IN THIS CHAPTER

- Defining decentralized finance
- Comparing CeFi and DeFi processes
- Considering the cons of a DeFi world
- Exploring promising DeFi implementations

Chapter 1

Introducing Decentralized Finance

The modern *decentralized finance* (DeFi) era truly began with Bitcoin, the first widespread implementation of a decentralized method of recordkeeping that is permissionless yet reliable and secure. Bitcoin effectively provides a currency that doesn't rely on the stability of a central authority.

The implications of such a technology are huge for developing economies where faith in central government is low and bank runs are a serious risk, if not a reality. Moreover, much of the world's population is, at most, one generation removed from being forcibly chased from their homes. Just 70 years ago, Seoul, the capital of Korea, was captured and recaptured four times, and families were permanently separated in a war that ultimately resulted in two separate nations. The fall of Saigon 50 years ago resulted in a mass exodus of Vietnamese refugees

seeking asylum; and more recently, the fall of Kabul (2021) and the Russian invasion of Ukraine earlier this year (2022) led to more waves of emigrants who found themselves in sudden exile.

But aside from more dire circumstances — like the collapse of a banking system or the fall of your government — it's natural to question what true value Bitcoin's underlying technology adds in a stable and wealthy nation. After all, I trust that Bank of America won't maliciously siphon funds from my account, and despite the infamous Wells Fargo fake account scandal (for which it was ultimately fined $3 billion), I would even entrust my money to a Wells Fargo checking account. Nonetheless, reliable economies still have submarkets that are inherently rife with distrust of the central operator, with dark pools (securities exchanges in which participants can trade anonymously and with less transparency) being a case in point. (Try Googling "dark pool lawsuit"!) This trust issue naturally goes away if there is no central operator to distrust, and with the advent of Bitcoin, a proven technology now exists to implement modern DeFi processes across many use cases in finance.

This book isn't about touting the next big cryptocurrency or NFT. It's about the promise of the underlying technology, and where and how that technology can be elegantly applied in ways that truly add value to the situation at hand.

Demystifying DeFi

The idea of decentralized processes is certainly not new. After all, before *centralized finance* (CeFi) arose to establish trusted intermediaries, primitive DeFi was the status quo. Transactions were all peer-to-peer, and you were constrained by your local neighborhood to gain access to capital and to obtain goods by bartering one item for another. Recordkeeping was minimal, and ownership was determined by physical possession.

In modern markets, transactions require confidence in the validity of the agreement, which is provided by reliable and secure recordkeeping systems. After all, when you sell your car,

you are really transferring the legal right to access the car. Without a reliable recordkeeping system in place, chaos would ensue. (Imagine the return of Finders Keepers as a rule of law!)

What's truly exciting now is the distributed-ledger technology that provides a reliable and secure method of recordkeeping that is not maintained by a trusted intermediary, such as Bank of America or the DMV. Behold the dawn of the modern DeFi era!

From autonomous collectives to trillion-dollar DAOs

Well-functioning, leaderless communities are all around us, and in each circumstance, an inherent governance mechanism incentivizes and gels the group to act in concert — all without an elected official to assign roles and lead the process. From homework teams to neighborhoods to informal potlucks, small groups can effectively and efficiently self-govern when there are grades to maintain, property prices to protect, or reputational concerns at stake.

These small-scale examples probably feel reasonable and natural. But what if I told you that a trillion-dollar organization could autonomously validate, execute, secure, and provide ongoing updates to an entire system without an elected leader to assign tasks? The concept sounds naïve at best, and possibly crazy.

And yet, Bitcoin has provided a battle-tested case in point for the underlying technology that enables it to function in a decentralized and autonomous fashion. Yes, Bitcoin is indeed a trillion-dollar *decentralized autonomous organization* (DAO)! Of course, at this scale and with the value at stake, a DAO can't rely solely on simple mechanisms like reputational concerns to incentivize participants to behave honestly and in a way that upholds the values of the system. Instead, the underlying protocol must be foolproofed against malicious players who may work hard to cheat the system. I explain these protocols in greater depth in Chapter 9, "DeFi Building Blocks."

Transacting in DeFi versus CeFi

By this point in the chapter, DeFi may still seem rather abstract. Comparing examples of DeFi versus CeFi processes for certain types of transactions can help to demystify the distinction.

Borrowing assets

Suppose you want to borrow money. How would this transaction be implemented in primitive DeFi versus modern CeFi versus modern DeFi?

- **Under a primitive DeFi process:** You hit up everyone you know within reasonable geographic proximity — a neighbor, a friend, a family member — and hope that someone will lend you something that you can barter with at your local marketplace.
- **Under a modern CeFi process:** People have checking accounts, savings accounts, CDs, and so on with the bank, which means that all these people have lent money to the bank. In turn, the bank lends some of this money to you.
- **Under a modern DeFi process:** People lock up funds in a *smart-contract account*, which is a software program on a public blockchain that automatically enforces and executes the rules in the smart-contract code. This smart-contract account is programmed to function as a lending pool from which you can borrow funds. (See Chapter 7 for details on how decentralized loans work.)

Selling assets

Suppose that instead of borrowing assets, you have assets that you want to sell. Comparing the three types of processes again, here's how this transaction would be implemented:

- **Under a primitive DeFi process:** You again hit up everyone you know within reasonable geographic proximity — a neighbor, friend, family member — and attempt to barter by trial and error.
- **Under a modern CeFi process:** Liquidity providers stand by, waiting to buy the asset from those who want to sell

and to sell the asset to those who want to buy. These liquidity providers commit to buy and sell a certain quantity of assets at varying prices on designated exchanges that serve as official marketplaces for the assets in question. In turn, you place an order to sell the asset through your brokerage firm (who has custody of the asset).

- **Under a modern DeFi process:** Liquidity providers lock up assets and funds in a smart-contract account. This smart-contract account serves as a liquidity pool and is programmed to function as an *automated market maker.* (See Chapter 6 for details on how automated market makers work.) In turn, you can swap your assets for funds from this smart-contract account.

Check out Chapter 4, "Making Your First DeFi Transactions," for a quick, hands-on tutorial if you want to get your hands dirty without learning the technical underpinnings.

Dispelling harmful DeFi myths

REMEMBER

Of course, both the CeFi and DeFi worlds have some bad actors, but DeFi activity is *not* synonymous with illicit activity. The misconception that DeFi applications primarily facilitate or promote criminal activity is untrue and harmful to the DeFi community.

In contrast to cash transactions, which typically aren't recorded, crypto transactions (such as in bitcoins or ether) are memorialized for all time on a public recordkeeping system known as a *blockchain.* In fact, any legitimate entity that touches crypto must employ the services of at least one blockchain analytics firm (such as Chainalysis) to credibly convey that it is serious about adhering to anti-money laundering (AML) provisions.

As the lowest-hanging fruit, blacklisted accounts (such as those associated with ransomware attacks or on the OFAC list) are barred from transacting with legitimate institutions. From there, blockchain analytics firms assign risk scores to graylisted accounts based on suspicious activity that suggests a possible connection to other graylisted or blacklisted accounts. Chapter 9, "DeFi Building Blocks," introduces you to tracing activity on a block explorer, and Chapter 11, "Launching a Smart Contract on Ethereum," delves more deeply into this process.

Just as it's (nearly) impossible to spend $10 million in ill-gotten cash (you can't show up with suitcases of cash to buy a home), it's (nearly) impossible to spend $10 million in ill-gotten crypto.

Going Full Circle: The DeFi-CeFi Infinity Loop

A large part of DeFi activity really entails learning (or relearning) why CeFi arose in the first place and is so critically important. The following sections explain how primitive DeFi processes were made more efficient by CeFi processes, which were then challenged by modern DeFi processes (but which, in turn, demonstrated weaknesses of their own, highlighting again the value of CeFi and perpetuating the DeFi-CeFi infinity loop).

Safeguarding wealth

Suppose you want to save assets and keep them safe. How would this process be improved from primitive DeFi to modern CeFi to modern DeFi (and then back to modern CeFi)?

- **Starting with a primitive DeFi process:** Perhaps you keep your money (or gold or diamonds) under your mattress (or in a hole) and hope that no one finds it (but also that you don't forget where you stored it). Given the danger and other obvious flaws in trying to safeguard your money, trusted institutions arise to take over this function.
- **Transitioning to a modern CeFi process:** You entrust your money to a bank. But then Bitcoin emerges, and perhaps traditional banking seems boring (or maybe you're in a country with a precarious banking system or volatile political climate).
- **Trying out a modern DeFi process:** You keep your private crypto key (a sequence of numbers) in a safe place, or you split your private key and store it across multiple safe places (maybe under your mattress or in a hole, and again, hope that no one finds it but also that you don't forget where you stored it). But then you remember that you're

bad at being your own bank. You may forget where you hid your keys, or someone may steal them, or they may become damaged in a fire. You decide to entrust your crypto wealth to a vault service, and now you're back to modern CeFi!

Transferring funds

Now suppose you want to transfer funds to another party. Comparing the evolution of processes again, here's how this transaction might be attempted and improved across iterations:

- **Starting with a primitive DeFi process:** You physically hand over the money (or gold or diamonds) and hope that no one robs you along the way. Given the danger and other obvious flaws (you can't send money to someone far away), trusted institutions arise to take over this function.
- **Transitioning to a modern CeFi process:** You write a check or request your bank to wire money to another account. But this process can be slow and expensive, especially for international wire transfers.
- **Trying out a modern DeFi process:** You use a noncustodial wallet service, such as MetaMask, to send crypto to another account. But then you realize that you sent the funds to the wrong account! Sadly, there's no one to call and no one who can halt or reverse the process. So then you decide to go back to writing checks or wiring money through your trusted bank.

Continuing the cycle

As the preceding examples show, the need to have a way to track transactions and troubleshoot problems while finding cost savings causes people to go full circle, from DeFi to CeFi and back again. Overall, we really aren't good at being our own banks, and we benefit from well-defined property rights. Intermediaries naturally arose to provide legitimacy, protection, order, and reliable recordkeeping. Sadly, these intermediaries became complacent and charged more than they should, and the particularly accelerated pace of technological development in the

last 10–15 years brought on the *financial technology* (FinTech) movement. With that movement came the aggressive push to *disintermediate* — that is, to cut out the middleman and democratize the system for smaller players.

However, truly decentralized platforms can be clunky and frustrating, with bad UI/UX (user interface/user experience) and little to no customer support, and updates take a long time to coordinate in leaderless organizations (*and* we are bad at being our own banks). So then a defined group or elected leader steps in again to provide a better and more streamlined experience, and the DeFi-CeFi infinity loop goes on . . . .

Deciding to DeFi or Not to DeFi

As you've likely gathered from the previous sections, a large part of the DeFi thought process is learning and relearning the efficiencies and deficiencies of both CeFi and DeFi. In the fervor to embrace DeFi, it's important to remain mindful of CeFi market mechanisms in place and why those mechanisms may be important.

So before you explore the remaining chapters that expound on all the wonderful things you can do with modern DeFi, such as trading on decentralized exchanges (see Chapter 6) or taking on a decentralized loan (see Chapter 7), the following sections offer some important caveats.

Acknowledging inherent deficiencies in DeFi

Decentralized processes have some built-in problems that are difficult to avoid or resolve. They are fraught with inefficiencies and coordination issues, which is why identifiable entities with elected leaders naturally arise. After all, Microsoft would achieve far less if it lacked centralized leadership and all shareholders had to be consulted before any decision can be implemented.

Societal costs to individuals arising from coordination issues are particularly tangible when you consider commercial banks and other types of lending institutions. When you walk into Bank of America to borrow money, an entire back-end process with its investment-banking arm is involved. This back-end process is critical to your ability to get the loan in the first place. The process entails pooling and securitizing the bank's loans so that they can be sold to other financial institutions (such as funds and other asset management firms). If Bank of America can't sell the loans to get them off of its balance sheet, it will issue fewer loans. Without integrating this critical back-end process, decentralized lending volume will remain constrained, as evidenced by the thousands of small community banks that don't issue as many loans or even certain types of loans because they lack coordinated access to sell off the loans.

Overall, complete reliance on decentralized, peer-to-peer lending would have the perverse effect of making capital less accessible to smaller players.

Recognizing CeFi problems that migrate into DeFi

Simply taking CeFi processes and slapping them onto a blockchain can't magically wave away problems from the CeFi world.

For example, improperly structured and insufficiently backed assets are as toxic in the DeFi world as they are in the CeFi world. A recent debacle with the so-called stablecoin, TerraUSD (UST), saw its value plummet from its dollar peg to just a few cents on the dollar, creating a situation reminiscent of the Financial Crisis of 2007–2008, also known as the Great Recession. This crisis etched the terms *mortgage-backed securities* (MBS) and *collateralized debt obligations* (CDOs) into the minds of the general public, who until that point had been blissfully unaware of the shadow banking system and structured products.

Moreover, securities laws must be followed in the DeFi world as well as in the CeFi world, and problems with enforcing ownership rights of physical assets aren't solved by simply storing ownership records on a public blockchain. Overall, DeFi is not the answer to all of CeFi's problems.

Identifying hurdles to adoption

Even for truly amazing and value-adding DeFi applications, the hurdles to adoption remain high for the general population. Most tutorials leave much to be desired because they are either out of date, overly simplified, or far too complicated, and navigating DeFi protocols is far from intuitive. (You can get your first taste in Chapters 3 and 4.) Overall, when it comes to DeFi processes, the user experience is relatively unfriendly compared to that of CeFi processes that have better production teams, user interfaces, and help desks.

For instance, consider the process of obtaining bitcoins from a Bitcoin ATM (BTM), as shown in Figure 1-1. This transaction should be one of the easiest and friendliest entry points into the DeFi ecosystem. However, the process still confuses many users, who are ill equipped to know what to do with the paper wallet that materializes after the BTM has swallowed their cash.

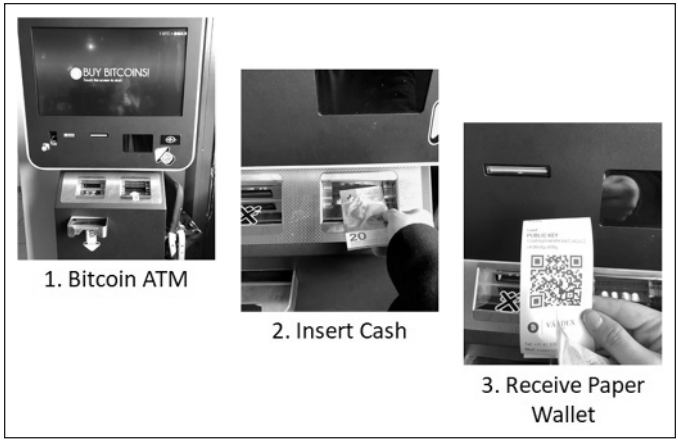

FIGURE 1-1: Bitcoin ATM (BTM) in Zurich.

DeFi also still suffers from the *crypto horn* effect, which refers to the negative impressions of crypto that spill over into anything even tangentially related to crypto (the opposite of a *halo* effect). With extreme price swings generating instant millionaires and overnight paupers, crypto hasn't been placed in the most favorable light. Because no way to meaningfully talk about true, modern DeFi exists without embedding crypto into the conversation, the DeFi movement sadly suffers from the ensuing misunderstandings and even disdain that plagues crypto.

Contemplating the Future of DeFi

The most exciting prospects for DeFi relate to projects that provide a practical pathway toward solving issues of distrust in modern financial markets. This umbrella extends to projects that provide access to financial services and concessions (such as delayed settlements, covered in Chapter 7) that, so far, have been available only to large institutions.

For example, to solve issues of distrust, perhaps a decentralized exchange will soon materialize as a registered *alternative trading system* (ATS) on which to trade tokenized securities. Imagine a decentralized dark pool free from concerns that a central operator may be illegally soliciting and placing orders ahead of a large trade that was placed first! Automated market makers are currently far from being able to handle the magnitude of volume required by institutional trades, but current implementations (explained in Chapter 6) provide a promising starting point.

Another promising development in DeFi is the ongoing empowerment of smaller (non-institutional) players. One of my favorite DeFi applications is Aave's flash loan protocol (detailed in Chapter 7), which democratizes delayed settlements and reduces up-front capital requirements for small retail traders. Perhaps the next phase in decentralized trading could entail decentralized clearing corporations!

The potential amazingness of seemingly unimportant applications

Practical considerations aside for a moment, implementing a DeFi process for its own sake can provide interesting puzzles and thought experiments, and I'm hugely in favor of creating DeFi implementations just for DeFi's sake. After all, *RSA encryption* technology, which for decades provided an effective method for secure data transmission, was born from a subfield within *number theory,* which is a branch of *pure mathematics* — a discipline focused purely on mathematics for its artistic merits and without consideration for external applications. Sometimes creative problem solving simply for the sake of creative problem solving yields the most practical applications of all!

In a similar vein, it's exciting to watch how DeFi processes are being implemented and improved in decentralized *metaverses* (discussed further in Chapter 8). Gamified analogues can highlight real-world use cases and pave the way for real-world implementations, as evidenced by how the addictive aspects of video games have shaped motivational processes in the real world. The prevalence of dashboards and gamified progress reports across professional and educational settings shows that life does indeed take lessons from art. Likewise, if million-dollar plots of virtual land in decentralized metaverses can be secured as ERC-721 non-fungible tokens (NFTs) on the Ethereum blockchain, perhaps developing nations with less reliable recordkeeping systems can follow suit.

Less than one-third of the world's population enjoys secure property rights — a problem identified by the World Bank as fundamental to reducing poverty and fostering growth. Imagine, for example, if such governments were to commit to well-defined and well-protected property rights. Transparent and reliable records of ownerships and transfers could be implemented as NFTs on a well-established public blockchain, and automated lending protocols could allow borrowers to access funds by posting their NFT-ized land titles as collateral. Such an endeavor could help to forge the path toward creating digital records of substantial non-fungible assets in economies fraught with poor recordkeeping systems.

The ERC-721 NFT standard began with CryptoKitties, an overwhelmingly successful digital collectible (like a digital, blockchain-based analogue of Beanie Babies) that was launched on the Ethereum blockchain in 2017. Perhaps the world needs more adorable cats and creepy apes (such as the famous Mutant Ape Yacht Club NFTs) to be unnecessarily slapped onto a public blockchain to demonstrate the feasibility of greater concepts.

Can we completely replace CeFi?

Once upon a time, the world ran on primitive DeFi, so it's certainly possible to replace CeFi with decentralized processes, complemented by modern technology where possible. However, the real question to ask is *should* we? This chapter covers some serious drawbacks to DeFi. Some of these drawbacks are largely

cosmetic issues that can be overcome, but others point to unavoidable problems inherent in decentralized processes.

As it stands, there's still much value to be extracted from the DeFi movement — and I see a world with CeFi and DeFi processes humming along at some point in (possibly symbiotic) coexistence.

Proceeding on Your DeFi Journey

I hope this book is an enjoyable and insightful journey into a modified way of thinking (and possibly a new way of life!).

Along the way, I hope to spark ideas, dispel harmful misconceptions, and encourage creative development. I wish you a fulfilling and productive experience as you go on to select your next chapter. Cheers!