ao remover toda a liquidez, deixando o mercado com tokens sem valor ($MEOW).
2. Deixaram um *backdoor* no contrato inteligente de *farming* que possibilitava uma mudança de permissões para sacar os fundos por meio da “Permissão ilimitada de fundos” mencionada acima.
3. Para cobrir rastros, um novo contrato inteligente foi criado para cada vítima que transferia a posse da posição para um novo contrato.
4. Cada novo contrato recebia os fundos, trocava na Uniswap por $ETH e enviava para o endereço proprietário da UniCat.

Com esse exemplo de informação oculta, fica claro a relevância do risco moral em um ambiente tokenizado com design mal estruturado.

#### Seleção Adversa

Seleção adversa é resultado de **sinais de preço ineficientes** por meio de **assimetria de informação** (um partido tendo mais informação ou informação diferente comparado ao outro).

Exemplo 1: Vendedores possuem mais informação que compradores. Mecânicos de carro entendem mais sobre carros (informação assimétrica) e podem vender soluções/serviços mesmo quando não são necessários (sinais de preço ineficientes). Donos de carro geralmente não sabem tanto quanto o mecânico.

Exemplo 2: Compradores às vezes possuem mais informação sobre o quanto podem extrair de benefício de um serviço do que vendedores.

Um buffet liberado (coma o quanto quiser) que define preço único para todos os consumidores (sinal de preço ineficiente) toma o risco de selecionar adversamente clientes com maior apetite, e obviamente menos lucrativos. O restaurante não tem como saber se um cliente está com muito ou pouco apetite (informação assimétrica). O consumidor é o único que sabe como está seu apetite. Nesse caso, consumidores com mais apetite podem utilizar essa informação e ir a restaurantes com buffet liberado.

Uma possível solução é usar proxies (comparações) para ter uma sinalização sobre a informação faltante.

#### Seleção Adversa e Economia de Token

No mundo cripto, investidores de varejo podem experienciar seleção adversa. Protocolos de DeFi geralmente começam com recursos de *venture capitals* (VCs) ou de investidores varejo que são também usuários.

Vamos imaginar o exemplo de um mercado de crédito descentralizado *peer-to-peer* (DeFi, P2P).

Sistemas de empréstimos de P2P necessitam balancear o número de credores e devedores. Caso contrário, não haverá liquidez suficiente ou interesse por empréstimos. A plataforma se beneficia por meio de uma porção dos rendimentos. O papel da plataforma é agregar os participantes do ecossistema e manter a confiança dos mesmos, balanceando a oferta e demanda do mercado P2P.

Investidores de VCs[[36]](#footnote-37) e investidores de varejo[[37]](#footnote-38) se comportam de forma diferente. VCs são mais propensos a realizarem análises técnicas e diligências mais robustas porque eles têm incentivo e capacidade para fazê-las. Eles estão investidos no protocolo por um longo período e com quantias muito mais significativas. Por outro lado, investidores de varejo tendem a relevar essas análises técnicas e são apenas usuários do protocolo.

É nesse momento que a seleção adversa ocorre. Visto que ambos os partidos possuem horizontes de investimento e níveis de sofisticação diferentes, suas obrigações não correspondem às expectativas.

VCs geralmente possuem mecanismo de *vesting* em seus investimentos, em que os fundos são liberados e distribuídos gradualmente durante anos. Com investidores de varejo geralmente temos regras mais brandas, sem travas excessivas.

Investidores de varejo podem abrir e fechar posições com muita facilidade. São motivados pelas alternativas atuais de mercado. DeFi se mostra atrativo quando retornos são maiores do que os de TradFi. Porém, quando as principais ações começam a subir no mercado tradicional, investidores de varejo podem rapidamente mover seus fundos para fora de DeFi e para dentro de TradFi. Seleção adversa como nesse exemplo contribui para a criação de um “mercado de limões” em DeFi com apenas investidores de varejo de baixa qualidade.

*Esclarecimento: “Mercado de limões” é quando a qualidade dos bens negociados no mercado (plataforma) reduz na presença de assimetria de informação entre compradores e vendedores. Isso resulta em um mercado com apenas limões à venda*

Como exemplo, temos um dos VCs que participou na primeira rodada de investimento da Ribbon Finance. Ribbon Finance é um protocolo de opções. Para desenvolver o protocolo, levantaram capital de alguns VCs, em troca do token $RBN. $RBN é o token da plataforma Ribbon. VCs possuem tokens bloqueados (*vested*). Ao mesmo tempo, possuem a informação sobre prêmios (*airdrops*) que serão distribuídos para todas as carteiras que transacionarem um valor mínimo de opções. A informação pública é que 3% de toda a oferta de $RBN será distribuída. A informação privada é que existe um valor mínimo da transação para que ela seja elegível ao *airdrop*.

Dessa forma, esse VC criou dezenas de carteiras novas para interagir com o contrato de opções, e consequentemente receber grande parte dos tokens distribuídos. Quando o mercado foi aberto para negociações, o VC vendeu todos os seus tokens em cima de quem não tinha a mesma informação.

## Objetivos e Restrições

Esse livro é principalmente sobre design: definir e construir a economia de um ecossistema. Isso pode ser comparado com você criar um novo sistema próprio de leis da física em um novo planeta.

Nesse capítulo iremos focar em como podemos começar a estruturar o design desse ecossistema. Precisamos definir o espaço de design, os objetivos e as restrições.

### Objetivo

Definir o objetivo primário do ecossistema é uma das coisas mais importantes no processo de estruturação do token. O objetivo determina os mecanismos em questão, a estrutura de governança, as normas, os protocolos, e tudo que está nesse meio. Sem o objetivo, incentivos e punições não têm valor algum pois não influenciam no comportamento dos participantes do ecossistema de forma efetiva.

O objetivo é o que todo o ecossistema (agentes e mecanismos) trabalha para atingir. Isso significa que todos os mecanismos de incentivo devem ter o propósito de atingir o objetivo.



Figura 16

Podem existir mais de um objetivo, mas deve existir apenas UM objetivo principal. Tokens são usados para atingir o objetivo principal, primário.

Por exemplo:

* Objetivo do Bitcoin é ser uma moeda descentralizada *peer-to-peer* (P2P). Qualquer governança, mecanismo, ou melhorias futuras são feitas com o objetivo primário em mente. É muito improvável que o Bitcoin mude seu foco e comece a emitir stablecoins pareadas em dólar. Eles até poderiam fazer isso, mas seria improvável pois não faz parte do objetivo principal.
* Objetivo da Ethereum é ser o “maior computador global”. A rede está focada em pesquisa, DAOs, novos mecanismos, introduzir novos DApps em sua blockchain, etc. Todas essas atividades estão alinhadas com o principal objetivo de ser o “maior computador global”.
* Objetivo da MakerDAO é prover uma stablecoin e um token de governança. Visto que existem dois objetivos, possuem dois tokens no ecossistema. Não é eficiente um token ter mais de um objetivo pois não há foco único. $DAI é a stablecoin da MakerDAO, e $MKR é seu token de governança.

Conforme mencionado anteriormente, há vários objetivos em ecossistemas de token, mas apenas um objetivo principal. Isso é muito importante, visto que estruturamos os modelos econômicos do token com principal foco em otimizar seu objetivo primário.

### Restrições

Restrições são necessárias para limitar o escopo do ecossistema. Caso contrário, há fatores demais para considerar no modelo, e seria muito difícil definir seu design e implementação.

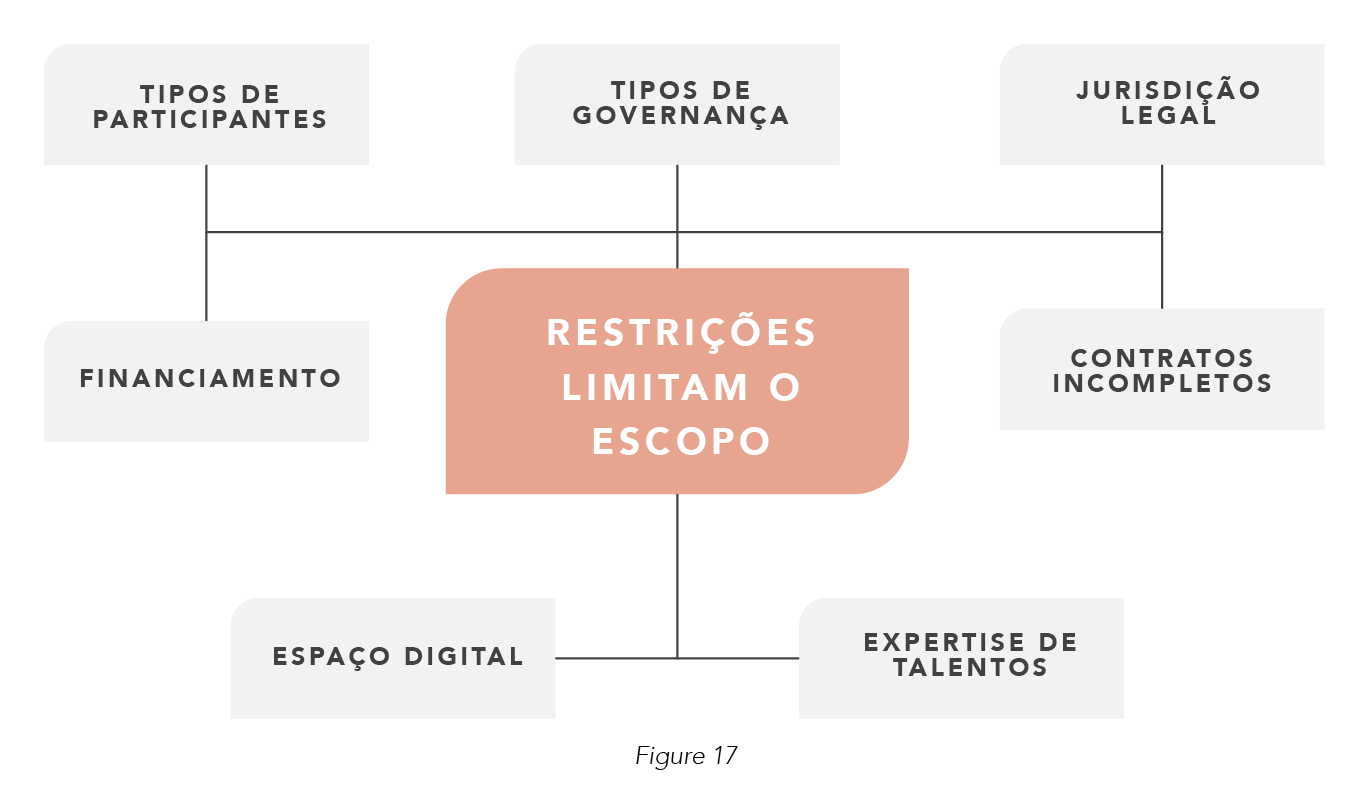


Figura 17

Restrições comuns:

* Tipos de participantes que o ecossistema busca atingir.
* Espaço: espaço digital e físico/jurisdição legal em que o projeto atua.
* Talento e expertise dos designers, desenvolvedores, e demais profissionais.
* Tipo desejado de governança: nível de centralização da governança precisa ser considerado dependendo da função, caso de uso e objetivo do token.
* Contratos incompletos: algumas contingências são difíceis de prever ou descrever antecipadamente, ou são complicadas demais para serem incorporadas em contratos legais e inteligentes.

### Processo de Design

Quando tanto os objetivos quanto as restrições estão no lugar, o processo de design pode iniciar. Design econômico se funde com design de sistemas para atingir os objetivos, com base nas restrições definidas.

#### Qual a importância?

Ter um objetivo primário claro é a chave para a estruturação de incentivos e mecanismos eficientes na influência de comportamentos dos participantes. Esse processo de design pode ser separado em duas camadas: design econômico e design de sistemas.

*Se economia clássica é definida pela racionalidade limitada, e física quântica significa racionalidade ilimitada, então design econômico é a irracionalidade limitada.*

**

*Figura 18*

Há três pilares em design econômico: design de mercado, design de mecanismo e design de token. Eles têm como base conceitos de micro e macro da economia tradicional – conversam com a **racionalidade** das pessoas.

Design de sistemas mistura economia comportamental, psicologia do consumidor e UI/UX para criar sistemas que conversam com a **irracionalidade** das pessoas.

Por esse motivo, temos incentivos diferentes para lidar com partes diferentes de nosso cérebro, o lado racional e o lado irracional.

## As Sete Maravilhas da Economia de Token

Economia é um tópico muito amplo, e a economia de token não é diferente. Economia de token pode ser dividida em muitos conceitos, teorias, e classificações.

Economia de token pode parecer ser complexa, mas não necessariamente. Antes de nos aprofundarmos nos pilares da estruturação/design, vamos começar com as Sete[[38]](#footnote-39) Maravilhas da Economia de Token.

Esses são conceitos econômicos já existentes no mundo físico, e aplicados no mundo digital cripto. Espero que esses conceitos te ajudem a entender o poder da economia na tecnologia de registros distribuídos (DLT) e te inspirem a estudar mais à fundo.

### Efeitos de Rede (*Network Effects*)

Você já ouviu esse termo inúmeras vezes. Há todo momento, pessoas dizem que “é tudo sobre os efeitos de rede”, o que não deixa de ser uma verdade. Efeitos de rede são importantes para a nova economia de rede que discutimos anteriormente. Efeitos de rede contribuem na aceleração do processo de adoção.

Efeitos de rede, que são tidos como “fossos econômicos[[39]](#footnote-40)”, ocorrem quando o sistema se torna mais valioso conforme mais pessoas são introduzidas a ele. Efeitos de rede estão diretamente ligados às propriedades de escalabilidade de ativos intangíveis.

Existem muitos tipos de efeitos de rede. Vamos começar com os efeitos de rede bilaterais, visto que a maioria dos ecossistemas de token também são bilaterais.

**Comunicação**

Ter um telefone é ótimo, mas caso você seja a única pessoa no mundo com um, não há valor algum em tê-lo.

Nossos métodos de comunicação mudam conforme as tecnologias avançam. O início da comunicação moderna se deu por meio de telegramas, por telefones fixos, pelos saudosos *pagers*,e finalmente os celulares. Depois vieram os serviços de mensagens instantâneas, como o MSN, AOL, e o chat do Yahoo. Hoje, existe uma abundância de aplicativos de comunicação que funcionam em nossos celulares e computadores, de acordo com as mais diversas preferências dos consumidores.

Pense nos seus aplicativos de comunicação preferidos. Eu uso o WhatsApp, Telegram e Twitter. Não porque eu gosto de dar meus dados para a Meta por meio do WhatsApp, mas simplesmente porque são os aplicativos mais utilizados pela minha rede. Aplicativos de comunicação só possuem utilidade se pudermos nos comunicar com os demais por meio deles.

Mesmo assim tenho um problema: WhatsApp foi banido na China, o que não facilita minha comunicação com meus colegas chineses. Eles não estão presentes no aplicativo. Como alternativa, usamos o WeChat. Além do WeChat, posso me comunicar com eles por meio de e-mails ou enviar uma carta por correios. Aplicativos de comunicação são mais úteis quando sua rede está presente nele.

Outros aplicativos de comunicação incluem KakaoTalk (Coréia do Sul), Line (Taiwan, Tailândia, Hong Kong), Viber (Filipinas), Meta Messenger (praticamente em todos os países), e iMessage (EUA e outros países em que iPhones são comuns). Qualquer um pode instalar o aplicativa da Line, por exemplo, mas a utilidade oferecida por ele será mínima caso sua rede/comunidade não esteja presente.

Pelo fato de efeitos de rede possibilitarem maior escalabilidade, muitas empresas buscam criar seus próprios efeitos de rede para dominarem o mercado. Mas, na prática, é muito difícil fazê-lo. Conforme mencionado no 5.1, existem diferentes tipos de efeitos de rede.

Tabela resumo dos mais diversos tipos de efeitos de rede:

* **Direto**: trens, estradas e rodovias
* **Bilateral**: Uber, Airbnb, Tinder
* **Dados**: Google, Waze, Amazon (valor do produto com base nos dados)
* **Performance tecnológica**: VPN, BitTorrent
* **Social**: idioma, crenças, religião, moeda, teorias da conspiração[[40]](#footnote-41)

No momento em que uma empresa é bem-sucedida na criação de seus efeitos de rede, ela começa a fazer parte de um grupo restrito de empresas grandes e dominantes.

No ambiente digital de tokens, empresas que pretendem competir com os detentores de ativos intangíveis escaláveis estão em uma situação bastante complicada – é uma situação de *winner-takes-all*, ou o vencedor leva tudo. A rede Ethereum, em combinação com sua rede de promoção e serviços agregados que aumentam os efeitos de rede, é muito difícil de ser ameaçada. Eles possuem financiamento para melhorar a performance tecnológica, uma nova linguagem de programação própria, e o *branding* da Ethereum como principal nome junto com o Bitcoin quando o assunto é blockchain.

DeFi e suas aplicações, tópico abordado na segunda metade do livro, existem principalmente na blockchain da Ethereum. Isso possibilita os mais variados ativos de cripto a se comunicarem entre si, com troca de dados e informação. Tokens/ativos de DeFi possuem maior usabilidade e utilidade por causa da Ethereum, que possibilitou maior maturidade e robustez do setor.

### Sinalização

**O que é Sinalização?**

Teoria da Sinalização funciona como um jogo de charadas. Outra pessoa tenta adivinhar sua carta, e você não pode dizer nada!

Falar é fácil. A mensagem fica mais clara quando mostramos com ações e outros métodos (i.e. “mostre ao invés de falar”. Em termos econômicos, isso geralmente se traduz em “colocar seu dinheiro onde boca/palavra está”.

**Namoro e casamento**

Como as pessoas sinalizam que são bons parceiros para dividir uma vida? Isso é sinalizado por meio das definições da sociedade sobre adequação masculina e feminina. Pode ser em termos de beleza, renda, educação, classe social, religião, entre outros, e pode mudar ao longo do tempo. Padrões de beleza femininos, por exemplo, mudam o tempo todo: o mundo fez transições de preferência por mulheres com corpos mais sinuosos (talvez como um sinal de riqueza, fartura) para mulheres mais magras (talvez como sinal de boa genética ou educação alimentar) para mulheres em forma (talvez como sinal de boa administração de tempo e valorização da saúde).

**Sinalização no ambiente de token**

No ambiente cripto, dadas as propriedades de escalabilidade e não-rivalidade de ativos intangíveis, é simples criar um novo token/ativo. Faça um *fork* do $BTC ou $LTC, mude alguns detalhes e você tem uma nova moeda. Qualquer um com o conhecimento técnico pode criar novos tokens e inundar o mercado. Praticamente não há custo para fazer o que acabei de explicar. Mas, como podemos sinalizar que esse ativo é “bom” ou melhor do que os outros de alguma forma? Como podemos aumentar o número de usuários reais e ativos?

Visto que é barato e relativamente fácil emitir um novo token, a sinalização precisa ser custosa. Caso contrário, o mercado seria entupido de tokens sem valor que poderiam de forma fácil e barata sinalizar que são “bons” ativos. Sinalização contribui para as barreiras de entrada. No fim, isso resulta em um mercado com tokens de maior qualidade, dado o alto custo da emissão de tokens sem valor.

**Exemplos de sinais:**

* Seja inovador na atração de grandes publicações sobre seu projeto. Isso sinaliza para o público que sua empresa é digna de sua atenção e começa a construir confiança.
* Pague para ter um artigo/publicação na Forbes, CoinTelegraph, TechCrunch etc. Isso gerará um sinal parecido. Não é orgânico mas, pelo fato de custar dinheiro, ajuda na sinalização de força - não faz sentido gastar dinheiro em um projeto sem valor.
* Whitepaper academicamente revisado por outros profissionais da indústria.
* GitHub atualizado frequentemente.
* Time composto por experts de vários campos de conhecimento (cientistas da computação, empreendedores, economistas, acadêmicos etc.).
* Comunidade real e ativa em redes sociais como Twitter, Telegram, e Discord.
* Caso o MVP[[41]](#footnote-42) seja lançado: TVL (Valor Total Travado) do protocolo e índice de TVL para o preço do token.
* Além do whitepaper, publique artigos econômicos sobre o token, artigos técnicos, litepapers etc.

### Políticas Monetárias

*Mais detalhes sobre políticas monetárias no Capítulo 10.*

**O que é política monetária?**

Em nosso contexto, política monetária aplica-se principalmente a moedas digitais e criptoativos – que são formas de dinheiro. Alguns aspectos de política monetária *podem* ser aplicados a outras funções de token (utilidade, títulos tokenizados), mas nessa seção focaremos em moedas.

**Moeda centralizada**

Considerações a fazer sobre economia monetária:

* Políticas fiscais: alteração de taxas/impostos, gastos governamentais, empréstimos (i.e. administrar indiretamente o dinheiro por meio de mecanismos de governança).
* Políticas monetárias: aumento/diminuição da oferta (*supply*), controle inflacionário para sustentar a demanda pela moeda, foco na estabilidade de preço.
* Regimes de câmbio (caso necessário):
  + Uniões monetárias (ex: União Europeia)
  + Câmbio flutuante controlado (ex: HKD-USD)
  + Câmbio flutuante (ex: USD, GBP, CHF, JPY)
  + *Pegs*, ou câmbio indexado, pareado (ex: Belize-USD)

Bancos centrais controlam a moeda de um país. O Fed, banco central dos Estados Unidos, controla a administração do dólar (USD) por meio de políticas monetárias. O Banco Central do Brasil controla o real (BRL). A Autoridade Monetária de Singapura (“MAS”) controla a forma que o dólar de Singapura (SGD) é administrado. Basicamente, um grupo pequeno[[42]](#footnote-43) formado por pessoas inteligentes dessas organizações decidem a forma que a moeda é controlada e governada. Isso me parece muito centralizado.

**Moeda descentralizada**

Com moedas descentralizadas, muitas das decisões centrais estão embutidas no código e inclusas no ecossistema do token, ao invés de serem determinadas por uma autoridade central (apenas inicialmente no seu desenvolvimento). Dependendo do design de mecanismos, participantes da rede podem votar para mudar regras ou sistemas. Distribui poder para os membros daquele comunidade da blockchain. No mundo cripto, não existe um consenso sobre a forma perfeita de manejar uma moeda digital/token. Alguns preferem com oferta limitada (*capped supply*), outros preferem com oferta dinâmica/ilimitada (*uncapped supply*), e existem muitos outros modelos nesse meio. $BTC (Bitcoin) é limitado a 21 milhões de unidades, enquanto outros não tem limite algum, como $MKR (MakerDAO).

Há muitas maneiras de estruturar moedas digitais *peer-to-peer* com políticas monetárias já inclusas no código para reduzir a volatilidade de preço. Ampleforth, por exemplo, é um projeto que balanceia por algoritmo o preço da moeda para atingir estabilidade de preços no longo prazo (vide Cápitulo 10).

### Direito de Propriedade

Direito de propriedade é uma construção imposta socialmente para determinar a forma como um recurso/bem é usado/controlado. Esse é um tópico muito amplo por si só, visto que há muitas maneiras de determinar a alocação dos direitos de propriedade, e ideologia política tende a influenciar no que as pessoas acreditam ser melhor. Vamos focar nas novas formas de administrar o direito de propriedade com ativos digitais (vide Cápitulo 13 para mais detalhes sobre direito de propriedade).

**Direito de propriedade financeiro padrão**

Em finanças tradicionais (TradFi), você possui o direito de participar no sucesso de uma empresa caso seja detentor de ações da mesma (por meio de dividendos e/ou apreciação de valor das próprias ações).

**Novo direito de propriedade**

A parte boa é que existem novos tipos de direito de propriedade! (vide Capítulo 13 e Capítulo 25).

Títulos tokenizados (*securities*) já estão sendo emitidos na blockchain, o que garante seu direito sobre o ativo. Como a WeFunder e a SeedInvest fizeram, startups podem levantar capital diretamente da blockchain. Tokens possibilitam investidores a adquirirem participação no projeto e se beneficiarem por meio de dividendos e divisões de lucro.

Visto que tokens podem ser programados, designers podem codificar modelos inovadores de votação, direito de propriedade etc. O fato de estar na blockchain não resolve todos os problemas, mas ajuda a reduzir ineficiências de transparência e coordenação de transações.

Com a invenção de bens digitais, o direito de propriedade – e a forma como percebemos ele – está evoluindo. Criatividade é crucial para determinar como alocar bens digitais de forma que crie valor. O mecanismo de taxação de propriedade proposto inicialmente por Harberger[[43]](#footnote-44), por exemplo, é uma nova forma de interpretar o direito de propriedade. Ao invés das forças normais de mercado determinarem o preço base e proprietários pagarem impostos de acordo com esse preço, o proprietário determina o preço de mercado e impostos são pagos de acordo com esse valor.

Você pode estar pensando, *então é só precificar o mais baixo possível para pagar menos impostos*.Com a taxação de propriedade de Harberger, qualquer um pode forçar o proprietário a vender o ativo no preço determinado. Isso incentiva diretamente uma precificação honesta. Caso proprietários coloquem um valor baixo demais, alguém irá comprar o ativo com ótimo desconto. Caso coloquem um valor alto demais, terá que pagar impostos exorbitantes. Esse mecanismo é o tipo de compatibilidade de incentivos que falamos no 3.3.1, que alinha os objetivos de todas as partes interessadas e cria um sistema autogovernado.

### Lock-In

**O que é *lock-in*?**

*Lock-in* é um conceito relativamente novo (implementado nos últimos 20-40 anos, no mesmo período da famosa “era .com”) comparado aos demais conceitos da economia tradicional. Foi popularizado com as inovações da tecnologia da informação (que provocou a evolução da economia da informação).

*Lock-in* é a forma de manter pessoas em seu sistema. Existem muitas formas tradicionais de fazer isso, como:

* Tornar difícil logisticamente de sair do sistema.
* Continuar atualizando o sistema para terem uma razão para ficar.
* Fazer com que a mudança de sistema seja custosa, cara.

Podemos criar efeitos de *lock-in* em três pontos: no produto por si só, produtos complementares (redes), e conhecimento tácito (conhecimento subjetivo e individual).

**Elementos da informação digital e *lock-in***

*Sunk cost*: custo não recuperável

Informação intangível é fácil de vender, mas difícil de pegar de volta (retornar). Isso aumenta o *lock-in* pois quando você adquire o “conhecimento”, não tem como se livrar dele. Essas informações também estão geralmente ligadas ao ecossistema da empresa (marca, processos operacionais, cadeia de suprimentos etc.).

Um processo operacional automatizado, por exemplo, provavelmente é útil apenas para a empresa em questão. Geralmente não é transferível, por ser customizado para aquela empresa. Tudo isso retém o conhecimento de trabalho dentro do ecossistema. O custo não recuperável é o investimento no desenvolvimento do processo operacional automatizado e na qualificação de profissionais.

*Spillovers:* Efeitos de transbordamento

*Spillovers* podem fortalecer os efeitos de *lock-in* por meio do compartilhamento de ideias, transbordamento de marketing, transbordamento de treinamentos e transbordamento do ecossistema.

Por exemplo, o ecossistema do Uber se beneficia do *spillover* da tendência de mais pessoas possuírem smartphones.

Sinergias

Algumas ideias são melhores quando combinadas de forma complementar, criando incentivos robustos para o trabalho conjunto. Sinergias são também uma forma alternativa de proteção de investimentos intangíveis contra competidores, por meio de grupos de rede sinérgicos, ao invés de gastar recursos protegendo ativos individuais.

A EEA[[44]](#footnote-45) (Ethereum Enterprise Association), por exemplo, apoia seus desenvolvedores e investe em treinamentos sobre Solidity (linguagem de programação da Ethereum), mas não sobre outras linguagens de *smart contracts*.

**Windows XP**

Você sabia que 1,15 porcento[[45]](#footnote-46) do mundo ainda usa Windows XP? Por que isso acontece, mesmo a Microsoft tendo criado sistemas mais novos e melhores? Simples. É caro mudar para o Windows 10, por exemplo.

O preço do Windows 10 não é necessariamente o problema, visto que muitos usuários podem atualizar seu Windows de graça. Porém, o custo de mudança (*switching costs*) pode ser mais do que apenas o preço da licença, como o trabalho para fazer a atualização, a possibilidade de precisar de um hardware melhor, e as ineficiências de adaptação ao novo sistema operacional. Alguns sistemas empresariais que foram feitos para o Windows XP talvez nem funcionem no Windows 10, mesmo com o modo de compatibilidade.

**Ethereum**

Ethereum está trabalhando para ser “A” plataforma de segunda camada para sistemas de blockchain. EEA e Consensys estimulam participantes e projetos na rede. Como a Ethereum pode aumentar ainda mais seus efeitos de *lock-in*?

O segredo de seu *lock-in* está na linguagem de programação (Solidity) e demais conhecimentos tácitos presentes na tecnologia. Além disso, a Ethereum oferece subsídios e apoia muitos projetos construídos na rede.[[46]](#footnote-47).

### Problema do Principal-Agente, Risco Moral, e Informação Assimétrica

Economias de token bem estruturadas e pensadas podem mitigar muitos efeitos do problema do principal-agente, por conta de seu discernimento sobre incentivos dos participantes envolvidos (principais e agentes).

#### Introdução ao problema do principal-agente

O problema do principal-agente (teoria do principal-agente) se refere aos perigos que surgem quando um “agente” representa outra entidade, o “principal”. Agentes são indispensáveis em certas transações. Porém, às vezes podem agir por interesse próprio, engajar em ações arriscadas, ou faltar com boa-fé, em prejuízo do principal, por saberem que é ele que irá arcar com as consequências econômicas decorrentes de seu comportamento.

Isso geralmente acontece quando principal e agente possuem interesses diferentes e assimetria de informações, onde um partido (nesse caso, o agente) tem mais informação do que o outro (principal). O principal fica limitado na sua habilidade em monitorar e garantir que o agente agirá com boa-fé. Quando as prioridades do principal são custosas para o agente, ou quando o monitoramento do agente é custoso, esse problema se agrava. Esses custos são chamados de “custos de agência”:

* Custo de monitoramento – esses são custos pagos pelo principal para mitigar o problema do principal-agente por meio de investigações, monitoramento, auditorias etc., e para alinhar incentivos com seu objetivo (ex: distribuir participação para funcionários-chave para garantir que irão agir de acordo com os interesses do principal).
* Custo de ligação (*bonding cost*) – esses são custos arcados pelo agente dada sua limitação na tomada de decisão e/ou aumento de transparência impostos pelo principal para reforçar a confiança.
* Custo residual – esses são custos que o principal sofre quando o agente age de forma contrária a seus interesses (ex: prejuízo/resultados piores, multas, custos de reputação etc.).

Breve nota sobre os exemplos: Sabemos que a maioria dos agentes nos exemplos abaixo agem com boa-fé e oferecem serviços importantes em seus setores. Exemplos servem para ilustrar o conceito do problema do principal-agente, e não para alertar o leitor sobre os “perigos” de trabalhar com os agentes mencionados.

Exemplo 1 – Advogados

Clientes (os principais) geralmente têm pouca visão sobre seus advogados (os agentes) estarem agindo de acordo com seus interesses ou não. Será que a estratégia legal longa e custosa é realmente necessária para atingir o objetivo do cliente? Ou será que o advogado quer apenas ganhar o máximo possível com o serviço?

Advogados nos Estados Unidos são obrigados a aderirem ao código de conduta profissional imposto pela associação estadual, que geralmente se baseia no modelo de código de conduta profissional da associação nacional[[47]](#footnote-48). Associações estaduais oferecem recursos para clientes reportarem má conduta ou improbidade, pesquisarem a licença de advogados e históricos disciplinares, e até mesmo fundos para a proteção de clientes caso sofram perdas por condutas desonestas de advogados. As supremas cortes dos estados investigam essas matérias, impõem medidas disciplinares contra advogados que violam as regras do código de conduta profissional (podendo até mesmo perder sua licença advocatícia) e recompensam as vítimas.

Exemplo 2 – Corretores Imobiliários

Corretores imobiliários podem hipoteticamente ter conflitos de interesse ao intermediar a compra de um imóvel. Por exemplo, o agente vendedor pode fazer promessas irreais sobre o preço de venda do imóvel, impactando a probabilidade de venda do ativo. O agente pode também priorizar um negócio rápido ao invés de priorizar o melhor preço possível para o cliente (volume acima de valor). Ou agentes compradores podem usar uma informação sabida do comprador (como sua renda ou patrimônio) e simplesmente não “pechincharem” até o limite que poderiam porque sabem que o cliente “pode pagar”, ganhando uma comissão maior no processo como agravante.

Nos Estados Unidos existem medidas públicas e privadas para diminuir os impactos negativos do problema do principal-agente nos clientes. Agências estaduais regulatórias oferecem aos consumidores a possibilidade de abrirem reclamações e investigações para determinar se medidas disciplinares são necessárias. Medidas disciplinares geralmente ordenam que corretores imobiliários façam a coisa certa para manterem ou recuperarem sua licença. Além disso, a Associação Nacional de Corretores oferece treinamento, certificação, código de ética, e procedimentos disciplinares que podem ameaçar o status de corretores que se comportem mal.

Exemplo 3 – Conselho Corporativo de Diretores

Conselhos de diretores e administradores corporativos são os agentes dos acionistas (que são, por sua vez, os principais). Existem estatutos corporativos e outros mecanismos em funcionamento para garantir a priorização dos interesses dos acionistas. Outras prioridades porém, como a aquisição de outras empresas ou investimentos em projetos não-lucrativos, podem desviar recursos da companhia para coisas que não maximizam o valor para o acionista.

Exemplo 4 – Relação Locador/Locatário

Locadores (proprietários) que pagam as contas (água, luz, gás etc.) das propriedades alugadas com o aluguel dos locatários (ex: contrato com “conta de luz e água inclusas”) têm pouca influência no consumo dos mesmos. Locatários (agentes, nesse caso) não têm consequência alguma por desperdiçarem no consumo de água e luz; proprietários (principais) arcam com as consequências econômicas desse comportamento. Porém, quando proprietários implementam políticas que alinham as consequências econômicas de consumo desregrado com a conta bancária do locatário, o consumo é reduzido. Isso pode ser feito por meio de acordos até certo valor limite, ou colocando as contas no nome do locatário. Esses acordos podem ser escritos em contratos de aluguel e são governados pelas leis de locador/locatário do estado.

Só a possibilidade de arcar com esses custos de agência muitas vezes pode ser suficiente para impedir alguém (um principal) até mesmo de engajar em uma negociação, o que pode resultar em efeitos ainda piores em alguns casos. Alguns desses fatores podem ser intensificados em protocolos de DeFi com designs mal estruturados, o que aumenta ainda mais a importância de mitigar os fatores catalisadores do problema do principal-agente.

De forma simples, a melhor forma de mitigar os efeitos negativos do problema do principal-agente é alinhar os incentivos de todos os participantes na transação por meio de mecanismos que coloquem “a pele deles em risco” (*skin in the game*). Caso agir de boa-fé seja mais lucrativo para os participantes, ou a punição de comportamentos indesejados seja efetiva, custos de agência são significativamente reduzidos.

#### Soluções de Web 3.0 para o problema do principal-agente

**Pagamento por performance**

Pagamento por performance pode mitigar parcialmente o problema do principal-agente no caso de contratos incompletos[[48]](#footnote-49) que limitam a capacidade do principal (ex: a comunidade do Bitcoin) em determinar variáveis cruciais com antecedência. “Pagar por performance” possibilita transações mais abertas a mudanças na rede, mercado macro global, ou acordos de transação.

No caso do Bitcoin, um aspecto do problema do principal-agente é o custo de equipamentos de hardware que os agentes (ex: mineradores) precisam dedicar, o que poderia influenciá-los a não “trabalharem duro”. A “variável crucial” que o contrato do Bitcoin não especifica com antecedência é a quantidade de poder computacional necessária que cada minerador precisa contribuir para garantir a validação correta do bloco. Essa incapacidade de determinar com antecedência quanto de poder computacional é necessário é um exemplo de contrato incompleto.

Bitcoin utiliza mecanismos de pagamento por performance em seus contratos inteligentes para resolver o problema do principal-agente. Agentes só são pagos (recompensa de blocos) após a verificação da finalização do trabalho (validação do bloco). Esse mecanismo alinha de forma efetiva os incentivos entre o principal (a rede do Bitcoin, que precisa de poder computacional para verificar novos blocos), que pode oferecer recompensas condicionadas ao desempenho dos agentes (mineradores), e agentes que estão dispostos a dedicarem recursos para resolução do problema, dependendo do retorno potencial. Por exemplo, um minerador pode decidir por contribuir para o ecossistema do Bitcoin investindo em GPUs ou mineradoras ASICs melhores (“*Application-Specific Integrated Circuit*”, dispositivos eletrônicos integrados com desenvolvidos única e exclusivamente com o propósito de mineração de criptomoedas).

### Ponto Focal ou Ponto de Schelling

**O que é o Ponto Focal?**

O ponto focal, ou Ponto de Schelling, cunhado pelo teórico de jogos Thomas Schelling em seu livro *The Strategy of Conflict*, descreve o fenômeno de quando as pessoas são capazes de se coordenarem sem utilizar a comunicação, baseando-se apenas no que *eles pensam* que outras pessoas irão fazer.

**Fazendo escolhas**

Talvez o exemplo mais conhecido do Ponto de Schelling seja o seguinte questionamento: “Você precisa encontrar uma pessoa estranha em Nova York, mas não pode se comunicar com ela. Aonde você iria para esse encontro?” A resposta mais comum após inúmeros estudos foi, mesmo em condições controladas, que o melhor seria “no terminal central, no balcão de informações, ao meio-dia.” Esse não é um sistema perfeito, como sugerido pelo Dilema do Prisioneiro[[49]](#footnote-50), mas geralmente leva a resultados positivos em termos de cooperação.

**Fazendo escolhas na blockchain**

Pontos de Schelling são críticos para cooperação em sistemas descentralizados. Imagine que você precisa coordenar as atividades de vários indivíduos, com incentivos diferentes, preferências etc. Isso pode ser feito por meio da utilização de pontos focais no design da blockchain.

É assim que o consenso, de forma simplificada, funciona na rede Ethereum. Dada uma situação em que temos duas cadeias de informação: uma mais longa (com muitos blocos verificados) e outra mais curta (possivelmente devido à um hard fork), em qual cadeia você adicionaria seu bloco? Provavelmente na cadeia mais longa, que oferece melhores indicativos de validade de verificação e possibilita a cooperação por meio de consenso sem a necessidade de comunicação.

A SchellingCoin[[50]](#footnote-51) é um outro exemplo – feed de dados desenvolvido pela Ethereum para contratos financeiros e derivativos para possibilitar contratos inteligentes acessarem informação do “mundo real”, externo. De forma resumida, a SchellingCoin possibilita usuários submeterem informação. Os que oferecem informações honestas e corretas são recompensados e os que fazem o contrário são punidos.

Esse mecanismo funciona porque a “verdade” é o ponto focal mais forte que existe. Ao incentivar a verdade, participantes podem seguramente assumir que todos, ou pelo menos a grande maioria, irão submeter informações honestas para receberem recompensas.

## Design de Mercado

*Existem três pilares no design de ecossistemas de token. Esse é o primeiro.*

### Design de Mercado: Parte 1 – Introdução

Design de mercado é a estrutura do ambiente em que os participantes interagem e realizam transações entre si. No mundo físico, design de mercado é utilizado no nicho de transplantes de rim[[51]](#footnote-52), mercado de trabalho para economistas[[52]](#footnote-53), ou escolhas de alocação na educação primária[[53]](#footnote-54).

Mas não é disso que estamos falando. Estamos falando sobre design de mercado em ecossistemas digitais descentralizados, ecossistemas de token.

Design de mercado é uma forma de engenharia microeconômica[[54]](#footnote-55). Aplica conceitos de ciências (economia) e artes (design).

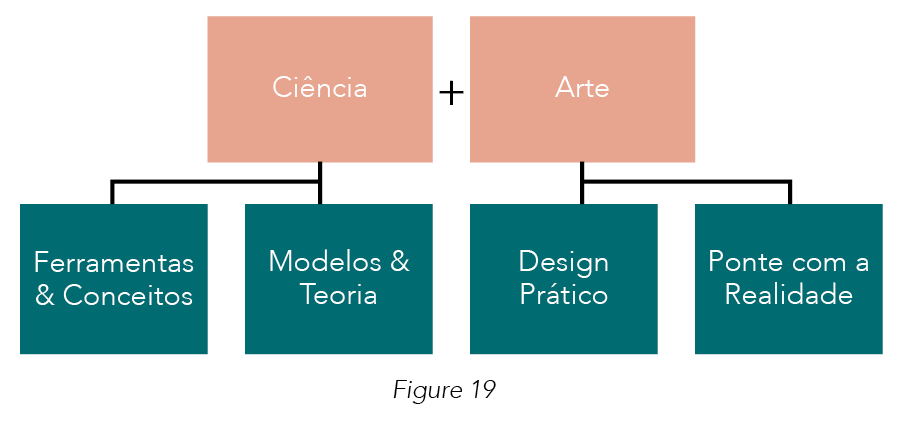


Figura 19

Design de mercado é uma ciência pois aplica ferramentas e conceitos da teoria dos jogos e design de mecanismo.

É, também, uma arte pois utiliza design prático de tomada de decisão que vai além da teoria. Lembra quando mencionei que humanos são seres muito irracionais? Em ciência, geralmente assumimos que as pessoas são racionais, e que se comportam perfeitamente. Mas, esse não é o caso. Por isso precisamos do design e da arte, para aplicar a ciência na realidade de forma prática.

### Por que Design de Mercado é Importante para Ecossistemas de Token?

Existem alguns problemas potenciais resultantes de mercados mal estruturados, mas os dois principais são:

1. Mercados não são inerentemente estáveis, o que pode gerar ineficiência – e ninguém gosta de ineficiências!
2. Mercados podem promover diversos desfechos (idealmente, os descritos como objetivos e discutidos no 4.1). Participantes de mercado têm a intenção de agir conforme objetivos do protocolo, mas só dará certo se os incentivos e a estruturação do ecossistema estiverem bem elaborados.

Design de mercado adequado pode resolver esses problemas ao:

1. Garantir que o mercado é seguro e estável, para que usuários decidem transacionar dentro do próprio ecossistema – ao invés de ambientes externos.
2. Incentivar participantes de negociarem no mercado próprio, dentro do ecossistema. No início do Airbnb, as pessoas usavam a plataforma para encontrar acomodações, e posteriormente entravam em contato com o proprietário por fora para fechar o acordo sem pagar as taxas de serviço da empresa. Para incentivar os usuários a permanecerem **dentro do ecossistema**, o Airbnb desenvolveu processos de pagamento de alto padrão, para que os proprietários tivessem a certeza de que receberiam o pagamento e eliminasse o atrito de cobranças posteriores por falta de pagamento. Restringiu também algumas informações públicas antes do fechamento da reserva, como o endereço exato do local, e implementou monitoramento para impedir a troca de informações e o fechamento de negócios por fora do ecossistema.
3. Adicionar regras e restrições para encorajar comportamentos específicos e promover a cooperação no mercado.

Design de mercado adequado é crucial para ecossistemas de token. Nos auxilia a incentivar bons comportamentos para atingir os objetivos do ecossistema, como moeda estável, monitoramento eficiente da cadeia de suprimentos etc. Também nos ajuda a entender os pontos de fraqueza do mercado, e como mitigar esses riscos. Mercados com bons designs encorajam a participação na rede e, consequentemente, geram mais valor para todos envolvidos.

### Design de Mercado: Parte 2 – Definindo Design

Design de mercado é uma forma de engenharia econômica para modelagem e codificação de regras formais, com a intenção de governar as interações entre participantes de mercado. Em ecossistemas de token, por exemplo, design de mercado define o que participantes podem/não podem fazer, ou devem/não devem fazer.

Pessoas possuem predisposição a fazer o que acreditam ser melhor considerando seus próprios interesses. Por isso, mercados não funcionam devidamente sem a existência de incentivos que alinham os interesses próprios com os interesses dos demais.

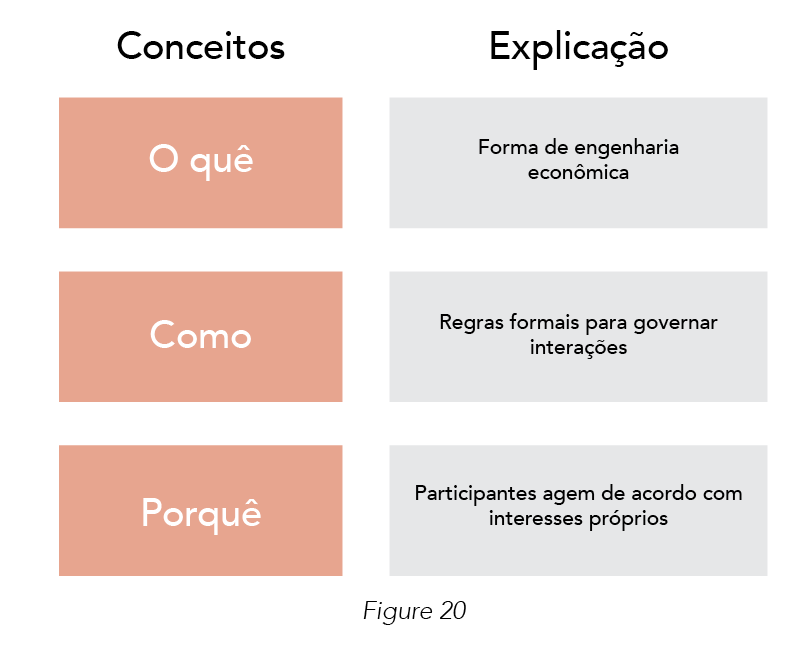


Figura 20

“Engenheiros econômicos”, ou designers, analisam a situação com base na teoria de jogos não-cooperativa e focam nos incentivos de comportamentos **individuais**.Fazemos isso por meio da observação do ambiente (ecossistema) e das consequências de cada ação.

#### Componentes do Design de Mercado

* Solucionar problemas em mercados existentes por meio de **incentivos**
* Criar decisões individuais estratégicas com base nas interações (**comportamentos**)
* Organizar e entender os mercados por meio de **regras**
* Considerar economia comportamental na interação de usuários (**comportamentos**)

### Design de Mercado: Parte 3 – Por Que Estudar Design de Mercado?

Geralmente, economistas analisam uma situação e fazem previsões de comportamentos e resultados.

Porém, em design de mercado, temos uma abordagem mais proativa. Ao invés de observar como mercados se comportam, podemos projetar como mercados **deveriam** se comportar.

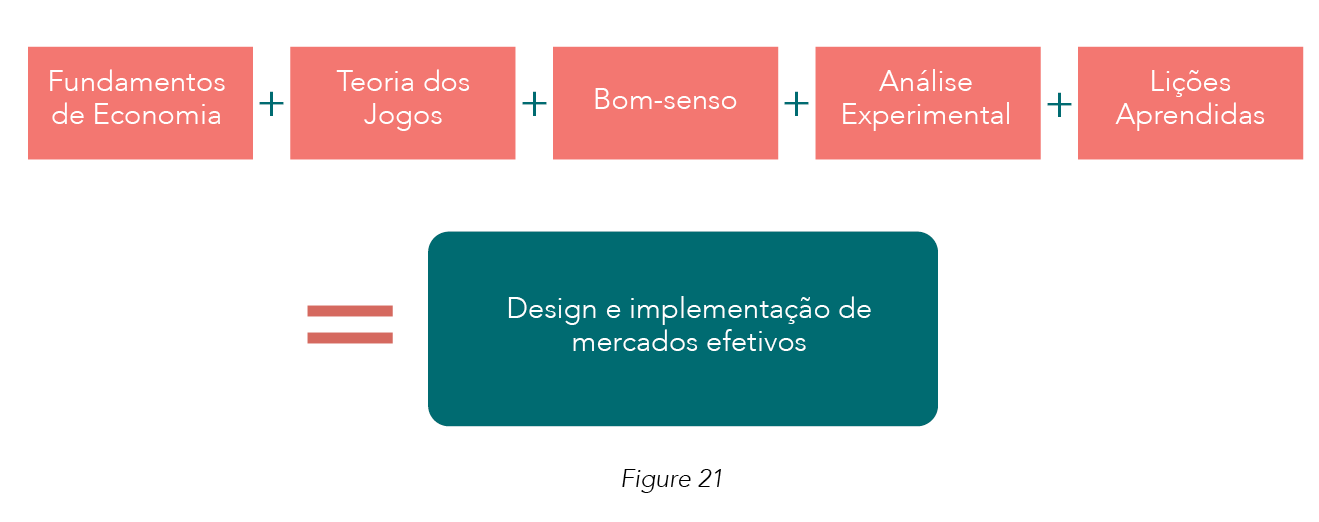


Figura 21

#### Novos Mercados Digitais



Figura 22

Graças à tecnologia, podemos criar “mercados inteligentes”, que determinam resultados com base em dados e variáveis complexas.

Plataformas como a Amazon, por exemplo, oferecem diversas fontes de informação para determinarmos qual produto comprar, como avaliações de outros compradores e sugestões de compra da própria Amazon. Esses mercados nos ajudam a tomar decisões mais inteligentes, com a ajuda de algoritmos projetados para entregar o melhor resultado: comprarmos o melhor produto de acordo com nossas preferências e interesses.

#### Deficiências de Mercado

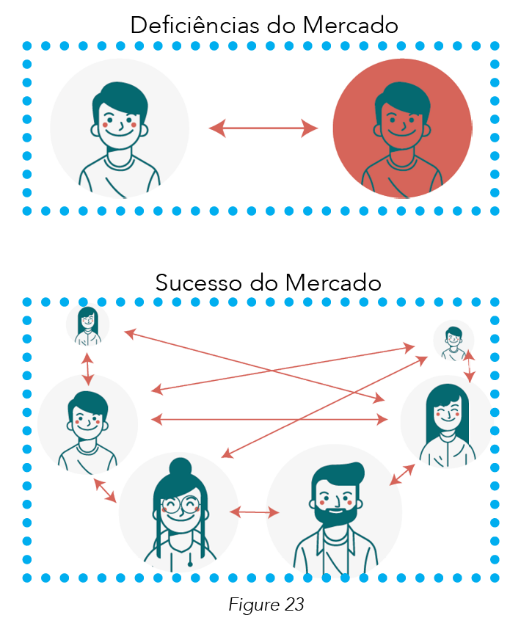


Figura 23

Outra razão para estudarmos design de mercado é o fato de que eles podem fracassar. Podem fracassar na instituição do mercado (ecossistema de token), ou nas mais diversas atividades que o mercado performa (transações). Falhas no design são geralmente a raiz do problema.

Nos novos mercados digitais, estamos falando na maioria das vezes de mercados bilaterais. Mercados bilaterais precisam atrair ambos compradores e vendedores (ex: Amazon).

Nesse caso, queremos encorajar transações dentro do marketplace – ao invés de fora – para evitar resultados ineficientes (deficiências de mercado).

#### Design de Mercado Adequado



Figura 24

Design de mercado adequado permite que a confiança seja construída no ecossistema. Essa confiança vai além da tecnologia.

Confiança incentiva os participantes de compartilharem suas preferências honestas mais facilmente (ver Compatibilidade de Incentivos da Estratégia Dominante e Compatibilidade de Incentivos Bayesiana no Capítulo 3).

Quando participantes **de fato acreditam** que outros (usuários, usuários com autoridade, parceiros do ecossistema) serão honestos, podem confiar que todos estão alinhados e trabalhando para atingir o mesmo objetivo.

Imagine que você e seu parceiro(a) marcaram de cozinhar um jantar para alguns amigos. Um de vocês pode cozinhar, enquanto o outro arruma a casa. Você pode assumir, com certa confiança, que seu parceiro irá cozinhar ou arrumar a casa da melhor forma possível, visto que ambos têm o objetivo de impressionar os convidados e prover uma experiência agradável.

Design de mercado bem-sucedido incentiva usuários a participarem de fato da rede, aumentando o valor do ecossistema.

Vamos analisar os principais fatores necessários para construir melhores modelos de mercado.

### Fatores no Design de Mercado

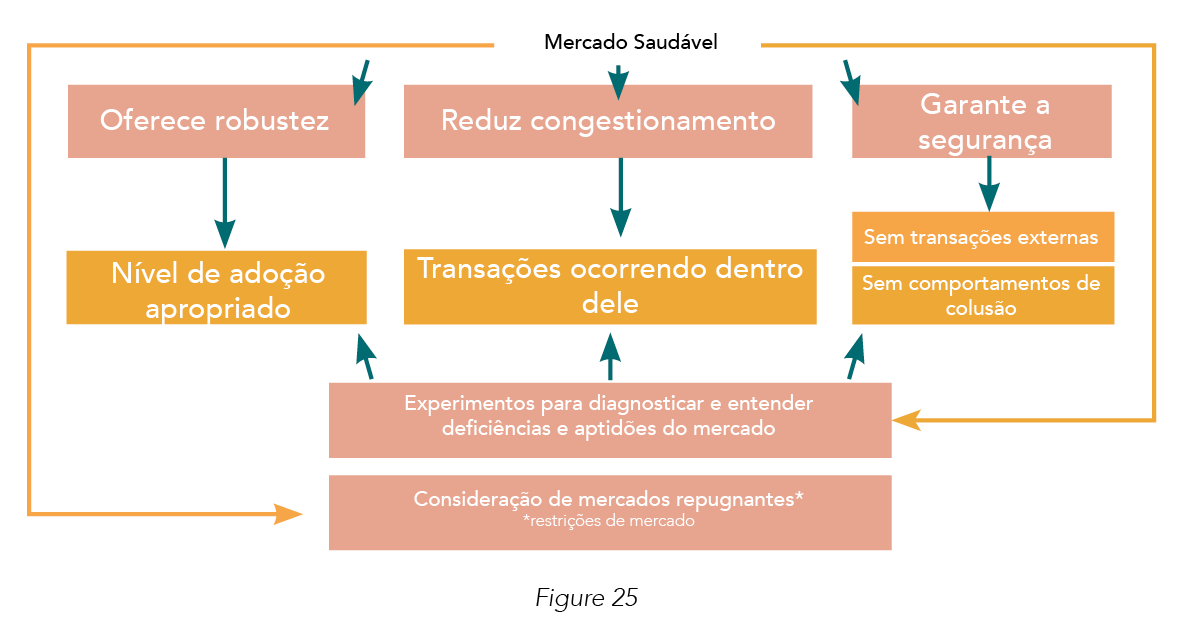


Figura 25

Para ter um bom funcionamento, mercados precisam[[55]](#footnote-56):

* + - 1. Oferecer **robustez**. Mercados precisam atrair participantes suficientes para atingir um nível de adoção apropriado. Não faz sentido ter um ecossistema com meia dúzia de participantes – não terá efeitos de rede.
      2. Reduzir **congestionamento**. Robustez pode aumentar o volume de transações. Precisamos de transações rápidas, e com tempo suficiente para considerar todas as opções alternativas.
      3. Garantir a **segurança**. Compartilhar todas as informações relevantes (ex: eBay precisa compartilhar informações sobre os vendedores e respectivos produtos),
* para evitar transações por fora do marketplace, ou
* para evitar comportamentos estratégicos que reduzem o bem-estar geral
  + - 1. Considerar **mercados repugnantes**. Esses são os mercados que sofrem forte pressão social para que não exista transação alguma por causa de sua natureza (ex: assassino de aluguel, doação de órgãos, tráfico sexual, entre outros). Mais detalhes na seção [6.9.4](#_Additional_Consideration:_Repugnanc).
      2. Realizar experimentos para diagnosticar e entender deficiências e aptidões do mercado por meio de novos designs e comunicação de resultados com os tomadores de decisão.

Precisamos considerar também as oportunidades e comportamentos de **fora do mercado ou ecossistema.** Por mais que não possamos modelar essas questões, é importante tê-los em mente quando estruturando seu próprio mercado.



Figura 26

### Robustez (ou Densidade)

Mercados se tornam robustos quando conseguem acomodar várias transações simultâneas; sendo possível comparar as mais diversas ofertas de negócios (ofertas). Airbnb, por exemplo, oferece opções de casas inteiras, apartamentos, ou quartos, na localidade de sua escolha ou regiões próximas etc.

O principal desafio para atingir robustez está relacionado às externalidades da rede e outras economias de escopo.

### Congestionamento Reduzido

Congestionamento ocorre em mercados quando não há tempo hábil ou informações suficientes para avaliar transações disponíveis em sua totalidade.

Congestionamento é um problema que assombra os mercados de diversas maneiras diferentes. No mesmo exemplo do Airbnb, a plataforma oferece opções parecidas demais, tornando mais difícil a tomada de decisão (paralisia por análise). Airbnb tenta mitigar essa questão por meio da categorização com status de “Superhost” e por meio das avaliações (número de estrelas).

### Segurança & Facilidade de Uso

Caso seja arriscado participar do mercado, participantes individuais podem querer compensar esse risco de formas danosas para o ecossistema ou tentar impedir que suas contrapartes recebam outras ofertas.

Mesmo em mercados robustos, é possível que participantes se comportem de forma indesejada e efetuem transações por fora do ecossistema (*off-chain*).

Por exemplo, hóspedes do Airbnb podem entrar em contato diretamente com os proprietários do imóvel e fechar negócio – sem a necessidade de pagar taxas de serviço e limpeza da plataforma. Para reduzir esse risco, Airbnb adicionou uma funcionalidade de segurança que só cobre danos caso a transação tenha sido fechada e paga dentro da plataforma.

Em ecossistema de token, onde a segurança pode ser analisada por análise de código, camadas de segurança adicionais podem ser inclusas como funcionalidades de privacidade, agilidade criptográfica[[56]](#footnote-57), e códigos algorítmicos revistos por pares.

### Design de Mercado e Economia de Token

Todos os mercados são **diferentes**. Vários fatores constituem os blocos de construção fundamentais para o design de mercado, mas o design de **soluções** pode variar dependendo do ecossistema.

#### Robustez (Tamanho da Rede)

Aproxime todas as partes interessadas em transacionar de forma conjunta. Não se esqueça de considerar o *timing* das transações – quando ofertas devem ser feitas, quanto tempo dura uma transação (ex: período de votação ou período para validação de transações).

1. Mineração (Relevante para o modelo de PoW – ou Proof of Work (Prova de Trabalho)
   1. Incentivar participação na rede por meio de recompensas de bloco (ex: $BTC)
2. Distribuir mais recompensas no início para atrair adoção de pioneiros
3. Parcerias
   1. Fechar parcerias com empresas relacionadas para impulsionar adoção inicial e efeitos de rede (ex: Ethereum Enterprise Alliance)
   2. Tokens para atrair rede de parceiros entre as empresas (protocolos) e usuários – *business to peer*
4. Bônus
   1. Tokens extra ao entrar na rede por meio de códigos de referências – *peer to peer*
   2. *Airdrops*

#### Congestionamento Reduzido

Garanta que há tempo hábil para usuários considerarem todas as opções. Caso contrário, terá opções demais e pouco tempo para a tomada de decisão, gerando congestionamento. Faça com que seu protocolo ajude clientes a tomarem melhores decisões.

Um ótimo exemplo é a Yearn Finance. Utilizam dados *on-chain* para determinar os melhores retornos de juros, onde depositam os fundos dos clientes.

1. Governança de transações
2. Classifique as transações e elimine as transações de baixa qualidade[[57]](#footnote-58) para diminuir o congestionamento
3. Controle de acesso
4. Cobre taxas
   1. Taxas de acesso
   2. Taxas de congestionamento (como pedágios, mas para horários de pico)
5. Controle de validadores
   1. Conjunto fixo de validadores para o consenso (ex: uso de carteiras multi-sig, com mais de uma assinatura requerida)
   2. Seleção randômica de validadores para execução do consenso
   3. Especificação de “super-nós” (validadores) para o consenso (ex: MakerDAO)
   4. Notas Autenticadas por Prova de Autoridade, ou *Proof of Authority* (principalmente utilizado em aplicações de nível empresarial)

#### Segurança & Facilidade de Uso

Simplifique a entrada de participantes e garanta a segurança em transacionar.

1. Resolva assimetria de informação ao:
2. Aumentar a transparência para os participantes (ex: compartilhe mais detalhes sobre as contrapartes antes da transação)
3. Staking
4. Depósito de segurança que pode ser acionado em caso de disputa
5. Imponha *skin in the game* de todos os participantes, para que todos tendam a agir de boa-fé (ex: Synthetix)
6. Funções de privacidade
7. Mecanismos de privacidade como provas de *zero-knowledge* (ex: zCash)
8. “Assinaturas em anel”, ou *Ring Signatures* (ex: Monero)
9. Agilidade criptográfica
10. Segurança pós-quântica (ex: QRLedger, IOTA, Corda)
11. Compatibilidade com hardwares de segurança e administração de chaves
12. Whitepaper revisto por pares (*Peer-reviewed*)
    1. Problemas fundamentais do algoritmo podem ser identificados – no caso de algoritmos tendenciosos, resultados não-randômicos, colisões etc.

#### Considerações Adicionais: Repugnância (ou Aversão)

Em alguns casos, transações repugnantes podem ser feitas com design de mercado adequado. Repugnância[[58]](#footnote-59) refere-se às restrições sociais que previnem uma transação de ocorrer mesmo em preços positivos.

Esses mercados existem porque as transações são consideradas como tabu. Por isso, a maioria delas são feitas fora do mercado padrão de transações – onde compramos ovos ou leite. São transações consideradas imorais.

Exemplos de mercados repugnantes:

* Adoção de crianças
* “Barriga de aluguel”
* Tráfico humano/sexual
* Serviços militares
* Compra de votos[[59]](#footnote-60)
* Poluição
* Transplante de órgãos
* Admissão a escolas/faculdades
* Prêmios Nobel
* Genes ou tecido vivo

BitTorrent, por exemplo. Os *uploaders* fornecem os dados inicialmente enquanto os *downloaders* baixam as informações por meio de várias fontes. Essas transações não utilizam dinheiro para transacionar por conta da filosofia dos participantes, que não apreciam o uso de dinheiro em suas negociações. Mesmo assim, existem formas de administrar os participantes como limitando a velocidade do *download*, ou a quantidade de arquivos limite em cada período, a não ser que ele(a) também contribua com arquivos/informações.

## [Estudo de Caso] Nexus Mutual

Nexus Mutual é um dos principais protocolos de seguro em DeFi.

### O que é o Nexus Mutual

Nexus Mutual é um protocolo descentralizado de seguros baseado na rede Ethereum. Até o Q4 de 2020 (quarto trimestre), cobria apenas riscos de contratos inteligentes na Ethereum.

O token $NXM é usado para alinhar incentivos de vários participantes econômicos do sistema. $NXM é colocado em *stake*, e é utilizado para pagar reivindicações confirmadas de clientes, para votar em decisões de governança, entre outros.

O preço do $NXM é determinado por duas coisas principais: total de $ETH na *pool* de capital e índice de capital mínimo requerido (CMR, ou *MCR* em inglês). A determinação é feita por meio de funções de “Curvas de Ligação”, ou *bonding curves*.

### Primeiros Passos com $NXM

**Diretamente**

Participação direta requer a entrada no ecossistema da Nexus Mutual e o pagamento de uma taxa de inscrição. Só membros podem comprar cobertura de seguros, realizar o *staking*, e participar da governança.

Ao comprar cobertura de seguros na Nexus Mutual, usuário escolhem:

1. Ativos a serem cobertos
2. Termos da apólice
3. Limite da apólice

**Indiretamente**

Participação indireta por meio da compra de versões “embrulhadas” (*wrapped*)do token nativo $NXM, chamado de $wNXM.

Podemos comparar esse sistema com os tokens $BTC e $wBTC. Um custodiante retém $BTC e emite $wBTC, uma versão embrulhada do bitcoin que pode interagir com contratos inteligentes. Da mesma forma, investidores podem comprar $wNXM ao invés do token nativo $NXM. Isso evita compradores de terem que passar por processos de KYC (conheça seu cliente) e pagamento de taxas de inscrição.

Tokens $NXM nativos não são negociáveis no mercado secundário pois o processo de KYC da Nexus Mutual exige que indivíduos detentores do token passem pela identificação e realizem o pagamento da taxa de inscrição. Com a funcionalidade de resgate de $NXM para cada unidade de $wNXM, porém, é possível contornar todo esse processo. $wNXM pode ser comprado/vendido em corretoras como Uniswap.

### Como a Nexus Mutual Funciona?

Ecossistema da Nexus Mutual possui três tipos de participantes:

1. **Compradores de Cobertura de Seguros**: Pagaram pela adesão e têm o direito de comprar cobertura de seguros com $NXM.
2. **Avaliadores de Risco**: Examinam códigos e outras informações sobre um projeto. Verificam se os contratos inteligentes estão bem-feitos e sem bugs/vulnerabilidades.
3. **Avaliadores de Reivindicações**: Votam para aceitar ou rejeitar reivindicações para pagar os assegurados (compradores de cobertura de seguros) caso algo aconteça.

*Nexus Mutual é uma plataforma que agrega e coordena os participantes acima, a cobertura de seguros, e os fundos disponíveis para facilitar o seguro.*

Como exemplo aleatório, 0.5 $ETH poderia ser utilizado (pago na cobertura) para assegurar 300.000 $ETH possuídos na Aave. Nexus Mutual coloca esses 0.5 $ETH em uma grande *pool* de fundos, contendo taxas de inscrição e prêmios recolhidos, assim como $NXM em *stake*. Essas taxas são utilizadas para cobrir atividades asseguradas válidas, como empréstimos na Aave, e recompensar os avaliadores de risco e reivindicações (vide 7.1).

#### Qual o Papel dos Avaliadores de Risco?

Avaliadores de risco examinam protocolos de DeFi que são de alguma forma cobertos pelas políticas de seguros da Nexus Mutual.

Avaliadores de risco adquirem $NXM. Eles podem tanto segurar os $NXM e aguardar para valorização de preço, ou colocar os $NXM em *stake* com base na sua expertise na *pool* de um protocolo específico. Essa é a liquidez disponível para pagar os assegurados caso perdas monetárias sejam realizadas por conta de erros no contrato inteligente. Em retorno, os prêmios pagos pelos comprados de seguros são distribuídos para os avaliadores de risco que examinaram os códigos e forneceram liquidez na *pool* do protocolo específico.

**Processo dos Avaliadores de Risco**

1. Aprofundamento técnico de um protocolo.
2. Verificar que os contratos inteligentes estão livres de bugs e vulnerabilidades.
3. Colocar $NXM do próprio bolso em *stake* na *pool* de cobertura de seguros específica do protocolo.
4. Prêmios são pagos aos avaliadores de risco que colocaram $NXM em *stake* na *pool*. Caso o pagamento para assegurados seja necessário, virá dessa mesma *pool* de liquidez que os avaliadores depositaram.

Avaliadores de risco fazem isso pois estão apostando que seu conhecimento específico dos contratos inteligentes daquele protocolo é suficiente para determinar a inexistência de bugs e vulnerabilidades, e que as chances são baixas de existirem reivindicações válidas de seguro para deduzir de seu montante contribuído. Eles são como “hackers do bem” (ou *white hat hackers*[[60]](#footnote-61)), mas ao invés de especialistas de segurança cibernética, são especialistas em contratos inteligentes.

Sem uma plataforma como a Nexus Mutual, o conhecimento advindo da identificação de vulnerabilidades e bugs feita por avaliadores serviria apenas para uso próprio. Com a plataforma, é possível terem retorno financeiro por sua experiência, *expertise*.

Membros normais do ecossistema podem pagar taxas baixas para assegurar suas transações. Caso um bug aconteça, a *pool* formada pelos avaliadores de risco cobre as perdas.

Visto que os especialistas haviam auditado os contratos inteligentes e determinaram a inexistência de bugs, o seguro pago pelos assegurados não é distribuído para os avaliadores de risco.

#### Qual o Papel dos Avaliadores de Reivindicações?

Avaliadores de reivindicações fazem exatamente o que diz no nome: avaliam reivindicações/sinistros.

Eles analisam as declarações de sinistro e decidem na aprovação/reprovação.

Avaliadores de reivindicações também precisam colocar $NXM em *stake* para participarem. Eles colocam $NXM no *stake* em forma de voto, como “aprovado” ou “reprovado”. A resposta final é determinada pela maioria de votos dos avaliadores de reivindicações.

A resposta da maioria pode ser aprovado, “isso é um erro e será assegurado pela Nexus Mutual”, ou reprovado, “não há erros e portanto não possui cobertura da Nexus Mutual”.

* Avaliadores que votarem contrários à maioria terão seus tokens travados por um período determinado.
* Avaliadores que votarem conforme a maioria receberão os tokens colocados em *stake* de volta, além de $NXM adicional.

### Aplicando Design de Mercado na Nexus Mutual

Recapitulando: design de mercado define o ambiente em que usuários e tokens coexistem para que seja eficientemente operado e administrado. Falamos também sobre efeitos de rede, sugerindo que design de mercado é um pré-requisito para alcançá-los. Mercados bem estruturados (i.e. bom ambiente de ecossistema) encorajam maior participação dos usuários e aumentam o valor gerado no ecossistema.

Em resumo, design de mercado analisa três fatores:

* Robustez do mercado
* Congestionamento reduzido
* Segurança e facilidade de uso



Figura 27

### Robustez do Mercado

Robustez é o nível de adoção do mercado. Demanda por seguros em DeFi é diretamente dependente da prévia adoção de cripto e DeFi em geral. O mercado de seguros em DeFi só se tornará robusto com certo nível de adoção. Caso DeFi falhe em atingir maturidade de mercado ou adoção, Nexus Mutual terá muita dificuldade em escalar.

Robustez de mercado depende principalmente do aumento no tamanho da rede de usuários do sistema (B2B, empresa para empresa) e do aumento no número de participantes (B2C, empresa para consumidor).

#### Mercado B2B (empresa para empresa)

Nexus Mutual oferece seguros a outros protocolos que também poderiam se beneficiarem por meio dele. Vamos olhar dois exemplos de sistemas que “reembalam” seguros da Nexus para benefício próprio.

O primeiro é a **Yinsure** Finance. Yinsure pega as coberturas de seguro que a Nexus Mutual oferece, cria uma oferta própria *white label*[[61]](#footnote-62), e vende em seu ecossistema.

O segundo é o **Cover** Protocol[[62]](#footnote-63). Ao invés de pegar os seguros da Nexus Mutual e transformar em *white label*, eles transformaram o protocolo inteiro em um marketplace *white label* e *peer-to-peer* que vende não só os seguros da Nexus Mutual, mas também para outras coisas não oferecidas pela Nexus.

#### Mercado B2C (empresa para consumidor)

No mercado B2C, Nexus Mutual busca aumentar a base de usuários ao estruturar diversas funções e responsabilidades para os participantes. Existem quatro funções básicas do token $NXM:

1. Membros podem comprar seguros
2. Membros podem ser assessores de risco
3. Membros podem ser assessores de reivindicações
4. Membros podem participar na governança

Ao expandir as oportunidades de participação, Nexus Mutual atrai mais usuários para a plataforma e aumenta o envolvimento pessoal/emocional dos participantes na plataforma – motivando a compra de mais $NXM.

Com o crescimento de DeFi e conforme mais pessoas interagirem com os protocolos que a Nexus Mutual cobre, o protocolo terá crescimento orgânico de usuários. Com mais protocolos desenvolvidos, e maior demanda de assessores para analisar contratos inteligentes, maior volume de propostas de melhorias. Nesse momento a competência de governança se torna importante, e participantes utilizam seus $NXM para votar. Dessa forma aumentam a participação de compra no nível B2C – quase um modelo *peer-to-peer*, consumidor para consumidor.

### Congestionamento Reduzido

Nexus Mutual cria um ambiente amigável a participação de todos os agentes. Participantes podem escolher livremente a competência que desejam exercer, com a única condição de adquirir e colocar em *stake* o token nativo do protocolo - $NXM.

Para prevenir ações indesejadas (fraudes) de usuários assegurados, assessores de reivindicações possuem um período mínimo de espera de 12 horas entre cada avaliação.

Contratos inteligentes da Nexus Mutual garantem que, caso um assessor complete a avaliação de um contrato inteligente do protocolo Aave, terá que esperar no mínimo 12 horas antes de iniciar outra avaliação – mesmo em outro protocolo. Isso limita usuários assegurados submeterem múltiplas alegações de sinistros fraudulentas para tentarem explorar o sistema.

### Segurança & Facilidade de Uso

#### Segurança por Design

O design do token $NXM, da Nexus Mutual, sinaliza os riscos. **Compradores de seguros** só conseguem adquirir cobertura quando há assessores suficientes oferecendo seus tokens (em *stake*) para sinalizar que o protocolo é seguro.

*A existência de ofertas de seguros sinaliza que o protocolo foi auditado por um terceiro, o que fortalece a sinalização de segurança.*

Quando uma reivindicação é submetida, um grupo de vários usuários (**assessores de reivindicações**) é mobilizado para determinar a validade da alegação. Votação dos assessores precisa atingir consenso mínimo de 70% para confirmar o pagamento do seguro. Caso contrário, voto será direcionado para a plataforma como um todo, e a decisão será por contribuição coletiva (*crowdsourcing*).

#### Determinação de Preço

O preço do $NXM é definido pela matemática da “curva de ligação”, ou *bonding curve*, reduzindo especulação.

Além disso, a curva de ligação é determinada por dois fatores – variáveis de curto e longo prazo. Investidores podem interpretar o preço do $NXM como indicador de curto prazo (capital total) ou longo prazo (Capital Mínimo Requerido, ou *MCR*[[63]](#footnote-64)) em suas previsões. $NXM utiliza essas variáveis em seu modelo de valor intrínseco.

#### KYC e Adesão

Nexus decidiu seguir as diretrizes de regulamentação da Inglaterra como companhia mútua. Usuários precisam passar pelo processo de KYC (conheça seu cliente) e pagar uma pequena taxa de adesão para comprar o token $NXM. Isso reduz os riscos de a empresa ser contestada pelo governo.

#### Facilidade de Uso

Tirando detalhes de interface e experiência do usuário (*UI/UX*), membros podem comprar cobertura de seguros de forma relativamente fácil no sistema. O dashboard de membros também ajuda a entender visualmente a situação do ecossistema.

## Design de Mecanismo

*Esse é o segundo pilar do design de ecossistemas de token.*

### Design de Mecanismo: Parte 1 - Introdução

Design de mecanismo define as regras[[64]](#footnote-65) do ecossistema.

Essas regras existem para governar as ações dos participantes. Podem estar embutidas no código de contratos inteligentes ou utilizar regras comportamentais (voto, consenso).

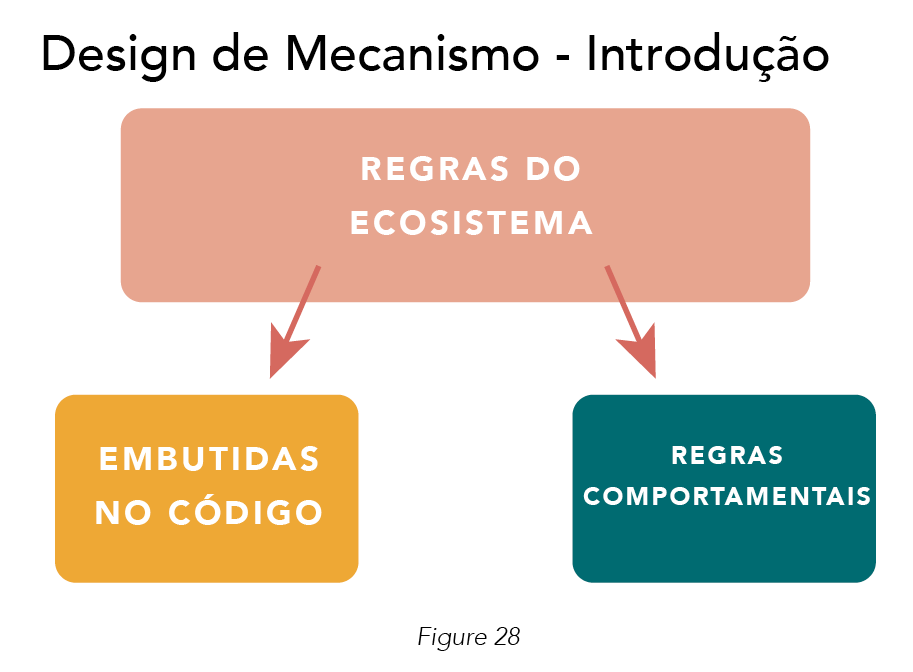


Figura 28

### Por que Precisamos de Design de Mecanismo?

No primeiro pilar, aprendemos que design de mercado define o ambiente para participantes interagirem e transacionarem entre si. O segundo pilar – design de mecanismo – irá definir as regras de comportamento **dentro** desse ambiente.

Esse conceito é aplicável para além de ecossistemas digitais descentralizados. Qualquer instituição, mercado, ecossistema, ou empresa, pode se beneficiar de regras[[65]](#footnote-66). Design de mecanismo impõe regras que, junto com a dinâmica do ambiente, determinam como atingir o objetivo do ecossistema.

Design de mecanismo é um dos instrumentos na caixa de ferramenta de um designer econômico. Por mais que não exista uma fórmula geral para o design de mecanismo, vamos estudar esse pilar por meio de vários fatores.

### Por que é Importante para Ecossistemas de Token?

Mecanismos bem estruturados impactam na sustentabilidade a longo prazo de ecossistemas de token descentralizados.

Design de mecanismo é importante pois influencia as ações e comportamentos de pessoas na rede. Além disso, busca incorporar mudanças e novas preferências do ecossistema, fatores cruciais para um design eficiente de mecanismo.

Usamos o design de mecanismo também para entender quais são os mecanismos ideias para cada tipo de participantes (agente econômico). No Capítulo 3, discutimos o fato de participantes diferentes terem incentivos diferentes, especificamente na seção 3.5.4. Em outras palavras, busca entender quais os melhores mecanismos para cada participante e encontrar mecanismos apropriados para responder aos diversos incentivos no ecossistema.

### Design de Mecanismo: Parte 2 – O Que é?

Design de mecanismo é o processo que cria as regras do ecossistema. Estabelece o framework para análise de um ecossistema, mercado ou instituição. Busca entender os problemas associados com incentivos e informação privada (hipóteses, informação confidencial, expectativas).

Design de mecanismo é necessário pois existem muitos tipos de participantes em um ecossistema, com objetivos diferentes e, portanto, mecanismos de incentivos diferentes. Queremos alinhá-los com regras ou incentivos (vide 3.1), para que ninguém se beneficie às custas de outro (ex: Maria não ganha nada a mais pelo fato de João perder algo – jogo de soma-zero).

Foco é total em incentivos e comportamentos de participantes. O objetivo é otimizar as regras do ecossistema para incentivar comportamentos desejáveis e desincentivar os indesejáveis.

#### O Que Design de Mecanismo Engloba?

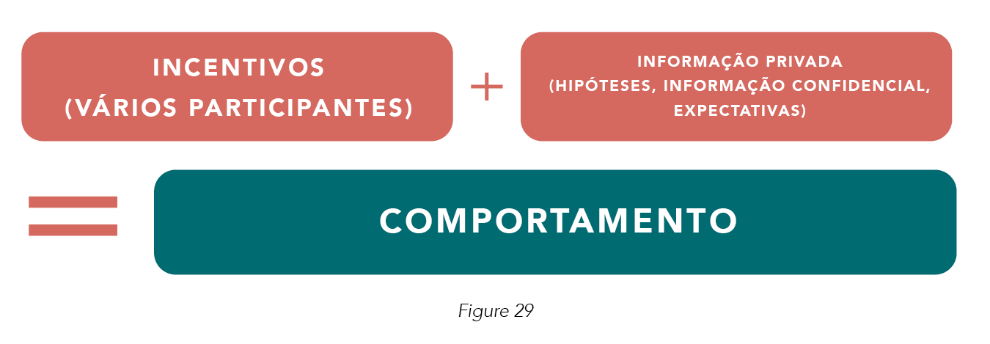


Figura 29

Design de Mecanismo:

* Alinha objetivos distintos de vários tipos de participantes por meio de incentivos
* Revela preferências privadas de usuários
* Influencia o comportamento de usuários

### Design de Mecanismo: Parte 3 – Por que estudar?

Precisamos de regras para governar jogos que jogamos e ações que tomamos. A finalidade é de alinhar incentivos de todos os participantes. Não é uma tarefa fácil no mundo centralizado, e mais difícil ainda no mundo descentralizado.

No mundo “real” centralizado, entidades centralizadoras (ex: governo, banco central, conselho de administração) podem agir de forma conjunta e pontual para resolver problemas conforme eles aparecem. Porém, no mundo descentralizado, especialmente em ambientes de governança distribuída (como nas DAOs), é necessário estabelecer as regras **antes do tempo** para desincentivar comportamentos negativos e garantir a saúde econômica do protocolo.

Meta (dona do Facebook), por exemplo, é uma entidade centralizada. Eles possuem autoridade para banir sua conta ou remover um post, caso você faça postagens que violem suas políticas – e em alguns casos, até mesmo sem nenhuma violação.

A maioria dos ecossistemas descentralizados não possui autoridade centralizadora para tomar decisões, e precisam ser definidas ou estipuladas em código com antecedência. Quem possui a palavra final para remover uma conta? Como comunidades podem expurgar agentes negativos? Como podem incentivar participação contínua de agentes positivos?

Por isso design de mecanismo (ou regras) é tão crucial. Com ponderação suficiente, pode resolver a maioria dessas preocupações automaticamente, especialmente as ações de boa-fé.

#### O que estamos fazendo em Design de Mecanismo?

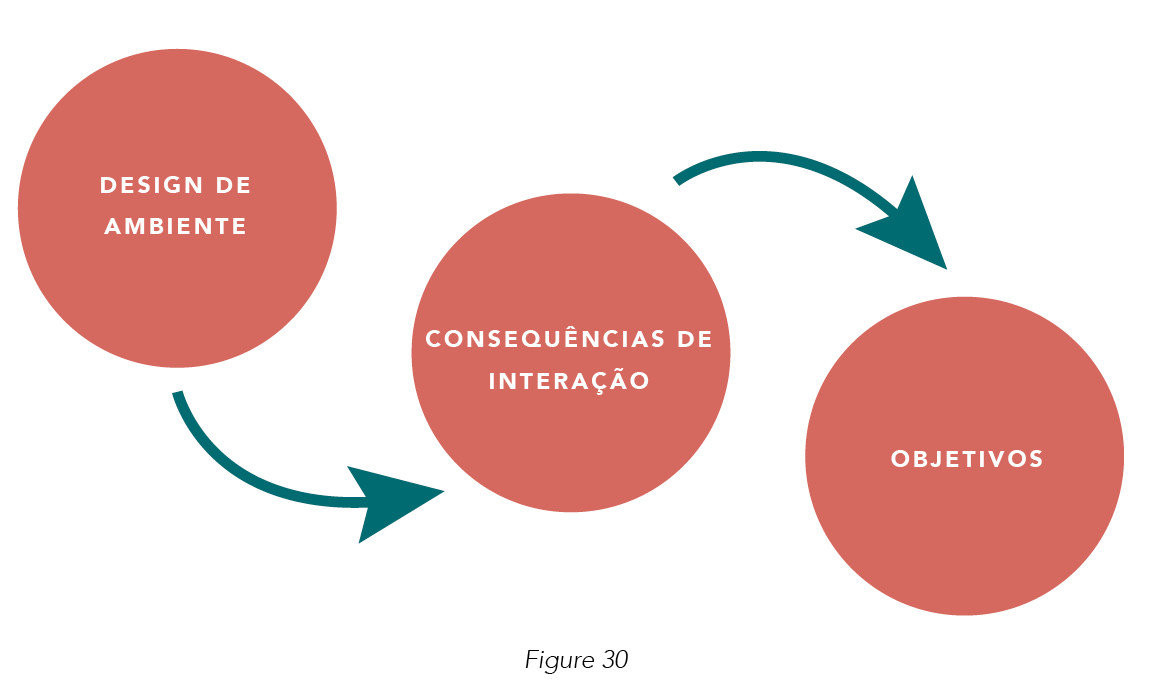


Figura 30

Design de mecanismo estuda a estrutura de instituições, mercados, e ecossistemas (i.e. ambiente) para entender como ela impacta no resultado das interações entre instituições/participantes (i.e. comportamentos), ajudando a alcançar os objetivos (i.e. consequências).

#### Premissas Provisionais

Por mais que pessoas sejam imperfeitas e irracionais, geralmente assumimos que irão agir da melhor maneira em benefício próprio, de acordo com as informações privadas que possuem. Essa é uma premissa muito forte.

Por meio do design de sistemas gamificados que discutimos no Capítulo 2, podemos fortalecer ainda mais essa premissa. Mas para essa camada de design econômico, vamos assumir essa premissa, considerando todo o resto constante (*ceteris paribus*).

#### Função de Escolha Social

Função de escolha social é a análise de vários fatores para atingir uma decisão ou resultado coletivo. Isso pode ser por meio da maximização de utilidade, minimização de custos, redução de tempo gasto, aumento do nível de felicidade, garantia de igualdade entre participantes etc.

No mundo real, somos governados por um conjunto de leis sob uma constituição (pelo menos no mundo democrático).

Função de escolha social é importante pois queremos tomar decisões coletivas e atingir metas socialmente aceitáveis para todos (escolha social). Podemos analisar, por meio da função de escolha social, se nossa decisão ou design de mecanismo é eficiente.

#### Design de Mecanismo Adequado

Os efeitos esperados em um bom design de mecanismo dependem dos objetivos que querem alcançar.

Pode incluir:

* Eficiência de Pareto[[66]](#footnote-67)
* Mecanismos à prova de estratégia[[67]](#footnote-68)
* Justiça[[68]](#footnote-69)
* Objetivos gerais representados pela função de bem-estar social de Bergson-Samuelson[[69]](#footnote-70) que permite compensações entre eficiência e igualdade.

Não há regras fixas ou fórmulas perfeitas para criar os mecanismos, conforme dito anteriormente. Porém, temos direcionamentos para os primeiros passos a se tomar inicialmente.

### Primeiros Passos

1. Definir o problema que precisa ser resolvido
2. Determinar a meta social que precisa ser atingida
3. Entender as restrições/limitações existentes

Já discutimos esses pontos antes no Capítulo 4, com objetivos e restrições. Na criação de mecanismos, às vezes vamos mais à fundo em objetivos e restrições para especificar as **metas** e restrições. Também é possível colocá-las em fórmulas matemáticas, caso necessário.

### Fatores no Design de Mecanismo

Design de mecanismo é complexo. Vai desde a teoria do equilíbrio geral até ambientes não clássicos. Em alguns casos, pode ser usado na criação de teorias de normativa geral para política econômica.

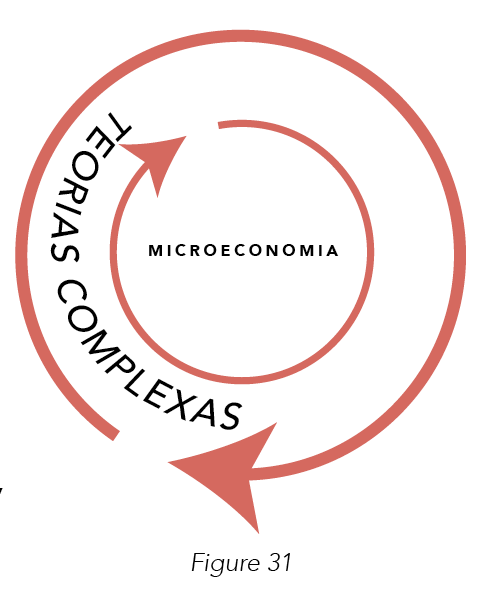


Figura 31

Mas, vamos começar pelo mais simples.

O modelo econômico de token possui diversos fatores que devem ser ponderados na estruturação dos mecanismos. Vale lembrar que, dependendo do ecossistema descentralizado em questão, nem todos os fatores serão igualmente relevantes. Depende da função, caso de uso, modelo de negócios, entre outros.

Três principais fatores do design de mecanismo são:

1. Governança
2. Incentivos não-financeiros
3. Estrutura

#### Governança

Governança é a parte que define como decisões são tomadas e problemas são resolvidos. Revisitando o tópico de contratos incompletos, é fato que muitos imprevistos podem ocorrer ao longo do tempo que não estão embutidos nas “regras do ecossistema” (i.e. design de mecanismos). Governança é a parte do modelo de mecanismo que lida com a tomada de decisão e resolução de conflitos, mesmo se não forem tratados pelos contratos inteligentes.

O **protocolo de consenso** determina como decisões são tomadas. Processo geralmente manual.

O **mecanismo de resolução** determina como conflitos são resolvidos. Geralmente feito por meio de contratos inteligentes automatizados.

#### Incentivos Não-Financeiros

Economia de token é sinônimo de incentivos. Além de incentivos financeiros como recompensas monetárias, incentivos não-financeiros tem grande importância no design de mecanismos. Isso inclui a forma que votações ocorrem (mecanismo de votação) e como o ecossistema aloca seus recursos.

O **protocolo de votação** determina como votações são realizadas. Processo geralmente manual.

O **mecanismo de alocação** determinar como o ecossistema aloca seus recursos. Geralmente feito meio de contratos inteligentes automatizados.

#### Estrutura

Estrutura de mecanismo tem relação com a forma que os participantes transacionam entre si e como o ecossistema coleta informações de forma justa e descentralizada para conectar os mundos *on-chain* e *off-chain*.

O **protocolo de barganha** determina como as pessoas transacionam entre si. Processo geralmente manual.

**Informação da comunidade** refere-se à forma que o ecossistema se conecta com o mundo *off-chain*. Geralmente feito meio de contratos inteligentes automatizados.

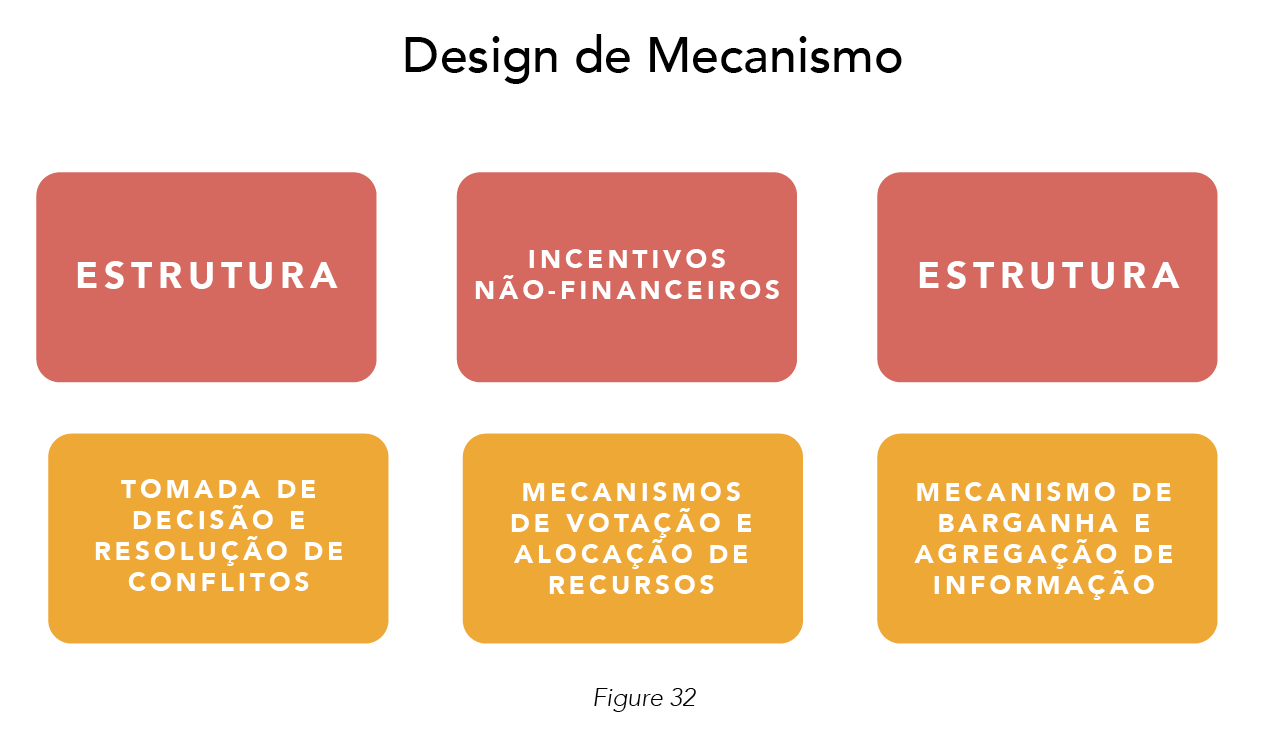


Figura 32

No contexto de ecossistemas de token, design de mecanismo precisa:

* + - 1. Oferecer **governança** adequada. Em ecossistemas descentralizados, governança é absolutamente importante na administração de ações de participantes no ecossistema.

1. Incluir **incentivos não-financeiros**. Incentivos financeiros serão discutidos no próximo pilar, em design de token. Outros incentivos precisam ser considerados para levar em conta preferências e assimetrias de informação.
2. **Estrutura** do design de mecanismo. Os melhores mecanismos são eficientes conforme teoria de Pareto para proteger seus ecossistemas, enquanto preservam seu objetivo principal.

### Governança

Ecossistemas e mercados existem para coordenar atividades entre participantes no mercado. Isso é muito mais simples em ecossistemas centralizados pois a autoridade central tem a última palavra.

*O debate sobre centralização vs. centralização sugere que um certo nível de centralização é útil. No caso de hack da KuCoin em setembro de 2020, os hackers tiraram os fundos da corretora centralizada e trocaram para outros ativos.*

*Desenvolvedores de alguns protocolos decidiram executar um fork no código para devolver os tokens, como o Ocean Protocol (híbrido de centralizado/descentralizado), enquanto outros seguiram em frente, como a Synthetix (totalmente descentralizada).*

Em ecossistemas descentralizados, não existe uma “última palavra” centralizada. Portanto, sistemas de governança efetivos se tornam ainda mais importantes.

Governança pode facilitar transações e atividades no ecossistema, tornando a participação mais segura e prevenindo congestionamento quando conflitos aparecem. Pode tomar diversas formas, incluindo legislação e design de contratos (inteligentes).

Governança pode restringir o ecossistema de diversas formas, dependendo da função do token, caso de uso e objetivo. Isso pode tanto mitigar uma centralização excessiva, como contratos inflexíveis, protocolos de consenso, e regulamentações e leis de várias jurisdições. Governança não está limitada a contratos inteligentes, mas inclui também mecanismos de resolução, protocolos de consenso e outras camadas de governança.

**Exemplos do mundo real**

Governança está diretamente ligada ao processo de tomada de decisão:

* Como países são governados
* Como empresas tomam decisões

### Incentivos Não-Financeiros

Dependendo de quão atrativos sejam os incentivos financeiros, incentivos não-financeiros podem fazer parte das estratégias de mecanismo. Esse tipo de incentivo fortalece mecanismos de incentivos compatíveis para atingir o objetivo.

Incentivos não-financeiros buscam reduzir assimetria de informação ou reforçar a estratégia desejada no design de incentivos. Incentivos não-financeiros podem alcançar resultados óptimos por meio do endereçamento de mecanismos envolvidos e na observação de consequências de cada ação.

Reputação é uma variável importantíssima para reduzir a assimetria de informação e incentivar participantes a compartilharem suas informações de forma honesta, reduzindo a quantidade de informações ocultas (risco moral) nas transações do ecossistema.

Incentivos não-financeiros são cruciais, visto que contratos incompletos são inevitáveis. A maioria dos ecossistemas são contínuos e dinâmicos, e algumas situações são difíceis de prever ou descrever com antecedência. E mesmo se for possível prever, pode ser um grande desafio a incorporação desses mecanismos no design.

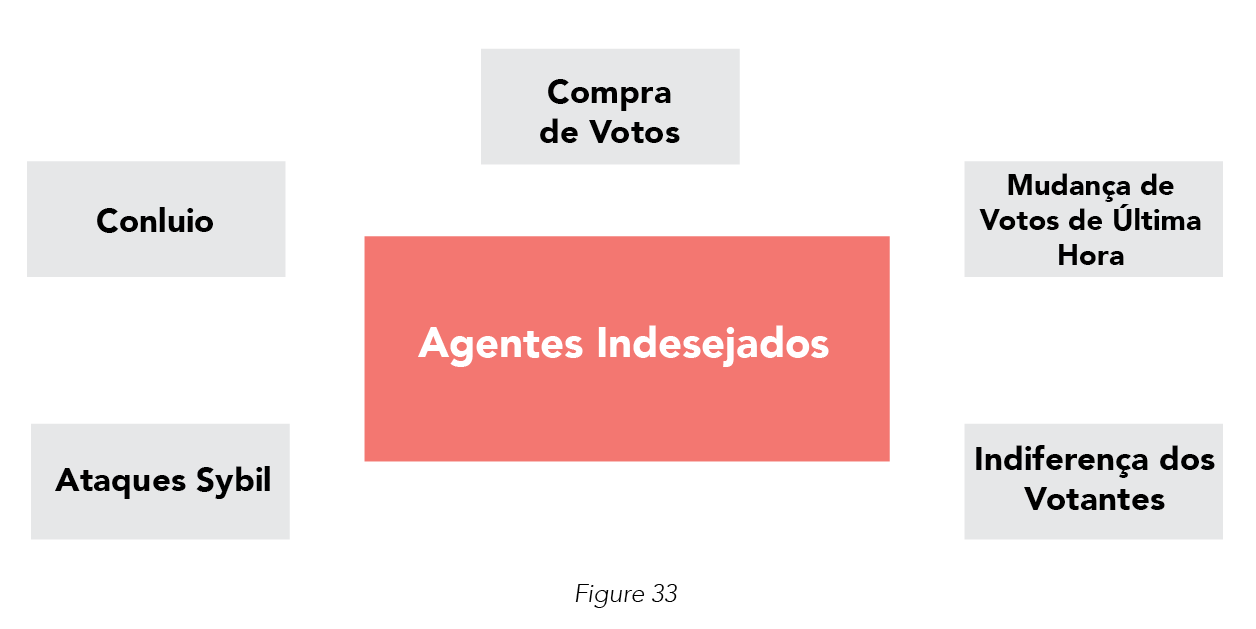


Figura 33

Ao mesmo tempo que queremos incentivar participantes a fazerem parte do ecossistema, queremos também usar esses mecanismos para desincentivar agentes indesejados. Comportamentos indesejados típicos incluem a compra de votos, plutocracia, mudanças de voto de última hora, e indiferença dos votantes.

Portanto, outros princípios econômicos e princípios da teoria da complexidade de engenharia são necessários. Princípios fundamentais têm origem em mecanismos microeconômicos, que buscam entender o motivo de pessoas se comportarem como se comportam. Teoria da complexidade tenta entender como sistemas descentralizados funcionam em sua natureza. Ecossistemas de token estão evoluindo constantemente e se adaptando a novas informações. Por isso, ao invés de ecossistemas estáveis com mecanismos fixos ou modelos estatísticos aplicados para encontrar equilíbrios, precisamos observar como participantes se adaptam em ecossistemas dinâmicos e descentralizados, por meio da observação de ações prévias e fazendo previsões para possíveis resultados futuros.

**Exemplos do mundo real**

* Status de “Superhost” no Airbnb incentiva usuários a alugarem suas propriedades. Boas avaliações por conta de alto nível de serviço e acomodações limpas para seus clientes, assim como fotos de alta qualidade, reduzem a assimetria de informação.
* Incentivos não-financeiros não afetam diretamente ou imediatamente os participantes, mas afetam no longo prazo, especialmente quando as interações são repetidas.

### Estrutura

Estrutura de mecanismos nos ajuda a determinar como os diferentes grupos de informação se relacionam entre si em um ecossistema. Facilita na coordenação de transações dentro do sistema e mitiga conflitos quando eles aparecem. Idealmente, queremos estruturar um mecanismo eficiente.

Dado que precisamos entender como informações e dados se relacionam entre si (*on-chain*, para *off-chain* e vice-versa, ou até mesmo *on-chain* para *on-chain*), temos que considerar fatores como a cadência de transações entre participantes, a possibilidade de participantes grandes e influentes (i.e. os chamados “baleias”), arbitragem, e barganha.

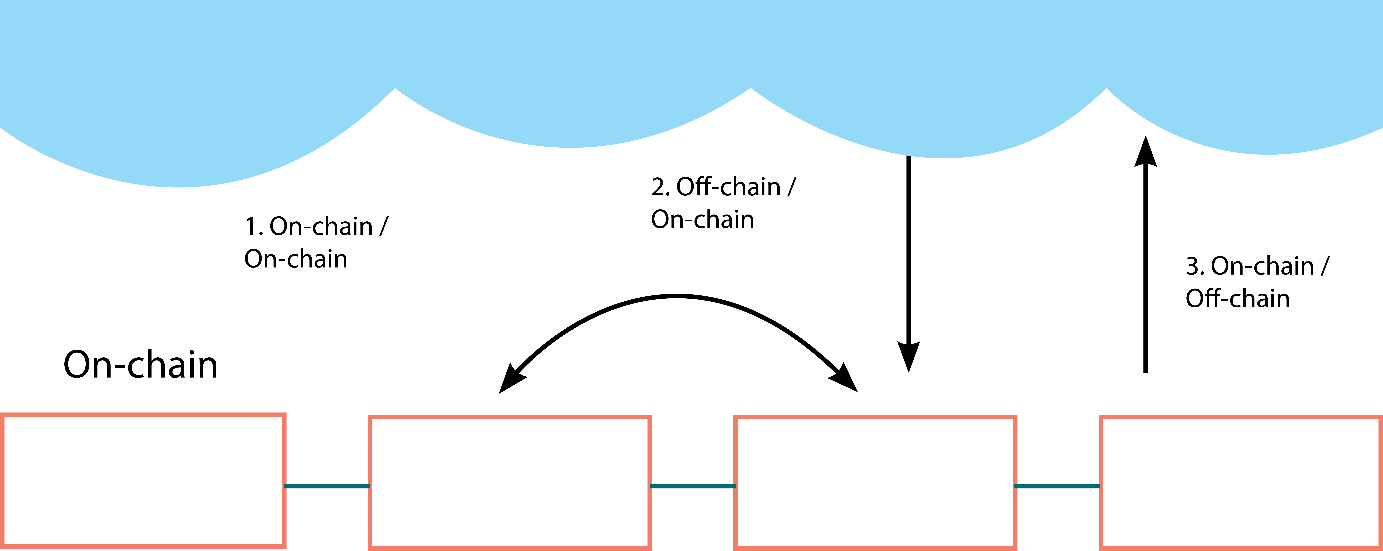


Figura 34

Um dos principais problemas com estrutura de mecanismos é quando temos funções de resultado diferentes (ex: objetivos de investidores/especuladores vs. objetivo de usuários). Não está claro ainda se teorias tradicionais de design de mecanismos seriam úteis nesse contexto, ou se abordagens por meio de análises específicas do mecanismo seriam mais adequadas. De qualquer forma, foi exatamente por meio da exploração de funcionalidades especiais de diferentes contextos econômicos que houve a geração de novos insights valiosos.

**Exemplos do mundo real**

Estrutura depende da indústria, caso de uso e objetivos. Design de estrutura pode variar drasticamente, caso a caso.

Ações coletivas

Ações coletivas são processos iniciados por um grupo que possui reivindicação de injustiça. Contratam um advogado para defendê-los no caso contra outra parte, geralmente uma empresa.

O advogado é pago pelo esforço que coloca no caso. Dependendo da habilidade de observar os esforços do advogado, a estrutura de compensação difere. Pode ser pelo método de Lodestar (cobrado por hora ou por outra matriz observável) ou baseado em uma taxa de contingência (geralmente 35% nos Estados Unidos) quando a observação de esforços não é possível.

Por um lado, é logisticamente mais simples implementar o método de Lodestar, mas custos de administração são altos. Por outro, é mais fácil para advogados burlarem o acordo caso não seja possível observar seus esforços.

A solução depende do nível de visibilidade que clientes possuem sobre as atividades do advogado.

Esse é apenas um pequeno estudo de caso específico da indústria advocatícia. Estrutura é altamente dependente de outras variáveis. A próxima seção possui exemplos simplificados e sugestões iniciais para você.

### Design de Mecanismo e Economia de Token

Todos os ecossistemas são **diferentes.** Esses fatores diferenciais formam os blocos de fundação para a criação dos mecanismos.

Ecossistemas possuem duas camadas:

1. Mecanismos automatizados em código (ex: contratos inteligentes e algoritmos[[70]](#footnote-71)).
2. Mecanismos dinâmicos que requerem contribuição de participantes do ecossistema.

#### Governança (Regras e Estratégias)

Governança descentralizada em ecossistema de token requer equilíbrio entre automação e contribuição humana.

Protocolo de tomada de decisão (participantes têm voz nesse processo)

1. Várias camadas descentralizadas de governança, em caso de falhas externas, com objetivos diferentes (ex: requerimento mínimo de tokens em *stake* para suportar uma proposta antes que seja submetida à votação)
2. Interação honesta entre participantes
   1. Mecanismo de TCR (*Token Curated Registry*, ou Registros Curados de Tokens) para revelar o real valor
   2. TCR em camadas
   3. Detalhes do design (ex: DAOs)

2) Mecanismos de resolução (mecanismo automatizado)

a) Contratos inteligentes: predefinidos no sistema (ex: fundos serão automaticamente pagos quando condições forem cumpridas)

b) Pontos focais, ou Pontos de Schelling

|  |
| --- |
| Caixa 1: DAOs, O Futuro da Governança Descentralizada  Conforme o mundo se aproxima da digitalização, muitas coisas estão mudando. Isso inclui governança. Conceitos econômicos organizam e coordenam recursos em nossa economia. Governança no sentido econômico busca organizar e coordenar a **tomada de decisão** em nossa economia. Introduzindo as DAOs, uma nova forma de organizar nossa cada vez mais dinâmica economia!  **Lacunas da Governança Tradicional**  Existem muitas lacunas na governança centralizada. Execução ineficiente, desalinhamento de incentivos, minoria com pouca voz. Uma possível solução, quando possível, é a descentralização com tomada de decisão autônoma, com automação e execução por máquinas.  DAOs — *decentralized autonomous organizations*, ou Organizações Autônomas Descentralizadas são uma manifestação dessa solução.  Por mais que abordamos o tópico de DAOs relacionado a blockchain, essas organizações também podem existir em ambientes fora da tecnologia blockchain. Podem funcionar em qualquer ambiente digital ou plataforma.  DAO é basicamente uma nova forma de tomada de decisão e governança. Pode ser combinado com execução automatizada por meio de contratos inteligentes.  **Importância das DAOs**  **DAOs implementam processos de tomada de decisão para toda a organização. Todos que são em parte donos da organização têm o direito de votar em decisões. Natureza das decisões pode variar – como alocar fundos, quais projetos apoiar, ou votações de governança.**  **DAOs são:**   1. **Não centralizadas**, de forma que nenhum indivíduo possa interferir por si só na tomada de decisões 2. Transparentes e auditáveis 3. Não podem ser encerradas por um indivíduo isolado   **Economia de DAOs**  Economia é mais do que apenas oferta e demanda. Em DAOs, vamos discutir três conceitos econômicos:   * Economia da confiança: queremos confiar nas partes as quais estamos interagindo. Isso é feito por meio de contratos inteligentes e *skin in the game* (ex: PieDAO) * Economia da coordenação: tomada de decisão em grupos de acionistas pequenos é difícil. Tomada de decisão em um grupo descentralizado é ainda mais. DAOs ajudam nessa coordenação (ex: MolochDAO, MakerDAO). * Economia da alocação: assim como governos coletam impostos e decidem como alocá-los, DAOs podem decidir sobre a estrutura de governança do ecossistema (ex: KyberDAO, Dash, e The LAO (a primeira Organização Autônoma de Responsabilidade Limitada, “LAO”)   Por fim, DAOs representam uma nova e descentralizada forma de organização conforme nossa economia continua evoluindo. Caso você se aprofunde no funcionamento de DAOs, verá que existem mecanismos muito diferentes – algumas DAOs podem mudar tudo em um protocolo, algumas podem mudar apenas algumas coisas, outras focam em decisões administrativas de tesouraria de um projeto, e outras focam apenas em decisões sobre propostas de melhorias.  *Parte II: Capítulo 22 analisa mais à fundo o conceito de DAOs.* |

#### Incentivos Não-Financeiros (Outros Incentivos para Reforçar Estratégia)

Garanta que incentivos levam em consideração variáveis financeiras e não-financeiras para reforçar a estratégia desejada no design de mecanismo.

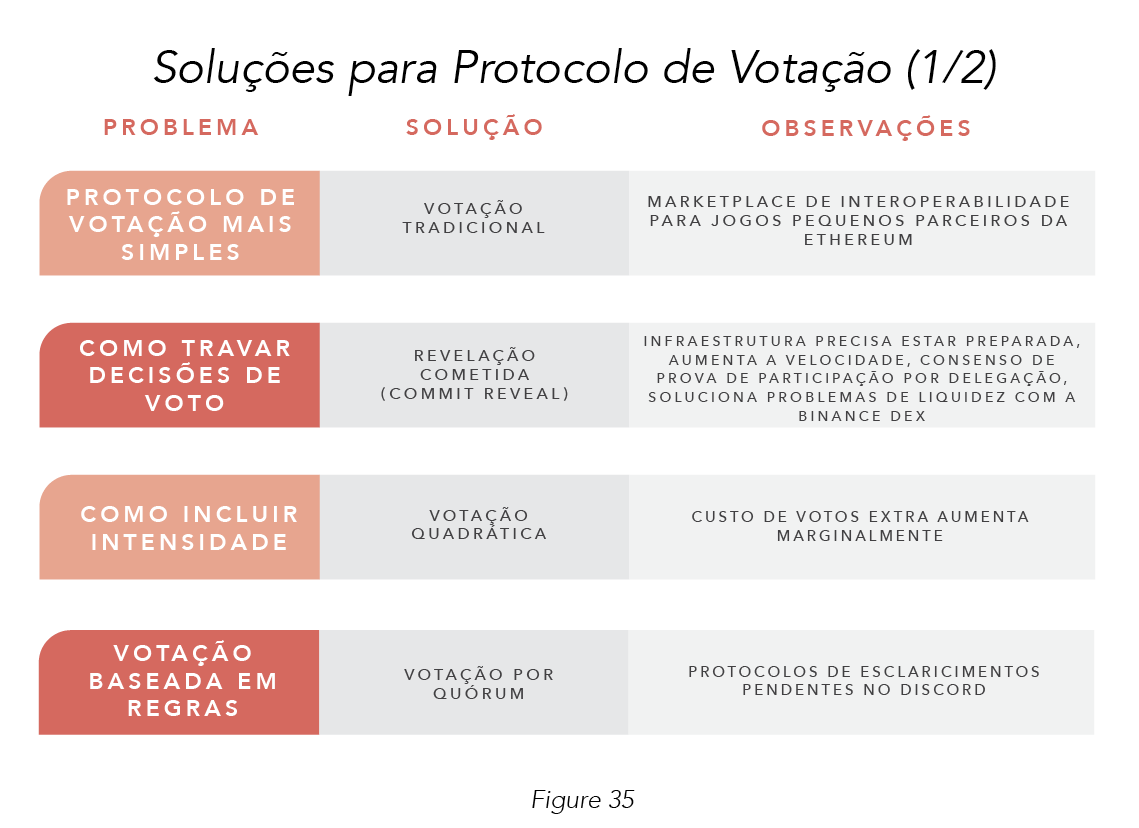


Figura 35

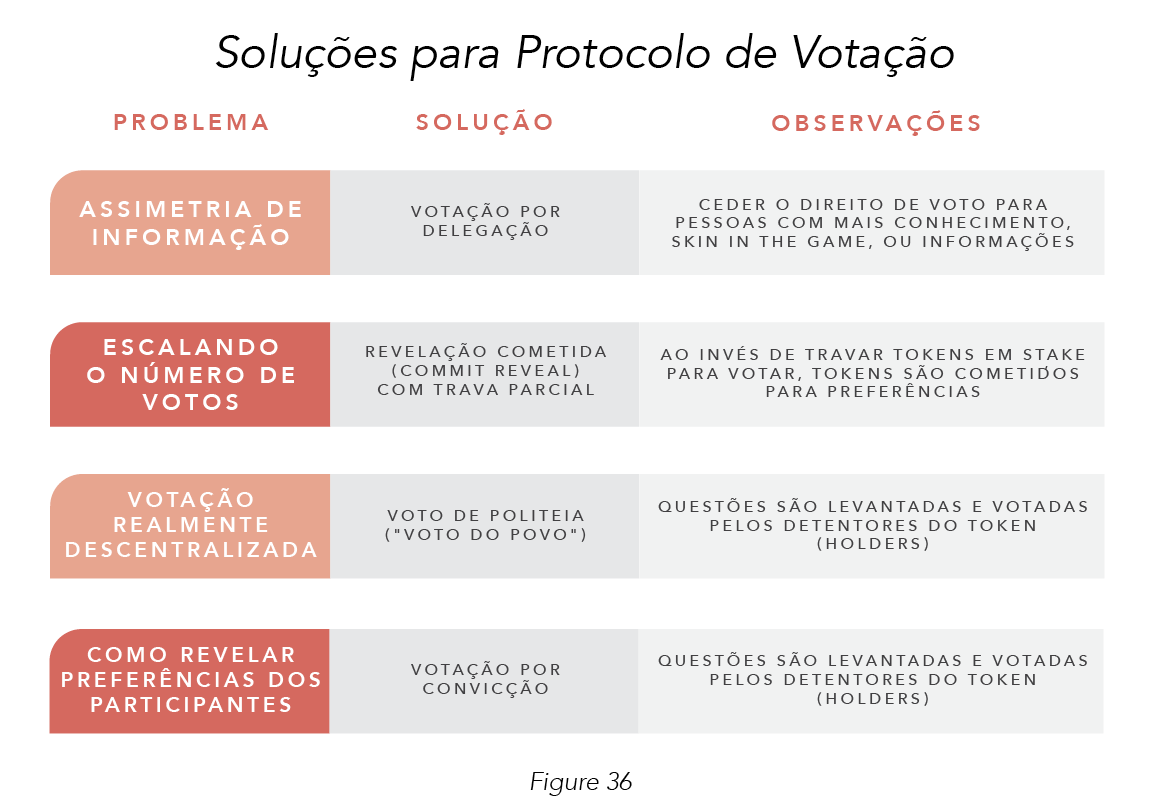


Figura 36

Protocolo de votação (participantes tem voz nesse processo)

1. Votação tradicional: cada pessoa pode votar com base na quantidade de tokens detidos, embora isso possa levar à plutocracia e outros ataques (ex: tokens de governança).
2. Revelação cometida (*Commit-reveal*): Imagine que você publica sua escolha para todos na rede. Em seguida você revela a escolha, e os demais podem verificar se é igual ao que submeteu (publicação) inicialmente. (Ex: Contratos inteligentes da Ethereum)
3. Votação quadrática: Ao invés da estrutura padrão de um voto por pessoa, votantes recebem (ou compram) uma quantia de votos para utilizarem em várias questões/votações. Por exemplo, caso um membro de uma DAO seja alocado 10 votos para 10 questões, pode escolher dividir os votos igualmente para cada votação ou abster-se de algumas para alocar **mais** votos nas questões mais importantes para ele(a). Isso demonstra a intensidade das preferências. As votações quadráticas das rodadas de subsídios (*grants*) da Gitcoin são feitas de forma bastante única. Existe um fundo limitado de capital para ser alocado em cada rodada para um número enorme de propostas de subsídios de diferentes projetos. Para a votação, incentivam usuários a passarem pelo processo de KYC para evitar a criação de múltiplas contas e o consequente aumento artificial do suporte de um projeto específico. Votantes podem votar quantas vezes quiserem por meio de doações em cripto, mas o valor e a frequência dos votos têm menos peso no subsídio total recebido por cada proposta do que o número de votantes únicos. Votantes que passarem pelo KYC possuem multiplicadores que aumentam o subsídio total em até 150% por projeto.
4. Votação por quórum: número mínimo de pessoas para validar a votação (ex: Balancer utiliza a Snapshot em seu processo de governança, requerendo quantidade mínima em *stake* em cada proposta antes de ser submetida à votação de governança).
5. Votação por delegação: usuários delegam seus votos para outros que possuem mais conhecimento sobre o tópico – e portanto podem exercer a governança de forma qualificada (ex: Tezos).
   1. Votação por Revelação Cometida (*Commit Reveal*) com trava parcial: votação ponderada por token. Votantes podem participar em várias votações ao mesmo tempo e tokens não ficam travados em *stake* (ex: Mecanismo de TCR (vide 10.6.4.2).
   2. Voto de Politeia (“voto do povo”): acompanhamento de propostas para votação (ex: Dcred, Politeia).
   3. Votação por convicção: processo de votação contínua em que votantes colocam seus votos em *stake* por determinado período até que o patamar mínimo seja atingido, aprovando a proposta (ex: Giveth).

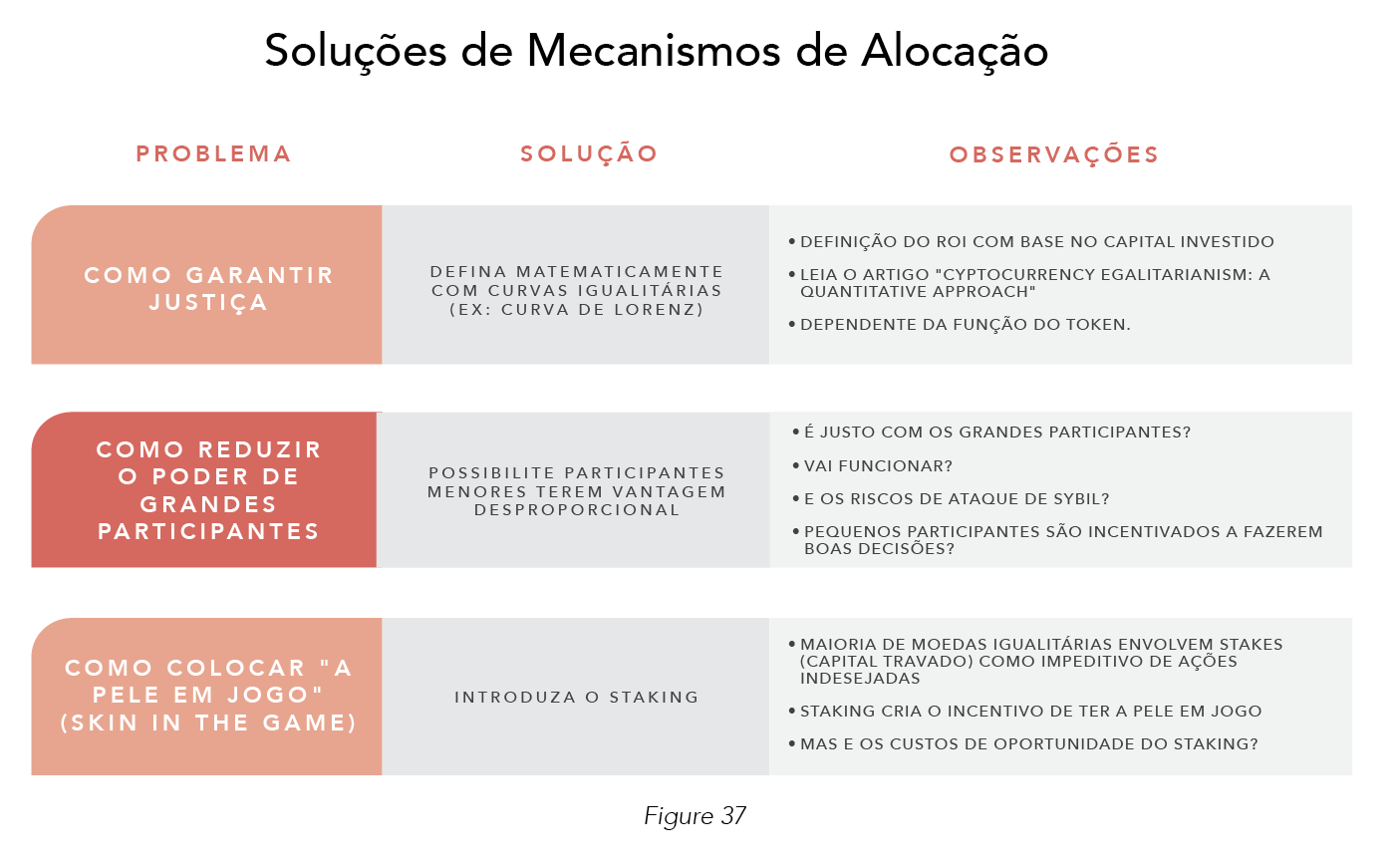


Figura 37

1. Mecanismos de alocação (mecanismo automatizado)
   1. Reputação: para mitigar risco moral em transações
   2. Modelos de mecanismos igualitários (*egalitarian*): todo participante do ecossistema desfruta de retornos em forma de taxas de transação, seja *online* ou *offline* (ex: Algorand).

#### Estrutura (Incentivos, Estratégias e Comércio Eficiente)

Garantir que o mecanismo base que possibilita o sistema funcionar é eficiente. A estratégia precisa prevenir que maus atores possam formar conluios e agir em conjunto.

1. Protocolos de barganha (participantes têm voz nesse processo)
   1. Mecanismos de leilão: Leilões com múltiplos atributos, mecanismos de pagamento, cadência de leilões como solução para congestionamento e segurança.
   2. Mecanismos de pagamento de barganha (dentro do ecossistema)
      1. Preço fixo: Preço definido pelo sistema/criador do projeto. É “pegar ou largar” (ex: preço de tokens nas corretoras).
      2. Maior oferta/preço: A pessoa responsável pelo lance de maior valor será escolhida (ex: taxas de transação do Bitcoin).
      3. Segundo maior preço: A pessoa com maior lance será escolhida, mas ao invés de pagar o preço de seu próprio lance, pagará o segundo maior preço ofertado (ex: domínios ENS).
      4. Leilão de Vickrey-Clarke-Groves[[71]](#footnote-72): A pessoa com lance que maximiza o bem comum será escolhida (ex: Celer Network).
      5. Leilão holandês invertido: Preços caem conforme o tempo passa (ex: Gnosis, Algorand).
      6. Todos pagam: Todos os participantes precisam pagar (ex: Augur).
      7. Preço dinâmico: Preço definido pelo contrato inteligente, dependendo da liquidez existente (ex: mercados autônomos como Uniswap e Bancor).
2. Informação de comunidade: Oráculos, ou *Oracles* (mecanismo automatizado)

Oráculos agregam o fluxo de informações e dados do *off-chain* para o *on-chain,* dentro do ecossistema:

* 1. Oráculos de software: lidam com informações disponíveis *online* (ex: Chainlink)
  2. Oráculos de hardware: lidam com informações disponíveis *offline*, por meio de clientes como sensores RFID e dispositivos de IoT (ex: VeChain, Weeve).
  3. Oráculos de entrada: fornecem dados do mundo externo para contratos inteligentes (ex: preço do $ETH em dólares, como a Oraclize).
  4. Oráculos de saída: Enviam dados para o mundo externo. Pagamentos feitos na blockchain podem ativar serviços no mundo externo (ex: desbloquear um patinete ao escanear um código QR, que é aprovado após o pagamento ser recebido na plataforma, como a Airbie).
  5. Oráculos baseados em consenso: Indivíduos fornecem entradas para o sistema de oráculo para informar/atualizar o contrato inteligente (ex: Augur, SchellingCoin, Witnet).

## [Estudo de Caso] MakerDAO

### Plataforma baseada em DAO

MakerDAO é uma plataforma baseada no conceito de DAOs que possui os tokens $MKR e $DAI. Ambos tokens são de tipos diferentes e fazem parte do ecossistema, sendo $MKR o token de governança e $DAI o token de moeda corrente. $MKR (e seus detentores) governam o token $DAI e sua estabilidade.

*$DAI é pareada livremente (soft-pegged) ao dólar. 1 $DAI representa algo em torno de $1 USD. Esse valor é mantido pelos colaterais existentes e pelos detentores do token $MKR.*

Uma DAO é uma organização autônoma descentralizada em que não há entidade centralizadora para governar o ecossistema. DAOs são governadas de forma descentralizada, tanto com máquinas (automação) quanto com humanos (manual).

MakerDAO é uma plataforma de contratos inteligentes desenvolvida na Ethereum. O contrato inteligente cria tokens $DAI quando colaterais são colocados em jogo. Colaterais são ativos digitais na blockchain, como $ETH, $BAT, $YFI).

#### Objetivos da MakerDAO

O objetivo da MakerDAO é criar uma moeda global governada de forma descentralizada, por meio de respostas autônomas e mecanismos de incentivo.

Até o quarto trimestre de 2020, $DAI tem sido uma ferramenta importante em finanças descentralizadas (DeFi). Um dos problemas do atual modelo de mercado financeiro tradicional é a opacidade e limitação em termos de acesso. Com MakerDAO e DeFi em geral, é possível aumentar a eficiência do mercado financeiro por meio de moedas descentralizadas e transparentes, mantendo o valor do token relativamente estável para facilitar transações.

Mais sobre como a MakerDAO impulsiona DeFi pode ser encontrado no Capítulo 13.

#### Como funciona

Para entender o design de mecanismo por trás da MakerDAO, vamos analisar como o sistema funciona.

O contrato inteligente usa criptoativos (ex: ETH), por meio de posições de dívidas colateralizadas, para criar tokens $DAI. O valor desses tokens $DAI são “garantidos” pelos colaterais *on-chain* (ex: $ETH, $BAT). Ecossistema da MakerDAO está sempre sobre-colateralizado, com o valor de colaterais total maior do que a dívida.

Sistema da MakerDAO possibilita que qualquer indivíduo utilize ativos digitais como insumo (ex: $ETH) e produza $DAI, o resultado. Como qualquer outra moeda, $DAI pode ser utilizada livremente.

Outra forma de interpretar é que novos tokens $DAI são emitidos quando um usuário coloca seus ativos em *stake* (trava), como $ETH, $LINK, $USDC, em um contrato inteligente da MakerDAO. Ao fazer o *staking* de seus ativos, podem criar $DAI.

##### Tipos de colateral na MakerDAO

MakerDAO começou com collateral único, aceitando apenas $ETH. Em 18 de novembro de 2019[[72]](#footnote-73), a fundação Maker mudou o token $DAI de colateral único para multi-colateral.

Essa inovação do token multi-colateral possibilitou à MakerDAO maior proteção contra flutuações significativas em ativos digitais individuais. Esse mecanismo está relacionado ao conceito de “cesta de produtos”, utilizado para medir o poder de compra de um país, “cesta de moedas de reserva”, para suportar a moeda nacional do país, ou “cesta de empresas”, em portfólios de investimentos. A meta é reduzir o risco de eventuais movimentos em variáveis individuais.

Mesmo assim, criar designs de economias de token e lançar modelos quase perfeitos é muito desafiador. Por isso, o objetivo é incluir mais ativos digitais como colateral conforme o ecossistema da MakerDAO cresce e passa por testes reais de mercado.

#### Tokens da MakerDAO

MakerDAO usa um modelo de dois tokens. Cada token tem seu objetivo e função diferentes.

$DAI é o token com função monetária, e funciona como o meio de pagamento. É uma forma de pagamento (via DeFi), reserva de valor (1 $DAI = 1 USD), e unidade de medida (1 $DAI = 1 USD).

$DAI é conhecida como uma “*stablecoin*”, visto que é pareada livremente (*soft peg*) ao dólar. O valor é suportado por colaterais *on-chain*, de forma totalmente descentralizada, via CDP (posição de dívida colateralizada). Qualquer indivíduo pode comprar $DAI em uma corretora ou colocar $ETH em *stake* para emitir $DAI.

$MKR é um token de utilidade, e age como uma forma de governança no ecossistema da MakerDAO. Detentores de $MKR são parte da governança descentralizada do token $DAI. São responsáveis pelo processo de tomada de decisão. Eles podem votar em conflitos e propostas do ecossistema. Tokens $MKR são criados ou destruídos de acordo com flutuações de preço do token $DAI para manter o mais próximo possível de $1 USD. O valor do $MKR é determinado pelas forças de mercado, como oferta e demanda.

Abaixo temos uma comparação entre os dois tokens:

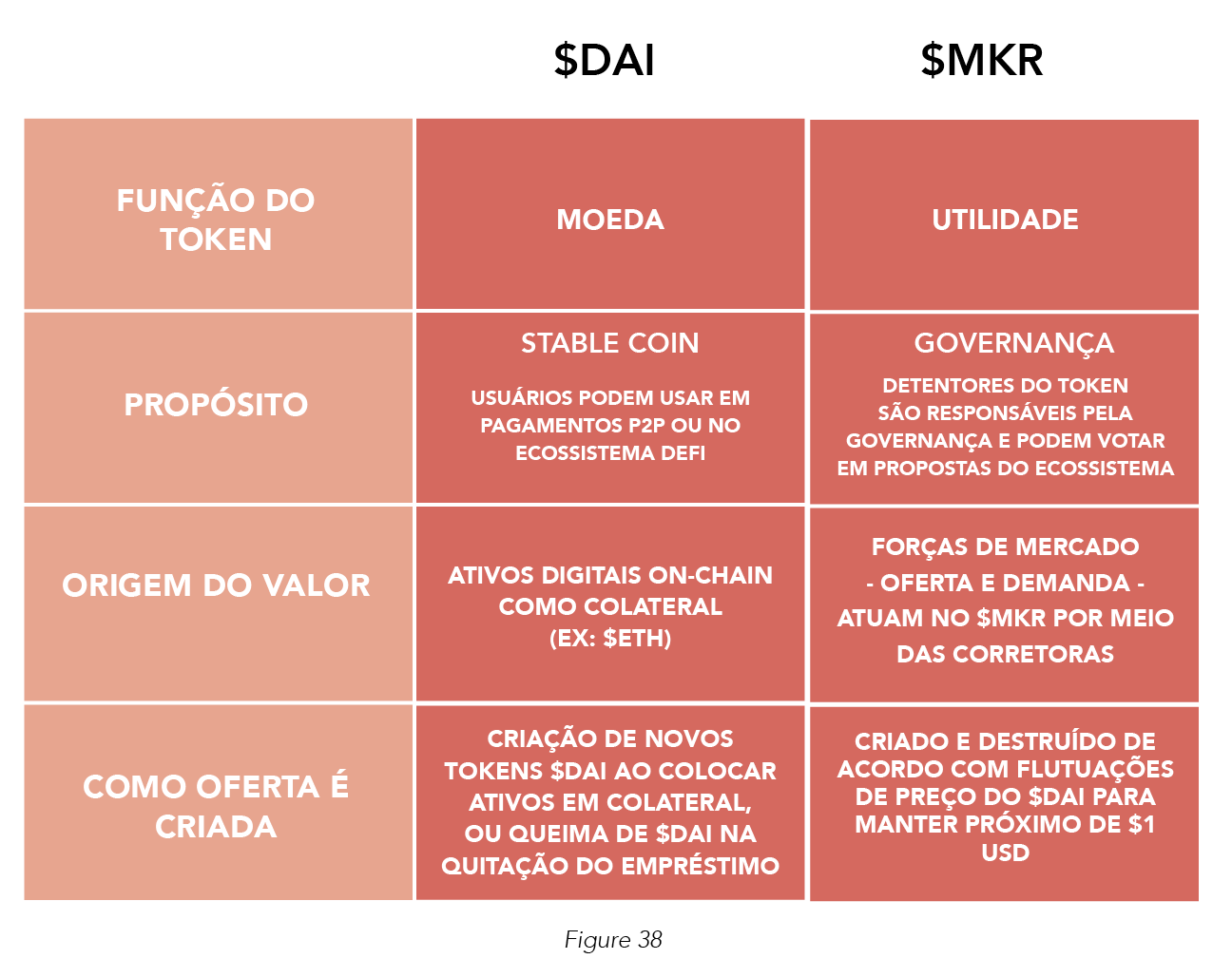


Figura 38

#### MakerDAO em DeFi

DeFi significa finanças descentralizadas. DeFi busca transformar o ambiente financeiro ao trazer transparência, velocidade e acessibilidade. Não busca mudanças radicais, mas introduzir novos casos de uso, novos produtos, e melhorar a eficiência por meio da tecnologia.

Existem duas formas de entrar no ambiente de DeFi. Por meio de um protocolo de empréstimos ou por uma corretora:

* Protocolos de empréstimos são utilizados quando você coloca ativos como collateral (ex: $ETH) para receber outros ativos (ex: $DAI). Essa operação possui custo de juros.
* Corretoras são utilizadas quando você abre mão de seus ativos (ex: $ETH) em troca de outros (ex: $DAI). Essa operação possui pequeno custo de transação.

*$DAI é uma solução de empréstimos no ambiente DeFi.*

##### Quem utiliza MakerDAO em DeFi?

Para entender a efetividade dos mecanismos de incentivo do protocolo, é importante notar os diversos tipos de participantes e usuários do sistema.

MakerDAO segue sendo um dos protocolos mais utilizados por conta da demanda por ativos pareados em dólar, como o $DAI.

* Protocolos de empréstimo como Aave, Compound, e Celsius utilizam $DAI, dado que possui baixa volatilidade de preço e possibilita empréstimos mais estáveis.
* Corretoras descentralizadas como Uniswap, Curve, e Balancer também usam $DAI como token comum pela paridade histórica com dólar, facilitando cálculo e execução de transações.
* Plataformas de derivativos como a Chai utilizam as taxas oferecidas pela MakerDAO via $DAI (*DAI Savings Rate*, or DSR) para representar o direito sobre juros recebidos no depósito dos tokens. Outras plataformas de derivativos como Opyn usam DSR para executar posições de *short* ou *long* no token $DAI.

### Governança

No modelo de dois tokens da MakerDAO, governança é mais clara por conta do token com essa função específica[[73]](#footnote-74), $MKR. Porém, o mecanismo de tomada de decisão e resolução de conflitos não é tão simples quanto possuir $MKR com esperanças de valorização.

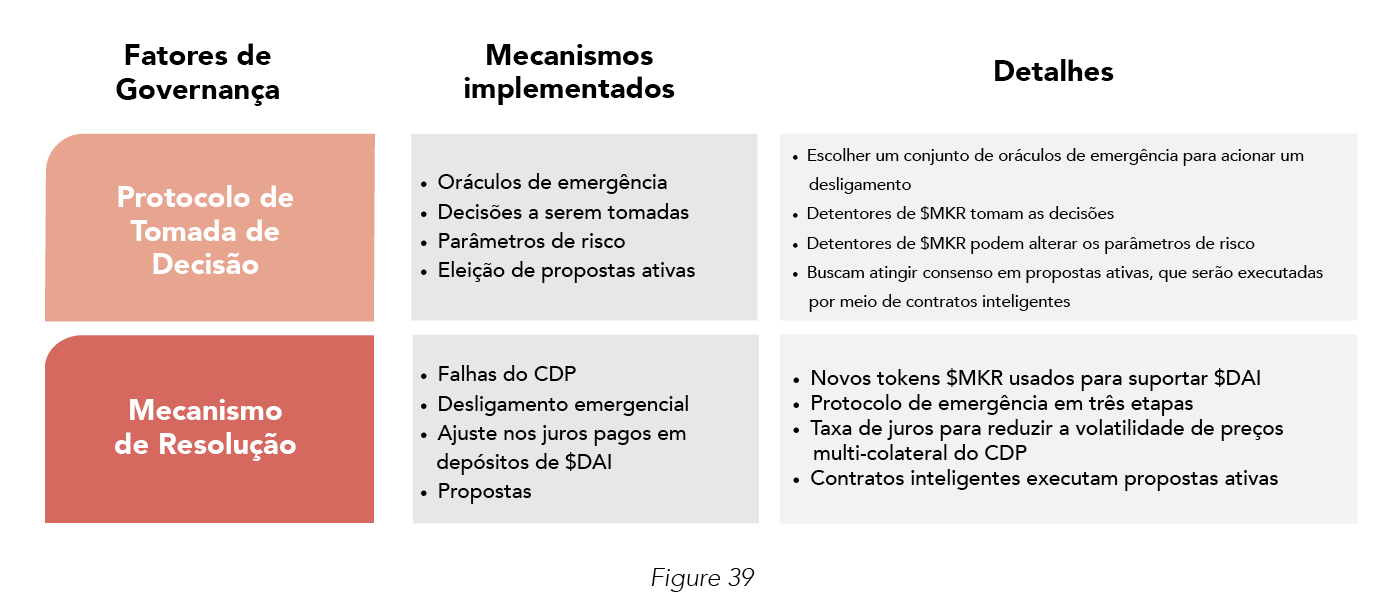


Figura 39

#### Protocolo de tomada de decisão

##### Oráculos de emergência

O processo de governança seleciona um grupo de oráculos emergenciais para acionarem um desligamento de emergência. Oráculos de emergência são parte do mecanismo de desligamento emergencial. Possibilita que a plataforma sobreviva em cenários de *bank run* (corrida aos bancos), desvalorização súbita de colaterais etc. MakerDAO tem sua própria solução de oráculo que provém informações do ambiente de DeFi e outras áreas.

##### Decisões a serem tomadas

Detentores de $MKR (*holders*) tomam decisões em questões como:

* Acionar o desligamento de emergência
* Adicionar novos tipos de CDP (posição de dívida colateralizada)
* Modificar tipos existentes de CDP
* Modificar taxas de juros de depósitos em $DAI
* Escolher o conjunto de oráculos de preço
* Escolher o conjunto de oráculos de emergência

##### Parâmetros de risco

Detentores de $MKR governam os seguintes parâmetros de risco:

* Teto de dívida
* Índice de liquidez
* Taxa de juros
* Penalidade de liquidações
* Duração de leilões
* Tamanho das fases dos leilões

##### Eleição de propostas ativas

*Holders* de $MKR buscam atingir consenso em propostas ativas. Isso está relacionado ao mecanismo de resolução. A proposta é comissionada por contratos inteligentes para modificar as variáveis internas da plataforma.

#### Mecanismos de Resolução

MakerDAO possui algumas soluções e mecanismos de resolução implementados para quando as coisas não vão conforme o esperado.

##### Falhas de CDP (posição de dívida colateralizada)

Caso a CDP falhe, novos tokens $MKR serão utilizados para suportar $DAI. O limite de tokens $MKR em existência é de 1 milhão.

##### Desligamento de emergência

Impõe um preço-alvo para detentores de $DAI e CDPs. Segue três passos de acordo com o seguinte protoloco de emergência:

1. Desligamento de emergência é acionado por votantes ($MKR) ou pelo oráculo emergencial escolhido pela governança da MakerDAO. Caso isso aconteça, usuários de CDP irão tentar sacar seus colaterais. O desligamento de emergência impede criação de CDPs e eventuais manipulações. Em seguida, congela os preços em um valor fixo determinado e utiliza esse preço referência para processar os pedidos de todos os usuários proporcionalmente. Dessa forma, usuários de CDP podem sacar imediatamente o valor líquido de colateral em suas posições de dívida.
2. Processamento de leilões pós-desligamento de emergência. Existe um temporizador para possibilitar a finalização de leilões de colateral pré-existentes. O período de processamento do leilão é definido pela governança da MakerDAO para ser mais longo do que o leilão de colateral mais demorado.
3. *Holders* de $DAI podem reivindicar colaterais remanescentes diretamente com seus tokens, à uma taxa fixa. Não há data limite para quando as reivindicações precisam ser feitas. No modelo multi-colateral, detentores de $DAI podem fazer reivindicações proporcionais aos tipos de colaterais em seu portfólio.

|  |
| --- |
| **Mini-Caixa: Cripto"*Black Thursday*"**  Em 12 de Março de 2020, um colapso aconteceu no mercado financeiro tradicional. Isso causou também um colapso repentino no mercado cripto que acionou o desligamento de emergência.  **Qual foi o motivo do colapso?**  Duas coisas aconteceram:   1. Covid-19, uma pandemia global, causou pânico geral nos mercados de capitais. 2. Houve uma guerra de preços de barris de petróleo em Fevereiro de 2020, que também afetou os mercados de capitais.   Por mais que nossa intenção seja de que os mercados tradicionais e de cripto sejam independentes um do outro, são diretamente conectados até o momento. O colapso nos mercados de capitais tradicionais causou um colapso gigantesco no mercado cripto. Mercado cripto perdeu 50 porcento de seu valor.  **O que aconteceu com o mercado cripto?**  Blockchain é uma estrutura de tecnologia com pacotes de dados e transações fluindo do ponto A para o ponto B em qualquer dado momento. Podemos imaginar como se fosse uma rodovia com carros dirigindo em ambas as direções, e com tamanho fixo.  Por conta da perda de valor devido ao colapso, mais transações foram geradas conforme pessoas moviam suas criptomoedas para cobrir chamadas de margem, tentar liquidar posições, ou comprar ativos digitais. Essas transações adicionais são análogas à adicionarmos mais carros na rodovia em nosso exemplo.  O aumento do número de transações causou congestão de rede (tráfego pesado no horário de pico). Como discutido em Design de Mercado (Capítulo 6), taxas de "gás" podem resolver esse congestionamento. Análogo à implementação de pedágios na rodovia.  Durante esse período, o valor dos colaterais também caiu. CDPs (posições de dívidas colateralizadas) ficaram sub-colateralizadas e seus detentores tiveram que:   * 1. Aumentar o colateral e pagar altas taxas de gás, ou   2. Leiloar seu colateral para quitar a posição de dívida   **Qual foi o resultado?**  Os altos preços de "gás" impediram muitos donos de posições em CDP de aumentarem seu colateral antes do desligamento de emergência. O mecanismo foi acionado e o colateral de muitos CDPs foi leiloado.  **Lado bom**: Sistema funcionou conforme planejado.  **Lado ruim**: Todos estavam atolados com transações e colaterais. Alguns CDPs e colaterais foram leiloados a preços baixíssimos, até mesmo $0 USD. Alguns compradores, portanto, adquiriam grandes quantias de $ETH de graça, menos a dívida devida. Esse montante totalizou em torno de 5.4 milhões de $DAI.  Para explicações mais detalhadas, MakerDAO documentou a experiência em um recurso online[[74]](#footnote-75). |

##### Ajuste da taxa de juros de $DAI

Preços flutuam no curto prazo. Para lidar com isso, a DSR (taxa base) se comporta de forma dinâmica, para reduzir volatilidade de preço. A DSR é um parâmetro global, influenciando em quanto os detentores de $DAI recebem ao longo do tempo e funcionando como taxa base para empréstimos – emitindo novos $DAI em forma de CDPs (posição de dívida colateralizada).

##### Contratos de propostas

Donos de $MKR votam inicialmente para eleger propostas como “ativas”. Propostas são executadas quando recebem aprovação necessária dos *holders*. Mudanças nas variáveis de governança interna são implementadas imediatamente após ser aprovada - com 24 horas de espera entre a aprovação e a execução para proteger possíveis propostas maliciosas, e a lógica antiga é apagada.

##### Ataques Maliciosos/hacks

*Hacks* podem atacar a infraestrutura de contratos inteligentes. No pior cenário possível, todos os colaterais estariam comprometidos. De qualquer forma, os contratos inteligentes da MakerDAO passaram por auditoria de segurança, demonstrando pelo menos algum nível de segurança. O contrato também exige verificação formal para prevenir *hacks*, visto que pode ser um ataque interno (exploração de falhas no código) ao invés de externo.

##### Eventos de “Cisne negro”

Uma das ameaças é o risco de eventos chamados de “Cisne Negro”. São raros, mas muito significativos, e geralmente causam forte impacto negativo no ecossistema que atingem. Para tentar prevenir, o colateral de CDPs possui um teto de dívida que aumenta gradualmente ao longo do tempo, além do ecossistema estar sempre “super colateralizado”.

##### Erros de precificação

Oráculos enviam informações para o sistema, e podem ocorrer problemas técnicos nessa transmissão que afetam o valor do token $DAI, como erros de precificação ou outros fatores de mercado. A comunidade da MakerDAO estruturou uma reserva de capital para garantir a continuação do token independente de erros de mercado, criando a função de *Keepers* que são recompensados por maximizar racionalidade e eficiência de mercado.

Keepers[[75]](#footnote-76) são incentivados por oportunidades de lucro por meio de sua contribuição honesta em sistemas descentralizados.

### Incentivos Não-Financeiros

MakerDAO possui muitos incentivos com intenção de garantir o alinhamento todos os participantes e a estabilidade do $DAI com relação ao dólar. $MKR é parte dos mecanismos de governança, e possui outras considerações em seus incentivos.



Figura 40

#### Protocolo de Votação

*Como é feito, qual é o propósito e quais tipos de votação existem?*

Tokens $MKR são usados para votar em propostas. 1 $MKR = 1 voto. Essas propostas incluem, por exemplo, determiner a DSR (taxa base).

##### Tipos de voto

Existem dois tipos de voto disponíveis:

* Votação com tempo limitado. Votações de governança que buscam estabelecer consenso limitado em questões importantes e sondar o entendimento geral sobre possíveis parâmetros de risco.
* Votação de aprovação contínua. Ao atingir certo patamar de aprovação (de forma contínua), executa mudanças definitivas no sistema.

##### Votações de governaça com tempo limitado

Votações de governança são utilizadas para atingir um consenso inicial na comunidade antes de votos serem submetidos de fato – para economizar taxas de transação. Portanto, o resultado da votação já é sabido antes da votação real acontecer. O processo de votação não é a tomada de decisão por si só, mas sim uma forma segura de encaminhar as decisões tomadas no sistema.

##### Votações de aprovação contínua

A saúde do ecossistema MakerDAO, a estabilidade da $DAI, e a defesa contra eventuais propostas ruins faz parte do papel dos *holders* de $MKR. Tokens $MKR são usados para votar em propostas benéficas ao ecossistema que serão implementadas.

A política de trava dos tokens usados como voto desafia e reforça a situação do sistema. Propostas são submetidas à maioria dos votos, propostas antigas são deletadas, e a governança funciona em ritmo contínuo. Novas propostas podem ser submetidas a qualquer momento por detentores de $MKR.

##### Cálculo de Votos

Votos são calculados com base no total de $MKR depositados em uma proposta. Imagine o seguinte caso: um grupo de 50 investidores tem 600 $MKR e vota pela proposta A. Outro grupo, de 100 investidores, tem 400 $MKR e votam na proposta B. Proposta A será aprovada pois teve 60% dos votos totais utilizados na proposta (600 / [600+400] = 60%).

##### Contrato de Votação

O contrato de votação utiliza mecanismo simples de contrato inteligente. Basicamente trava os tokens $MKR e é controlado por carteiras quentes e frias (*hot* e *cold wallets*) para garantir segurança dos fundos. O custo de voto é a taxa de transação paga no momento do voto.

#### Mecanismo de Alocação

##### Contratos Inteligentes

O contrato inteligente que controla a emissão e queima de $DAI cria um mecanismo de feedback autônomo por meio de:

* Geração de $DAI por meio do CDP colateralizado
* Depósito de colateral
* Pagamento de empréstimos e taxas de estabilidade
* Saque de colateral e fechamento de CDPs

Ativos em colateral (ex: $ETH) são mantidos pelo contrato inteligente e possibilitam o usuário emitir a quantia referente em $DAI. Usuário pode posteriormente repagar o empréstimo em $DAI (mais juros) e pegar seus ativos em colateral de volta.

##### Taxa de estabilidade

Taxa de estabilidade altera o custo de emissão de $DAI. Funciona como uma taxa de juros dinâmica.

O contrato inteligente da Maker coleta taxas sobre saques de $DAI retirados de CDPs, e donos de $MKR podem votar sobre a taxa base cobrada em empréstimos (DSR).

Usuários pagam a taxa de estabilidade quando repagam seus empréstimos em $DAI. Pense nisso como juros sobre empréstimos. A taxa é proporcional à quantidade de $DAI retornada. Empréstimos podem ser pagos em $DAI ou $MKR.

Esse parâmetro de risco é usado para administrar a oferta e demanda por $DAI durante períodos de crise. Quando a demanda por $DAI aumenta, as taxas associadas com a geração de mais tokens aumenta. Mais usuários irão repagar o CDP (empréstimo) e $DAI será queimado, reduzindo a oferta de $DAI e causando pressão positiva no preço.

A taxa é calculada de forma contínua usando a fórmula: . As taxas coletadas são queimadas.

### Estrutura

MakerDAO foca na transparência e descentralização. A estrutura de mecanismos econômicos precisa ser clara e facilmente entendida. Especialmente para o token de governança, $MKR.

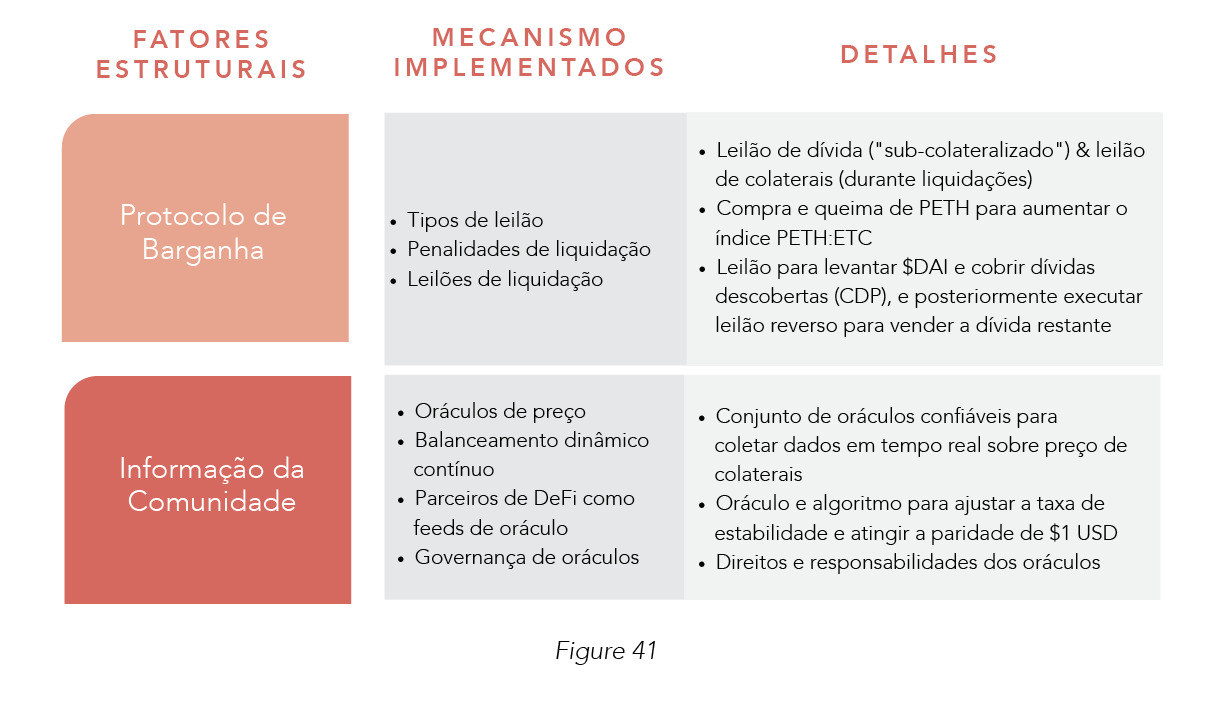


Figura 41

#### Protocolo de Barganha

##### Tipos de leilão

Existem dois tipos de leilão na MakerDAO em cenários de desligamento emergencial e liquidações:

* Leilão de dívida: quando CDP se torna “sub-colateralizado” [[76]](#footnote-77), leilão reverso é criado para vender os $MKR por $DAI.
* Leilão de colateral: colateral da CDP é vendido por meio de leilões durante a liquidação. Mecanismo busca garantir que a dívida pendente seja coberta, enquanto garante o melhor preço para fundos colaterais em excesso.

##### Penalidade de liquidação

Penalidade de liquidação determina o máximo de $DAI levantado em um leilão. Esses fundos são usados para comprar $MKR e tirar de circulação. Colaterais em excesso são retornados ao detentor da CDP. Pense como se fosse um *buyback* padrão no mercado tradicional de ações, para reduzir a oferta e aumentar o preço.

##### Penalidade de liquidação ($DAI com colateral único)

*Nota: esse sistema não está mais em uso, mas é útil entender como funcionava antes de entrarmos na forma mais complicada de colaterais múltiplos.*

No modelo de colateral único $DAI, a penalidade de liquidação compra e queima $PETH para aumentar a proporção de $PETH para $ETH.

O protocolo de liquidação funciona de seguinte forma:

1. CDPs “inadimplentes” são finalizados por um *Keeper*. Ativos são enviados para um contrato inteligente chamado contrato de provisão de liquidez (LPC) e colocados à venda.
2. Penalidade de liquidação E taxas de estabilidade são pagas sobre o empréstimo em $DAI.
3. LPC retira o colateral de $PETH para cumprir a dívida pendente.
4. Donos de CDPs podem retirar seus colaterais restantes, recebendo o valor colateral subtraído da dívida, taxa de estabilidade e penalidade de liquidação.
5. Os $PETH “apreendidos” são colocados à venda.
6. $DAI recebido da venda de $PETH é queimado e tirado de circulação.
7. Caso não haja $DAI suficiente da venda, $PETH é retirado da reserva e colocado à venda, impactando negativamente o índice ETH:PETH.

##### Leilão de liquidação ($DAI com múltiplos colaterais)

Leilões de liquidação foram implementados no final de 2019, quando a MakerDAO passou a utilizar o formato de $DAI com múltiplos colaterais.

###### Entendimento geral

Imagine uma CDP (posição de dívida colateralizada) de com valor de 500 $DAI. MakerDAO compra esse colateral, quitando a dívida da CDP em $DAI, e vende por meio de um leilão automático. Esse leilão acontece em duas etapas.

O primeiro tem o objetivo de levantar o valor correspondente à dívida, 500 $DAI. Investidores vão dando seus lances para quanto pagariam no colateral até atingir o valor da dívida - nesse caso, 500 $DAI.

Após atingir o patamar mínimo, processo parte para a etapa 2: um leilão reverso. A CDP é leiloada com preços decrescentes, em que os investidores fazem lances inversos - quanto a menos do colateral estão dispostos a receber para a mesma quantia de $DAI. Leilão acaba quando o tempo se esgota.

###### Explicação técnica

MakerDAO compra o colateral e vende em um leilão. O leilão determina o preço da CDP por forças normais de mercado. O sistema roda até que levantem $DAI suficiente para cobrir a dívida da CDP. Isso é feito por meio de emissão de tokens $MKR e posterior venda para os participantes do leilão.

Colateral da CDP é vendido e o montante, correspondente ao valor da dívida e penalidade de liquidação somadas, usado para recomprar $MKR e tirar de circulação - anulando o efeito da emissão anterior.

Quando a quantia de $DAI suficiente para pagar a dívida e a penalidade é atingida no leilão, o sistema se inverte para que seja vendido o mínimo de colateral possível. Caso reste algum colateral, será retornado para o dono original.

#### Informação da Comunidade

Como a MakerDAO reúne informações descentralizadas da comunidade? O que faz com esses dados e como influencia o circuito-fechado do ecossistema de token?

##### Oráculos de preço

Um conjunto de oráculos de preço confiáveis são escolhidos por votantes detentores de $MKR. Eles fornecem informações em tempo real sobre preços de ativos colaterais.

Oráculos da MakerDAO usam dois feeds, *Light Feed* e *Dark Feed*[[77]](#footnote-78). O primeiro tem como fonte bases de dados brutas de outros protocolos de DeFi, enquanto o segundo é fornecido por indivíduos anônimos. O objetivo é ter uma proporção de 50/50. Qualquer protocolo pode aplicar para contribuir como *Light Feed*.

##### Balanceamento dinâmico contínuo

No sistema de $DAI com múltiplos colaterais, oráculos e algoritmos são usados para ajustar a taxa de estabilidade e atingir a paridade de 1 para 1 com o dólar. Um contrato inteligente é acionado e afeta a taxa de estabilidade quando $DAI está sendo negociada acima ou abaixo de $1 USD. Esse sistema funciona de forma semi-automática e *holders* de $MKR podem exercer suas preferências no processo.

##### Parceiros de DeFi e feeds de oráculo

*Feeds* são robôs (*bots*) operados por indivíduos para a publicação de preços de ativos em tempo real. A inclusão de parceiros de DeFi não só contribui para o ecossistema com *feeds* pseudo-anônimos, mas coloca também a reputação dos mesmos em jogo, reduzindo o risco de informações falsas.

Até o quarto trimestre de 2020, os parceiros de DeFi eram dYdX, 0x, TokenSets, Gnosis, Kyber[[78]](#footnote-79), Infura, Etherscan, Gitcoin e Argent[[79]](#footnote-80) – chamados de *Light Feed*, conforme explicado anteriormente.

##### Oráculos de governança

O framework (estrutura) de oráculos de governança[[80]](#footnote-81) é uma proposta de definição sobre os direitos e responsabilidades do mecanismo de governança. Está incluso:

* Definição de critério para seleção de novos *feeds*
* Definição de critério para seleção de novos oráculos
* Adição e remoção de *feeds*
* Adição e remoção de oráculos
* Identificação de métricas de performance para *feeds* e oráculos
* Seleção de parâmetros de sensibilidade de preço dos oráculos
* Seleção do parâmetro de atraso do Módulo de Segurança de Oráculo (OSM)

### Conclusão

Por mais que a MakerDAO seja conhecida pela $DAI, stablecoin pareada em dólar, funciona como uma plataforma monetária transparente e descentralizada. O ecossistema da Maker é robusto, com mecanismos automatizados e não-automatizados.

Existem inúmeros casos de uso de $DAI para aplicações DeFi que poderiam auxiliar em várias limitações presentes em FinTechs. Essa é apenas a primeira fase de possíveis evoluções na indústria financeira tradicional.

## Design de Token

*Esse é o último dos três pilares do design de ecossistemas de token.*

### Token Design: Parte 1 - Introdução

Tokens são os incentivos do ecossistema. Portanto, podemos afetar diretamente os comportamentos de participantes por meio de incentivos efetivos. Design de tokens está relacionado às funções principais: segurança, utilidade, moeda, e estabilidade (SUMS). Podem ser tanto fungíveis, quanto não-fungíveis.

Design de token inclui tudo o que for relacionado ao token, como o uso dele como incentivo de comportamentos específicos, a oferta de tokens em circulação no mercado, e políticas de token (ou monetárias). Política de token refere-se à forma que tokens são governados e administrados.

### Por que precisamos de Design de Token?

No primeiro pilar (Capítulo 6) aprendemos que o design de mercado cria o ambiente para participantes interagirem e transacionarem entre si. Já o segundo pilar, design de mecanismo (Chapter: 8), define as regras de comportamento dentro do ecossistema. Por fim, esse último pilar, foca na estruturação do incentivo de fato: o token.

Fatores de consideração variam muito de um token para outro, dependendo de suas funções. Dependem também dos objetivos do ecossistema, para definir se é melhor incentivar usuários a segurarem ou usarem seus tokens, ou para incentivar comportamentos específicos. O token é um meio para atingir os objetivos do ecossistema.

### Por que é Importante para um Ecossistema?

Dependendo do sistema de registro distribuído – permissionado ou não-permissionado, alguns fatores de design de token podem não ser relevantes. Alguns sistemas permissionados não precisam necessariamente de tokens. Regras (design de mecanismo), porém, continuam sendo obrigatórias. Por esta razão, design de mecanismo e design de token são dois pilares distintos.

### Design de Token: Parte 2 – O que é?

**O que?** Design de token é a construção de tokens, incentivo primário do ecossistema.

**Como?** Busca definir como tokens serão governados e administrados, assim como funções e direitos que carregam – design de mecanismo, por outro lado, busca definir como o **sistema** é governado e administrado.

**Por que?** Design de token são regras em código ou embutidas no token que influenciam comportamentos dos participantes. Mudanças afetam os custos e benefícios das escolhas que participantes podem tomar.



Figura 42

#### Abrangência do Design de Token

Dado que design de token é a engenharia de tokens como o incentivo principal, um dos principais fatores que afetam o design é a função do token. Pode ter a função de ser uma *security*, token de utilidade, moeda corrente, ou estabilidade. Dependendo das funções, a estrutura pode mudar completamente de acordo com o domínio econômico (ex: economia monetária, economia financeira, e direitos de propriedade).



Figura 43

### Token Design: Parte 3 – Por Que se Aprofundar?

Regras de design de token são codificadas ou embutidas no sistema descentralizado, às vezes por meio de contratos inteligentes. Contratos inteligentes (*smart contracts*) podem conter funções matemáticas que governam a taxa de câmbio do token, por exemplo, ao invés de ficar exposto à fatores externos do ecossistema que podem afetar a estabilidade de valor do mesmo.

Design de token é crucial para garantir que o token siga as regras estipuladas pela economia. Por conta da descentralização, é importante estabelecer certas regras em código para impor um nível mínimo de coordenação e governança.

### Fatores no Design de Token

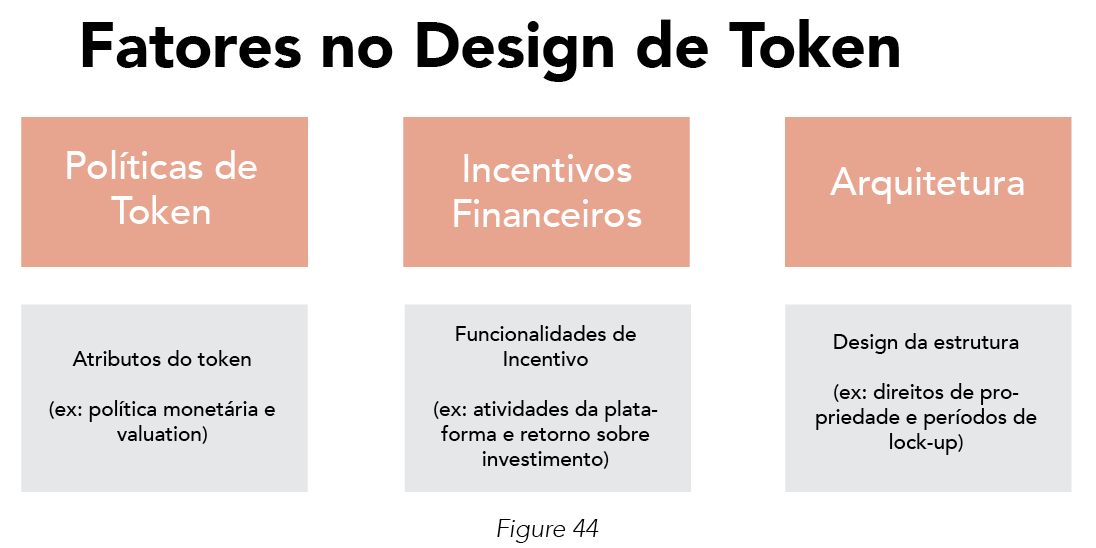


Figura 44

Para funcionarem bem, tokens precisam:

* Definir **políticas de token**. Recompensar com **incentivos financeiros** para encorajar ações desejadas e estipuladas no Design de Mecanismo.
* Estruturar **arquitetura adequada** para o token, considerando vários aspectos como direito de propriedade, identidade, e recompensas.
* **Provas ou modelos matemáticos** para realizar projeções de *valuation*, oferta circulante etc.

#### Política de Token

Política de token é um termo adaptado da economia e política monetária tradicionais, e busca definir como tokens serão governados e administrados. Diferente do design de mecanismo, que foca na forma que o **sistema** é governado, design de token está focado no funcionamento do token em si.

Políticas de token incluem políticas monetárias e *valuation* (avaliação) do token.



Figura 45

Política monetária tradicional inclui operações em mercado aberto (*OMO*), descontos, reservas mínimas, e menor restrição quantitativa. Em política de tokens, a listagem em corretoras centralizadas/descentralizadas ou mercados secundários seria o equivalente à abertura de mercado.

O incentivo para um *Holder* manter seus tokens é uma função do crescimento esperado na demanda e na oferta monetária[[81]](#footnote-82). Reservas mínimas podem ser atingidas no estágio de design do lançamento do token (ICO), usando “curvas de ligação” (*bonding curves*[[82]](#footnote-83)) ou como alavancagem com colaterais em contratos inteligentes[[83]](#footnote-84).

Política de tokens restringe os mercados de diversas formas com base nos objetivos do token, como garantir estabilidade de preços (tokens pareados), justiça no processo de participação ativa etc.

Ao contrário da política monetária, os casos de uso da política de tokens vão além da função de moeda corrente. Política de tokens considera políticas expansionistas e contracionistas[[84]](#footnote-85), como a emissão (*mint*) e queima (*burn*) de tokens para controlar a oferta circulante conforme necessidade.

##### Valuation de Tokens

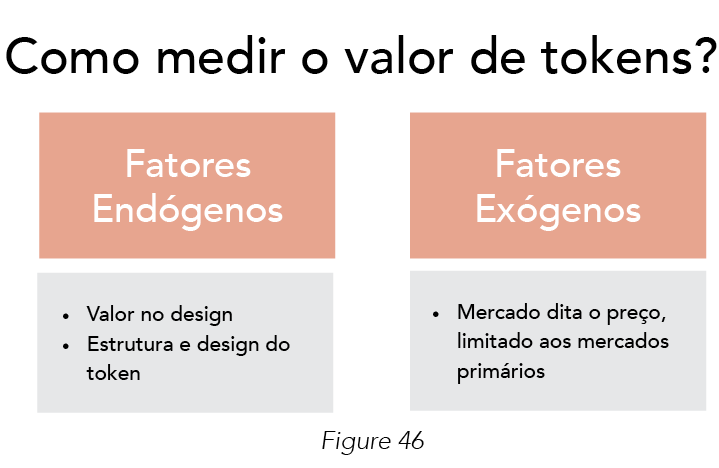


Figura 46

*Valuation* é um fator mais importante para tokens com funções de *securities* ou moeda corrente. Tokens devem ter seu valor atrelado a fatores internos do ecossistema, como atividades da plataforma, crescimento, equilíbrio de preços dinâmico etc.   
  
Política monetária também influencia no *valuation* de um token. Dois modelos de *valuation* para tokens de utilidade são equilíbrio de preço dinâmico e adoção dinâmica[[85]](#footnote-86).

**Exemplos do Mundo Físico**

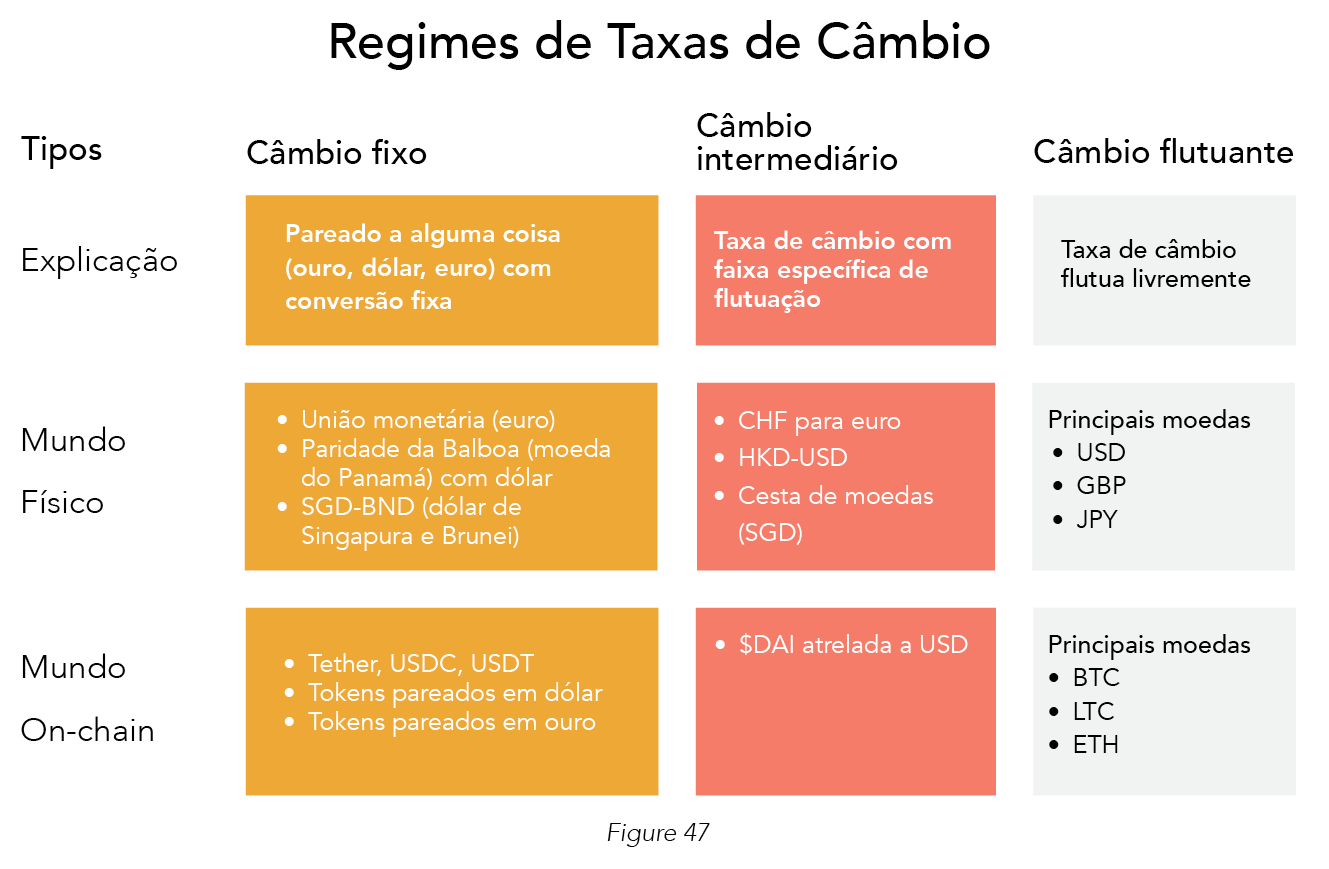


Figura 47

No 5.1, discutimos sobre como os bancos centrais são controlados por grupos pequenos de pessoas, criando uma alta centralização.

Já o mundo cripto é majoritariamente descentralizado. Em outras palavras, as decisões principais estão embutidas no código e são suportadas pelo ecossistema estruturado do token. Dependendo do design de mecanismo, pessoas na rede podem votar para mudar algumas coisas do sistema, dando mais poder aos membros da comunidade.

Bitcoin, por exemplo, aumenta sua oferta de forma algorítmica, cortando as recompensas de bloco pela metade a cada quatro anos. Além disso, existe o limite máximo de 21 milhões de unidades que serão emitidas. Por outro lado, MakerDAO aumenta a oferta de $DAI por meio de colaterais, sem limitação máxima. Detentores do token $MKR podem votar na taxa de estabilidade que o colateral gera.

#### Incentivos Financeiros

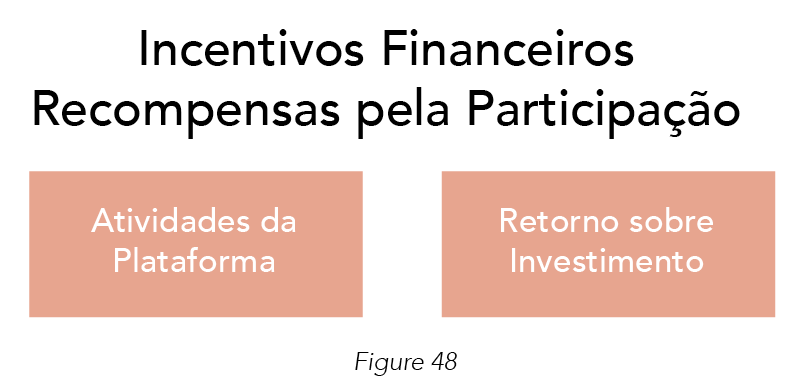


Figura 48

Ecossistemas podem atingir adoção em massa mais facilmente com incentivos financeiros encorajando a participação. Incentivos financeiros incluem atividades da plataforma e retornos sobre investimento. Alguns incentivos são originados na política fiscal em termos de taxas/impostos (taxas de transação), e reservas ou investimentos (oriundos da fundação ou outra entidade operadora do ecossistema).

#### Atividades da Plataforma

Atividades da plataforma podem envolver recompensas financeiras por adesão (ex: *airdrops*), retornos sobre investimento, ou arbitragem nas taxas de câmbio. Incentivos financeiros atuam como condicionantes para o atingimento de efeitos de rede, mas o excesso deles pode causar movimentos de “*pump and dump”*.

##### Inflação de tokens de utilidade

Atividades da plataforma consistem em operações em que o token nativo é usado como recompensa, mesmo quando a atividade em si não está relacionada ao próprio token. Exemplos:

* Compound recompensa credores e devedores com tokens $COMP, sem a necessidade de interação com $COMP.
* Uniswap recompensa provedores de liquidez com $UNI em troca de seu *stake* em mercados descentralizados, sem a necessidade de transacionar em $UNI.

#### Retorno sobre *stake*

Retorno sobre investimento ou retorno sobre *stake* é outra alternativa de incentivo financeiro. Existem muitas maneiras de recompensar *stakers* como forma de mecanismos de incentivo.

##### Inflação de tokens por staking

Diferente do modelo inflacionário de tokens de utilidade, esse tipo de inflação é resultado do *staking*. Usuários podem travar seus tokens nativos e receber recompensas de mais tokens nativos (ex: Kyber recompensa $KNC para *stakers* por meio da alocação de votos de governança).

Esse mecanismo gera uma relação interessante entre tokens travados e índice de inflação do ecossistema.

##### Registros Curados de Tokens (TCR)

TCR (*Token Curated Registry*, ou Registros Curados de Tokens) era muito popular em 2018/19 (vide 8.11.1 para mais detalhes). Ao invés de utilizar *staking* como colateral, provisão de liquidez, ou parte da governança, TCRs usam *staking* como sinalização de preferências. Usuários são recompensados por sua participação em tokens nativos. Ocean Protocol usa um tipo de TCR em camadas[[86]](#footnote-87), possibilitando usuários ranquearem conjuntos de dados e receberem $OCEAN.

##### Ativos Financeiros/Ações Tokenizadas (Securities)

Tokens considerados *securities* podem funcionar como uma alternativa para ativos de finanças tradicionais, mas existe um custo de oportunidade em manter esses tokens. O retorno do investimento é um fator crucial para projetos de DeFi em desenvolvimento.

*Em DeFi, esse mecanismo de “retorno sobre o stake” é combinado com funções de utilidade de governança para adicionar valor agregado ao token nativo. Na prática, temos uma mistura de duas classes de ativos em finanças tradicionais: ações e renda fixa.*

##### Tokens não-fungíveis

No final de 2020, vimos uma fusão de duas categorias cripto: finanças (DeFi) e arte (arte digital, generativa, colecionáveis, games). Aavegotchi, por exemplo, foi um dos projetos que combinou ambos. Protocolo possibilita que usuários coloquem seus $aDAI em *stake* (sub token $DAI do protocolo Aave), gerando tokens não-fungíveis (NFTs) e concede acesso à plataforma Aavegotchi.

Sistemas como esse possuem capacidade de composição, facilitando a interação e construção conjunta com outros protocolos.

#### Arquitetura

*Tokens podem ajudar no controle de ações por meio de direitos de propriedades e no nível de confiança por meio de estrutura apropriada.*

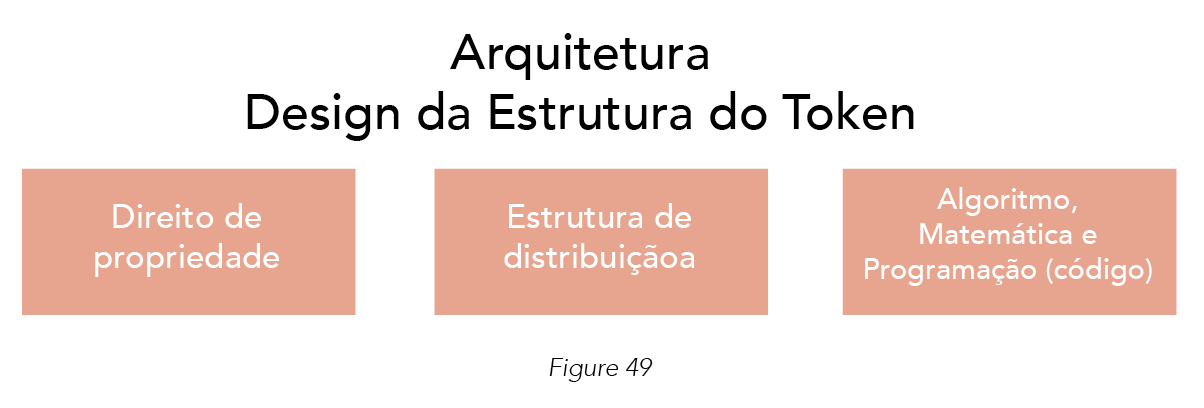


Figura 49

A arquitetura do token reflete exatamente os componentes que formam o próprio token, como direitos de propriedade (definir os direitos que o token oferece, e retornos baseados nesses direitos) e elementos de identidade.

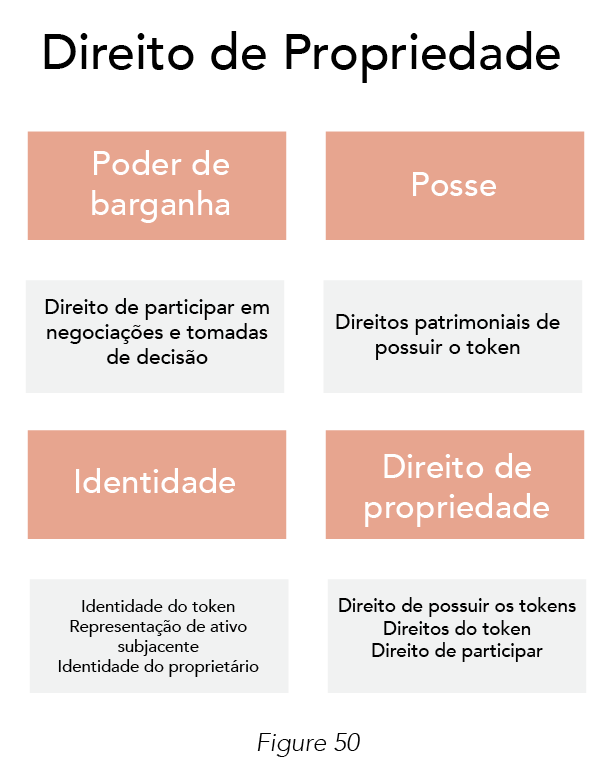


Figura 50

Direito de propriedade inclui poder de barganha, posse, e identidade. Além do direito de possuir o token, pode incluir também direito de fazer *stake* (travar tokens em troca de rendimentos no próprio token), direito de participar nos mecanismos de governança, direito de ser proprietário de pequena parte do projeto ou ativo subjacente etc. Quando combinamos esses conceitos com políticas de token como juros, possibilitamos formas novas e criativas para incentivar os usuários.

Identidade é outra variável a se considerar. Blockchain possibilita o direito de propriedade inerente ao conceito de identidade própria, dada alta rastreabilidade de propriedade sem a necessidade de um terceiro.

##### Design de tokens não-fungíveis (NFTs)

Na estruturação de tokens, é sempre importante ter em mente os demais tipos de token existentes. A classe de tokens não-fungíveis representa ativos do mundo real, ativos digitais únicos, ou direitos - como de propriedade intelectual, e irá criar novas formas criativas para enriquecer a estrutura de incentivos de tokens.

|  |
| --- |
| Caixa 2: Estudo de Caso Sobre Moedas (Dinheiro) Digitais  Uma das principais estratégias para atingir adoção em massa é estender a função dos tokens para fora do ecossistema nativo, ao invés de restringir transação internamente.    Figura 51  Moedas digitais existem apenas na forma eletrônica e podem ser operadas independentemente de um banco central. Assim como moedas ou notas físicas, moedas digitais são uma forma de dinheiro com três funções principais: unidade de medida, meio de troca, reserva de valor.  Moedas digitais têm as seguintes vantagens, entre outras, comparadas à moedas físicas:   * Transações instantâneas * Atualização automática do “livro razão” (*ledger*) * Transferência livre de propriedade entre países   Moedas digitais não são uma novidade. O que **é novo** é a infraestrutura tecnológica em que essas moedas são desenvolvidas. Moedas digitais só podem existir em *ledgers* (registros, livro razão) digitais, e hoje temos outros modelos inovadores, como a tecnologia de registro descentralizado.  **Tipos de Moedas Digitais**    Figura 52  **Moedas com curso legal (*Legal Tender*)**  Moeda Digital do Banco Central  CBDCs funcionam como uma nova forma digital da moeda tradicional (*fiat*), e são emitidas pelo banco central. *Fiat* é o dinheiro estabelecido por meio de regulamentações ou leis do governo. Outras terminologias incluem moeda *fiat* digital, ou base monetária digital.  Base monetária é o dinheiro presente em uma economia, incluindo reservas de bancos comerciais, dinheiro em circulação, e notas físicas armazenadas nos cofres do banco central (ou na *ledger* deles). É basicamente dinheiro líquido, podendo trocar por outros ativos sem dificuldades.  Podem ser construídos em DLT ou em *ledgers* digitais privadas não-distribuídas.  **Moedas sem curso legal**  Moedas digitais sem curso legal incluem criptomoedas emitidas de forma privada e moedas virtuais.  Criptomoedas de Emissão Privada  Criptomoedas emitidas de forma privada são moedas digitais emitidas em DLTs (tecnologia de registros distribuídos) e protegidas por criptografia. Por isso o termo, combinação de “cripto” e “moeda”. Emissão privada significa que foi feita por uma instituição privada, fundação ou consórcio.  Isso é diferente das moedas emitidas por instituições regulamentadas pelo governo, como bancos centrais, ou instituições de crédito.  O propósito de desenvolver cripto em DLTs é que funciona de forma distribuída, de várias formas, dependendo da DLT específica utilizada.  Moedas Virtuais de Emissão Privada  Moedas virtuais são um tipo de dinheiro virtual geralmente não-regulamentado e aceito apenas no ecossistema ou comunidade específica. Possui características similares às moedas tradicionais (*fiat*), mas não possuem curso legal e não são emitidas por um banco central.  A comunidade *gamer* do World of Warcraft, por exemplo, utiliza “ouro” (*gold*), enquanto usuários Tencent podem usar a moeda “QQ” em vários ambientes do ecossistema da empresa.  **Políticas monetárias que podem ser implementadas**    Figura 53  Visto que moedas digitais são uma forma de dinheiro, políticas monetárias podem ser usadas para sua administração. Políticas monetárias governam tanto dinheiro físico, quanto moedas digitais. Mais especificamente, políticas monetárias afetam a oferta existente de determinada moeda – enquanto as forças de mercado afetam a demanda por essa moeda.  **Curso Legal**  Moeda Digital do Banco Central  Assim como com dinheiro físico, bancos centrais implementam em CBDCs políticas monetárias para agir sobre a oferta circulante da moeda – aumentar ou diminuir. Ferramentas comuns usadas por bancos centrais incluem:   * Taxa de inflação * Taxa de juros * Reservas mínimas exigidas * Taxa interbancária * Operações em Mercado Aberto (*OMO*): Compra ou venda de títulos governamentais * Flexibilização quantitativa   **Sem Curso Legal (*Non-legal Tender*)**  Existem dois tipos de moeda sem curso legal:   1. Moedas que tem taxa de conversão (câmbio) fixa de 1:1 (ou outra proporção) 2. Moedas com políticas monetárias independentes. Pode ser uma taxa fixa ou auto-determinada   Taxa de Conversão Fixa  Moedas digitais com taxas de câmbio fixas[[87]](#footnote-88) não possuem políticas monetárias independentes e seguem as políticas da moeda a qual estão atreladas (ex: uma moeda digital pareada com dólar segue as políticas monetárias do Federal Reserve, ou Fed).  Política Monetária Independente  Moedas digitais de câmbio livre (*un-pegged*) têm suas políticas monetárias independentes. Implementam medidas assim como bancos centrais:   * Taxa de juros * Ativos colateralizados (ativos referentes ao colateral que suporta o valor da moeda nativa) * Emitir ou remover moedas nativas de circulação * Alavancando ativos colateralizados: diferente dos índices obrigatórios impostos por bancos centrais aos bancos comerciais, política monetária pode alterar a alavancagem sobre um determinado ativo colateralizados   Moedas digitais não são novidade, assim como as políticas monetárias usadas para intervir na oferta de uma moeda. O que há de novo, porém, são ferramentas inovadoras com implementação eficiente de políticas monetárias. |

### Design e Economia de Tokens

Todos os tokens são **diferentes** em suas funções. Muitas dessas funções formam a base dos mecanismos do token e da economia – umas mais relevantes do que outras.

#### Políticas de Token (Atributos de um Token)

Políticas de token podem ser definidas na etapa de design, e posteriormente implementadas no código do ecossistema do token.

1. Políticas monetárias
   1. Oferta de tokens, aumento de moedas em circulação esperado
   2. Tokens inflacionários, desinflacionários, ou deflacionários
   3. Distribuição na alocação de tokens
   4. Velocidade: frequência em que os tokens mudam de mãos
   5. Regime de taxas de conversão: taxa fixa (*pegged*), taxa intermediária, taxa livre
   6. Zero Lower Bound - ou "limite inferior a zero": alteração nas taxas de juros de curto prazo para estimular/desestimular consumo
   7. Taxa de juros negativa ou moeda com data de expiração – aplicável para tipos de token específicos
   8. Índice de reserva mínima ou nível de alavancagem concedido sobre colaterais
2. *Valuation* do token: variáveis que permitem o token ter valor endógeno:
   1. Fatores endógenos
      1. Garantido por ativos off-chain: moedas *fiat,* ouro, possivelmente títulos governamentais
      2. Curvas de ligação (*Bonding curves*, tema abordado no Capítulo 11)
      3. Valor presente líquido
      4. Valor esperado dos fundos
      5. Equilíbrio dinâmico de preço
      6. Crescimento da demanda pela plataforma ou token
      7. Função poupança, dependendo da taxa de crescimento

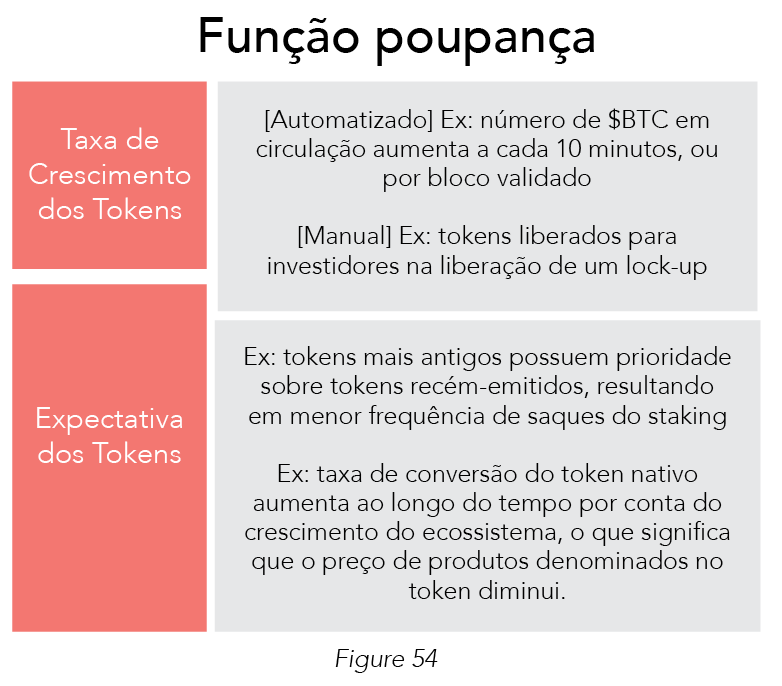


Figura 54

**Taxa de Crescimento dos Tokens**

* 1. [Automatizado] Tokens com inflação fixa aumentam o limite da oferta em cada período
  2. [Manual] Inflação de token relacionado às recompensas de *staking* ou tokens travados (*lock-up* )

**Expectativa de preço futuro (ou utilidade) de tokens**

* + - * 1. Segurar o token por mais tempo aumenta a prioridade (rank) sobre tokens emitidos mais recentemente. Pode resultar em períodos de *lock-in* mais curtos em mecanismos de *staking*
        2. Taxa de conversão do token nativo aumenta ao longo do tempo por conta do crescimento do ecossistema, o que significa que o preço de produtos denominados no token diminui. Cria o incentivo de segurar os tokens com expectativas de preços de produtos menores.
    1. Heterogeneidade da base de usuários revela níveis de tolerância ao risco diferentes, assim como a demanda em diferentes momentos.
    2. Produtividade da plataforma reflete na expectativa de crescimento da demanda, eficiência na coordenação de participantes, e atingimento de objetivos.

1. Mercado dita:
   * 1. Leilão holandês: Como o leilão de Vickrey-Clarke-Groves. Leilão holandês maximiza o bem-estar social gerado. Funciona para muitos tipos de ativos, e ativos são precificados pelo mercado. Por exemplo, títulos governamentais ou lançamento de um novo token.
     2. Taxas de conversão dos tokens referente ao dólar reflete a disposição de compradores em adquirir o ativo por meio de *order books* e formadores de mercado automatizados (*Automated Market Maker)*
     3. Escassez de tokens influenciando na precificação causa competição de compradores e revela os valores dos consumidores
     4. Expectativas racionais da taxa de câmbio no próximo período
     5. Valor para os usuários: ecossistema ou efeitos de rede que agregam valor aos usuários
     6. Formadores de mercado automatizados usam cada *pool* de tokens para determinar os preços de mercado. Traders de arbitragem facilitam esse processo de atingimento de equilíbrio de preços em várias corretoras diferentes

#### Incentivos Financeiros (Elementos)

Incentivos financeiros podem oferecer recompensas pela participação no ecossistema e fortalecer o mecanismo de compatibilidade de incentivos para atingir os objetivos:

1. Atividades da plataforma
   1. Taxa de transação
   2. Recompensas pela afiliação à rede
   3. Tokens de desconto (see Chapter: 14)
   4. Links de referência
   5. Políticas de recompensas além da mineração
2. Retorno sobre investimento
   1. Retornos esperados sobre tokens possuídos: via *staking* ou mudanças no valor do ativo subjacente
   2. Arbitragem de preço de tokens em corretoras
   3. Volatilidade de preço
   4. Mecanismos de liquidez: corretoras, funcionalidades para liquidez
   5. Nível de risco do token

#### Arquitetura (Design da Estrutura do Token)

Tokens podem ajudar a governar ações por meio de direitos de propriedade, e estabelecer a confiança por meio de economias de escala.

1. Direito de propriedade
   1. Economia do Direito de Propriedade: direito de reivindicação, direito de posse, direito de participar na governança
   2. Taxa de Harberger
   3. Representação de identidade e direitos da identidade (ex: pessoa, arte, representação digital de algo físico)
2. Distribuição
   1. Alocação e trava (*lock-up*) de tokens em períodos diferentes
   2. Financiamento inflacionário “por convicção”: distribuição de novos tokens como função do número de tokens em *stake* e duração do período de *staking*
3. Algoritmo e código de token revisado por pares

|  |
| --- |
| Caixa 3: Curso Rápido sobre Política Monetária Tradicional  Banco Central  Política monetária determina como a moeda é administrada e governada. Em TradFi, bancos centrais nacionais geralmente comandam essas decisões.  Política monetária busca atingir dois objetivos:   * Garantir estabilidade de preços por meio da administração da oferta de dinheiro em circulação comparado à demanda real sobre o ativo * Garantir confiança sobre a moeda, encorajando as pessoas a transacionarem por meio dela   Existem dois tipos básicos de política monetária: expansionista (mais dinheiro em circulação) e contracionista (menos dinheiro em circulação). Dependendo da economia, que define a **demanda real pelo dinheiro**, um desses dois tipos será implementado.  **Ferramentas Comuns de Política Monetária**  **Operações de Mercado Aberto**  Uma das maneiras que a oferta de dinheiro pode ser alterada é alterando a taxa de juros do dinheiro por meio de operações de mercado aberto (*Open Market Operations*, ou *OMO*). Na prática, temos bancos centrais vendendo ou comprando títulos governamentais, para aumentar ou diminuir a oferta circulante.  Quando vendem, pegam dinheiro de cidadãos e outros países emprestado, com a promessa de retornar o valor cheio, mais algum extra em forma de dividendos (taxa de empréstimo) por período definido. Esses títulos governamentais também podem ser negociados no mercado secundário.  **Taxa de Desconto**  Bancos centrais também ajustam a taxa de desconto, que é basicamente a taxa de juros cobrada pelo próprio banco central à bancos comerciais.  A taxa de desconto influencia no quanto bancos comerciais pegam emprestado do banco central, e consequentemente no quanto podem emprestar para clientes. Taxas de juros maiores fazem bancos comerciais pegarem menos empréstimos, enquanto taxas menores induzem a pegarem mais empréstimos.  **Reservas Mínimas Exigidas**  Bancos centrais também impõem reservas mínimas, determinando o quanto bancos comerciais precisam manter em seus cofres - e quanto podem emprestar para clientes. Essa política busca garantir que bancos tenham dinheiro suficiente para quando as pessoas solicitarem seus saques.  Em setembro de 2019, o PBoC (Banco do Povo Chinês) cortou a reserva mínima para 13 porcento nos grandes bancos e 11 porcento nos pequenos para aumentar a oferta em circulação e estimular as atividades econômicas. Quanto menor a reserva exigida, mais empréstimos podem oferecer aos consumidores.  **Flexibilização Quantitativa (ou *Quantitative Easing)***  Mais conhecida como "impressão de dinheiro". Na prática, porém, por mais que introduza mais dinheiro na economia, não está relacionada à impressão de dinheiro físico, cash. Bancos centrais criam novas reservas em seu balanço patrimonial, e usa essa nova reserva para comprar títulos governamentais ou outros ativos financeiros, resultando na inserção de dinheiro adicional da reserva criada na economia. Política de flexibilização quantitativa é uma forma relativamente nova de política expansionária e usada quando políticas típicas são ineficientes.  **Trindade Impossível**  A trindade impossível é um trilema que bancos centrais enfrentam; podem escolher até duas das três opções a seguir, e têm de lidar com os *trade-offs*:   * Taxa de câmbio fixa: taxa de conversão fixa com relação à moeda de outro país, e portanto afetada pelas políticas monetárias da mesma * Fluxo livre de capital: dinheiro pode se movimentar para dentro e para fora do país com facilidade. Juros e taxas de câmbio influenciam na direção desse fluxo de dinheiro, visto que há um custo de oportunidade dessa movimentação. Taxas de juros favoráveis (maiores) em outro país pode causar fluxo de saída de capital do país nativo, reduzindo a demanda pela moeda corrente do país e aumentando a demanda pela moeda do outro país * Política monetária soberana: política monetária independente, em que bancos centrais podem alterar unilateralmente a taxa de juros   **Economia Monetária**  Política monetária é um dos aspectos de economia monetária. Existem outros fatores a se considerar, e que afetam a oferta circulante de dinheiro, podendo ser administrados pelo banco central ou outras agências de estado.   * Política fiscal: Administra oferta monetária indiretamente na mudança de impostos, gastos governamentais, e emissão de títulos governamentais. * Âncoras nominais: variável, para limitar as expectativas de agentes com relação ao nível de preço nominal   + Métodos de longo prazo para estabilidade de preço e confiança   + Regimes de câmbio   + Uniões monetárias (UE)   + Câmbio flutuante controlado (HKD-USD)   + Câmbio flutuante (USD, GBP, CHF, JPY)   + *Pegs* (Panama-USD) |

## “Curvas de Ligação”, ou *Bonding Curves*

Curvas de ligaçãosão usadas para vincular duas[[88]](#footnote-89) variáveis. Essa ferramenta é mais utilizada por DEXs[[89]](#footnote-90) e ou em captação de recursos.

### Definindo Curvas de Ligação

Curva de ligação, ou *bonding curve*, é uma curva gráfica (equação) que conecta duas variáveis. Por exemplo, o preço do token muda conforme a oferta em circulação. Esse valor é determinado matematicamente, por meio do código do contrato inteligente. Nesse caso, fatores como transações no mercado secundário não influenciam no preço.

Existem três principais casos de uso para curvas de ligação:

1. Captação de recursos utilizando uma função de compra e venda (ex: Aragon, Hegic)
2. Determinar preços em um economia fechada (ex: precificação do $NXM, da Nexus Mutual, ou corretoras descentralizadas)
3. Captação de recursos contínua de protocolos (por mais que isso aproxime o ativo da classificação de *security*, classe ainda não regulamentada até 2022)

No caso de captação de recursos, incentiva investidores a comprarem seus tokens o mais cedo possível, visto que é mais barato nos estágios iniciais da rodada.

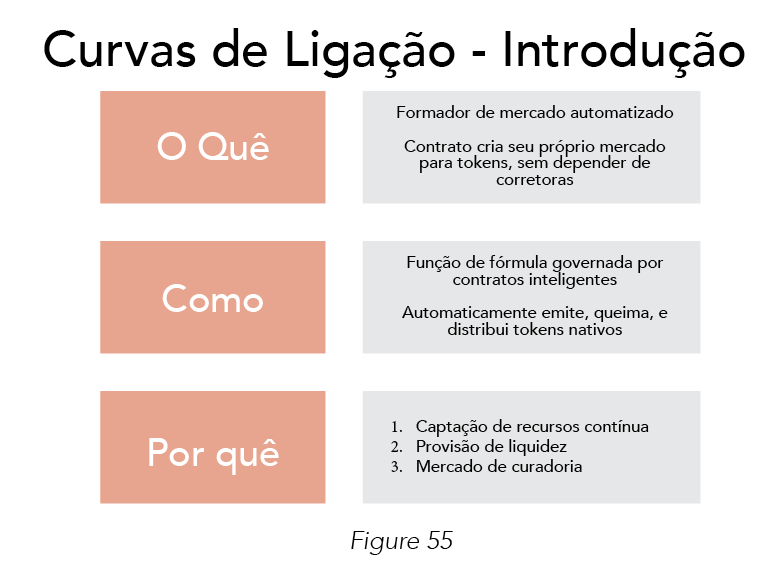


Figura 55

#### Caso de Uso 1: Corretoras Descentralizadas via Formadores de Mercado Automatizados (Automated Market Makers)

*Exemplos e cálculos específicos no Capítulo 13.*

Curvas de ligação são executas por contratos inteligentes e podem criar suas próprias dinâmicas de mercado/precificação, sem a necessidade de *order books*. O termo mais utilizado em web3 para isso é “*Automated Market Maker*” (AMM), ou formadores de mercado automatizados. Duas principais diferenças desse sistema comparado à corretoras tradicionais:

1. AMMs precificam ordens de compra ou venda de ativos por meio de fórmulas matemáticas, ao invés de livros de ordens centralizados (CLOBs).
2. AMMs funciona via crowdsourcing, com vários indivíduos participantes ao invés de empresas especializadas ou baleias – conceito de **pool de liquidez**.

Formadores de mercado automatizados, ou AMMs, precisam ter acesso à uma pool de liquidez. Para incentivar pessoas a contribuírem para a liquidez, provedores recebem taxas de transação em tokens nativos quando transações são executadas.

**Exemplo:** A pool de liquidez tem dois tipos de token: $ETH e $TOKEN. Provedores adicionam valores correspondentes de $ETH e $USDC (50/50). Vamos dizer que um investidor tenha o montante total referente a 10% dessa pool específica. Quando alguma transação entre $ETH e $TOKEN é processada, investidor recebe 10% das taxas de transação.

Na execução de trades em corretoras descentralizadas (DEXs), o que está efetivamente sendo feito é o depósito de um Token A em troca de outro Token B da pool. A quantidade de Token B recebida nessa transação é determinada matematicamente e executava por meio de contratos inteligentes.

**Exemplo:** Giovanni adiciona X $ETH na pool e recebe Y $TOKEN em troca. A quantidade de $TOKEN recebida por Giovanni (Y) depende da proporção total dos montantes de $ETH e $TOKEN existentes na pool de liquidez. Preços não são fixos e flutuam com base em cálculos feitos pelos AMMs.

#### Caso de Uso 2: *Bonding Curve* para Captação de Recursos

Captação de recursos requer contratos inteligentes imutáveis. Esses contratos inteligentes utilizam *bonding curves*, ou curvas de ligação para emitir, queimar e distribuir tokens de forma automática.

A quantidade emitida, queimada e distribuída é definida pela fórmula matemática.

#### Caso de Uso 3: Mercado de Curadoria

“Mercados de curadoria” têm relação com o uso de tokens como sinal para reduzir assimetria de informações (ex: Ocean Protocol). Vamos falar um pouco mais desse caso de uso na Parte II: Capítulo 25.

Mercados de curadoria ficam mais evidentes quando combinamos NFT e DeFi. Usuários podem colocar seus tokens em *stake*, de acordo com a *bonding curve*, em troca de NFTs. Esse conceito utiliza tanto mecanismos de DEX do Caso de Uso 1, quando mecanismos de captação do Caso de Uso 2, dependendo da situação. As possibilidades são imensas, e são importantes para o futuro da tecnologia DeFi.

### Quatro Propriedades de *Bonding Curves* (“Curvas de ligação”)

1. **Preço é predefinido no código, de acordo com a curva matemática.**

Tokens podem ser emitidos ou trocados a qualquer momento diretamente com o contrato inteligente, garantindo aos usuários uma parte da reserva (colateral) ou ativos proporcionais ao capital contribuído. O contrato inteligente se torna o formador de mercado.

1. **Preço é definido por uma fórmula, que está codificada no contrato inteligente.**

De forma geral, preços aumentam conforme mais tokens estão em circulação. A curva matemática[[90]](#footnote-91) pode ser definida com várias variáveis que afetam os objetivos do ecossistema.

1. **Contratos inteligentes governam o sistema**

No primeiro caso de uso, contratos inteligentes executam as transações com a pool de liquidez, funcionando como um formador de mercado automatizado. O preço depende na “profundidade” da pool, ao invés de preços de corretoras externas. No segundo caso de uso, colateral é mantido em contratos inteligentes como reserva e contratos inteligentes executam a fórmula matemática referente.

1. **Possibilita o direito à fluxos de caixa futuros governado por contratos inteligente.**

Para não funcionar como esquemas Ponzi, tokens devem oferecer fluxos de caixa futuros do ecossistema. Pode ser em forma de taxas de transação, ou outros tipos de retornos do sistema.

### Considerações Sobre *Bonding Curves*

#### Valor Intrínseco

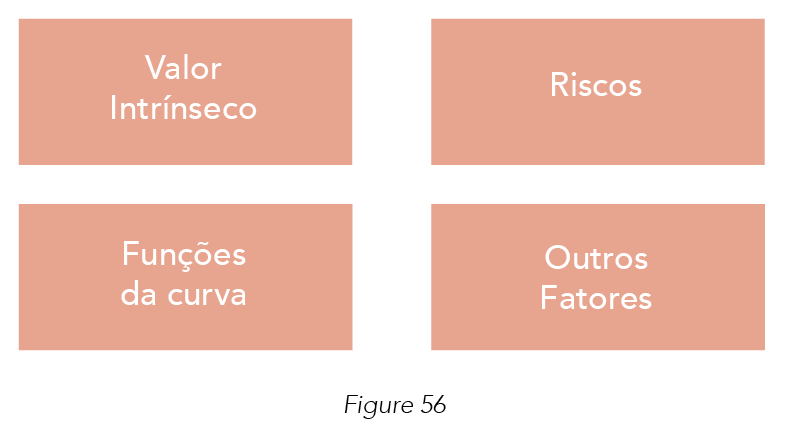


Figura 56

Valor intrínseco varia dependendo do caso de uso.

##### Corretores descentralizadas

Valor está baseado na facilidade de acesso e ampla disponibilidade de liquidez, assim como a rede de integração e possibilidade de interação com outros tokens.

##### Captação de Recursos

Valor está baseado no direito à fluxos de caixa futuros. Além disso, o valor aumenta conforme mais participantes entram no ecossistema e de acordo com a receita gerada. Dependendo do sistema, é provável que reguladores interpretem esse tipo de token como *security* (ativo/ação tokenizada, devendo obrigatoriamente atender às normas tradicionais da instituição responsável no país, como a CVM por exemplo).

##### Mercados de Curadoria

Valor pode ser derivado do direito à fluxos de caixa futuros ou da sinalização precisa de sentimentos de mercado.

Para produtos no domínio de propriedade intelectual, NFTs podem ser emitidos e transacionados por meio de *bonding curves* para a compra e venda de direitos de propriedade intelectual (IP). A propriedade intelectual é anexada ao NFT, possibilitando a transferência de posse. Essa transferência ocorre por meio de uma *bonding curve* e o comprador envia os fundos como colateral para o contrato inteligente para receber o NFT em troca. O preço dos NFTs aumentam quanto maior a demanda por eles (sinais tokenizados para curadoria[[91]](#footnote-92)). Em outras palavras, quando o preço do NFT sobe, significa que a demanda pela propriedade intelectual também aumenta. Portanto, essa “IP” está sendo curada por sinais de preço via NFT.

#### Mitigando Riscos

##### Corretoras Descentralizadas

Riscos: transações são validadas logo antes de uma compra massiva por meio de taxas de transação (gás) maiores.

Soluções: colocar limite máximo nas taxas de cada transação, ou uma taxa baseada em uma porcentagem do total transacionado.

##### Captação de Recursos

Riscos: Ponzi, pirâmide, esquemas de *pump and dump*.

Soluções: garantir que não há lucros a se receber no curto prazo, reduzindo a especulação e encorajando pessoas de participarem no longo prazo. Isso influencia no comportamento de usuários e incentiva a manterem seus tokens na carteira para receberem lucros futuros. Além disso, garante que a curva é suportada por uma parte da receita do ecossistema.

* Trava de tempo na venda de tokens
* Prêmio por vender tokens
* Desabilitar função de venda (exceto em mercados secundários)
* Proporção da receita que suporta a curva

##### Mercado de Curadoria

Riscos: manipulação de dados por alguém com muitos tokens, definindo seu retorno para o período.

Soluções: contrato pode incluir o mecanismo de *staking* contínuo e curadoria para aumentar o custo de manipulação de dados.

#### Funções da Curva

Não existe uma função perfeita para curvas de ligação – *bonding curves*. Depende dos objetivos do ecossistema e do caso de uso. Algumas funções comuns incluem: linear (), potência (), exponencial (), logarítmica (), e variações ()[[92]](#footnote-93).

Vale mencionar o uso de curvas 3D. Esse modelo introduz o eixo Z (além do X e Y), outras formas de afetar o preço do token. Pode ser o nível de produtividade da plataforma, curva de adoção da tecnologia, usuários no sistema, usuários ativos em comparação ao total de usuários (*churn*) etc.

##### Função Linear

Preço e oferta estão relacionados linearmente, o que pode ser um problema quando o tamanho e demanda pelo projeto aumenta. Funções lineares recompensam os primeiros entrantes de forma excessiva comparado aos investidores retardatários. Por último, não oferece muitas alternativas matemáticas, já que temos apenas as variáveis **m** e **c** para manipular.

##### Função Exponencial

Funções exponenciais aumentam o preço lentamente nos primeiros períodos, encorajando participantes a segurarem seus tokens. Porém, a função acelera agressivamente nos últimos 20% da curva e preços se tornam mais voláteis. Essa característica causa especulação adicional, além de taxas de crescimento acentuadas e insustentáveis. Taxas de crescimento exponenciais podem ser afetadas por meio da criação de valor ou administração da oferta monetária (controle de inflação).

Funções logarítmicas funcionam de forma oposta: preços aumentam bruscamente nos primeiros períodos, criando especulação e volatilidade, mas eventualmente estabilizam.

##### Outros fatores a considerar

* Incentivar pioneiros na adoção (*early adopters*)
* Estabilidade de preços no período de maturidade
* Aumento de custos baseado em algum fator de oferta circulante (produtividade da plataforma ou token)
* Prevenção de abusos ou arbitragem
* Crescimento do produto (*s-curve*, ou “curva S” como uma função do eixo Z)

### Perguntas Práticas para Começar

* Qual é a função das chamadas *bonding curves*, ou curvas de ligação? Corretora descentralizada (liquidez immediate), captação de recursos, mercado de curadoria ou outra?
* Quantos usuários o projeto consegue atrair e manter? (Tanto no estágio introdutório, como no estado de maturidade)
* Pioneiros e retardatários estão sendo incentivados adequadamente para participarem? Você quer que eles sejam incentivados de forma igual?
* É possível levantar a quantidade de capital necessária para levar o projeto à um nível satisfatório de adoção?

### Duas Variações de Curvas de Ligação (*Bonding Curves*)

#### Aumentada (ABC)

Baseada em pesquisas de sistemas complexos. Faz parte do design de um novo mecanismo de incentivo. Seu objetivo é criar uma nova forma de modelo de financiamento, governada pelos participantes das organizações.

O problema com o modelo básico de curvas de ligação é estar sujeita à manipulação e especulação.

Curvas de Ligação Aumentada (ou *ABC*) usam o princípio físico de leis de conservação[[93]](#footnote-94) e outros mecanismos para criar ambientes robustos e controlados, administrar a especulação, e alinhar incentivos para gerar retornos positivos. Tokens emitidos inicialmente ficam travados no primeiro período, para reforçar a estabilidade da reserva. Em resumo, essa variação combina o conceito da curva de ligaçãobásica com elementos de financiamento, mecanismos de *lock-in*, e sistema interno de loops de feedback[[94]](#footnote-95).

#### Dinâmica (DBC)

O objetivo é incentivar os primeiros participantes do ecossistema (*early adopters*), punir agentes parasitas, e encorajar participação ativa no ecossistema.

O problema com curvas de ligação genéricas é que são facilmente manipuladas por usuários com grandes quantidades de token (baleias), o que aumenta a volatilidade de forma injusta.

Por isso, curvas de ligação do tipo DBC adicionam uma funcionalidade para que o preço do token seja determinado pela proporção de tokens possuídos[[95]](#footnote-96). Esse mecanismo encoraja a participação contínua de usuários.

## [Estudo de Caso] Bancor

O protocolo da Bancor é parte do movimento DeFi e age como um formador de mercado automatizado, ou AMM. Bancor possibilita liquidez instantânea e contínua de tokens com menos demanda/volume de transação. Os preços e circulação dos tokens é definido matematicamente e governado por contratos inteligentes.

Existem dois tipos de tokens no ecossistema, um token de utilidade que tem o objetivo de prover liquidez ao ecossistema (*liquidity token*), e um token que representa a reserva do protocolo – e *relay tokens,* ou tokens de LP, uma derivação de ambos os tipos de token.

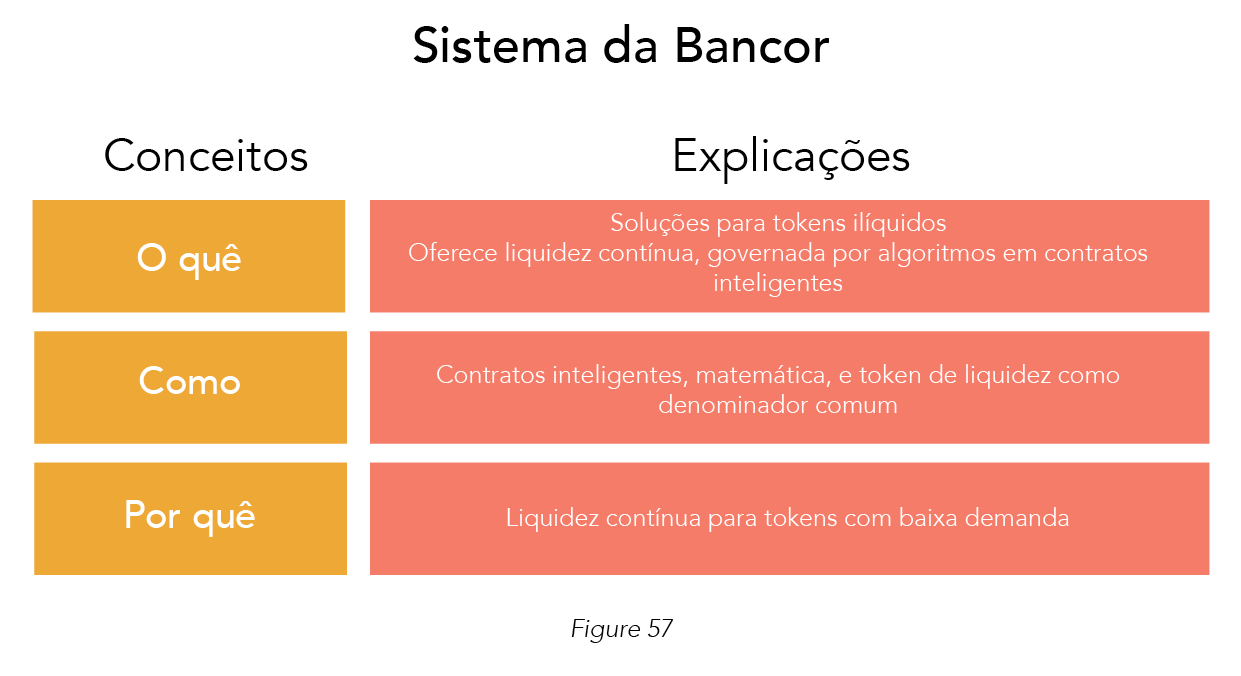


Figura 57

### Introdução ao Protocolo Bancor

**Liquidez contínua**

Bancor oferece soluções para tokens com problemas de liquidez. O protocolo provém liquidez contínua[[96]](#footnote-97), e a liquidez é governada por algoritmos em contratos inteligentes[[97]](#footnote-98). Bancor não precisa de corretoras ou oráculos para fornecer preços de tokens, taxas de conversão, ou liquidez. Utiliza um mecanismo de liquidez autônoma, que determina automaticamente o preço do token (vide Caso de Uso 1 de curvas de ligação no Capítulo 11).

**Governado por contratos inteligentes**

Liquidez é executada e governada por contratos inteligentes, utilizando um token como denominador[[98]](#footnote-99) comum do ecossistema Bancor. Esses tokens são chamados de *network tokens* (“tokens de rede”), mais conhecidos como tokens líquidos. Até o final desse capítulo, o termo “token líquido” será usado para nos referir à esse token de denominador comum.

Contratos inteligentes armazenam saldos de outros tokens e provêm liquidez instantânea entre os vários tokens presentes no ecossistema.

#### Introdução Simples (ELI5)

Imagine uma loja de doces com vários potes de cookies. Cada pote possui uma combinação de cookies de chocolate e um outro sabor.

Você pode trocar cookies de baunilha por chocolote, usando os potes de armazenamento. Visto que todo pote tem cookies de sabor chocolate, você pode trocar seu cookie de baunilha por de chocolate no Pote 1, e posteriormente trocar o cookie de chocolate por de macadâmia.

Da mesma maneira, token da Bancor, $BNT, facilita transações entre uma gama de tokens presentes no “pote”. Ao invés de um “pote”, temos pools de liquidez. Ao invés de cookies de baunilha e macadâmia, existem tokens de vários projetos.

#### Introdução Técnica

Bancor é uma corretora não-custodial que utiliza pools de liquidez para facilitar transações. Intermediários ou mecanismos de *order book* não são necessários.

Ao invés de unir compradores e vendedores, um mecanismo algorítmico formador de mercado provém a liquidez por meio de contratos inteligentes. A proporção (*ratio*) entre o colateral em reserva do contrato inteligente e o token líquido é fixa e embutida no mecanismo algorítmico.

Além de facilitar liquidez entre dois tokens na mesma blockchain, Bancor também oferece liquidez entre blockchains diferentes[[99]](#footnote-100).

O protocolo da Bancor construiu uma rede de liquidez com a gama de tokens do ecossistema conectados ao token de denominador comum (cookie de chocolate). Dado que cookies de baunilha e macadâmia podem ser facilmente trocados pelo token líquido (cookie de chocolate), por propriedade transitiva[[100]](#footnote-101) torna-se simples trocar cookies baunilha por macadâmia (via cookies de chocolate).

Pense no dólar americano (USD) como o denominador comum das moedas globais. A maioria dos bancos centrais ao redor do mundo possuem USD em suas reservas. Caso Hong Kong, por exemplo, queira trocar dólares de Hong Kong (HKD) por franco suíço (CHF), mas a Suíça não tenha interesse em sua moeda, o que eles podem fazer? Podem simplesmente trocar HKD por USD, e no momento seguinte trocar USD por CHF. O fato de ambos os países aceitarem o dólar como denominador comum facilita as transações.

Nesse sentido, o token líquido da Bancor ($BNT) possui utilidade similar ao dólar no mercado financeiro tradicional. Funciona como uma ponte comum facilitadora de transações, visto que todas as criptos existentes no ecossistema (análogo à moedas de países específicos no exemplo acima) aceitam $BNT com liquidez imediata.

### Objetivos da Bancor

O principal objetivo do protocolo da Bancor é prover liquidez como formador de mercado automatizado (AMM)[[101]](#footnote-102) para prover liquidez à tokens com emissão privada. Mesmo que o token seja novo, seja utilizado apenas por usuários de comunidades nichadas, ou tenha pouca demanda no geral, protocolo da Bancor pode prover essa liquidez.

#### Problemas com Liquidez

**Coincidência dupla de desejos/vontades**

Tradicionalmente, liquidez funciona quando existe acordo de desejos entre compradores e vendedores. Ambos precisam querer a **mesma quantia**, no **mesmo momento**, e no **mesmo lugar** para executarem uma transação. A dificuldade está em viabilizar esse encontro entre compradores e vendedores. Pode ser ainda mais difícil quando a demanda (e o volume) é baixo.

**Confiabilidade de corretoras**

Problemas de liquidez podem ser solucionados por meio de corretoras. Porém, a não ser que o token tenha um volume de transações suficiente para a plataforma encontrar compradores e vendedores, estabilidade de preço e liquidez serão comprometidas. Apenas 10 porcento dos tokens listados em corretoras são ativamente negociados – os outros 90 porcento têm pouca demanda e frequência de transações, diminuindo as chances de que uma ordem seja executada[[102]](#footnote-103).

**Problema da “cauda longa”**

A barreira de entrada para um indivíduo criar uma nova criptomoeda emitida de forma privada é muito baixa. Temos visto, como resultado, uma explosão no número de tokens nos últimos anos. Precisamos considerar, porém, a relevância desses tokens. Apenas as criptos no top 10 porcento são transacionadas ativamente, e concentram mais de 95 porcento do volume de transações. Isso significa que 90 porcento dos tokens no mercado possuem baixo volume de trade e pouca (ou nenhuma) liquidez. Esse é o problema da cauda longa: a cauda consiste nos milhares de tokens com baixo volume de transação, representando 90 porcento dos tokens em corretoras. Podem ser tokens de nicho com comunidades restritas ou níveis iniciais de adoção.

#### Soluções para Liquidez

**Formadores de Mercado Manuais[[103]](#footnote-104)**

A solução adotada no mercado financeiro tradicional (TradFi) utiliza formadores de mercado “manuais”. Esses formadores de mercado manuais exercem a função de constantemente comprarem/venderem os mais variados produtos financeiros para solucionar o problema de liquidez – geralmente grandes instituições financeiras com altas reservas de capital. Esses grandes agentes assumem o risco de liquidez e recebem retornos por meio do *spread* – diferença entre o preço “*spot*” atual (preço de tela)e o preço cobrado pelo formador de mercado. Já no mercado cripto, devido à sua volatilidade e nível de risco, não vemos muitos formadores de mercado manuais como em TradFi.

**Formadores de Mercado Automatizados (ou Autonomous, Descentralizados)**

Outra solução envolve a criação de uma liquidez descentralizada por meio de mecanismos embutidos no sistema. A transação sempre será executada por meio de contratos inteligentes. Preços são determinados por algoritmos, de acordo com fórmulas matemáticas específicas, e governados por contratos inteligentes, possibilitando operações de compra e venda ininterruptas. O token de liquidez está integrado com vários tokens, e atua como denominador comum.

### Tokens no Protocolo Bancor

Bancor aplica um modelo de tokens com duas categorias distintas: token líquido e tokens de reserva – e *relay tokens,* ou tokens LP[[104]](#footnote-105) formados pela combinação de ambos.

Nota: Tokens de reserva podem ser liquidados no protocolo da Bancor. Exemplos de tokens de reserva são do tipo ERC20 ou compatíveis com EOS, como $ETH, $BAT, $DAI, $EOS, $EMT e $DICE.

Token líquido funciona como um token inteligente, emitindo ou queimando tokens de acordo com o recebimento/retirada de tokens de reserva. Para aderir ao ecossistema da Bancor, o token precisa incluir $BNT como token de reserva. Todos os tokens da plataforma possuem $BNT como parte de sua reserva. Na prática, $BNT é um token líquido “assegurado” por sua reserva em $ETH.

Tokens de reserva são usados por meio do mecanismo de *staking* para prover liquidez ao ecossistema – *tokens de LP*. Esses provedores de liquidez têm direito a sua fração proporcional dos fluxos de caixa futuros.

#### Elementos de Tokens na Bancor

Existem três tipos de tokens que a Bancor possui: (1) Token líquidos, (2) Token de LP, e (3) Token matriz.

A tabela abaixo explora os tipos de tokens nativos do protocolo Bancor, explicações e exemplos para entendermos essa diferenciação.

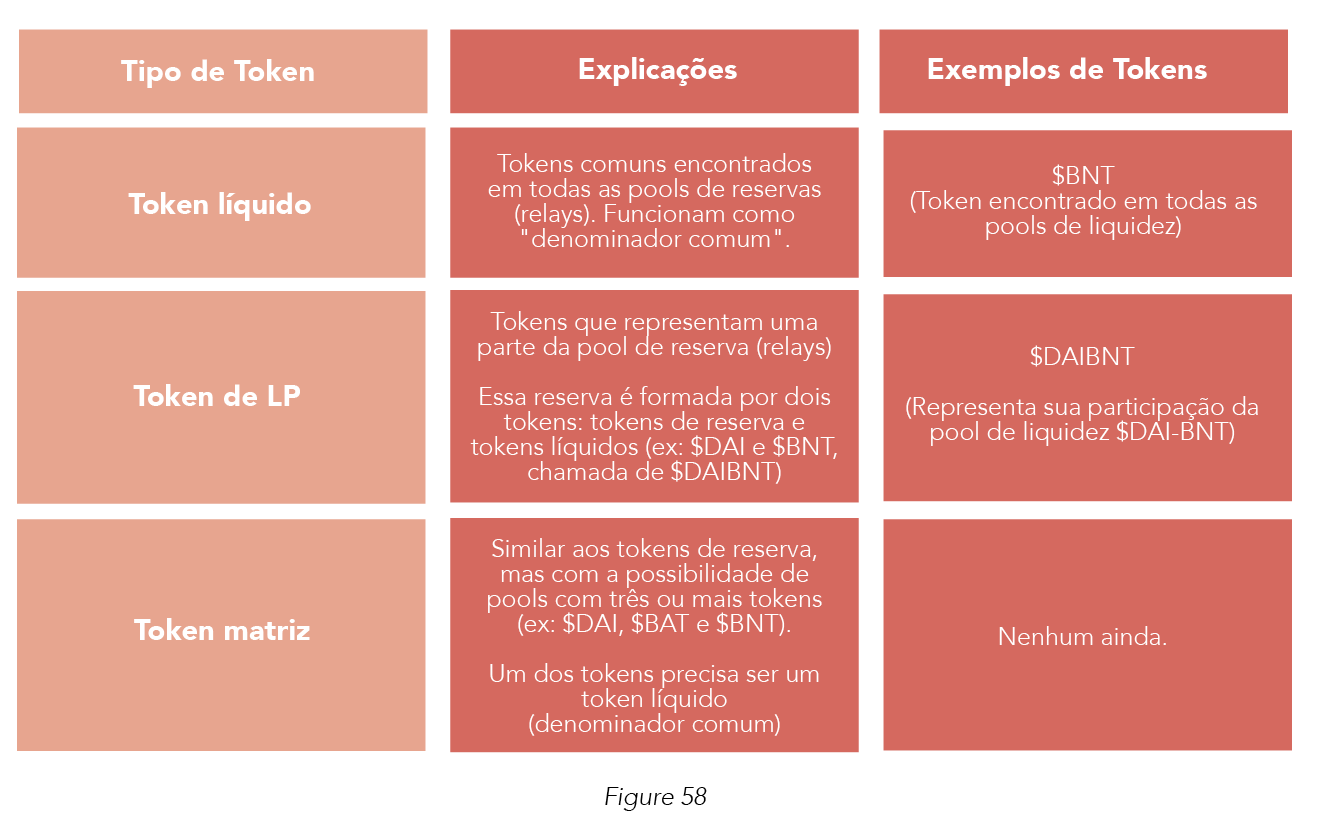


Figura 58

#### Token Líquido

Tokens líquidos são tokens de utilidade que possibilitam a conversão no ecossistema da Bancor. Na prática, permite a convertibilidade instantânea para diversos tokens da rede.

Tokens líquidos são o denominador comum em todas as *pools* de reserva (*relays*) do ambiente. Em suas devidas proporções, são como o dólar: moeda universal e aceita por todas (ou quase todas) reservas monetárias ao redor do mundo. Além disso, não estão sujeitos à riscos de liquidez, graças ao sistema de formador de mercado automatizado via contratos inteligentes.

Qualquer um pode adquirir tokens líquidos ao transferir tokens de reserva para o contrato inteligente, recebendo em troca tokens líquidos recém-emitidos.

Exemplo: tokens ERC20, $DAI e tokens líquidos, $BNT.

1. Use $DAI para comprar $BNT.
2. Envie $DAI para o contrato inteligente, que irá calcular a quantidade a ser emitida e recebida em $BNT.
3. Usuários podem receber $DAI de volta ao enviar $BNT para o contrato. $BNT é queimado, e $DAI é emitido da reserva.

##### Cálculo de Preço

Preços são determinados pela oferta circulante no mercado e um índice de reserva fixo[[105]](#footnote-106). É como as famosas *bonding curves*, ou curvas de ligação[[106]](#footnote-107). Esse índice é fixo e determinado pelo emissor do token. Emissores calculam essa métrica usando o valor da reserva sobre o valor do token líquido.

Utilizado para manter a estabilidade de preços no token líquido.

##### Token Bancor ($BNT)

$BNT é um token líquido da rede Bancor, e está presente em todas as *pools* de reserva. Seu valor deriva-se da capacidade de transacionar com qualquer outro ativo do ecossistema. O protocolo não cobra taxas em transações de $BNT, mas o gás da rede pode variar (taxas da Ethereum variam de acordo com a demanda).

$BNT é um token de utilidade, com propósito de conceder acesso ao ecossistema da Bancor. Seu valor deriva-se de fatores intrínsecos como efeitos de rede e métricas de uso do token $BNT (volume e frequência de transações). O token possui oferta fixa de 75.843.715 $BNT, fazendo com que seu valor varie de acordo com a adoção e ritmo de emissão.

#### Token de LP (*Relay* *Token*)

Tokens de LP representam posse de uma participação dessa reserva. Permitem participação nas *pools* de forma descentralizada. Participantes são incentivados a comprarem tokens de reserva que oferecem taxas de transação como recompensa, gerados quando esses tokens são negociados.

Quando alguém compra um token de LP, ou “*relay*”, está na prática adicionando liquidez às reservas. Os tokens recebidos em troca representam sua contribuição.

##### Cálculo de Preço

Preços são determinados pelos tokens na reserva. Geralmente, dois tokens são usados na *pool* de reserva, tokens de LP e tokens de reserva. Ambos são governados pelo contrato inteligente. A reserva normalmente mantém uma proporção fixa de 50 porcento de cada token da *pool*.

#### Tabela de Resumo dos Tokens

A tabela abaixo compara os dois tipos tokens nativos da Bancor (tokens líquidos e tokens de LP) e tokens de reserva (não-nativos).

**Tipos de Token na Bancor**

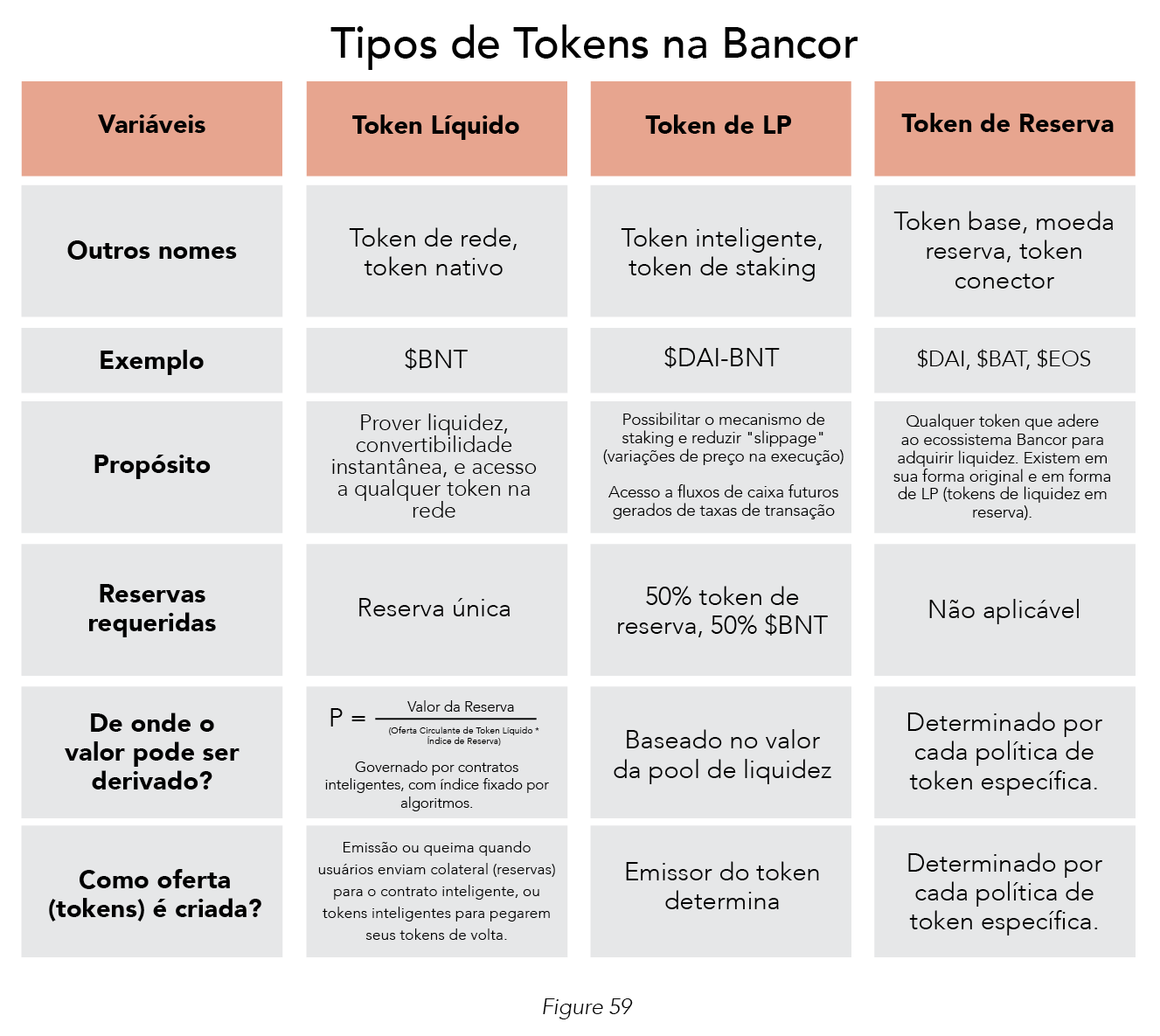


Figura 59

### Bancor e DeFi

DeFi busca transformar o panorama financeiro por meio de transparência, velocidade, e acessibilidade. Não estamos nos referindo a mudanças radicais, mas sim na introdução de novos casos de uso, novos produtos, e melhorias de eficiência. Um dos elementos mais importantes da indústria financeira é a liquidez. Quando ativos presentes no ecossistema são líquidos, temos maior facilidade em executar transações e transferências.

#### Qual a Atuação da Bancor em DeFi?

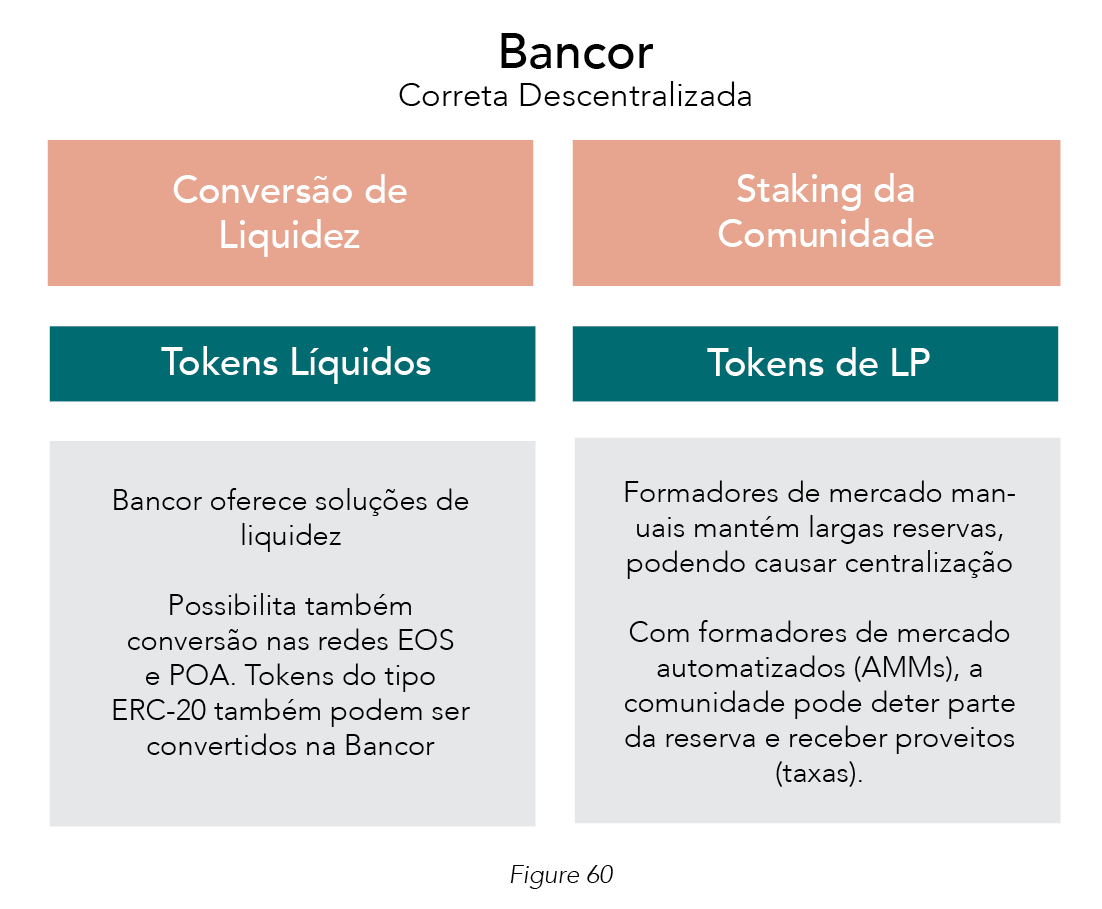


Figura 60

##### Liquidez

Bancor provém liquidez para vários protocolos de DeFi. Além de apenas tokens da rede Ethereum, possibilita também conversão nas redes EOS e POA. Tokens do tipo ERC-20, por exemplo, podem ser convertidos na Bancor por tokens EOS.

##### Staking da Comunidade

Tradicionalmente, formadores de mercado manuais mantém largas reservas, o que possibilita a formação de mercado e pagamento de *spreads* (taxas). Porém, essa necessidade de reservas significativas pode causar centralização.

Com o uso de formadores de mercado automatizados (AMMs), a comunidade pode deter parte da reserva e receber proveitos (taxas) – por meio dos tokens de LP (*relay tokens*).

### Aplicações de Design de Token no protocolo Bancor

Design de token foca na estruturação e construção do token. Busca definir como tokens serão governados e administrados, além de funções e direitos embutidos no ativo.

Nesse estudo de caso específico, vamos discutir a Bancor e seu design de token.

Três principais fatores são:

1. Políticas de token
2. Incentivos financeiros
3. Arquitetura

**Políticas de token**

Política de token determina como tokens são governados e administrados. Pode incluir uma combinação de automação por contratos inteligentes e contribuição de participantes por mecanismos de governança.

**Política monetária:** como tokens são governados.

**Valuation:** como tokens ou ecossistemas são avaliados/precificados.

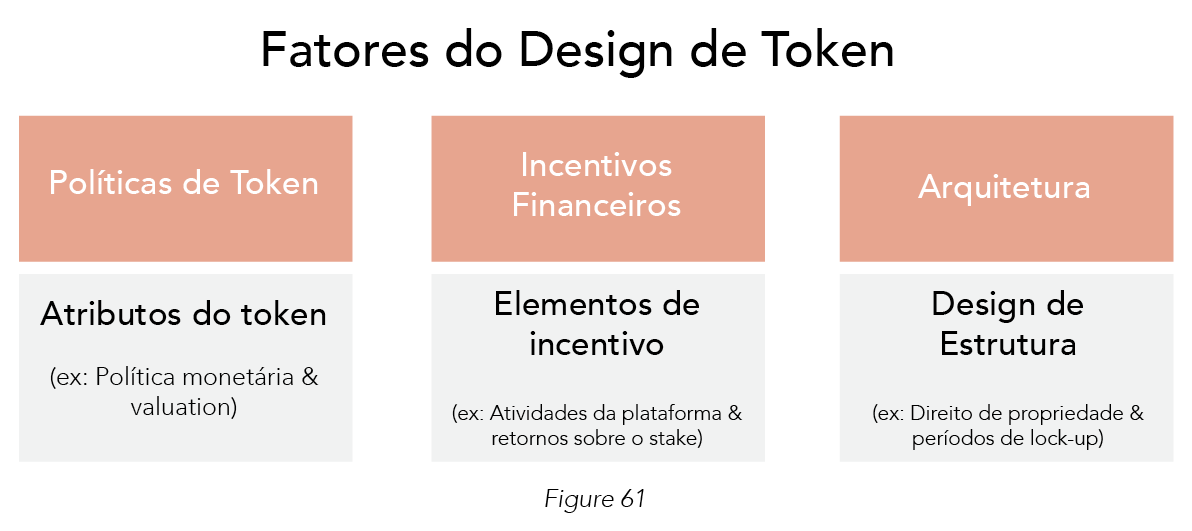


Figura 61

**Incentivos Financeiros**

Economia está diretamente ligada à incentivos. Os incentivos com impacto mais diretos são os incentivos financeiros. Encorajam comportamentos específicos e coordenam participação em direção ao objetivo comum do ecossistema. A meta principal é o objetivo comum, não o preço do token no mercado secundário.

**Atividade da plataforma**: forma em que comportamentos são incentivados no ecossistema.

**Retorno sobre investimento**:como o token e seu ecossistema geram retornos. Está relacionado à política de token implementada.

**Arquitetura**

Dado que tokens podem ser integrados com códigos/programas, a arquitetura foca nos pilares fundamentais do token. Pode incluir aspectos técnicos como fórmulas algorítmicas embutidas no código ou direito de propriedade, assim como não-técnicos como a alocação inicial e distribuição do token.

**Direito de propriedade:** direitos garantidos aos detentores do token.

**Distribuição:** determina como tokens são inicialmente alocados e distribuídos.

O **algoritmo e o código** executam a governança do token.

### Política de Token

Bancor possui dois tipos de tokens (tokens líquidos de utilidade e tokens LP, ou *relays*).

#### Política Monetária

Política monetária determina como a oferta de tokens é controlada. Toda a discussão da parte matemática no 12.8.3.

##### Oferta e precificação do token líquido

Oferta e preço são governados por uma fórmula matemática presente no contrato inteligente. Contrato executa a fórmula para administrar a emissão e governança dos tokens líquidos.

Ambas as variáveis de preço e oferta circulante mudam constantemente, visto que o contrato inteligente emite e queima tokens de forma contínua, conforme dinâmica do ecossistema (mercado primário). Preços no mercado secundário não são definidos por essa política monetária e seguem o mecanismo de *pools* de liquidez.

O preço efetivo de tokens líquidos é:

##### Índice de reserva do token líquido

Também chamado de índice de reserva constante, reserva fracionária, ou taxa de câmbio. Definido pela proporção fixa entre o valor do token e o valor de sua reserva.

Em outras palavras, o preço de tokens líquidos ($BNT) muda conforme a reserva do mesmo. Esse preço é constantemente recalculado para manter o índice fixo.

Exemplo: Preço do HKD (dólar de Hong Kong) muda em termos de USD (dólar americano). Ao invés de preços flutuantes, queremos que tenha conversão fixa. Para isso, a oferta e o preço do HKD se ajustam para garantir o preço **fixo em termos de** USD.

##### Construindo uma nova reserva (pool)

É possível criar novas reservas por meio de $BNT e o novo token de reserva. Provedores de liquidez[[107]](#footnote-108) precisam depositar valores equivalentes de $BNT e esse novo token. O valor mínimo da reserva é de $20 mil dólares, sendo que $10 mil (50%) devem ser em $BNT.

#### *Valuation* do Token

Valuation refere-se à precificação do token.

##### Curvas de ligação para tokens líquidos

Preço do token líquido é definido pela fórmula, .

é o preço do token

é a oferta

é o índice de reserva

é uma constante arbitrária

Custo total do token líquido em tokens de reserva é definido pela fórmula,

, onde é o custo total em tokens de reserva, é o valor inicial monetário dos tokens de reserva, é o índice constante de reserva, é a mudança na oferta do token líquido e é a oferta inicial do token líquido.

##### Curvas de ligação para tokens líquidos

Transações em um token de reserva afetará o preço do token líquido em termos de outros tokens de reserva. Visto que a Bancor ainda não implementou esse sistema, não vamos entrar à fundo nos detalhes. De qualquer forma, provemos a fórmula matemática para tal.

##### Preços da pool de reserva para tokens de LP

Tokens de LP representam proporções da reserva (*relay*). O preço é derivado do valor da reserva, o que inclui o valor de $BNT e token de reserva presentes na *pool*.

### Incentivos Financeiros

#### Atividades da Plataforma

##### Seguro para Perdas Impermanentes (Impermanent Loss)

Um dos principais riscos de corretoras descentralizadas é o chamado de *Impermanent Loss* (ou “perdas impermanentes”, em bom português). Essas perdas são incorridas pelos provedores de liquidez que depositaram tokens de LP na *pool* por conta de flutuações de preço causadas por negociações de terceiros.

Para combater esse risco, Bancor oferece seguros para *impermanente loss*.Nessa linha, uma das mudanças na versão Bancor V2.1[[108]](#footnote-109) é possibilitar a provisão de liquidez unilateral (apenas um token). O protocolo emite $BNT conforme necessário, e ganha taxas de transação por essa provisão própria. Essas taxas são utilizadas para pagar os assegurados.

Caso proventos de taxas não sejam suficientes, Bancor emite mais $BNT para compensar as perdas.

##### Slippage de preço no token líquido ($BNT)

"Slippage" de preço refere-se às variações de preço que acontecem na execução da transação. *Slippage* ocorre por conta da profundidade do mercado (tamanho da *pool* de reserva), e não pela diferença de preços de compra e venda.

Tokens de LP representam a *pool* de reserva, que armazena tokens de reserva e tokens líquidos. A reserva emite e queima tokens líquidos para atender transações e determinar preços. Quando uma pessoa vende $BNT para a reserva em troca de tokens de reserva, está efetivamente aumentando a quantidade de $BNT e diminuindo a de tokens de reserva. Com isso, o índice de reserva se altera e o preço do $BNT automaticamente muda, de forma que o índice retorna para a constante.

Quanto maior for o número de tokens transacionados relativo ao tamanho da reserva, maior será o *slippage* de preço (variações no preço). Tecnicamente, não há a necessidade de se ter $BNT para executar transações – ele funciona como meio de pagamento e denominador comum.

##### Taxas de Corretagem

A principal fonte de receitas de corretoras é a taxa de corretagem, ou taxa de transação. Esse tipo de taxa é aplicado quando um ativo é negociado por outro na plataforma. Além disso, existe a taxa de transação relacionada ao “gás” da rede – para possibilitar a execução da transação. Essas taxas incentivam usuários a proverem liquidez e auxiliar na redução de *slippage*.

ELI5: Em finanças tradicionais, caso você queira trocar USD (dólar américa) por GBP (libra esterlina), você pode utilizar corretoras cambiais. Vamos dizer que £1 GBP custa $1.25 USD. A corretora pode te cobrar dois tipos de taxas: taxas de transação e taxas de comissão – ambas afetando a taxa de conversão entre USD e GBP.

1. A taxa de conversão oferecida pela corretora pode ser algo em torno de £1 : $1.30. Em outras palavras, o custo na verdade é $0.05 a mais do que a taxa de conversão base ($1.25). Chamamos essa diferença de taxas de corretagem, ou *spread*.
2. A corretora pode cobrar também taxas de comissão para executar a transação.

No caso do protocolo Bancor, eles são a corretora. Não há cobrança de taxas de transação porque a conversão é fixa. O protocolo, porém, cobra taxas de comissão que são pagas para os provedores de liquidez (*holders* de tokens LP).

##### Mecanismo de liquidez

Contratos inteligentes governam o mecanismo de liquidez, constantemente emitindo e queimando tokens de acordo com o mecanismo definido.

#### Retorno sobre Investimento

##### Staking na Bancor: Taxas de transação de tokens de LP

Em toda transação que acontece na reserva, uma pequena taxa é cobrada. Geralmente varia entre 0.1-0.3%. Essa taxa é cobrada por conversão e é depositada na *pool* de reserva. Essas taxas incentivam a provisão de liquidez por parte dos investidores, ajudando a diminuir efeitos de *slippage*. Quanto maior for a reserva, menor é o *slippage*.

##### Arbitragem no preço de tokens líquidos

$BNT é o token de utilidade da Bancor e é usado em todos os pares de transação. Porém, $BNT também é negociado em várias outras corretoras (mercados secundários). Preços nesses mercados podem ser diferentes dos preços no ecossistema Bancor. Devido à oportunidades de arbitragem, essa diferença não dura muito tempo e é absorvida por investidores até atingir o equilíbrio.

Arbitragem é quando o mesmo ativo tem preços diferentes em sistemas diferentes. Cria a possibilidade de comprar o ativo em um mercado com preços baixos e vender em outros mercado à preços mais altos. *Traders* aproveitam essa oportunidade de risco mínimo (diferença de preço) para lucrarem. Na prática, investidores compram $BNT das corretoras até que o preço se iguale ao preço interno do ecossistema Bancor.

##### Token líquido no mercado secundário

Por mais que $BNT seja negociado em mercados secundários, preço e oferta no ecossistema Bancor não mudam. Preço primário é determinado pela oferta circulante de $BNT, e visto que mercados secundários não afetam a emissão/queima de tokens, oferta circulante se mantém a mesma. A única coisa que muda é a posse de $BNT – de um investidor para outro.

Preços só mudam quando existe interação direta com $BNT, como por exemplo em conversões de token via *pools* de reserva na Bancor.

### Arquitetura

Tokens líquidos e tokens de LP possuem arquiteturas e fundamentos diferentes.

#### Direto de propriedade

Tokens líquidos não possuem direito de propriedade. Atuam como meio de troca e facilitadores de acesso ao ecossistema.

##### Direito de propriedade para tokens de LP

Tokens de LP (ou *relay tokens*) garantem o direito à fluxos de caixa futuros, gerados por meio de taxas de transação.

Quando uma transação é executada na *pool*, taxas de transação são cobradas. Essas taxas, em contrapartida, são redirecionadas para a própria *pool*. Quando tokens de LP são queimados (redimidos), recebem de volta sua proporção da reserva, incluindo tokens originalmente *stakados* e rendimentos de taxas de transação.

Por exemplo, vamos assumir que um provedor de liquidez tem 10 porcento da reserva de $DAI-BNT. Quando investidores compram ou vendem $DAI na *pool* de reserva (aumentando ou diminuindo a oferta de $DAI), pagam taxas de transação. A *pool* de liquidez recebe 10 porcento dessas taxas. Quando o provedor de liquidez redime seus tokens $DAI-BNT, recebe 10 porcento de todo o valor da reserva, além de taxas de transação incorridas.

#### Distribuição

##### Distribuição do Token $BNT

Oferta total de $BNT é 79,323,978[[109]](#footnote-110).

###### Distribuição

* 20% na *pool* de reserva de $ETH-BNT
* 40% para desenvolvimento do protocolo e outras tecnologias (P&D)
* 12% para marketing e incentivos do ecossistema
* 10% para criação de tokens de LP, tokens matriz e outros
* 18% para custos operacionais e legais

#### Algoritmo e Código

#### 

#### *Figura 62*

##### Fórmula de preço para tokens líquidos

Existem quatro variáveis na fórmula:

* é o valor total de token reserva (Ex: se $ETH está $1,500 e possuo 10 $ETH na reserva, o valor total é $15,000)
* é a oferta circulante do token líquido
* é o preço do token líquido
* é o índice de reserva fracionária. Valor flutua entre 0 e 1, e por isso o termo “fracionária”.

O índice de reserva é a proporção entre o valor do token de reserva e o valor de mercado do token líquido.

Isso significa que o valor do token de reserva é uma fração do valor do token líquido.

O valor de mercado do token líquido é também conhecido como *market capitalization*, ou *market cap*.

O preço do token líquido é definido como:

Cenário: uma pequena quantidade de tokens líquidos é comprada ().

1. A reserva se altera. Comprados paga tokens de reserva para receber tokens líquidos .
2. Dado que , .
3. Combinando ambas as fórmulas, temos .
4. Quando a oferta muda, preços também mudam. Mas o índice de reserva se mantém igual. Usando a regra da cadeia, temos .
5. Isolando em um lado, temos .
6. Isolando em um lado, temos .
7. Assumindo que , temos .
8. Isolando em um lado, temos .
9. Ao expandir, temos .
10. Usando diferenciação inversa de funções logarítmicas, .
11. Visto que S e P são ambas variáveis – e não uma função, ao integrar a equação temos .
12. Expandindo mais um nível, temos
13. Por fim, simplificando, temos

Onde *A* é uma constante arbitrária e *e* é o número natural. Essa é a fórmula de preço que os contratos inteligentes utilizam.

##### Fórmula de conversão para tokens líquidos

Vamos considerar um cenário diferente. Imagine que temos alguns tokens de reserva, chamados de “E”. Desejo convertê-los em tokens líquidos “T” para poder usar em outros protocolos. Quantos tokens líquidos eu receberei?

A fórmula acima não pode ser usada, dado que não possui variáveis de tokens de reserva. Precisamos então, utilizar um método regressivo para calcular.

1. Qual é o novo preço considerando a nova oferta circulante?
2. Qual é o custo total para comprar novos tokens, dada alteração na oferta?
3. Qual a mudança de oferta em função do custo total?

A seguinte fórmula pode ser usada como fórmula de conversão[[110]](#footnote-111):

1. Novo preço, dado aumento em oferta circulante, é:
2. Novo custo, em termos do token de reserva, é a área embaixo da curva. . Solucionando essa fórmula, temos .
3. Reorganizando a equação em termos de “T”, temos . Esse é o número de tokens líquidos recebidos quando pagamos ‘E” tokens reserva.

##### Impactos do Índice de Reserva

Visto que a fórmula de preço é uma função exponencial sujeita ao índice de reserva, o formato da curva depende do índice. O índice de reserva[[111]](#footnote-112) varia entre 0 e 1.

###### Índice de Reserva = 1

Quando índice de reserva é igual a 1, a curva se torna uma linha horizontal. Isso significa que preços não mudam e são sempre constantes – não responde de acordo com oferta circulante. Conhecido como “paridade fixa” (ex: paridade do dólar do Panamá com dólar americano).

###### Índice de Reserva = 0.5

Quando o índice é igual a 0.5, a curva possui inclinação positiva e reta. Isso significa que preços se movem linearmente com a oferta circulante. Formato de linha reta faz sentido no caso do $BNT, que não possui possibilidade de rendimentos.

Porém, caso seja possível receber rendimentos com o token líquido, onde taxas de transação contribuem para o aumento da reserva base, um índice de 0.5 pode não ser um bom modelo. Primeiros participantes serão exageradamente recompensados quando comparados aos demais.

###### 0 < Índice de Reserva < 0.5

Nessa faixa, temos uma curva exponencial positivamente inclinada. Quanto mais próximo de 0.5, mais inclinada fica a curva. Isso significa que preços se tornarão cada vez mais sensíveis à mudanças na oferta circulante (vide 11.3.3.2).

##### 0.5 < Índice de Reserva < 1

Nessa faixa, temos uma curva exponencial com inclinação em decrescimento. Quanto mais próximo de 1, mais inclinada a curva fica inicialmente. Ou seja, preços inicialmente aumentam rapidamente, criando especulação e volatilidade.

Dado que o protocolo da Bancor utiliza essa fórmula como parte do token $BNT, que possui objetivo central de funciona como meio de troca, o melhor caso seria manter o índice de reserva em 0.5[[112]](#footnote-113). Conforme esses objetivos mudem, o índice ideal também se altera.

### Conclusão

Bancor provê liquidez para sua rede de tokens por meio do conceito de token líquido, possibilitando conversão instantânea entre os mais variados tokens. O sistema também oferece seguros contra *impermanent loss* incorridos durante as operações. Todos esses mecanismos se alinham para prover mais liquidez ao sistema, reduzindo efeitos de *slippage* e aumentando o valor econômico agregado pelo protocolo.

## Outros Princípios Econômicos

### Tokens de Desconto

Tokens de desconto são um tipo de ativo digital, classificados como tokens de utilidade e concedem direito a descontos em certas transações. Esse modelo é utilizado majoritariamente para serviços, não para produtos. Tokens de desconto não são usados para definição de preços, mas sim para determinação do desconto **sobre o preço** original. Tokens de desconto são desenvolvidos pela Sweetbridge[[113]](#footnote-114).



Figura 63

Diferente de cartões-presente ou cupons, tokens de desconto não são queimados ou destruídos após o uso – continuam na posse do proprietário original. Similar a cartões-presente e cupons, por outro lado, tokens de desconto possibilitam usuários receberem descontos. Máximo de desconto possível é 100 porcento, o que faria o serviço ser de graça.

O valor do token de desconto é derivado de duas formas: valor de uso (ganhar desconto nos itens) e valor de revenda. Funciona como as antigas permissões de Táxi. A permissão possui um valor por si só (permitir que motoristas prestem serviços como táxis) e o valor de venda.

#### Quatro Critérios Gerais para Tokens de Desconto



Figura 64

1. Quando e , não temos tokens ativos e não temos descontos.
2. O número de tokens necessários para eliminar todo o custo – tornando o serviço grátis – é , satisfazendo . Quando a quantidade de tokens reflete a totalidade do custo, desconto recebido é de 100%.
3. Quantidade de tokens de desconto requerida para receber 100 porcento de desconto () é estritamente crescente quando . . Ou seja, quanto maior o custo do serviço, maior a quantidade de tokens necessárias para desconto.

#### Funções de Tokens de Desconto

1. Custo do serviço é
   * Onde é a função de custo que inclui , tokens ativados, , quantidade comprada e , stato geral da rede.
   * A função de desconto (dada pelo token de desconto) é .
2. Modelo de Descontos

Serviços podem ser comprados com ou sem tokens. De qualquer forma, preços são definidos originalmente pelo provedor do serviço, e estão sujeitos a flutuações de mercado.

A quantidade de desconto recebida por token, porém, é ditada pela necessidade e utilidade da rede. No geral, o tamanho dos descontos aumenta conforme a rede cresce. Esse é um método para determinar o *valuation* do token utilizando variáveis endógenas relacionadas ao crescimento da rede. Oferece incentivos para usuários pioneiros comprarem tokens de desconto, dada possibilidade de maiores descontos no futuro.

1. Métricas de utilização da rede
   * Função de desconto quando [[114]](#footnote-115) é .
   * O desconto máximo que uma pessoa pode receber é 100 porcento – ou seja, 1, onde o item em questão se torna grátis. Com isso temos: .
2. Receita operacional suficiente na presença de tokens de desconto
   * O token de desconto reflete o uso geral da rede, .
   * O custo, dado token de desconto atual, .
3. Efeitos do crescimento da rede

Primeiros usuários, os pioneiros, têm descontos crescentes conforme a utilidade da rede cresce. Isso se dá pois, no momento de compra desses tokens, a utilização da rede ainda é muito baixa. Conforme a utilidade aumenta, o tamanho dos descontos por token também aumentam. Ou seja, a quantidade necessária de tokens de desconto diminui para atingir o mesmo valor, e os tokens em excesso podem ser vendidos.

* + , onde é a taxa operacional ou qualquer outro parâmetro de design no nível do sistema (), é a quantidade de tokens ativados pelo proprietário e é a utilização da rede. Utilização da rede, , aumenta conforme número de usuários ativos.

1. Derivando valor da utilidade
   * Valor de utilidade por token ativo por unidade de tempo pode ser definido por . Esse valor é calculado ao derivar parcialmente *t* da função de custo.
   * Especificamos por unidade de tempo visto que estamos assumindo um serviço de software com tempo limite. Em casos de utilidade por licença e por período, por exemplo, valor pode ser definido de duas maneiras: (1) compra e uso do token de desconto, ou (2) manter a posse do token para receber retornos futuros, *r*. O valor teórico do token é definido por: . Esse cálculo é feito por meio do valor presente de anuidades perpétuas.
   * Para serviços sem limitação de tempo, defina pelo nível de serviço a cada novo período de ativação – por exemplo, aluguel de serviços como delegação de *stake* para operação de validadores blockchain, ou aluguel de Axies para usar em batalhas.
2. Custos operacionais

Custos operacionais podem vir de custos de transação na blockchain, custos de manutenção, e custos operacionais do serviço. Tokens de desconto precisam levar em consideração esses custos de operação.

* + Uma restrição pode ser definida como, para que os serviços nunca sejam de graça.
  + Adicione na função de custo para que usuários recebam de receita e possa ser usado nos custos operacionais. Receita da rede pode ser definida como .   
    Custo operacional: .

1. Incentivar utilidade crescente aos tokens de desconto ao tornar o uso mais benéfico do que a acumulação (*holding*).

Ao utilizar o token, o usuário recebe descontos perpétuos. Caso o valor do token aumente, o usuário pode vende-lo. Caso um indivíduo compre o token de desconto apenas esperando sua valorização, o único benefício econômico é o lucro da venda. Para o usuário que está utilizando o token, terá não só o valor econômico da valorização, mas também as economias recebidas por meio do token em serviços.

### Direto de Propriedade

Direito de propriedade é um conceito imposto socialmente para determinar como recursos e bens são usados e detidos.

#### Tipos de Direito de Propriedade



Figura 65

1. Livre acesso (ex: códigos no Github, ou o oceano)
2. Propriedade pública (ex: Ethereum, ou um parque) – Pertencente à todos, mas acesso e uso controlados pelo estado ou comunidade
3. Propriedade comum, ou bem comum (ex: DLT permissionada ou participação em empresas privadas) – pertencente à um grupo de indivíduos
4. Propriedade privada (ex: sua chave privada, ou uma residência privada)

Direto de propriedade é um tópico muito amplo por si só, visto que há muitas maneiras de estruturar a distribuição de propriedades. Vamos focar nas novas formas de administrar direito de propriedade para ativos digitais.

#### Taxação de Harberger

Taxação de Harberger pode ser implementada para administrar o direito de propriedade associado à artes digitais.

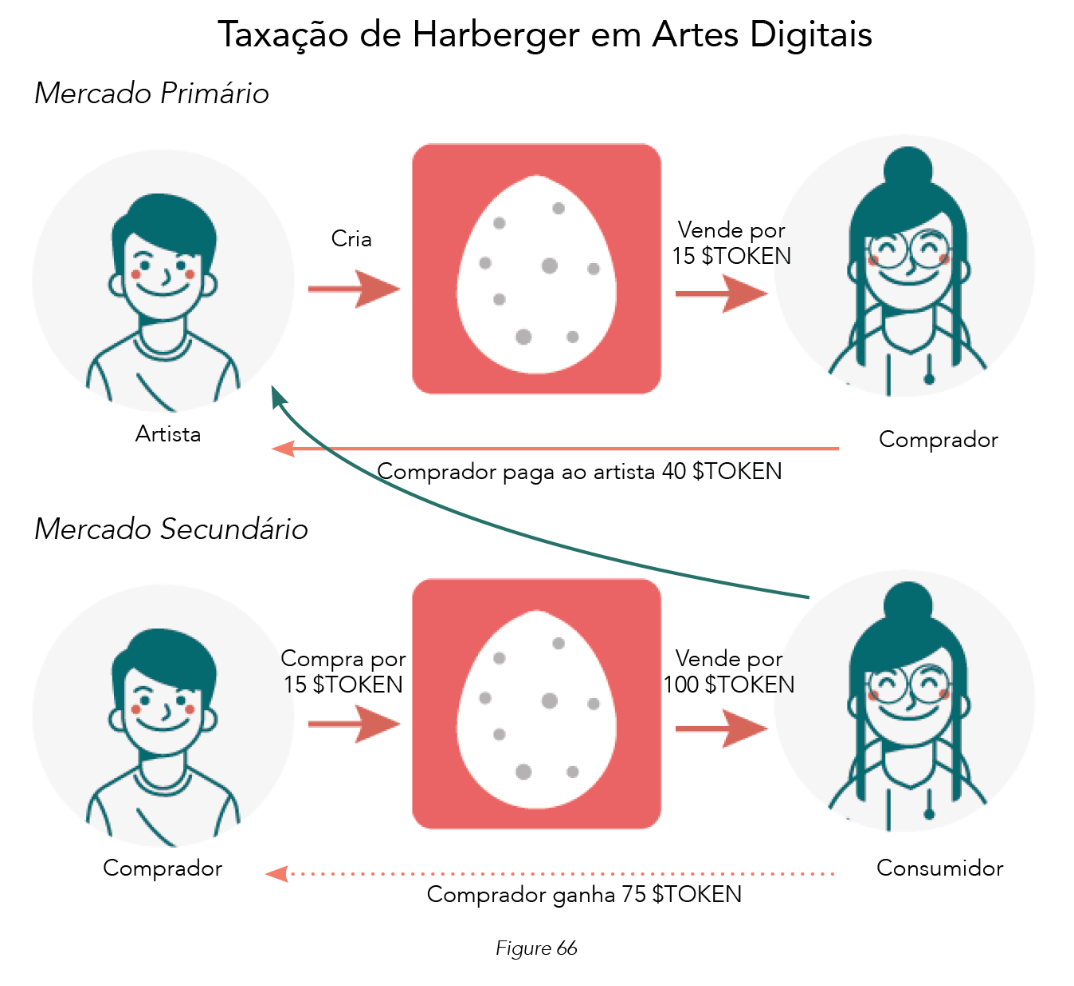


Figura 66

O objetivo é garantir que o artista se beneficie da arte que criou, assim como incentivar que o comprador da arte a revenda, gerando taxas adicionais ao artista original. Mais colecionadores a valores justos significa maior possibilidade de participação dos demais. Por exemplo:

1. Artista (A) cria a arte.
2. Quando A vende a arte para o Comprador (B) – de “*buyer*”, (A) recebe os lucros.
3. (B) vende a arte para o Consumidor (C).
4. (B) fica com os lucros da venda e as taxas de transação – ex: taxação de Harberger – são repassadas para (A).
5. Essa é uma dinâmica contínua, em que a taxa de transação sempre é repassada para (A).
6. Novos compradores não irão colocar preços exorbitantes, visto que a taxa é baseada no preço. Além disso, torna-se preferível manter o ativo em sua posse do que vender a preços baixos – e consequentemente sem lucro devido às taxas de transação.

### Financiamento Inflacionário por Convicção de *Stake*

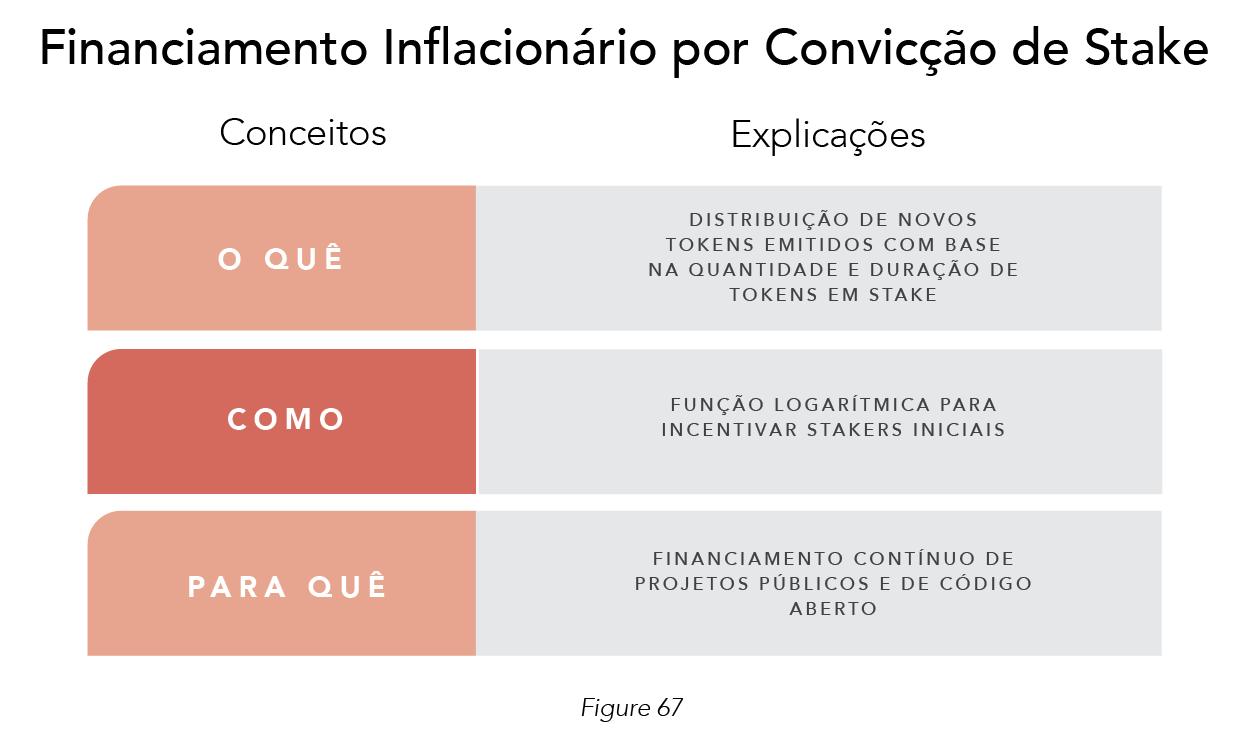


Figura 67

Esse modelo é usado para financiamento contínuo de projetos públicos e de código aberto. Detentores de tokens colocados em *stake* são recompensados com base na quantidade e tempo em que os mesmo estão “travados”.

O modelo é operado por uma função logarítmica[[115]](#footnote-116). Quanto maior o período e quantidade em *stake*, maior a proporção recebida de novos tokens emitidos. As duas variáveis desse modelo são a quantidade em *stake* (*s*), e o tempo (*t*).

Funções logarítmicas são usadas para garantir que usuários com poucos tokens e períodos extensos de *staking* possam receber mais benefícios do usuários com muitos tokens e pouco tempo de *stake*.

Custo de oportunidade também aumenta de acordo com o tempo, dado que a curva de oferta do token se achata. Conforme o custo de oportunidade cresce, usuários decidem alocar seus recursos em outros lugares, removendo especuladores do ecossistema. Os investidores (*stakers*) restantes realmente acreditam no projeto (“por convicção”), ao invés de serem meros especuladores.

O custo de oportunidade pode também ser um risco, visto que dententores do token possuem menos incentivos para manter seus fundos em *stake* por períodos mais longos devido à natureza das funções logarítmicas. Além disso, o ritmo de crescimento inicial de recompensas é bastante elevado, podendo atrair especuladores. Esse modelo funciona melhor para projetos públicos, onde a maioria dos usuários está mais interessada no bem comum do que em lucros pessoais – o projeto por si só é um incentivo de *stake* para o longo prazo, ao invés de buscarem recompensas de curto prazo ou especulação.

### Teoria Geral dos Contratos

Contratos são inerentemente incompletos, executáveis apenas de acordo com eventos verificados em tempo real por oráculos de terceiros.

Custos de plano de saúde, por exemplo, é determinado pela situação atual de saúde da pessoa. Esse variável, porém, é difícil de ser verificada remotamente. Seguradoras utilizam, então, sinais como variáveis alternativas – como é sua alimentação, qual frequência pratica exercícios físicos etc. Um aplicativo de saúde ou um relógio inteligente (*smart watch*) podem agir como oráculos de terceiros e prover informações mais confiáveis.

**Mesmo que** toda informação relevante seja verificável, seria custoso demais, se não impossível, desenvolver um contrato que leva em consideração todo e qualquer tipo de problema.

Então por que precisamos de contratos se eles não são holísticos? Mercados tradicionais facilitavam originalmente transações imediatas – comprador e vendedor executam a troca ao mesmo tempo. Isso possibilitava os participantes de verificarem o produto e pagarem o valor em dinheiro físico ao mesmo tempo.

Conforme os mercados evoluíram, as coisas se tornaram mais complexas. Verificação não é sempre feita de forma instantânea. Transações podem não ser executadas imediatamente. Essas complicações podem ser resolvidas por meio do uso de contratos. Contratos garantem que uma transação seja executada conforme acordo entre partidos – na maioria dos casos.

O objetivo final é aumentar a transparência de transações em mercados tradicionalmente opacos, reduzindo a necessidade de intermediários. Mercados são opacos por conta da quantidade de informação customizada existente, tornando difícil a criação de mercados profundamente líquidos e com sistemas simples de transação. É como comparar a venda de ações da empresa ABC na bolsa de valores (liquidez profunda) com a venda de títulos da mesma empresa ABC (baixa liquidez). Além dos métodos comuns de KYC (conheça seu cliente), precisamos implementar o KYT (conheça seu token) para avaliar o ecossistema antes de abrir para outros participantes transacionarem no mercado secundário.

Com contratos inteligentes, o problema não é em executar o que está presente nele, mas sim o que não está. Em termos de facilitação de transações, o benefício de contratos inteligentes não está em sua habilidade de execução automática. Isso já funciona dessa maneira, com suas ressalvas, em sistemas tradicionais de sensores e dispositivos de IoT. O benefício real está na possibilidade de agentes econômicos atualizarem as regras, de acordo com dinâmicas atuais. Contratos inteligentes permitem a construção de modelos matemáticos e atualizações ao contrato[[116]](#footnote-117) para refletir mudanças no sistema. Contratos físicos (em papel) são muito mais difíceis de se alterar.

Contratos inteligentes focam em melhorar a **qualidade da informação** para que mais fatores possam ser usados em contratos, tornando-os mais completos. Comportamento de condutores de veículos, por exemplo, é muito difícil de se contabilizar/prever. Hoje, com a tecnologia existente, podemos extrair, gravar e verificar dados (maior qualidade de informação), criando ganhos reais de eficiência e permitindo decisões mais bem-informadas.

Outro exemplo de contrato é o “pagamento por performance”, que é o modelo de consenso de prova de trabalho, ou *Proof of Work*. Pode existir além de protocolos de primeira camada (*layer 1*). Dapps, por exemplo, podem facilitar a negociação de tokens em *pools* de liquidez. Recompensas são distribuídas em forma de taxas de transação quando há a verificação de que o “trabalho” foi completo.

Por mais que protocolos de DEX não consigam integralmente especificar os aspectos-chave do resultado esperado com antecedência (ex: montante ideal de liquidez) por conta da teoria de contratos incompletos, usuários (provedores de liquidez e usuários da corretora) podem decidir o que desejam contribuir e negociar, baseado no quanto querem prover de liquidez e quanto desejam receber em taxas.

Risco de receitas:

Esse risco pode ser considerável, visto que o comportamento desejado (ex: montante total de liquidez) não pode ser acordado nem especificado com antecedência. Portanto, provedores de liquidez são incapazes de estimar o risco (ex: *slippage* ou *impermanent loss*) e precisam de compensações para manter o mesmo nível de provisão de liquidez. Geralmente, tokens nativos são oferecidos para compensar esse risco, e tornar a entrada de provedores de liquidez mais atrativa.

Esse contrato específico distribui tokens nativos aos provedores como forma de compensação por assumirem o risco de perdas futuras. Dado que a profundidade de liquidez pode ser precisamente medida em qualquer momento (mas não prevista), esse modelo já é mais eficiente do que o “pagamento por performance”, que precisa compensar usuários pela incerteza da quantidade necessária de poder computacional para validar um bloco.

### Registros Curados de Tokens (TCRs)

TCRs foram introduzidos no 10.6.4.2 quando abordamos o tópico de Design de Token.

TCRs são listas descentralizadas. Podem ser listas de basicamente qualquer coisa: melhores pizzarias de São Paulo, ou as melhores atrações turísticas do Rio de Janeiro. Para votar em um TCR, você precisa de determinada quantia de tokens em *stake*. Indivíduos podem contestar seu voto, com a possibilidade de ganhar ou perder a parte do outro. TCRs criam o efeito de coordenação e acordo entre indivíduos diferentes. São uma forma de comunicação em forma de tokens em *stake*.

*Isso te lembra de alguma coisa discutida anteriormente? Esse é um ótimo exemplo de ponto focal, ou ponto de Schelling, a sétima maravilha no 5.7! A meta é a que a comunidade encontre a resposta “correta”.*

#### Aplicações

**Ranqueamento de conjunto de dados**

Discutimos o uso de TCRs por parte do Ocean Protocol para curar e ranquear conjuntos de dados de inteligência artificial. Na superfície, curvas de ligação utilizam respostas externas para fazer a verificação externa e ranquear as bases de dados. Tokens são colocados em *stake* para sinalizar que aqueles dados serão importantes.

Mineradores recebem recompensas por hospedarem os conjuntos de dados publicados, e por disponibilizá-los quando necessário – esse é um requerimento para manterem seus tokens em *stake.* Além disso, ao hospedar e disponibilizar os dados para outros usuários, recebem taxas. Esse processo é chamado de “*data farming*” no protocolo da Ocean.

**Ranqueamento de cursos online**

Economics Design administra uma escola online de economia para estudantes. Nesse caso, poderíamos hipoteticamente utilizar tokens de reputação, $EREP[[117]](#footnote-118).

Ao completar um curso, estudantes poderiam avaliar o quão proveitoso foi o conteúdo. Caso o conteúdo seja bom, mais pessoas entrarão no curso, e colocariam $EREP em *stake* naquele curso específico. Ao longo do tempo, isso se tornaria uma lista ranqueada dos melhores cursos. Conceito similar a esse é aplicado na Web2, na <https://www.ratemyprofessors.com/>, mas com professores sendo ranqueados ao invés de cursos.

Os últimos 20 porcento de estudantes poderiam perder seus tokens, que seriam posteriormente distribuídos proporcionalmente a todos os usuários nos demais cursos.

Isso cria valor reputacional aos cursos e naturalmente direciona as pessoas para os cursos com mais fundos travados (em *stake*).

Caso os tokens tenham valor monetário e sejam negociados em mercados secundários, pode desincentivar as pessoas a participarem, visto que o token pode ser vendido por USD e usado em outros lugares. Por isso, esses tokens devem ser tidos como tokens de utilidade interna para propósitos de reputação e recompensas de cursos online.

# FINANÇAS DESCENTRALIZADAS

## Economia em Finanças Descentralizadas (DeFi)

Existem muitos intermediários no setor financeiro, incluindo corretores, *traders*, portais de financiamento, entre muitos outros. Um dos principais efeitos de DLT (tecnologia de registros distribuídos) é eliminação da necessidade de intermediários. Desse conceito surgiu a uma das maiores tendências da economia de tokens: DeFi.

Tokenização possibilita a codificação de lógicas de negócio e a execução automatizada por meio de máquinas (contratos inteligentes). Com a remoção de intermediários, as taxas cobradas pelos serviços dos mesmos é economizada e pode ser distribuída para usuários do sistema.

O conceito de finanças descentralizadas é importante dado seu potencial de revolucionar as finanças tradicionais de algumas maneiras:

* Dinheiro pode ser administrado por políticas monetárias embutidas em códigos, algoritmos, e contratos inteligentes. Dinheiro pode ser um ativo “neutro”, sem depender de questões políticas.
* Ativos (tokens) podem ser negociados sem a necessidade de *order books* (compilado de ordens de compra e venda), já que os AMMs (formadores de mercado automatizados) provém a liquidez nas *pools*.
* Portfólios de investimentos são constantemente balanceados com base no perfil de risco do cliente. Contratos inteligentes podem fazer isso automaticamente, sem a necessidade de investidores pagarem caro pelo serviço de gestores para fazê-lo.

As possibilidades de melhorar as muitas ineficiências do mercado tradicional são infinitas. Trazer esses sistemas para o âmbito digital aumenta a velocidade e eficiência do mesmo, além de facilitar transações para usuários por meio da liquidez contínua presente em vários ecossistemas de DeFi. Por isso, é importante entender a matemática econômica de DeFi e a infraestrutura que estamos construindo. Aplicações para gestão de portfólio, corretoras descentralizadas, e seguros descentralizados podem existir em negócios com lógica codificada.

### Introdução ao DeFi

#### Definição de DeFi

DeFi é um movemento que utiliza redes descentralizadas para remover intermediários do sistema financeiro.

DeFi reconstrói versões análogas de sistemas financeiros existentes (ex: NASDAQ, B3) em novos modelos de governança, incentivos e mecanismos. É um mundo completamente novo.

|  |
| --- |
| Caixa 4: Comparando Finanças Tradicionais com Finanças Descentralizadas    Figura 68  Assim como empresas tradicionais, protocolos de DeFi também incluem os clássicos Ativos, Passivos e Patrimônio no balanço. Ao invés de leis e regulamentações definidas pelo governo local de onde a empresa está situada, protocolos de DeFi definem as regras que usuários e tokens devem seguir[[118]](#footnote-119).  Essas “regras” são todas as que discutimos na primeira metade desse livro. Protocolos de DeFi operam como empresas tradicionais, mas estruturados de forma inovadora.  Discutimos a diferenças entre ativos tangíveis e intangíveis na Seção Parte I: 2.2.3 com visão econômica.  A segunda metade desse livro é sobre DeFi, e as novas formas de liquidez colaborativa (passivo) e distribuição de propriedade para a comunidade (patrimônio).  DeFi é exatamente sobre isso: remover intermediários e distribuir valor adicional para os usuários do sistema.  Os princípios de empresas tradicionais continuam existindo em DeFi. Porém, o mecanismo de **implementação** desses princípios é diferente, com foco primário na descentralização. |

#### Por Que Precisamos de DeFi?

Antes de nos aprofundarmos nos detalhes de como esse tal de “DeFi” funciona, é importante começarmos do início: Por que precisamos de DeFi? O sistema financeiro, infraestrutura e produtos atuais existem há décadas. Mesmo com várias crises financeiras, a economia tem sobrevivido. Então, qual a necessidade de DeFi?

Simples. O sistema atual é ineficiente, e incentivos não são distribuídos igualmente. DeFi inova os modelos de TradFi (finanças tradicionais) e CeFi (finanças centralizadas), substituindo a necessidade da “confiança em humanos e contratos físicos” por “contratos inteligentes, com aplicação legal e criptográfica”, e “auditorias de terceiros” por “códigos abertos e registros públicos”[[119]](#footnote-120).

Existem formas de aumentar a eficiência do sistema, e podemos fazê-lo por meio de infraestruturas financeiras descentralizadas.

#### Como DeFi Funciona?

1. **DeFi depende de matemática e códigos para a tomada de decisão**

A forma de executar é codificar a lógica de cada negócio em contratos inteligentes.

Por exemplo, ao invés de usar *order books* para unir compradores a vendedores em corretoras (ex: B3), podemos usar máquinas como a contraparte. Essas “máquinas” seguem fielmente o código implementado, definido matematicamente. No caso de corretoras, o código utiliza o princípio físico da lei de conservação de energia.

Matemática é a fundação que define a infraestrutura de DeFi. Código é a linguagem que computadores usam para processar as informações e cálculos matemáticos.

1. **Governança é distribuída entre os participantes**

Remover intermediários e executar a lógica do negócio por códigos é uma mudança muito poderosa. Outra mudança significativa é trazer novas soluções, ou reduzir ineficiências, para governança.

Governança é um grande problema, tanto no mundo físico “real” quanto no mundo digital online. Coates[[120]](#footnote-121) (2018) destacou que indexação passiva, investimentos privados, e globalização estão reformulando a ideia de propriedade e governança.

O advento de DeFi intensifica esses problemas com governança. Porém, assim como toda tecnologia inovadora, também traz novas oportunidades de solucionar esses problemas. Ao invés de deixar a governança na mão de um pequeno grupo de pessoas, podemos distribuir a governança para acionistas que de fato usam a plataforma. Também é possível delegar votos de governança para especialistas, caso o indivíduo não tenha conhecimento específico ou ache que essa é a melhor decisão.

Seja diretamente ou por delegação, usuários do sistema possuem voz ativa na governança. Ainda temos muitos problemas a resolver, mas esse é um passo positivo na direção correta.

1. **Incentivando ações/comportamentos**

As taxas de intermediários que são economizadas possibilita o redirecionamento de capital para encorajar certos comportamentos.

Por exemplo, enquanto empresas tradicionais pagam taxas exorbitantes para listagem na NASDAQ, podem agora fazer o mesmo praticamente de graça em corretoras descentralizadas. O capital economizado pode ser usado para incentivar usuários a proverem liquidez, recompensando-os com taxas.

Esse conceito muda o jogo. Abre novas oportunidades de exploração e novas formas de incentivar ações desejáveis, criando produtos e serviços de interesse comum. Ao invés da “Tragédia dos Comuns” (vide 14.4.2), novos incentivos são criados para movimentos colaborativos.

#### Quais são os participantes do setor DeFi?

DeFi é sobre descentralização. Com isso, podemos imaginar um segmento bastante distribuído em termos de participantes.

Modelo de Arranha-céus

**Investidores** financiam a contração de um arranha-céu (edifício muito alto) comercial. O **arquiteto** faz odesign do prédio e da planta interna. **Engenheiros civis e construtores** usam máquinas como guindastes para construir o arranha-céu de acordo com o plano do **arquiteto. Empresas** alugam os escritórios do edifício. **Funcionários** das empresas utilizam o espaço dos escritórios.

Valor é distribuído para todos no sistema. Investidores recebem retornos dos aluguéis. Arquitetos, engenheiros e construtores recebem salários e outras remunerações. Empresas e funcionários agora possuem lugar para trabalhar, possibilidade de networking com outras empresas, e uma comunidade para transacionarem.

Modelo DeFi

*Ao invés de arranha-céus, é uma comunidade com um protocolo.*

**Investidores** financiama ideia de construir a comunidade. Podem ser VCs, fundos de investimento, ou qualquer pessoa com capital. O **arquiteto** estrutura a lógica do negócio, incentivos, e a planta de como comunidade, protocolo e sistema funcionam (ex: design de regras econômicas do sistema). **Máquinas** fazem a execução do trabalho (ex: protocolo em si, ou seja, códigos e contratos inteligentes). Ao invés de engenheiros e construtores, temos **engenheiros da computação** que transformam a “planta” e o design em códigos. A parte especial é que **empresas** e **funcionários** podem ser a mesma pessoa. Pense nisso como uma empresa controlada por funcionários (no caso de uma DAO). Muitos dos integrantes dessa empresa também serão investidores e usuários do produto.

**Tabela Resumo**



Figura 69

#### Onde podemos interagir com DeFi?

DeFi existe digitalmente e online. Portanto, precisamos entender as diferentes jurisdições em que os participantes se encontram (veja figura acima).

Regulamentação tem papel fundamental em TradFi, e todos nós (incluindo reguladores) estamos tentando descobrir como e se é necessário regulamentar DeFi. Essa é uma questão bastante complexa, visto que o ecossistema segue inovando com conceitos e tecnologias todos os dias. Estamos em uma fase da nossa história muito interessante!

#### Quando DeFi começou?

DeFi pode ser rastreado até o primórdios do Bitcoin.

Treze anos atrás, tivemos a criação do bitcoin – uma moeda descentralizada. DeFi foi construído em cima da fundação estabelecida pela estrutura tecnológica do Bitcoin[[121]](#footnote-122). Bitcoin é como a linguagem de programação do seu sistema. DeFi é como o sistema operacional do seu celular (ex: iOS, Android). Dapps são os diversos aplicativos instalados no seu dispositivo.

### Nove Perguntas Frequentes Sobre DeFi

1. Por que descentralização é importante?

Usuários podem administrar melhor seu dinheiro, ao invés de depender de bancos e outros intermediários – geradores de custos adicionais que podem ser evitados e redistribuídos para o sistema.

1. Quais vantagens DeFi traz?

Possibilita pessoas criarem e moverem dinheiro ao redor do mundo a qualquer momento. Busca também solucionar problemas de pessoas sem acessibilidade financeira.

1. Qual a diferença de DeFi e Bitcoin?

Bitcoin é um ativo único pelo fato de ter criado a “criptomoeda” (um tipo de token que funciona como dinheiro programável) **e** oarcabouço tecnológico necessário para seu funcionamento. DeFi é o ecossistema que foi gerado pelo Bitcoin como prova de conceito para tokens que podem ser programados para atingir certos objetivos (no caso do Bitcoin: dinheiro programável). DeFi não é dinheiro programável, mas um sistema em que várias pessoas podem utilizar DLTs parecidas com a do Bitcoin para programar diversas funções financeiras.

1. DeFi é um golpe?

DeFi é um subcategoria de finanças. É um golpe financeiro? Não, finanças são neutras. Mas atores maliciosos podem tentar aplicar golpes, como em qualquer outro setor. Existem projetos reais em DeFi que buscam “disruptar” os sistemas financeiros tradicionais existentes.

1. Por que é DeFi é importante?

Como mencionado anteriormente, descentralização é uma das questões fundamentais de nosso futuro próximo. Outros podem alegar que é inclusão financeira ou digitalização, mas vamos olhar com perspectiva econômica.

Suponha que temos dois recursos: Trabalho (T) e Capital (K). No passado, precificávamos bens com base nas horas de trabalho necessárias para produzi-los.

Conforme evoluímos, começamos a usar máquinas para completarem tarefas. De repente, a precificação de bens não era apenas o custo do trabalho, mas o custo das máquinas. Máquinas são forma de capital. Pessoas que possuíam máquinas eram detentoras desse capital. Pessoas com capital passaram a colher quase todos os lucros, enquanto provedores de trabalho recebiam muito menos.

O mundo de amanhã está caminhando gradualmente para favorecer detentores de capital (K) ao invés de provedores de trabalho (T). Tecnologias como GPT-3[[122]](#footnote-123), aprendizado de máquina, contratos inteligentes, e outras formas de automação irão redirecionar os lucros para detentores de capital. A desigualdade social aumenta quando substituímos pessoas provendo trabalho (T) pelo uso eficiente de máquinas (K). Economia não diz que está necessariamente **errado** substituirmos (T) pelo uso eficiente de (K), mas sim, examina os resultados dessa mudança.

Nesse momento que DeFi entra. Constrói uma camada de base – arcabouço tecnológico de código aberto (K) – que não é possuído por nenhuma pessoal individual. Qualquer um (T) pode acessar esse capital para desenvolver produtos e soluções inovadoras. Torna acessível e disponível para todos que desejam aprender.

1. Seria DeFi uma solução que está procurando por um problema para resolver?

Muitas pessoas perguntam isso. Nós acreditamos que não, mas é uma solução em estágio inicial para um problema. Intermediários causam **desalinhamentos** **de incentivos** em finanças tradicionais, aumentam **custos de transação**, aumentam **opacidade de dados,** dependem da **confiança em pessoas e marcas** ao invés da confiança nos dados transacionados, e contribuem para o **problema do principal-agente**. DeFi busca, entre outras coisas, solucionar isso.

Hoje, ainda vivemos em um mundo predominantemente físico. Nós (T) ainda não fomos totalmente substituídos por máquinas (K). Porém, estamos mais perto de um mundo digital a cada dia. O problema da desigualdade de detentores de capital (K) e provedores de trabalho (T) continuará crescendo. DeFi busca formas inovadoras de alinhar incentivos em um sistema distribuído.

1. Qual o papel de DeFi na Web3?

Web 3.0[[123]](#footnote-124), ou web3 para os íntimos, é um novo mundo de código aberto e colaborativo que possibilita operações conjuntas entre humanas e inteligência de máquina. Máquinas fazem o trabalho pesado de cálculos, e humanos utilizam o resultado desses cálculos para criar novos sistemas.

Web 1.0 é geralmente classificado como uma base de dados de “**apenas leitura**”. A base de dados cria o conteúdo e usuários o consomem, como um jornal ou revista física. Assinantes leem revistas para consumir o conteúdo, mas não podem alterar ou adicionar a ele.

Web 2.0 aumenta o papel de usuários na rede. É uma base de dados de “**leitura e escrita**”, o que significa que podemos **consumir** **e** **criar conteúdo.** Funciona como os sites de notíciaque possuem seção de comentários.

Web 3.0[[124]](#footnote-125), ou Web3 leva a internet para um novo nível. É uma base de dados de **“leitura e escrita” com inteligência de máquina**. Culturalmente, web3 foca no aprendizado de máquina e inteligência artificial, internet das coisas (IoT), robótica, e blockchain. Inteligência de máquina é o que é criado quando máquinas são programadas com alguns (mas não todos) aspectos da inteligência humana, incluindo a capacidade de aprender, resolver problemas, e definir prioridades. Com essas habilidades (limitadas), uma máquina pode resolver problemas bastante complexos.

Inteligência de máquina envolve lógica por necessidade. Sistemas tidos como inteligência de máquina “real”, por exemplo, conseguem identificar quando cometem erros, buscar dados similares que poderiam levar ao mesmo equívoco, e evitá-lo.

Web3 expande as técnicas de aprendizado de máquina, especialmente com o aumento de dados disponíveis por conta da transparência das blockchains. 

Figura 70

1. Qual é a inovação de DeFi?

Algumas inovações são enxutas, mas importantes. Nos capítulos 16 a 20, iremos explorar as várias fórmulas matemáticas que suportam contratos inteligentes e AMMs em DeFi.

Outra inovação é o uso de curvas de ligação (*bonding curves*) como arcabouço tecnológico para esses protocolos. Existem muitas maneiras de usar curvas de ligação, conforme discutido no Capítulo 11.

1. O que é primeira camada (*Layer 1*) e segunda camada (*Layer 2*)?

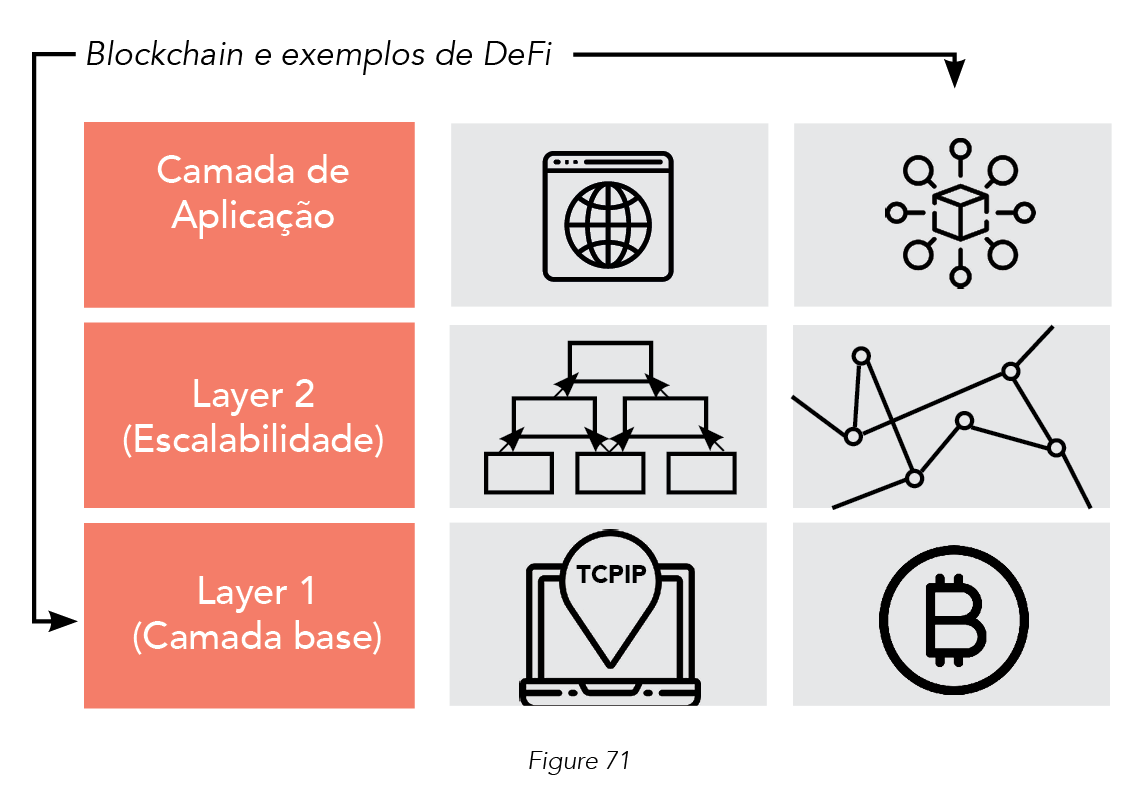


Figura 71

Layer 1 é a camada base – e a tecnologia estrutural da maioria das DLTs. Exemplos são Bitcoin, Ethereum, e o Internet Computer Protocol. Essa é a tecnologia “blockchain”. Um dos elementos centrais dessas camadas base (*Layer 1*) é o conceito de registros distribuídos, geralmente auditáveis publicamente e distribuídos através de uma rede de computadores ao redor do mundo. Isso é muito diferente de registros centralizados usados para monitorar transações, como livros físicos de transações, software como o QuickBooks, registros gerais administrados por bancos, e *order books* administrados por aplicativos como Robinhood.

Protocolos de segunda camada, ou *Layer 2*, são soluções de escalabilidade. São muito úteis dado que as camadas de base, ou *Layer 1*, podem ser lentas ou custosas para processos altos volumes de transação. Protocolos de segunda camada geralmente resolvem esse problema ao assumir o trabalho de processamento das transações, e deixando as camadas de base lidarem com a parte de segurança, dados, disponibilidade e descentralização. O resultado é a redução no congestionamento da camada base e maior escalabilidade da mesma. Solução mais comum de segunda camada é chamado de “*rollups*”, ou “*zk-rollups*”, que empacota transações antes de submeter à camada base, reduzindo significativamente os custos.

A Camada de Aplicação é onde a maioria dos protocolos de DeFi se encontram. Podem ser construídos em blockchains de *Layer 1* ou *Layer 2*. O foco dessa camada é produzir soluções para usuários finais, ao invés de soluções de *back-end* para os protocolos (Layer 1 e 2).

|  |
| --- |
| Caixa 5: Comparando Empréstimos em TradFi com DeFi  Vamos imaginar a seguinte situação: Giovanni tem $100 e Eduarda precisa de $100 emprestado. Como funcionaria? Caso eles confiem um no outro, Giovanni pode simplesmente emprestar diretamente para Eduarda, e até cobrar uma taxa de juros de cinco por cento, por exemplo.  Em TradFi (finanças tradicionais), a maioria dos credores e devedores não se conhecem e funciona da seguinte forma: Giovanni deixa seu dinheiro no banco, que paga juros a ele pelo direito de emprestar seu dinheiro para outros clientes que o banco conhece, como Eduarda, que paga ainda mais juros para o banco.  DeFi pode substituir os bancos centralizados e solucionar o problema da “confiança” ao redor do mundo. Ao invés de conhecer e confiar em indivíduos, DeFi direciona a confiança para códigos do sistema. DeFi consegue fazer isso pois (1) dinheiro é programável e (2) o sistema operacional do dinheiro também é programável.  Com DeFi, Giovanni pode encontrar todas as “Eduardas” ao redor do mundo **sem precisar**:   * 1. Confiar ou conhecer Eduarda pessoalmente.   2. Interagir com bancos ou terceiros que cobram taxas exorbitantes nessas transações.   3. Encontrar uma instituição centralizada que atende suas necessidades (especialmente importante em regiões que carecem de instituições financeiras robustas).   **Empréstimos em DeFi**  Protocolos de empréstimos em DeFi codificam tokens monetários (ex: $TOKEN). O código é estruturado para incentivar pessoas a depositarem ou sacarem seu dinheiro.  Isso é feito por meio de taxas de juros dinâmicas, que alteram o comportamento das pessoas ao encorajar e prover oportunidades para emprestar ou tomar, dependendo da taxa.  Quando a demanda cai, taxas de juros também caem. Custo para obter dinheiro diminui. Pessoas têm mais incentivos para pegar empréstimos em $TOKEN, visto que o custo está mais baixo.  Quando a demanda aumenta, oferta circulante aumenta para atender o nível de demanda. Com maior demanda por empréstimos, taxas de juros também aumentam por meio de contratos inteligentes para atrair fundos de credores para o protocolo. Esse processo ajuda a equalizar a oferta e demanda do $TOKEN no curto prazo. |

### Economia vs. Valor Monetário

Tokens são uma forma de extrair o valor econômico de uma plataforma ou ecossisitema, e distribuir esse valor para a comunidade. Isso é ótimo! Em DeFi, temos tokens para capturar o valor da comunidade e distribuí-lo de forma justa.

Valor monetário entra quando esses tokens como valor econômico são negociados em mercados secundários por meio do descobrimento de preços.

Uber começou de uma forma similar. Pagavam pessoas para usarem seus serviços. Perdiam dinheiro em toda transação, mas ajudou a deslanchar a economia de rede no longo prazo.

Nas economias de mercados, tokens podem representar tanto valor monetário como meio de pagamento, quanto valor econômico por agregação de valor do ecossistema. Esse sistema facilita o crescimento de forma sustentável para o protocolo.

### Como DeFi Cria Valor Econômico Agregado?

DeFi agrega valor por meio de três áreas-chave:

1. Efeitos de rede e externalidades positivas
2. Colaboração dos comuns
3. Blocos com interoperabilidade

#### Efeitos de Rede e Externalidades Positivas

Em economias de rede, valor é criar de dentro da economia e pelas externalidades positivas.

Em economia, externalidade positiva é um benefício adicional que afeta um terceiro que não recebe o benefício diretamente. Em mercados imobiliários em desenvolvimento, por exemplo, externalidades positivas podem ser melhoras na saúde pública, vizinhanças mais convidativas, livrarias ao redor, ou parques mais limpos.

##### Exemplo de Vacinas

Quando alguém é vacinado, possui menor chance de ser infectado por doenças específicas. Consquentemente, também possuem menos chances de transmitir e infectar outras pessoas. Tomar vacina, nesse caso, tem efeitos de externalidade positiva para a comunidade.

##### DeFi e Política Fiscal

Tokens nativos de cada setor de DeFi são usados para capturar valor econômico no sistema. Em DeFi, economias de rede são multi-laterais, o que cria e gera externalidades positivas em todos os lados do mercado. Tokens nativos são utilizados entre esses setores de DeFi, aumentando ainda mais o valor da plataforma.

Visto que a maioria dos tokens nativos são uma forma de token de governança, a comunidade toma as decisões, incluindo a política fiscal. Cada plataforma tem seu “governo” e poder de tomada de decisão. Em breve, será possível integrar diferentes plataformas para tomada de decisão conjunta, aumentando o valor geral da plataforma e externalidades positivas para a comunidade.

#### Colaboração dos comuns

“Colaboração dos comuns” é um sistema que reduz a centralização de propriedade e se apoia em ter valor econômico compartilhável para estimular cooperação/colaboração. Como protocolos de DeFi são geralmente de código aberto, e não possuem um “dono’, podem ser usados para incentivar colaboração entre pares (*peer-to-peer*).

Esses sistemas buscam gerar o máximo de valor para o protocolo, sem exagerar. Quando há excesso, temos um fenômeno chamado “Tragédia dos Comuns”. Isso ocorre quando usuários extraem o máximo de valor e o mais rápido possível dos recursos compartilhados, sem considerar custos futuros. Essa decisão é tomada pois caso um usuário decida não explorar esses recursos, outro irá fazê-lo, dado que não são eles que irão pagar pelas consequências futuras do abuso (vide riscos morais na Parte I: 3.5 e Parte I: 5.6).

Água, nosso recurso mais valioso, é um ótimo exemplo. Água é um recurso compartilhado que nos beneficia hoje, e precisa beneficiar também as gerações futuras. Indivíduos ou empresas oportunistas utilizam água de forma irresponsável, esgotando ou deteriorando o recurso com suas ações coletivas. A crise de seca na África do Sul de 2017[[125]](#footnote-126), em que tivemos águas subterrâneas[[126]](#footnote-127) destruídas e lagos poluídos, é um ótimo exemplo disso.

Hoje, estamos mudando a forma que pensamos no bem comum. Sabemos que recursos podem ser facilmente explorados, e podemos criar incentivos para reduzir a exploração destrutiva de bens comuns e promover a colaboração.

#### Blocos com Interoperabilidade

No 14.5 vamos revisar os nove setores de DeFi. Esses setores funcionam como peças de Lego, podendo ser empilháveis e com comunicação aberta entre eles.

##### ETFs Tradicionais vs. ETFs Cripto

Vamos imaginar o seguinte cenário: Você tem dinheiro (USD) e quer comprar um derivativo (ETF) em uma corretaora (NASDAQ) para receber retornos (dividendos).

Você pode utilizar dinheiro programável ($USDC, USD em cripto) para comprar um derivativo (um ETF com balanceamento automático) em uma DEX (Balancer) e receber retornos ($BAL + retornos de taxas de transação).

##### Exemplo: Empréstimos em DeFi

Detentores de tokens podem empresar seu dinheiro (ex: $USDC). Outros podem pegar esse dinheiro emprestado e utilizá-lo como colateral em outras plataformas de DeFi. Os credores realizam retornos na forma de juros, assim como tokens nativos em alguns protocolos.

Devedores podem, em contrapartida, colocar esse dinheiro em *stake* (ex: Curve Vault) em uma DEX com baixo risco de perdas impermanentes (*impermanent loss*) e receber não só juros, mas também tokens nativos de governança (ex: $CRV) dependendo da plataforma.

O sistema inteiro funciona como peças de um Lego, que podem ser colocadas uma em cima da outra. Esse conceito gera muitas externalidades positivas provenientes do valor compartilhado entre os diversos protocolos de DeFi.

Tokens inicialmente existiam apenas em seus próprios protocolos (ex: somente na Ethereum, somente na Algorand). Hoje, tokens podem cruzar diferentes camadas de blockchains por meio de pontes (*cross-chain bridges*) e corretoras. Alguns exemplos notáveis são o CCIP (Cross-Chain Interoperability Protocol), da Chainlink, e a IBC (Inter-Blockchain Communication).

Valor econômico agora pode existir além de protocolos de primeira camada. Diferente de finanças e redes tradicionais, onde custo de mudança inibe externalidades positivas, soluções interoperáveis possibilitam o fluxo de valor econômico entre os protocolos.

Imagine cada protocolo de *Layer 1* como um idioma. Ethereum só fala inglês, EOS só chinês, e Algorand apenas espanhol. Esses são idiomas completamente diferentes. Caso haja uma boa ideia na comunidade que fala inglês, será difícil compartilhar com a comunidade chinesa ou espanhola. Polkadot quer ser o tradutor para possibilitar os três idiomas de se comunicarem entre eles – é daqui que o valor econômico surge!

A partir do momento que vários protocolos de primeira camada tenham comunicação aberta entre eles, imagine o quanto valor econômico será gerado para toda a comunidade.

### Nove Setores de DeFi

*Nota: caso você esteja no ambiente de mercado de capitais, veja o Apêndice A para comparação dos termos usados em DeFi.*



Figura 72

Finanças é um campo complexo. Quando alguém te fala que trabalha em finanças, raramente se pergunta na sequência “qual área?”, a não ser que você também trabalhe em finanças. Em medicina, por outro lado, seria mais provável perguntar sobre a especialização como pediatra, cardiologista, neurologista etc.

E isso se dá porque finanças é um conceito “caixa preta” (teoria dos sistemas) para a maioria das pessoas. Existem muitos setores e todos eles requerem conhecimento especializado. Vamos abordar nove deles, que nos dará uma noção do ambiente de DeFi.

Os nove setores são moedas como meio de pagamento, ativos, armazenamento de ativos, corretoras e trade, empréstimos, derivativos, fundos e portfólios, seguros, e aplicações além de finanças.

#### Moedas como Meio de Pagamento

Meios de pagamento do mercado financeiro tradicional inclui moedas como USD, GBP, EUR, JYP, e BRL.

Essas moedas são governadas por economistas monetários brilhantes do banco central de cada país. Eles definem a taxa de juros, a meta de inflação, e controlam a “facilitação quantitativa” (*quantitative easing*) e impressão de dinheiro.

Em DeFi, codificamos a lógica do negócio com máquinas (códigos) e matemática. Isso possibilita comunidades de DeFi estabelecer estabilidade de preços matematicamente para reduzir a influência política que torna o dinheiro tradicional tão parcial (“não-neutro”). DLT nos permite terceirizar a confiança da moeda para máquinas ou códigos.

Nesse contexto, DeFi utiliza tokens para suprirem várias funções. Moedas como meio de pagamento é uma das funções. Porém, não se esqueça do “SUMS” abordado anteriormente, que descreve as diferentes formas de interação por meio de tokens com vários setores de DeFi.

Os meios de pagamento do DeFi incluem tokens como $ETH[[127]](#footnote-128), $wBTC, $USDT, $AMPL.

#### Ativos

Em TradFi, temos as seguintes classes de ativos:

* Ações
* Títulos (*Bonds*)/Renda fixa
* Dinheiro/Fundos do mercado monetário (FMM)
* Imobiliário, commodities, e outros ativos tangíveis
* Futuros e derivativos financeiros

DeFi criou uma nova classe de ativo. Ativos de cripto como $SNX, $AAVE, $YFI, $MKR podem se comportar de forma similar a algumas das classes citadas acima. São ativos relativamente novos ainda e possuem elementos de várias classes de TradFi, como ações, bonds e outros instrumentos de renda fixa, e até mesmo derivativos. Esses ativos possuem outras propriedades únicas que são características de cada ambiente de DeFi.

Esses ativos acima são exemplos de tokenização análoga de ativos existentes no mercado tradicional. Novas classes de ativos estão sendo desenvolvidas com o passar do tempo.

O trabalho de precificação desses ativos é feito pelo mercado por meio de negociações no mercado secundário, AMMs (formadores de mercado automatizados), e outras projeções financeiras – com novas técnicas de precificação sendo constantemente desenvolvidas.

#### Armazenamento de Ativos

Ativos tradicionais são armazenados em bancos como o Banco do Brasil, Bradesco, e Itau. Bancos chamados de “Fintechs” como NuBank, Banco Inter, Banco Original estão inovando com novas soluções para armazenamento desses ativos.

*Holders* de ativos cripto relacionados a DeFi utilizam carteiras (ou *wallets*) como Metamask, Phantom, e Trezor para guardar meus ativos de forma segura (assim esperamos). Novas soluções de carteiras também vêm sendo desenvolvidas.

#### Corretoras & Trade

Exemplos de corretas tradicionais são a NASDAQ, a nossa querida B3, a NYSE etc. Esses sistemas são basicamente um livro gigante de ordens de compra e venda, onde investidores submetem suas operações (compra e venda). A transação é feita quando outra contraparte corresponde àquela ordem, ou por um formador de mercado manual.

Em um sistema de contraparte, donos de ferro só podem trocar por cimento quando alguém também tem interesse, como um sistema de permuta. Um sistema com formador de mercado manual seria como ter uma empresa gigantesca de ferro e cimento com liquidez suficiente em estoque de cimento e ferro que poderiam executar a troca de ferro por cimento sem a necessidade de uma contraparte.

Na indústria de DeFi temos corretoras descentralizadas (DEXs) como Uniswap, Bancor, e Curve. Ao invés de fazer a correspondência de contrapartes, a máquina executa a transação. Contratos inteligentes das DEXs usam fundos da liquidez para executar a troca. A *pool* de liquidez é análoga ao tamanho da carteira de formadores de mercado em TradFi.

#### Empréstimos (ou Crédito)

Bancos tradicionais oferecem serviços de custódia (depósitos com rendimento mínimo) e empréstimos (com juros altos). Em DeFi, temos protocolos de crédito como Aave, Maker, e Compound.

Voltando ao exemplo da Caixa 5, em que Giovanni tem $100, e Eduarda quer pegar $100 emprestado. Como eles não se conhecem, o banco executa a “troca”. Giovanni deposita $100 no banco, e o banco paga a ele uma taxa mínima (ex: 1%).

Eduarda então pede ao banco um empréstimo de $100, e o banco cobra X de juros enquanto a dívida estiver pendente. Eduarda recebe $100 e o banco ganha X-1%[[128]](#footnote-129).

DeFi utiliza códigos e protocolos de empréstimo para substituir o papel do banco e otimizar todo o processo. Protocolos de empréstimo determinam matematicamente as taxas de juros oferecidas para Eduarda no momento da operação. Eduarda pode comparar a taxa entre os diversos protocolos e escolher a melhor opção. Giovanni não precisa nem estar envolvido diretamente.

Assim como corretoras e plataformas de trade, empréstimos também vão desde centralizados (Celsius, Nuo Network) até descentralizados (Aave, Compound). Ambos os sistemas oferecem taxas de juros para credores e tomadores de empréstimo (devedores) para incentivá-los a utilizarem a plataforma. Não existe uma fórmula padrão; taxas são determinadas de forma independente por cada protocolo usando lógicas únicas de cada um.

#### Derivativos

Contratos de futuros, swaps de taxas de juros, opções, e operações estruturadas são alguns exemplos de derivativos do mercado tradicional. O mercado de derivativos possui o maior volume de capital de todo o setor financeiro – seu valor nocional é 48 vezes maior[[129]](#footnote-130) do que o valor de mercado bruto.

Em DeFi, derivativos ainda estão em fase de exploração. Protocolos como Synthetix, Opyn, Hegic, e GMX oferecem produtos desse tipo. Derivativos comuns de cripto são futuros, futuros perpétuos, opções, e opções binárias. Novos produtos estão em desenvolvimento como ETFs cripto e índices DeFi. Vamos explorar esse ponto na próxima seção.

Matemática é usada para definir a lógica do negócio em aplicações simples como balanceamento de portfólio e administração de posições alavancadas.

#### Fundos & Portfólios

ETFs (fundos negociados em bolsa), fundos mútuos, hedge funds, e fundos municipais são exemplos de TradFi. Fundos podem ser administrados de forma passiva ou ativa por empresas como a Fidelity. Existem também os chamados VCs – venture capitals – para outros tipos de exposição em termos de risco/retorno.

Em DeFi, fundos e portfólios podem ser administrados por fundos de VC tradicionais ou fundos de asset management. Esses fundos podem ser automatizados com contratos inteligentes, permitindo transações em ativos específicos. PieDAO e Balancer são exemplos disso.

Índices são um tipo de fundo mútuo ou ETF que acompanha ativos em índices de mercado. Exemplos do mercado tradicional são a S&P 500 e o Russell 200. Não iremos cobrir fundos de índice em DeFi, mas o mecanismo é parecido no sentido de que utilizam matemática para a definição de alocação.

#### Seguros

Empresas como AIG, AXA, Ping An, AVIVA, e Prudential são parte do mercado tradicional e oferecem seguros variados.

O mercado de seguros inicialmente funcionava quase que em um modelo de peer-to-peer. Fazendeiros captavam dinheiro para assegurarem uns aos outros. Caso a safra do Fazendeiro A fosse destruída por algum motivo, o montante captado servia para cobrir as perdas. Em retorno, fazendeiro A precisa pagar determinada quantia mensalmente ao fundo.

Com os efeitos da globalização e maior dificuldade de administrar localmente esses fundos compartilhados de seguros, empresas de seguros foram criadas para agregar e assumir o risco. Indivíduos pagam um prêmio (*premium*) para transferir esse risco para as seguradoras.

Na indústria DeFi, o mercado de seguros ainda é relativamente novo, mas com muito potencial. Pagamentos podem ser automatizados por códigos e matemática. Riscos podem ser calculados, considerando dados *on-chain* e *off-chain* disponíveis.

Nexus Mutual, por exemplo, oferece seguros financeiros para erros de contratos inteligentes. Opyn, por outro lado, oferece seguros para diminuir exposição ao risco em contratos de opções.

#### Além de Finanças

Produtos financeiros são usados de muitas maneiras, indo além somente do setor financeiro. Pessoas usam dinheiro para comprar produtos no seu dia a dia, assim como governos utilizam o mesmo dinheiro para resolver questões contábeis como a dívida externa.

DeFi como um todo ainda é novo. Aplicações de DeFi além de finanças incluem artes e pesquisas por meio de NFTs, e mercados de apostas. Alguns exemplos de NFTs incluem Aavegotchi, Rarebits, SuperRare, e tokens de acesso a comunidades. Augur e Gnosis são exemplos de mercados de aposta em DeFi.

## Ponzinomics

*Ponzinomics = Ponzi + economics.*

Ponzinomics é a economia relacionada a “esquemas Ponzi” – golpe de investimento, ou operações fraudulentas.

### Economia (*Economics*) vs. Ponzinomics

Lembre-se, economia é uma **ferramenta**, então não é intrinsecamente **boa** ou **ruim**. Pode ser **usada** para causar bons ou maus resultados. Os resultados podem ser ótimos quando a economia é usada para incentivar comportamentos que criam valor econômico. Por outro lado, podem ser péssimos quando são usados para fraudes, golpes, ou roubos. Economia por si só não pode ser culpada pelos maus resultados. **Pessoas** podem usar essa ferramenta para o bem ou para o mal.

Do mesmo modo, tecnologia também é neutra, e pessoas podem criar usos positivos ou negativos. Facebook, como plataforma tecnológica de conexão de pessoas e compartilhamento de informações é neutro. Mas, essa plataforma pode ser usada para o bem, como possibilitando amigos e famílias a se conectarem ao redor do mundo, ou para o mal, com o compartilhando de fake news ou campanhas políticas.

#### Os Três Fundamentos da Economia

Economia possui três conceitos fundamentais. Falamos sobre eles o tempo todo durante o livro!

1. Oferta.
2. Demanda.
3. Custo de oportunidade – reflete as escolhas individuais quando há duas ou mais opções.

#### Introdução a Ponzinomics

Ponzinomics também tem três conceitos fundamentais, todos baseados em uma “economia duvidosa”. Esse tipo de modelo começa com uma **crise de liquidez.** Oferta começa muito limitada, geralmente de forma artificial. Preços aumentam exponencialmente de alguma maneira, também geralmente artificial. Por exemplo, um indivíduo malicioso pode executar centenas de transações (*pumping*) para aumentar o preço. Essa crise é criada da seguinte forma:

1. Oferta do token precisa ser muito baixa.
2. Demanda precisa aumentar artificialmente, impulsionando preços para cima.
3. Atores maliciosos usam o FOMO**[[130]](#footnote-131)** - termo muito comum na web3 para se referir à sensação de ver preços subindo e querer comprar – para influenciar usuários a comprarem em busca de ganhos de curto-prazo.

### Fundamentos de Ponzinomics

No geral, ponzinomics é um sistema econômico perverso estruturado para induzir crises de liquidez. Essa crise ocorre quando não há oferta suficiente no lado dos vendedores para cumprir com a demanda dos potenciais compradores. Demanda se torna altíssima, mas não há liquidez suficiente para comprar porque a oferta circulante é mínima. Em crises de liquidez na blockchain, a quantidade de tokens não é suficiente para todos que desejam comprar.

Voltando para o conceito do “Economics Design Framework” que eu criei, atores de boa-fé tentam criar incentivos robustos e sustentáveis em um ecossistema. Isso possibilita que o sistema cresça e agregue valor. Tokens internos representam o real valor econômico que é criado na rede; isso não tem relação com o valor de mercado que os tokens são negociados nas corretoras, mas com o valor que a rede cria por existir e funcionar. Quando um token é negociado em mercados secundários, gera dados que podem ser usados para descobrimento de preços e valor monetário, além do conceito de valor econômico.

No geral, esse sistema funciona. Porém, em esquemas Ponzi, o valor monetário do token interno só existe **por causa** dos “pumps” (impulsionamentos artificiais de preço) no mercado secundário. Esses movimentos restringem a oferta circulante, e estimula a demanda. Em situações normais, oferta limitada estimulando a demanda é uma característica de economia saudável; mas, quando mercados secundários estão criando propositalmente demanda artificial e crises de liquidez, isso caracteriza um esquema Ponzi em ação.

Descobrimento de preços no mercado secundário reflete o aumento artificial de preço causado por esses esquemas de “*pump and dump*” (sobe e depois cai tudo). Esses movimentos não são baseados em fundamentos sólidos do mercado primário, mas em esquemas econômicos para influenciar o preço temporariamente. Nada além de *hype* e manipulação técnica.

### Estudo de Caso: Ponzinomics Sete Passos

1. Seja influente de alguma forma. É relativamente fácil, hoje em dia, criar uma conta fake e gerar algum engajamento por meio de redes sociais.
2. Defina o valor usando sua influência. Pode ser por percepções de poder de uma comunidade, ou convencendo investidores de determinar seu valor com base no que você deseja.
3. Disponibilize uma quantidade pequena de tokens para corretas (como 3%).
4. Consiga que pessoas comprem o montante disponível nas corretoras (veja o passo 1).
5. Valor de mercado total é definido, então, por esses 3% da oferta circulante. De uma hora para outra, torna-se muito valioso.
6. Com o uso de FOMO, indivíduos correm para comprar o token e realizando transações “forçadas”. Esse movimento aumenta o volume transacionado e impulsiona o preço ainda mais para cima.
7. Venda (*dump*) os tokens lentamente, visto que você tem 97% da oferta para operar. Liquide o máximo possível até que o mercado descubra.
8. Desapareça.

### Dez Mecanismos de Ponzinomics

1. Execute um *fork* (bifurcação) de algum protocolo de código aberto e copie seu código. Isso não é raro, mas literalmente copiar o código adiciona pouco valor.
2. Liste um token na Uniswap com nome parecido, mas falso de moedas conhecidas. Execute algumas transações na *pool* de liquidez. Também é bastante comum, visto que esquemas de fraude e projetos Ponzi sempre querem “pegar carona” na reputação de projetos legítimos.
3. Construa uma comunidade no Twitter usando uma conta anônima para promover o projeto.
4. Use um nome similar a tokens reconhecidos/promissores. Essa é uma tática muito comum, dado que novos usuários de DeFi facilmente se confundem com a quantidade de informação existente.
5. Promova o projeto no Facebook, nos comentários do YouTube, timeline do Twitter, etc[[131]](#footnote-132).
6. Aplique o “puxão de tapete”, ou *rug pull*, removendo a liquidez existente na DEX (corretora descentralizada). Usuários ficam com tokens inúteis na mão, pois alguém retirou todo o colateral existente na *pool* de liquidez.
7. Liste tokens que nunca serão negociados abertamente. Alguns tokens são de pura utilidade e existem apenas em protocolos bem-sucedidos com o objetivo de conceder acesso aos detentores. Golpistas podem criar tokens com nomes similares e listar em corretores descentralizadas para enganar usuários, que podem pensar que o token terá a utilidade do protocolo bem-sucedido.
8. Troque o link real do token por um link fake[[132]](#footnote-133).
9. Faça uma pré-venda e liberação lenta para tokens da venda pública para permitir que compradores da pré-venda liquidem seus tokens sobre a liquidez dos demais.
10. Auditoria própria dos contratos inteligentes por criadores anônimos.[[133]](#footnote-134).

## Matemática de Tokens Estáveis

Até agora, destacamos a matemática principalmente na segunda metade desse livro, abordando DeFi. Matemática define a lógica do protocolo, que é então transformada em código para que máquinas entendam e executem.

Fórmulas são muito importantes nesse contexto. Auditorias são cruciais, para evitar falhas no código. Transações são baseadas na integridade da matemática para automatizar e executar a lógica corretamente.

### Conceitos Matemáticos de DeFi

Não existe uma fórmula perfeita para DeFi ou até mesmo para um setor específico. Depende dos objetivos, da lógica do protocolo, e nos resultados esperados. Mas, pelo menos temos fórmulas gerais para começarmos a pensar, dependentes de algumas variáveis.

### Moedas Como Meio de Pagamento

Dinheiro tem três funções. Aqui, queremos focar no dinheiro como meio de pagamento.

Existem três formas gerais de criar uma moeda *on-chain* para o ecossistema DeFi:

* Paridade 1-para-1 (*peg*)
* “Sobrecolateralizado” (*over-collateralized*)
* Balanceamento algorítmico
* Paridade 1-para-1 (*peg*)

#### Paridade 1-para-1 (*peg*)

Fórmula Geral:

Esse é o método mais simples e básico. Um token novo é emitido para cada token de colateral. Isso funciona para paridades estritas como $BTC-wBTC, $ETH-sETH, $USDT-aUSD, e $aAAVE-AVE.

Contratos inteligentes podem ser programados para executarem essa emissão e queima ao invés de confiar em um terceiro para fazê-lo. Promove confiança na matemática e código ao invés de terceiros terem custódia de seus ativos colaterais.

#### “Sobrecolateralizado” (*over-collateralized*)

O método de sobrecolateralização é usado para possibilitar a provisão de ativos como colateral, e subsequente emissão ou empréstimo de uma quantia baseada naquele colateral.

MakerDAO emite (“minta”) $DAI com base nos colaterais que usuários fornecem. Precisam colocar 150% em valor de colateral para receber 100% em $DAI.

Aave e Compound permite usuários depositarem ativos que podem ser usados como colateral para receber empréstimos. Usuários podem tomar empréstimos até uma certa porcentagem de seu colateral – algo em torno de 60-70 por cento.

Outra nota interessante com uma perspectiva de economia monetária é a mudança para bancos de reserva total[[134]](#footnote-135). Banco de reserva total[[135]](#footnote-136) significa que para cada dólar emitido, 100% de colateral é mantido em reserva. DeFi vai um passo além, com a “sobrecolateralização”.

#### Balanceamento Algorítmico

Esse último método usa matemática para balancear o token e manter a estabilidade de preços. Atualmente, a maioria desses tokens são pareados a $1 USD, mas isso pode mudar conforme o sistema amadurece e podem ser atrelados a uma cesta de produtos, ou outras referências. Tokens $XTC do Internet Computer Protocol (ICP), por exemplo, são pareados a Direitos Especiais de Saque (DES) do FMI, ou Fundo Monetário Internacional. DES são colateralizados com uma cesta de moedas: USD, EUR, RMB, JPY, e GBP.

$AMPL, como outro exemplo, possui um método único de valuation pois, ao invés de definir o preço, ele é determinado pela proporção possuída da rede. Vamos entender melhor.

Imagine que você tem 0.1% de todos os tokens (valor de mercado), e essa quantia é igual a $1 USD ou 10,000 $AMPL. No momento seguinte, o preço sobe para $1.15 USD. A oferta circulante de tokens aumenta proporcionalmente, e você continua possuindo a mesma porcentagem da rede.

Funciona similar ao conceito de desdobramento de ações (ou *stock split*). Esse mecanismo geralmente indica boa saúde e crescimento da empresa, que tornou o preço de cada ação muito cara, dificultando a liquidez nas transações. A empresa emite mais ações e distribui proporcionalmente para os acionistas (tipicamente em proporções como 1:3— para cada ação possuída será trocada por três). O aumento na oferta causa uma redução no preço proporcional.

O algoritmo de balanceamento utiliza um conceito matemático chamado de “invariantes” (vide 17.2.1). Invariantes são um tipo de constante que requer o algoritmo balancear ambos os lados da equação (no caso da $AMPL, tokens possuídos e preço do token). Nesse exemplo, a invariante é a porcentagem possuída da rede. Independente de preços subirem ou descerem, a proporção de cada acionista deve se manter a mesma.

## Matemática dos Mecanismos de AMMs Descentralizados

Curvas de ligação (as *bonding curves*) determinam a relação entre o token A e o token B por meio de fórmulas matemáticas. O formato do gráfico é geralmente parecido (côncavo), mas as fórmulas matemáticas são bastante diferentes. A similaridade entre as diversas fórmulas é que utilizam constantes “invariantes”. Seguem as leis da física de conservação de energia.

Formadores de mercado automatizados são muito úteis pois facilitam descobrimento de preço com total transparência. Podemos também explorar gráficos multi-dimensionais, ao invés de apenas gráficos em 2D (duas variáveis). Isso é feito com a adição de outras variáveis (ex: tokens, oferta total, e oferta circulante) para interagirem nas *pools* de liquidez.

Existem outras formas inovadoras surgindo no ecossistema, mas vamos focar na estrutura básica de AMMs (formadores de mercado automatizados).

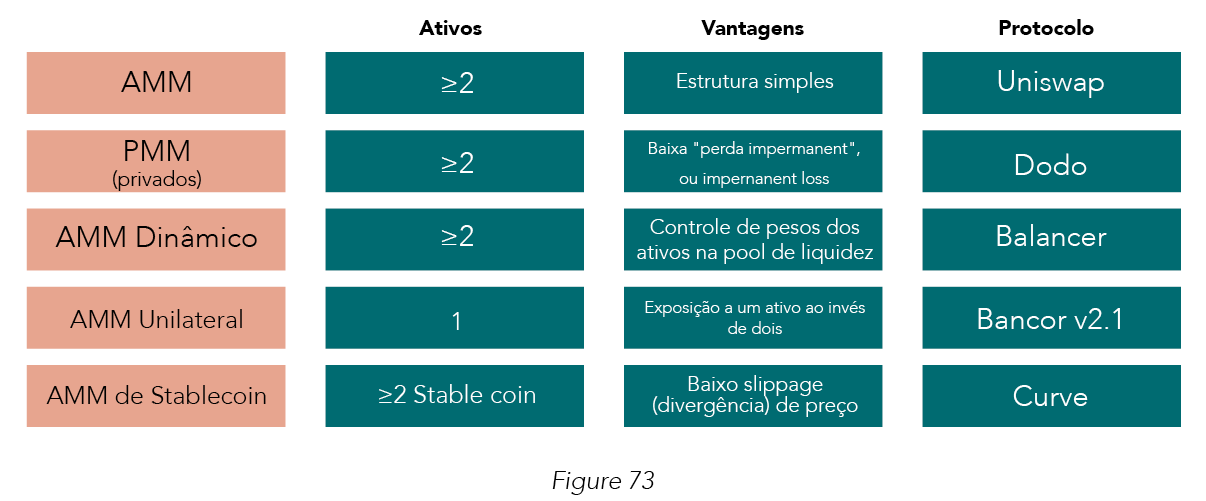


Figura 73

### CeFi vs. DeFi

Existem dois tipos de corretoras no mundo cripto: corretoras centralizadas com *order books* como a Binance, Huobi e Kraken, e corretoras descentralizadas como Uniswap, Bancor, Curve.

Matemática é mais aplicável a corretoras descentralizadas com relação a forma que transações são executadas em cada uma.

Matemática é usada como o algoritmo base para essas corretoras descentralizadas, ou formadores gerais de mercado automatizados em DeFi. No geral, curvas de ligação (*bonding curves*) são o principal mecanismo por trás de todas as corretoras descentralizadas. A diferença é como são executadas, determinado pelos algoritmos do protocolo.

Corretoras de CeFi (centralizadas) simplesmente balanceiam o preço e a quantidade de ativos que você deseja comprar. São como sistemas de correspondência (ou *matching*), ao invés de relações matemáticas complexas. Em DeFi, o preço da quantidade de ativos (Token A) que você deseja comprar ou transacionar é dependente de uma fórmula matemática. Essa fórmula leva em consideralção a quantidade total de ativos (Token A e Token B) na *pool* de liquidez. Utiliza matemática para facilitar transações, ao invés de mecanismos de livro de ordens e correspondência de compradores e vendedores.

### Formadores de Mercado Automatizados (AMMs)

O formato da curva difere dependendo do caso de uso das curvas de ligação (*bonding curves*). Em corretoras descentralizadas, a estrutura da curva é praticamente a mesma (côncava). Porém, as fórmulas são muito diferentes. A única similaridade é que todas dependem de constantes invariantes.

A tabela abaixo resume os algoritmos generalizados

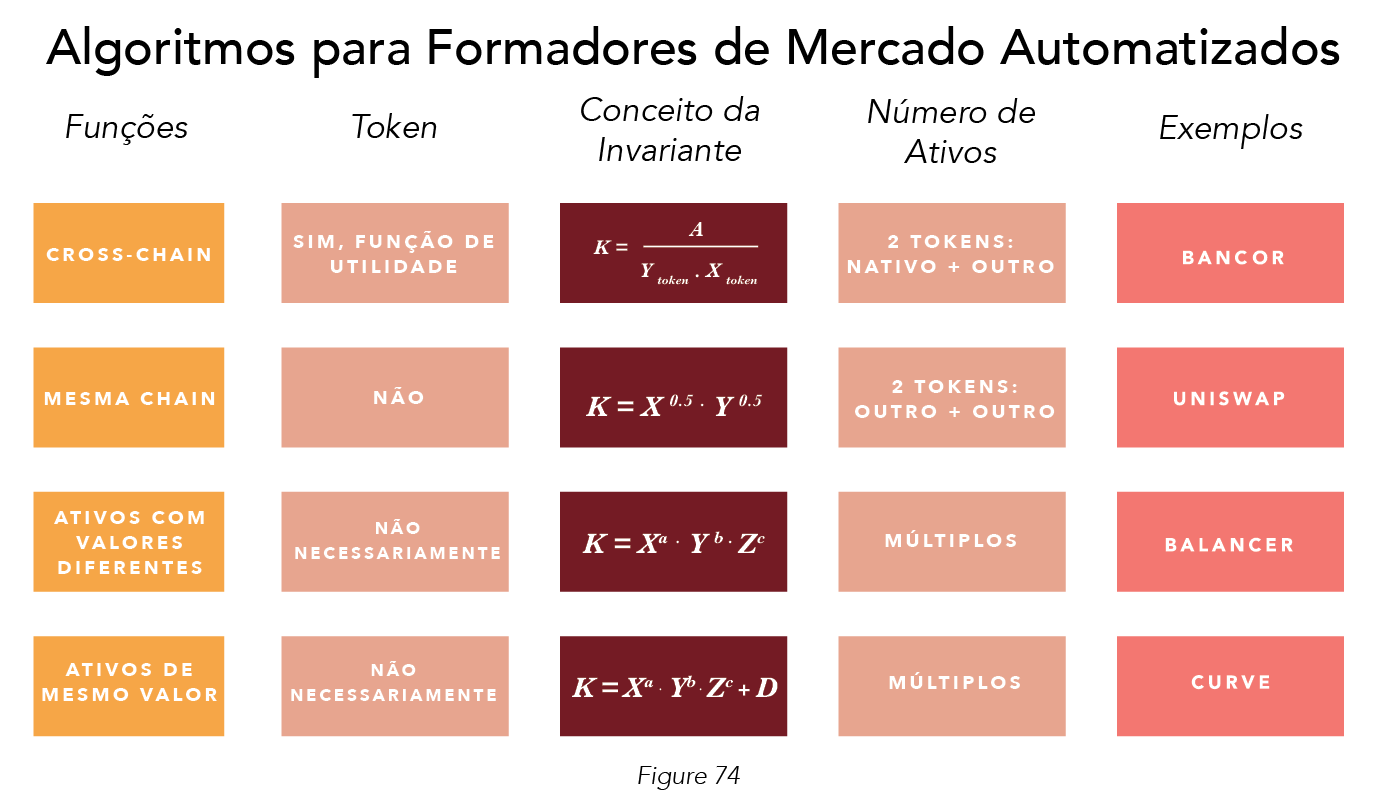


Figura 74

#### Constante Invariante “K”

Para AMMs funcionarem, precisam aplicar invariantes em suas fórmulas matemáticas. Uma invariante é um tipo de constante matemática que nunca se altera. As funções da variável podem mudar (ex: token X e token Y), mas como uma “constante”, a invariante não muda. É como o princípio físico de conservação de energia.

A invariante é crucial para a governança dos códigos de contratos inteligentes. Permitem a execução de transações em preços determinados pela curva de ligação (*bonding curve*)*.* O que deixa a desejar em perfeição de preços[[136]](#footnote-137) é compensado pela previsibilidade de preços. Conforme a liquidez aumenta, preços se tornam mais precisos, e o AMM pode transacionar com margens mais apertadas – ou seja, taxas mais baratas.

Constantes invariantes são análogas à pressão imposta sobre o líquido em pressas hidráulicas. Quando um lado diminui, o outro aumenta para balancear.

Diagram

Description automatically generated

Figura 75

Da mesma maneira, quando $ETH é adicionado à *pool* de liquidez (força aplicada sobre a pressa hidráulica), a quantidade de $TOKEN é reduzida (líquido se move para o outro lado). O AMM foi programado para garantir que o produto (a constante invariável) do número de $TOKENs e $ETH seja sempre o mesmo.

### Gráfico Geral

No geral, o gráfico tem formato côncavo com inclinação descendente. Assumindo que não há adição de nova liquidez, o gráfico representa o preço a qual um token pode ser negociado por outro.

No gráfico da Figura 76, em 50 tokens do eixo x, você recebe 40 tokens do eixo y. Significa que você poderiam por exemplo, trocar 50 $TOKEN por 40 $ETH.

Chart

Description automatically generated

Figura 76

Assumindo que não há adição de nova liquidez, a área embaixo do gráfico em cada negociação de token A por token B é sempre a mesma.

E isso é efeito da invariante que estamos tanto falando sobre.

O sistema pode se expandir em termos de dimensões envolvidas no cálculo. Em gráficos 3D, qualquer ponto da superfície do gráfico representa uma taxa de conversão apropriada.

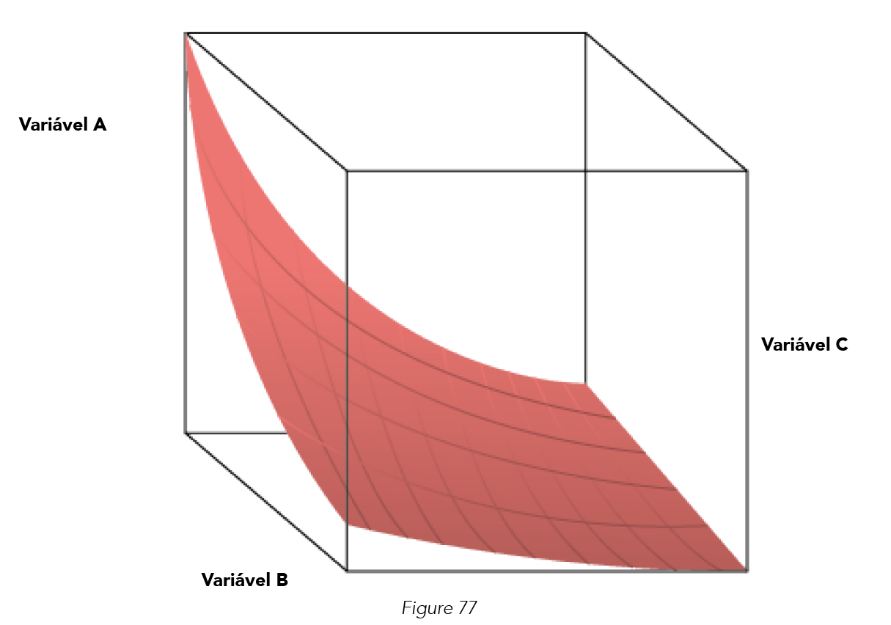


Figura 77

O volume embaixo da curva é a invariante.

Shape

Description automatically generated

Figura 78

## Curvas de Ligação para Captação de Recursos (*Fundraising*)

Outro caso de uso para curvas de ligação, ou *bonding curves*,é para captação de recursos - tipicamente chamada de *fundraising*.

### Aplicações para Fundraising

Conforme discutido na Parte I: Capítulo 11, curvas de ligação emitem novos tokens com base no colateral recebido. Quando novos ativos ($ETH) são adicionados à reserva de colaterais, novos $TOKEN são emitidos.

Ao contrário de formadores de mercado automatizados (AMMs), curvas de ligação para captação de recursos não seguem uma fórmula geral. Mesmo assim, precisamos fazer algumas considerações sobre variáveis e questões adicionais

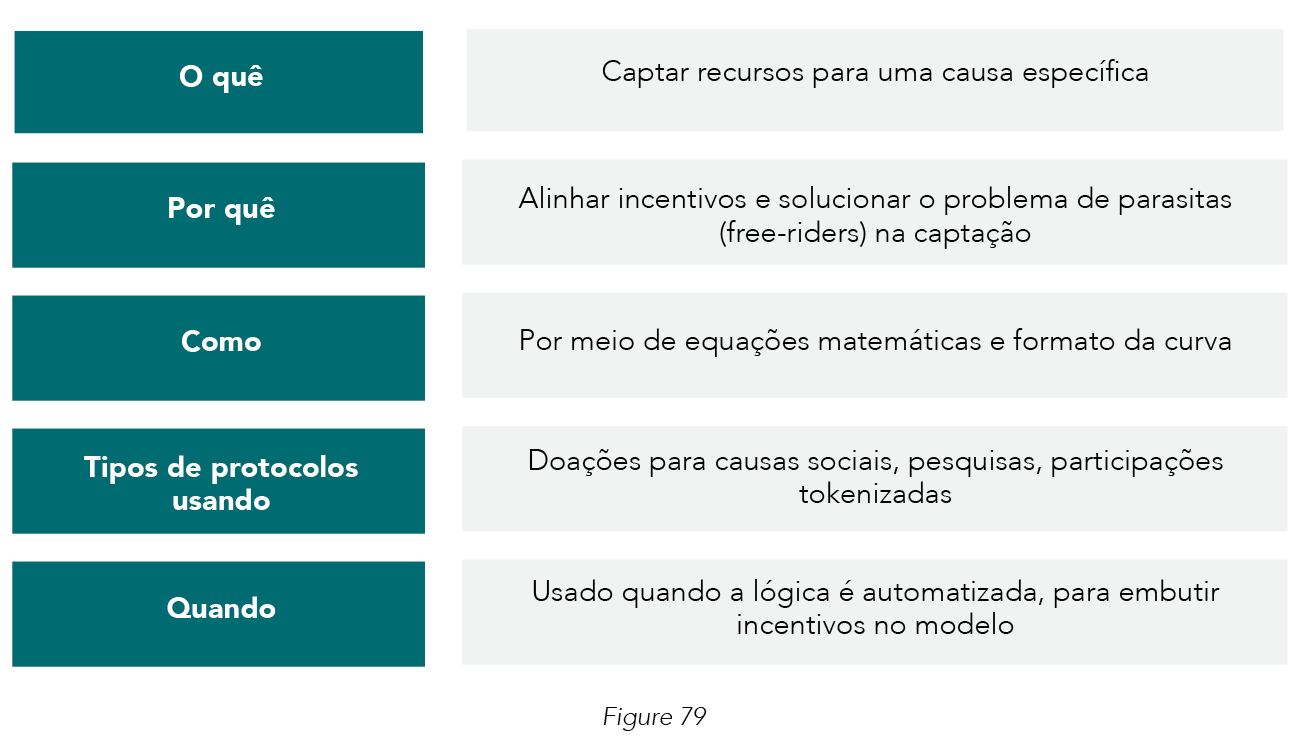


Figura 79

### Captação para Tokens com Função de Utilidade

Tokens de utilidade (*utility tokens*) facilitam transações internas de ecossistemas. A maior parte das interações são envolve o mercado secundário ou mundo externo.

"*Utility tokens*" tem três casos de uso:

1. Captação de doações para apoiar diferentes causas
2. Captação individual por meio de curvas de ligação
3. Captação contínua para projetos com pesquisa em andamento

#### Captação de doações

Um exemplo de captação de doações é a plataforma Giveth. Giveth é uma organização que apoia várias causas sociais. Fundos são doados para o sistema e governados pela curva de ligação (*bonding curve*) - uma variação da curva comum que discutimos anteriormente.

**Como fundos são coletados?**

De modo geral, a curva de ligação funciona da mesma forma. Fundos ($DAI) são adicionados à curva de ligação e outro token ($TOKEN) é emitido.

Quando $DAI é adicionado ao sistema, parte do valor vai para uma reserva colateral da fundação e outra parte é direcionada para uma reserva de financiamento para apoiar as diversas causas sociais.

A reserva de colateral é onde usuários resgatam seu colateral em $DAI ao submeter de volta a quantia referente em $TOKEN.

Visto que Giveth é totalmente voltada pra causas sociais, fundos doados e adicionados à reserva são usados para vários fins - coleta de lixo em praias, por exemplo.

**Como recursos (fundos) são distribuídos entre as causas?**

Várias causas são apoiadas por meio de votações. Usuários submetem propostas para apoiar uma causa específica. $TOKEN pode ser usado para votar em propostas, e fundos são alocados de acordo com os resultados.

No caso do protocolo Giveth, o outro fator da curva é o tempo. Existe um período de *lock-in* (tempo que tokens comprados nas rodadas de captação ficam travados) para prevenir investidores iniciais de removerem seu capital da reserva de colateral.

A função da curva no modelo de liquidez constante do Giveth é um gráfico com inclinação positiva. Um modelo simples pode ser: .

Especificamente, temos cinco variáveis utilizadas no modelo matemático da curva de ligação da plataforma Giveth:

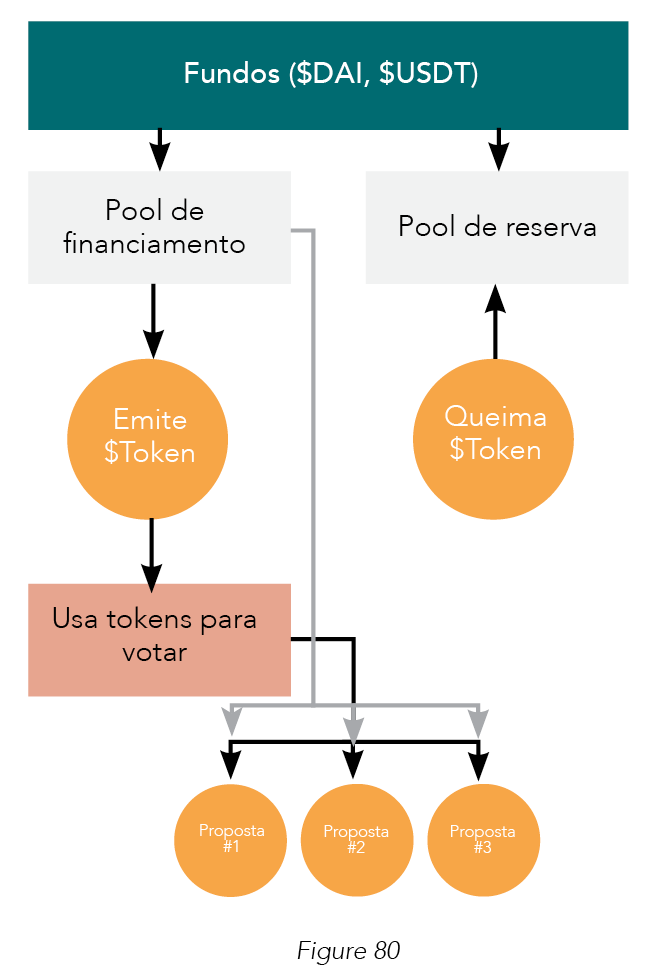


Figura 80

1. Token Nativo ($TOKEN)
2. Token Colateral ($DAI ou $USDT)
3. Pool de Reserva
4. Pool de Financiamento
5. Fator tempo: período de *lock-in* (trava)

#### Captação Inicial com Reserva

Aragon utiliza uma combinação de AMM (vide Capítulo 17) e liquidez constante (vide exemplo da Giveth acima) em seu método de captação de recursos.

Esse AMM utiliza uma função côncava similar ao de outros protocolos de formadores de mercado automatizados. Além disso, faz a provisão constante de liquidez com disponibilidade contínua para negociações. A fórmula de seu índice de reserva é similar ao modelo de AMM.

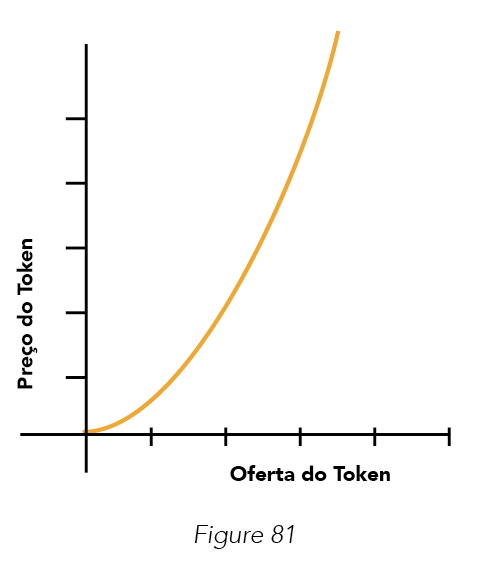


Figura 81

Assim como a plataforma da Giveth, fundos adicionados ao sistema são direcionados para duas *pools* diferentes: *pool* de reserva e *pool* de financiamento (chamada de *pool* discricionária pela Aragon).

A diferença é que a plataforma é governada por uma DAO (Capítulo 19). Ao invés de distribuir fundos de forma determinística por códigos, como acontece na plataforma de doações para causas sociais da Giveth, Aragon possibilita que usuários votem sobre a divisão e distribuição das diferentes *pools* de fundos existentes no ecossistema.

A função da curva é similar à utilizada na Giveth, com inclinação positiva. Um modelo simples pode ser definido por . Para separar as proporções de reserva e financiamento, temos uma curva similar, mas diferente. Por exemplo, , onde .

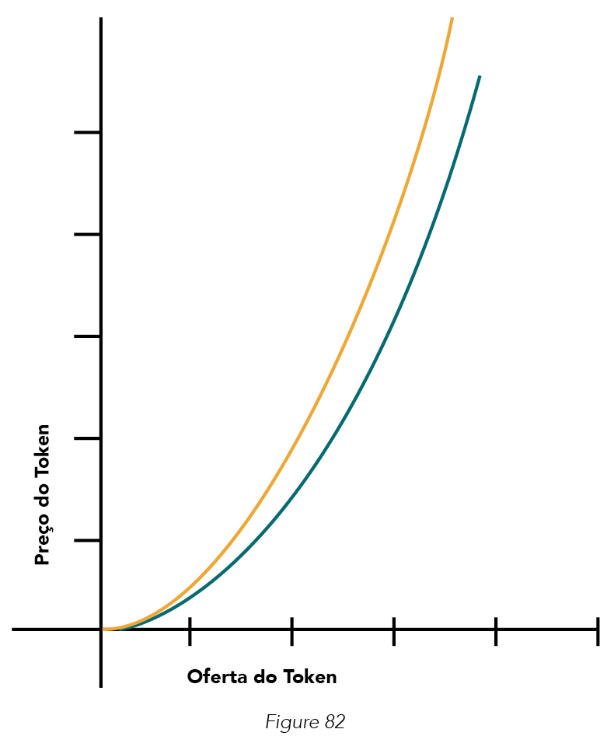


Figura 82

Na Aragon, temos cinco variáveis utilizadas no modelo matemático da curva de ligação (*bonding curve*):

1. Token Nativo ($TOKEN)
2. Token Colateral ($DAI ou $USDT)
3. Pool de Reserva
4. Pool Discricionária
5. Governança por DAO

#### Captação de Recursos para Pesquisa

Outro caso de uso é a captação para pesquisas acadêmicas, especialmente em campos de estudos criados recentemente. Geralmente, organizações governamentais ou empresas privadas financiam essas pesquisas. Essas entidades são incentivadas a prover financiamento por meio da possibilidade de promover produtos ou ideias com os resultados das pesquisas.

Muitas vezes, empresas possuem incentivos perversos para inclinar os resultados de pesquisas de acordo com o que desejam. Um exemplo disso seria se a Coca Cola financiasse pesquisas para tentar (falsamente) mostrar que açúcar não causa obesidade. Outro exemplo é o da Purdue Pharma, farmacêutica que publicou pesquisas enganosas convencendo as autoridades de que o consumo de opioides era seguro. Isso contribuiu para uma epidemia de opioides, viciando e tirando a vida de dezenas de milhares de pessoas. A razão por trás disso tudo é que, na maioria dos casos, pesquisas são influenciadas para benefícios dos financiadores[[137]](#footnote-138).

Apoiadores de pesquisas feitas pela comunidade podem utilizar curvas de ligação (*bonding curves*) para financiar estudos que irão informar a população de fatos científicos.

Molecule é um projeto focado na captação de recursos para pesquisas farmacológicas. Ao invés de gráficos complicados – como os que discutimos anteriormente, a Molecule usa duas linhas retas, uma de compra e outra de venda. A curva de compra está acima da curva de venda, e portanto com preços mais altos na compra do token. A curva de venda fica abaixo da curva de compra para desincentivar a venda. Esse mecanismo contribui para o alinhamento de incentivos e vai de acordo com a causa de financiar pesquisas públicas. Dependendo do objetivo da plataforma, a diferença entre as duas curvas pode variar drasticamente.

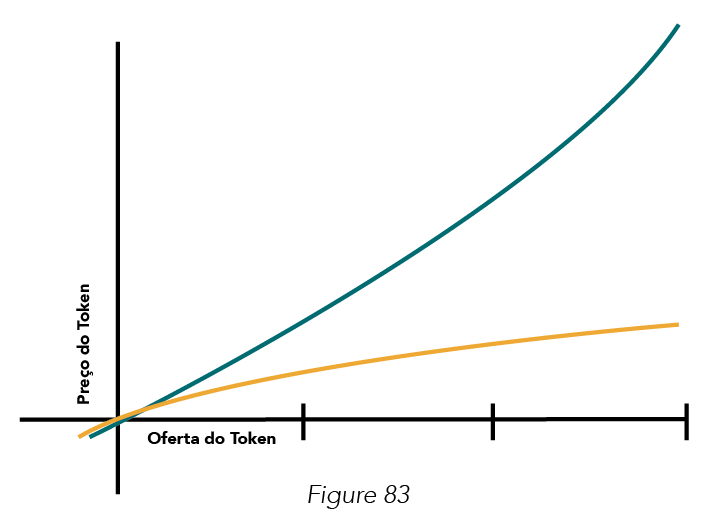


Figura 83

No caso da plataforma da Molecule, existem quatro fatores:

1. Curva de compra
2. Curva de venda
3. Propósito da captação de recursos
4. Limite da captação

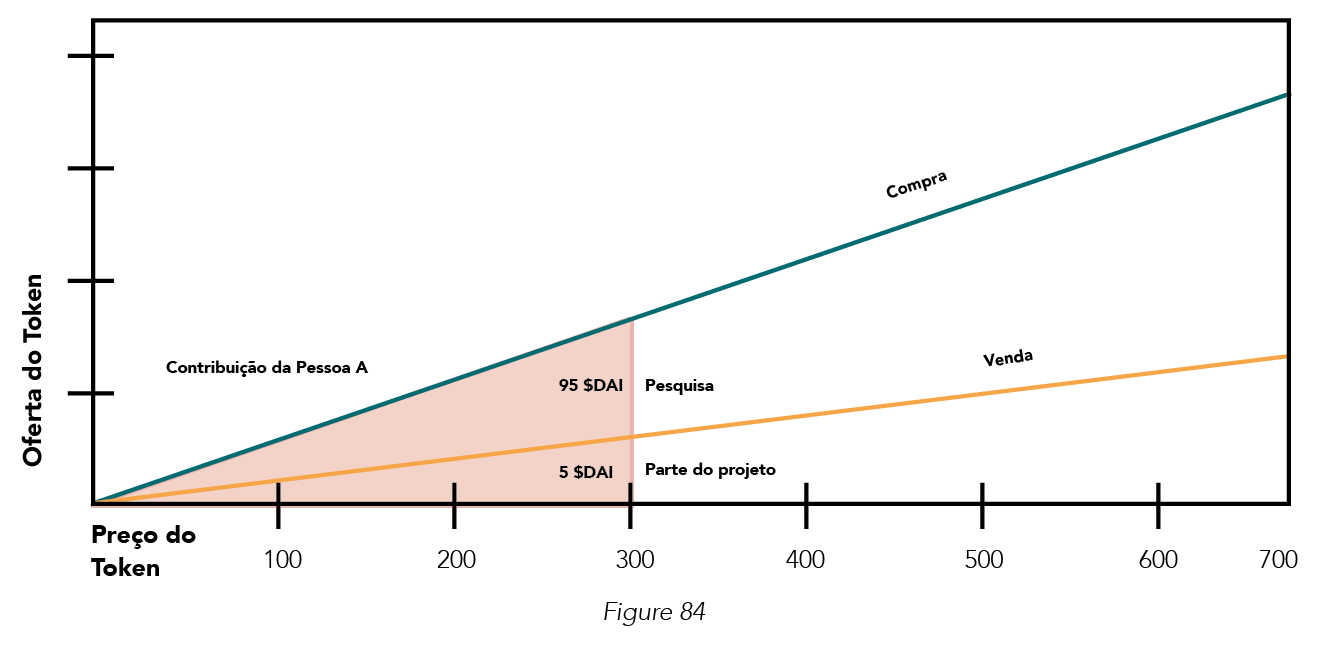


Figura 84

Fundos são usados na captação; sendo o montante definido pela diferença nas duas curvas.

Vamos imaginar que 100 $DAI são adicionados ao sistema. O contrato inteligente calcula a área abaixo das curvas e emite a quantidade referente a 100 $DAI. Nesse caso, 300 $TOKEN.

A curva de venda representa 5% do total – ou seja, 5% de $100 DAI é alocado para a curva de venda. No final, 95 $DAI é direcionado para apoio do projeto e 5 $DAI para a reserva.

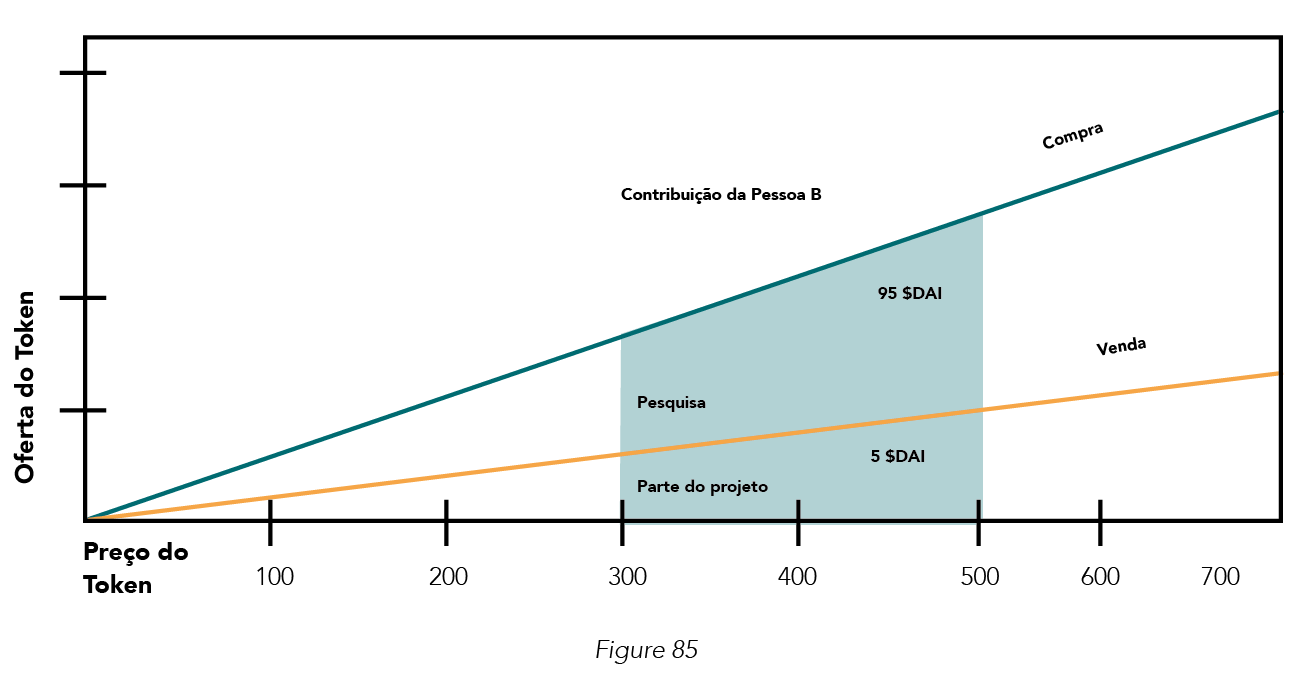


Figura 85

Na sequência, outra pessoa deseja fazer o mesmo. Ela deposita 100 $DAI. A área inferior da curva se mantém proporcional a 100 $DAI, porém a quantidade emitida é reduzida para 200 $TOKEN. Esse é um modelo justo, por incentivar os primeiros investidores pelo risco tomado – recebendo mais tokens como resultado.

Novamente, 5% dos 100 $DAI serão alocados para a reserva e 95 $DAI para o projeto de pesquisa.

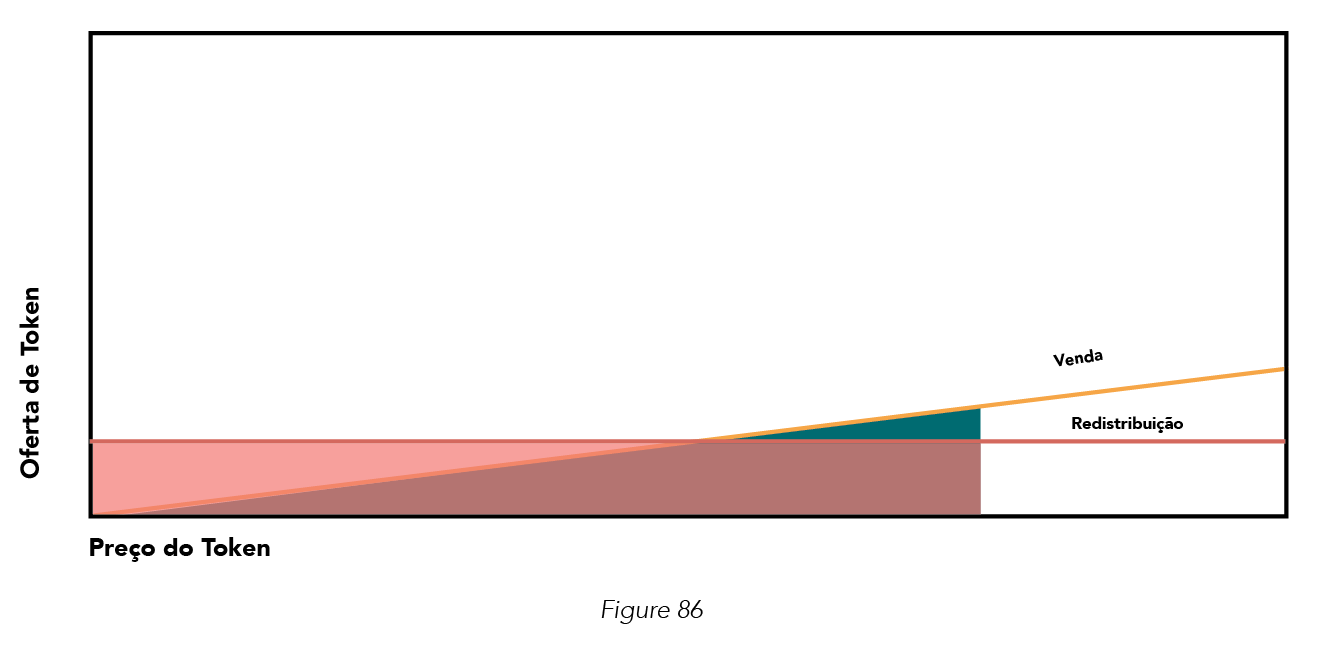


Figura 86

Quando a captação termina, o financiamento é encerrado. Todos os fundos restantes são distribuídos proporcionalmente para os investidores.

Caso você esteja considerando esse modelo, sugiro que também pense em formas de entregar valor para os financiadores – pelo menos nos casos em que a pesquisa é bem-sucedida. Isso cria incentivos de longo prazo para que os investidores continuem participando de outras captações. Estou fazendo algumas experimentações com um modelo nessa linha (vide Capítulo 25).

#### Resumo

Na plataforma Giveth, o capital que entra no sistema é alocado pelo contrato inteligente. Na Aragon, alocação é decidida pela DAO. Já na Molecule, duas curvas (funções matemáticas) independentes definem a alocação.

### Captação para Tokens Classificados como Securities

Tokens de utilidade podem ser usados para **contabilizar** captações de recursos ou outras atividades. Não representam rendimentos do protocolo ou especulações de valor futuro. Por outro lado, tokens do tipo *security* (tokens “garantidores”, similar às ações tradicionais, porém tokenizados) sim – representam ganhos e expectativas de valor futuro.

Tokens *security* representam ativos subjacentes, como instrumentos financeiros (ações de uma empresa). Esse ativo pode gerar receita, que por sua vez é definida pelas curvas de ligação (*bonding curves*).

Proprietários do token possuem o direito de participar de lucros futuros da empresa. Funciona da mesma maneira que participações societárias do mundo de TradFi. Um acionista com 10% de participação (*equity*) receberá a distribuição de lucros proporcional ao que possui.

A principal diferença entre tokens *security* e tokens de utilidade é a **área embaixo da curva.** No modelo de token de utilidade, essa área é definida pelo colateral existente no sistema. Já no token do tipo *security*, o próprio projeto recebe parte dos rendimentos e o restante é adicionado ao colateral.

Digamos que a Economics Design levante capital utilizando uma curva de ligação. Você pode investir na empresa, e receber tokens que representam parte da nossa receita em retorno. Os primeiros entrantes terão direito à mais tokens do que os seguintes, com base na curva.

Ao final do primeiro ano, a Economics Design fez $X de lucro. Dessa quantia, 20% serão adicionado à curva de ligação (*bonding curve*). O modelo não é o mesmo ao de *buybacks,* mas possui efeito similar de aumentar o preço do token (ação). Quando fundos são adicionados à reserva, cada token passa a valer mais.

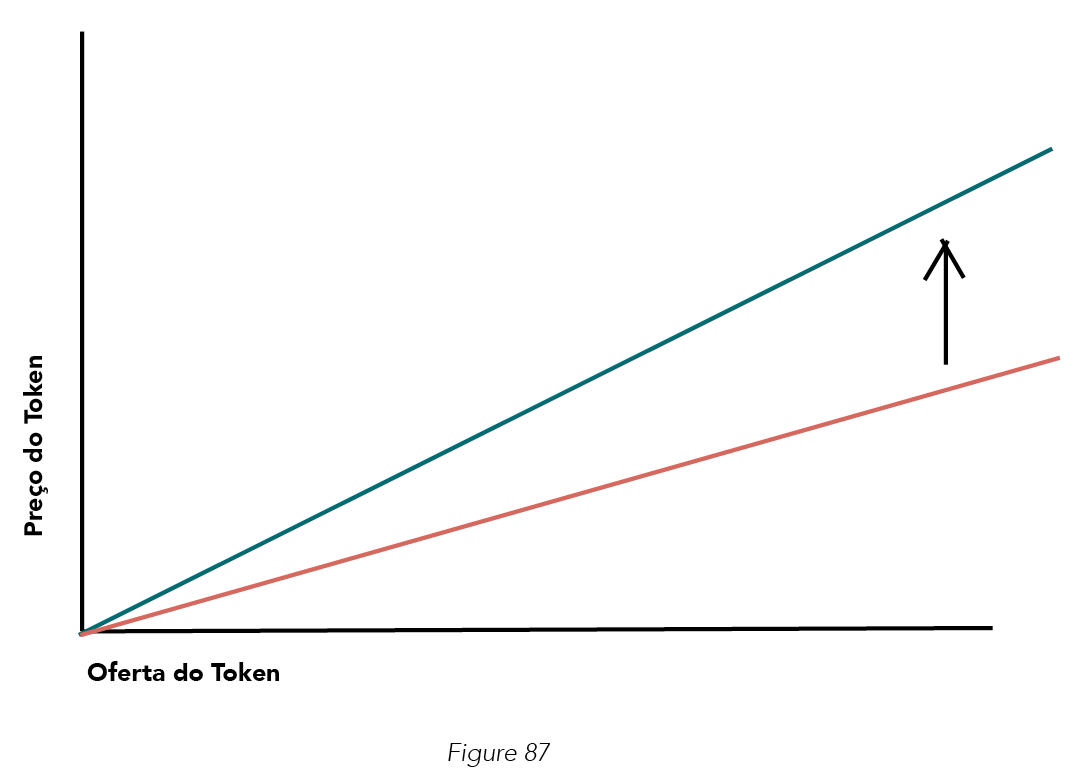


Figura 87

Nesse modelo, temos quatro formas de negociar os tokens:

1. Emitir novos da reserva ao adicionar colaterais ao sistema por meio de *staking*/trava de tokens.
2. Comprar colaterais a preço de mercado dos proprietários existentes.
3. Vender tokens a preço de mercado: transação OTC ou por meio de mercados secundários.
4. Redimir tokens diretamente da curva de ligação (*bonding curve*).

Independentemente de como são negociados, pelo fato de serem considerados “*securities*”, precisam cumprir com regulamentações locais. Consulte advogados especializados no assunto antes de tomar qualquer decisão.

## Seguros em Cripto

### Seguros de Contratos Inteligentes

Dado que a maioria das regras econômicas e mecanismos de incentivo estão definidas no código, contratos inteligentes podem ser um ponto de falha crítica. Por isso, seguros para proteger contra riscos técnicos internos podem ser cruciais.

Nexus Mutual é um dos protocolos provedores desse tipo de seguros. Na política monetária do $NXM, existem duas constantes e duas variáveis. **A** e **C** sãoas constantes. As duas variáveis são o CRM (capital mínimo requerido) e o capital total. Segue a seguinte fórmula:

**CRM—fator de curto prazo**

CRM é como reservas de bancos. Quando um usuário da Nexus Mutual coloca 100 $ETH na *pool* de capital (reserva), parte fica de fato na reserva e parte vai para outras atividades, como pagamentos aos assessores de risco.

**Capital total—fator de longo prazo**

Aumento do capital total significa maior adoção de DeFi e do mercado no geral. À medida que esses protocolos são adotados, temos também o aumento de capital correspondente.

CRM, portanto, pode funcionar como um indicador de curto prazo para entendermos o crescimento do protocolo da Nexus Mutual, enquanto capital total nos dá perspectivas de longo prazo. CRM é a reserva total disponível para pagamento imediato, enquanto capital total está ligado à adoção geral do protocolo (e de DeFi como um todo).

**Três elementos da curva de ligação**

1. Capital total.
2. CRM (importante pois determina a quantidade disponível para pagar assegurados conforme for necessário) .
3. Índice CRM (capital total dividido por CRM), relacionando as duas outras variáveis.

*Leia mais sobre o caso da Nexus Mutual no* *Parte I: Capítulo 7.*

### Seguros de *Impermanent Loss* (“Perdas Impermanentes”)

Um dos principais riscos de corretoras descentralizadas é o risco de incorrer *impermanente loss*, ou “perdas impermanentes” no português livre. Essas são perdas ocasionadas por atividades de negociações externas quando um investidor coloca seus tokens na *pool* de liquidez ao invés de mantê-los na carteira.

Bancor oferece seguros para *impermanente loss*, caso ocorra. Na versão Bancor V2.1[[138]](#footnote-139), existe a possibilidade da provisão de liquidez unilateral. Nesse caso, o protocolo da Bancor emite a quantidade referente em $BNT para suportar a proporção na *pool* de liquidez. Dessa forma, o protocolo também recebe taxas de transação, que podem ser usadas para pagar perdas incorridas.

Caso não haja fundos suficientes na *pool* de seguros, Bancor emite tokens $BNT adicionais para compensar a diferença.

## Derivativos em Cripto

DeFi está explodindo. E isso é apenas o começo. O pode de DeFi vem de duas coisas principais:

1. Governança descentralizada, e
2. Códigos programáveis e cálculos internos que podem ser tokenizados.

No início da indústria DeFi, tivemos muitos esquemas de “*pump and dump*” – tokens que aumentam de preço exponencialmente, logo antes de despencarem à valores próximos de zero. Porém, no estágio atual da indústria, representam valor econômico real (ex: tokens de rede) ou valor interno real (ex: tokens alavancados).

Nos capítulos anteriores, discutimos a matemática e engenharia econômica de muitos produtos financeiros básicos, como títulos (ou *bonds*). Esse tipo de instrumento é menos complicado de traduzir do mundo TradFi para o mundo DeFi. Nessa seção, vamos abordar derivativos, que iremos nos referir de forma geral como “ativos sintéticos” (ou *synth assets*). Esse tipo de ativo é um mais complexo, mas também oferecem novas formas de explorar ativos tokenizados.

Alertamos que são produtos complicados pois o entendimento completo é crucial antes de você fazer qualquer investimento. Por favor refira ao Apêndice A para uma comparação de termos financeiros entre TradFi e DeFi.

### Ativos Sintéticos

Ativos sintéticos são análogos aos derivativos existentes no mercado tradicional. São criados para referenciar o valor de um ativo subjacente. Por exemplo, contratos futuros de milho ou soja.

Assim como em finanças tradicionais, ativos sintéticos existem no mundo DeFi. Colaterais são submetidos ao protocolo e novos tokens nativos são emitidos. Ao invés de possuir $TSLA diretamente (ações da Tesla), você pode ter a versão sintética do ativo, parecido com um contrato de *swap* (derivativo do mercado tradicional que representa uma operação sobre a variação de preços do ativo, mas não o ativo de fato). A versão sintética das ações $TSLA terá retornos econômicos similares ao da ação “original”, mas não representará propriedade sobre ativos da empresa como ações originais.

**Como é feito?** Você coloca um ativo ($ABC) como colateral para emitir ativos sintéticos $TSLA. Esse ativo se move da mesma forma que $TSLA. A diferença é que você encontra contrapartes para negociar no mercado de ativos sintéticos, e o acionista da ação comum negocia no mercado tradicional.

O mecanismo de criação de ativos sintéticos é parecido com o que ocorre com a $DAI. Você coloca ativos como colateral ($ETH, $YFI, $USDC) para emitir $DAI na plataforma da MakerDAO (vide Capítulo 9 para mais detalhes). A diferença na criação de ativos sintéticos é que estamos usando **tokens de rede** para criar esses ativos, ao invés de $DAI. Esse mecanismo aborda problemas de liquidez e *slippage* que vemos em DEXs, enquanto mantém a proporção de colateral vista em ativos pareados.

#### Estudo de Caso: Synthetix

Vamos pegar como exemplo a Synthetix. A ideia desse estudo de caso é abordar como ativos sintéticos podem ser criados e qual é a matemática por trás.

Synthetix é um protocolo que emite ativos sintéticos. O único colateral aceito é o token nativo da plataforma $SNX, e os ativos sintéticos são negociados dentro da própria Synthetix. $SNX captura o valor da rede e das taxas de transação geradas. Atualmente, possui ativos sintéticos como $sUSD, $sEUR, $sBTC, $sETH, $sDEFI (index), $sGold e $sSilver.

#### Emissão de Ativos por Colateral

A Synthetix mantém um índice de "sobrecolateralização" de 750%. Em outras palavras, para emitir 1 $sUSD (equivalente a $1.00) são necessários $7.50 em tokens $SNX. Caso o valor do colateral caia para menos do que 750%, precisa-se adicionar mais tokens $SNX ou queimar ativos sintéticos.

Assim como nas CDPs (posições de dívida colateralizadas) da MakerDAO, uma taxa é cobrada na emissão de ativos sintéticos. Para resgatar o $SNX que foi colocado como colateral, uma taxa em $SNX é cobrada e queimada. Por outro lado, *holders* podem receber taxas ao travar seus tokens $SNX como colateral (*staking*).

#### *Pool* de Dívida da Synthetix

A *pool* de dívida é uma variável importante, pois determina o montante de capital que está suportando o sistema. Mensura a participação proporcional de investidores e eventuais mudanças com emissão/queima de tokens.

Essa é uma informação crucial, pois continuamente recalcula as posições de dívida de cada indivíduo.

Para calcular uma nova dívida devida, podemos usar a seguinte fórmula:

Participação do usuário na *pool* de dívida após adicionar novas dívidas:

Quando o usuário quita (repaga) sua dívida por meio da queima dos ativos sintéticos, sua quantia em $SNX travada como colateral é desbloqueada. Essa operação altera a quantidade de dívida no ecossistema.

Porcentagem de dívida do usuário após o pagamento:

O protocolo oferece um método inovador e versátil para a criação de ativos sintéticos, recompensando usuários por isso e alinhando incentivos para um bom funcionamento do ecossistema.

### Tokens Alavancados

Tokens alavancados (ou *leveraged tokens*) são apenas um exemplo do que a tokenização oferece de possibilidade. A chave está nas regras internas e no sistema de governança embutido nos códigos dos tokens.

Esse tipo de token pode, não só pelas forças de oferta e demanda presentes no mercado, ter valuation interno relativo ao ativo subjacente em questão – ativo a que o token se refere. Riscos como volatilidade, *beta slippage* (discrepâncias no monitoramento de preços), e movimentos de preço do ativo principal.

Tokens alavancados são ativos sintéticos negociáveis que representam posições alavancadas de um ativo. Ao invés de manualmente administrar o balanceamento ou estruturação, podemos executar uma posição de alavancagem por contratos inteligentes. Podem ser usados tanto para posições *long,* quanto *short*.

No geral, os dois tipos de alavancagem são:

* *Long*: acredita que os preços irão subir
* *Short*: acredita que os preços irão cair

A alavancagem comum para esses tipos de operação é de 3x, porém múltiplos maiores estão disponíveis em mercados de derivativos cripto (ex: 10-20x).

#### Benefícios das Posições Alavancadas Tokenizadas

Um dos principais benefícios de posições alavancadas tokenizadas é a redução nos riscos de liquidez, dados mecanismos de balanceamento automático e funcionalidades de retornos compostos oferecidos por esses tokens. Por mais que esses recursos existam no mercado tradicional, geralmente são administrados por corretores que encarecem a operação e criam novos riscos. A tokenização permite a automação eficiente dessas operações.

**Aumentar retornos**

Retornos (lucros) serão automaticamente reinvestidos no ativo subjacente. Caso uma posição alavancada seja lucrativa, o valor referente a 3x desse montante estará inclusa na posição. É composta.

**Reduzir riscos**

Quando perdas são realizadas, a posição é automaticamente liquidada para cobrir a quantia referente. Em outras palavras, caso um investidor tenha aberto uma posição de *short* e o preço do ativo subiu, parte será liquidada para cobrir esse prejuízo, como uma ordem de *stop-loss*[[139]](#footnote-140).

**Cálculo de Rebalanceamento**

Vamos ver um exemplo para entender como o balanceamento é calculado. O objetivo é que a exposição seja sempre 3x, referente à alavancagem dessa posição em questão.

* Posição: LONG ETH
* Valor: $25 mil
* Token Alavancado (LT): 100 ETH/token
* ETH preço de mercado: $400

Exposição =

requeridos para balancear a posição

Esse cálculo não inclui taxas da plataforma como taxa de transação, taxa de resgate, ou taxas de administração.

Tokens alavancados como o desse exemplo podem não ser a forma final de estruturas de derivativos. Combinando outros protocolos e mecanismos, podemos ter novas formas criativas de estruturar derivativos.

### Tokenização de Títulos de Cripto

Títulos de cripto, ou cripto *bonds*, são produtos de renda fixa criados dentro de protocolos de DeFi ou por meio de mercados futuros ou spot.

Conforme avançamos para derivativos financeiros mais complexos, o conceito se torna mais relacionado à engenharia financeira do que engenharia econômica (discutida do capítulo 1 ao 13 desse livro). Tokens e contratos inteligentes são apenas os meios usados para possibilitar esses produtos financeiros.

#### Valor de Cripto Bonds

Podemos interpretar *bonds* como instrumentos de renda fixa ou como veículo para financiamento colaborativo (*crowdsource*). Dependendo da função dessa *bond*, pode ser estruturado de formas bastante distintas.

No caso de financiamentos colaborativos, o modelo de curvas de ligação é o mesmo do utilizado em tokens do tipo *security*, discutidos no Capítulo 18.3.

Para instrumentos de renda fixa, *bonds* podem ser usadas para diferentes níveis de risco. Os produtos discutidos nos capítulos 16, 17, 18 e 19 são focados na otimização de retornos, buscando o melhor alpha possível.

Porém, além da geração de resultados, finanças também é sobre a redução de riscos. Isso é possível por meio da definição de perfis de risco em cripto ativos que funcionam como *bonds* e possuem calibragem automática.

#### Calibragem Automática

Tokens alavancados podem ser combinados com outras ferramentas para criar novos modelos de *bonds.*

Um dos problemas de *bonds* no mercado tradicional é a dificuldade para investidores constantemente calcularem sua exposição em termos reais, ao invés de nominais.

DeFi pode adicionar muito valor nesse sentido. Pode ser programado para criar produtos financeiros estruturados e tokenizados, geralmente com maior eficiência comparado ao TradFi. Imagine, por exemplo, a possibilidade de criar estratégias com nível de risco definido e utilizar contratos inteligentes para constantemente administrar sua exposição – isso evitaria muita dor de cabeça!

Declaração de Estratégia da Estrutura

Órgãos reguladores exigem diversas documentações e prestações de conta, criando ineficiências no mercado tradicional (ex: declaração oficial preliminar por um escrevente). O problema é que são estruturas e estratégias complexas para se criar, e difícil de medir potenciais riscos. Contratos inteligentes e descentralização podem trazer melhorias, principalmente no quesito de transparência.

Contratos inteligentes podem ser utilizados para criar *dashboards* com informações sobre a origem de cada rentabilidade e a diversificação de riscos nos diversos protocolos, por exemplo. Esse modelo reduz efeitos de assimetria de informação e ajuda pessoas e empresas a tomarem decisões melhores e mais bem-informadas.

#### Estrutura da Bond

Não há fórmula única para estruturação de *bonds*. Esse instrumento foca tanto nos retornos, quanto nos riscos – parâmetros versáteis e que podem ser customizados de diferentes formas. Vale lembrar que, na criação de *bonds,* precisamos sempre de uma contraparte para tomar o outro lado do risco.

Engenharia financeira, nesse caso, pode incentivar o indivíduo com exposição ao risco em uma negociação. Esses incentivos dependem não só da forma que o instrumento é estruturado, mas também quais são os riscos envolvidos.

#### Estudo de Caso: FlexUSD

Por mais que seja possível criar diversos produtos similares a *bonds* no ecossistema de DeFi, esse exemplo está presente no mercado de futuros, buscando atingir uma estrutura que funcione como instrumento de renda-fixa.

FlexUSD é uma stablecoin remunerada que recebe rendimentos sobre a diferença entre preços spot e preços de mercados derivativos. Isso é possível pois a CoinFlex, empresa por trás da FlexUSD, aplica liquidação física[[140]](#footnote-141) em sua corretora.

Combinando os conceitos de repo (ou acordo de recompra)[[141]](#footnote-142) e futuros perpétuos, FlexUSD possibilita que investidores recebam rendimentos de juros ao longo de um período de oito horas. Essas taxas de juros são geralmente mais atrativas do que a maioria dos protocolos de empréstimos P2P.

Repo está disponível no mercado tradicional, mas apenas oferecido a bancos. Tokenização permite que investidores de varejo também aproveitem uma fatia desse mercado, deixando que a tecnologia (bots, algoritmos, códigos) execute toda a mecânica financeira. Investidores de varejo não necessitam executar manualmente suas transações, mas ainda assim aproveitam os benefícios de retornos atrativos.

## Riscos Financeiros de DeFi

Existem muitos outros riscos além de riscos financeiros em DeFi, como a inexistência ou insuficiência de regulamentação, riscos de segurança do protocolo, contratos inteligentes não-auditados, falta de experts em economia de token para revisar a lógica matemática e de incentivos, e outras questões relacionadas ao estágio experimental atual de DeFi. Esses riscos, porém, estão além do escopo desse livro.

Nesse capítulo vamos focar apenas nos riscos financeiros.

### Custo de Oportunidade

Graças à tecnologia de contratos inteligentes, tornou-se mais fácil calcular o custo de oportunidade (em comparação ao mercado tradicional) por conta da maior transparência e disponibilidade de informação existente.

Com o avanço da indústria DeFi nos últimos anos, temos quatro setores de alocação de capital para considerarmos quando estamos pensando em investir:

1. Mercado TradFi (ex: ETFs, ações, ou títulos de renda fixa).
2. Mercado de fundos monetários que geram retornos baixos mas com pouco risco (em termos de volatilidade.
3. Investimento de longo prazo em tokens como $BTC ou $ETH. Não à toa, temos visto empresas tradicionais como Microstrategy e Tesla adicionando ativos como $BTC em seu portfólio.
4. Mercados DeFi (ex: compra e venda de tokens em corretoras descentralizadas (DEX) como Uniswap, ou provisão de liquidez com altos retornos) com ativos alternativos e de perfis de risco variados.

Com base na expectativa de retornos, e considerando a volatilidade das diferentes classes de ativos, é possível calcular o custo de oportunidade do capital.

### Reduções de Liquidez

Redução (ou perda) de liquidez é mais relevante em protocolos que possuem mecanismos de balanceamento de oferta circulante e preço, como o modelo algorítmico da Ampleforth. Ao invés de vincular o token às políticas internas dos Estados Unidos e manter uma paridade ao dólar (USD), Ampleforth altera a oferta monetária circulante com base na demanda global pela moeda.

O protocolo executa isso por meio de sistemas de governança automatizados embutidos no código, que internalizam a volatilidade de preço do mercado secundário.

Essa governança automatizada possui duas funções matemáticas:

1. Calcula a diferença de preços entre o “preço ideal” (ex: $1 USD) e a cotação atual no mercado secundário (ex: $1.15 USD).
2. Emite tokens adicionais para que o preço volte ao valor de $1 USD. Esse processo acontece ao longo de dez dias para evitar movimentos bruscos; mecanismo chamado de “*supply smoothing*”, ou nivelamento da oferta.

O token da Ampleforth, $AMPL, pode ser usado como colateral em muitos projetos de DeFi. $AMPL não está estritamente atrelado ao dólar – diferente da $DAI por exemplo, o que torna o token mais independente e útil no longo prazo, podendo até ser utilizado como uma nova moeda global sem controle de bancos centrais.

Porém, quando a oferta monetária é baseada na demanda pela moeda, temos impactos diretos na oferta e possibilidade de reduções (ou perdas) de liquidez.

O modelo da Ampleforth é diferente de outros, pois ao invés de definir o valuation por meio de preços, é definido pela proporção da rede detida por cada investidor. Quando preços aumentam, a quantidade total do token em circulação também aumenta, reduzindo o preço. Esse conceito é comumente conhecido como “*debasement*”, significando uma redução de valor/qualidade de um ativo.

Vamos para um exemplo. Imagine que um investidor possui 0.0000618% do valor total da rede (*market cap* total), representando o valor total de $1 USD ou 10,000 tokens. Caso preços aumentem para $1.15, a quantidade total de tokens desse investidor aumenta e o preço do token diminui (conceito de *debasement*). O investidor continua tendo a mesma participação anterior da rede. Quando isso acontece, não há perda de liquidez; pelo contrário, visto que temos mais tokens em circulação para facilitar as negociações, **aumentando** a liquidez. O mecanismo inflacionário do sistema não é problemático, pois flutua de acordo com a proporção original de cada investidor.

Porém, liquidez pode ser perdida quando o cenário contrário ocorre. Quando preços caem abaixo do preço determinado pela constante “invariante” (ex: $1 USD = 10,000 tokens no exemplo acima), tokens são queimados proporcionalmente e temos uma consequente redução na quantidade possuída por cada um. Com isso, investidores são forçados a negociarem em uma unidade de valor maior, dificultando transações pequenas. Essa redução de liquidez por meio da queima de grandes quantidades do token torna-se um risco relevante em estruturas financeiras mais complicadas.

### *Slippage* de Preço

Formadores de mercado automatizados (AMMs) oferecem dois tipos principais de riscos. Para recapitular: AMMs implementam mecanismos para possibilitar a negociação de tokens sem intervenção manual. Constantes invariantes formam o conceito matemático principal dos algoritmos que executam os processos de transação.

Por mais que o processamento de transações seja definido por matemática, ainda assim temos riscos criados por fatores não-matemáticos:

1. Risco interno na execução de transações, chamado de *slippage*.
2. Risco externo quando há baixo volume de transações, e quando preços fora do ecossistema mudam, chamado de perdas impermanentes (ou *impermanente loss*).

*Slippage* é a diferença entre o preço esperado antes da transação, e o preço real executado na transação. Por esse motivo, na Uniswap por exemplo, usuários são informados sobre o “mínimo a receber” e o impacto de preço antes da execução.

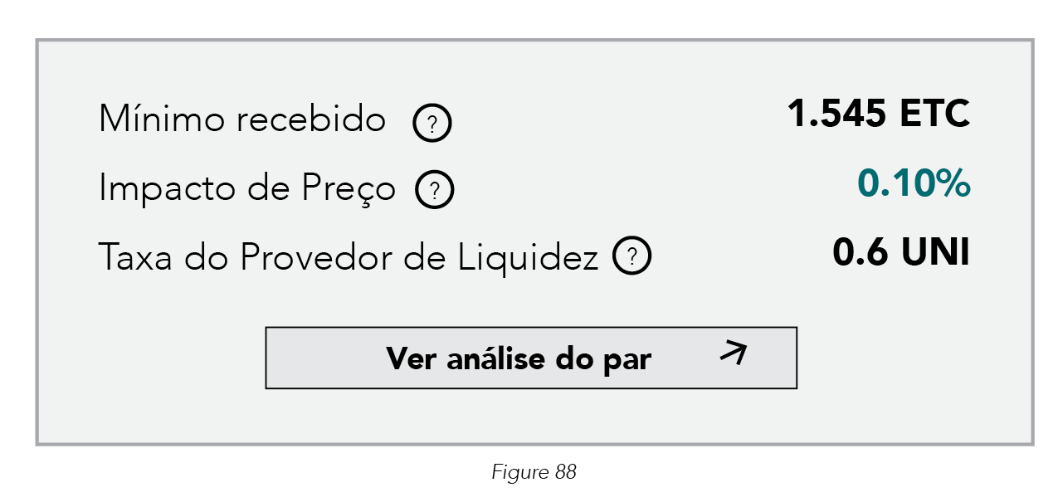


Figura 88

*Slippage* ocorre pelas negociações contínuas executadas pela DEX. O preço do Token A e do Token B são definidos pelo modelo matemático do AMM. Quanto maior for a transação com relação à *pool* de liquidez, maior será o efeito do *slippage*.

Em outras palavras, caso você queira negociar 9,000 tokens e existe um total de 10,000 tokens na *pool* de liquidez (90% da liquidez), o *slippage* de preço será muito alto, e tem grandes chances de receber um valor diferente do esperado.

Existem algumas formas de mitigar esse efeito:

1. Aumente incentivos para que mais pessoas decidam prover liquidez por meio de mecanismos de *staking*. Quanto maior (ou mais profunda) for a liquidez, menor o efeito potencial de *slippage*.
2. Utilize oráculos (vide 8.11.3) para ter acesso ao valor correto por meio de comparação de preços.
3. Pague taxas de transação (gás) mais altas para ter prioridade no processamento. Nota: esse aumento de custo com taxas de gás pode exceder o efeito do *slippage*.
4. Escolha *pools* de liquidez em que sua transação representa uma pequena porcentagem da liquidez. Por exemplo, traders que desejam trocar $COMP por $ETH, podem fazer por meio da Balancer, Uniswap ou Bancor. Escolha a *pool* com a maior liquidez disponível!

### Perdas Impermanentes, ou *Impermanent Loss*

O risco de perdas impermanentes é um tipo de custo de oportunidade, comparando o valor de tokens depositados em uma *pool* de liquidez com o valor dos mesmos tokens armazenados em uma carteira sob as forças normais de mercado.

Perdas impermanentes só são realizadas caso você retire o token da *pool* de liquidez. Para fazer um paralelo com o TradFi, o mercado tradicional, podemos pensar em ações ou quotas de fundos mútuos. O valor dessas ações aumenta ou diminui de acordo com a movimentação do mercado. Vamos imaginar que um investidor comprou ações da Tesla por $500. Por conta da volatilidade, o preço do ativo caiu para $400, significando uma perda potencial de $100. Perceba que chamamos de **perda potencial**, pois ainda não foi realizada. Caso o investidor não venda suas ações e o preço suba de volta para $500, essa perda é extinguida. Prejuízos são realizadas apenas quando há a liquidação dos ativos, ou venda, por um preço abaixo do preço de entrada.

**Quando Perdas Impermanentes podem acontecer?** Somente quando provedores de liquidez retiram seus fundos da *pool*, geralmente em DEXs como Uniswap, Bancor, Curve, e Balancer. O risco existe a qualquer momento a partir da alocação dos tokens na liquidez. Porém, é importante distinguir entre o **risco** de perdas impermanentes, e a **realização** de perdas impermanentes.

**Qual a origem dessa perda?** Parao propósito dessa discussão, vamos assumir que tokens podem ser armazenados em dois lugares: carteiras e *pools* de liquidez (vide 21.1). Perdas são causadas quando “caçadores” de arbitragem (*arbitrageurs*) identificam uma discrepância de preços de um dos tokens presentes na *pool* de liquidez com relação ao mercado externo. Para explorar essa arbitragem, compram tokens da *pool* à uma taxa de desconto, reduzindo a oferta interna desses tokens. Esse movimento causa um ajuste de preço no outro ativo, para preservar o valor total da liquidez. Quando um provedor de liquidez resgata seus tokens que estavam na *pool* de liquidez, mesmo que o valor recebido seja maior que o incialmente depositado, **eles realizam perdas em comparação ao valor que teriam se tivessem apenas mantido os tokens na carteira.**

Exemplo da Uniswap

Vamos assumir que a Uniswap não cobra taxas de transação, para simplificação. Uma determinada *pool* de liquidez possui dois tokens: $ETH e $USDT.

No momento da escrita original desse livro, 1 $ETH = 400 $USDT[[142]](#footnote-143). Esse valor se aplica apenas para os tokens presentes **dentro da *pool***.

Agora, imagine que fora dessa *pool* de liquidez temos corretoras com cotações de 1 $ETH por 420 $USDT (ex: Binance).

**Como investidores podem explorar essa oportunidade de arbitragem?** Lucros podem ser realizados quando percebem que 1 $ETH está mais barato na *pool* de liquidez do que em corretoras descentralizadas externas. Eles simplesmente compram 1 $ETH por 400 $USDT – ao invés de 420 $USDT na Binance – e imediatamente vendem esses ativos pela cotação superior na outra corretora, por 420 $USDT. Essa operação daria 20 $USDT de lucro sem nenhum tipo de risco – menos taxas de transação. Sim, essa é uma operação legal, e acontece muito no mercado tradicional (ex: Forex).

Esses “arbitragistas” expõem provedores de liquidez ao risco de perdas impermanentes quando compram e vendem o token (ex: $ETH) até que a conversão seja exatamente a mesma (1 $ETH = 420 $USDT).

Parece intuitivo pensar: “tudo bem, mas é o preço correto de qualquer forma, então como isso afeta o provedor de liquidez?” Durante esse processo de compra e venda, observe o que acontece na prática.

Estado inicial: Montante total na *pool* = 25 $ETH e 10,000 $USDT.

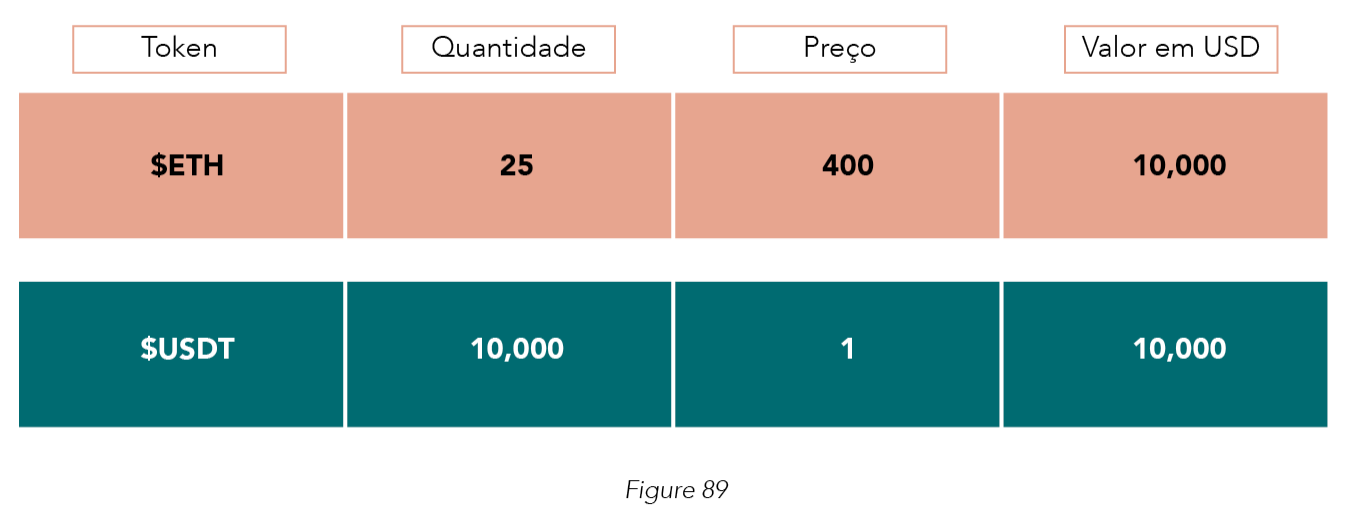


Figura 89

Produto constante = . Esse valor de produto constante precisa ser mantido o tempo todo na *pool* – o que é feito por meio de algoritmos do AMM.

Quando o preço sobe para 1 $ETH = 420 $USDT, “arbitragistas” começam a transacionar.

Esse é o resultado:

Assumindo que um provedor de liquidez possui 10% da *pool*, será intitulado a 2.43975 $ETH + 1,024.695 $USDT após a arbitragem ser realizada.

O valor desses ativos em $USDT é equivalente a .

Caso o provedor de liquidez tivesse mantido o montante inicial parado em sua carteira, teria o total de 2.5 $ETH + 1,000 $USDT.

Convertendo para $USDT, temos .

Valor da perda:

.

#### Calculando Perdas Impermanentes

Essa é a fórmula geral para calcular perdas impermanentes na Uniswap. Note que essa fórmula é relevante no caso da Uniswap, e não incluir qualquer tipo de taxa de transação.

Risco de *impermanent loss* acontece independente das taxas de transação recebidas pelo provedor de liquidez (LP). Uma das boas práticas que pode ser aplicada é calcular retornos de taxas de transação e subtrair o risco de perdas impermanentes.

Outra consideração importante é que estamos assumindo que apenas um lado da *pool* está mudando em cada momento. Por exemplo, $ETH muda de preço, mas $USDT se mantém exatamente o mesmo. Quando estamos lidando com tokens como $ETH e $COMP, que possuem correlação positiva, quando o preço de um se move, quase sempre também temos alterações no preço do outro. Liquidez em pares de tokens com correlação positiva pode reduzir o risco de perdas impermanentes.

## DAO, O Futuro da Governança

A filosofia da distribuição não é apenas sobre distribuir poder, mas também sobre a distribuição de responsabilidades. “Com grandes poderes vêm grandes responsabilidades”[[143]](#footnote-144). Essa distribuição pode ser atingida por meio da coordenação efetiva da governança.

Imagine uma entidade legislativa feita por, ao invés de políticos fazendo campanhas e pedindo votos, pessoas “normais” da sociedade. Além disso, a execução das leis feita por máquinas (códigos), ao invés de pessoas.

### Potenciais Melhorias para o Sistema Atual

*Você consegue identificar melhorias com o conceito acima?*

Políticos possuem incentivos para serem reeleitos no fim de seu mandato e nem sempre irão apoiar decisões de melhorias no longo prazo. Economistas keynesianos, por exemplo, acreditam que aumentar impostos e diminuir gastos do governo em tempos prósperos da economia pode ser benéfico para o país no longo prazo. Porém, políticos possuem contratos de curto prazo com o governo, e desejam ser reeleitos. Para ser direto, incentivos não estão bem alinhados.

Políticos possuem visão limitada do panorama global. As normas existentes nem sempre são as melhores para a maioria das pessoas e geralmente são focadas em objetivos de curto prazo, beneficiando pequenos grupos.

Na parte da execução das políticas implementadas, o sistema atual é ineficiente por conta de erros humanos, burocracia excessiva, problemas com a força de trabalho, e em muitos casos, corrupção.

Descentralização, tomada de decisão distribuída, e execução autônoma podem solucionar todos esses problemas.

DAOs podem fazer todas essas coisas, sendo governadas por pessoas (proprietários do token) e executadas por meio de contratos inteligentes.

O escopo desse livro discute DAOs no contexto de blockchain, mas elas também podem existir em outros tipos de ecossistemas, plataformas ou base de registros.

O conceito de DAO refere-se à uma nova forma de governança e tomada de decisão. Pode ser combinado com execução automatizada por contratos inteligentes.

### Definição básica: Contratos inteligentes

“Contratos inteligentes”, ou *smart contracts*, são contratos digitais que executam ações específicas de forma pré-definida e automatizada quando condições específicas são apresentadas. Caso os participantes de uma DAO decidam que $100 deve ser transferido da reserva para Chen, basta assinarem a decisão de cada um e o contrato inteligente irá identificar e executar a transferência dos fundos. Não há envolvimento ou necessidade de confiança em terceiros, supervisão manual, ou diferentes aprovações em etapas.

Contratos inteligentes são programas. Eles inserem regras (ex: enviar fundos após o acordo ser assinado) que podem executar (ex: enviar para Chen) quando condições específicas são cumpridas (ex: no mínimo três assinaturas).

A base tecnológica de contratos inteligentes dispensa a necessidade de contadores e processos manuais. De forma automatizada, pode provar que três pessoas de fato assinaram, verificar a existência e validade da conta do recipiente (ex: Chen), e executar a transferência de fundos.

Esse processo pode se tornar mais sofisticado e complexo conforme adicionamos mais lógicas de negócio no código, introduzimos variáveis no contrato inteligente como informações de dispositivos de IoT (“internet das coisas”), ou quando interligamos diversos contratos entre si.

Contratos inteligentes também podem facilitar o sistema de governança em DAOs. No momento que a DAO toma uma decisão e a registra oficialmente (Etapa 1), o contrato inteligente pode executar automaticamente a decisão (Etapa 2) caso esteja propriamente programada no código.

Decisões comuns executadas por contratos inteligentes incluem:

* Como alocar fundos
* Quais projetos apoiar
* O que fazer com os fundos arrecadados

A habilidade da DAO de tomar decisões em prol do sistema, com ou sem contratos inteligentes, é essencial para governança efetiva em ecossistemas descentralizados. Em ambientes centralizados, oficiais do governo, diretores de empresas, e conselhos de administração tomam essas decisões. Já em descentralizados, os membros **são** a diretoria, ou o conselho. Por esse motivo, processos de tomada de decisão efetivos (ex: por meio de contratos inteligentes) são parte importante dessa evolução de economias digitais.

### Exemplo: Como Alocar Fundos

Assim como conselhos de administração e legisladores, membros de DAOs submetem propostas para diferentes formas de alocação dos fundos. Vamos imaginar que fizeram uma proposta de alocar 5,000 $USDT para financiar um projeto que possibilita a interoperabilidade da Ethereum com outras blockchains.

A DAO irá analisar a proposta e votar. Nesse contexto, existem três coisas principais para considerarmos, mas não vamos entrar muito no detalhe.

1. Qual é a estrutura de votação?
2. Quem pode votar: voto delegado, qualquer usuário, indivíduos com quantia específica de tokens?
3. Qual é o poder de voto de cada um: um voto por carteira, poder de voto baseado na participação total de tokens possuída, votos por reputação?

Caso a DAO aprove a proposta (Etapa 1), o contrato inteligente incluso na proposta irá executar a decisão e enviar 5,000 $USDT da carteira da tesouraria para o projeto de interoperabilidade.

Essa é uma ideia bastante genérica de como uma DAO funciona. São organizações que coordenam o processo de tomada de decisão.

Agora que já introduzimos o conceito geral, vamos voltar ao ponto principal: O que são DAOs?

Imagine uma piscina comunitária – sim, piscina de nadar mesmo. Todos os integrantes da vizinhança trazem um balde de água para encher a piscina. Dado que todo mundo contribuiu, todos possuem direito à uma parte da piscina.

Em um dia de muito sol, as árvores que provém sombra à piscina começam a pegar fogo. Todos precisam votar se devem utilizar a água da piscina para extinguir o fogo, e poderem aproveitar sem preocupações de alastrar para suas casas.

Da mesma maneira, membros de uma DAO juntam seus fundos por meio da compra de tokens. Esses tokens concedem o direito de votar em decisões, como em questões da operação ou como os fundos serão utilizados. Quando as atividades dão retorno positivo, o valor é adicionado às reservas da organização. Os membros, proprietários de parte da DAO, recebem parte desses retornos.

Vale lembrar que até mesmo DAOs não são necessariamente organizações totalmente descentralizadas e autônomas. Centralização e descentralização não fazem parte de uma dicotomia, mas sim de um espectro. Cada ecossistema tem suas regras de governança e diferentes níveis de descentralização, conforme seja apropriado.

DAOs geralmente são arquitetadas de forma descentralizada, com participantes muitas vezes localizados em diferentes países do mundo. A lógica de execução, porém, é centralizada nos contratos inteligentes.

### Economia de DAOs

Com melhor entendimento sobre o conceito de DAO, vamos abordar sua parte econômica.

Economia vai além de oferta e demanda. DAOs dependem especificamente de três conceitos econômicos:

* Economia da confiança
* Economia da coordenação
* Economia da alocação

#### Economia da Confiança

Pessoas precisam confiar para transacionar e negociar em uma economia. Além disso, precisam confiar nas decisões tomadas dentro do ecossistema pelas diversas partes envolvidas (ex: DAO, programador, fundadores, membros, etc).

Assim como no mundo físico, “residentes” do mundo digital precisam de confiança entre si, ou de interações de confiança inerente (chamadas de *trustless*).

Voltando ao exemplo da piscina comunitária, temos um ecossistema em que qualquer um pode contribuir com um balde de água e aproveitar os benefícios. Caso queiram vender sua participação, podem vender para algum vizinho que ainda não faz parte.

O problema é que é necessário um nível altíssimo de confiança para manter a contabilidade e o controle de acesso a esse sistema. Como proceder se alguém contaminar a água? Ou simplesmente não manterem? Existem muitas possibilidades de negligência e dolo.

Com blockchain, ao invés de confiar em alguém para controlar a reserva de fundos/ativos, contratos inteligentes fazem isso de forma automática. Esse sistema possibilita a DAO de focar em tomar as melhores decisões, e deixando a execução ser feita por máquinas.

Confiamos no código ao invés de pessoas. Podemos codificar a confiança em regras programáveis. Dessa forma, interações entre pessoas não dependem da confiança entre si, somente da confiança no próprio sistema.

PieDAO, por exemplo, é uma DAO que administra fundos de índice de criptomoedas. As decisões tomadas pela DAO são de votações para definir ou criar parâmetros para os fundos em questão. Esses fundos são então criados por meio de contratos inteligentes. Não há a necessidade de confiar em um terceiro para administrar seu dinheiro exatamente como você espera, visto que temos máquinas executando de forma automática e transparente.

#### Economia da Coordenação

Um dos pilares de uma economia é a coordenação dos participantes existentes. Quem passa o conhecimento para novas gerações? Quem cultiva alimentos para a população consumir? Quem é responsável por cuidar dos doentes e enfermos? Quem cria normas e regras para melhorar a economia?

DAOs coordenam e distribuem essas decisões ao invés de poucas pessoas serem encarregadas de fazê-lo.

Coordenação é difícil. Mesmo se conseguirmos coordenar as atividades, como podemos garantir que as pessoas irão cooperar entre si? Humanos não cooperam naturalmente, a não ser que existam incentivos efetivos implementados. Considerando todo o resto constante, cada tomador de decisão segue seus próprios objetivos. O sistema de interações independentes de confiança (*trustless*) cria incentivos para que esses agentes desejem coordenar suas decisões. Sem essa comunicação transparente, há grandes chances das votações resultarem em decisões indesejadas.

MolochDAO, por exemplo, é uma DAO que provém subsídios para projetos que focam na infraestrutura pública da Ethereum. A DAO toma decisões por meio de votações sobre a aceitação ou rejeição de novos membros, assim como sobre a emissão de novas ações para esses novos integrantes. Cada ação representa um voto.

Esse mecanismo facilita a entrada e saída de membros. Caso você não queira mais participar da DAO, pode destruir suas ações (queimar), resgatar seu capital, e sair. Ou seja, o mecanismo é efetivo em termos de coordenação, mantendo apenas os participantes alinhados com o objetivo do projeto.

#### Economia da Alocação

Alocação pode ser exemplificada pela forma que governos cobram impostos e decidem em como gastar (ex: programas de educação, manutenção de rodovias, projetos de iluminação, investimento em saúde pública etc.).

Governança é exatamente sobre isso em qualquer ecossistema. O exemplo equivalente no contexto de blockchain é como estruturar taxas de transação e avaliar propostas para uso de fundos da comunidade. Nesse caso, decisões são tomadas pela DAO, e não por um governo central.

Kyber, por exemplo, é um protocolo de liquidez *on-chain*. A KyberDAO governa o ecossistema Kyber, onde membros votam sobre como taxas de rede acumuladas são alocadas (ex: distribuição de rendimentos, queima, ou recompensa para determinados participantes do sistema).

### Outros Tipos de DAO

Essa lista está sempre aumentando, conforme projetos experimentam novos tipos de estruturação dessas organizações descentralizadas. No geral, podem ser divididas nas seguintes categorias: gestão de ativos (*asset management*), gestão de protocolo, e financiamento de projetos.

**Gestão de Ativos: PieDAO**

PieDAO decide sobre a forma que os ativos da comunidade são administrados. Máquinas são boas na execução de tarefas, mas decisões ainda são dependentes de humanos – nesse caso, membros da PieDAO.

PieDAO administra e monitora os fundos de índice tokenizados no protocolo da Balancer. Criam diferentes *pools* de ativos e votam sobre os parâmetros de cada uma dessas *pools*. É como se fosse um ETF descentralizado. A DAO age como a camada social que administra a *pool* e equilibra os ativos existentes. Proprietários do token têm direito às taxas geradas.

**Gestão de Protocolo: MakerDAO & KyberDAO**

DAOs também podem ser usadas na administração em larga escala de protocolos ou ecossistemas. Por mais que esses ecossistemas descentralizados não tenham uma governança central, decisões ainda precisam ser tomadas de alguma maneira.

MakerDAO e KyberDAO provém administração do protocolo em seus ecossistemas. Proprietários do token podem participar das decisões de governança e influenciar em mudanças do protocolo. Esse é um passo importante para a distribuição de poder aos usuários do ecossistema.

**Financiamento de Projetos: MolochDAO, LAOs, Dash, Aragon**

Por último, DAOs podem decidir sobre a alocação de fundos. Isso é feito pela coordenação de recursos para distribuir subsídios – as famosas *grants*. Participantes da juntam seus recursos e os alocam no desenvolvimento do fundo. Esses participantes têm direito aos retornos obtidos por esses projetos. Vale notar que esse mecanismo pode ser complicado em termos regulatórios e legais. MolochDAO e Dash alocam fundos para decisões de investimento e subsídios.

Existem também as chamadas LAOs – Organizações Autônomas de Responsabilidade Limitada, criadas para conceder status legal para as DAOs. LAOs funcionam da mesma forma que DAOs e alocam fundos para projetos de investimento. Dado que são entidades legais tradicionais, membros de LAOs estão protegidos de eventuais passivos, como se fosse uma “Ltda.” (sociedade de responsabilidade limitada).

Polkastarter[[144]](#footnote-145) é similar, com a ressalva de que não utiliza fundos de investidores individuais na alocação, mas fundos da rede em si. Usuários precisam pagar para submeter propostas, e votantes precisam travar seus fundos em *stake* para participar da votação.

## Economia de Yield Farming

*Yield farming* – expressão sem uma expressão específica em português, mas que significa algo como cultivo de rendimentos – é parte do mecanismo de distribuição de tokens e aquisição de usuários. Na prática, aumenta a quantidade de tokens existentes e distribui para usuários do protocolo. Quando usuários executam uma transação no protocolo, são recompensados com tokens nativos, independente do retorno na transação específica. Muitos projetos usam isso como uma das principais atrações de novos usuários, oferecendo até 100% de APY (retorno médio anual). Esse sistema, porém, oferece vários riscos.

Mineração de liquidez e *yield farming* são similares. *Yield farming* é um termo geral, enquanto mineração de liquidez é mais específico – referente à quando *stakers* recebem novos tokens pela adição de liquidez em sistemas como DEXs (corretores descentralizadas) e protocolos de empréstimo.

### Projetos Utilizando Yield Farming[[145]](#footnote-146)

* **Synthetix**: Emite $SNX para provedores de liquidez.
* **Curve Finance**: Emite tokens nativos como $SNX, $REN, $BAL, e $CRV para provedores de liquidez.
* **Compound**: Total de ativos no mercado da Compound superou o da Maker, o principal aplicativo de DeFi até então. É o mercado primário do mercado monetário descentralizado. Tokens $COMP são emitidos para usuários com base no volume transacionado.
* **Balancer**: Tokens $BAL são emitidos semanalmente para usuários com base no volume transacionado. Após a distribuição ser implementada, volume passou de $2 milhões para mais de $5 milhões em meados de 2020.

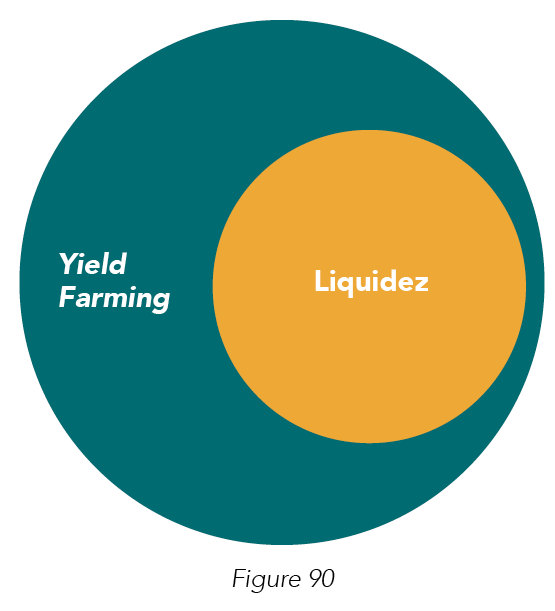


Figura 90

### O Bom, Ruim, e Pior

Tokens nativos emitidos por meio de *yield farming* – distribuição de tokens conforme uso do protocolo – são geralmente tokens de utilidade, mais especificamente tokens de governança. Porém, o mecanismo de *yield farming* não é perfeito, possuindo prós e contras na utilização do mesmo como estratégia de aquisição de usuários e volume de transação.

#### O Bom

**Realmente funciona.** *Yield farming* atua como forte incentivo para **provisão de liquidez**. Corretoras utilizam bastante esse recurso com seus tokens nativos para incentivar formadores de mercado. Agrega valor ao usuário por meio de recompensas extra no token nativo. Cria valor para a plataforma como todo pois **atrai novos usuários** para o ecossistema.

Esse modelo de *yield farming* é relativamente maduros. Existem muitos protocolos funcionais, com tempo de mercado e muitos usuários utilizando esse incentivo.

#### O Ruim

*Yield farming* pode ser apenas um **incentivo de curto prazo e insustentável no longo prazo.** O que acontece quando o alto volume especulativo (hype) terminar? Ou quando taxas de transação estiverem caras demais, e não faça sentido econômico negociar? Ou quando todos os tokens tiverem sido distribuídos (limite de oferta circulante atingido)?

Até o momento, parece que o mecanismo de *yield farming* é um **jogo de soma zero**. Pode ser que isso mude no futuro, aumentando o tamanho total da fatia de cada usuário do protocolo. Por hora, não seja o último a ficar investido em um protocolo, pois o risco de esquemas de *pump and dump* são altíssimos nesse modelo. Caso você não tenha conhecimento técnico suficiente sobre *yield farming* ou sobre o protocolo em si, provavelmente estará agregando mais valor ao ecossistema do que colhendo. Assim como em todo tipo de investimento, em especial os mais especulativos, você só deveria participar se realmente entende o que está fazendo.

**Mercado de capitais reduz imediatamente após o incentivo cessar.** Uniswap, por exemplo, introduziu a mineração de liquidez e distribuiu tokens nativos $UNI. Em 17 de novembro de 2020, Uniswap encerrou a mineração de liquidez. Em 24 horas, capital total do protocolo caiu de $3.3 bilhões para $1.8 bilhões.

#### O Pior

Existem outros riscos ocultos. Quando o volume de transação na Ethereum está alto, como durante o ciclo de alta de 2021, o valor das taxas de gás aumenta exponencialmente. Fique atento com os custos de **taxas de gás, *slippage*, volatilidade, e risco de perdas impermanentes**.

**Transações alavancadas** podem muitas vezes assegurar retornos positivos exponenciais, mas movimentos negativos também serão impactados de forma proporcional (exponencial negativo). Conforme submetem toda sua liquidez para aplicativos de DeFi, investidores podem esgotar seus caixas e frear a entrada de capital no ecossistema.

Para combater esse aumento nas taxas de transação, a Ethereum **aumentou o tamanho de seus blocos**. Isso permite que validadores tenham maiores retornos no curto prazo, mas cria um **risco no longo prazo de potenciais ataques à rede**.

### Economia de Yield Farming

Vamos usar o Framework Economics Design como base para analisar a economia de mecanismos de *yield farming*.

* **Design de token:** Mecanismo autossustentável. Incentivos do token criam liquidez e iniciam um ciclo que se retroalimenta (*feedback loop*).
* **Valuation:** *Yield farming* estimula efeitos de rede mesmo sem criar valor econômico real. Para que projetos e protocolos sejam bem-sucedidos, desenvolvedores e usuários precisam continuar utilizando a plataforma por um bom tempo, e não apenas durante o período em que especuladores entram na comunidade, extraem valor, e retiram-se. No curto prazo, temos também efeitos de impulsionamento nos preços do token.
* **Oferta circulante do token:** Gera um aumento na oferta circulante, chamado também de inflação de oferta. Além disso, essa nova oferta é geralmente distribuída para os usuários com grandes quantias do token. Ao invés de precisarem pagar por tokens, recebem “de graça” direto da plataforma.
* **Retorno sobre tokens:** Esses tokens não são de fato “de graça”. Investidores iniciais investiram seu capital no projeto e receberam tokens. Estão satisfeitos quando o preço do ativo sobe, e muitas vezes decidem liquidar suas posições e garantir seus retornos (como o chamado “IPO pop”[[146]](#footnote-147)). Porém, a não ser que você tenha um plano estratégico para usar os tokens e tirar seu próprio retorno, você provavelmente está apenas servindo de liquidez para esses outros investidores.
* **Atividades de transação:** Devedores estão dispostos a tomar mais empréstimos pois a distribuição de tokens nativos basicamente subsidia os juros cobrados. O aumento no volume de transações resulta em taxas mais altas e maiores retornos para os credores (financiadores).

### Valor do Yield Farming

De forma geral, *yield farming* é um mecanismo efetivo para dar o “solavanco inicial” (*bootstrap*) em comunidades descentralizadas.

Tokens nativos emitidos geralmente possuem funções de governança. Portanto, o poder de governança é distribuído para os usuários ao invés de limitar decisões ao time fundador ou fundos de investimento.

Dependendo do protocolo e de sua função financeira (corretora vs. crédito), a emissão de tokens nativos pode servir propósitos diferentes.

**Corretoras**

Corretoras oferecem vários tipos de risco, incluindo o risco de perdas impermanentes (*impermanent loss*). Essas corretores emitem tokens nativos por meio de *yield farming* para atrair provedores de liquidez, mesmo com os riscos mencionados.

**Crédito – Empréstimos e Financiamentos**

Tokens nativos atraem capital para a plataforma para que possam ser emprestados como dívida, atividade principal da plataforma e responsável pela geração de rendimentos.

Tokens nativos emitidos por meio de *yield farming*, nesse contexto, torna-se uma classe de ativo interessante. Oferecem ações de participação (com direito a voto) e dividendos (fluxo de caixa da utilização do protocolo, rendimentos). Visto que esses “dividendos” são gerados por meio de tokens diferentes ao da transação de fato, não pode ser considerado como retorno sobre juros.

Emprestar $USDC na Compound, por exemplo, oferece ao credor retornos sobre juros em $USDC e tokens nativos $COMP como dividendos.

### Resumo

*Yield farming* tem o seu valor. Pode ser um ótimo mecanismo para tração inicial de projetos. Por outro lado, pode oferecer riscos ao ecossistema quando esses incentivos e o interesse geral da comunidade diminuem. Esse efeito pode ser mitigado por meio da criação de mecanismos de retenção do usuário durante o período de *yield farming*, convencendo a comunidade de que vale a pena continuar transacionando ou utilizando a plataforma.

## [Estudo de Caso] Binance

Economia de tokens considera aspectos de todo o ecossistema em que o ativo existe. Vai além do próprio token em si. Assim como na economia tradicional, focamos em vários outros fatores além do dinheiro.

Vamos nos aprofundar em um estudo de caso da Binance e analisar a empresa por meio do Framework Economics Design.

### Design de Mercado

Design de mercado é sobre o ambiente em que os tokens existem e operam. O conceito segue muitos dos princípios tradicionais. Assim como calcular a função de otimização em cálculo requer conhecimento sobre **o que** precisamos otimizar, design de mercado requer profundo entendimento sobre os **objetivos primários** do token, para que o mercado seja estruturado de forma apropriada.

#### Objetivos

O principal objetivo do token $BNB (pelo menos atualmente, mas pode mudar no futuro), é ser um token de utilidade para taxas de transação descontadas.

Objetivos secundários incluem:

* Funcionar como reserva de valor, dadas características deflacionárias
* Transacionar com outros tokens como um meio de pagamento/troca
* Comprar produtos/serviços
* Doar para instituições de caridade

De fato, existem mais de 20 casos de uso para o token $BNB, o que nos leva para o primeiro fator do design de mercado – Robustez.

#### Robustez (ou Densidade)

Robustez é um pré-requisito para atingir efeitos de rede. Assim como toda e qualquer corretora, a Binance é uma plataforma bilateral, e precisa de densidade em abos os lados da base de usuários. No geral, temos os formadores de mercado e tomadores de mercado (usuários). Na Binance, a corretora possui formadores e tomadores de mercado que utilizam $BNB. Além disso, $BNB tem sua própria blockchain em que protocolos e usuários precisam usar $BNB para pagar pela validação de transações na rede.

**Modelo de Negócios**

Binance, como a principal corretora do mercado atualmente, pode explorar sua rede de conexões para fechar parcerias. Ao invés de engajar com intermediários, pode interagir diretamente para que potenciais parceiros aceitem $BNB como pagamento em sua rede.

Pode funcionar para atividades como compra de viagens, pagamento de contas, rendimento de juros por meio de *staking*, etc.

Como mencionado, esses são exemplos de objetivos secundários. O objetivo primário continua sendo a utilização do token para descontos sobre taxas de transação na Binance. Vamos discutir design de token na próxima seção.

**Usuários**

Binance lançou o token $BNB por meio de um ICO (*initial coin offering*, ou venda inicial de tokens/coins). Essa foi a única distribuição de tokens, e o resto é mantido em reserva. Para atrair usuários e aumentar a retenção, estruturam o $BNB de forma deflacionária, potencialmente aumentando seu valor ao longo do tempo, e incentivando investidores a segurarem seus tokens.

Outros casos de usos são focados em atrair tipos de usuários diferentes, além dos traders normais. Binance, por exemplo, possui sua própria incubadora de projetos e *launch pad* (plataforma de lançamento de tokens). Nesses ambientes, todas as transações são feitas com $BNB.

O token em si é negociado principalmente (ou exclusivamente, em alguns casos) na Binance, gerando descobrimento de preços e valor monetário para o token. As características deflacionárias e o mecanismo de descobrimento de preços incentiva investidores a manterem suas posições de $BNB intactas.

### Estrutura do Token

Estrutura do token faz parte do design do token. Vamos abordar as políticas monetárias do token e valuation.

#### Oferta

A quantidade máxima de tokens $BNB é de 200 milhões de unidades. Desse total, 100 milhões foram distribuídos ao público por meio do ICO, 80 milhões para o time, e 20 milhões para investidores.

##### Mudanças na Oferta Circulante

Diferente do bitcoin, não há aumento gradual da quantidade de tokens em circulação. O total de 200 milhões de tokens foi distribuído e pronto – não serão emitidos novos tokens conforme mais ativos são adicionados e transacionados no protocolo.

A quantidade de tokens $BNB diminui ao longo do tempo. A cada trimestre, Binance queima uma certa quantia de $BNB – e continuará fazendo até que 100 milhões sejam queimados, ou seja, 50% da oferta total.

“Queimar” um token é quando destruímos o ativo e o retiramos de circulação para sempre. Pode ser feito, por exemplo, enviando os tokens para um endereço “inativo” (endereço que ninguém possui a chave privada ou qualquer tipo de acesso). Esses tokens são permanentemente retirados de circulação.

Funciona como se fosse um *buyback* de ações no mercado tradicional, onde a empresa recompra suas ações do mercado e as retira de circulação, consequentemente aumentando o valor das ações restantes. Da mesma maneira, Binance queima parte de seus lucros para aumentar o valor dos tokens remanescentes no mercado.

Lembre-se que o principal objetivo da utilização de $BNB é para reduzir as taxas de transação. Binance recebe seus lucros em forma de $BNB.

#### Política Monetária: Estrutura Hiper Deflacionária

$BNB é deflacionário – a quantidade de tokens diminui, mas o valor de cada token aumenta ao longo do tempo. Isso é feito por meio da queima de parte da oferta circulante existente.

##### Queima de $BNB

Inicialmente, a queima era feita de forma proporcional aos lucros gerados pela corretora. Por exemplo, 50% dos tokens $BNB usados para pagar taxas de transação eram queimados a cada trimestre. Atualmente, porém, conforme os casos de uso do token expandiram, a quantidade queimada passou a ser sobre métricas de volume divulgados pela própria Binance. Essa mudança causou certa controvérsia na comunidade, visto que esses valores não são totalmente transparentes.

Vamos quebrar essa questão nos dois princípios fundamentais do design econômico: 1) oferta e demanda, e 2) economia comportamental.

##### Explicação sobre oferta e demanda

Conforme seu objetivo principal, $BNB é usado para facilitar transações e reduzir taxas de processamento. Quanto mais casos de uso temos para o token, maior a demanda pelo token e potencial redução de taxas de transação.

À medida que mais usuários utilizam $BNB para ter acesso à taxas mais baixas, mais tokens são queimados, e mais valor é direcionado para o ativo. Assumindo o mesmo valor de mercado da empresa, em cenários normais de mercado, quando diminuímos a quantidade total de tokens, aumentamos o valor de cada token, já que representam o mesmo montante total anterior. Cada token representa uma participação maior sobre o mesmo valor de mercado.

Com cada queima, o valor do token aumenta; não necessariamente em termos de valor monetário, mas pelo menos de valor percebido pelo usuário.

##### Explicação sobre economia comportamental

Para as pessoas que acreditam na tese de valorização no longo prazo, elas tendem a segurar seus $BNB e usar como pagamento outros tokens antes, como $USDT por exemplo. Esses outros ativos são inflacionários e investidores convencidos do longo prazo tendem a comprar e segurar suas posições de $BNB.

Existem também aqueles que veem valor no curto prazo. Pode ser um trader executando uma transação relevante, e o desconto recebido em taxas de transação ao pagar em $BNB excede o valor de segurar esses tokens, por exemplo. Nesse caso, provavelmente irão preferir utilizar os tokens imediatamente.

Em termos de comportamentos coletivos de grupo, por outro lado, quando a maioria das pessoas está gastando seus $BNB para pagar taxas de transação, pode sinalizar uma redução na confiança sobre a valorização do token. Mesmo que a estrutura de mecanismos seja deflacionária, o modelo comportamental sugere o contrário.

Essa transparência sobre a queima de $BNB é uma “faca de dois gumes”. Por um lado, podemos observar e monitorar a quantidade de tokens queimados. Por outro, quando temos períodos de altas taxas de queima, significa que o valor percebido de investidores para o longo prazo pode estar comprometido. Caso o volume em $BNB esteja baixo, pode também sugerir menos valor no uso do token, desincentivando a compra na esperança de apreciação de preços.

Considerando que existe um número limitado de casos de uso para o $BNB (31, até o momento de escrita desse livro), faz sentido que a Binance controle a dimensão das queimas trimestrais por meio de métricas internas, ao invés de apenas volume transacionado. $BNB pode gerar mais valor em outros mercados, além de usar para taxas de transação.

#### Situação Atual

Até o quarto trimestre de 2020, na 13a [[147]](#footnote-148) queima de $BNB, já tinham sido queimados mais de 26 milhões de tokens. Com a variação de preços do token, o valor queimado também muda em cada período. Até dezembro de 2020, o montante queimado totalizava $970,580,000 USD.

#### Valuation

O preço do $BNB tem flutuado ao longo do tempo, mas se manteve como uma das principais *altcoins* do mercado. Com base em pesquisas no momento de escrita do livro sobre métricas de preço-lucro (conhecido como P/E), token $BNB parecia subvalorizado.

Analistas usam o índice P/E para determinar o **valor relativo** de ações de empresas em comparação à suas competidoras ou aos dados históricos da mesma. Pode ser uma métrica útil na avaliação de tokens também. Lembre-se, porém, que $BNB não é de fato uma ação ou participação da empresa.

Não há nada de errado com o índice P/E, mas há outros fatores a se considerar quando estamos avaliando um token. Assim como muitos outros tokens, $BNB funciona de forma similar às famosas milhas aéreas, as quais companhias aéreas não possuem obrigação legal de manter seu valor. Binance também não possui obrigações legais sobre o valor do $BNB, diferente de ações tradicionais de empresas, que possuem responsabilidade legal para com seus acionistas. O preço do $BNB, então, está atrelado apenas ao sucesso da Binance como empresa.

Milhas aéreas podem internalizar valor do ecossistema e explorar parceiros de sua rede como hotéis e locadoras de carros. Mas esses valores secundários são dependentes do sucesso da empresa aérea como um todo. Quando essas empresas vão à falência, o valor dessas milhas aéreas despenca em conjunto. Caso a Binance “quebrasse”, valor do $BNB cairia drasticamente.

Mecanismos deflacionários, vale lembrar, **tendem** a aumentar o valor do ativo, mas não é nada garantido. Queima de tokens afeta apenas o lado da oferta diretamente. Você ainda tem o lado da demanda para completar a equação. Somente porque existem menos tokens em circulação, não significa que o mercado irá pagar mais para os tokens remanescentes. Baixa oferta para algo que não possui demanda significa somente que não existe muito mercado para o ativo.

Dado que a Binance não pode depender somente desses mecanismos deflacionários para manter ou aumentar o preço do $BNB, podem criar formas de garantir a demanda pelo ativo. Isso nos leva à última seção: incentivos financeiros.

### Incentivos Financeiros

##### Atividades da Plataforma

Incentivos financeiros compõem um dos pilares do design de token. Na Binance, cada transação gera uma taxa base de 0.1%. Investidores podem usar $BNB para pagar essa taxa e receber descontos.

O desconto segue uma tabela decrescente. Em 2017, pagar em $BNB concedia 50% de desconto sobre as taxas. Esse valor foi reduzindo para metade a cada ano. Em 2020, o desconto era de 6.75% - em 2023, retornaram esse valor para 25%.

Claramente, no início da plataforma tínhamos descontos altíssimos (50%). Olhando para a queima acumulada de $BNB por meio de transações, fica claro o motivo da Binance ter alterado sua referência de valor para calcular a quantidade removida do sistema. Com os 6.25% de desconto que tinham implementado em 2020, pressão deflacionária, e vários outros casos de uso, usuários possuem mais incentivos para usarem $BNB de outras formas do que apenas para descontos em taxas de transação.

Ao longo do tempo, é provável que o desconto continue reduzindo. Incentiva casos de uso para $BNB em outras plataformas, como *staking* ou concessão de outros serviços.

Quando a Binance oferecia aos usuários taxas reduzidas com o uso de $BNB, estavam basicamente realizando uma pré-venda do período de ICO. Usuários compravam $BNB para utilizarem depois. Existia um caso de uso real, ao invés de apenas a compra na expectativa de valorização de preços.

Esse mecanismo incentivou investidores de larga escala a comprarem $BNB para reduzirem suas taxas. Esses investidores estão não só preservando uma maior parte de seu capital, mas aumentando esse montante total – Binance está basicamente distribuindo esse “valor” – na utilização do token para redução de taxas cobradas.

Usar o token $BNB para pagar taxas de transação também era econômico para a Binance. De fato, esse mecanismo dilui uma de suas principais fontes de receita que iriam para seus investidores iniciais. Porém, visto que essa receita é em tokens que eles mesmos criaram, não há muito a perder na concessão desses descontos – talvez por isso tenham retornado momentaneamente com o desconto de 25%, ao invés de 6.25%.

#### Staking (Retornos Sobre Stake)

Na prática, mecanismos de *staking* afetam a oferta circulante do token enquanto permitem que o mercado dite a demanda. Com *staking*, Binance está influenciando a oferta circulante na plataforma. Traders de altos volumes precisam manter determinadas quantias de $BNB em suas contas para desbloquear descontos adicionais.

Pense nisso como se fosse um modelo de assinatura. Vamos supor que você assine o boletim (*newsletter*) da Economics Design por meio de submeter e travar tokens $NEWS[[148]](#footnote-149). Esses tokens são congelados e não podem ser movidos – mas você não está perdendo seus tokens ao longo do tempo. Isso te dá acesso a todos os itens relacionados à Economics Design.

Para esses investidores de larga escala, esse modelo de assinatura é melhor do que utilizar o próprio token para ter descontos em transações individuais. Até maio de 2020, 33 milhões de $BNB estavam travados, levando a oferta circulante a 147 milhões – subtraindo também tokens queimados e em *lock up*.

Além do *staking* para esses traders, proprietários de $BNB podem realizar o *staking* para receber rendimentos em cima do ativo – conforme atualização de abril de 2020. Binance estava mudando para um mecanismo de consenso baseado em *stake*, além de possibilitar a execução de contratos inteligentes. Taxas de gás pagas em $BNB, validadores coletando essas taxas de transações, e necessitando o *stake* de certa quantia de $BNB para ser elegível como validador.

### Conclusões

Tokens nativos ($BNB nesse caso) são criados pela empresa (Binance). Ao invés de reciclarem os tokens e colocarem de volta ao ecossistema, alguns são queimados. Esse processo de reciclagem de tokens é também conhecido como “efeito multiplicador”. Como exemplo do mundo físico, quando um cliente paga por uma refeição, o restaurante usa parte desse dinheiro para pagar seus fornecedores. A quantidade de dinheiro no sistema aumenta. Quando tokens são queimados, é como se parte do capital pago pelo cliente desaparecesse, reduzindo a oferta circulante no sistema. A queima em si não afeta diretamente os preços no curto prazo, mas pode influenciar no longo prazo por meio do controle de inflação.

A queima ajuda o ecossistema a atingir o objetivo proposto pelo $BNB. Mas é difícil afirmar categoricamente que queima de tokens é um bom método, dado que ativos deflacionários oferecem outras potenciais consequências que podem não ser adequadas para certos casos de uso.

*Staking* também é um dos mecanismos utilizados, visto que não é possível a Binance continuar recomprando e queimando tokens para sempre. Esse mecanismo garante à empresa mais tempo para consolidar sua rede de parceiros, recompensar apoiadores iniciais, e construir uma comunidade robusta. Ao invés de oferecer preços baixos para atrair mais usuários como outros protocolos fazem, Binance emite tokens nativos como recompensa para esses usuários e continuamente gera valor para o ecossistema como um todo.

## [Estudo de Caso] Esse Livro

Esse livro é tokenizado. Não é exatamente um desses livros “colecionáveis tokenizados”, mas estou testando a tokenização dos direitos editoriais. Esse é um experimento de direitos tokenizados que inclui direitos de propriedade intelectual, direitos de distribuição, e direitos de licenciamento.

### Pensamentos Por Trás Dessa Ideia

É apenas um experimento!

Tokenizar é uma nova forma de representar o valor de algo. Conforme discutido ao longo desse livro, geralmente tokenizamos o valor econômico de ecossistemas. Esse é um tópico bastante amplo por si só, e tenho certeza que sabe do que estou falando caso tenha lido o restante do livro! E é exatamente isso que estou experimentando.

Essa iniciativa foi inspirada principalmente por duas pessoas. Uma me disse: “você deveria tokenizar esse livro, já que é o que você ensina”. A outra, tenho tido diversas discussões sobre a tokenização de *securities* na forma de NFTs. Era a ideia certa no momento correto!

### Direitos de Distribuição como NFT

Primeiro, esse token apenas está disponível para empresas editoras, e não para o público em geral.

Segundo, o token é uma forma de contabilidade sobre a quantidade de livros vendidos. Essa é uma informação muito importante pois define como podemos fazer o design do token adiante.

E terceiro, pode ter certeza que irei usar curvas de ligação – ou as famosas *bonding curves*!

#### Por Que NFTs?

O valor que o token representa é do direito de publicar e distribuir esse livro em diferentes geografias. Escolhi NFTs pois eles oferecem a possibilidade de embutir regras (ex: limite de livros vendidos) no próprio token. Ou seja, cada token será único por si só.

#### Por Que Tokenizar?

Acredito na tokenização de algo apenas quando essa nova versão tokenizada adiciona valor real ao sistema/produto. No mundo editorial, existem duas formas de publicar um livro: por meio de editoras, ou por publicação independente.

A opção de editoras é ótimo porque são experts no assunto. Porém, eles também tomam parte do risco, e não estão sempre dispostos a fechar negócio – especialmente em novas áreas de especialização, como Tokenomics. Gastei dois anos em conversas sem sucesso com editoras, visto que achavam o tópico muito nichado, complexo demais, ou simplesmente não tinham interesse. O principal motivo era que não conseguiam entender a demanda de mercado por esse tipo de livro.

Isso nos leva para a segunda opção: publicar e fazer tudo por conta própria. Por mais que seja ótimo ter controle sobre todos os detalhes da publicação de seu livro, autores perdem algumas habilidades técnicas importantes desses experts, como estratégias de campanhas de lançamento, edição profissional, rede de conexões e parcerias, e maior alcance de distribuição.

Decidi que a tokenização dos direitos de publicação era uma boa solução. Permitirá que eu:

1. Ajude editoras profissionais a entenderem a demanda de mercado por esse material por meio da demanda real;
2. Por consequência, também ajude outros autores independentes a atingirem conexões em sua rede para especializações necessárias.

#### Por Que Agora?

A ideia de tokenizar direitos de publicação ainda é muito nova. Discussões geralmente envolvem a tokenização de reputação, comunidades, ou bens digitais. Tudo o que foi discutido nesse livro, porém, também está em fase de experimentação; está evoluindo constantemente. Da mesma forma, a tokenização dos direitos de publicação desse livro testa[[149]](#footnote-150) e desenvolve o conceito como um todo – faz parte do processo de evolução da indústria.

Essa ideia está na minha cabeça desde o segundo trimestre de 2019, quando estava aprendendo sobre curvas de ligação (*bonding curves*). Um problema técnico que ainda não foi solucionado, por exemplo, é a agregação do “mundo real” (*off-chain*) com a execução de contratos inteligentes *on-chain*. Essa é minha maior preocupação. Minha conclusão foi: por que não começar com esse experimento logo, e ir atualizando com novas soluções e mecanismos conforme a indústria se adapte?

### Design Econômico desse NFT - $EDBK

$EDBK significa “Economics Design Book”, um nome muito criativo - rs!

A ideia geral é:

1. Limitar o direito de publicação de livros físicos para cada região geográfica
2. Precificar os direitos de publicação de acordo com os riscos percebidos
3. Utilizarm o token para contabilizar a distribuição de retornos adicionais

O principal problema de editoras é não saber a demanda do mercado por um livro específico (exemplo de assimetria de informação, visto que **eu** entendo a demanda do mercado!). Por isso, o NFT $EDBK sinaliza a demanda e diminui a assimetria de informação. Visto que $EDBK é um NFT que representa o direito que revender e publicar esse livro, a única diferenciação está nos detalhes – quanto tempo dura o direito de publicação, geografia permitida, e a quantidade de livros.

O preço do $EDBK é determinado por uma curva de ligação. Quanto mais cedo uma editora comprar o livro, menor é o custo. Isso significa que os primeiros a tomarem o risco são recompensados com custos muito mais baixos de publicação do livro. Conforme a demanda do mercado aumenta, incentiva outras editoras a adquirirem os direitos também. Editoras terão mais certeza sobre a demanda do mercado pelo livro, e terão menos risco percebido em sua tomada de decisão. Portanto, pagam uma taxa maior para comprar os mesmos direitos dos compradores iniciais – estão pagando a mais pela segurança.

A editora paga royalties para o autor, no caso eu, e fica com o *markup* – margem acrescida ao preço de venda. Parte desse royalty é adicionado à *pool* e distribuído para os proprietários de $EDBK proporcionalmente, incluindo quaisquer outras vendas pelo autor original (eu). Essas regras e acordos serão implementadas na curva de ligação, por meio de contratos inteligentes.

#### Design de Mercado

Design de mercado é o design do ambiente em que $EDBK e seus proprietários existem. Visto que estruturei o token como um NFT e restringi seus proprietários para apenas editoras profissionais, o ambiente fica bastante limitado. Assim como em blockchains “permissionadas”, participantes são verificados fora da rede (*off-chain*). Robustez do mercado e congestionamento não são problemas críticos nesse tipo de ecossistema.

Em termos de segurança, a ideia é que tokens representem o nível de risco e demanda de mercado. Essa informação é útil para editoras determinarem quando tomar decisões de compra e distribuição de livros. A prova social está no preço do $EDBK.

Em termos de cálculo, será utilizado computação e agregação de dados por meio de um contrato inteligente de código aberto. Como ainda está na Versão 1, irei coletar dados relevantes e calcular a distribuição de receita adicional publicamente. Até encontrarmos formas de verificar dados *off-chain* e transmitir para *on-chain*, ainda precisaremos usar ferramentas de Web2 em projetos de Web3 – ou seja, irei divulgar publicamente.

#### Design de Mecanismo

Atualmente, não possuo inteção de embutir outras regras não relacionadas ao token no sistema. Um incentivo comumente utilizado é a governança e o poder de voto. Dado que a única votação seria sobre a distribuição de rendimentos adicionais, não vejo benefícios econômicos de introduzir tal mecanismo. Isso não alinha os incentivos dos diversos agentes e pode criar mais problemas do que soluções.

Na **reformulação da economia de tokens 2.0**, podemos explorar outros métodos de design de mecanismo. Quando dados são provenientes de fontes externas (*off-chain*) e pode ser integrada aos contratos inteligentes *on-chain*, consigo ver a necessidade de validadores e *stakers* no meu projeto. Caso isso se tornasse realidade, aumentaria a necessidade de mecanismos de governança apropriados e incentivos.

Até então, esse experimento passará bem por si só.

#### Design do Token

Token será emitido com base na curva de ligação. No próprio token, vários elementos serão embutidos, como por exemplo:

* Duração dos direitos de publicação para editoras
* Quantidade mínima ou máxima a ser distribuída
* Área geográfica exclusiva da distribuição

Podemos construir esse racional como uma curva de ligação, tendo o ativo no formato de NFT e com o mesmo ativo subjacente: o livro.

Uma nota importante é que $EDBK inclui somente livros físicos[[150]](#footnote-151). Na curva de ligação, portanto, temos outra curva de fonte de receitas relacionada às vendas do e-book. Editoras divulgam o livro, e geram valor para todo o ecossistema de parceiros.

Para recompensar o bem comum, distribuição de receita proveniente do e-book também é implementada por meio da curva de ligação. Conforme esse experimento amadurece, e a “Tragédia dos Comuns” aparece, compensação quadrática será considerada com relação ao NFT e ao orçamento para ações marketing. Na **reformulação da economia de tokens 2.0,** isso pode ser embutido e calculado diretamente nos contratos inteligentes, adicionando valor às atividades de tokenização e distribuição do ativo.

Caso você seja uma editora que tenha interesse em participar desse experimento, favor entrar em contato por meio do e-mail: book@economicsdesign.com!

## O Futuro de Ecossistemas Tokenizados

Para concluir, estamos apenas começando nesse setor. Pioneiros na adoção (nós) estão construindo e experimentando com a infraestrutura base do futuro. Isso irá mudar a forma que fazemos as coisas. O sistema de Web2 que o mundo está acostumado, assim como os princípios que todos temos seguido, estão prestes a mudar.

### O Que Esperar Para o Futuro da Engenharia de Tokens e DeFi

DeFi e engenharia de tokens ainda estão em fase experimental. Ideias e conceitos estão sendo testados. Pelo fato de DeFi ser uma tecnologia agnóstica, pode agir como uma rede de testes para o nosso futuro. A indústria apresenta um número crescente e saudável de novos entrantes para testar o impacto do uso de tokens em vários aspectos, como:

* Aquisição de usuários
* Alinhamento de incentivos
* Novos mecanismos fundamentais como DLT e outros

O próximo passo é traduzir esses benefícios para o mundo físico “real”, ao invés de permanecer apenas *on-chain*. Para isso, teremos que nos comunicar com reguladores para estabelecer regras antes que esses sistemas possam ser adotados pela grande massa da população mundial.

### Setores Para Ficar de Olho

Quais setores vão continuar amadurecendo conforme olhamos para o futuro?

**O mercado de seguros** possui potencial de continuar crescendo. Construindo sobre o que já foi criado em termos de infraestrutura de seguros relacionados à cripto, ou criando novos mecanismos para alinhar incentivos de agentes.

**NFT,** não somente como arte colecionável, mas como uma propriedade fracionada de um ativo específico. Podemos usar esses tokens para criar novos produtos estruturados e únicos. Pode ser uma nova classe de ativo negociável.

**Jogos e metaverso** são importantes e agem como pontes entre os mundos *on-chain* e *off-chain*. Esses ecossistemas sociais utilizam do poder de economias customizáveis e da infraestrutura de DeFi para criar valor nos diferentes “mundos” em que vivemos.

Web2 está limitada à divisão entre o mundo “real” (*off-chain*) e o mundo digital (*on-chain*). Conforme a indústria avança, podemos ver mais protocolos conectando esses dois mundos. Podem ser **oráculos**, estruturas de padronização de dados (ex: velha guarda da Web3), ou novos mecanismos para obter informação do mundo real, *off-chain*.

Esse livro cobriu principalmente tokens fungíveis. O próximo setor que podemos explorar é o amplo tópico de **tokens não-fungíveis**.

Tokenização de ativos financeiros tradicionais (*securities*) são os próximos na fila. Atualmente, DeFi está tokenizando os serviços mais óbvios do mundo tradicional, como empréstimos e negociações de trade. Provavelmente veremos mais mecanismos de tokenização para ativos financeiros – como ações, por exemplo. Regulamentação será crucial nesse processo.

Tokenizar ativos únicos como propriedade intelectual (IP), direito de propriedade, e outros tipos de ativos intangíveis também são aplicações óbvias. DeFi entra em cena com a distribuição de retornos e potencialmente incentivando o comportamento dos proprietários para acumulação de longo prazo. Os capítulos de DeFi abordaram apenas a ponta do iceberg.

### Futuro Ideal

Imagino um mundo em que existimos digitalmente, transcendendo jurisdições geográficas e criando economias digitais que supram nossos próprios valores. Regras de governança digitais governando por si só, e em conjunto com as pessoas do ecossistema. Você poderia deficir quais regras de governança prefere e definir seu ecossistema de permanência. Não teríamos limites de raça, cor de pele, ou idioma, mas sim sobre filosofia e ideologia de vida. Deixamos para o mercado, então, decidir quais organizações autônomas serão bem-sucedidas.

O futuro é extremamente empolgante. Estamos experimentando e construindo conceitos e mecanismos inovadores todos os dias, em busca de um futuro mais próspero e acessível para todos. Esse é apenas o começo. O futuro está nas mãos de pessoas como eu e você. Que nosso futuro seja mais eficiente e justo do que o que temos atualmente!

O que fazer agora?

**Eu quero me manter atualizado:**

Você pode se inscrever em minha newsletter semanal sobre design econômico em https://www.newsletter.economicsdesign.com. Eu compartilho estudos de caso, entrevistas com protocolos e discuto tópicos econômicos.

**Eu quero me educar mais:**

Você pode se inscrever no curso digital sobre a economia da engenharia de tokens em <https://academy.economicsdesign.com>.

**Eu sou um investidor e quero aprender mais sobre fundamentos:**

Se você está interessado em relatórios fundamentais, você pode encontrar mais informações em www.economicsdesign.com. Publicamos relatórios de mercado e relatórios específicos de protocolo.

**Preciso de ainda mais informações. Dê-me mais dados brutos:**

Para outros recursos, eu mantenho uma lista de recursos de código aberto em bit.ly/tokenomics-resources. Confira!

**Quero me conectar com a Lisa**

**Lisa Twitter:** <https://twitter.com/lisajytan>

**Economics Design Twitter:** <https://twitter.com/EconsDesign>

**Econteric Twitter:** <https://twitter.com/econteric>

**Econteric Website:** <https://econteric.com/> **LinkedIn:** <https://www.linkedin.com/in/lisajytan/>

**Economics Design LinkedIn:** <https://www.linkedin.com/company/economicsdesign/>  **YouTube:** <https://www.youtube.com/@EconomicsDesign> **Economics Design Email:** [token@economicsdesign.com](mailto:token@economicsdesign.com)

**Discord:** <https://discord.com/invite/gZGEZfu74X>

**Podcast:** <https://anchor.fm/economicsdesign>

**Quero me conectar com o Giovanni**

**Giovanni Twitter:** <https://twitter.com/7gioeth>

**LinkedIn:** https://www.linkedin.com/in/giovanni-populo-7b5746118/

Appendix A

**Financial terms**

These are analogies, not equations.

|  |  |  |
| --- | --- | --- |
| **Traditional Finance** |  | **Decentralized Finance** |
| Agreement |  | Consensus mechanism |
| Availability of  market makers to provide liquidity |  | Liquidity pools |
| Bad trade |  | “Rekt” |
| Bank account |  | Wallet address |
| Banks borrowing from and lending to each other |  | P2P lending  (e.g., Aave, Compound) |
| Board of Directors |  | DAO |
| Broker that executes trade on your behalf |  | Smart contract |
| Buy and hold strategy |  | “Hodl” |
| Bond, Money market  fund⸺anything where you add assets into a product as an investment strategy |  | Vault, pool |
| Collateral |  | Stake |
| CDO, or using collaterals to create an asset in any way |  | Collateralized Debt Position (CDP) |
| Database, ledger |  | Blockchain |
| Derivatives |  | Synthetic assets |
| Earning returns  denominated in another asset |  | Liquidity mining  or yield farming |
| Equity holders with  voting rights |  | Governance token holders |
| ETF |  | DeFi ETF (e.g., Hashdex, PieDAO) |
| Exchange  (e.g., NASDAQ) |  | DEX (Decentralized exchange)  (e.g., Uniswap) |
| Futures contract rollover |  | Perpetual Futures |
| Interest-bearing assets |  | aTokens, interest bearing assets on Aave that accrue interest from P2P lending |
|  |  |  |
| IPO |  | ICO, IDO, IEO |
| Long |  | Moon |
| Lottery |  | No-loss lottery (e.g., PoolTogether) |
| Market maker |  | Liquidity provider |
| Money (e.g., USD) |  | Stablecoin (e.g., $DAI, $USDT) and currency tokens |
| Money markets |  | Aave, Compound,  Curve, Maker |
| Penny stock |  | Shitcoin |
| PIN |  | Private key |
| Portfolio manager |  | Non-custodial portfolio manager (e.g., Balancer) |
| Repo |  | Borrow against stake or collaterals, yield farming |
| Returns |  | Yield |
| Robo advisor but only focusing on investing in the best interest rates in money market funds |  | Yearn Finance |
| Stock buyback |  | Token burn |
| Third-party data source |  | Oracle |
| Transaction fee |  | Gas fee |
| Unrealized loss |  | Impermanent loss |
| Whale |  | Whale |

Glossary

**Economics**

1. Allocation mechanisms: Determines how to allocate products to the right participant. Example: auction market, voting.
2. Behavioral economics: newest school of thought in economics. Recognizes that people are irrational. Behavioral considerations are important in decentralized ecosystems. Token incentives attempt to influence people’s behaviors through behavioral economics.
3. Cooperative game theory: participants work together, cooperate, and behave in certain ways. Example: everyone agrees to trade on-chain and agrees not to make private transactions off-chain.
4. Crypto economics: economics behind blockchain ecosystems. This includes token ecosystems and the economics of blockchain platforms themselves.
5. Deflation: the value of money increases in the future. While this is good, it prevents other economic activities like using that money to invest in other value-adding activities. It becomes better to hold on to the money instead.
6. Dominant strategy: a strategy that is always better than the rest of the strategy options. Example: I have three possible strategies: eat a Kobe beef steak, murder a person, get eaten by a shark. The best strategy is always to eat a Kobe beef steak, so that is the dominant strategy.
7. Economies of scale: efficiencies formed by volume, not variety.
8. Economies of scope: efficiencies formed by variety, not volume.
9. Economic efficiency: pareto optimum. No one can benefit more without another party losing out.
10. Economic models: models to represent reality. No model is perfect, but having a model is better than not. They can be used to predict the future or to analyze the past.
11. Egalitarian mechanism: a mechanism that is fair to participants in games. There are criteria to determine whether a mechanism is egalitarian.
12. Fiscal policy: Government spending and taxation designed to affect the monetary market. More government spending could boost the economy. Fiscal policy also decides tax rates.
13. Game theory: strategic decision-making. Used to analyze options to make decisions or analyze why such decisions are made.
14. Governance: the rules by which people (or tokens) must play in a specific space (e.g., digital ecosystem, game, theme park, country).
15. Government bonds: contract issued by the government to borrow money from people and to return the money (with interest) later.
16. Incentives: rewards to encourage certain behavior. These can be financial or non-financial.
17. Incomplete contracts: Contracts are designed to provide solutions when something happens. However, in practice contracts “incomplete”, because they do not and cannot address every potential situation, much less provide corresponding solutions.
18. Inflation: decrease in value of money because there is an increase in supply. For example: I could use £1 to buy a chocolate bar. There is a 50 percent inflation, and now for the same chocolate bar, I must use £1.50 for the same chocolate bar.
19. Interest rates: amount charged when you borrow something or lend something. Example: interest incurred when you borrow money from the bank. The bank pays you interest when you store your money with them.
20. Markets: place where consumers and producers come together to buy/sell, change prices and outputs until equilibrium market prices and market output levels are determined.
21. Macroeconomics: aggregate behavior. Higher-level governance, monetary policy.
22. Market design: designing the environment the market can interact in. It can be anything from organizing organ donation to token ecosystems or platforms like Amazon and Airbnb.
23. Market failure: when the market does not function as it is supposed to. Example: oversupply of products, inability for people to transact with each other, etc.
24. Mechanism design: reverse game theory or rules of the game. Instead of participants choosing a strategy based on the outcome of their choices, mechanism design creates the rules of the game to constrain the behaviors of participants toward a desired outcome.
25. Microeconomics: analyzes, models, and investigates individual behaviors (e.g., market design, Nash equilibrium).
26. Monetary economics: economics of money. Central banks make decisions regarding money in general; policies are set by the central bank to control the movement from a high level.
27. Monetary policy: central bank changing interest rates and money supply to manage the economy.
28. Moral economies: a moral economy is an economy that is based on goodness, fairness, and justice, as opposed to one where the market is assumed to be independent of such concerns.
29. Multi-stage game: the opposite of multi-stage game is a single-stage game. A single-stage game is where everyone plays together once, and then they leave and do not interact anymore. Therefore, a multi-stage game is a game form that follows a sequence of one game after another.
30. Nash equilibrium: a steady state where no one changes their decisions because there is no incentive to do so.
31. Noncooperative game theory: cooperation is tough. People naturally do not cooperate unless there is an incentive to. Hence, noncooperative game theory is the natural state of people. We use this state to analyze behaviors and actions of participants.
32. Pareto efficiency: a state of how things are allocated. The allocation is known as pareto efficient if you cannot increase someone’s benefit without someone suffering or paying for it. Pareto efficiency always be a zero-sum game.
33. Price: an allocation mechanism for goods and services.
34. Private information: information that is not public, like insider information, analysis, private observation, etc.
35. Property rights: the right to decide how a good is used and owned. It is usually a socially-enforced construct.
36. Repugnance: Repugnance refers to strong social pressure to *not* transact in a specific the market because of what it peddles (e.g., murder-for-hire, organ donation, sex trafficking, adoption).
37. Required reserves: amount of physical cash (reserve) that needs to be in the bank. This amount is stated by the central bank.
38. Resolution mechanism: different mechanisms to resolve disagreements within the ecosystem. Example: specific codes in smart contracts, TCRs (not really a form of consensus).
39. Savings function: the relationship between income and savings. It shows the willingness to save, given the amount of income.
40. Schelling point: natural point that people tend toward without communication. Example: If someone asks you to meet you at your car, where would you look? It is helpful when we have decentralized ecosystems and need to decide based on what people are likely to do.
41. Social choice: a collective decision that is the best for everyone.
42. Token: anything that represents value.
43. Token economy: an environment in which participants interact with each other in a digital space, facilitated by tokens or other unit of measure.
44. Token economics: the economics underlying a token economy. It sets forth the architecture of the token economy, including governance mechanisms, token monetary policy, and property rights. It determines the structure of the overall token governance and ecosystem design.
45. Token policy: how tokens are governed and managed.
46. Zero-sum game: someone wins at the expense of another.

**Finance and DeFi**

1. Algorithmic rebalancing: rebalancing to an agreed-upon value algorithmically.
2. Automated market maker: a system to allow exchange between assets using math (also known as autonomous market maker or decentralized market maker).
3. Bond: debt security with an obligation to repay.
4. Bonding curve: a curve (equation) that connects two or more variables mathematically.
5. Composability: a system design principle that deals with the inter-relationships of components. A highly composable system provides components that can be selected and assembled in various combinations to satisfy specific user requirements.
6. Collateralized Debt Obligation (CDO): A specific type of derivative that pools loans and other income-bearing assets like credit card receivables and aircraft leases and derives its value through the collateralization of the promised repayment from those assets.
7. DeFi: decentralized finance is a movement that uses decentralized networks to transform the financial system as we know it by removing intermediaries.
8. Derivatives: contracts that derives its value from the assets in the contract.
9. Digital currency: a category of currency (legal tender and non-legal tender) that exists digitally.
10. Discount rate: interest rates when a commercial bank borrows from a central bank.
11. Effective lower bound: the point at which further reductions in the interest rate no longer stimulate demand, or the point at which other negative effects arise. This can be a positive or negative rate, or zero.
12. ETF: exchange-traded fund. A type of low-cost index fund that is traded on the stock market. Typically purchased and sold by brokers or retail investors.
13. Exchange rates: the amount of currency A needed to acquire currency B.
14. Flash loan: a loan that you can secure through a smart contract from the DeFi protocols liquidity pool. It allows the smart contract to execute in many protocols, to borrow, use and repay the loan in a single transaction.
15. Futures contract: legal agreement to buy or sell an asset at predetermined price at a specific time in the future.
16. Hedge fund: an investment fund that invests in assets using complex strategies and financial instruments intended to improve the returns of the fund.
17. Howey test: Created by the US Supreme Court to determine whether a certain transaction qualifies as an “investment contract,” and therefore a financial security. If the transaction qualifies, it is subject to disclosure and regulation requirements under the Securities Act of 1933 and Securities Exchange Act of 1934.
18. Impermanent loss: The opportunity cost of depositing and later withdrawing assets from a liquidity pool as opposed to leaving them in a wallet and allowing their value to grow from market fluctuation. Even if one withdraws more than one deposits, the increased value can still be less than the value she would have had had it sat in the wallet.
19. IPO pop: a situation where the value of the stock increases when it is initially listed on an exchange. Early buyers of the stock can profit from this trade. For example, nCINO’s price jumped 195 percent upon listing on NASDAQ in July 2020. Baidu was the largest IPO pop on NASDAQ in 2005, with a 354 percent price increase on Day 1.
20. Market maker: institute that always buys and sells on the exchange.
21. Monetary policy: how money is governed and managed.
22. Leverage: a financial strategy to use funds to increase exposure to your trade. For example, I have $10 and the leverage I receive is 10x. So now, I have $100-worth of leverage that I can use to trade.
23. Liquidity: ease of exchanging an asset for another kind of asset.
24. PE ratio: current stock price divided by earnings.
25. Perpetual futures: futures contract to buy or sell an asset at a predetermined price without an end date.
26. Ponzinomics: economics of Ponzi scams.
27. Physical delivery: in terms of options and futures contract, the actual underlying asset is delivered upon a specific date, rather than offsetting with cash transactions based on the difference between the spot price on the date of settlement and the contract price.
28. Present value: current value of future sum of money, given a specific rate of return.
29. Price discovery: overall process of setting spot price or price of an asset, financial security, commodity, or currency.
30. Price stability: prices are consistent over time.
31. Price slippage: difference between the expected price before the transaction and the actual price when the token is transacted.
32. Repo: repurchase agreement. It is a short-term borrowing rate between institutional players like banks and central banks. It typically lasts overnight. Think of this as borrowing and lending, but for banks instead of retail people like you and me.
33. Venture capital: a form of private funding in exchange for equity. This is usually for start-ups with high growth potential.
34. Yield: returns from investment.

**Technology**

1. ASIC Miners: Computerized devices that use “application-specific integrated circuits” for the sole and specific purpose of “mining” digital currency; usually only one kind of digital currency (e.g., bitcoin).
2. Data: raw records.
3. Dapp: decentralized applications. These are applications built on blockchain.
4. DPoS: delegated proof of stake. Validation tasks are delegated to a group of people. This can help to increase transaction speed because there are fewer validators. It can also increase safety because delegated validators usually must meet certain criteria.
5. Fork: copy the source code, make changes to it, and run the code independently.
6. Information: transformed data (clean).
7. Intangible assets: assets that typically involve the development of specific products or processes, or are investments in organizational capabilities, creating, or strengthening product platforms that position a firm to compete in certain markets.
8. Invariant: a mathematical constant which remains unchanged after variables are modified in a formula. AMM algorithms use invariants to execute trades and algorithmically rebalance pools of tokens.
9. Fungible tokens: interchangeable tokens. Example: one $BTC is the same as any other $BTC.
10. GPT-3: machine language that uses deep learning to produce human-like text.
11. Interoperability: the ability for different systems to speak to one another. For example, an app running on iOS can send data to another app running on Android.
12. Knowledge: the ability to connect information with evidence and reflect on or analyze the results to form a coherent understanding.
13. Layer 1: blockchain’s base technology layer.
14. Layer 2: a layer above Layer 1, usually to resolve scalability problems in Layer 1.
15. Merkle tree: a way of organizing information in cryptography. It looks quite like a business organizational chart.
16. Non-fungible tokens: unique tokens that are not easily interchangeable. Example: a Crypto Kitty is unique and cannot be exchanged for another Crypto Kitty.
17. Operational rules: rules that govern distinct operations in an ecosystem, institution, or organization. They are usually hard coded and clear. For example, hard-coded algorithms, law, or standard operating procedures.
18. Plasma Chain: a form of childchain to Ethereum. It is designed specifically to increase transaction speed to 1-3 seconds. Imagine you eat a lot throughout the day, and you like to count your calories. Every hour, you eat something, like an apple, banana, chocolate bar, etc. It is inconvenient and time-consuming to continually track calories every hour. Instead, add it up at the end of the day. That is how Plasm Chain works. Plasma Chain aggregates all the transactions and updates the Ethereum mainchain at once.
19. PoS: proof of stake. Think of a lottery. You have a chance of winning if you buy the lottery ticket. Similarly, PoS is where you place your name and stake (some tokens) in a box for a chance to be a validator. Meaning you get to approve the transactions and be rewarded in block rewards or transaction fees. A stake must be added to prevent bad actions. For example, if you validate an empty block, you will lose your stake.
20. Protocol: The language that systems run on. Protocols are codified and systemized processes and steps to do something. Instead of listing Step 1, Step 2, Step 3, the protocol writes that in the code. Systems then follow the steps and execute an action.
21. Quantitative easing: central banks create new bank reserves on their balance sheets, and then use those new reserves to buy back government bonds or other financial assets from major financial institutions, thereby infusing additional bank reserve currency (money supply) into the economy. This reduces the purchasing power of each unit of currency.
22. Rollup: Layer 2 blockchain scalability solution. Aggregates transactions over a certain period and updates all the mainnet blockchain with the bundled transactions all at once.
23. Sharding: instead of keeping a physical cup, imagine smashing it on the floor and giving each friend a small piece of the cup. One scalability solution is sharding, which is to break information into small pieces and having different validators keep these pieces. Only the owner of the data can retrieve the information through the privately-held key.
24. Smart contract: software that executes specified activities contractually and automatically (if condition A is met, do action B).
25. Sidechain: Imagine the main chain as a national highway where vehicles can run, sometimes at high speeds, but often with a lot of traffic congestion. Speeds can vary between national highways and frontage roads. Sidechains are the frontage roads that join the highway to cities. The frontage roads (sidechains) can lead vehicles to and from national highways (main chains) whenever needed.
26. Private key: password in the crypto world.
27. Protocol: an operation or set of rules that is defined and written down.
28. Sybil attack: an attacker creates multiple pseudonymous identities on a network and uses them to gain disproportionately large influence over the network. Imagine a person creating multiple Meta accounts to like their own post.
29. ZK-rollups: an application of zero-knowledge proofs. They aggregate transactions and update the mainnet, significantly reducing transaction fees.
30. ZKP: zero-knowledge proof: a cryptography protocol developed in the 1980s.
31. ZK-SNARKS: a category of ZKP. It allows one party to prove an action is done without identifying who did it.

Acronyms

AI Artificial Intelligence

AMM Automated Market Maker

BIC Bayesian Incentive Compatibility

BoE Bank of England

BoJ Bank of Japan

CBDC Central bank digital currency

CCIP Cross-Chain Interoperability Protocol

CLOB Central limit order book

DEX Decentralized exchange

CDO Collateralized debt obligation

CDP Collateralized debt positions

CHF Swiss Francs

DAO Decentralized autonomous organization

DLT Distributed ledger technology

DSIC Dominant strategy incentive compatibility

DSR $DAI saving rates

EEA Ethereum Enterprise Alliance

ENS Ethereum Name Service

ETF Exchange-traded fund

FED Federal Reserve (US Central Bank)

FOMO Fear of missing out

GBP British Pounds

GPT-3 Generative Pre-trained Transformer 3

HKD Hong Kong dollars

HSBC Hong Kong Shanghai Bank Cooperation

IBC Inter-blockchain communication

ICO Initial coin offering

IoT Internet of Things

IPO Initial public offering

IM Instant messenger

IP Intellectual property

IPR Intellectual property rights

IT Information technology

KYC Know your customer

LAO (Limited) Liability autonomous organizations

LP Liquidity provider or liquidity pool

LPC Liquidity provider contract

LT Leverage token

MAS Monetary Authority of Singapore

MCR Minimum capital requirement

MVP Minimum viable product

NFT Non-fungible token

OMO Open market operation

OSM Oracle Security Module

OTC Over-the-counter

PBoC People’s Bank of China

PE Price-earning

POA Proof of authority

RFID Radio-frequency identification

SEC Securities and Exchange Commission

SGD Singapore dollars

TCR Token-curated registry

UI/UX User Interface, User Experience

VC Venture capital

VPN Virtual private network

**Protocols and their Token Names**

AMPL Ampleforth

BAL Balancer

BNB Binance

BNT Bancor

BTC Bitcoin

COMP Compound

DAI Stablecoin soft-pegged to USD using MakerDAO

DAIBNT $DAI-Bancor liquidity pool in Bancor

EDBK Economics Design Book (this book)

EOS EOS, a Layer 1 platform

EREP Fake token created for examples

ETH Ether

ICP Internet Computer Protocol

KNC Kyber

LTC Litecoin

MEOW Unicat

MKR Maker

NXM Nexus Mutual

PETH Pooled ETH

SNX Synthetix

TOKEN Fake token created for examples

UNI Uniswap

USDC Circle’s stablecoin

USDT Tether

Recommended Economics Books

You don’t think I would leave without giving you more resources, do you? Here are some great books, both academic and easy reading.

1. John Maynard Keynes, *The General Theory of Employment, Interest, and Money* (Cham: Springer International Publishing, 2018). [Keynesian Economics]
2. Milton Friedman, *Capitalism and Freedom* (Chicago: The University of Chicago Press, 2020). [
3. Mises, Ludwig. *Human Action: A Treatise on Economics*, vol. 2 (LF ed.). Indianapolis: Liberty Fund, 1996. [Chicago/Austrian Economics]
4. Daniel Kahneman, *Thinking, Fast and Slow* (New York, NY: Farrar, Straus and Giroux, 2015). [Behavioral Economics]
5. Bruce R. Kingma, *The Economics of Information: A Guide to Economic and Cost-Benefit Analysis for Information Professionals* (Englewood, CO: Libraries Unlimited, 2001).
6. Jonathan Haskel and Stian Westlake, *Capitalism without Capital the Rise of the Intangible Economy* (Princeton: Princeton University Press, 2018).
7. Carl Shapiro and Hal R. Varian, *Information Rules: A Strategic Guide to the Network Economy* (Boston, Mass: Harvard Business School Press, 1998).
8. Eric A. Posner and E. Glen Weyl, *Radical Markets: Uprooting Capitalism and Democracy for a Just Society* (Princeton, NJ: Princeton University Press, 2019).
9. Alvin E. Roth, *Who Gets What--and Why: The New Economics of Matchmaking and Market Design* (Boston, Mass: Houghton Mifflin Harcourt, 2016).
10. Nir Vulkan, Alvin E. Roth, and Zvika Neeman, *The Handbook of Market Design* (Oxford, England: Oxford University Press, 2015).
11. David S. Evans and Richard Schmalensee, *Matchmakers: The New Economics of Multisided Platforms* (Boston, Mass: Harvard Business Review Press, 2016).
12. Joseph A. Schumpeter and Reinhold Aris, *Economic Doctrine and Method: An Historical Sketch* (Mansfield Centre, CT: Martino Publishing, 2012).
13. Shan Ling Pan and M. S. Sandeep, *Digital enablement: the consumerisation & transformational effects of digital technology* (New South Wales, Australia: World Scientific 2018).
14. Klaus North, Ronald Maier, and Oliver Haas, *Knowledge Management in Digital Change New Findings and Practical Cases* in *Progress in IS:* 10.1007/978-3-319-73546-7 (Springer Cham 2018).
15. Jeremy Rifkin, *The Zero Marginal Cost Society: The Internet of Things, the Collaborative Commons, and the Eclipse of Capitalism* (New York, NY: Palgrave Macmillan, 2015).
16. Robert J. Shiller, *Narrative Economics. How Stories Go Viral and Drive Major Economic Events* (Lawrenceville, GA: Princeton University Press, 2019).

1. Exemplos de protocolos no mundo da tecnologia são TCP/IP, HTTPS, FTP etc. Existem inúmeros tipos de protocolos. Alguns são governados por agências de padrões internacionais como ISO, ITU e RFC. [↑](#footnote-ref-2)
2. Solidity é a linguagem de programação feita para o desenvolvimento de contratos inteligentes que podem ser executados na Máquina Virtual Ethereum (EVM) (<https://github.com/ethereum/solidity>).  
    [↑](#footnote-ref-3)
3. Glow é uma nova linguagem de domínio específico (DSL) para aplicações descentralizadas em desenvolvimento (dapps) na blockchain da Cardano (<https://developers.cardano.org/en/programming-languages/glow/overview/>).   
    [↑](#footnote-ref-4)
4. Rust é uma de muitas linguagens de programação que utilizam o framework Substrate (<https://wiki.polkadot.network/docs/en/build-build-with-polkadot>).   
    [↑](#footnote-ref-5)
5. Motoko (<https://internetcomputer.org/howitworks/motoko/>) é uma linguagem de programação open-source desenvolvida para o protocolo Internet Computer (<https://internetcomputer.org/>). [↑](#footnote-ref-6)
6. Modelos de consenso são mecanismos para tomar decisões descentralizadas em um sistema. Existem muitas formas de coordenar agentes econômicos para tomar uma decisão cooperativa. Os dois modelos mais populares são o Proof of Work (Bitcoin) e o Proof of Stake (Ethereum).   
    [↑](#footnote-ref-7)
7. Em economia, sistemas de circuito fechado estão em um “estado de autarquia”, mas interagem entre eles. É importante iniciar em sistema de circuito fechado. Caso um sistema não seja sustentável ou robusto o suficiente, abrir o protocolo para interagir com outros não adiciona valor econômico no longo prazo. [↑](#footnote-ref-8)
8. Comportamentos, no contexto desse livro, demonstram a intenção de comprar ou vender, a habilidade de coordenar e colaborar com outros agentes econômicos, e influenciar oferta e demanda e usuários. Comportamentos são os resultados que medidos, enquanto incentivos e desincentivos são as entradas (*inputs*) que podem ser estruturadas. [↑](#footnote-ref-9)
9. A economia keynesiana é a norma aceita na maioria das economias capitalistas. Ela se baseia em ciclos de crescimento e recessão. O governo é considerado necessário para gerenciar esses ciclos por meio de regulamentação, dívida e tributação. A economia keynesiana mede o crescimento econômico em termos de crescimento do PIB. [↑](#footnote-ref-10)
10. A economia austríaca se concentra mais em um mercado livre sem a interferência do governo. Os indivíduos tomam decisões racionais, incluindo poupança e gastos lógicos. O crescimento econômico é medido em termos de taxas de poupança e produção. [↑](#footnote-ref-11)
11. Os tokens não-fungíveis (NFTs) ganharam popularidade no final de 2020. O token é único, não substituível, não-intercambiável e, portanto, não-fungível.  
     [↑](#footnote-ref-12)
12. Por favor, consulte a segunda definição de "translate" no dicionário Merriam-Webster (https://www.merriam-webster.com/dictionary/translate).  
     [↑](#footnote-ref-13)
13. Embora seja tecnicamente possível capturar o feedback do estado, a entropia em um sistema de circuito aberto é mais difícil de medir. Portanto, é mais caro capturar a informação perdida por meio da entropia. É aqui que o sistema pode atualizar e regular-se com base em situações e informações em constante mudança.  
     [↑](#footnote-ref-14)
14. Agentes econômicos são quaisquer participantes em um ecossistema. Eles podem ser usuários, investidores, corpos de governança, instituições ou até mesmo os próprios tokens.  
     [↑](#footnote-ref-15)
15. Análogo aos legisladores, ou agentes políticos de sistemas de circuito aberto.  
     [↑](#footnote-ref-16)
16. Silvio Gesell, Philip Pye, e Silvio Gesell, *The Natural Economic Order* (London: Owen, 1958). [↑](#footnote-ref-17)
17. Adam Smith, Edwin Cannan e Max Lerner, A Riqueza das Nações: Investigação sobre sua natureza e suas causas (Nova York: Random House, 1937). [↑](#footnote-ref-18)
18. Sucesso é mensurado pela capacidade do token de atingir seu objetivo programado. [↑](#footnote-ref-19)
19. SEC v. W.J. Howey Co., 328 U.S. 293 (1946) ("Howey"). Veja também os casos United Housing Found., Inc. v. Forman, 421 U.S. 837 (1975) ("Forman"); Tcherepnin v. Knight, 389 U.S. 332 (1967) ("Tcherepnin"); SEC v. C. M. Joiner Leasing Corp., 320 U.S. 344 (1943) ("Joiner") (n.d.). [↑](#footnote-ref-20)
20. Gareth William Peters, Efstathios Panayi, and Ariane Chapelle, “Trends in Crypto-Currencies and Blockchain Technologies: A Monetary Theory and Regulation Perspective,” *SSRN Electronic Journal*, 2015, https://doi.org/10.2139/ssrn.2646618. [↑](#footnote-ref-21)
21. Você pode notar que há momentos em que bitcoin está escrito com letra maiúscula e outros em que está com letra minúscula. Bitcoin é escrito com letra maiúscula quando se refere à tecnologia ou à rede em si, mas com letra minúscula quando se refere exclusivamente à moeda. [↑](#footnote-ref-22)
22. “ELI5”, sigla muito utilizada nos Estados Unidos, e que significa “Explain Like I’m 5”, ou em tradução livre, “explique como se eu tivesse 5 anos de idade”. Será utilizada ao longo do livro para destacar exemplos que simplificam um conceito por meio de exemplos bastante simplificados. [↑](#footnote-ref-23)
23. McKinnon, Ronald I, 1993. "The Rules of the Game: International Money in Historical Perspective", *Journal of Economic Literature, American Economic Association*, vol. 31(1), páginas 1-44, março.   
     [↑](#footnote-ref-24)
24. Fisher, Irving. “‘The Equation of Exchange,’ 1896-1910.” *The American Economic Review* 1, no. 2 (1911): 296–305. http://www.jstor.org/stable/1804304. [↑](#footnote-ref-25)
25. Este modelo é também conhecido como a equação de troca, que afirma que o crescimento da oferta de dinheiro determina o crescimento do nível de preços a longo prazo. Quando os bancos centrais criam mais dinheiro, o nível de preços dos bens aumentará proporcionalmente. Ele faz parte de uma teoria maior chamada Teoria Quantitativa da Moeda (TQM). [↑](#footnote-ref-26)
26. A frequência com que uma unidade da moeda X é usada para comprar bens por Y unidade de tempo. Isso é um sinal do valor dessa moeda. [↑](#footnote-ref-27)
27. TradFi se refere a finanças tradicionais, em oposição a DeFi, que é finanças descentralizadas.  
     [↑](#footnote-ref-28)
28. Assista a esta aula online sobre Contratos Inteligentes Legais, apresentada por Wong Meng Weng em https://www.youtube.com/watch?v=1Fa\_2FXBAjA. [↑](#footnote-ref-29)
29. Sem a Netflix, você teria que:

    a) Checar quais filmes estão em cartaz no cinema,   
    b) Escolher um filme baseado nas limitadas opções disponíveis,   
    c) Checar os horários de cada sessão,  
    d) E pode ser que você não encontre o horário ou assento que você gostaria disponível. [↑](#footnote-ref-30)
30. A Economia teve início com Aristóteles no século IV a.C. como uma filosofia, fundamentada na teoria do valor e preços. No século XVI, Scruffi (Gasparo Scaruffi, L'Alitinonfo (Reggio, Emilia, Itália: Hercoliano Bartoli, 1582)) e Davanzanti (Bernardo Davanzati, Lezione Delle Monete (1588)) ampliaram a ciência com a teoria "metálica" do dinheiro, baseada na concepção geral de valor utilizada na época. Nos séculos XVII e XVIII, Montanari (Montanari, Geminiano e Filippo Argelati. Trattato Del Valore Delle Monete in Tutti Gli Stati. Publicado em Pars Tertia Del De Monetis Italiae. Milão, Itália: Stamperia della Regia Curia, 1750. Trattato del valore delle monete foi publicado postumamente por Argelati em “De monetis Italiae”) e Galiani (Galiani Ferdinando e Peter R Toscano. 1977 em “Money : A Translation of Della Moneta, Ann Arbor”. Publicado para o Departamento de Economia da Universidade de Chicago pela Universidade Internacional de Microfilmes.) escreveram sobre a teoria do dinheiro, superando substancialmente esses trabalhos anteriores.

    Então, Adam Smith, o pai da economia, escreveu sobre o fluxo circular da vida econômica. Embora ele seja provavelmente mais famoso por seu livro “A Riqueza das Nações” e o conceito de “a mão invisível”, ele também estava preocupado com o sentido econômico e a formulação do fenômeno da economia. Ele descobriu como cada período econômico se torna a base para o subsequente. Esse processo visava compreender fenômenos técnicos, observar o ciclo econômico, entender a causalidade econômica e obter insights sobre o funcionamento interno e as características gerais da economia. As perguntas que ele fez incluíam: “Como a produção acontece como um processo social?”, “Como a produção determina o consumo dos indivíduos?”, “Como o consumo determina mais produção?”, “Como cada ato de produção e consumo afeta cada outro ato de produção e consumo?” e “Como os elementos de energia econômica completam um caminho definido ano após ano sob a influência de forças motivadoras definidas?”.  
     [↑](#footnote-ref-31)
31. Existem algumas estratégias fiscais que intencionalmente resultam em perdas, mas isso está fora do escopo deste livro. [↑](#footnote-ref-32)
32. “Facebook–Cambridge Analytica Data Scandal”, Wikipedia (Wikimedia Foundation, 19 de novembro, 2022), https://en.wikipedia.org/wiki/Facebook%E2%80%93Cambridge\_Analytica\_data\_scandal.   
     [↑](#footnote-ref-33)
33. Pedro Fiuza/NurPhoto/Zuma Press, “Amazon Met with Startups about Investing, Then Launched Competing Products,” *The Wall Street Journal* (Dow Jones Company, 24 de julho, 2020), https://www.wsj.com/articles/amazon-tech-startup-echo-bezos-alexa-investment-fund-11595520249. [↑](#footnote-ref-34)
34. Se todos entendessem as externalidades de suas decisões, isso poderia dar informações muito úteis para decidir coletivamente a melhor maneira de gerenciar bens sociais. Exemplos são protocolos de código aberto e finanças descentralizadas. A chave para o sucesso é alinhar incentivos por meio da tokenização e ter uma governança adequada em vigor. Uma governança adequada implica poder suficiente, responsabilidade e capacidade para punir maus atores.

    Ao projetar sistemas tokenizados e descentralizados, podemos realinhar essas estruturas de incentivos e projetar mecanismos de governança adequados (tomada de decisão e punição). Igualdade de poder e pontos de partida iguais são difíceis de encontrar ou criar no mundo real. O mundo descentralizado e tokenizado oferece soluções para esses problemas. [↑](#footnote-ref-35)
35. Thanks to Alex Manuskin for the case study. You can read the thread here: <https://twitter.com/amanusk_/status/1313070958794727430> (Amanusk(.eth), “If You Are Not Yet Convinced That You Should Not Be Approving Infinite Tokens to Some Random Smart Contract/DAPP, Here's a Story of How Jhon Doe Lost $140k Worth of UNI in Their Sleep.1/👇 Pic.twitter.com/Qltkevnzdy,” Twitter (Twitter, October 5, 2020), https://twitter.com/amanusk\_/status/1313070958794727430.) [↑](#footnote-ref-36)
36. Investidores de VCs trabalham em empresas que levantam rodadas de investimento, coletam fundos, e investem de acordo com um mandato. [↑](#footnote-ref-37)
37. Investidores de varejo em cripto geralmente são investidores individuais ou usuários de protocolos. [↑](#footnote-ref-38)
38. Esta não é uma lista exaustiva de conceitos econômicos. Eu simplesmente escolhi sete dos mais importantes porque faz um bom título! [↑](#footnote-ref-39)
39. O termo “fossos econômicos” foi popularizado por Warren Buffet, e refere-se à habilidade de uma empresa de manter sua vantagem competitiva sobre os demais no mercado, referência aos fossos de proteção construídos antigamente ao redor de castelos. [↑](#footnote-ref-40)
40. Teorias da conspiração são complexas. No verão de 2020, a OMS teve que escrever um report para afirmar que a tecnologia 5G não era a causa do coronavírus, em uma tentativa de frear teorias da conspiração. Teorias da conspiração possuem efeitos de rede em termos de aceitação social. 2020 foi um ano muito estranho! [↑](#footnote-ref-41)
41. MVP significa produto mínimo viável. É o produto em sua forma mais básica e simples que ainda serve ao objetivo para o qual foi criado e pode ser vendido a um cliente. Outro conceito é o MVE, economia mínima viável: a economia mais básica necessária para construir esses modelos de token. [↑](#footnote-ref-42)
42. Realmente depende de como o banco central está estruturado. Nos EUA, o FED tem 12 bancos regionais da Reserva Federal. Nacionalmente, as políticas monetárias são aprovadas pelo conselho de 12 pessoas, sete membros do conselho e os 12 presidentes dos bancos regionais da Reserva Federal. Quando se trata de votação, apenas cinco dos 12 presidentes votam de cada vez. No Reino Unido, o Banco da Inglaterra é governado pelo Comitê de Política Monetária do banco, composto por nove pessoas. [↑](#footnote-ref-43)
43. NATIONAL BUREAU OF ECONOMIC RESEARCH. “Role of Direct and Indirect Taxes in the Federal Reserve System: A Conference Report of the NBER and the Brookings Institution”. Princeton University Press, 1964. http://www.jstor.org/stable/j.ctt183pv55. [↑](#footnote-ref-44)
44. EEA é a sigla para Ethereum Enterprise Association. Seu objetivo é ajudar organizações a adotarem e utilizarem a rede Ethereum. Saiba mais em <https://entethalliance.org>. [↑](#footnote-ref-45)
45. Isso é muito para um sistema operacional antigo. Windows XP foi lançado em 2001. Microsoft descontinuou suporte para o XP em abril de 2014. No Q4 2020, mais pessoas ainda utilizavam XP do que Windows 8 (0.54%) e Windows Vista (0.11%)! Dados de Novembro 2020 de <https://www.netmarketshare.com/operating-system-market-share.aspx>. [↑](#footnote-ref-46)
46. Pense nisso como a Apple recompensando os desenvolvedores de iOS por desenvolverem aplicativos para a App Store. A Ethereum Foundation é análoga a Apple; a blockchain da Ethereum é análoga ao iOS; os projetos da rede Ethereum são análogos ao aplicativos da App Store. [↑](#footnote-ref-47)
47. “Model Rules of Professional Conduct.” Americanbar.org. Acessado em 9 de dezembro, 2022. https://www.americanbar.org/groups/professional\_responsibility/publications/model\_rules\_of\_professional\_conduct/model\_rules\_of\_professional\_conduct\_table\_of\_contents/. [↑](#footnote-ref-48)
48. É impossível (hoje em dia) criar um contrato completo, seja legal ou programaticamente, que detalhe todos os possíveis resultados, então praticamente todos os contratos são incompletos. [↑](#footnote-ref-49)
49. Time, The Investopedia. “What Is the Prisoner's Dilemma and How Does It Work?” Investopedia. Investopedia, 13 de setembro, 2022. https://www.investopedia.com/terms/p/prisoners-dilemma.asp#:~:text=A%20prisoner's%20dilemma%20is%20a,many%20aspects%20of%20the%20economy.  
     [↑](#footnote-ref-50)
50. SchellingCoin foi discutido pela primeira vez em 2014 por Vitalik Buterin ("Schellingcoin: A Minimal-Trust Universal Data Feed," Ethereum Foundation Blog, acessado em 9 de dezembro de 2022), https://blog.ethereum.org/2014/03/28/schellingcoin-a-minimal-trust-universal-data-feed/ [↑](#footnote-ref-51)
51. Tayfun SÖnmez and Utku M. Ünver, “Market Design for Kidney Exchange,” *The Handbook of Market Design*, 2013, pp. 92-137, https://doi.org/10.1093/acprof:oso/9780199570515.003.0005.  
     [↑](#footnote-ref-52)
52. Peter Coles et al., “The Job Market for New Economists: A Market Design Perspective,” *Journal of Economic Perspectives* 24, no. 4 (January 2010): pp. 187-206, https://doi.org/10.1257/jep.24.4.187. [↑](#footnote-ref-53)
53. Atila Abdulkadiroğlu and Tayfun Sönmez, “School Choice: A Mechanism Design Approach,” *American Economic Review* 93, no. 3 (Janeiro 2003): pp. 729-747, https://doi.org/10.1257/000282803322157061.  
     [↑](#footnote-ref-54)
54. Alvin E. Roth, “The Economist as Engineer: Game Theory, Experimentation, and Computation as Tools for Design Economics”, *Econometrica* 70, no. 4 (2002): pp. 1341-1378, https://doi.org/10.1111/1468-0262.00335. [↑](#footnote-ref-55)
55. Alvin E. Roth, “What Have We Learned from Market Design?,” *Innovation Policy and the Economy* 9 (2009): pp. 79-112, https://doi.org/10.1086/592422. [↑](#footnote-ref-56)
56. Uma prática de criptografia de dados usada por organizações para garantir uma resposta rápida a uma ameaça criptográfica.  
     [↑](#footnote-ref-57)
57. Isso pode ser útil para combater negociações de front-running (refere-se à prática de uma pessoa ou empresa realizar uma negociação antes de uma grande ordem conhecida ser executada, para obter lucro com a movimentação de preços que a ordem pode causar). [↑](#footnote-ref-58)
58. Alvin E. Roth, Repugnance as a Constraint on Markets (Boston, Mass: Division of Research, Harvard Business School, 2007) é o título de um artigo escrito por Alvin E. Roth que discute como os mercados podem ser afetados por questões morais e culturais que podem criar barreiras para a sua eficiência. [↑](#footnote-ref-59)
59. Schaffer, F. C., & Schedler, A. (2005). “*What is vote buying? The limits of the market model”*. In “*Poverty, Democracy, and Clientelism: The Political Economy of Vote Buying”.* Universidadede Stanford, Departamento de Ciências Políticas, Bellagio Center, Rockefeller Foundation, 28 de novembro – 2 de dezembro, 2005*.* [↑](#footnote-ref-60)
60. Os hackers white hat são hackers éticos. Eles são especialistas em segurança cibernética que testam a segurança de um sistema. Eles não invadem o sistema para explorá-lo e obter benefícios. Eles têm permissão para invadir o sistema e testar o quão seguro ele é. [↑](#footnote-ref-61)
61. White label se refere a produtos que são vendidos com marca própria, mas produzidos por terceiros. [↑](#footnote-ref-62)
62. Cover Protocol vende seguros para basicamente qualquer coisa, além de contratos inteligentes e cripto. O protocolo base utilizado é o da Nexus Mutual. [↑](#footnote-ref-63)
63. Capital Mínimo Requerido serve como aproximação para quantificar a alavancagem no protocolo Nexus Mutual. [↑](#footnote-ref-64)
64. Dilip Mookherjee, “The 2007 Nobel Memorial Prize in Mechanism Design Theory,” *Scandinavian Journal of Economics* 110, no. 2 (2008): pp. 237-260, https://doi.org/10.1111/j.1467-9442.2008.00535.x. [↑](#footnote-ref-65)
65. “2007 Leonid Hurwicz, Eric S. Maskin e Roger B. Myerson,” *Nobel Lectures in Economic Sciences (2006–2010)*, 2014, pp. 71-141, https://doi.org/10.1142/9789814635585\_0002. [↑](#footnote-ref-66)
66. Ross, Stephen A. “The Economic Theory of Agency: The Principal’s Problem.” *The American Economic Review* 63, no. 2 (1973): 134–39. <http://www.jstor.org/stable/1817064>. [↑](#footnote-ref-67)
67. P. A. Samuelson, “Reaffirming the Existence of ‘Reasonable’ Bergson-Samuelson Social Welfare Functions,” *Economica* 44, no. 173 (1977): p. 81, https://doi.org/10.2307/2553553. [↑](#footnote-ref-68)
68. Justiça é uma palavra simples, mas com muito peso, e sua definição não é simples de determinar. O que é justo para um, pode não ser para outro. Justiça por inteligência artificial é dependente em quem a construiu e que dados foram fornecidos. Por isso, justiça nesse contexto é um termo em evolução. Conceito de justiça pode mudar dependendo dos usuários e participantes no ecossistema. É importante entender quem é a entidade responsável por definir o que é justo. Nesse contexto, tokens de governança podem ser muito úteis, capturando o valor de decisão da “justiça” em um ambiente de token. [↑](#footnote-ref-69)
69. Samuelson, P. A. (1977). Ibid. [↑](#footnote-ref-70)
70. Existem também algoritmos de contratos não-inteligentes que pertencem especificamente a mecanismos automatizados, comportamentos, estrutura etc. Um exemplo é a Zapier.com, solução de Web2. Em breve soluções como essa estarão disponíveis na Web3. [↑](#footnote-ref-71)
71. Varian, Hal R. e MacKie-Mason, Jeffrey K., Generalized Vickrey Auctions (1994). Disponível em SSRN: https://ssrn.com/abstract=975873 ou http://dx.doi.org/10.2139/ssrn.975873. [↑](#footnote-ref-72)
72. “Currency Re-Imagined for the World: Multi-Collateral Dai Is Live!,” MakerDAO Blog, acessado em 9 de dezembro, 2022, https://blog.makerdao.com/multi-collateral-$DAI-is-live/. [↑](#footnote-ref-73)
73. No segundo trimestre de 2020, os tokens de governança se tornaram uma das funções de token mais populares para tokens nativos. Eles servem à filosofia de um ecossistema descentralizado, governado e de propriedade da comunidade. Embora a narrativa seja importante, também é importante adicionar o mecanismo de incentivo e a função de governança no design do token, ou seja, como as decisões são determinadas, como os votos são avaliados e como garantir um nível de governança que seja considerado suficientemente "descentralizado". [↑](#footnote-ref-74)
74. O evento permitiu que a MakerDAO testasse seu sistema em tempos de grandes variações de preço, ao mesmo tempo em que testava a robustez do protocolo. Como resultado desse evento, foram feitas melhorias no mecanismo de governança. Especificamente, foi criado um portfólio de colaterais mais diversificado, um processo de governança estruturado (máquinas), resposta versátil (humanos) e melhorias no papel de Keeper no sistema de governança. ("The Market Collapse of March 12-13, 2020: How It Impacted MakerDAO," MakerDAO Blog, acessado em 9 de dezembro de 2022, https://blog.makerdao.com/the-market-collapse-of-march-12-2020-how-it-impacted-makerdao/). [↑](#footnote-ref-75)
75. A crise de 12 de março de 2020 destacou algumas limitações do ecossistema de Keepers. Durante o colapso do mercado, os bots de Keepers tiveram dificuldade em acessar fundos para fins de liquidez e alguns não puderam participar dos leilões. [↑](#footnote-ref-76)
76. No mundo DeFi, empréstimos em sua grande maioria (ou totalidade, dependendo do conjunto de protocolos) exigem o comprometimento de mais de 100% do valor do empréstimo em colaterais – “super colateralizado”. [↑](#footnote-ref-77)
77. Para mais informações, acesse https://forum.makerdao.com/c/oracles/13. [↑](#footnote-ref-78)
78. "MakerDAO aprova 4 novos feeds de dados leves para Oracles," MakerDAO Blog, acessado em 9 de dezembro de 2022, https://blog.makerdao.com/makerdao-approves-4-new-light-feeds-for-oracles/. [↑](#footnote-ref-79)
79. "Enquetes de Governança: Implementação PSM, Nomeação da Argent como Feed de Dados Leves de Oracle, e Mais," MakerDAO Blog, acessado em 9 de dezembro de 2022, https://blog.makerdao.com/governance-polls-psm-implementation-appoint-argent-as-an-oracle-light-feed-and-more/. [↑](#footnote-ref-80)
80. "Blog MakerDAO", MakerDAO Blog (blog) (Maker Foundation, 3 de setembro de 2019), https://blog.makerdao.com/introducing-oracles-v2-and-defi-feeds/. [↑](#footnote-ref-81)
81. Catalini, Christian e Gans, Joshua S., Ofertas Iniciais de Moedas e o Valor dos Tokens Cripto (5 de março de 2019). MIT Sloan Research Paper No. 5347-18, Rotman School of Management Working Paper No. 3137213, Disponível em SSRN: https://ssrn.com/abstract=3137213 ou http://dx.doi.org/10.2139/ssrn.3137213. [↑](#footnote-ref-82)
82. Lisa JY Tan, "Bancor Token Economics Paper" é um documento que discute os aspectos econômicos do token Bancor. O documento foi escrito por Lisa JY Tan e publicado pela Economics Design em 2019. Ele está disponível online em https://econteric.com/wp-content/uploads/2021/06/Bancor-Protocol-Token-Economics-Paper.pdf. [↑](#footnote-ref-83)
83. Lisa JY Tan, "MakerDAO Token Economics Paper" (Economics Design, setembro de 2019), https://econteric.com/wp-content/uploads/2021/06/MakerDAO-Token-Economics-Paper.pdf. [↑](#footnote-ref-84)
84. Leia “Caixa 2: Estudo de Caso Sobre Moedas (Dinheiro) Digitais”. [↑](#footnote-ref-85)
85. Esses são modelos criados e analisados por dois artigos diferentes (Catalini e Gans [2018] ibid e Lin William Cong, Ye Li, Neng Wang, “Tokenomics: Dynamic Adoption and Valuation, The Review of Financial Studies, Volume 34, Issue 3”, março 2021, páginas 1105–1155, https://doi.org/10.1093/rfs/hhaa089) que explanam sobre o valor de tokens de utilidade. [↑](#footnote-ref-86)
86. Trent McConaghy usa um sistema TCR de várias camadas para aumentar gradualmente os direitos e responsabilidades dos usuários à medida que adicionam mais participação. Isso contribui para uma camada mais diversa na governança (design de mecanismos) em relação à tomada de decisões, controle de acesso, reputação e resolução (Trent McConaghy, Dimitri de Jonghe e Fang Gong, "Ocean Protocol Blog", Ocean Protocol Blog (blog) (Ocean Protocol, 1 de maio de 2018), https://blog.oceanprotocol.com/the-layered-tcr-56cc5b4cdc45.). [↑](#footnote-ref-87)
87. As taxas de câmbio fixas não precisam ser uma relação de 1:1. Elas podem ser uma relação de 1:0.725, por exemplo, dependendo da instituição que governa a política monetária. [↑](#footnote-ref-88)
88. Isso pode envolver mais do que duas variáveis, mas nos ateremos a modelos simples de duas variáveis, já que é possível representá-los graficamente em um gráfico 2D. Quanto mais variáveis forem adicionadas, mais dimensões serão necessárias. Por exemplo, uma curva de bonding de três variáveis requer um gráfico 3D para visualização. [↑](#footnote-ref-89)
89. DEX é um acrônimo de "decentralized exchange" ou "corretora descentralizada". Uma corretora descentralizada não é de propriedade ou controlada por uma entidade central. [↑](#footnote-ref-90)
90. Embora a maioria das pessoas pense em uma curva de ligação como uma função 2D, as curvas de ligação também podem ser funções 3D. Elas também podem ser usadas para facilitar a negociação sem dinheiro (por exemplo, usando uma curva de ligação para determinar a relação entre o volume de upload e o volume de download no BitTorrent). Em um mercado de conteúdo de código aberto, elas podem facilitar a troca de volume de informações sem dinheiro. [↑](#footnote-ref-91)
91. Quando o preço de um NFT aumenta, a demanda pela propriedade intelectual aumenta. A propriedade intelectual é assim selecionada por meio do sinalização de preço através do NFT. [↑](#footnote-ref-92)
92. Experimente várias funções e parâmetros aqui: <http://bit.ly/bondingcurve>. [↑](#footnote-ref-93)
93. O princípio da conservação é um princípio da física, onde a fórmula de conservação de energia (K1 + U1 = K2 + U2) está sujeita a uma função invariante constante. [↑](#footnote-ref-94)
94. Confira https://medium.com/giveth/deep-dive-augmented-bonding-curves-3f1f7c1fa751 para o design do sistema, fluxo e matemática por trás. [↑](#footnote-ref-95)
95. Confira https://tokeneconomy.co/dynamic-token-bonding-curves-41d36e43befa para um estudo de caso e função matemática. [↑](#footnote-ref-96)
96. A liquidez contínua é quando um token pode ser convertido em outro token a qualquer momento. Isso não requer que outra pessoa compre ou venda o token, ele pode ser convertido (liquidado) a qualquer momento.  
     [↑](#footnote-ref-97)
97. Um contrato inteligente é um programa de software simples que, uma vez submetido à uma blockchain, é executado de forma inalterada pelo tempo que a blockchain subjacente permanecer operacional. Os contratos inteligentes têm muitas das mesmas capacidades que as blockchains padrões (por exemplo, podem invocar outros contratos inteligentes e manter saldos de tokens em garantia). Um contrato inteligente bem estruturado pode ser visto como um intermediário confiável, incorruptível e totalmente automatizado. [↑](#footnote-ref-98)
98. Um denominador comum é uma característica comum que existe em uma rede. Por exemplo, a maioria dos bancos centrais do mundo possui dólares americanos em suas reservas. Isso torna o dólar americano um denominador comum entre muitos bancos centrais. Ter um denominador comum facilita a correspondência entre as partes. [↑](#footnote-ref-99)
99. A liquidez cruzada é a capacidade de converter um token de uma blockchain para um token em outra blockchain. A capacidade de converter $DAI, um token baseado em Ethereum, para LEO, que é um token baseado em EOS, é um exemplo de liquidez cruzada [↑](#footnote-ref-100)
100. The transitive property of equality means that if a is equal to b, and b is equal to c, then a is equal to c. This property can be used to simplify mathematical expressions and proofs. [↑](#footnote-ref-101)
101. Um formador de mercado autônomo é um programa que compra e vende continuamente tokens de acordo com os preços algorítmicos. Ele substitui os livros de ordens por código e ajuda na precificação de tokens. [↑](#footnote-ref-102)
102. Negociações ocorrem quando o mercado (corretora) encontra um comprador e um vendedor, e eles engajam em uma troca de bens (ou tokens). Isso será difícil quando houver falta de compradores e vendedores para bens (ou tokens) específicos. Essa falta de comprador ou vendedor causa baixa liquidez. [↑](#footnote-ref-103)
103. TradFi não chama esses agentes de mercado de "Formadores de Mercado Manuais", apenas de "Formadores de Mercado". Mas para fins de clareza, nós os chamaremos de " Formadores de Mercado Tradicionais" para diferenciá-los dos " Formadores de Mercado Automatizados".  
      [↑](#footnote-ref-104)
104. Tokens LP representam uma porção da pool de liquidez (ou reserva). [↑](#footnote-ref-105)
105. Outros termos incluem taxa de reserva constante, taxa de reserva fracionária e peso do conector. [↑](#footnote-ref-106)
106. Vide Capítulo 11 para aprender mais sobre curvas de ligação. [↑](#footnote-ref-107)
107. Isso pode ser uma instituição, fundação do token de reserva, um grupo de pessoas ou um indivíduo. [↑](#footnote-ref-108)
108. Apurado em Outubro 2020. [↑](#footnote-ref-109)
109. Aputado conforme lançamento da Bancor de 2017 (Stan Higgins, Alex Sunnarborg, e Pete Rizzo, “$150 Million: Tim Draper-Backed Bancor Completes Largest-Ever ICO,” *CoinDesk* (CoinDesk, 12 de junho, 2017), https://www.coindesk.com/150-million-tim-draper-backed-bancor-completes-largest-ever-ico.) [↑](#footnote-ref-110)
110. Detalhes sobre a fórmula de conversão podem ser encontrados em http://meissereconomics.com/assets/abfe-lesson5-bancor.pdf (Meni Rosenfeld, “Formulas for Bancor System” (Meisser Economics, 11 de junho, 2017), http://meissereconomics.com/assets/abfe-lesson5-bancor.pdf.). [↑](#footnote-ref-111)
111. A flexibilidade nos pesos das proporções de reserva torna-se mais útil à medida que o sistema evolui, especialmente quando o mundo adota totalmente a Web3. [↑](#footnote-ref-112)
112. A reserva fracionária permite a flexibilidade de mudar o peso da troca. Isso permite que o sistema integre preços de outros mercados secundários para determinar o valor dos tokens e reduzir as perdas impermanentes. No entanto, devido ao atraso do sistema, isso permite que os exploradores de arbitragem obtenham lucro às custas dos provedores de liquidez até que os preços atinjam o equilíbrio. Assim, até que a Web 3.0 resolva isso, o peso permanecerá em um peso fixo de 0.5. [↑](#footnote-ref-113)
113. Veja <https://sweetbridge.com> para aprender mais sobre o projeto. [↑](#footnote-ref-114)
114. A premissa de y=1 nesse caso assume que o “produto” é um serviço de software, e que o usuário está comprando acesso ao sistema. Por isso, a quantidade comprada é exatamente 1. [↑](#footnote-ref-115)
115. Este modelo ainda está sendo discutido e explorado. Acompanhe a conversa aqui https://github.com/ethereum-funding/blockrewardsfunding/issues/39. [↑](#footnote-ref-116)
116. Embora a maioria das blockchains seja um livro razão imutável, incluindo os smart contracts nela, que não podem ser alterados uma vez que são "lançados". No entanto, os smart contracts podem ser atualizados, como o que o Uniswap fez da v1 para a v2 e agora a v3. Até corrigir um bug pode ser considerado uma atualização. Por favor, consulte aqui para obter mais informações: https://docs.openzeppelin.com/learn/upgrading-smart-contracts. [↑](#footnote-ref-117)
117. Esse não é um token real, mas apenas um exemplo. [↑](#footnote-ref-118)
118. Em alguns casos, os protocolos DeFi ainda podem ser restritos por regulamentações governamentais, especialmente no caso de tokens de valores mobiliários (security tokens). [↑](#footnote-ref-119)
119. Adith Podhar, Kamini Shivalkar, e Et Contributors, “Why DeFi Is the Biggest Thing in the History of Finance,” *Economic Times* (India Times, 2 de fevereiro, 2022), https://economictimes.indiatimes.com/markets/cryptocurrency/why-defi-is-the-biggest-thing-in-the-history-of-finance/articleshow/89745980.cms.  
      [↑](#footnote-ref-120)
120. John C. Coates, “The Future of Corporate Governance Part I: The Problem of Twelve,” *SSRN Electronic Journal*, 2018, https://doi.org/10.2139/ssrn.3247337. [↑](#footnote-ref-121)
121. Nota: O Bitcoin ocupa um lugar interessante nesse ecossistema, já que a tecnologia que alimenta o Bitcoin como rede é a base para o ecossistema DeFi, mas ele também é um protocolo de moeda financeira, como ETH e outros. [↑](#footnote-ref-122)
122. https://openai.com/api/ [↑](#footnote-ref-123)
123. Recursos intangíveis da Web3 têm algumas características diferentes de outros recursos intangíveis. [↑](#footnote-ref-124)
124. Não confundir com a "antiga" Web3 cunhada por Tim Berners-Lee, que previu um estado da tecnologia da web que teria padrões de metadados formais para permitir operações máquina-a-máquina, o que por sua vez permitiria uma compreensão semântica padronizada da máquina de dados na web. [↑](#footnote-ref-125)
125. Meredith McFadden, “Tragedy of the Commons in Cape Town's Water Crisis,” Prindle Institute (The Prindle Post e The Janet Prindle Institute for Ethics da Universidade DePauw, 2018), https://www.prindleinstitute.org/2018/02/tragedy-commons-cape-towns-water-crisis/. [↑](#footnote-ref-126)
126. Brian Depew, “Water: Overcoming a Tragedy of the Commons,” Center for Rural Affairs (Center for Rural Affairs, 22 de outubro, 2013), https://web.archive.org/web/20200927040338/https://www.cfra.org/news/131022/water-overcoming-tragedy-commons. [↑](#footnote-ref-127)
127. Tokens são geralmente meios de troca para a compartilhamento de informações e dados entre usuários, enquanto o Ethereum ($ETH) é um meio de troca entre protocolos. [↑](#footnote-ref-128)
128. Esse é um exemplo bastante simplificado. Na realidade, não é uma relação de 1-para-1. [↑](#footnote-ref-129)
129. 129 “OTC Derivatives Statistics at End-December 2019,” The Bank for International Settlements (The Bank for International Settlements, 7 de maio, 2020), https://www.bis.org/publ/otc\_hy2005.htm. [↑](#footnote-ref-130)
130. FOMO significa “Fear of Missing Out”, que significa o medo de ficar de fora de um movimento de alta de preços ou outras especulações. [↑](#footnote-ref-131)
131. Portanto, você deve sempre estar ciente das informações compartilhadas e sempre fazer pesquisas. Não acredite apenas nas palavras de estranhos online.  
      [↑](#footnote-ref-132)
132. Sempre verifique os endereços dos tokens ao realizar transações. A Uniswap lembra aos usuários para conferirem o endereço do token antes de realizarem qualquer transação.  
      [↑](#footnote-ref-133)
133. Imagine que a Meta diga que seus livros estão limpos porque eles auditaram seus próprios livros. Isso seria suspeito. Nestes protocolos, a auditoria está no contrato inteligente. Quando afirmam que o código foi auditado, certifique-se de verificar quem o auditou e quando. [↑](#footnote-ref-134)
134. Lainà Patrizio, “Proposals for Full-Reserve Banking: A Historical Survey from David Ricardo to Martin Wolf”, *Economic Thought* 4, no. 2 (28 de setembro, 2015). [↑](#footnote-ref-135)
135. A última vez que vimos um banco com reserva total em ação foi no século XIX. À medida que o mercado de capitais e o mercado financeiro tradicional amadurecem, sistema bancário também mudou e evoluiu. Hoje em dia, a maioria dos bancos tem reservas baixas ou nenhuma reserva para respaldar seus empréstimos. Em DeFi, a maioria das moedas privadas emitidas na rede com uma paridade com o dinheiro fiduciário são “sobrecolateralizadas”. Depois da crise financeira global de 2008, muitos economistas começaram a brincar com a ideia de um banco de reserva total novamente. Embora seja desafiador implementar um banco de reserva total nos bancos (especialmente em 2020), é possível implementá-lo em DeFi. [↑](#footnote-ref-136)
136. Um preço perfeito agrega todas as informações do mercado, mas não inclui especulação. [↑](#footnote-ref-137)
137. Julia Belluz, “Food Companies Distort Nutrition Science. Here's How to Stop Them.”, Vox (Vox Media, 21 de abril, 2016), https://www.vox.com/2016/3/3/11148422/food-science-nutrition-research-bias-conflict-interest. [↑](#footnote-ref-138)
138. Conforme dados de Outubro 2020. [↑](#footnote-ref-139)
139. Ordens de stop-loss são ordens de compra ou venda de investimentos específicos quando atingem certo preço. [↑](#footnote-ref-140)
140. O ativo é transferido para o nome do comprador, em oposição à liquidação em dinheiro, que entrega a diferença entre o preço à vista no dia da liquidação e o preço do contrato do derivativo que está sendo negociado.  
      [↑](#footnote-ref-141)
141. Repo significa acordo de recompra. É uma taxa de empréstimo de curto prazo entre atores institucionais como bancos e bancos centrais. Pense nisso como empréstimos, mas para bancos em vez de pessoas físicas como você e eu. [↑](#footnote-ref-142)
142. Ao reescrever esse livro, fiquei com um sentimento engraçado por ver a realidade de preços há apenas alguns anos atrás. Como os valores não fazem diferença para o racional do exemplo, deixei como estava originalmente pela nostalgia.   
      [↑](#footnote-ref-143)
143. A atribuição varia desde a Espada de Dâmocles, o Comité de Salut Public, Voltaire, Lord Melbourne, Ulysses S. Grant e o Princípio Peter Parker ("Com Grandes Poderes Vem Grandes Responsabilidades", Wikipedia (Wikimedia Foundation, 12 de novembro de 2022), https://en.wikipedia.org/wiki/With\_great\_power\_comes\_great\_responsibility.) [↑](#footnote-ref-144)
144. Polkastarter (https://www.polkastarter.com) é uma plataforma que se autodescreve como "Empoderando projetos Web3 a lançar pools de token descentralizados e de troca fixa. Permitindo que patrocinadores garantam investimentos em IDOs, NFTs e jogos em um ambiente multi-chain seguro nas redes Ethereum, BNB Chain, Polygon, Celo e Avalanche. [↑](#footnote-ref-145)
145. Esses projetos e estratégias existem, ou pelo menos existiam, quando o livro estava sendo pesquisado e escrito. [↑](#footnote-ref-146)
146. Um "pop" de IPO é uma situação em que o valor das ações aumenta quando as ações são listadas em uma bolsa de valores. Compradores precoces da ação podem lucrar com essa negociação. Por exemplo, o preço da nCINO aumentou 195 por cento após a listagem na NASDAQ (NCNO) em julho de 2020. O Baidu foi o maior "pop" de IPO na NASDAQ em 2005, com um aumento de preço de 354 por cento no primeiro dia (Renaissance Capital, “NCINO Jumps 195% in Biggest IPO Pop for a US Tech Company since the Internet Bubble”, Nasdaq (Nasdaq, Inc, 15 de junho, 2020), https://www.nasdaq.com/articles/ncino-jumps-195-in-biggest-ipo-pop-for-a-us-tech-company-since-the-internet-bubble-2020-07). [↑](#footnote-ref-147)
147. A 13a queima trimestral ocorreu em outubro de 2020, conforme relatado no anúncio da Binance intitulado "Binance Completes 13th Quarterly BNB Burn" em seu site: https://www.binance.com/en/support/announcement/4db101d45b204c3a9206c057f0f6856a. [↑](#footnote-ref-148)
148. Exemplo de token. Até o quarto trimestre de 2020, esse token não existia. [↑](#footnote-ref-149)
149. Trata-se de melhorar os experimentos em vez de buscar a perfeição. É comum nos concentrarmos em encontrar o melhor mecanismo, ou “perfeito”. A realidade é que tais mecanismos evoluem continuamente. Devemos nos concentrar em experimentos em vez de perfeição. [↑](#footnote-ref-150)
150. Os direitos de propriedade são um componente na arquitetura do token. E no caso específico do NFT $EDBK, o direito de propriedade de possuir $EDBK é a capacidade de distribuir e revender o livro físico. [↑](#footnote-ref-151)