KENNETH BOK

DECENTRALIZING FINANCE

HOW DEFI, DIGITAL ASSETS, AND DISTRIBUTED LEDGER TECHNOLOGY ARE TRANSFORMING FINANCE

FOREWORD BY TIMOTHY DRAPER
FOUNDER, DRAPER ASSOCIATES, DFJ AND DRAPER UNIVERSITY

WILEY

Praise for DECENTRALIZING FINANCE

"In a space that is often fast-moving and difficult to fully understand, Bok successfully demystifies many of the key questions that surround DeFi. At R3 we have witnessed first-hand the evolution of emerging innovations such as CBDCs and tokenization, and what this book accomplishes is a detailed overview of the convergence between these new economic models and traditional financial frameworks. The book's thoughtful breakdown of important industry initiatives, such as the Regulated Liability Network, enables readers to gain detailed insight into DeFi, without being overwhelmed by its complexities. Overall, *Decentralizing Finance* is a must-read for those interested in the impact of DLT and digital assets on today's financial services industry."
—**Todd McDonald,** Co-Founder and Chief Strategy Officer, R3

"In the rapidly changing world of DeFi, Kenneth's book is both relevant and timely, offering authoritative insights on the industry's current evolution. In sharing his vision for the future, he brings valuable perspectives from deep experience in digital assets and blockchain as an investor, trader and more. Whether you are a crypto-native or just starting out in DeFi, I recommend this as an essential and informative read."
—**Darius Sit,** Founder & CIO, QCP Capital

"Kenneth Bok's book provides a solid overview of the fast-moving Decentralized Finance ecosystem. In particular, he introduces critical developments within and outside the regulatory perimeter. But Ken does not stop there; he also shares his future vision for DeFi — pick up a copy to find what it is. I recommend his book to anyone who wants to understand DLT & blockchain-based finance and is overwhelmed by the pace of industry developments and the quantity of academic papers released daily. Ken uniquely contributes to our understanding of DeFi by delivering the future standard introductory work for industry practitioners."
—**Daniel Liebau,** Affiliated Faculty, Singapore Management University

"Kenneth Bok offers a comprehensive overview of the DeFi landscape by clearly defining the various layers of the application and infrastructure stack, presenting the key use cases and the differing mechanisms, and relating them to the current traditional finance and regulatory systems. Kenneth also offers glimpses into how factors such as government and market competition will change the landscape moving forward. This book should be read by anyone looking to understand DeFi from a theoretical and practical lens, as well as the associated benefits and risks of participating directly in the ecosystem."
—**Lasse Clausen,** Founding Partner, 1kx

Cover Design: Wiley
Cover Image: © amasterphotographer/Shutterstock
Author Photo: Courtesy of Kenneth Bok

www.wiley.com

WILEY

Also available as an e-book

ISBN 978-1-394-15497-5
90000
9 781394 154975

In *Decentralizing Finance: How DeFi, Digital Assets, and Distributed Ledger Technology Are Transforming Finance,* blockchain and digital assets expert Kenneth Bok offers an insightful exploration of the current state of decentralized finance (DeFi). As distributed ledger technology (DLT) increasingly optimizes and democratizes financial ecosystems worldwide, this book serves as a comprehensive guide to the most salient aspects of the ongoing transformation.

The text delves into both crypto-native DeFi and DLT applications in regulated financial markets, providing:

- Comprehensive analysis of crypto-native DeFi across key areas such as its competitive landscape, infrastructure, financial instruments, activities, and applications
- Coverage of key risks, mitigation strategies, and regulatory frameworks, analyzed through the perspective of international financial standard-setting bodies
- Insight into how DLT is reshaping traditional financial systems through innovations like central bank digital currencies (CBDCs), tokenized assets, tokenized deposits, and institutional-grade DeFi platforms

In a world where financial technology is rewriting the fundamental code of

(continued on back flap)

(continued from front flap)

digital currency, the future of money is undeniably DLT-centric. How will this seismic shift interact with existing financial infrastructures? Can decentralization and traditional banking coexist and potentially synergize? This book endeavors to answer these pressing questions for financial professionals navigating these transformative times.

Authored by a former Goldman Sachs trader, past Head of Growth at Zilliqa, and an early Ethereum investor with extensive experience in both traditional finance and the crypto ecosystem, *Decentralizing Finance* provides you with an insider's perspective on the revolution that is DeFi.

KENNETH BOK is Managing Director of Blocks. sg, a digital assets advisory based in Singapore. He started his career in finance as an equities derivatives trader for Goldman Sachs. He was previously Head of Growth and Strategy at Zilliqa, where he led ecosystem and business development, and lead organiser for De/Centralize 2018, a groundbreaking conference on digital assets and blockchain.

Additional Praise for *Decentralizing Finance*

Kenneth Bok's book *Decentralizing Finance* helps to demystify DeFi and goes further by explaining how traditional financial services are being unbundled by new technologies. We need more literature to explain why self-managed finance needs to be an integral component of the future digital economy.

—**Linda Jeng**, Head of Global Web3 Strategy at the Crypto
Council for Innovation, Visiting Scholar on Financial
Technology and Adjunct Professor at the Georgetown University
Law Center's Institute for International Economic Law

Kenneth has displayed his vast experience, deep insights and thoughtful views on the fast-moving, often-misunderstood world of blockchain and distributed ledger technology, as well as digital/crypto assets with his notable knowledge and experience gained from traditional finance. His book, *Decentralizing Finance* is indeed valuable for not only the uninitiated who are seeking to learn more about this space, but also for the veteran who would gain much from Kenneth's opinions, reflections and forward-looking views, in this realm. Kenneth has managed to pack all that into less than 250 pages of clear and concise, systematic reading, which makes it so much more pleasurable to read. I would highly recommend this to anyone interested in this industry.

—**Hsu Li Chuan**, Senior Partner, Dentons Rodyk & Davidson LLP

In this book *Decentralizing Finance*, Kenneth Bok comprehensively and systematically covers the many areas that are evolving in this new world. What is clear is that the institutions and instruments in the world of finance are changing. How will it look going forward? How will it be different from the world we already know? These are the pertinent questions addressed in this book. The author gives the reader a timely and authoritative overview of how, as finance decentralizes, digital assets and distributed ledgers are bringing about fundamental change. An essential read for anyone who wants to have a competent grasp of the tools needed to analyze the new status quo.

—**Joo Seng Wong**, Founder and CEO at Spark Systems

In his book on decentralized finance, Kenneth unveils profound insights into this dynamic landscape. Kenneth's perspective on the evolving DeFi realm is truly enlightening, providing valuable understanding of trends, challenges, and opportunities. With his expertise and clarity, he demystifies DeFi's complexities, making it accessible to readers of all levels. A must-read for both novices and experts, Kenneth's book enriches our comprehension of this transformative space.

—**Yi Ming Ng**, CEO at Tribe

Everyone who works towards the greater good

"Finance, at its best, does not merely manage risk, but also acts as the steward of society's assets and an advocate of its deepest goals. Beyond compensation, the next generation of finance professionals will be paid its truest rewards in the satisfaction that comes with the gains made in democratizing finance extending its benefits into corners of society where they are most needed. This is a new challenge for a new generation, and will require all of the imagination and skill that you can bring to bear. Good luck in reinventing finance. The world needs you to succeed."

—Professor Robert J. Shiller, Speech to Finance Graduates,
Finance and the Good Society

This book is dedicated to everyone working towards a more inclusive and efficient financial system.

Contents

Acknowledgments

The creation of this book was a collaborative effort, enriched by the knowledge, support, and insights of many individuals and organizations. I extend my deepest gratitude to those who played a crucial role.

Thank you to the numerous researchers and authors whose reports have been integral to this book. Their detailed insights have shaped many of the ideas and concepts presented here, and I have strived to reference their work appropriately.

Daniel Liebau: Thank you Dan for your support of this project. Your contribution to my journey in this DeFi path has been invaluable. I appreciate all the reports, introductions, and feedback you've sent my way.

A heartfelt thank you to my editors – Vithusha Rameshan, Syd Ganaden, Susan Cerra, and Purvi Patel – as well as the entire Wiley team responsible for bringing this book to life. Special appreciation goes to Carol Thomas for her meticulous copyediting. Your dedication and patience throughout the publishing process have been invaluable.

To my family, especially my mother, thank you for your love, encouragement, and understanding. Your belief in me has been a guiding force.

Timothy Draper, for being so generous with his time to speak at De/Centralize 2018 and writing the foreword for this book. The first time I had heard that Singapore was becoming a crypto hub was during an event at Draper University in San Mateo, California, back in 2014.

Special thanks to various professionals who have provided invaluable feedback and detailed commentary on the material, including Jeremy Kim, staff at the Monetary Authority of Singapore, and Lasse Clausen along with his team at 1kx.

Finally, thanks to all my colleagues, past and present, who supported me throughout this endeavor: Brandon Possin for editing and feedback on early chapters, Tim Han for previous support with De/Centralize, David Tan and Jennifer Lewis for constant encouragement and advice.

1

What Is DeFi?

> *I've developed a new open source P2P e-cash system called Bitcoin. It's completely decentralized, with no central server or trusted parties, because everything is based on crypto proof instead of trust.*
>
> —Satoshi Nakamoto

Decentralized Finance (DeFi) is an alternative financial infrastructure that is open, permissionless, and interoperable, built on public blockchains such as Ethereum. DeFi consists of a wide variety of internet-native applications and protocols that enable existing financial activities such as trading, investing, and payments, and also for entirely new financial capabilities. DeFi applications, being permissionless by design, are available for retail and institutional investors to utilize globally, with only an internet connection and sufficient know-how being the prerequisites required to participate in DeFi. Like many emergent movements and technological trends, DeFi outpaces regulation and many aspects of DeFi are unregulated and suffer from a lack of standards necessary in financial applications. Nonetheless, DeFi represents an entirely new way to deliver financial services and could interface with traditional finance as well as financial technology (FinTech) in many ways.

Interfaces for DeFi take place through software tools and infrastructure already built for the existing cryptocurrency system, such as blockchains, managed infrastructure, web-based browser wallets, centralized and decentralized exchanges, and the plethora of tools available for creating and maintaining decentralized applications (dApps). A more detailed explanation of the infrastructure, instruments, and applications will be covered in the following chapters.

Historically, core DeFi applications such as Uniswap and Aave occurred earlier in about 2018, but DeFi only came into prominence in Q2 2020, "DeFi Summer," when the *total value locked-up* by smart contracts skyrocketed above

Decentralizing Finance: How DeFi, Digital Assets, and Distributed Ledger Technology Are Transforming Finance, First Edition. Kenneth Bok.
© 2024 John Wiley & Sons Ltd. Published 2024 by John Wiley & Sons Ltd.

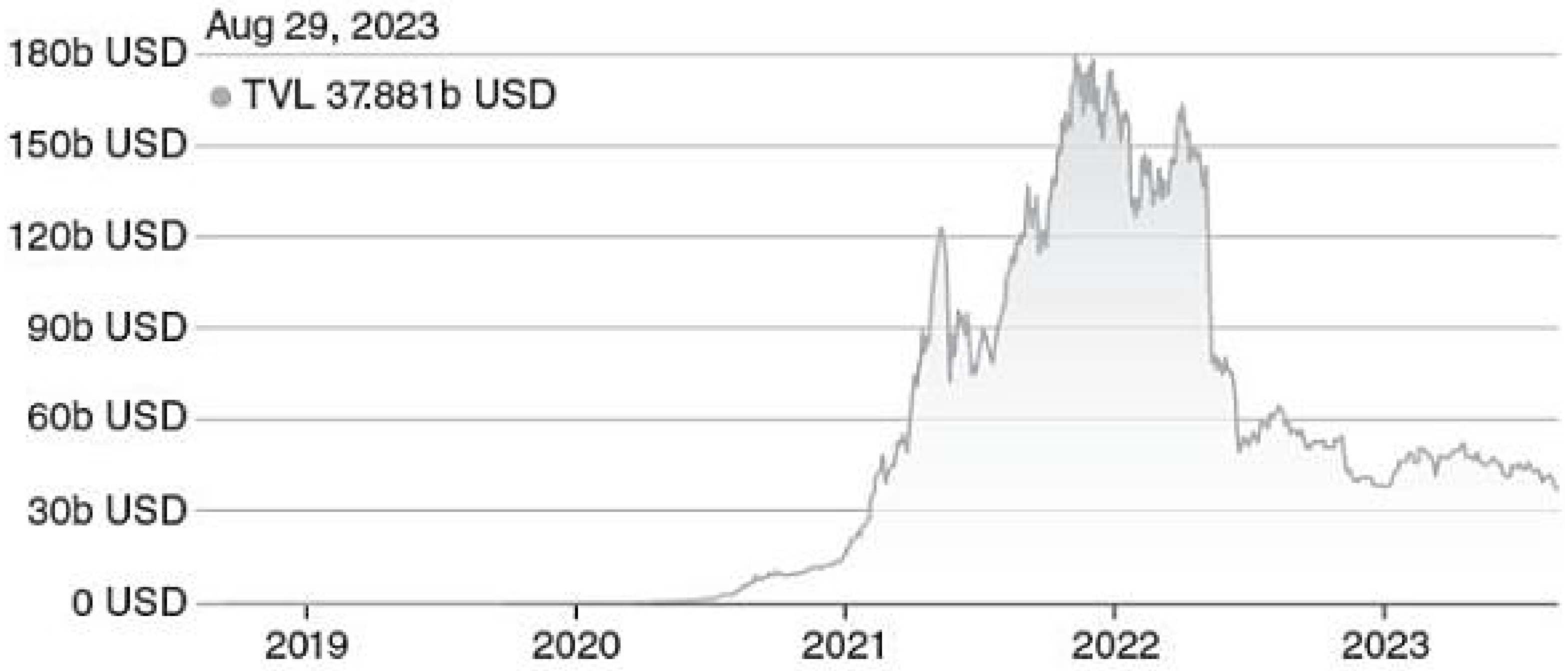


Figure 1.1 Total value locked-up in DeFi (2019–2023).
Source: https://defillama.com/

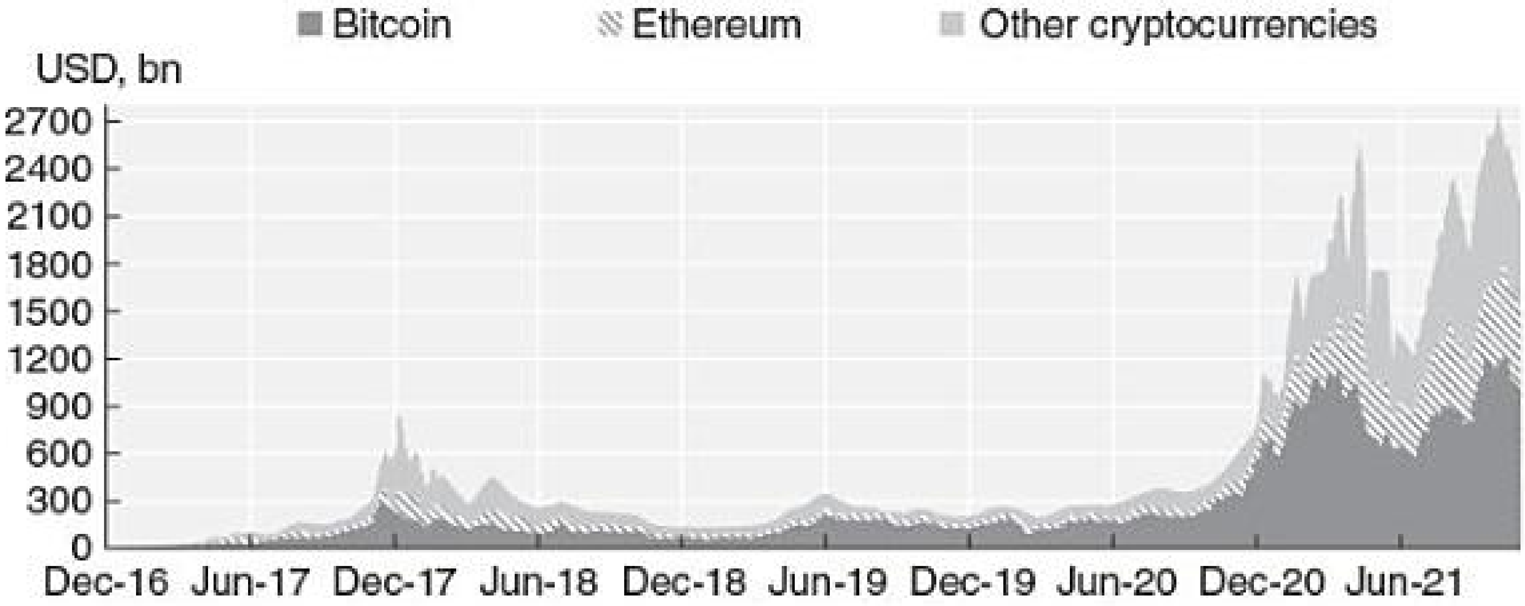


Figure 1.2 Market capitalization of all cryptocurrencies (2016–2022).
Source: Thompson Reuters Eikon, OECD. https://www.oecd.org/daf/fin/financial-markets/Why-Decentralised-Finance-DeFi-Matters-and-the-Policy-Implications.pdf

US$100 billion, coinciding with a bull market in cryptocurrencies which peaked in late 2021. See Figures 1.1 and 1.2.

Within the cryptocurrency industry, DeFi is an established vertical, with well-defined business models and product offerings. Other key verticals in crypto include general-purpose blockchains (L1 / L2s), Games, Non-Fungible Tokens (NFTs) and stablecoins. dApps are built on a specific blockchain, which results in distinct ecosystems for each blockchain. Each blockchain thus tends to have a DeFi ecosystem which consists of key dApps which serve a specific niche or function, such as decentralized exchanges, aggregators, and lending / borrowing platforms. dApps are also able to be multi-chain or cross-chain, allowing for bridging and aggregation of liquidity and functionality across multiple blockchains. The majority of DeFi apps are on Ethereum, although there now exist DeFi applications and ecosystems on other L1s such as Solana, Binance Smart Chain, Polkadot, and Avalanche.

On a broader level, DeFi is being analyzed and monitored by many TradFi industry participants, and also supranational organizations such as the Bank of International Settlements (BIS), the Organisation for Economic Co-operation and Development (OECD), and the International Organization of Securities Commissions (IOSCO), with all three having produced reports and analysis on DeFi. The reports assess risks to global financial stability and implications to regulation and policy, but strike a cautiously optimistic tone to the technological innovations which DeFi and smart contracts might bring to finance as a whole.

> DeFi applications have the potential to provide benefits to financial market participants in terms of speed of execution and transaction costs, driven by the efficiencies produced by DLT-technological innovation and disintermediation of third parties replaced by software code of smart contracts. DeFi could possibly allow for a more equitable participation of users in markets depending on the design of governance arrangements. Given the open source nature of protocols, DeFi may promote innovation in financial services and could have some potential to promote financial inclusion depending on the design and transaction arrangements (e.g. fees charged).
>
> —Why Decentralised Finance (DeFi) Matters and the Policy Implications, p. 10, OECD

DeFi has tremendous potential to lower transaction costs, improve financial inclusion and facilitate financial innovation through its global, open nature. It could prove as significant as FinTech in enabling a more democratic access to financial services by way of projects such as MPesa. It could reduce fees associated with financial services for lower-income groups and small businesses. Given its nascent nature, DeFi faces significant structural and cultural challenges towards these aspirational goals.

DeFi is not without its risks, a topic we will explore in detail in Chapter 4. Some of the highest-profile collapses in crypto, although primarily related to centralized crypto, have had ripple effects on DeFi as well. Two such examples are Terra and FTX.

The implosion of the Terra ecosystem and UST, an algorithmic "stablecoin," was one of the biggest cryptocurrency collapses in history, affecting thousands of retail users and institutions involved in crypto asset trading and investing. At its peak, the market capitalization of LUNA, the token of the Terra ecosystem, was US$36 billion and UST was the third largest stablecoin (behind USDT and USDC) with a market capitalization of US$18 billion.[1] Many people flocked to the promise of 19.5% per year rate that Anchor (a yield platform operated by Terra) paid out until it all collapsed very suddenly. The collapse of Terra was the beginning of a cryptocurrency financial contagion which led to the collapse of several other cryptocurrency firms including Celsius, Three Arrows Capital, BlockFi, FTX, and others.

1.1 The Role of Intermediaries in TradFi

A core tenet of DeFi is the disintermediation of financial intermediaries with the blockchain. Intermediaries are middlemen. If DeFi seeks to replace intermediaries through software, then it is only appropriate to ask what those existing functions are. How will blockchain-based software enable them?

Most financial entities such as banks, exchanges, and insurance companies are intermediaries. Intermediaries perform the important functions of connecting those who have capital (investors and lenders) with those who seek capital (entrepreneurs and borrowers) in accountable, rigorous, auditable, and risk-prudent processes. Intermediaries are core to the healthy functioning of the global financial system, and enable monetary and fiscal policy to be transmitted from central banks and governments down to businesses and consumers.

Global financial centers such as New York City, London, Shanghai, and Singapore are also frequently associated with good rule-of-law, infrastructure, and governance that enable financial market participants to operate stable businesses. This is critical in fast-changing financial environments that demand a tremendous amount of interconnectivity.

Intermediaries perform a large number of roles, including investor protection, market integrity, and other systemically important functions. Regulators ensure intermediaries meet these goals through licensing requirements and legal enforcement.

Two examples of financial intermediaries are stock exchanges and banks. The New York Stock Exchange (NYSE) is the world's largest stock exchange, with an average daily trading volume in the hundreds of billions of dollars. By facilitating order books for different stocks and supporting the millions of orders that change price and size constantly on a millisecond basis, the NYSE allows for buyers and sellers of stocks to trade with one another securely and with low transaction costs. Stock exchanges enable traders to find the other side of the transaction, at the right price.

Banks that you and I have accounts with are also financial intermediaries. Banks accept deposits from savers and lend money to businesses and borrowers, who have to pass screening from the banks in light of their credit scores and other estimates on their ability to pay. This screening is a key role in making sure that loans are financially viable and that borrowers ultimately are being economically productive.

Banks are also fundamentally in the business of matching their assets and liabilities and ensuring that the interest they earn from their borrowers is higher than the interest paid to their lenders. Banks hedge and control their financial risk through the money markets (short term debt markets).

One of the key issues of DeFi is that most of the lending takes place pseudo-anonymously (anonymous but having a distinct blockchain address) and is based on overcollateralization. This is in large contrast to the way loans are disbursed in TradFi as discussed briefly earlier. We will examine some initiatives such as decentralized identity and credit scoring that seek to bridge this gap.

1.2 Definitions

For the scope of this book, I will define DeFi in two ways: narrow and broad.

A narrow definition of DeFi:

> DLT-based finance that is self-custodial, uncensorable, and community-driven.

A broader definition of DeFi:

> DLT-based finance that disintermediates centralized entities.

There do not exist many formal definitions of DeFi, and distinctions vary between industry practitioners and academics. Nonetheless, here is a summary of the key features of DeFi, with both narrow and broad definitions.

The one feature that most industry practitioners and academics agree on is the non-custodial or *self-custodial* aspect of DeFi. That is, users are able to own their crypto assets directly through the use of private keys and not rely on a third-party custodian to custody their assets. For clarity, I will henceforth refer to non-custodial as self-custodial, since that tends to be less confusing.

The other feature around DeFi custody which stems from public blockchains is that *smart contracts* (computer code executed on the blockchain, to be covered in Chapter 2) can custodize crypto. Smart contracts can hold funds and enable for a wide range of functionality owing to the programmable nature of the blockchain. Many of the DeFi protocols, such as automated market makers and borrow / lending platforms, utilize this feature of smart contract custody.

The second feature of DeFi is that it should be *uncensorable*, both on the transaction layer and the protocol layer. For example, if you are using Uniswap on Ethereum, both Uniswap (the application) and Ethereum (the protocol) must not have the ability to censor your transaction – that is – have no way of stopping your transaction. In direct contrast, a relationship where your assets are held or custodized by a central entity is referred to as centralized finance or CeFi.[2] Figure 1.3 shows a decision tree to differentiate between DeFi and CeFi.

The third feature of DeFi, especially within crypto, is about incentives for specific groups of actors for doing particular tasks and distributed governance. In other words, DeFi is *community-driven*. Some might call these DAOs, or distributed autonomous organizations. The majority of DeFi projects have a circulating governance token that is designed for token holders to be able to

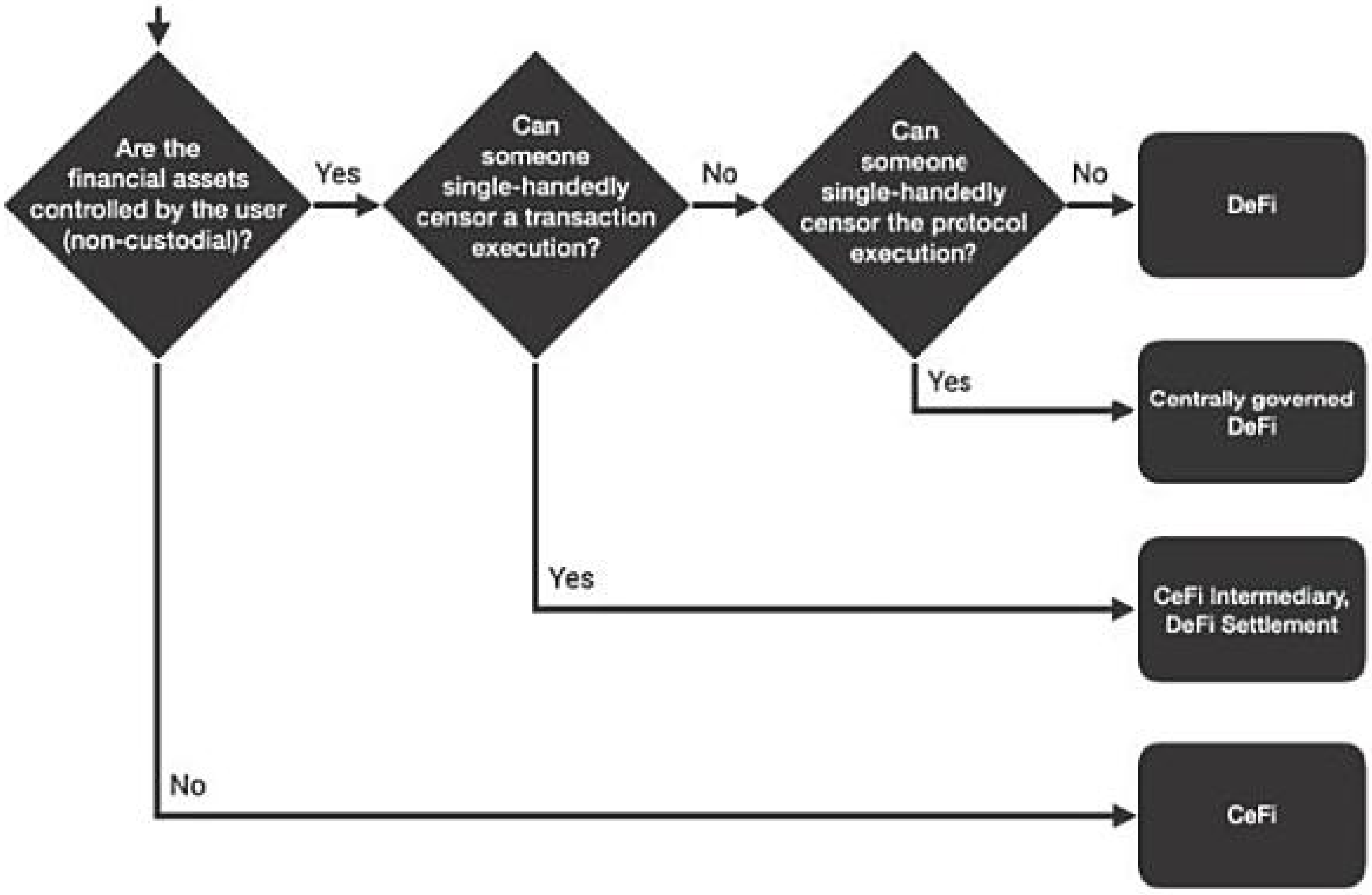

Are the financial assets controlled by the user (non-custodial)?
Yes
Can someone single-handedly censor a transaction execution?
No
Can someone single-handedly censor the protocol execution?
No
DeFi
Yes
Centrally governed DeFi
Yes
CeFi Intermediary, DeFi Settlement
No
CeFi

Figure 1.3 Decision tree to differentiate between DeFi and CeFi.
Source: Qin, K., Zhou, L., Afonin, Y. et al. (2021). CeFi vs. DeFi – Comparing Centralized to Decentralized Finance. arXiv:2106.08157

propose and vote for issues that are material to the ongoing functioning of the project. For example, in Curve (a decentralized exchange), the CRV token is used for the control of the emission gauge of the rewards in the staking pools. The extent to which decentralized governance actually is decentralized is another topic of discussion that has been discussed by BIS[3] and other research into governance.

More broadly speaking, the core mission and tenet of DeFi is *disintermediation*. This is also in line with a similar sounding "decentralization." A broader definition of DeFi is financial disintermediation with smart contracts and blockchains. To be more precise, smart contracts that run on *public* blockchains, since private blockchains are limited by design. In regards to this broader definition of DeFi, *DeFi* and *crypto* are almost interchangeable by meaning.

The adoption of DeFi from TradFi institutions is also promising. One example is the tokenization of regulated securities and putting them on-chain to be used in DeFi-style trading pools as collateral. Thus, I would argue that the definition of DeFi is broadening from the crypto-native perspective. Just as with Central Bank Digital Currencies (CBDCs) and permissioned blockchains, innovations in crypto have readily transposed to the centralized world, albeit in piecemeal ways that fit within existing mandates, requirements, and processes.

1.3 Other Characteristics of DeFi

Here are a few more key characteristics of DeFi that set it apart from TradFi. Some of them are advantages, some of them are disadvantages and there are some that are both. Here are the key ones that will help you to understand DeFi from a high-level perspective.

1.3.1 Interoperability / Composability

DeFi applications and protocols are designed to be "money legos" – being able to interoperate with one another with application programming interfaces (APIs). Complex transactions may involve multiple calls to multiple applications in one transaction. Interoperability of applications and protocols allow for easy aggregation and other kinds of abstraction, such as dashboards.

1.3.2 Transparency

DeFi takes place on smart contracts, which are by nature transparent and auditable. Like open-source software, this makes it easy to audit the code. Verification of transactions is also easier in a transparent system: for example, for a simple token transfer from Alice to Bob, Alice would not even need to ask Bob if he has received the token to verify the transaction has completed – all she needs to do is to look at his address on the block explorer.

1.3.3 Openness

DeFi is designed to be permissionless and open. One does not need to provide any kind of identification to the blockchain in order to open a wallet or account. In theory, this has great potential for DeFi to serve the billions of the unbanked and underbanked who do not have formal identification or have challenges opening a bank account.

The other dimension of openness is open-source. Many DeFi applications have their source code posted on software development platforms such as GitHub where developers can collaborate, audit, and re-use software code. This is arguably positive for innovation as a much larger set of developers, beyond those who work in TradFi, have the ability to work on financial software.

1.3.4 Decentralized / Peer-to-peer

Decentralization can occur on different levels and layers. Miles Jennings of *a16z* has offered a categorization of decentralization in web3 into three categories: technical, economic, and legal.[4]

In most countries, the banking sector is concentrated in a few players. This hurts the consumer as there is less competition and other kinds of behavior such as price setting. Decentralization enables for a more open-playing field and for open-access to financial infrastructure. On the flip-side, there is also no one to call when things go wrong, and promotes a greater level of risk-taking due to the unregulated nature of DeFi.

DeFi takes peer-to-peer business models in FinTech to the next level. DeFi enables individuals to lend and borrow from one another, using DeFi platforms as the intermediaries. We'll examine some of these businesses in Chapter 3.

1.3.5 Unregulated

It is not just the novelty of DeFi that makes it a "wild west." The entire basis of financial regulation (currently) is around licensing and centralized control over known corporate entities, and individuals who can be subject to enforcement actions if rules are not complied with. The fundamental architecture of DeFi and its global nature makes it difficult to regulate, as there are no centralized entities to censure, and DeFi companies can move or choose one regulatory regime over another (regulatory arbitrage). In DeFi, pseudo-anonymity (i.e., I know you by your on-chain address, but not your real name) is an accepted norm. There are teams that operate on this basis that have received funding from venture capital (VC) firms,[5] and there have also been cases where founders have abused this norm of anonymous developers to create an illusion of success.[6]

1.4 The DeFi Stack

The following framework is from Fabian Schär, Professor at the University of Basel, describing the five layered DeFi stack:

1. **Settlement Layer**
   This is the core layer of the blockchain and consists of the node operators, consensus mechanisms, and the hardware that powers it such as PoW (Proof-of-Work) mining rigs, GPUs (Graphics Processing Units) and CPUs. Different blockchains may have vastly different architectures and there is an entirely separate line of analysis that looks to compare them. (You can see my presentation on L1 comparisons on my website.)[7] This is the foundational layer of DeFi.
2. **Asset Layer**
   This layer consists of the assets that are issued on the blockchain, and may differ by token type. In Figure 1.4, ETH is the native crypto-asset of the Ethereum blockchain, and is directly linked with the core blockchain as it is

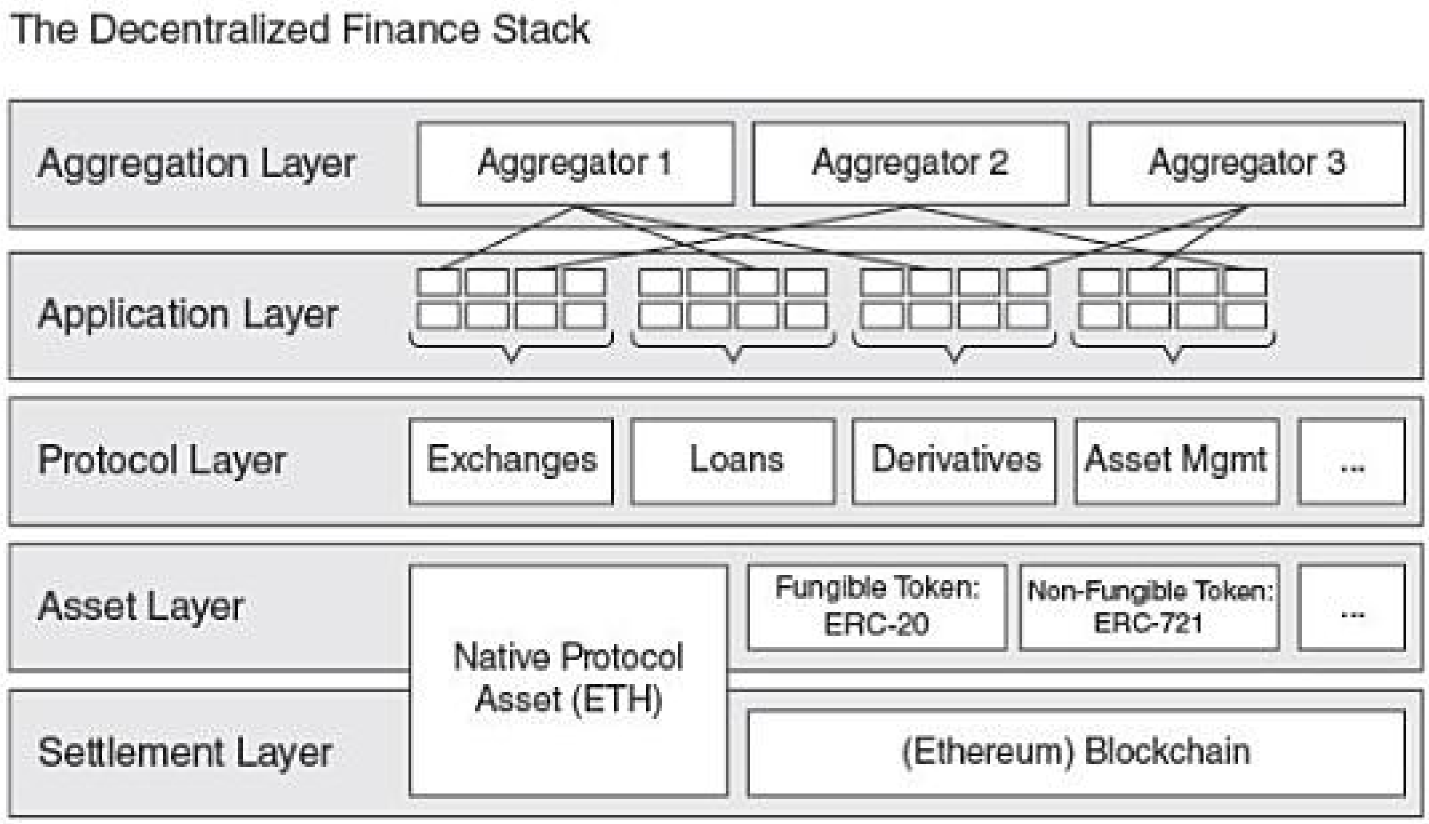


Figure 1.4 The DeFi stack.
Source: https://research.stlouisfed.org/publications/review/2021/02/05/decentralized-finance-on-blockchain-and-smart-contract-based-financial-markets

utilized in staking, miner rewards, and other incentives that power the blockchain. The ERC-20 standard specifies fungible token contracts, and the ERC-721 standard specifies non-fungible token contracts.

3. **Protocol Layer**
   This layer consists of the smart contracts that power specific applications such as decentralized exchanges, borrowing and lending platforms, and derivatives platforms. These are written in the native programming language of the blockchain, in the case of Ethereum: Solidity and Vyper. Other tools such as IDEs (Integrated Development Environments), libraries and debugging tools assist developers with writing and deploying smart contracts on-chain.
4. **Application Layer**
   This is the front-end of the protocol layer. This is what the typical user sees via a Graphical User Interface (GUI) and where interactions and transactions occur between the protocols and the user's wallets. Components of the application layer such as graphics and other middleware are often hosted off-chain on centralized servers, cloud providers, or newer decentralized equivalents such as InterPlanetary File System (IPFS).
5. **Aggregation layer**
   The aggregation layer is yet another layer of abstraction above the application layer, and aggregates across different protocols and applications to provide the user with the best possible price and execution (for trading applications), visualize the user's positions across all the DeFi applications they are using, or perform other complex operations across multiple DeFi applications.

Chapter 2 will examine the settlement layer and asset layer. Chapter 3 will examine the protocol, application, and aggregation layers.

1.5 Size of DeFi

How big is DeFi? Here we can rely on a few metrics to measure the size and scale of DeFi, and whether or not it is actually "eating TradFi," as its supporters would say colloquially. (Nibbling perhaps?) One common measure is *Total Value Locked-up* (TVL) (Figure 1.5). This is a proxy for the total amount of crypto assets "locked up," or deposited as collateral in smart contracts of trading platforms and borrow / lending platforms. As of time of writing (Aug. 2023) TVLs (across all blockchains) are ~US$37.5 billion, down from the peak of ~US$250 billion in December 2021. (Source: DefiLlama.)

It should also be noted that there are many critiques of the TVL metric. The primary criticism being that it is an inflated number due to multiple counting of the same asset. For example, if a user deposits 100 ETH into Aave (a borrow / lending platform) and borrows 40 ETH (assuming a 40% collateralization ratio), the same user could subsequently deposit the same 40 ETH and borrow 15 ETH. The TVL metric counts 140 ETH even though there was only 100 ETH to begin with. The same is also true for "liquid staking" platforms such as Lido Finance where ETH can be staked for stETH, which in turn can be used in other DeFi applications.

The other measure, which pertains to the wider adoption of crypto, would be the number of *global crypto owners* Figure 1.6). Crypto.com's "Crypto Market Sizing" report in January 2023 estimates 425 million global crypto owners in December 2022.

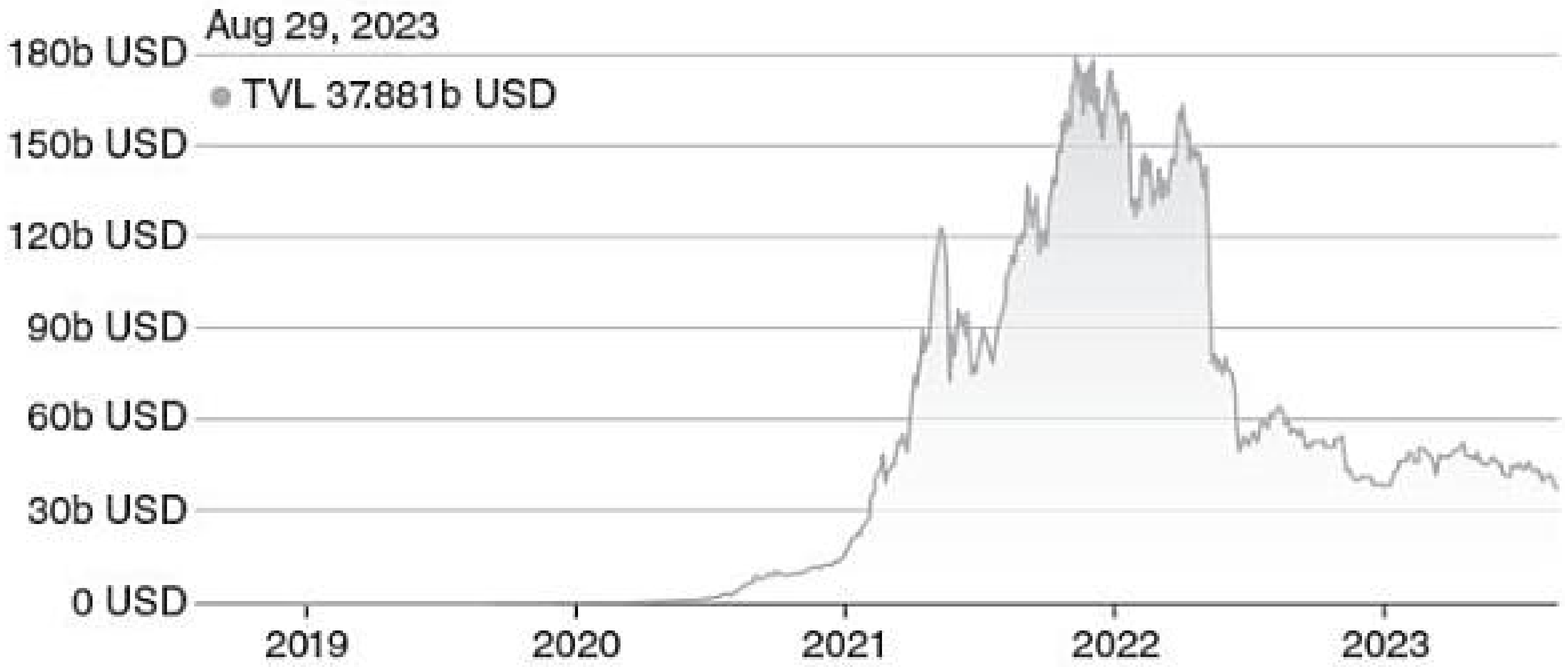


Figure 1.5 Total value locked-up in DeFi (2019–2023).
Source: https://defillama.com/

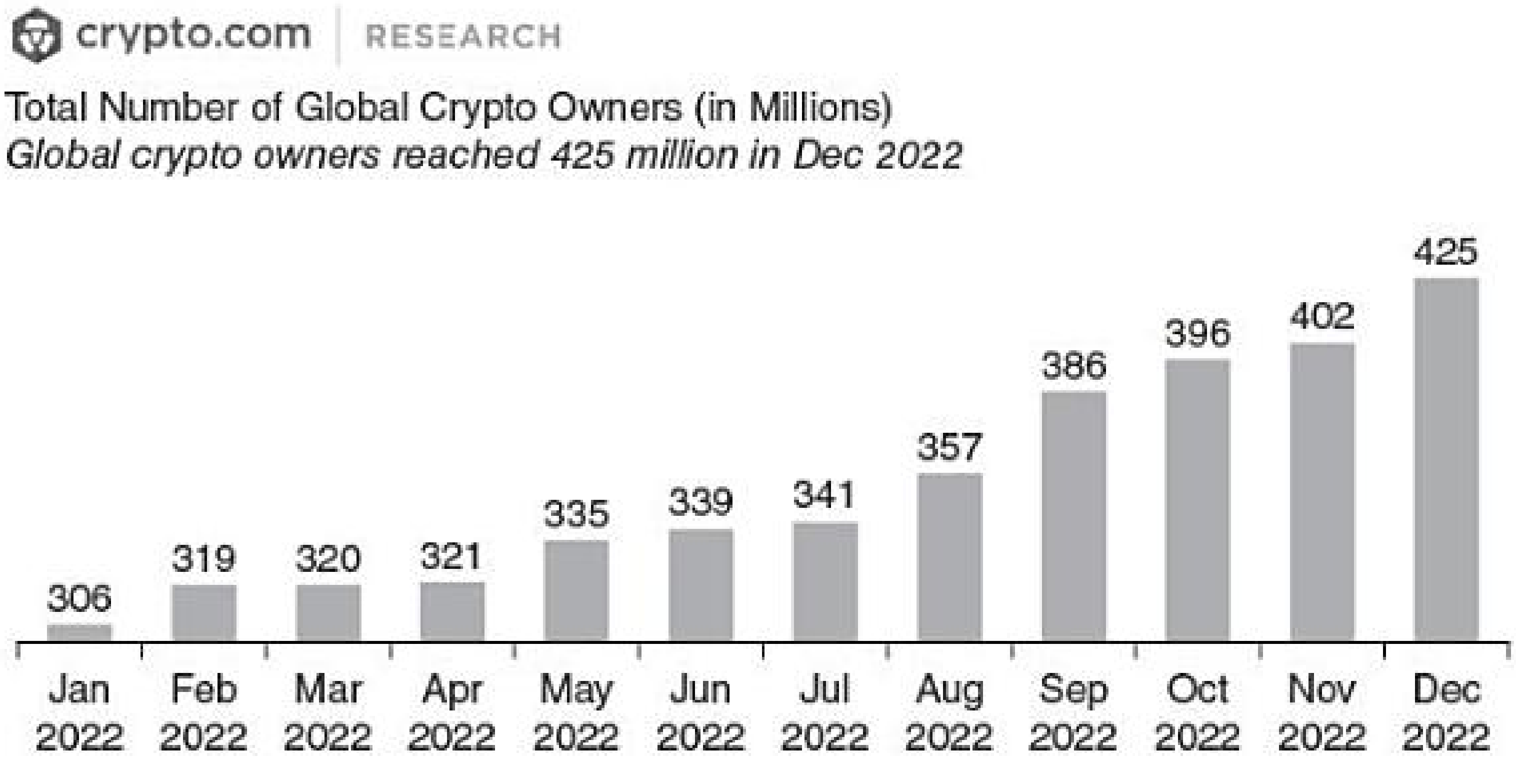


Figure 1.6 Total number of global crypto owners (in millions).
Source: Crypto.com, Crypto Market Sizing. https://content-hub-static.crypto.com/wp-content/uploads/2023/01/Cryptodotcom_Crypto_Market_Sizing_Jan2023-1.pdf

The third category would be *volume of transactions* (Figures 1.7 and 1.8). Coingecko estimates that the volume for all decentralized exchanges is US$84.17 billion, and represents 13.88% of CEX (centralized exchange) spot trade volume.

From these measures we can surmise that DeFi is quite cyclical and dependent on the broader bull / bear markets in cryptocurrencies, but on the whole has demonstrated significant growth in the last 3 years and continues to cannibalize market share from centralized crypto exchanges.

1.6 Key Participants in DeFi

DeFi is (at present) predominantly a subset of crypto. Thus the key actors in DeFi are similar to those in crypto. Nonetheless, this could change as DeFi evolves (especially with putting real world assets on-chain) and has more integrations with FinTech and TradFi.

1.6.1 Developers and Entrepreneurs

Developers typically focus on certain projects or a blockchain ecosystem as it takes time to build up expertise in the native programming language of the blockchain. Electric Capital has some great analysis of the number of developers in the crypto / DeFi / web3 space.

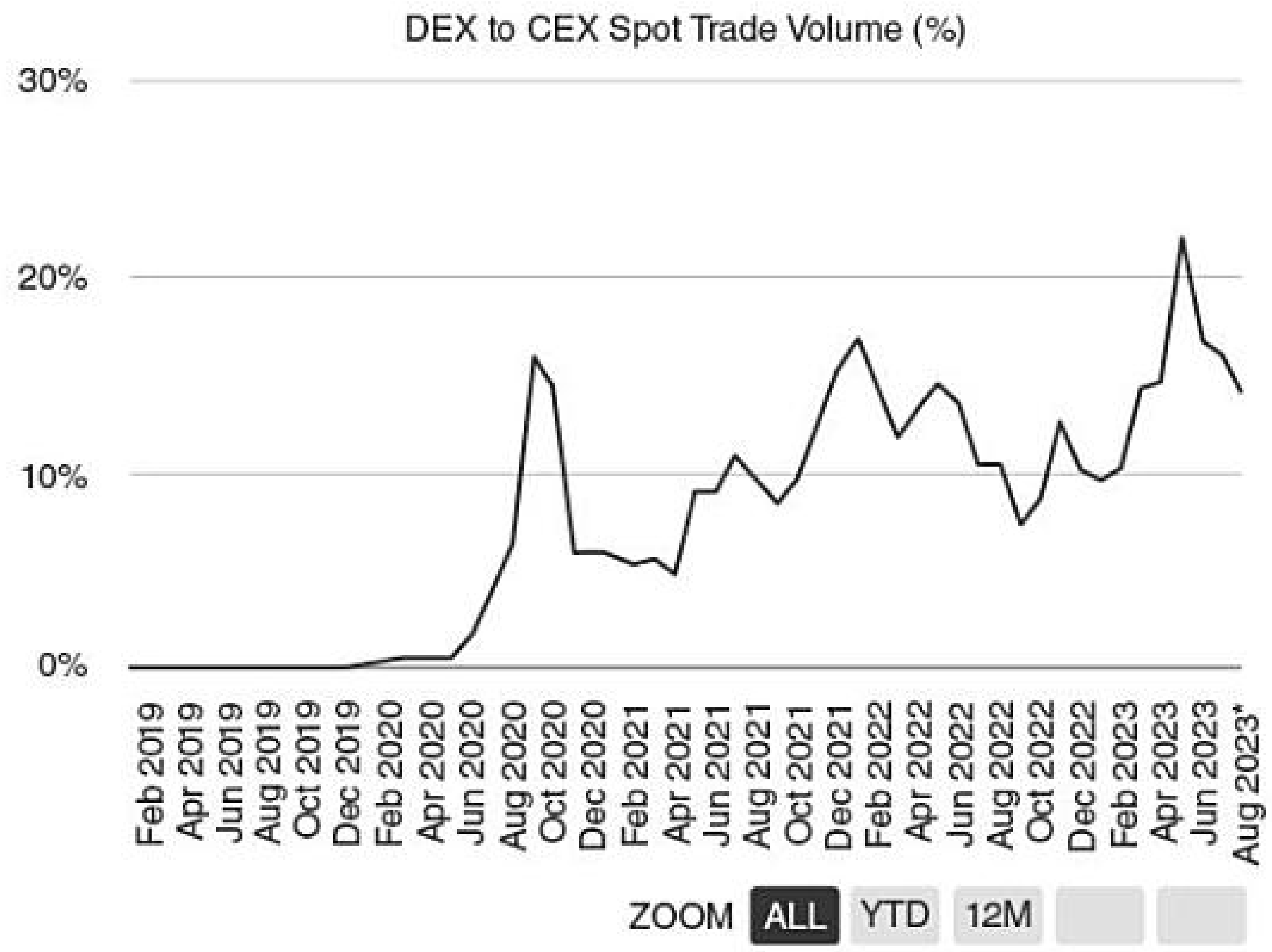


Figure 1.7 DEX to CEX volumes.
Source: The Block, Coingecko

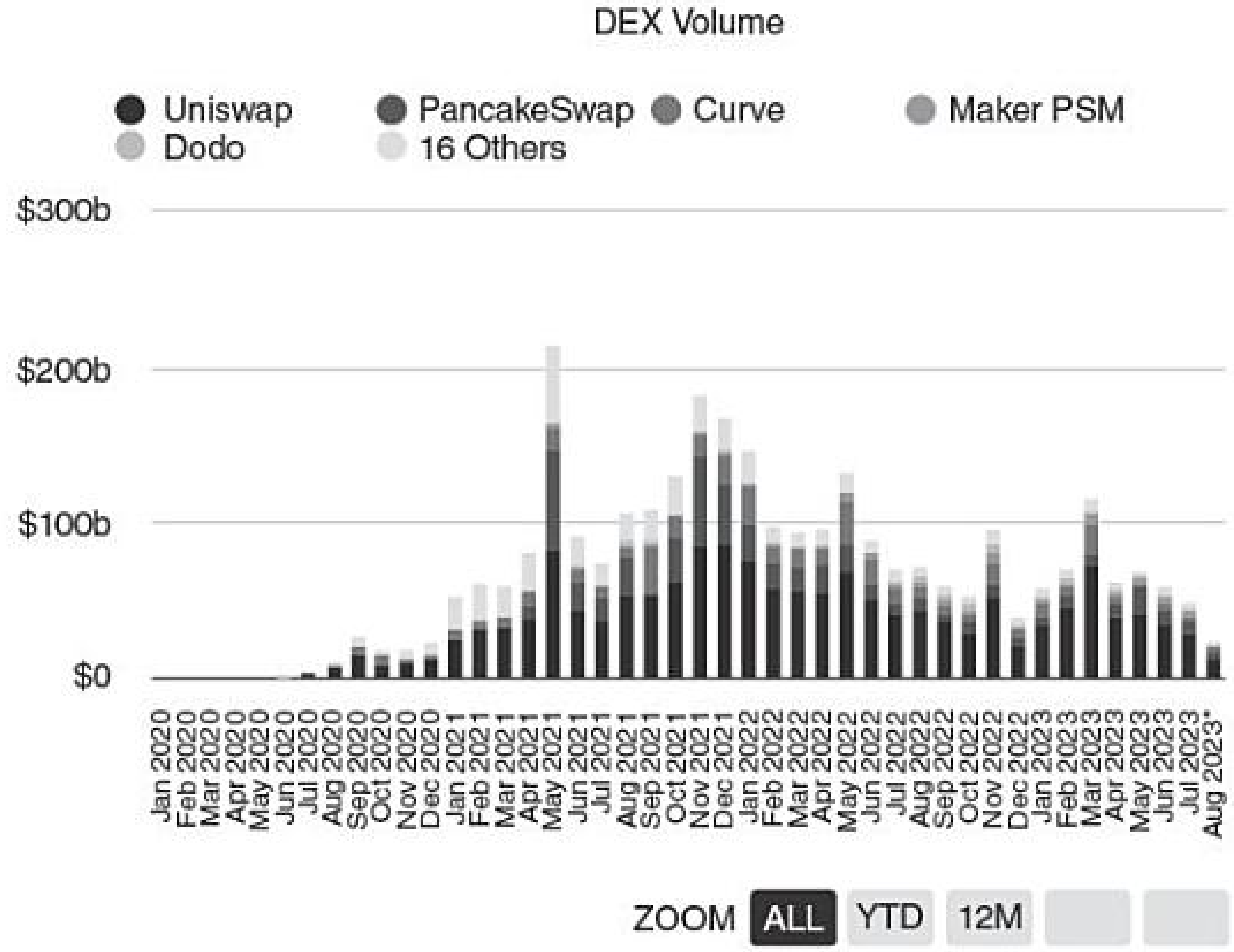


Figure 1.8 DEX volumes.
Source: The Block, Coingecko

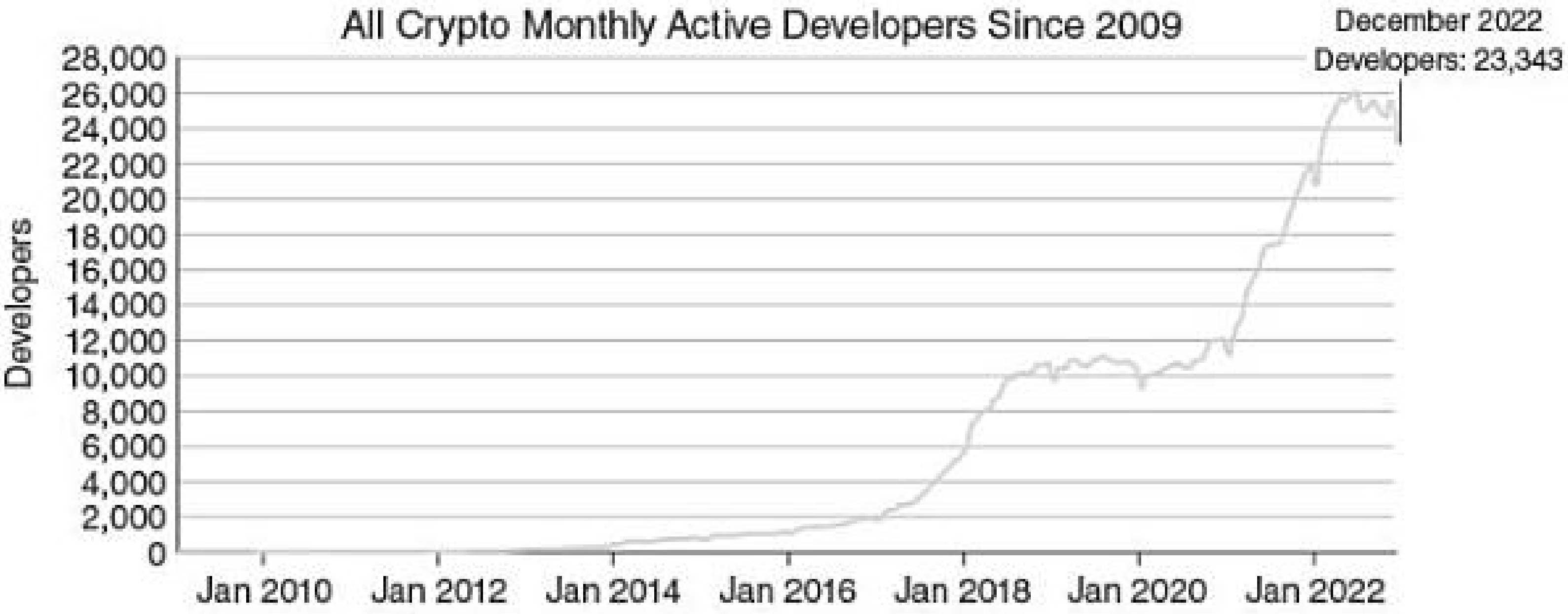


Figure 1.9 Web3 active developers since 2009.

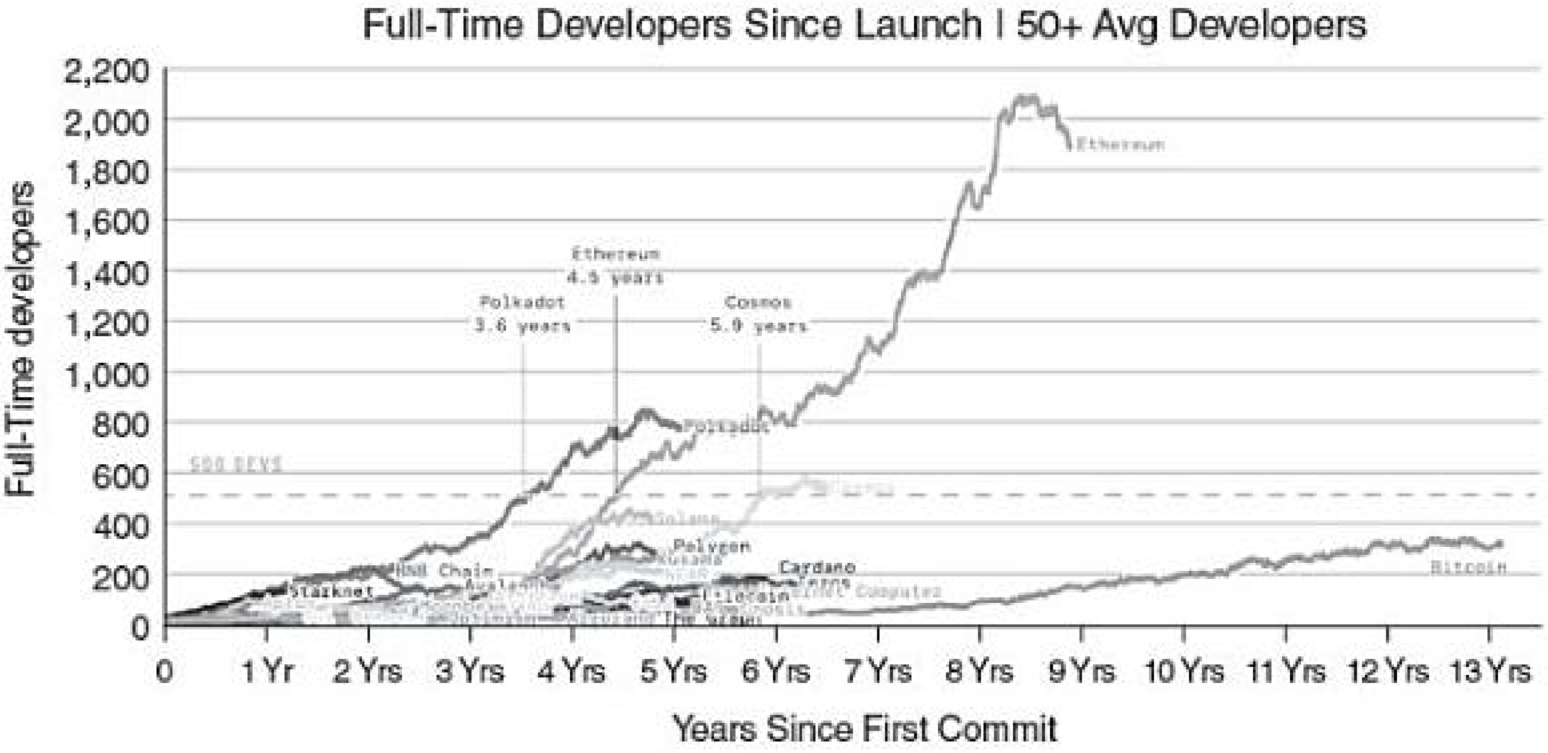


Figure 1.10 Web3 active developers since launch.
Source: Electric Capital Developer Report https://medium.com/electric-capital/electric-capital-developer-report-2021-f37874efea6d

From Figure 1.9 we can see that the number of software developers in the Web3 space in total has been steadily increasing to an all-time high of 23,343 in December 2022. Figure 1.10 (an interesting one for anyone looking to compare ecosystems) shows the growth of monthly active developers (on GitHub) since the launch of the blockchain. We see that Ethereum leads the pack, followed by Polkadot, Cosmos and Solana.

There exist a wide variety of ways for entrepreneurs to collaborate and find co-founders offline and online – through local networking events, hackathons, accelerator programs, grant programs, discord channels, and online forums.

In December 2021, *The New York Times* ran an article about tech executives and engineers quitting big tech companies such as Google, Meta, and Amazon to join crypto.[8] While this should be taken with a pinch of salt (given it was near the height of the last bull market), it highlights the vote of confidence that some of the best and brightest in tech have in crypto.

1.6.2 Institutions

1.6.2.1 Venture Capital Funds

Web3 and Crypto-specific venture capital (VC) funds account for a substantial portion of growth of the industry, and predominantly pursue a long-only strategy. Unlike web2 VCs, who have a longer holding period, web3 VCs can exit and reap the rewards of their investments as soon as tokens become liquid in the market. The lifecycle of web3 investments when tokens are involved tend to be much shorter than the typical 6–10 years in a traditional VC.

Nonetheless, this has been getting longer due to longer vesting periods and a general shift towards higher levels of commitment to the startups (i.e., not selling the token when it suits, but being invested for the longer term, and also participating in governance).

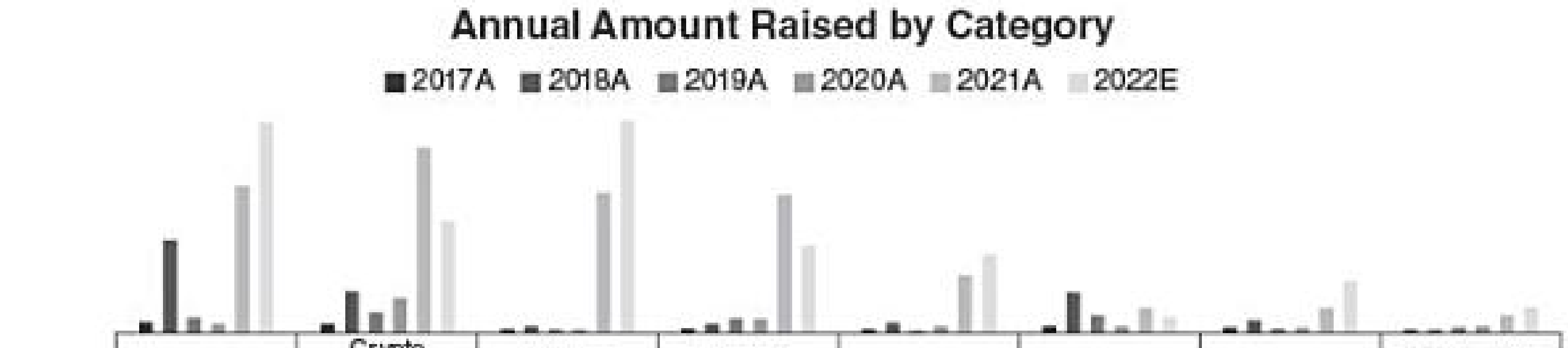
Figure 1.11 presents a detailed breakdown of fundraising across various cryptocurrency categories from 2017 to 2022. It's evident that 2021 and 2022 were notably robust years for investment. This was particularly true for sectors like infrastructure, NFTs/Gaming, and DeFi.[9] Many software and tech VCs have had a strong focus on web3 and DeFi in the last few years, for example a16z, which had closed their fourth crypto fund totaling US$4.5 billion in May 2022, and has raised a total of US$7.6 billion across all crypto funds.

> We are excited about developments in web3 games, DeFi, decentralized social media, self-sovereign identity, layer 1 and layer 2 infrastructure, bridges, DAOs & governance, NFT communities, privacy, creator monetization, regenerative finance, new applications of ZK proofs, decentralized content & story creation, and many other areas.
>
> —*Chris Dixon, a16z*[10]

Traditional VC firms such as Sequoia Capital[11] and Lightspeed Venture Partners[12] have also raised funds focused on liquid tokens and digital assets. Crypto-native VCs (i.e., their first fund was a crypto-specific fund) of note include Paradigm Capital, Multicoin Capital, Pantera Capital, and Polychain Capital. Many crypto exchanges also have their own VC arms, for example, Coinbase Ventures, and Binance Labs.

1.6.2.2 Hedge Funds

Hedge funds are not constrained by long-only strategies or buy and hold mandates. Like their TradFi hedge fund brethren, they employ a wide variety of strategies that may be market-neutral, relative value, arbitrage, discretionary,



	Infrastructure	Crypto Financial Services	NFTs/ Gaming	Trading/ Brokerage	DeFi	Enterprise	Web3	Data/Analytics/ Information
■ 2017A	$0.4	$0.4	$0.0	$0.2	$0.1	$0.2	$0.2	$0.0
■ 2018A	$3.6	$1.7	$0.3	$0.3	$0.4	$1.6	$0.4	$0.1
■ 2019A	$0.6	$0.8	$0.1	$0.5	$0.1	$0.6	$0.2	$0.1
■ 2020A	$0.4	$1.4	$0.1	$0.5	$0.3	$0.2	$0.2	$0.2
■ 2021A	$5.8	$7.3	$5.5	$5.4	$2.2	$1.0	$0.9	$0.7
■ 2022E	$8.2	$4.4	$8.3	$3.4	$3.0	$0.6	$2.0	$1.0

THE BLOCK | Research

Figure 1.11 Crypto / blockchain deals in 2017–2022 by category.
Source: The Block Research
Note: Amount in billion US Dollars.

event-driven, or quantitative in nature. DeFi hedge funds may look for discrepancies in cryptocurrency prices across DEXs, CEXs, and across different blockchains and look to lock-in short term, market-neutral profits. Hedge funds may also engage in yield-farming, staking, and borrowing / lending with DeFi applications and protocols.

The (now) infamous Three Arrows Capital (that has been in the news due to its meteoric rise[13] and fall[14]) had their origin in FX trading and at their peak their NAV was rumored to be in the multiple billions.

1.6.2.3 Market Makers

Jump Trading, GSR, Cumberland DRW, Wintermute, and QCP Capital are some of the largest market makers in crypto, and are engaged in making markets in the thousands of cryptocurrencies trading both on centralized and decentralized exchanges. Many have their origin from making markets in TradFi equities, commodities, FX, and other derivatives, and employ sophisticated HFT technology and techniques to capture spreads with the use of algorithms. When you are trading on an exchange, you might well be trading with one of these institutions.

1.6.2.4 Exchanges

Some of the largest decentralized exchanges are Uniswap, SushiSwap, PancakeSwap, Curve Finance, Serum, Raydium, and dYdX. A hallmark characteristic of DEXs is that they are permissionless: they do not need KYC (Know-your-customer) information to trade. These can be automated market makers or limit order book-based. We will examine how these work in greater detail in Chapter 3.

1.6.2.5 Foundations and L1s / L2s

Blockchains such as Ethereum, Avalanche, Solana, Binance Smart Chain, Polkadot, Polygon, NEAR, Algorand, Cosmos, and Tezos will all have a corporate structure that promotes the multi-fold mission of encouraging developers and startups to build on their blockchain, validators and miners to dedicate capital and hardware resources to mine / validate their blockchain, and investors (retail and institutional) to invest in their native token. Funds can be raised through crowdsales of their native token or through venture capital.

This could be in the form of a non-profit entity (e.g., Ethereum Foundation) that disburses grants to accelerate the growth of the ecosystem, promote its open-source software, and organize conferences. For-profit software development companies such as ConsenSys (specializing in the Ethereum blockchain) develop decentralized software services and applications for the blockchain. These software development companies work for corporations and governments looking to build projects on the specific blockchain ("Layer Ones – L1s") as well as derivative networks ("Layer Twos – L2s").

1.6.2.6 Retail Investors and Users

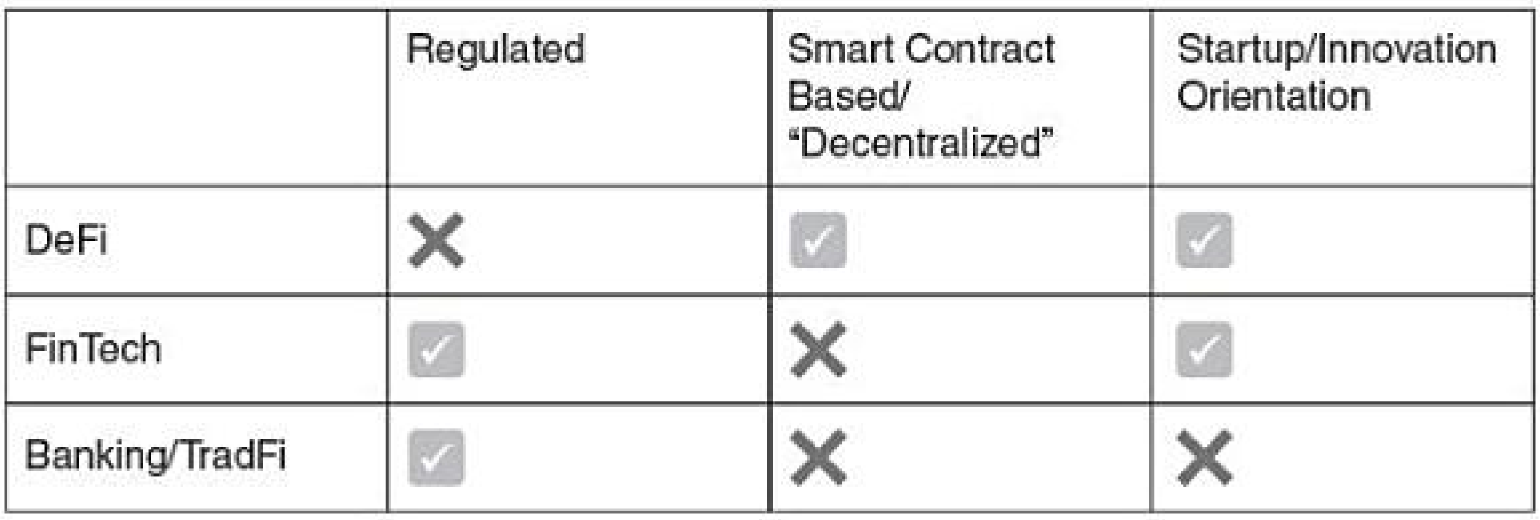
DeFi has become a mainstay for many crypto users as it is very convenient to perform transactions on DEXs. DEXs have enabled for a long-tail effect (i.e., being able to enable liquidity for many more tokens that would otherwise not be available on CEXs) and the best price for a less liquid token is often found on a DEX.

Automated market makers such as Uniswap pioneered the ability for retail investors to participate in the upside of market making, which traditionally was only available to large and sophisticated trading houses (as mentioned earlier). Retail investors can deposit crypto-assets to liquidity pools and receive LP (liquidity provider) tokens as representations of pro-rata shares of the total pool. Liquidity providers earn prorated trading fees charged by the pool, and sometimes the native token of the platform by participating in these activities. Such innovations are also beginning to translate to more complex products such as options with decentralized options vaults (DOVs).

Other methods of earning yields on DeFi platforms include lending, borrowing, and staking. Investors who believe in the growth potential of DeFi platforms may also hold tokens in DeFi applications. The value of these tokens may be derived from the potential and utility of the application or other kinds of business models. The DeFi Pulse Index, maintained by DeFi Pulse, is one example of an index of liquid DeFi tokens[15] on Ethereum, which includes Uniswap, Aave, Maker, Synthetix, Compound, Yearn, SushiSwap, and Kyber.

1.6.2.7 Traditional Institutional Investors

An increasing number of institutional investors are becoming more interested in DeFi in large part due to the yields that are much higher than in TradFi,



	Regulated	Smart Contract Based/ “Decentralized”	Startup/Innovation Orientation
DeFi	✗	✓	✓
FinTech	✓	✗	✓
Banking/TradFi	✓	✗	✗

Figure 1.12 Comparisons of DeFi, FinTech and TradFi.

FinTech

Software and technology oriented, regulated platforms that look to disrupt traditional financial services. These are payment services gateways, robo-advisers, neo-banks / digital banks, Buy Now Pay Later (BNPL) platforms, personal finance management platforms, and P2P platforms.

Examples include: PayPal, Stripe, Ant Financial, Adyen, LendingClub

DeFi and FinTech may sound similar, as both are fundamentally software-driven technological revolutions in finance, but DeFi fundamentally uses smart contracts and blockchain technology. FinTech might not utilize blockchains at all. For comparisons see Figure 1.12.

The key characteristics of DeFi are the use of smart contracts and tokens. The global, internet-native nature of token flows and smart contract interaction make DeFi fundamentally different from FinTech. One of the most promising use cases for crypto and DeFi is to enable more efficient cross-border value transfers, and could reduce costs for remittances and enable a greater degree of financial inclusion, since these costs tend to impact the poor more. Money movements within DeFi take place on blockchains which are global by default. FinTechs for the most part are regulated by a local financial authority or regulator, and will nearly always build in processes to satisfy know your customer / client (KYC), anti-money laundering (AML), and combatting the financing of terrorism (CFT) requirements.

The usage of digital assets / crypto is thus part of this disintermediation. We can also say that DeFi is a subset of FinTech, given that FinTech is much about the use of software in disintermediating human labor. Nonetheless, it is my own perception that they are still currently used in fairly distinct terms, owing to the narrow definitions of self-custodial, uncensorability, and distributed governance.

1.8 How Can I Try DeFi?

I'm a big believer in learning by doing, and combining theory with practice. I'm assuming you picked up this book with an intent to learn more about this new world. I'm going to stick my neck out and say this: if you haven't bought any crypto before, owning and transacting in a small amount of stablecoin might be one good way to get your feet wet. But let me say this first: *you can participate in DeFi without speculating.* You will need a small amount of crypto to pay for transaction fees, but you can absolutely use DeFi just with stablecoins. I can't guarantee that you won't get hacked or run into technical problems, but there's at least less chance of the value fluctuating wildly than other types of crypto like Bitcoin or Ethereum. It will give you a visceral sense of what DeFi is, beyond the theory.

If you're completely new, here's how I recommend you do it:

1. You'll need to open an account with a reputable crypto exchange.
2. You'll need to transfer some fiat into the exchange and buy USDC and a small amount of the native cryptocurrency of the blockchain you intend to use for "gas" (transaction fees).
3. Download and install the crypto wallet on your phone, mobile browser, or computer.
4. Create your wallet. You'll need to store your private key / seed phrase in a safe place, like a password manager. *Never show anyone else this.*
5. Transfer the USDC from the exchange to your crypto wallet.
6. Voilà! You're now a self-sovereign individual. Try paying your friends and family with USDC next time you split the check.
7. When you're done with the experiment, convert the USDC back into fiat via the exchange and back into your bank account.

Here are some recommendations:

Stablecoin: USDC
Blockchain: Solana or Polygon. Both have low gas fees and should not require more than a few dollars of SOL or MATIC for a few transactions
Wallets: Metamask (Polygon, Browser-based), TrustWallet (Polygon, Mobile-based) or Phantom (Solana, Mobile-based)

Cybersecurity and cyber hygiene are key skills while swimming in the shark infested waters of crypto. Store your private keys / seed phrases carefully and don't interact with applications you don't trust. Be careful of phishing attacks, and other kinds of scams that proliferate on Telegram, Discord, and the general crypto sphere. You've been warned!

If you're going deeper, you might want to buy a hardware wallet such as a Ledger Nano S. Hardware wallets can be used with browser wallets such as Metamask and Phantom and are a safer way of transacting in DeFi.

1.9 Where Does DeFi Meet TradFi?

At present, DeFi–TradFi links are still experimental due to the numerous challenges of compliance and risk as mentioned earlier. This could change as technology, operations, standards, and risk management improves in DeFi. Let's discuss some of the major crossovers that currently exist with DeFi and TradFi.

1.9.1 Stablecoins

Stablecoins are an important topic in DeFi and are arguably the biggest crossover point between DeFi and TradFi. We'll cover stablecoins in more detail in Chapter 2, but here is a brief overview.

Stablecoins are digital assets that circulate on public blockchains such as Ethereum, and are 1:1 representations of fiat currency. Some of them may be actually stable and some may not be. I say this beforehand because the label itself may mislead people into thinking that they are actually stable, when very often it is an aspiration. (See the UST / Terra collapse) They are issued by private companies who may or may not hold an equivalent amount of fiat (or short-term debt) in reserve to back the quantity of stablecoins they create.

The two largest in circulation are USDT and USDC (issued by Tether and Circle respectively) and have market capitalizations of US$66.5 billion and US$54.2 billion respectively at time of writing (Aug. 2022). Stablecoins are increasingly being used for cross-border transfers and a stable store of value that is crypto-native. They are used extensively in DeFi in liquidity pools, borrowing / lending platforms, and other staking and trading operations.

Stablecoins are a major bridge between crypto and fiat as they are representations of real-world value, but exist in a crypto-native infrastructure.

1.9.2 Central Bank Digital Currencies (CBDCs)

The parallel innovation that Bitcoin and crypto have spurred at the central banking level of finance (i.e., above the commercial banking layer) is with Central Bank Digital Currencies (CBDCs). The major difference here between stablecoins and CBDCs is that stablecoins are issued by private companies, whereas CBDCs are issued by central banks and governments. Which would you trust? Which would you hold? For the vast majority of people and businesses, the answer is fairly clear. The counterparty risk with CBDCs is much lower than that of stablecoins.

Strictly and technically speaking, CBDCs are not a part of DeFi yet. Most CBDCs pilots have been on permissioned networks and not public blockchains. It may seem odd to some, especially the libertarians, to be even discussing CBDCs in a book about DeFi. Nonetheless, I think this is a topic well worthy of coverage, given some of the latest developments with central banks. If governments eventually decide to utilize CBDCs on public blockchains, it would represent a quantum leap in DeFi adoption and utilization.

CBDCs and stablecoins may also combine in ways that harness the best in each system, in what Tobias Adrian, Financial Counselor and Director of the Monetary and Capital Markets Department at the IMF, has called a "synthetic CBDC" (sCBDC). In an sCBDC system, stablecoins may be used by the private sector and harnessing the innovative potentials of the private sector in distribution, interoperability, and utilization of money, whereas CBDCs are used as collateral for the stablecoins.

> A synthetic CBDC is essentially a public–private partnership that encourages competition between eMoney providers and preserves comparative advantages. The private sector concentrates on innovation, interface design, and client management. And the public sector remains focused on underpinning trust.
>
> —Tobias Adrian, Stablecoins, Central Bank Digital
> Currencies, and Cross-Border Payments:
> A New Look at the International
> Monetary System, May 2019.

In March 2022, the central bank of Brazil – the Banco Central do Brasil (BCB) – selected a number of crypto, DeFi, and FinTech companies such as Aave, Visa, ConsenSys, and Microsoft as part of the Lift Challenge Real Digital to develop pilot projects to evaluate CBDC use cases.[18]

1.9.3 Real World Assets (RWA) and Tokenized Assets

There are a number of startups and companies looking to bring real world assets on-chain, or otherwise connect real world assets with crypto. Most of them involve tokenizing the asset and could involve asset pools, which aggregate and segment the risk. Some of them that have a public-facing website are: Credix, Goldfinch, Maple, TrueFi, and Centrifuge. (Disclosure: I am an investor and advisor to Credix.)

Credix is a credit marketplace that currently enables FinTechs in Latin America to source for debt investors using USDC on Solana,[19] and currently has a loan book of US$17.5 million. Institutions that are already participating in DeFi can access yields up to 14% APY that are diversified from the more cyclical DeFi yield market. The onus of credit scoring and screening is left to the FinTechs and Credix facilitates the on-chain to off-chain value transfers and credit pool structuring.

Centrifuge takes an "asset-agnostic, wide-ranging approach that allows users to bridge limitless forms of RWA over to the DeFi space."[20] Centrifuge currently has a wide range of assets listed on its platform, ranging from real estate loans, revenue-based financing, and cash advances from a variety of issuers.

Unlike other DeFi platforms, the majority of RWA platforms require KYC identification, which may be issued in the form of a non-transferable token, and may be available for accredited investors only.

On the institutional side, two examples of bond issuance on public blockchains include the SocGen issuance of €100m of covered bonds in 2019, and another €100m, 2-year bond by the European Investment Bank (EIB), in collaboration with Goldman Sachs, Santander, and SocGen in 2021.[21] The EIB digital bond project was also selected for Banque de France's CBDC program. Both were issued on the Ethereum public blockchain. Some have taken to calling this method of bond issuance on blockchains as "smart bonds."[22]

1.9.4 Permissioned DeFi

Permissioned DeFi pools such as Aave Arc and Compound Prime are promising innovations that allow institutional investors to be able to participate in DeFi. These are institutional versions of the publicly available Aave and Compound platforms, but satisfy institutional requirements for KYC, AML, and CFT compliance, as well as enterprise-grade security. These networks consist of known institutional participants that are whitelisted by RegTech providers such as Fireblocks.[23]

We'll also examine the innovations of some TradFi institutions, such as central banks and commercial banks, that are exploring what is being referred to as institutional DeFi in Chapter 9. For these institutions, controlling access is critical for compliance and regulatory reasons, and there are several techniques to achieve this.

1.10 What are the Risks of DeFi?

DeFi is definitely a nascent and experimental field where there are many risks. One should be aware of these risks before investing significant amounts into DeFi. For anyone monitoring the news about crypto – it should be clear – not a week goes by without a hack or bug in crypto causing multimillion dollar losses. These losses occur as a result of cybersecurity issues, operational risks, technological risks, and other systemic risks in DeFi. Frontrunning (MEV) occurs frequently and retail users may not even realize they are front (and

2

Infrastructure and Instruments

2.1 The Infrastructure of DeFi

What is a blockchain? What are smart contracts? In this chapter we'll unpack some of the core technologies that drive DeFi. For many of us (read: not software engineers), the deep inner workings of computer science will be less relevant and we will only need to know the basics or a high-level understanding, in the same way most people don't really know how their car works. What's more important is to know how to drive, and what the risks are with driving. I'll be doing this in the same vein, and providing you with a high-level understanding so at least you'll be able to appreciate how DeFi works.

Nonetheless, if you are technical, and want a full understanding of how Bitcoin and Ethereum works – I recommend you check out *Mastering Bitcoin* (Antonopoulos 2017) and *Mastering Ethereum* (Antonopoulos and Wood 2018). Both will go into the details of the computing, mathematics, and protocol architecture, using Bitcoin and Ethereum as the key examples. Those details may not be relevant to all blockchain systems, but they are a great starting point.

There have been many building blocks before DeFi, and this chapter will describe some of the background, mostly surrounding Bitcoin and Ethereum. Ethereum was the first L1 and the first smart contract platform, and many of the first DeFi applications such as Uniswap and Compound were built on them. Currently, there is an intense competition between many of the newer L1s such as Solana, Polkadot, NEAR, and Avalanche for flows. In the same way that MacOS and Windows can result in totally different types of applications – DeFi ecosystems can differ as well, depending on the L1.

Decentralizing Finance: How DeFi, Digital Assets, and Distributed Ledger Technology Are Transforming Finance, First Edition. Kenneth Bok.

2.2 Basics of Blockchains

Blockchains are a shared and immutable list of records (blocks) that are sequentially linked to each other with cryptographic methods (Figure 2.1). Sometimes also referred to as *distributed ledger technology* (DLT), blockchains combine several technologies and methods in their implementation, including distributed computing, cryptography, and economic incentives. Blockchains enable trust through the security of the network. They maintain a common and constantly updating source of truth, among a large set of parties that may not trust each other.

Public blockchains enable participants to interact, transact, and contribute to the network in a permissionless fashion: no authorization from any centralized party is required. Validators (miners) maintain the network in exchange for economic rewards: usually the native crypto-asset of the blockchain. Blockchains are also usually transparent. Transactions can be viewed publicly with the use of block explorers or through running one's own node.

The first blockchain, Bitcoin, was created by the pseudo-anonymous Satoshi Nakamoto in 2008. It was the first cryptocurrency to solve the *double-spending problem* in a decentralized system. The design of Bitcoin has inspired other blockchains such as Ethereum, which was the first of many subsequent *general-purpose blockchains*, representing a dramatic upgrade in capability, namely, allowing for blockchains to run code, execute smart contracts, and act as a global computer. These properties enabled DeFi to emerge.

General-purpose blockchains, also referred to as "Layer 1s" or "Layer 2s" (L1s / L2s), are the fundamental operating layers of DeFi. In particular, since Ethereum was the earliest L1 and has the most active DeFi ecosystem, we will use Ethereum as the prime teaching example in this book, for describing how general-purpose blockchains work, and for the DeFi applications built on top of these L1s. This is not to say that another L1 could not overtake Ethereum in

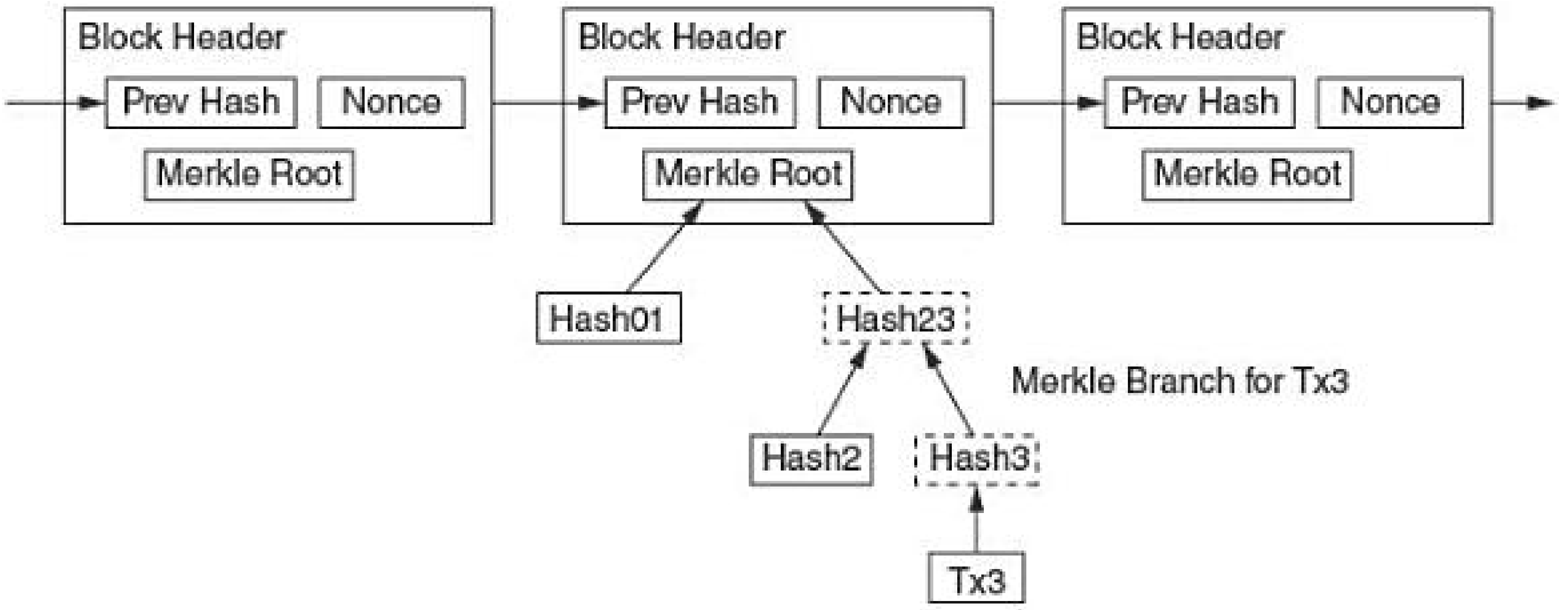


Figure 2.1 Blockchain structure.
Source: Bitcoin White Paper, Satoshi Nakamoto[1]

the future: innovation in this space is rapid and the possibilities are open-ended. We'll also take a brief look at how L1s compare to one another and what characteristics they are compared against.

2.2.1 Components of Blockchains

Blockchains usually consist of the following:

- A peer-to-peer (P2P) network that connects users and nodes;
- A set of rules that determine how consensus in the network is achieved (consensus algorithm);
- A chain of records (blocks) that are cryptographically linked together, that acts as the verified and valid record of the system;
- An incentivization and payment scheme that rewards and charges various actors in the network for providing and using resources;
- A set of rules for the emission of the native cryptocurrency; and
- Open source software implementation of the above (clients).

2.2.2 Cryptography

Cryptocurrencies got their colloquial name, "crypto," from cryptography. The Ancient Greek root of crypto, *kryptós*, means "hidden or secret." Cryptography has a large role to play in keeping the internet safe: this is the same technology that ensures your messages on instant messaging platforms are safe from prying eyes, and that your credit card numbers, passwords, and other sensitive information are kept secure when you enter them on e-commerce sites and other software platforms. Cryptography is also a key technology in blockchain. Three main methods of cryptography that are used in blockchains are *hash functions*, *public key cryptography*, and *digital signatures*.

2.2.3 Hash Functions

> *One-way hash functions are a cryptographic construct used in many applications. They are used with public-key algorithms for both encryption and digital signatures. They are used in integrity checking. They are used in authentication. They have all sorts of applications in a great many different protocols. Much more than encryption algorithms, one-way hash functions are the workhorses of modern cryptography.*
>
> —Bruce Schneier[2]

Hash functions transform data of arbitrary size to a fixed size. Hash functions are one-way, meaning that they are used to transform the input to the fixed size output, it is impossible to generate the original input just with the hash. Why is this useful?

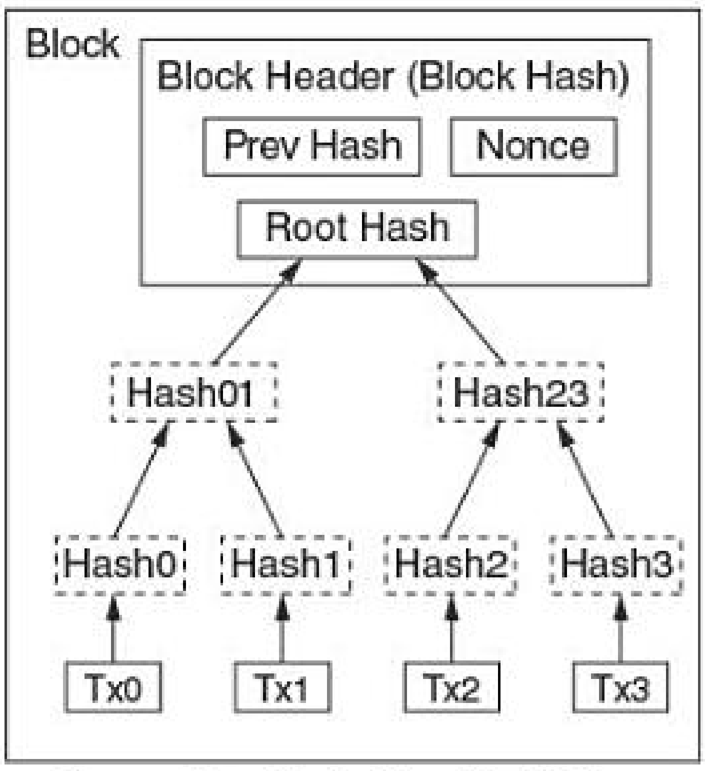


Figure 2.2 Merkle Tree in a blockchain.
Source: Bitcoin White Paper, Satoshi Nakamoto[3]

Hash functions are what link (or chain) the blocks together. They're an easy way to determine if the original data have changed, and serve as a method of data fingerprinting. A fingerprint is a small, verifiable imprint of your uniqueness: the same is true for a hash. Merkle trees (Figure 2.2) are a way to combine hash functions and allow for "efficient and secure verification of the contents of a large data structure."[4]

Hash functions are also used in proof-of-work-based blockchains such as Bitcoin. This is why Bitcoin miners are measured in "hash rate" or "hash power" – this is their ability to perform a number of hashes a second.

Cryptographic hash functions are specific types of hash functions that have special properties that are useful for blockchains. Ethereum utilizes the Keccak-256 cryptographic hash function and a special type of Merkle tree called Patricia Merkle trees.

2.2.4 Public-key Cryptography and Digital Signatures

Public-key cryptography (PKC) is a system that uses pairs of keys: a public key (viewable and shareable by others) and a private key (to be kept secret by the owner). Public keys are derived mathematically from the private key. In Ethereum, public addresses are similar to bank account numbers, and private keys are similar to the PIN code used to access the account. PKC allows for the authentication and verification of transactions.

Let's look at two examples to illustrate the basic workings of PKC. In the first case (Figure 2.3), Bob wants to send a message to Alice. He knows her public key but not her private key. He encrypts the message with Alice's public key

2.3 Bitcoin and Ethereum

> *Think of the difference between something like a pocket calculator and a smartphone, where a pocket calculator does one thing, and it does one thing well. But really, people want to do all these other things. And if you have a smartphone, then you have a pocket calculator as an app, you have a music player as an app, you have a web browser as an app, and pretty much everything else. So basically, [Ethereum is] taking that same kind of idea of increasing the power of the system by making it more general purpose and applying it to blockchains.*
>
> —Vitalik Buterin

This quote was a good analogy that Vitalik Buterin, the inventor of Ethereum, gave to describe the difference between Bitcoin and Ethereum. Bitcoin does one thing well: tracking where each Bitcoin is, and who owns how much Bitcoin at any given time. The *consensus state* of Bitcoin is relatively simple: the ledger of the units of Bitcoin and the addresses.

Ethereum does the same task of maintaining a consensus state, but with a *data store*. Whereas Bitcoin is money on a blockchain, this is what makes Ethereum a computer on a blockchain. Since this is getting technical and deep into computer science land, let's hear from one of the creators of Ethereum, Gavin Wood:

> Ethereum tracks the state transitions of a general-purpose data store, i.e., a store that can hold any data expressible as a key–value tuple. A key–value data store holds arbitrary values, each referenced by some key; for example, the value "Mastering Ethereum" referenced by the key "Book Title." In some ways, this serves the same purpose as the data storage model of Random Access Memory (RAM) used by most general-purpose computers. Ethereum has memory that stores both code and data, and it uses the Ethereum blockchain to track how this memory changes over time. Like a general-purpose stored-program computer, Ethereum can load code into its state machine and run that code, storing the resulting state changes in its blockchain. Two of the critical differences from most general-purpose computers are that Ethereum state changes are governed by the rules of consensus and the state is distributed globally. Ethereum answers the question: "What if we could track any arbitrary state and program the state machine to create a worldwide computer operating under consensus?"
>
> —Mastering Ethereum, *Andreas Antonopoulos and Gavin Wood*

This is quite a paragraph, so let's unpack this.

First off – what's a general-purpose computer? There's a computer in your microwave. That's *not* a general-purpose computer. It serves a specific purpose – helping you to heat up your food in the myriad of ways possible – different timings, heat settings, and so on. A general-purpose computer is like a desktop computer, laptop, or a mobile phone: allowing for new software programs to be installed. The architecture of a general-purpose computer allows for all sorts of new functions we haven't even thought of yet. General-purpose computers are open-ended and multipurpose. Another technical term that you might come across when reading about Ethereum's general-purpose nature is "Turing complete."

Second, why would you need a computer that's global? Isn't the internet already a global computer? Aren't platforms like Facebook or Google massive computer networks already?

The answer is that Ethereum allows for anyone with an internet connection to access and interface with it, and that it allows for one shared truth of what the network state is. That is – we can't disagree as to what your token balance is on Ethereum, and we also can't disagree as to whether, say, a program has been run or not. We can't disagree on the effects of that program either. Ethereum ensures agreement, amongst any party that decides to use Ethereum. Isn't that amazing?

This also means that transactions in Ethereum are quite unlike those on FinTech platforms or banks, where it is possible to contact them and reverse the transaction if it was made in error. There is no-one to call and transactions are irreversible on public blockchains.

In short, Ethereum is a world computer that tracks and maintains a consensus state. Computers run programs. Nodes in Ethereum thus maintain consensus of state changes that are caused by users or programs.

If you're still confused about this, don't worry. It will become clearer as we move along with the decentralized applications.

There are many aspects to cover as to how Ethereum works: accounts, smart contracts, transactions, and tokens to begin with. But first, a brief overview of permissioned and public blockchains.

2.4 Permissioned vs Public Blockchains

One of the big dividing lines between blockchains that you will find is between the permissioned and public blockchains. The line is sometimes not so obvious in the way different companies and individuals market the term "blockchain." The result is that newcomers to blockchain will find it confusing as they read different books, listen to different speakers on the internet, and so forth. So let me shine some light on this, based on my experience, so you are at least aware of what this dividing line is and why it exists.

Permissioned blockchains limit nodes on the network to *known* participants. This implies two key points that cause many dramatic differences with public blockchains. As the name suggests, permissioned blockchains require permission to join the network. This implies that someone, or some entity has the authority to admit or prohibit new participants into the network. This implies centralization. That is the first point.

The second difference is around network resources. Why would someone want to contribute resources – hardware, software, capital, and labor – to a network? For public (permissionless) blockchains, the incentive is the native crypto-asset of the network. Validators and miners contribute resources to the network in order to earn these rewards. Crypto-assets also are used to pay for utilization of network resources, "gas," and prevent users from spamming the network.

Permissioned blockchains are usually privately funded by the enterprises (or consortium) that decide to use them. The motivation for participants in permissioned blockchains tend to come from specific mandates of these enterprises or consortia. This allows for permissioned blockchains not to have a native crypto-asset at all.

Some permissioned blockchain platforms include Hyperledger (from the Linux Foundation, with multiple variants), Corda (from R3), and Quorum (a permissioned version of Ethereum). They are often used in enterprise settings where specific requirements such as KYC / KYB (know your client / business) and other compliance requirements favor more control and knowledge about the network. Scalability of these networks may also be higher.

Nonetheless, due to the centralization of permissioned blockchains, some argue that permissioned blockchains do not provide the key feature of trustlessness through the network.

Metcalfe's law estimates that the value of a network is proportional to the square of the number of the users of the network. It's hard to argue against the success of public blockchains in this regard. Public blockchains enable anyone with an internet connection to access crypto, join, and build on the network if they so wish. The network effects achievable with open and interoperable systems is very significant.

Nonetheless, permissioned blockchains definitely have a place in solving problems in highly regulated industries such as finance where there are strict compliance requirements on banks. The sheer volume that financial institutions transact is a major factor in favor of permissioned DLT. The difference between the two could well be a "B2C vs B2B" type of distinction. We will discuss permissioned blockchains in more detail in Chapter 6.

2.5 L1s and L2s

Remember how I said that general-purpose blockchains, or L1s, are the fundamental operating layers of DeFi? Well, this begs the question, which other L1s are there? How do they compare? How do they interact? How do they create different DeFi capabilities? While a full analysis and explanation of different L1s is simply too much detail to go into for the purposes of this book, let me highlight some of the key characteristics of L1s. Let's take a look at two tables from Galaxy Digital Research (Tables 2.1 and 2.2).

The *consensus algorithm* (Table 2.1) is the method in which blockchains reach agreement about the present state of the ledger. It must take into account how some nodes might fail, or behave in ways that are harmful or irresponsible. Two that you will commonly find are proof-of-work (PoW) and proof-of-stake (PoS). Most blockchains are moving towards PoS as it is more energy efficient, allows for greater decentralization, and it allows for sharding (resulting in greater throughput). In PoW systems, the longest chain of blocks is the valid version of the blockchain. In PoS systems, nodes may lose some of their stake in a mechanism known as "slashing" – penalties that are imposed due to downtime or double-signing. Both are behaviors that the network seeks to minimize. Consensus algorithms detail these rules for nodes, in computer code. Consensus algorithms also have important consequences on the security of blockchains.

The *transactions per second (TPS)* metric seeks to measure the throughput of the L1. This is a key metric as it looks to measure how fast a blockchain can process transactions. This is also where a great deal of innovation is happening to deliver high throughputs with newer L1s. By comparison, Visa can handle over 24,000 TPS[5] and PoW Ethereum can handle 15 TPS (PoS Ethereum looks to upgrade this significantly to 100,000 TPS). The speed of a blockchain tends to be higher in more centralized and less secure blockchains, as Vitalik Buterin's trilemma (Figure 2.5) suggests:

The trilemma posits that only two out of the three key attributes of scalability, decentralization, and security can be achieved in a blockchain.

Decentralization of a blockchain can be measured in a few ways. The first: the concentration of the validator or miners according to percentage of total stake or hash power. The Herfindahl score, a measure used in competition law and antitrust policy, can be computed using the squares of the stake (or hash power) of the validator set.

The other way to estimate decentralization is by the barrier to entry for validators. This is represented in Table 2.2, which lists the requirements of a validator node, for proof-of-stake systems. The higher the requirements, the less decentralized the blockchain will be.

EVM dApp support refers to the ability of the L1 to interface with Ethereum-based systems. This could be in the form of browser plug-ins, block explorers,

Table 2.1 Layer 1 comparisons.

Network	Consensus	Launch	Market Cap	DeFi TVL	% of Supply Staked	Annual Inflation Rate	Block Time (sec)	Transactions Per Second	EVM dapp Support
Ethereum	PoW	2015	$536bn	$163bn	6.80%	4.20$	13.35	15*	Yes
Binance Smart Chain	PoS/PoA	2020	$89bn	$32.2bn	76%	-2.35%	3	55-220	Yes
Solana	PoS/PoH	2020	$68bn	$12.4bn	78%	7.50%	0.53	50,000	Upcoming
Cardano	PoS	2017	$66bn	0	70%	5.70%	20	250	Upcoming
Polkadot	PoS	2020	$55bn	$321m	56%	10%	3	100,000**	Upcoming
Terra	dPoS	2019	$17bn	$9.8bn	35%	1.34%	6.6	10,000	No
Avalanche	PoS	2020	$15bn	$8.7bn	57%	5.57%	1.9	4,500	Yes
Algorand	pPoS	2019	$11bn	$83m	48%	29%	4.4	1,200	No
Internet Computer	PoS	2020	$8bn	Unknown	49%	Uncertain	0.12	Uncertain	No
Near	PoS	2018	$5bn	$45m	39%	5%	1	100,000	Yes
Tezos	PoS	2018	$280m	$147m	75%	4%	31	40	No

Source: Galaxy Digital Research
Data: Protocol Blogs, CoinGecko, Coin Metrics, Defi Llama, Various Other Sources
* ETH2 is estimated at 100k TPS:
** Polkadot is an estimate

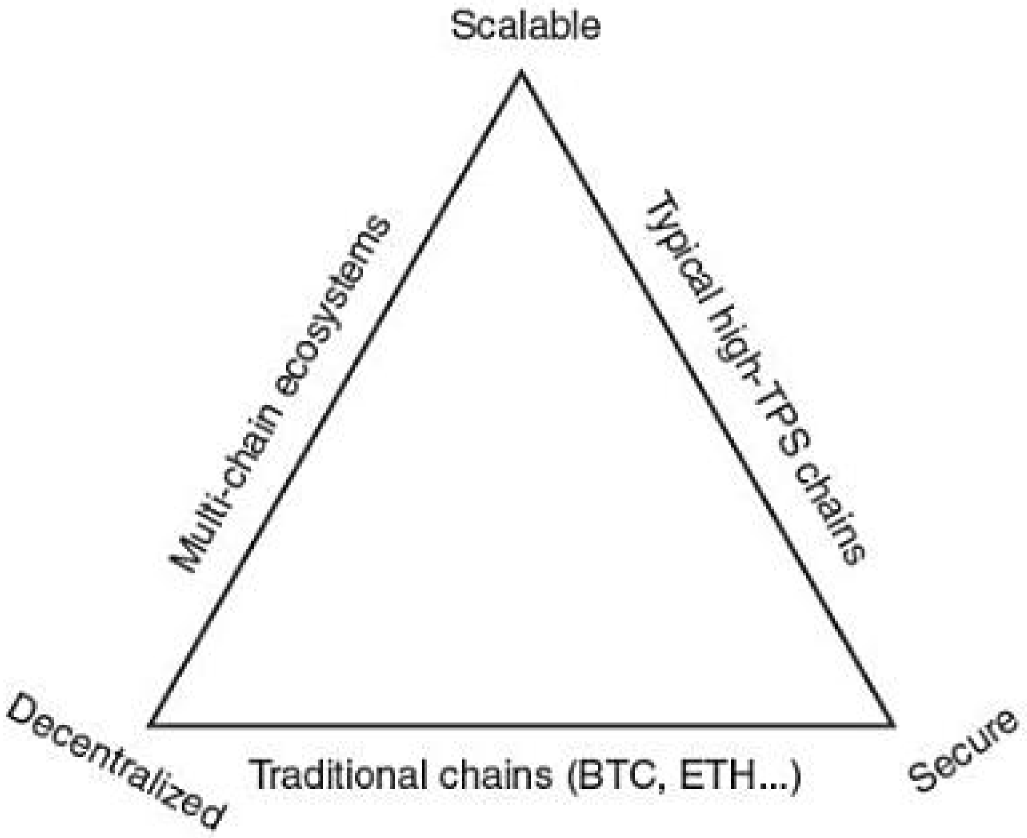


Figure 2.5 The blockchain trilemma.
Source: Vitalik Buterin's blog[6]

infrastructure, and tools that are already available for the Ethereum ecosystem. There is still a large advantage for L1s to be Ethereum virtual machine (EVM) compatible, as there will be a pre-existing base of users, developers, and infrastructure providers. The Metamask plug-in developed by ConsenSys, for example, has over 10 million monthly active users.[7]

Another dimension (not in Table 2.1) is *monolithic vs modular* blockchains. Some have also labeled modular blockchains as heterogeneous blockchains.[8] Some examples of modular / heterogeneous blockchains include Polkadot, Cosmos, Celestia, Polygon, and Avalanche. Modular blockchains allow for developers to create sub-blockchains, usually linked to the main blockchain, which can be built in a modular fashion. Modular blockchains may be composed depending on specific requirements that may utilize different execution, settlement, consensus, and data availability characteristics. Again, these may have implications on security, decentralization, and scalability of these blockchains. Monolithic blockchains like Solana may benefit from the centralization of liquidity within one ecosystem that does not require bridging.

Lastly, *L2s* are scalability solutions built on top of L1s. The Lightning Network for Bitcoin is one such example of an L2. In Ethereum, some of the leading L2s include Arbitrum, Optimism, zkSync, and Starkware. They may use technologies such as optimistic rollups and zero-knowledge rollups.

2.6 Accounts, Keys, Wallets, and Addresses

Let's come back to the micro and look at how accounts, keys, wallets, and addresses work in DeFi.

2.6.1 Accounts

There are two types of accounts in Ethereum: *externally owned accounts (EOAs)* and *contract accounts*. EOAs have private keys. Contract accounts do not. Essentially, EOAs are controlled by human beings, whereas contract accounts are controlled by smart contracts. When you use MetaMask or a Ledger, you are using an EOA. An example of a contract account would be a Uniswap smart contract for a token swap – liquidity pool. Both EOAs and contract accounts have unique addresses and it is impossible to tell them apart just by looking at the public address.

It is free to create an EOA, whereas it will cost gas to create a contract address (usage of network storage).

Multi-signature wallets are used in settings where the account needs to be owned / controlled by a group of individuals. Just like joint bank accounts, various rules can be set over the authorization of transactions (m-of-n). In Ethereum, a multi-signature wallet must be set-up using a contract account, since multi-signatures are not natively supported by EOAs.

2.6.2 Keys

Public-key cryptography is used to create public and private key pairs for EOAs. Private keys are made of 64 hexadecimal characters. Public keys can be derived from private keys, but not the other way around. Private keys are not used in the Ethereum system directly, and should not be stored or transmitted on Ethereum. Authorization is by means of digital signatures, which are created by the private keys.

In practice, private keys are rarely seen by end-users. They are usually encrypted and stored in special files, and managed by wallet clients. What end-users usually see and use as a proxy for their private keys are mnemonic seed phrases of up to 24 words. This seed phrase can be used to recreate the master private key in a *hierarchical deterministic* wallet.

2.6.3 Wallets

Wallets are systems used to store and manage keys. *Hierarchical deterministic (HD)* wallets (Figure 2.6), secured by a mnemonic seed phrase are common due to a few features:

- Privacy: Different keys can be generated for each transaction, allowing for one's transaction balance and history to be hidden
- Multi-chain: Unlimited number of keys can be generated for multiple cryptocurrencies
- Usability: There is a lower chance of error when writing down the seed phrase (as opposed to a hexadecimal sequence)
- Convenience: In an organizational setting, child keys can be assigned to specific departments

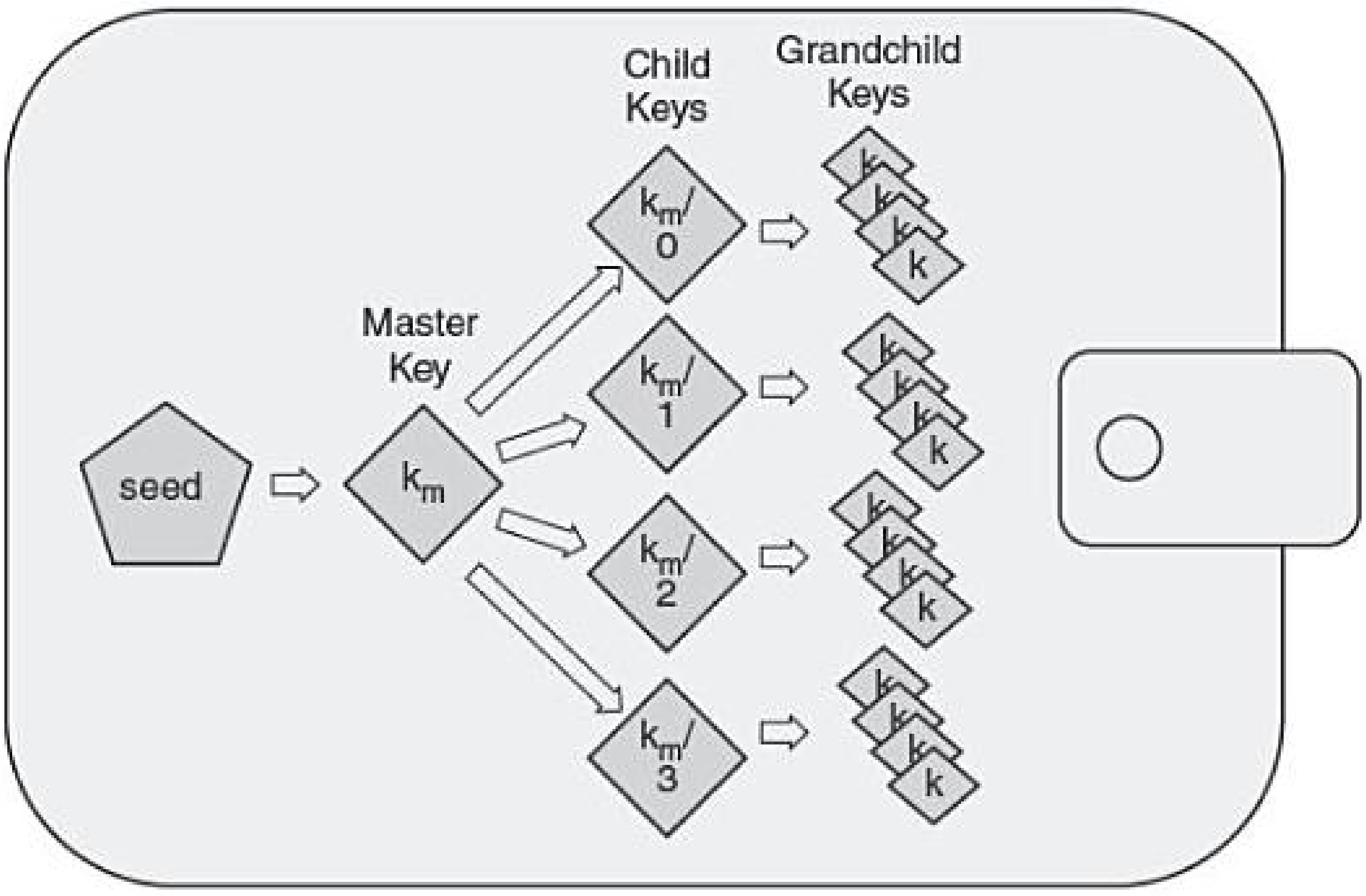


Figure 2.6 Hierarchical deterministic wallets.
Source: *Mastering Ethereum*

A few common standards enable wallet best practices, which are a contribution from the Bitcoin community, including BIP-32, BIP-39, BIP-43, and BIP-44.

2.6.4 Addresses

Public addresses in Ethereum are hexadecimal (base 16) numbers derived from the last 20 bytes of the Keccak-256 hash of the public key. The 0x prefix denotes hexadecimal format.

As an example, here's Vitalik's address: 0xAb5801a7D398351b8bE11C439 e05C5B3259aeC9B (if you're on a digital version of this book, you can click on the address and see what Vitalik holds and his trade history, on Etherscan – the block explorer for Ethereum).

The ability for individuals to choose not to link their real-world identities with their on-chain addresses is what pseudonymity means. In the above example, Vitalik willingly doxed himself, to prove a point.[9]

2.7 Transactions

Transactions are initiated by EOAs. They are signed messages originating from an EOA, transmitted by the network, and recorded on the blockchain. Smart contracts don't run autonomously – they must be called by transactions initiated from EOAs.

Transactions in DeFi have some unique characteristics that set it apart from TradFi.

2.7.1 Block-by-block Settlement

Settlement takes place on a block-by-block level. The more *block confirmations* there are, the more certain that the transaction has actually settled. It denotes the number of blocks that have been mined since the block that included your transaction. The higher the number of block confirmations, the lower the probability of disagreement amongst miners of the version of the blockchain that included your transaction. For example, FTX and Coinbase require 10 and 35 confirmations respectively, for Ethereum transactions to be considered final.

2.7.2 Irrevocable

As mentioned earlier, transactions in DeFi are irrevocable and irreversible by design. There is no central administrator or intermediary to reverse transactions. Mistakes can and do occur.[10] If errors do occur, the only course of remedy is to have the recipients send back the funds.

2.7.3 Composable

This is one of the key novel features of DeFi. Transactions may call multiple smart contracts and EOAs and change the state of the blockchain across multiple addresses, on a block-by-block level. Transactions may involve complex smart contracts that are effectively infinitely customizable. We will look at what these programs and applications are in Chapter 3.

2.7.4 Atomic

Transactions in DeFi are atomic: either the entire transaction executes, or none at all. If any individual step of the contract fails, the entire contract is reverted and does not execute. Gas is still charged by miners up to the point of failure. This allows for novel applications such as Flash Loans: uncollateralized loans which can be borrowed and paid back in one block.

2.7.5 Gas

In order to allocate the scarce resource of compute and memory on the blockchain, a fee called gas is charged for transactions. Without charging a fee for transactions, certain smart contract programs may run indefinitely, and users may spam the network.

The transaction fee in Ethereum currently (EIP-1559) is as follows: Gas limit * (Base fee + Tip).

The gas limit is the maximum amount of gas the user is willing to pay for the transaction. The base fee is set by the Ethereum network according to network usage. The tip is an optional fee that can be included to incentivize miners to include your transaction in the current block. An additional limit "Max fee per gas" can also be specified. If (Base fee + Tip) is more than "Max fee per gas," the transaction does not execute.

2.7.6 Mempool / MEV

The mempool (memory pool) is a waiting area for transactions that have not been included in a block and are unconfirmed. Nodes run a series of checks to determine if the transaction is valid, if the signature is valid, if funds are available, and other checks.

Due to the public visibility of the mempool, a phenomenon known as MEV (Maximal Extractable Value) has many consequences on execution of transactions and market dynamics. Just like HFT (High frequency trading) firms in TradFi, professional crypto trading teams scan and exploit short-term trading opportunities due to the mempool. Here are some examples.

Generalized frontrunning is possible with bots that scan the mempool for profitable transactions. The bot will copy and submit the transaction with a higher gas fee, frontrunning the transaction. Backrunning the transaction is also possible: when the victim's transaction moves the price on the local exchange, the trader can execute another arbitrage transaction to close the gap with the broader market.

The BIS has raised the various issues involved with MEV,[11] citing that MEV might form an "invisible tax" on regular market participants, and resemble front-running and insider trading activities that would be considered illegal in traditional financial markets.

2.8 Smart Contracts

The term *smart contracts* were originally coined by the computer scientist Nicholas Szabo in the 1990s. He writes:

> A smart contract is a computerized transaction protocol that executes the terms of a contract. The general objectives of smart contract design are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries. Related economic goals include lowering fraud loss, arbitration and enforcement costs, and other transaction costs.[12]
>
> —*Nick Szabo, Smart Contracts*

A canonical real-life example, which we might consider to be the primitive ancestor of smart contracts, is the humble vending machine. Within and functionality. Most wallets are *remote clients* that allow for creation, signing, and broadcasting of transactions without a large storage requirement.

Nodes make up the participants in the P2P network. They store the history of the blockchain, communicate with other nodes, and verify transactions. There are three types of nodes:

Full nodes participate in block validation and verify transactions. They store the most recent 128 blocks (Ethereum). Full nodes can be expensive and resource intensive to run because of the validation function.

Light nodes do not store a full copy of the blockchain and do not validate blocks, but are able to verify transactions. They store relevant information such as the block header, timestamps, and hash of the previous block. These are useful in mobile-devices such as smartphones.

Archive nodes maintain the complete copy of the blockchain data. This may take up a significant amount of storage – at the time of writing the Ethereum blockchain is 871GB. Archive nodes may not participate in validation and are used when a complete record of the chain is required, for example, by block explorers.

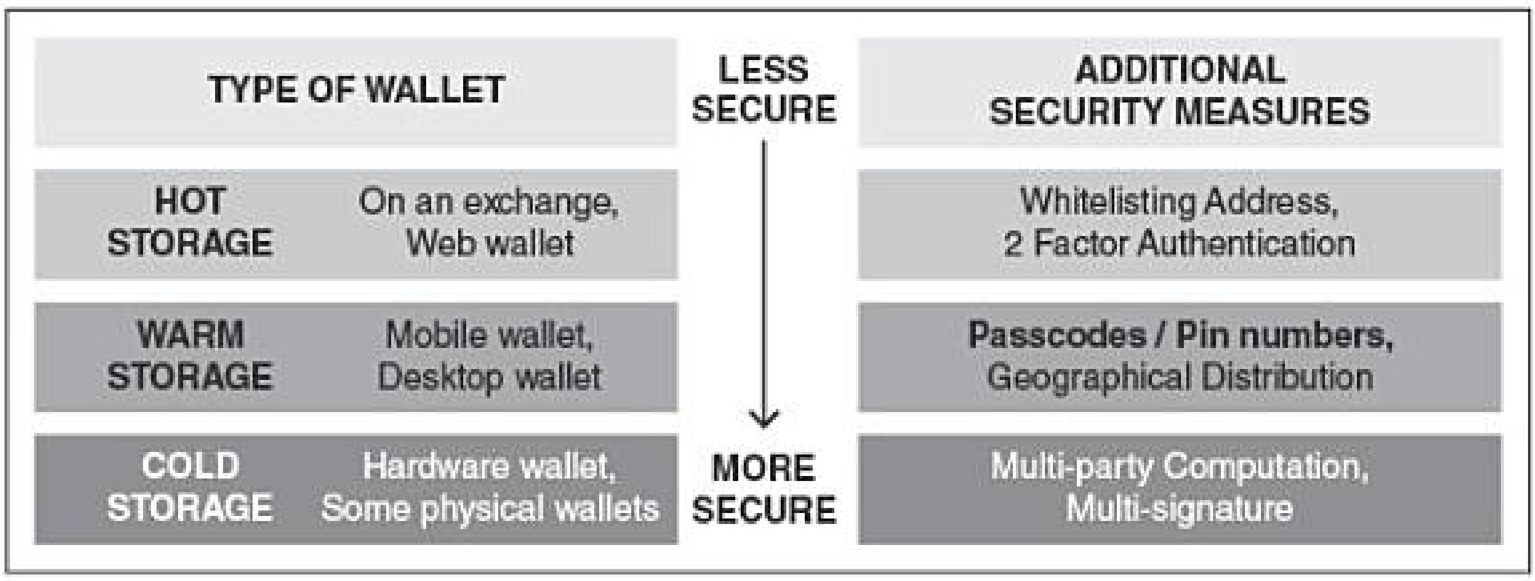
2.10 Block Explorers

Block explorers are online tools that allow users to search, query, and look at the history of the blockchain in a human-friendly way. They display information on addresses, transactions, and tokens. Etherscan is the most popular Ethereum block explorer.

2.11 Custody

There are many ways to hold crypto-assets. They differ in security, connectivity to the internet and convenience (Figure 2.7).

Hot wallets are always connected to the internet. The key issue here is where the private key is stored. Hot wallets may be more convenient but they are also less safe. If a hacker manages to install malware or a keylogger on your local machine, or somehow access your seed phrase that was stored in plaintext anywhere other than your password manager, your crypto-assets are at risk. There exists an entire plethora of cyberattack vectors including phishing, scam software, and misinformation. Be vigilant and be careful! Always update your system software and do not click on dubious links. An example of a hot wallet is MetaMask, a browser extension and mobile app for Ethereum. Mobile wallets are also in this category.



TYPE OF WALLET		LESS SECURE	ADDITIONAL SECURITY MEASURES
HOT STORAGE	On an exchange, Web wallet	↓	Whitelisting Address, 2 Factor Authentication
WARM STORAGE	Mobile wallet, Desktop wallet	↓	**Passcodes / Pin numbers,** Geographical Distribution
COLD STORAGE	Hardware wallet, Some physical wallets	MORE SECURE	Multi-party Computation, Multi-signature

Figure 2.7 Custody types.
Source: Blockdata: Crypto Custody[14]

Multi-signature smart contract wallets offer customizable ownership settings and are compatible with both hot and cold storage solutions. Safe, previously known as Gnosis Safe, enables users to specify the number of required signatures for both ownership of a particular smart contract wallet and transaction approval. For instance, a wallet could be controlled by three separate keys, requiring at least two signatures for any outgoing ETH transfer. Frequently employed by DAOs seeking a trustless asset storage solution, multi-signature wallets are also suitable for individual users aiming to mitigate single-point-of-failure risks and thereby reduce the likelihood of hacks or losses. As of 31 August 2023, Safe holds more than US$50 billion in assets.

Exchange custody offers another option for users, essentially delegating asset custody to the trading platform. The benefits of this approach include seamless asset conversion to and from fiat currency (provided the exchange supports fiat-to-crypto transactions), the flexibility to trade at will, and potentially easier transfers across multiple blockchains. However, the key downside is the risk of asset loss due to exchange insolvency or failure to honor withdrawals, as exemplified by the Mt. Gox debacle.

While centralized exchanges have attracted many retail and institutional traders in the crypto realm, they deviate from the principles of decentralization and self-custody intrinsic to blockchain technology, thereby introducing often-overlooked risks. Centralized platforms exercise ultimate control over user funds, becoming potential single points of failure susceptible to hacks or scams.

The risks are even greater with unregulated exchanges. Such platforms frequently lack transparency regarding their security measures and have been known to misuse and co-mingle customer funds to earn yield, often without proper disclosure, as evidenced by Celsius and FTX. Legal battles involving these exchanges have also resulted in the unwelcome public release of sensitive data.

Institutional custody has become a key component for institutional adoption of crypto-assets. There are many players including Fireblocks, Coinbase

Custody, BitGo, Copper, Ledger, Anchorage, and many others. They may offer full custody solutions (with a license and technology) or just the technology. Institutional custodians may also offer other services such as staking, prime brokerage, settlement, lending, and accounting services.

2.12 Oracles

Oracles are data feeds that bridge the blockchain environment (on-chain) with the real world (off-chain). These feeds may inform pricing information in DeFi and be referenced in smart contracts. Examples of oracles include Chainlink (Ethereum) and Pyth (Solana).

2.13 RegTech

As DeFi becomes more mainstream and regulated, crypto RegTech solutions are increasingly becoming an integral part of DeFi infrastructure. Companies such as Chainalysis, Elliptic, CipherTrace (Mastercard), and TRM Labs offer a suite of services including compliance, risk management, investigation, fraud prevention, transaction monitoring, and on-chain analytics. They may help in satisfying AML (Anti-Money Laundering) and CFT (Combating the Financing of Terrorism) requirements for regulated crypto entities. The sophistication of law enforcement in understanding and investigating on-chain processes and transactions has also increased significantly, with the aid of these RegTech tools. This has been demonstrated by the largest financial seizure ever by the US Department of Justice of US$3.6b from the 2016 Bitfinex hack .

2.14 Identity

Decentralized identity, also known as self-sovereign identity, looks to enable individuals and organizations to manage their digital identities and credentials without reliance on governments and big tech companies such as Google or Facebook. In particular for DeFi, decentralized identity could be a major part in bridging loans between DeFi and the real world.

2.15 Bridges

Just like real-world bridges, blockchain bridges connect two different networks, enabling cross-chain transfer of assets and information. Wrapped tokens are bridged tokens. As multi-chain becomes more common, bridges become more important. Bridges can come in centralized and decentralized forms. Nonetheless, some have highlighted security issues with bridges[15] and this has been witnessed with the US$320m Wormhole hack in 2022. Examples of bridges include: WBTC, Wormhole, Celer, and Anyswap.

2.16 DeFi Instruments

In this section, we'll look at the various instruments that are used in DeFi. Crypto tokens are open-ended and can be designed to represent nearly anything: real-world assets like gold, fiat currencies, software access rights, or identity tokens. At last count, CoinMarketCap lists 20,691 different crypto-assets, with a market capitalization of US$1 trillion. In 2018, the Swiss Financial Market Supervisory Authority (FINMA) defined three types of tokens:

Payment tokens used for payments,
Utility tokens used for access to blockchain-based applications or services,
Security tokens which are representations of assets, such as debt or equity claim on the issuer.

Hybrid tokens with characteristics of two or more categories also could exist. This categorization is a representation of the legal and regulatory dimension of crypto-assets, which hinges around payment and securities laws.

I prefer the term "crypto-assets" to refer to the superset of tokens, as the more commonly used "cryptocurrency" suggests a purely monetary function. For example, Bitcoin is a cryptocurrency but Ether, having utility functions in Ethereum, would be a crypto-asset. The term "utility" is also open-ended, and other functions such as access, governance, staking, and so on would fall under utility, insofar as it pertains to the access and usage of the decentralized application.

We can further categorize crypto-assets into the following categories:

Pure Cryptocurrencies

- In the intent of BTC, to be internet-native, state-independent money
- For example, BTC, DOGE, SHIB, LTC, XMR
- Aim to have the three functions of money: Store of value, medium of exchange, and unit of account (mileage may vary)
- Payment tokens

L1 / L2 tokens

- Tokens issued in conjunction with L1 or L2, and can represent a variety of functions on L1 or L2, including
  - Gas fees on the platform
  - Governance
  - Staking

- For example, ETH, SOL, DOT, MATIC, AVAX, ATOM
- These tokens can be native-money for the L1 ecosystem, and are often utilized for payments for ICOs / token launches on the platform and other DeFi activities
- Utility tokens

DApp tokens

- Tokens issued by decentralized applications, which typically have utility and governance aspects, that allow for token holders to propose and vote on issues pertaining to the application / platform
- For example, UNI, LINK, AAVE, MKR
- Typically issued using the fungible standard specification of the native L1, for example, ERC-20

Liquidity Provider (LP) tokens

- These are specific tokens issued by DeFi protocols as holding receipts for providing, locking-up, or staking liquidity in liquidity pools
- For example, cETH (Compound), stETH (Lido)
- Typically issued using the fungible standard specification of the native L1, for example, ERC-20

Exchange tokens

- Tokens issued by exchanges, designed to incentivize trading activity
- For example, BNB, FTT, CRO
- May grant fee discounts for trading or free transactions with a certain number of exchange token staked
- Tokens may be bought-back and burned by the exchange to increase the value of the token

Stablecoins

- Stablecoins look to solve the volatility problem of cryptocurrencies. They seek to represent units of fiat currency, but on the blockchain
- For example, USDT, USDC, BUSD, DAI
- Stablecoins may be fiat-collateralized, crypto-collateralized, commodity-collateralized, or algorithmic
- Stablecoins are a key aspect of DeFi: more on stablecoins in a later section

Token standards are commonly used in DeFi for a few reasons. Standards uniformly define functions such as transfers or checking total token supply, token balances, and approvals. They allow for interoperability between applications and security best-practices. Unlike Ether, which is handled at the protocol level, tokens are handled at the smart contract level. Token standards are smart contract templates.

Fungible tokens

- The most common and well-known standard: ERC-20
- Frequently used for dApp tokens.

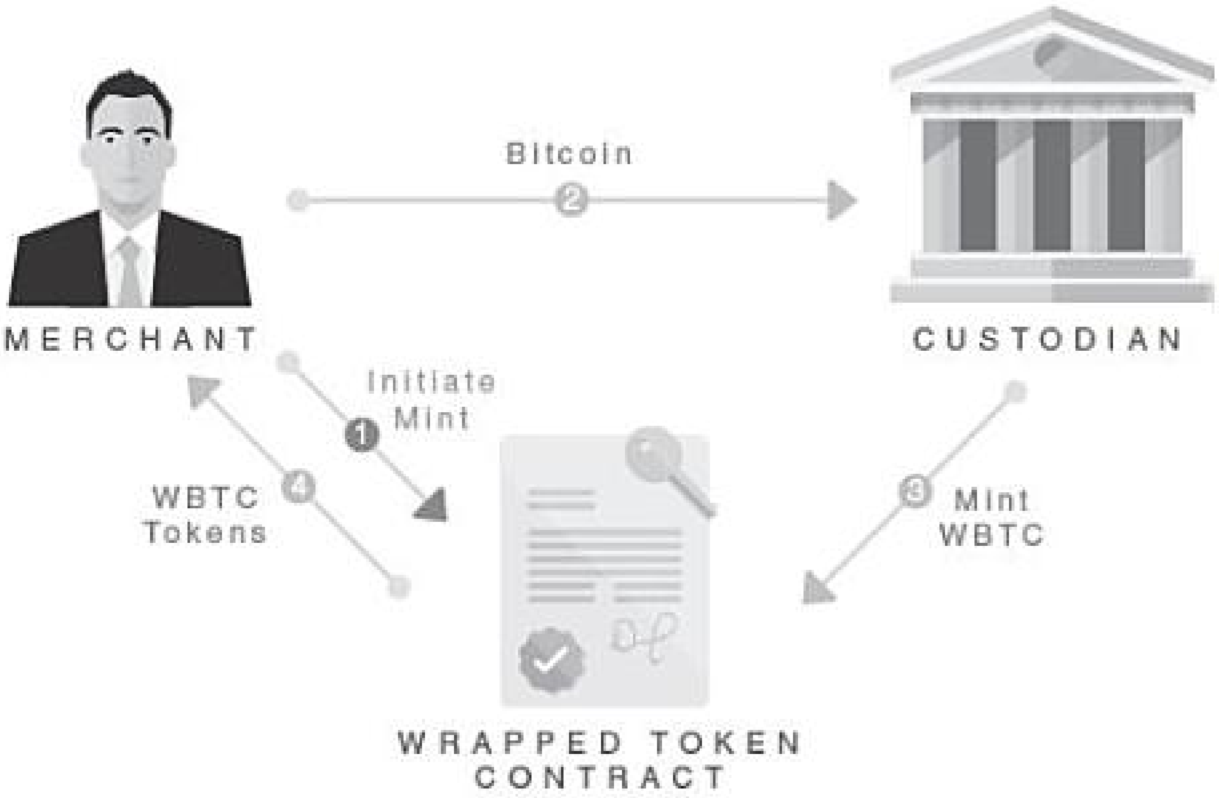


Figure 2.8 WBTC minting process.
Source: wbtc.network

may encounter different frictions with adoption of crypto-asset and blockchain infrastructure, and on-off fiat ramps.

Stablecoins have had incredible growth in the last three years, and have mirrored the growth of DeFi as a whole. Total stablecoin supply grew from US$5b to US$142b (Aug. 2019–Aug. 2022; Figure 2.9).[16] The vast majority of stablecoin issuance is in USD, with USD representing 99.4% of all stablecoin issuance. EUR represents 0.54% and GBP represents 0.03% of total stablecoin issuance.

The popularity of stablecoins is due to a few factors:

1. Stablecoins combine the best of both worlds – the stability of fiat and the cross-border, global nature of crypto.
2. If one does not want to hold crypto, it is much easier to store value in stablecoins than the alternative of converting into fiat, owing to frictions of cost and time between fiat–crypto on-off ramps.
3. Utilization of stablecoins in trading pairs in crypto–crypto exchanges (exchanges without fiat on-off ramps).
4. Stablecoin transfers are faster, simpler, and cheaper than bank transfers.
5. Opportunities for higher yields in DeFi than TradFi.

Stablecoins thus represent a major and growing crossover point between DeFi, FinTech, and TradFi. As with my suggestion on trying out USDC transfers on Solana or Polygon, it is entirely possible to transact in stablecoins without having significant crypto exposure (other than to pay for gas fees). One alternative way of thinking about DeFi could well be using stablecoins as value-transmission, on blockchain infrastructure. Other speculative crypto-assets may not even factor into this use-case, outside of L1 / L2 tokens supporting the infrastructure.

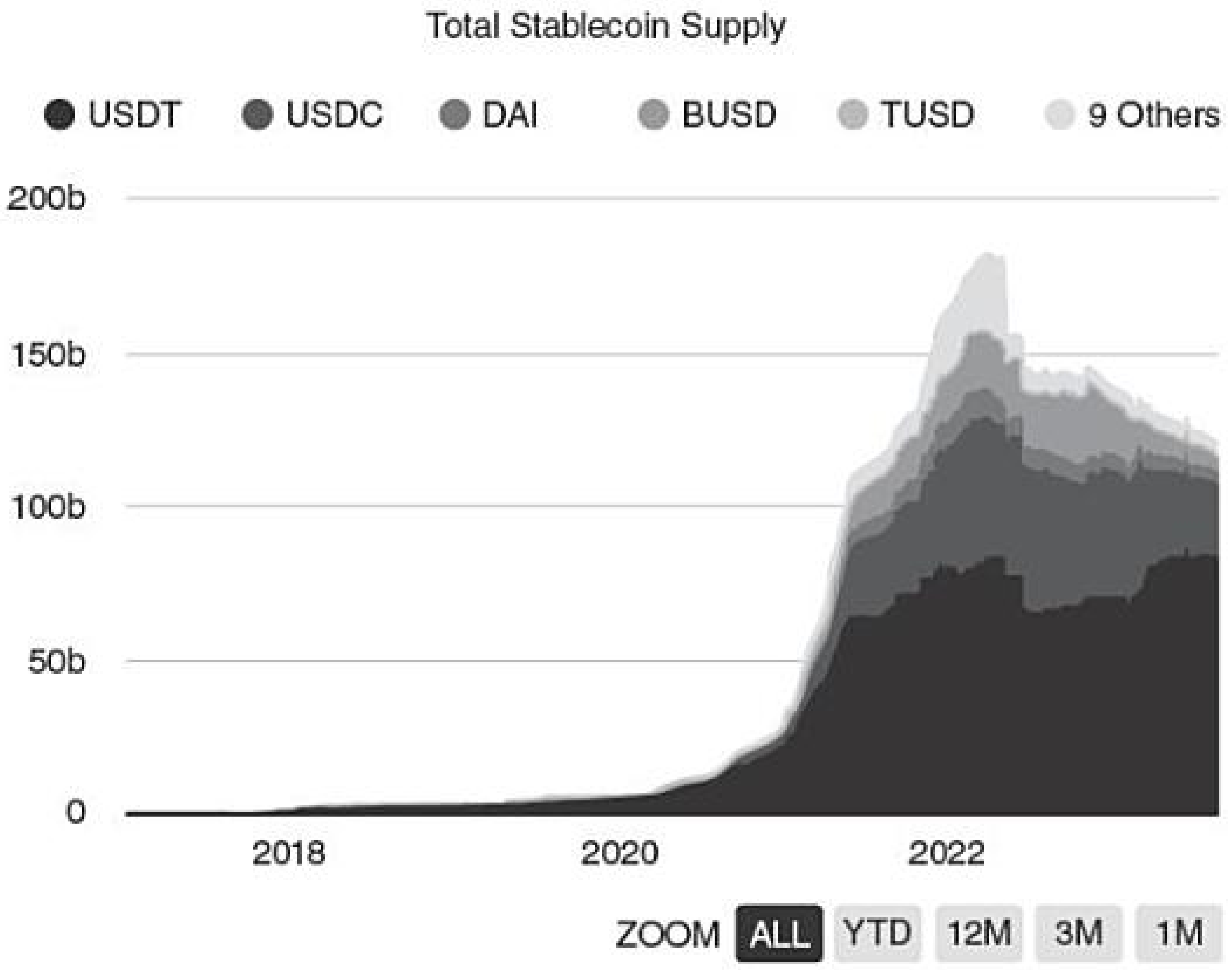


Figure 2.9 Total stablecoin supply.
Source: The Block, Coin Metrics

Many FinTech firms such as Stripe are actively looking into utilizing stablecoins for payments,[17] due to their global, internet-native nature.

> Making commerce more global is one of the most powerful ways we're going after our mission to increase the GDP of the internet. Because crypto protocols are global by default, they're a natural vector for doing this. With crypto payouts, platforms using Stripe can send money to verified recipients nearly anywhere in the world, instantaneously.
>
> —*Will Gaybrick, Chief Product Officer, Stripe*

Regulators and central banks worldwide have also begun to monitor developments in stablecoins closely, given their multiple implications on monetary policy, financial stability, consumer protection, and AML / CFT. In November 2021, the (US) President's Working Group, comprising of the Federal Deposit Insurance Corporation and the Office of the Comptroller of the Currency, released a report on stablecoins that recommended that Congress "act promptly to enact legislation to ensure that payment stablecoins and payment stablecoin arrangements are subject to a federal prudential framework on a consistent and comprehensive basis."[18]

Central banks are also looking at stablecoins for another reason: they serve as a pilot test for CBDCs and a possible adjunct to CBDCs. In particular, since central banks are not in the business of having direct relationships with consumers and businesses (this is left to commercial banks), stablecoins may provide clues as to how the private sector would handle the technology and distribution of CBDCs. More about CBDCs in Chapter 6.

While stablecoins may look and function similarly on the surface, they differ in many ways in terms of their collateralization and stabilization mechanisms under the hood. Let's examine the four different types:

1. Fiat-collateralized
2. Crypto-collateralized
3. Commodity-collateralized
4. Algorithmic

Fiat-collateralized stablecoins are issued by centralized entities who hold an equal amount of cash and short-term debt instruments equivalent to the total float of stablecoins (Figure 2.10). Typically, these entities publish audited reports of their reserves on their websites (Figure 2.11).

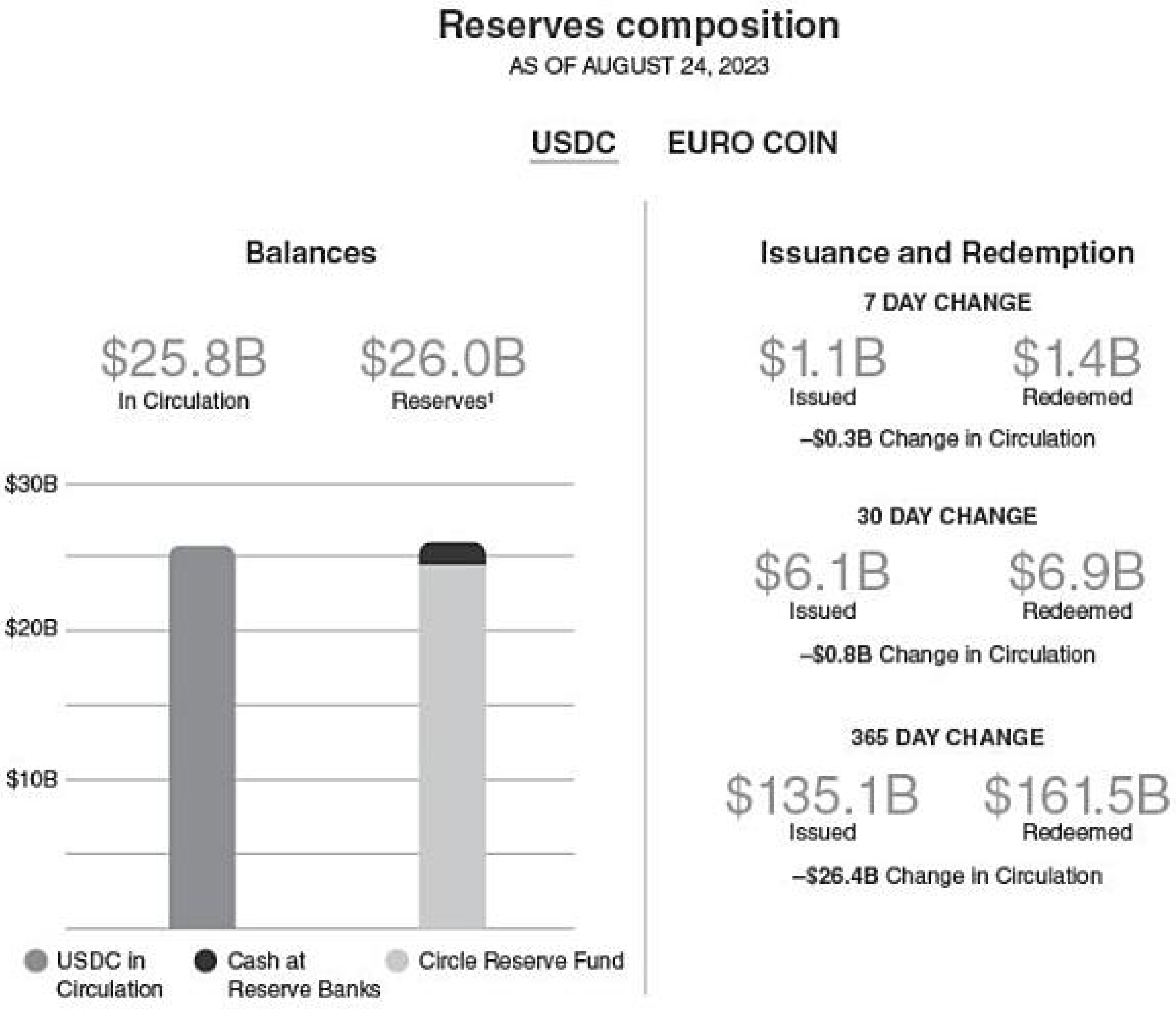


Figure 2.10 USDC reserves.
Source: Circle.com

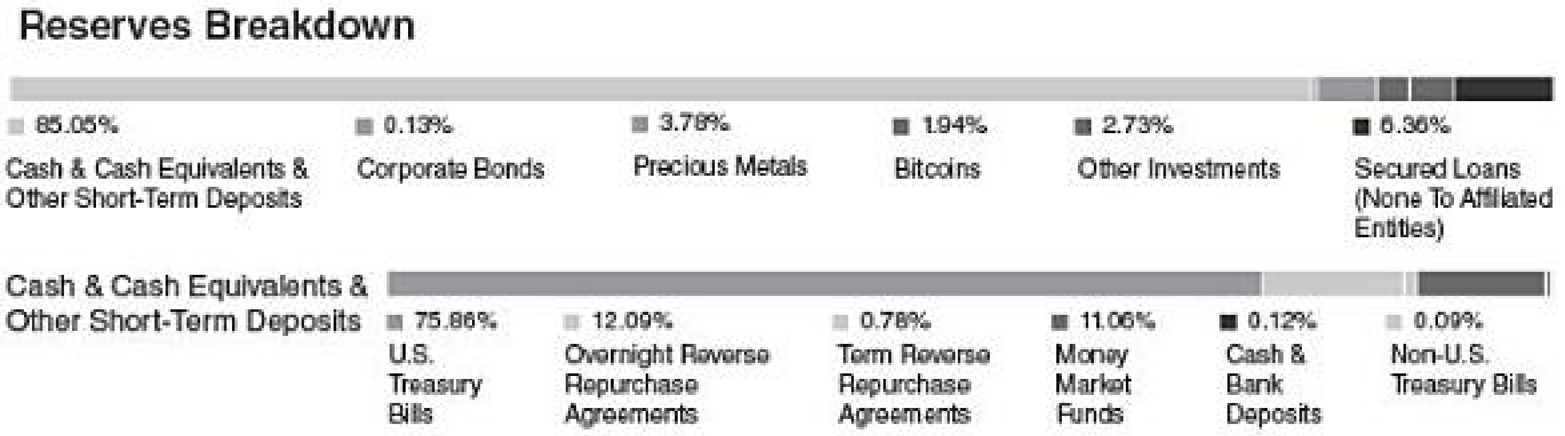


Figure 2.11 USDT reserves.
Source: Tether.com

Since they do not pay depositors (i.e., parties who deposit fiat with the issuers to create the stablecoins) interest, the interest earned on short-term debt instruments is their profit (minus other expenses).

Other examples include: USDC, USDT, BUSD, GUSD, TUSD, PAX

Crypto-collateralized stablecoins are backed by other crypto-assets. Since the collateral base is constantly fluctuating, overcollateralization is the norm here. DAI, issued by MakerDAO, has the highest market cap among the various crypto-collateralized stablecoins of ~US$7b, and accepts various crypto-assets such as USDC and ETH as collateral. As of time of writing, the collateral ratio for DAI is 139.27%.[19]

Additional examples of crypto-collateralized stablecoins include Liquity and Gravita. Liquity is a protocol that solely accepts ETH as collateral, while Gravita is a collateral-debt-position (CDP) based protocol that accepts a range of collateral types, including liquid staking tokens such as stETH (Lido staked ETH) and rETH (Rocket Pool ETH).

Commodity-collateralized stablecoins are collateralized by commodities, typically gold.

PAXG (Paxos Gold) and XAUT (Tether Gold) are the two most popular ones in this category. The issuers may also make it possible to redeem for physical gold.

Algorithmic stablecoins represent the deep (and arguably, dark) end of crypto experimentation. Uncollateralized stablecoins rely on methods such as *seigniorage* and *rebasing*.

Seigniorage models consist of at least two tokens, the most infamous case being UST / LUNA, which had a spectacular collapse in May 2022. The stabilization mechanism utilized LUNA as the collateral for UST. If UST traded above US$1, arbitrageurs could sell UST in the market and buy UST from Terra using LUNA. (Terra guaranteed 1 UST = US$1 of LUNA.) If UST traded below US$1, arbitrageurs could buy UST in the market and sell UST to Terra using LUNA. This mechanism worked, until market conditions and various circumstances created negative feedback loops (aka the death spiral). UST also combined the seigniorage model with Anchor, a "savings" protocol promising 19.5%/yr, enabling UST to reach a peak of US$18b.

In *rebasing* models, the supply of the stablecoin is adjusted algorithmically according to the peg. If the stablecoin price trades over the peg, supply is increased. If the stablecoin price trades under the peg, supply is decreased. This will apply to all holders of the token. An example of a rebasing algo stablecoin is Ampleforth.

Fractional-reserve algo stablecoins maintain a less than 1:1 ratio of collateral, and may combine seigniorage mechanisms. An example is FRAX.

Examples: UST (collapsed), FRAX, ESD (collapsed), DSD (collapsed), Basis Cash (collapsed), AMPL

As with all crypto-asset activities, please take caution and be cognizant of the risks. Many people have lost a lot of money with algorithmic stablecoins.

Since stablecoins (and possibly CBDCs) look to be a key part of DeFi, we'll discuss this further in Chapter 9.

2.18 Derivatives

"Derivatives" refers to financial instruments whose value is derived from another financial instrument (the underlying instrument). Derivatives may also reference indices or other kinds of financial data such as interest rates. The derivatives market in TradFi is enormous: the BIS estimates the gross market value of all derivatives contracts at US$12.4 trillion (end 2021).[20] Common derivatives include futures, forwards, options, and swaps. Derivatives can be said to trade over-the-counter (OTC, off-exchange) or on an exchange.

Just as with TradFi, numerous derivative products in DeFi have evolved over the last few years. They are used for the same purposes in TradFi: hedging risk, gaining leverage, gaining financial exposure, and speculation. Cash settlement often entails less friction than physical settlement of the underlying instrument. Many DeFi derivatives are not tokenized and exist as contracts between the buyer and seller.

A common type of futures contract in DeFi are *perpetual futures contracts*. They do not expire and are cash-settled. Payments are settled periodically between the buyer and seller of the contract and are a factor of the funding rate and the change in the price of future. They were pioneered by BitMEX in 2016, but were first proposed by the economist Robert Schiller in 1992. Perpetual futures are common on centralized exchanges and are also available on decentralized exchanges such as dYdX, Mango Markets, and Drift.

Options are also starting to be more common in DeFi. The largest crypto options exchange currently is Deribit (a centralized exchange), with the majority of volume being ETH and BTC options. Decentralized options exchanges

Bibliography and Online Resources

Here are some books and online resources to continue your learning:

Crypto and DeFi

Antonopoulos, A. and Wood, G. (2018) *Mastering Ethereum. Building Smart Contracts and DApps*. The Ethereum Book LLC.

Arslanian, H. (2018) *The Book of Crypto. The Complete Guide to Understanding Bitcoin, Cryptocurrencies and Digital Assets*. Springer.

Buterin, V. (2022) *Proof of Stake: The Making of Ethereum and the Philosophy of Blockchains*. Seven Stories Press.

Dalio, R (2021) *Principles for Dealing with the Changing World Order: Why Nations Succeed and Fail*. Avid Reader Press.

Harvey, C. R., Ramachandran, A., and Santoro, J. (2021) *DeFi and the Future of Finance*. John Wiley & Sons.

Lewis, A. (2018) *The Basics of Bitcoins and Blockchains*. Mango Publishing.

McDonald, O. (2021) *Cryptocurrencies: Money, Trust and Regulation*. Agenda Publishing.

Narayanan, A., Bonneau, J., Felten, E., Miller, A., and Goldfeder, S. (2016) *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton University Press.

Russo, C. (2020) *The Infinite Machine: How an Army of Crypto-hackers is Building the Next Internet with Ethereum*. Harper Business.

Werbach, K. (2018) *The Blockchain and the New Architecture of Trust*. MIT Press.

Decentralizing Finance: How DeFi, Digital Assets, and Distributed Ledger Technology Are Transforming Finance, First Edition. Kenneth Bok.

CBDCs

Prasad, E. S. (2021) *The Future of Money: How the Digital Revolution is transforming Currencies and Finance*. Belknap Press.
Turrin, R. (2021) *Cashless: China's Digital Currency Revolution*. Authority Publishing.

Payments and FinTech

Laboure, M. and Deffrennes, N. (2022) *Democratizing Finance: The Radical Promise of Fintech*. Harvard University Press.
Leibbrandt, G., and De Terán, N. (2021) *The Pay Off: How Changing the Way We Pay Changes Everything*. Elliott and Thompson Ltd.
Rogoff, K. S. (2016) *The Curse of Cash: How Large-denomination Bills Aid Crime and Tax Evasion and Constrain Monetary Policy*. Princeton University Press

Monetary History

Ferguson, N. (2008) *The Ascent of Money: A Financial History of the World*. Penguin.
Graeber, D. (2011) *Debt: The First 5,000 Years*. Melville House Publishing.
Hayek, F. A. (1976) *The Denationalisation of Money: An Analysis of the Theory and Practice of Concurrent Currencies*. The Institute of Economic Affairs.

Online Resources

Bankless: https://www.bankless.com/
CoinDesk: https://www.coindesk.com/
John Kiff's newsletter: https://kiffmeister.com/
The Block: https://www.theblock.co/
Vitalik Buterin's blog: https://vitalik.ca/

Index

Decentralizing Finance: How DeFi, Digital Assets, and Distributed Ledger Technology Are Transforming Finance, First Edition. Kenneth Bok.
© 2024 John Wiley & Sons Ltd. Published 2024 by John Wiley & Sons Ltd.