CAMPBELL R. **HARVEY**
ASHWIN **RAMACHANDRAN**
JOEY **SANTORO**

DeFi e o Futuro *das* Finanças

Prólogo de **FRED EHRSAM**
Cofundador da Paradigm e da Coinbase

Prefácio de **VITALIK BUTERIN**
Cofundador da Ethereum

ALTA BOOKS
EDITORA
Rio de Janeiro, 2023

SUMÁRIO

Prólogo **IX**

Prefácio **XI**

I. Introdução **1**
Cinco Problemas-Chave Para Os Sistemas Financeiros Centralizados 2
Implicações 6

II. As Origens Da Descentralização Financeira Moderna **9**
Uma Rápida História Das Finanças 9
Fintech 11
Bitcoin E Criptomoedas 13
Ethereum E O Defi 16

III. Infraestrutura Defi **19**
Blockchain 19
Criptomoedas 21
A Plataforma De Contratos Inteligentes 22
Oracles 24
Stablecoins 25
Aplicativos Descentralizados 28

IV. Fundamentos Do Defi **29**
Transações 29
Tokens Fungíveis 32
Tokens Não Fungíveis 37
Custódia 39
Ajuste De Fornecimento 40
Incentivos 46
Swap 50
Empréstimos Com Garantia 54
Empréstimos Flash (Sem Garantia) 56

V. Problemas Que O Defi Resolve **59**
Ineficiência 59
Acesso Limitado 61
Opacidade 64
Controle Centralizado 65
Falta De Interoperabilidade 66

VI. Defi Avançado **71**
Crédito/Empréstimo 72
Exchanges Descentralizadas 95
Derivativos 105
Tokenização 122

VII. Riscos **129**
Risco Do Contrato Inteligente 130
Risco Oracle 135
Risco De Escala 137
Risco De Dex 140

Risco De Custódia 143
Risco Ambiental 145
Risco Regulatório 146

VIII. Conclusões: Perdedores E Ganhadores 149

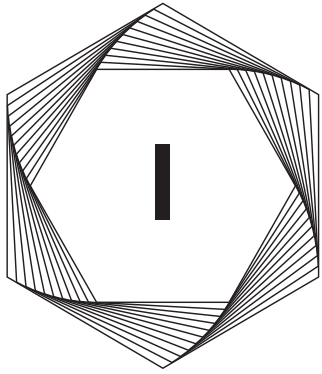
Agradecimentos 153

Referências 155

Glossário 157

Notas 173
Capítulo I 173
Capítulo Ii 174
Capítulo Iii 175
Capítulo Iv 177
Capítulo Vi 179
Capítulo Vii 184
Capítulo Viii 188

Índice 189



INTRODUÇÃO

Temos um círculo completo. A primeira forma de negócio no mercado consistia de uma permuta entre as partes envolvidas; isso também era conhecido como escambo.[1] A troca era altamente ineficiente porque oferta e demanda tinham que ser combinadas de maneira exata entre os pares. Para resolver o problema de combinar, o dinheiro foi introduzido como um meio de troca e reserva de valor. Os tipos iniciais de dinheiro não eram centralizados. Os agentes aceitavam qualquer número de itens, como pedras ou conchas, em troca de bens. Até que, por fim, o dinheiro em espécie surgiu, uma forma na qual a moeda tinha um valor tangível. Hoje temos moeda sem garantia (fiduciária) controlada pelos bancos centrais. A forma do dinheiro mudou com o tempo, mas a infraestrutura básica das instituições financeiras não.

No entanto, o caminho adiante está apontando para uma ruptura histórica de nossa atual infraestrutura financeira. O DeFi, ou finanças descentralizadas, busca construir e combinar blocos de construção financeiros de código aberto em produtos sofisticados com atrito minimizado e valor maximizado para os usuários que utilizam a tecnologia blockchain. Dado que não custa mais fornecer serviços para um cliente com US$100 ou US$100 milhões em ativos, acreditamos que o DeFi substituirá, no futuro, toda a infraestrutura financeira centralizada significativa. Essa é uma tecnologia de inclusão pela qual qualquer pessoa pode pagar a taxa fixa para usar e se beneficiar das inovações do DeFi.

O DeFi é fundamentalmente um mercado competitivo de aplicativos financeiros descentralizados que funcionam como vários fundamentos financeiros, tais como trocar, salvar, emprestar e tokenizar. Esses aplicativos se beneficiam dos efeitos de rede de combinar e recombinar produtos de DeFi e atrair cada vez mais participação de mercado do ecossistema financeiro tradicional.

Nosso livro detalha os problemas que o DeFi resolve: **controle centralizado, acesso limitado, ineficiência, falta de interoperabilidade** e **opacidade**. Em seguida, descrevemos o cenário de DeFi atual e de rápido crescimento e apresentamos uma visão das oportunidades futuras que o DeFi abre. Comecemos pelos problemas.

CINCO PROBLEMAS-CHAVE PARA OS SISTEMAS FINANCEIROS CENTRALIZADOS

Durante séculos, vivemos em um mundo de finanças centralizadas. Os bancos centrais controlam o suprimento de dinheiro. Negócios financeiros são feitos amplamente via intermediários.

Os empréstimos são realizados por meio de instituições bancárias tradicionais. Nos últimos cinco anos, no entanto, progressos consideráveis têm sido feitos em um modelo bem diferente: a descentralização financeira. Nessa estrutura, os pares interagem entre si por meio de um registro comum não controlado por nenhuma organização centralizada. O DeFi oferece um potencial considerável para resolver os cinco problemas-chave a seguir, associados com a centralização financeira: controle centralizado, acesso limitado, ineficiência, falta de interoperabilidade e opacidade.

1. ***Controle Centralizado***. A centralização tem muitas camadas. A maioria dos consumidores e empresas lida com um banco único, localizado, que controla impostos e taxas. A troca é possível, mas pode ser cara. Além disso, o sistema bancário dos EUA é altamente concentrado. Os quatro maiores bancos têm uma participação de 44% dos depósitos segurados, em comparação com os 15% de 1984.[2] Curiosamente, o sistema bancário dos EUA é menos concentrado do que em outros países, como o Reino Unido ou o Canadá. Em um sistema bancário centralizado, uma entidade consolidada tenta definir taxas de juros de curto prazo e influenciar a taxa de inflação.

   Esse fenômeno vai além do setor financeiro legado para protagonistas da tecnologia, como Amazon, Facebook e Google, que agora dominam setores como vendas no varejo e publicidade digital.

2. ***Acesso Limitado***. Hoje, 1,7 bilhão de pessoas não têm conta bancária, o que torna muito desafiador para elas obter empréstimos e operar no mundo do comércio pela internet. Além disso, muitos consumidores devem recorrer a operações de empréstimo consignado para cobrir

deficiências de liquidez. Estar no banco, no entanto, não garante o acesso. Por exemplo, um banco pode não querer se preocupar com o pequeno empréstimo que um novo negócio exige. Em vez disso, pode sugerir um financiamento com cartão de crédito, que traz consigo uma taxa de juros bem acima de 20% ao ano — uma alta barreira de dificuldade para encontrar projetos de investimentos rentáveis.

3. ***Ineficiência***. Um sistema financeiro centralizado tem muitas ineficiências. Talvez o exemplo mais flagrante seja a taxa das operadoras de cartão de crédito, que faz com que consumidores e pequenas empresas percam até 3% do valor de uma transação cada vez que passam o cartão, devido ao poder de precificação do oligopólio da rede de pagamento. As taxas de remessa estão entre 5% e 7%. O tempo também é desperdiçado nos dois dias necessários para "liquidar" uma transação de ações (transferir oficialmente a propriedade). Na Era da Internet, isso parece totalmente implausível. Outras ineficiências incluem transferências caras (e lentas) de fundos, taxas de corretagem diretas e indiretas, falta de segurança e a incapacidade de realizar microtransações, muitas das quais não são óbvias para os usuários. No sistema bancário atual, as taxas de juros dos depósitos permanecem muito baixas, e as taxas de empréstimos, altas, porque os bancos precisam cobrir seus custos físicos. Outro bom exemplo é a área de seguros.

4. ***Falta de Interoperabilidade***. Os consumidores e as empresas lidam com instituições financeiras em um ambiente que bloqueia a interconectividade. É notório que o sistema financeiro dos EUA é isolado e projetado para sustentar

altos custos de mudança. Mover o dinheiro de uma instituição para outra pode ser excessivamente demorado e complicado. Por exemplo, uma transferência eletrônica pode levar três dias para ser concluída.

Na tentativa de mitigar esse problema dentro do mundo das finanças centralizadas, em 2019 a Visa tentou adquirir a Plaid,[3] um produto que permite a qualquer empresa se conectar à pilha de informações de uma instituição com a permissão do usuário. Embora tenha sido um movimento estratégico para ajudar a Visa a ganhar algum tempo, não abordou os problemas fundamentais com a infraestrutura financeira atual.

5. ***Opacidade***. O sistema financeiro atual não é transparente. Os clientes dos bancos têm muito poucas informações sobre a saúde financeira de seus bancos e, em vez disso, devem confiar na proteção limitada do governo do seguro FDIC [seu equivalente no Brasil é o FGC — Fundo Garantidor de Créditos] em seus depósitos. Além disso, é difícil para eles saber se a taxa que lhes é oferecida em um empréstimo é competitiva. Embora o setor de seguros ao consumidor tenha feito algum progresso com serviços de fintech que se oferecem para encontrar o preço "mais baixo", o mercado de empréstimos é muito fragmentado, mas, ainda assim, todos os credores concorrentes sofrem com as ineficiências do sistema. O resultado é que o preço mais baixo ainda reflete o legado das lojas físicas tradicionais e dos custos inchados de back-office.

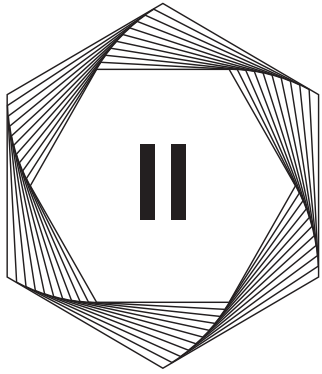
IMPLICAÇÕES

As implicações desses cinco problemas são duplas. Primeiro, muitos desses custos levam a um *crescimento econômico mais baixo*. Por exemplo, se as taxas de empréstimo forem altas devido a custos legados, projetos de investimento de alta qualidade podem ser abandonados, conforme explicado anteriormente. Uma ideia de alta qualidade de um empreendedor pode atingir uma taxa de retorno de 20% — precisamente o tipo de projeto que acelera o crescimento econômico. Se o banco disser ao empreendedor para pedir dinheiro emprestado em seu cartão de crédito a 24% ao ano, esse projeto aparentemente lucrativo pode nunca ser viabilizado. Segundo, esses problemas perpetuam ou agravam a *desigualdade*. Em todo o espectro político, a maioria das pessoas concorda que deve haver igualdade de oportunidades: um projeto deve ser financiado com base na qualidade da ideia e na solidez do plano da execução, e não em outros fatores. É importante ressaltar que a desigualdade também limita o crescimento quando boas ideias não são financiadas. Embora supostamente seja a terra das oportunidades, os EUA têm um dos piores registros de migração de renda do quartil inferior para o superior.[4] A desigualdade de oportunidades surge, em parte, da falta de acesso ao sistema bancário atual, da dependência de financiamento alternativo caro, como empréstimos com base em folha de pagamento e da incapacidade de comprar ou vender no mundo moderno do comércio eletrônico.

Essas implicações são de longo alcance e, por qualquer ângulo que se veja, essa é uma longa lista de graves problemas endêmicos ao nosso atual sistema de finanças centralizadas. A nossa infraestrutura financeira fracassou em se adaptar à era digital na qual vivemos. As finanças descentralizadas oferecem novas

oportunidades. A tecnologia é incipiente, mas o lado positivo é potencialmente transformacional.

Nosso livro tem vários objetivos. Primeiro, identificaremos as fraquezas do sistema atual, incluindo a discussão de algumas iniciativas preliminares que desafiaram os modelos de negócios de finanças centralizadas. Em seguida, exploraremos as origens da descentralização de finanças. Então, discutiremos um componente crítico do DeFi: a tecnologia blockchain, e em seguida, detalharemos as soluções que o DeFi oferece, associando a isso um aprofundamento de algumas ideias de ponta nesse espaço emergente. Por fim, analisaremos os principais fatores de risco e concluiremos olhando para o futuro e tentando identificar os ganhadores e os perdedores.



AS ORIGENS DA DESCENTRALIZAÇÃO FINANCEIRA MODERNA

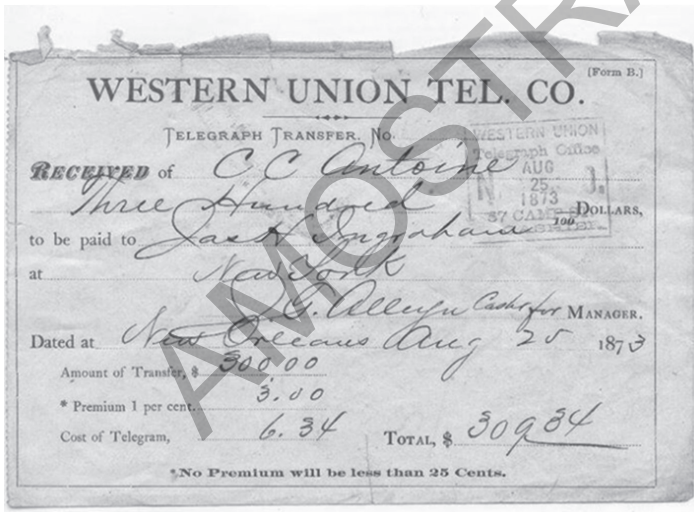
UMA RÁPIDA HISTÓRIA DAS FINANÇAS

Mesmo que o sistema financeiro de hoje seja atormentado por ineficiências, é muito melhor do que os do passado, nos quais as trocas de mercado eram realizadas pessoa a pessoa e exigiam que as necessidades de duas partes fossem mutuamente correspondentes. A partir disso, surgiu nas aldeias um sistema de crédito informal, em que as pessoas mantinham um registro mental de "presentes."[1]

A cunhagem moderna veio muito mais tarde, surgindo pela primeira vez na Lídia, por volta de 600 a.C. e fornecendo o que consideramos as funções atuais do dinheiro: unidade de conta, meio de troca

e reserva de valor. Entre as características importantes do dinheiro, estão: durabilidade, portabilidade, divisibilidade, uniformidade, oferta limitada, aceitabilidade e estabilidade. As notas bancárias, originárias da China, chegaram à Europa no século XIII.

As transferências não físicas de dinheiro surgiram em 1871, com a Western Union. A Figura 2.1 mostra a cópia de uma transferência antecipada de US$300. Repare como as taxas chegam a US$9,34, ou aproximadamente 3%. É notável que tão pouco tenha mudado em 150 anos: as transferências de dinheiro são rotineiramente mais caras, e as taxas de cartão de crédito são de 3%.


WESTERN UNION TEL. CO.

[Form B.]

TELEGRAPH TRANSFER. No.

RECEIVED of C C Antoine

Three Hundred DOLLARS,

to be paid to Jas N Ingraham

at New York

G. Allen Cash'r for MANAGER.

Dated at New Orleans Aug 25 1873

Amount of Transfer, $ 300 00

* Premium 1 per cent. 3.00

Cost of Telegram, 6.34 TOTAL, $ 309 34

*No Premium will be less than 25 Cents.

Figura 2.1 Transferência da Western Union de 1873
Fonte: Western Union Holdings, Inc.

Os últimos 75 anos viram muitas estreias no mercado financeiro: o cartão de crédito em 1950 (Diners Club); o caixa eletrônico ou "automated teller machine" (ATM) em 1967 (Barclays Bank); o "phone banking" em 1983 (Bank of Scotland); a "internet

banking" em 1994 (Stanford Federal Credit Union); os pagamentos de identificação por rádio frequência ou "radio-frequency identification payments" (RFID) em 1997 (Mobil Speedpass); os cartões de crédito com chip em 2005 (Mastercard); e o Apple Pay com dispositivos móveis em 2014 (Apple).

É importante ressaltar que todas essas inovações foram construídas na espinha dorsal das finanças centralizadas. Embora tenha havido alguns avanços tecnológicos, a estrutura do sistema bancário atual não mudou muito nos últimos 150 anos. Ou seja, a digitalização ainda suportava uma estrutura legada. Os altos custos associados com esse sistema legado estimularam novos avanços, conhecidos como *fintech*.

FINTECH

Quando os custos são altos, a inovação se encarrega de capitalizar as ineficiências. Às vezes, no entanto, uma poderosa camada de intermediários pode retardar esse processo. Um exemplo inicial de finanças descentralizadas surgiu no mercado de câmbio (forex) há vinte anos. Na época, grandes corporações usaram seus bancos de investimentos para administrar suas necessidades de forex. Por exemplo, uma corporação baseada nos EUA pode precisar de €50 milhões no final de setembro para pagar alguns bens comprados na Alemanha. Seu banco cotaria uma taxa extra para a transação. Ao mesmo tempo, outro cliente do banco pode precisar vender €50 milhões no final de setembro.

O banco cotaria uma taxa diferente. A diferença na taxa é conhecida como spread — o lucro que o banco tem por ser o intermediário. Dado o mercado forex de vários trilhões de dólares, isso se constituiu em parcela importante dos lucros dos bancos.

No início 2001, uma fintech ofereceu a seguinte ideia:[2] em vez de as empresas individuais consultarem vários bancos para obterem a melhor taxa, por que não ter um sistema eletrônico que combine os compradores e vendedores diretamente, a um preço acordado, e *sem* spread? Com efeito, o banco poderia oferecer esse serviço a seus próprios clientes e cobrar uma comissão modesta (em comparação com o spread). Além disso, dado que alguns clientes lidam com vários bancos, seria possível conectar clientes em todos os bancos participantes da rede peer-to-peer.

Você pode imaginar a recepção. O banco diria: "Você está sugerindo que devemos investir em um sistema eletrônico que canibalizará os nossos negócios e eliminará em grande parte um centro de lucro muito importante?" Contudo, mesmo há vinte anos, os bancos perceberam que seus maiores clientes estavam muito insatisfeitos com o sistema vigente. À medida que a globalização aumentava, esses clientes passaram a enfrentar custos desnecessários de transações forex.

Um exemplo ainda anterior foi a ascensão da negociação de ações em dark pools [locais privados para negociação de títulos]. Em 1979, nos EUA, a Securities and Exchange Commission (SEC) [equivalente no Brasil à Comissão de Valores Mobiliários] instituiu a Regra 19c3, que permitia às ações listadas em uma bolsa, como a de Nova York (NYSE), serem negociadas fora dela. Muitas grandes instituições mudaram seus grandes blocos de negociação para esses dark pools, negociando peer-to-peer com custos mais baixos do que as transações em bolsa.

Os custos excessivos de transação deram início a muitas inovações de fintech. O PayPal,[3] fundado há mais de vinte anos, é um precursor no mundo dos pagamentos; em 2017, sete dos principais

bancos dos EUA adicionaram seu próprio sistema de pagamentos, chamado Zelle.[4] Um importante ponto em comum desses avanços fintech de redução de custos é que eles contam com a espinha dorsal centralizada da infraestrutura financeira atual.

BITCOIN E CRIPTOMOEDAS

As dezenas de iniciativas de moeda digital que nasceram no início dos anos 1980 fracassaram.[5] O panorama mudou, no entanto, com a publicação do famoso white paper[6] [documento informativo] sobre o Bitcoin, de Satoshi Nakamoto, em 2008, que apresenta um sistema peer-to-peer descentralizado e que usa o conceito de *blockchain*. Inventado em 1991 por Haber e Stornetta,[7] o blockchain foi inicialmente concebido para ser um sistema de registro de data e hora para acompanhar as diferentes versões de um documento. A principal inovação do Bitcoin foi combinar a ideia de blockchain (carimbo de hora) com um mecanismo de consenso chamado de prova de trabalho (ou *proof of work*, introduzido por Back[8] em 2002). A tecnologia produziu um livro-razão imutável, que eliminou um problema importante com qualquer ativo digital: você pode fazer cópias perfeitas e gastá-las várias vezes. Blockchains levam em conta os recursos importantes desejáveis em uma reserva de valor, que antes nunca estavam presentes em um único ativo. Blockchains permitem escassez criptográfica (o Bitcoin tem um limite de oferta fixo de 21 milhões), resistência à censura e soberania do usuário (nenhuma entidade além do usuário pode determinar como usar os fundos) e portabilidade (pode ser enviada a qualquer lugar, em qualquer quantidade, a uma taxa fixa baixa). Esses recursos, combinados em uma única tecnologia, tornam a criptomoeda uma inovação poderosa.

A proposta de valor do Bitcoin é importante e pode ser mais bem compreendida se justaposta à de outros ativos financeiros. Por exemplo, considere o dólar (USD), que costumava ser lastreado em ouro antes que o padrão-ouro fosse abandonado em 1971. Agora a demanda por USD vem de (a) impostos, (b) compra de mercadorias dos EUA denominadas em USD e (c) pagamento de dívidas denominadas em USD. Esses três casos criam valor que não é intrínseco, mas sim baseado na rede que é a economia dos EUA. A expansão ou a contração nesses componentes pode impactar o preço do USD. Adicionalmente, choques na oferta de USD ajustam seu preço a um determinado nível de demanda. O Fed [Banco Central dos EUA] pode ajustar a oferta de USD por meio da política monetária, na tentativa de alcançar objetivos financeiros ou políticos. A inflação devora o valor do USD, diminuindo sua capacidade de armazenar valor ao longo do tempo. Alguém pode estar preocupado com a inflação descontrolada — aquilo que Paul Tudor Jones chama de *a grande inflação monetária* —, o que levaria a uma fuga para ativos resistentes à inflação.[9] O ouro provou ser um ativo bem-sucedido de proteção contra a inflação, devido à sua oferta praticamente limitada, utilidade concreta e confiabilidade global geral. Entretanto, como o ouro é um ativo volátil, sua capacidade histórica de cobertura é realizada apenas em horizontes extremamente longos.[10]

Muitos argumentam que o Bitcoin não tem valor "tangível" e, portanto, deveria não ter valor. Continuando com a comparação com o ouro, aproximadamente 2/3 dele são usados para joias, e outra quantidade adicional, em tecnologia de hardware. O ouro tem um valor tangível. O dólar americano, enquanto moeda fiduciária, tem valor como "moeda legal." No entanto, há muitos

exemplos na história em que a moeda surgiu sem qualquer respaldo que tivesse valor.

Um exemplo relativamente recente é o dinar suíço iraquiano, que foi a moeda do Iraque até a Guerra do Golfo, em 1990. As chapas de impressão foram fabricadas na Suíça (daí o nome), e a impressão, terceirizada para o Reino Unido. Em 1991, o Iraque foi dividido, com os curdos controlando o norte, e Saddam Hussein, o sul. Devido às sanções, o Iraque não pôde importar dinares do Reino Unido e teve que iniciar produção local. Em maio de 1993, o Banco Central iraquiano anunciou que os cidadãos tinham 3 semanas para trocar 25 dinares do modelo velho por novos (Figura 2.2). Depois disso, o antigo dinar seria irresgatável.

O velho dinar suíço iraquiano, todavia, continuou sendo usado no norte. No sul, o novo dinar foi castigado por uma inflação extrema. Por fim, a taxa de câmbio era de 300 dinares novos para um único dinar suíço iraquiano. O principal insight aqui é que o dinar suíço iraquiano não tinha apoio oficial — mas era aceito como dinheiro. Ele não tinha valor tangível, mas tinha valor. É importante ressaltar que o valor pode ser derivado de fontes tangíveis e intangíveis.

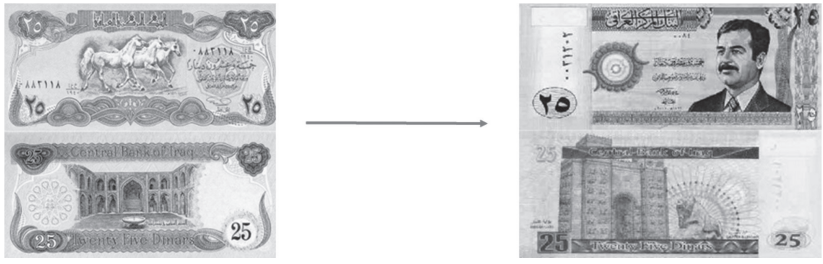


Figura 2.2 Dinares suíço-iraquianos e dinares novos
Fonte: Banco Central do Iraque

Os recursos do Bitcoin que mencionamos — particularmente a escassez e a autossoberania — o tornam uma reserva potencial de valor e possível proteção para a agitação política e econômica nas mãos dos governos globais. À medida que a rede cresce, a proposta de valor só aumenta, devido ao aumento de confiança e da liquidez. Embora o Bitcoin tenha sido originalmente pensado para ser uma moeda ponto a ponto, suas características deflacionárias e taxas fixas desencorajam seu uso em pequenas transações. Argumentamos que o Bitcoin é a nau capitânia de uma nova classe de ativos, as criptomoedas, que podem ter casos de uso variados com base na construção de suas redes. O Bitcoin, acreditamos, continuará a crescer como uma importante reserva e uma potencial proteção contra a inflação em horizontes longos.[11]

As criptomoedas originais ofereciam uma alternativa a um sistema financeiro que havia sido dominado por governos e instituições centralizadas, como bancos centrais. Elas surgiram em grande parte pelo desejo de substituir sistemas financeiros ineficientes e isolados por algoritmos imutáveis sem fronteiras e de código aberto. Essas novas moedas podem ajustar seus parâmetros, como inflação e mecanismos de consenso, por meio de seu blockchain subjacente para criar diferentes propostas de valor. Discutiremos blockchain e criptomoedas com maior profundidade mais tarde, mas por agora nos concentraremos em uma criptomoeda específica, com relevância especial para DeFi.

ETHEREUM e o DeFi

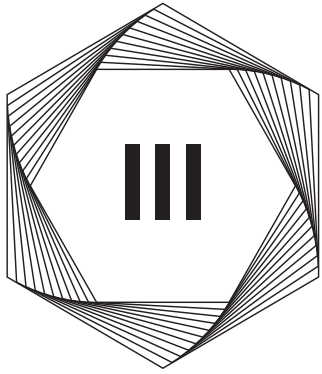
Ethereum (ETH) é atualmente a segunda maior criptomoeda em valor de mercado (US$260 bilhões). Vitalik Buterin apresentou a

ideia em 2014, e a Ethereum minerou seu primeiro bloco em 2015. Ethereum é, em algum sentido, uma extensão lógica das aplicações do Bitcoin porque permite *contratos inteligentes* [em inglês, "smart contracts"] — códigos que vivem em um blockchain, podem controlar ativos e dados e definem interações entre os ativos, os dados e os participantes da rede. A capacidade para contratos inteligentes define a Ethereum como uma *plataforma de contratos inteligentes*.

A Ethereum e outras plataformas de contratos inteligentes deram especificamente origem ao *aplicativo descentralizado,* ou *dApp*. Os componentes de backend desses aplicativos são construídos com contratos inteligentes transparentes e interoperáveis, que continuam a existir se a cadeia em que vivem existir. Os dApps permitem aos pares interagirem diretamente e eliminam a necessidade de uma empresa atuar como câmara de compensação central para interações com o aplicativo. Logo ficou claro que os primeiros dApps a mandar bem seriam os financeiros.

O impulso para os dApps financeiros tornou-se o movimento DeFi, que busca construir e combinar blocos de construção financeiros de código aberto em produtos sofisticados com atrito minimizado e valor maximizado para os usuários. Por não custar mais, em nível de organização, e fornecer serviços a um cliente com US$100 ou US$100 milhões em ativos, os proponentes do DeFi acreditam que toda infraestrutura financeira significativa será substituída por contratos inteligentes, que podem fornecer mais valor a um grupo maior de usuários. Qualquer um pode simplesmente pagar a taxa fixa para usar o contrato e se beneficiar das inovações do DeFi. Discutiremos plataformas de contratos inteligentes e dApps mais profundamente no Capítulo 3.

O DeFi é, essencialmente, um mercado competitivo de dApps financeiros, que funcionam como vários "fundamentos" financeiros, como câmbio, empréstimo e tokenização. Eles se beneficiam dos efeitos da rede de combinar e recombinar os produtos DeFi e atrair cada vez mais participação de mercado do ecossistema financeiro tradicional. Nossa meta neste livro é dar uma visão geral dos problemas que o DeFi resolve, descrever o cenário atual e em rápido crescimento do DeFi e apresentar uma visão das oportunidades futuras que o DeFi descerra.



INFRAESTRUTURA DEFI

Neste capítulo, discutiremos as inovações que levaram ao DeFi e apresentaremos a terminologia.

BLOCKCHAIN

A chave para todo o DeFi é sua espinha dorsal descentralizadora: um blockchain. Fundamentalmente, blockchains são protocolos de software que permitem que várias partes operem sob suposições e dados compartilhados sem confiar umas nas outras. Esses dados podem ser qualquer coisa, como informações de localização e destino de itens em uma cadeia de suprimentos ou saldo de tokens em uma conta. As atualizações são agrupadas em "blocos" (em inglês, *blocks*) e "trancadas" (em inglês, *chained*) juntas criptograficamente para permitir uma auditoria do histórico anterior — daí o nome.

Blockchains são possíveis por causa dos *protocolos de consenso* — conjuntos de regras que determinam que tipos de blocos podem se tornar parte de uma cadeia e, assim, a "verdade." Esses protocolos de consenso são projetados para resistir a adulterações maliciosas até um determinado limite de segurança. Os blockchains em que nos concentramos atualmente usam o protocolo de consenso de *prova de trabalho* [em inglês, "proof of work", PoW], que depende de uma loteria que requer alto poder computacional e consome muita energia para determinar qual bloco deverá ser adicionado. Os participantes concordam que a maior cadeia de blocos é a verdadeira. Se os invasores quiserem fazer uma cadeia mais longa que contenha transações maliciosas, eles devem superar todo o trabalho computacional do restante da rede. Em teoria, precisariam da maior parte do poder de computação da rede (taxa de hash) para conseguir isso — portanto, o famoso ataque 51% é o limite de segurança do PoW. Felizmente, é incrivelmente difícil para qualquer participante, mesmo um país inteiro, acumular tanto poder de rede nos blockchains mais usados, como Bitcoin ou Ethereum. Mesmo que a maior parte do poder de processamento da rede pudesse ser adquirida temporariamente, a quantidade de histórico de blocos que pode ser substituída é limitada por quanto tempo essa maioria ainda pode ser mantida.

Contanto que nenhuma parte mal-intencionada possa adquirir o controle majoritário do poder computacional da rede, as transações serão processadas pelos participantes de boa-fé e anexadas ao livro-razão quando um bloco for "ganho."

O foco aqui é a prova de trabalho, mas existem muitos mecanismos de consenso alternativo, sendo o mais importante deles a *prova de participação* [em inglês, "proof of stake", PoS]. Os validadores