The book is now published at:

https://www.amazon.com/DeFi-Future-Finance-Campbell-Harvey/dp/1119836018/ref=sr_1_3

The following is an older, unedited version of the manuscript

DeFi and the Future of Finance*

Campbell R. Harvey
Duke University, Durham, NC USA 27708
National Bureau of Economic Research, Cambridge MA USA 02138

Ashwin Ramachandran
Dragonfly Capital

Joey Santoro
Fei Protocol

ABSTRACT

Our legacy financial infrastructure has both limited growth opportunities and contributed to the inequality of opportunities. Around the world, 1.7 billion are unbanked. Small businesses, even those with a banking relationship, often must rely on high-cost financing, such as credit cards, because traditional banking excludes them from loan financing. High costs also impact retailers who lose 3% on every credit card sales transaction. These total costs for small businesses are enormous by any metric. The result is less investment and decreased economic growth. Decentralized finance, or DeFi, poses a challenge to the current system and offers a number of potential solutions to the problems inherent in the traditional financial infrastructure. While there are many fintech initiatives, we argue that the ones that embrace the current banking infrastructure are likely to be fleeting. We argue those initiatives that use decentralized methods - in particular blockchain technology - have the best chance to define the future of finance.

Comments: *Please comment directly on the live version of our paper. It is available here.*

Keywords: *Decentralized finance, DeFi; Fintech, Flash loans, Flash swaps, Automatic Market Maker, DEX, Decentralized Exchange, Cryptocurrency, Uniswap, MakerDAO, Compound, Ethereum, Aave, Yield protocol, ERC-20, Initial DeFi Offering, dYdX, Synthetix, Keeper, Set protocol, Yield farming*.

JEL: *A10, B10, D40, E44, F30, F60, G10, G21, G23, G51, I10, K10, L14, M10,O16, O33, O40, P10, C63, C70, D83, D85*

*Current version: April 5,2021. We appreciate the comments of Dan Robinson, Stani Kulechov, John Mattox, Andreas Park, Chen Feng, Can Gurel, Jeffrey Hoopes, Brian Bernert, Marc Toledo, Marcel Smeets, Ron Nicol, Daniel Liebau Giancarlo Bertocco, Josh Chen, Lawrence Diao, Deepanshu, Louis Gagnon, Herve Tourpe, Vishal Kumar, Jullian Villella, Yash Patil, Manmit Singh, on an earlier draft. Lucy Pless created the graphics and Kay Jaitly provided editorial assistance.

Table of Contents

1. Introduction

We have come full circle. The earliest form of market exchange was peer to peer, also known as barter. Barter was highly inefficient because supply and demand had to be exactly matched between peers. To solve the matching problem, money was introduced as a medium of exchange and store of value. Initial types of money were not centralized. Agents accepted any number of items such as stones or shells in exchange for goods. Eventually, specie money emerged, a form in which the currency had tangible value. Today, we have non-collateralized (fiat) currency controlled by central banks. Whereas the form of money has changed over time, the basic infrastructure of financial institutions has not changed.

However, the scaffolding is emerging for a historic disruption of our current financial infrastructure. DeFi or decentralized finance seeks to build and combine open-source financial building blocks into sophisticated products with minimized friction and maximized value to users using blockchain technology. Given it costs no more to provide services to a customer with $100 or $100 million in assets, we believe that DeFi will replace all meaningful centralized financial infrastructure in the future. This is a technology of inclusion whereby anyone can pay the flat fee to use and benefit from the innovations of DeFi.

DeFi is fundamentally a competitive marketplace of decentralized financial applications that function as various financial "primitives" such as exchange, save, lend, and tokenize. These applications benefit from the network effects of combining and recombining DeFi products and attracting increasingly more market share from the traditional financial ecosystem.

Our book details the problems that DeFi solves: **centralized control, limited access, inefficiency, lack of interoperability, and opacity**. We then describe the current and rapidly growing DeFi landscape, and present a vision of the future opportunities that DeFi unlocks. Let's begin with the problems:

- *Five Key Problems of Centralized Financial Systems*

For centuries, we have lived in a world of centralized finance. Central banks control the money supply. Financial trading is largely done via intermediaries. Borrowing and lending is conducted through traditional banking institutions. In the last few years, however, considerable progress has been made on a much different model - decentralized finance or DeFi. In this framework, peers interact with peers via a common ledger that is not controlled by any centralized organization. DeFi offers considerable potential for solving the five key problems associated with centralized finance:

Centralized control. Centralization has many layers. Most consumers and businesses deal with a single, localized bank. The bank controls rates and fees. Switching is possible, but it can

be costly. Further, the US banking system is highly concentrated. The four largest banks have a 44% share of insured deposits compared to 15% in 1984.[1] Interestingly, the US banking system is less concentrated than other countries, such as the United Kingdom and Canada. In a centralized banking system, a single centralized entity attempts to set short-term interest rates and to influence the rate of inflation. The centralization phenomenon does not just pertain to the legacy financial sector. Relatively new tech players dominate certain industries, for example, Amazon (retail) and Facebook/Google (digital advertising).

Limited access. Today, 1.7 billion people are unbanked making it very challenging for them to obtain loans and to operate in the world of internet commerce. Further, many consumers must resort to pay-day lending operations to cover liquidity shortfalls. Being banked, however, does not guarantee access. For example, a bank may not want to bother with the small loan that a new business requires and the bank may suggest a credit card loan. The credit card could have a borrowing rate well above 20% per year, a high hurdle rate for finding profitable investment projects. In developing countries, like India, this rate is closer to 40%.

Inefficiency. A centralized financial system has many inefficiencies. Perhaps the most egregious example is the credit card interchange rate that causes consumers and small businesses to lose up to 3% of a transaction's value with every swipe due to the payment network oligopoly's pricing power. Remittance fees are 5-7%. Another example is the two days it takes to "settle" a stock transaction (officially transfer ownership). In the internet age, this seems utterly implausible. Other inefficiencies include: costly (and slow) transfer of funds, direct and indirect brokerage fees, lack of security, and the inability to conduct microtransactions. Many of these inefficiencies are not obvious to users. In the current banking system, deposit interest rates remain very low and loan rates high because banks need to cover their bricks-and-mortar costs. A similar issue arises in the insurance industry.

Lack of interoperability. Consumers and businesses deal with financial institutions in an environment that locks interconnectivity. Our financial system is siloed and designed to sustain high switching costs. Moving money from one institution to another can be unduly lengthy and complicated. A wire transfer can take three days to complete. This problem is well-known and some attempts are being made to mitigate it. A recent example is Visa's attempted acquisition of Plaid in 2019. Plaid allows any company to plug into an institution's information stack with the user's permission. This is an example of a corporation operating in the world of centralized finance trying to acquire a product to mitigate a particular problem but not addressing the fundamental problems with the current financial infrastructure. It was a strategic move to buy time.

Opacity. The current financial system is not transparent. Bank customers have very little information on the financial health of their bank and must place their faith in the limited

[1] See Corbae, Dean and Pablo D'Erasmo, 2020, Rising Bank Concentration, Staff Paper #594, Federal Reserve Bank of Minneapolis, March. https://doi.org/10.21034/sr.594

government protection of FDIC insurance on their deposits. Bank customers seeking a loan find it difficult to determine if the offered rate is competitive. The market for loans is very fragmented, although the consumer insurance industry has made some progress with fintech services that offer to find the "lowest" price. The current list of competing lenders, however, all suffer from the system's inefficiencies. The result is that the "lowest" still reflects legacy bricks-and-mortar costs as well as bloated back-office costs.

The implications of these five problems are twofold. First, many of these costs lead to *lower economic growth*. For example, if loan rates are high because of legacy costs, high-quality investment projects may be foregone, as explained previously. An entrepreneur's high-quality idea may target a 20% rate of return precisely the type of project that accelerates economic growth. If the bank tells the entrepreneur to borrow money on her credit card at 24% per year, this profitable project may never be pursued.

Second, these problems perpetuate and/or exacerbate *inequality*. Most (across the political spectrum) agree there should be equality of opportunity: a project should be financed based on the quality of the idea and the soundness of the execution plan, and not by other factors. Importantly, inequality also limits growth when good ideas are not financed. While purported to be the "land of opportunity", the United States has one of the worst records in migrating income from the bottom quartile to the top quartile.[2] Inequality of opportunity arises, in part, from lack of access to the current banking system, reliance on costly alternative financing such as payday lending and the inability to buy or sell in the modern world of e-commerce.

These implications are far-reaching and, by any calculus, this is a long list of serious problems that are endemic to our current system of centralized finance. While we are in the digital era, our financial infrastructure has failed to fully adapt. Decentralized finance offers new opportunities. The technology is nascent but the upside is promising.

Our book has multiple goals. First, we identify the weaknesses in the current system, including discussion of some early initiatives that challenged the business models of centralized finance. Next, we explore the origins of decentralized finance. We then discuss a critical component of DeFi: blockchain technology. Next, we explore what solutions DeFi offers and couple this with a deep dive on some leading ideas in this emerging space. We then explore the major risk factors. We conclude by looking to the future and attempt to identify the winners and losers.

[2] See Chetty, R., N. Hendren, P. Kline, and E. Saez (2014), "Where is the land of opportunity? The geography of intergenerational mobility in the United States", *Quarterly Journal of Economics* 129:4, 1553-1623, and Narayan, A., R. Van der Weide, A. Cojocaru, C. Lakner, S. Redaelli, D. Mahler, R. Ramasubbaiah, and S. Thewissen (2018), *Fair Progress?: Economic Mobility Across Generations Around the World, Equity and Development*, Washington DC: World Bank.

2. The Origins of Modern Decentralized Finance

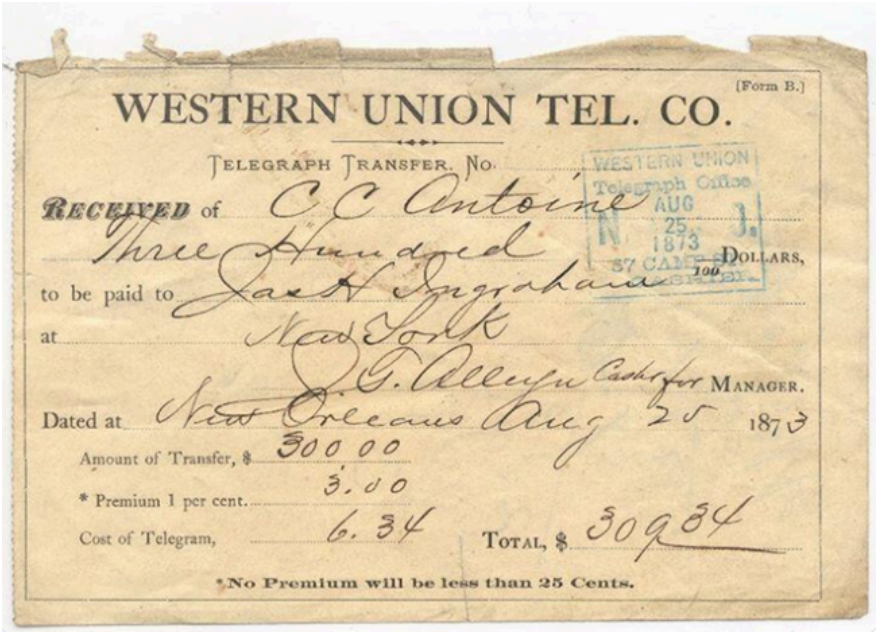
2.1 A brief history of finance

While we argue that today's financial system is plagued with inefficiencies, it is a lot better than systems of the past. As mentioned in the previous chapter, initial market exchanges were peer to peer. A barter system required the exact matching of two parties' needs. Likely at the same time and as response to the inefficiency in the barter system, an informal credit system emerged in villages whereby people kept a mental record of "gifts".[3]

Coinage came much later with the first modern coins in Lydia around 600 BCE. These coins provided the now traditional functions of money: unit of account, medium of exchange and store of value. Important characteristics of money included: durability, portability, divisibility, uniformity, limited supply, acceptability and stability. Bank notes, originating in China, made their way to Europe in the 13th century.

Non-physical transfer of money originated in 1871 with Western Union. Exhibit 1 shows a copy of an early transfer, for $300. Notice the fees amount to $9.34 or roughly 3%. It is remarkable that so little has changed in 150 years. Money transfers are routinely more expensive and credit card fees are 3%.

Exhibit 1: Western Union transfer from 1873



[Form B.]

WESTERN UNION TEL. CO.

TELEGRAPH TRANSFER. No.

WESTERN UNION Telegraph Office AUG 25 1873

RECEIVED of C C Antoine

Three Hundred 100 DOLLARS,

to be paid to Jas A Ingraham

at New York

J. G. Allyn Cashier for MANAGER.

Dated at New Orleans Aug 25 1873

Amount of Transfer, $ 300 00

* Premium 1 per cent. 3.00

Cost of Telegram, 6.34

TOTAL, $ 309 34

*No Premium will be less than 25 Cents.

[3] See https://www.creditslips.org/creditslips/2020/06/david-graebers-debt-the-first-5000-years.html

The pace of innovation increased in the last century: Credit cards (1950) with Diners Card, ATM (1967) by Barclays Bank, telephone banking (1983) from Bank of Scotland, and Internet banking (1994) by Stanford Federal Credit Union. Further innovation, RFID payments (1997) with Mobil Speedpass, chip and pin credit cards (2005), and Apple Pay (2014).

Importantly, all of these innovations were built on the backbone of centralized finance. Indeed, the current system of banking has not changed much in the past 150 years. While digitization was an important innovation, it was an innovation that supported a legacy structure. The high costs associated with the legacy system spurred further innovations that we now refer to as Fintech.

2.2 Fintech

When costs are high, innovation will arise to capitalize on inefficiencies. However, innovation may be slowed by a powerful layer of middle people. An early example of decentralized finance emerged in the foreign currency (forex) market 20 years ago. At the time, large corporations used their investment banks to manage their forex needs. For example, a U.S.-based corporation might need €50 million at the end of September to make a payment on some goods purchased in Germany. Their bank would quote a rate for the transaction. At the same time, another client of the bank might need to sell €50 million at the end of September. The bank would quote a different rate. The difference in the rate is known as the spread and the spread is the profit that the bank makes for being the intermediary. Given the multi-trillion dollar forex market, this was an important part of bank profits.

In early 2001, a fintech startup offered the following idea.[4] Instead of individual corporations querying various banks to get the best rate, why not have an electronic system match the buyers and sellers directly at an agreed-upon price and *no* spread. Indeed, the bank could offer this service to its own customers and collect a modest fee (compared to the spread). Furthermore, given that some customers deal with multiple banks, it would be possible to connect customers at all banks participating in the peer-to-peer network.

You can imagine the reception. The bank might say: “are you telling me we should invest in an electronic system that will cannibalize our business and largely eliminate a very important profit center?” However, even 20-years ago, banks realized that their largest customers were very unhappy with the current system: as globalization surged these customers faced unnecessary forex transactions costs.

An even earlier example was the rise of dark pool stock trading. In 1979, the US Securities and Exchange Commission instituted Rule 19c3 that allowed stocks listed on one exchange, such as

[4] See: https://faculty.fuqua.duke.edu/~charvey/Media/2001/EuromoneyOct01.pdf

the NYSE, to be traded off-exchange. Many large institutions moved their trading, in particular, large blocks, to these dark pools where they traded peer-to-peer with far lower costs than traditional exchange-based trading.

The excessive costs of transacting brought in many fintech innovations. For example, an earlier innovator in the payments space was PayPal, which was founded over 20 years ago.[5] Even banks have added their own payment systems. For example, in 2017, seven of the largest U.S. banks launched Zelle.[6] An important commonality of these cost-reducing fintech advances is that these innovations rely on the centralized backbone of the current financial infrastructure.

2.3 Bitcoin and Cryptocurrency

The dozens of digital currency initiatives beginning in the early 1980s all failed.[7] The landscape shifted, however, with the publication of the famous Satoshi Nakamoto Bitcoin white paper in 2008. The paper presents a peer-to-peer system that is decentralized and utilizes the concept of blockchain. While blockchain was invented in 1991 by Haber and Stornetta, it was primarily envisioned to be a time-stamping system to keep track of different versions of a document. The key innovation of Bitcoin was to combine the idea of blockchain (time stamping) with a consensus mechanism called *Proof of Work* (introduced by Back in 2002). The technology produced an immutable ledger that eliminated a key problem with any digital asset - you can make perfect copies and spend them multiple times. Blockchains allow for the key features desirable in a store of value, but which never before were simultaneously present in a single asset. Blockchains allow for cryptographic scarcity (Bitcoin has a fixed supply cap of 21 million), censorship resistance and user sovereignty (no entity other than the user can determine how to use funds), and portability (can send any quantity anywhere for a low flat fee). These features combined in a single technology make cryptocurrency a powerful innovation.

The value proposition of Bitcoin is important to understand, and can be put into perspective by assessing the value proposition of other financial assets. Consider the US dollar, for example. It used to be backed by gold before the gold standard was removed in 1971. Now, the demand for USD comes from: 1) Taxes; 2) Purchase of US goods denominated in USD; and 3) Repayment of debt denominated by USD. None of these three cases create intrinsic value but rather value based on the network that is the US economy. Expansion or contraction in these components of the US economy can impact the price of the USD. Additionally, shocks to the supply of USD adjust its price at a given level of demand. The Fed can adjust the supply of USD through monetary policy to achieve financial or political goals. Inflation eats away at the value of USD, decreasing its ability to store value over time. One might be concerned with runaway inflation,

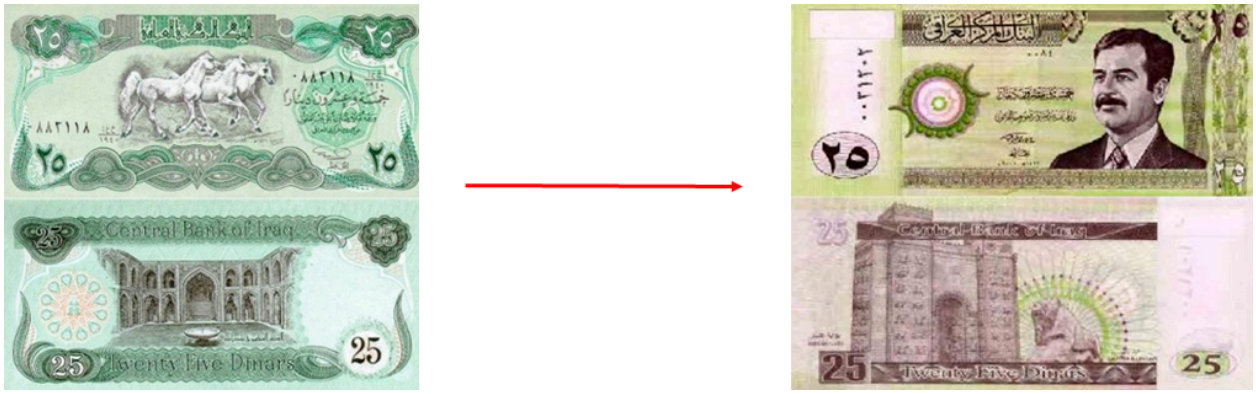
[5] PayPal founded as Confinity in 1998 did not begin offering a payments function until it merged with X.com in 2000.
[6] Other examples include: Cash App, Braintree, Venmo, and Robinhood.
[7] See Harvey, C. R., The history of digital money (2020), https://faculty.fuqua.duke.edu/~charvey/Teaching/697_2020/Public_Presentations_697/History_of_Digital_Money_2020_697.pdf

what Paul Tudor Jones calls, "The Great Monetary Inflation", which would lead to a flight to inflation resistant assets.[8] Gold has proven to be a successful inflation hedge due to its practically limited supply, concrete utility, and general global trustworthiness. However, given that gold is a volatile asset, its historical hedging ability is only realized at extremely long horizons.[9]

Many argue that bitcoin has no "tangible" value and therefore it should be worthless. Continuing the gold analogy, approximately two thirds of gold is used for jewelry and some is used in technology hardware. Gold has tangible value. The US dollar, while a fiat currency, has value as "legal tender". However, there are many examples from history whereby currency emerged without any backing that had value.

A relatively recent example is the Iraqi Swiss dinar. This was the currency of Iraq until the first Gulf War in 1990. The printing plates were manufactured in Switzerland (hence the name) and the printing was outsourced to the U.K. In 1991, Iraq was divided with the Kurds controlling the north and Saddam Hussien in the south. Due to sanctions, Iraq could not import dinars and had to start local production. In May 1993, the Central Bank of Iraq announced that citizens had three weeks to exchange old 25 dinars for new ones (Exhibit 2).

Exhibit 2: Iraqi Swiss dinars and new dinars



The old Swiss dinar continued to be used in the north. In the south, the new dinar suffered from extreme inflation. Eventually, the exchange rate was 300 new dinars for a single Iraqi Swiss dinar. The key insight here is that the Iraqi Swiss dinar had no official backing - but it was accepted as money. There was no tangible value yet it had fundamental value. Importantly, value can be derived from both tangible and intangible value.

The features of Bitcoin that we have mentioned, particularly scarcity and self-sovereignty, make it a potential store of value and possible hedge to political and economic unrest at the hands of

[8] https://www.lopp.net/pdf/BVI-Macro-Outlook.pdf
[9] C. Erb and Harvey, C. R., (2013) The Golden Dilemma, *Financial Analysts Journal,* 69:4, pp. 10-42, show that gold is an unreliable inflation hedge over short and medium term horizons.

global governments. As the network grows, the value proposition only increases due to increased trust and liquidity. Although Bitcoin was originally intended as a peer-to-peer currency, its deflationary characteristics and flat fees discourage its use in small transactions. We argue that Bitcoin is the flagship of a new asset class, namely cryptocurrencies, which can have varied use cases based on the construction of their networks. Bitcoin itself, we believe will continue to grow as an important store of value and a potential inflation hedge - over long horizons.[10]

The original cryptocurrencies offered an alternative to a financial system that had been dominated by governments and centralized institutions such as central banks. They arose largely from a desire to replace inefficient, siloed financial systems with immutable, borderless, open-source algorithms. The currencies can adjust their parameters such as inflation and mechanism for consensus via their underlying blockchain to create different value propositions. We will discuss blockchain and cryptocurrency in greater depth in section 3 and, for now, we will focus on a particular cryptocurrency with special relevance to DeFi.

2.4 Ethereum and DeFi

Ethereum (ETH) is currently the second largest cryptocurrency by market cap ($230b). Vitalik Buterin introduced the idea in 2014 and Ethereum mined its first block in 2015. Ethereum is in some sense a logical extension of the applications of Bitcoin. It allows for *smart contracts* - which are code that lives on a blockchain, can control assets and data, and define interactions between the assets, data, and network participants. The capacity for smart contracts defines Ethereum as a *smart contract platform*.

Ethereum and other smart contract platforms specifically gave rise to the *decentralized application* or *dApp*. The backend components of these applications are built with interoperable, transparent smart contracts that continue to exist as long as the chain they live on exists. dApps allow peers to interact directly and remove the need for a company to act as a central clearing house for app interactions. It quickly became apparent that the first killer dApps would be financial ones.

The drive toward financial dApps became a movement in its own right known as *decentralized finance* or *DeFi*. DeFi seeks to build and combine open-source financial building blocks into sophisticated products with minimized friction and maximized value to users. Because it costs no more at an organization level to provide services to a customer with $100 or $100 million in assets, DeFi proponents believe that all meaningful financial infrastructure will be replaced by smart contracts which can provide more value to a larger group of users. Anyone can simply pay the flat fee to use the contract and benefit from the innovations of DeFi. We will discuss smart contract platforms and dApps in more depth in chapter 3.

[10] Similar to gold, bitcoin is likely too volatile to be a reliable inflation hedge over short horizons. While theoretically decoupled from any country's money supply or economy, in the brief history of bitcoin, we have not experienced any inflation surge. So there is no empirical evidence of its efficacy.

DeFi is fundamentally a competitive marketplace of financial dApps that function as various financial "primitives" such as exchange, lend, tokenize, and so forth. These dApps benefit from the network effects of combining and recombining DeFi products and attracting increasingly more market share from the traditional financial ecosystem. Our goal is to give an overview of the problems that DeFi solves, describe the current and rapidly growing DeFi landscape, and present a vision of the future opportunities that DeFi unlocks.

3. DeFi Infrastructure

In this chapter, we discuss the innovations that led to DeFi and lay out the terminology.

3.1 Blockchain

The key to all DeFi is the decentralizing backbone, a blockchain. Blockchains are fundamentally software protocols that allow multiple parties to operate under shared assumptions and data without trusting each other. These data can be anything, such as location and destination information of items in a supply chain or account balances of a token. Updates are packaged into "blocks" and are "chained" together cryptographically to allow an audit of the prior history, hence the name.

The reason blockchains are possible is a *Consensus Protocol*, a set of rules that determine what kinds of blocks can become part of the chain and become the "truth". These consensus protocols are designed to be resistant to malicious tampering up to a certain security bound. The blockchains we focus on use the *Proof of Work (PoW)* consensus protocol, which relies on a computationally-intensive lottery to determine which block to add. The participants agree that the *longest chain* of blocks is the truth. If an attacker wants to make a longer chain that contains malicious transactions, they have to outpace all of the computational *work* of the entire rest of the network. In theory, they would need a majority of the network power to accomplish this, hence the famous *51% attack* being the boundary of PoW security. Luckily, it is extraordinarily difficult for any actor, even an entire country, to amass this much network power on the most widely-used blockchains such as Bitcoin or Ethereum. Even if a majority of the network power ("hashrate"), can be temporarily acquired, the extent of block history that can be overwritten is constrained by how long this majority can be maintained.

While we focus on Proof of Work, there are many alternative consensus mechanisms with the most important being *Proof of Stake (PoS)*. In Proof of Stake, validators commit some capital (the stake) to attest that the block is valid. Validators make themselves available by staking their cryptocurrency and then they may be selected to propose a block. The proposed block needs to

be attested by a majority of the other validators. Validators profit by both proposing a block as well as attesting to the validity of others' proposed blocks.

As long as no malicious party can acquire majority control of the network computational power, then transactions will be processed by the good-faith actors and appended to the ledger when a block is "won".

3.2 Cryptocurrency

The most popular application of blockchain technology is cryptocurrency. Cryptocurrency is a token (usually scarce) that is cryptographically secured and transferred. The scarcity is what assures the possibility of value, and is itself an innovation of blockchain. Typically digital objects are easily copied. As Eric Schmidt, the former CEO of Google has said,[11] "[Bitcoin] is a remarkable cryptographic achievement and the ability to create something that is not duplicable in the digital world has enormous value."

No one can post a false transaction without ownership of the corresponding account due to the *asymmetric key cryptography* protecting the accounts. You have one "public" key representing an address to receive tokens, and a "private" key used to unlock and spend tokens you have custody over. This same type of cryptography is used to protect your credit card information and data when using the internet. A single account cannot "double-spend" their tokens because the ledger keeps an audit of their balance at any given time and the faulty transaction would not clear. The ability to prevent "double-spend" without a central authority illustrates the primary advantage of using a blockchain to maintain the underlying ledger.

The initial cryptocurrency model is the Bitcoin blockchain, which functions almost exclusively as a payment network, with the capabilities of storing and transacting bitcoins across the globe in real-time with no intermediaries or censorship. This is the powerful value proposition that gives bitcoin its value. Even though its network effects are strong, technological competitors do offer enhanced functionality.

3.3 The Smart Contract Platform

A crucial ingredient of DeFi is a *smart contract* platform. These blockchains go beyond a simple payments network such as Bitcoin and allow for the creation of smart contracts that enhance the capabilities of the chain itself. Ethereum is the primary example of a smart contract platform. A smart contract is code that can create and transform arbitrary data or tokens on top of the blockchain of which it is a part. The concept is powerful because it allows the user to trustlessly

[11] From a panel discussion at the Computer History Museum in 2014. See: https://www.newsbtc.com/news/google-chairman-eric-schmidt-bitcoin-architecture-amazing-advancement/

encode rules for any type of transaction and even create scarce assets with specialized functionality. Many of the clauses of traditional business agreements could be shifted to a smart contract, which not only would enumerate, but algorithmically enforce those clauses. Smart contracts go beyond finance, and have applications in gaming, data stewardship and supply chain among other purposes.

An interesting caveat applies to Ethereum, but not necessarily to all smart contract platforms, is the existence of a transaction fee known as a *gas fee*. Imagine Ethereum as one giant computer with many applications (smart contracts). If someone wants to use the computer, they must pay a fee for each unit of computation they use. A simple computation, such as sending ETH, requires minimal work updating a few account balances. This has a relatively small gas fee. A complex computation that involves minting tokens and checking various conditions across many contracts costs correspondingly more gas.

A helpful analogy for Ethereum is a car. If someone wants to drive a car, a certain amount of gas is needed and there is a fee to acquire the gas. The gas fee may lead to a poor user experience, however. The gas fee forces agents to maintain an ETH balance in order to pay it and to worry not only about overpaying but also underpaying and having the transaction not take place at all. For this reason, initiatives are ongoing to abstract away gas fees from end users and support competitor chains that completely remove this concept of gas. Gas is important, however, as a primary mechanism for preventing attacks on the system that generate an *infinite loop* of code. It is not feasible to identify malicious code of this kind before running it, a problem formally known in computer science as *the halting problem*. Gas secures the Ethereum blockchain by making such attacks prohibitively expensive. Continuing our analogy, gas solves the halting problem in the following way: Suppose a "car" is on autopilot stuck in full throttle with no driver. Gas acts as a limiting factor, because the car has to stop eventually when the gas tank empties. This incentivizes highly efficient smart contract code, as contracts that utilize fewer resources and reduce the probability of user failures have a much higher chance of being used and succeeding in the market.

On a smart contract platform, the possibilities rapidly expand beyond what developers desiring to integrate various applications can easily handle. This leads to the adoption of standard interfaces for different types of functionality. On Ethereum these standards are called *Ethereum Request for Comments* (*ERC)*. The best known of these define different types of tokens that have similar behavior. ERC-20 is the standard for fungible tokens,[12] it defines an interface for tokens whose units are identical in utility and functionality. It includes behavior such as transferring units and approving operators for using a certain portion of a user's balance. Another is ERC-721, the non-fungible token standard. ERC-721 tokens are unique, and are often used for collectibles or assets such as P2P loans. The benefit of these standards is that application

[12] Fungible tokens have equal value just as every dollar bill has equal value and a $10 dollar bill is equal to two $5 dollar bills. Non-fungible tokens, in contrast, reflect the value of what they are associated with (e.g., one non-fungible token may be associated with a piece of art like a painting). They do not necessarily have equal value.

developers can code for one interface, and support every possible token that implements that interface. We will discuss these interfaces further in Section 4.

3.4 Oracles

An interesting problem with blockchain protocols is that they are isolated from the world outside of their ledger. That is, the Ethereum blockchain only authoritatively knows what is happening on the Ethereum blockchain, and not, for example, the level of the S&P 500 or which team won the Super Bowl. This limitation constrains applications to Ethereum native contracts and tokens thus reducing the utility of the smart contract platform and is generally known as the *oracle problem*. An *oracle*, in the context of smart contract platforms, is any data source for reporting information external to the blockchain. How can we create an oracle that can authoritatively speak about off-chain information in a trust-minimized way? Many applications require an oracle, and the implementations exhibit varying degrees of centralization.

There are several implementations of oracles in various DeFi applications. A common approach is for an application to host its own oracle or hook into an existing oracle from a well-trusted platform. One Ethereum-based platform known as Chainlink is designed to solve the oracle problem by using an aggregation of data sources. The Chainlink whitepaper includes a reputation-based system, which has not yet been implemented. We discuss the oracle problem later in more depth. Oracles are surely an open design question and challenge for DeFi to achieve utility beyond its own isolated chain.

3.5 Stablecoins

A crucial shortcoming to many cryptocurrencies is excessive volatility. This adds friction to users who wish to take advantage of DeFi applications but don't have the risk-tolerance for a volatile asset like ETH. To solve this, an entire class of cryptocurrencies called stablecoins has emerged. Stablecoins are intended to maintain price parity with some target asset, USD or gold for instance. Stablecoins provide the necessary stability that investors seek to participate in many DeFi applications and allow a cryptocurrency native solution to exit positions in more volatile cryptoassets. They can even be used to provide on-chain exposure to the returns of an off-chain asset if the target asset is not native to the underlying blockchain (e.g., gold, stocks, ETFs). The mechanism by which the stablecoin maintains its peg varies by implementation. The three primary mechanisms are fiat-collateralized, crypto-collateralized, and non-collateralized stablecoins.

By far the largest class of stablecoins are fiat-collateralized. These are backed by an off-chain reserve of the target asset. Usually these are custodied by an external entity or group of entities which undergo routine audits to verify the collateral's existence. The largest fiat-collateralized stablecoin is Tether (USDT) with a market capitalization of $24 billion dollars, making it the

third largest cryptocurrency behind Bitcoin and Ethereum at time of writing. Tether also has the highest trading volume of any cryptocurrency but is not audited.[13] The second-largest is USDC, backed by Coinbase and Circle is audited. USDC is redeemable 1:1 for USD and vice-versa for no fee on Coinbase's exchange. USDT and USDC are very popular to integrate into DeFi protocols as demand for stablecoin investment opportunities is high. There is an inherent risk to these tokens however as they are centrally controlled and maintain the right to blacklist accounts.

The second largest class of stablecoins are crypto-collateralized. These are stablecoins which are backed by an overcollateralized amount of another cryptocurrency. Their value can be hard or soft pegged to the underlying asset depending on the mechanism. The most popular crypto-collateralized stablecoin is DAI, created by MakerDAO and it is backed by mostly ETH with collateral support for a few other cryptoassets. It is soft pegged with economic mechanisms that incentivize supply and demand to drive the price to $1. DAI's market capitalization is $1 billion as of writing. We will do a deep dive into MakerDAO and DAI in section 6.1. Another popular crypto-collateralized stablecoin is sUSD. This is part of the Synthetix platform we explore in section 6.6. It is backed by the Synthetix network token (SNX) and is hard-pegged to 1 USD through their exchange functionality. Crypto-collateralized stablecoins have the advantages of decentralization and secured collateral. The drawback is that their scalability is limited. To mint more of the stablecoin, a user must necessarily back the issuance by an overcollateralized debt position. In some cases like DAI there is even a debt ceiling that further limits the supply growth.

The last and perhaps the most interesting class of stablecoins are non-collateralized. These are not backed by any underlying asset, and use algorithmic expansion and contraction of supply to shift the price to the peg. They often employ a seigniorage model where the token holders in the platform receive the increase in supply when demand increases. When demand decreases and the price slips below the peg, these platforms would issue bonds of some form which entitle the holder to future expansionary supply before the token holders receive their share. This mechanism works almost identically to the central bank associated with fiat currencies, with the caveat that these platforms have an explicit goal of pegging the price rather than funding government spending or other economic goals. A noteworthy early example of an algorithmic stablecoin is Basis, which had to close down due to regulatory hurdles. Current examples of algorithmic stablecoins include Ampleforth (AMPL) and Empty Set Dollar (ESD). The drawback to non-collateralized stablecoins is that they have a lack of inherent underlying value backing the exchange of their token. In contractions, this can lead to "bank runs" in which the majority of holders are left with large sums of the token which are no longer worth the peg price.

It is still an open problem to create a decentralized stablecoin which both scales efficiently and is resistant to collapse in contractions. Further, there are regulatory issues which we will discuss

[13] On March 30, 2021, Tether produced an "attestation" (third party verification of holdings) prepared by the Moore Cayman of its holdings as of February 28, 2021.

later.[14] Stablecoins are an important component of DeFi infrastructure as they allow users to benefit from the functionality of the applications without risking unnecessary price volatility.

3.6 Decentralized Applications

As mentioned earlier, dApps are a critical DeFi ingredient. dApps are similar to traditional software applications except they live on a decentralized smart contract platform. The primary benefit of these applications is their *permissionlessness* and *censorship-resistance*. Anyone can use them, and no single body controls them. A separate but related concept is a *decentralized autonomous organization* (*DAO)*. A DAO has its rules of operation encoded in smart contracts that determine who can execute what behavior or upgrade. It is common for a DAO to have some kind of *governance token,* which gives an owner some percentage of the vote on future outcomes. We will explore governance in much more detail later.

4. DeFi Primitives

Now that we have laid the groundwork by detailing the DeFi infrastructure, in this chapter we will describe the primitive financial actions that developers can use. A developer can combine these actions to create complex dApps. We will explain in detail each of the primitive actions and the advantages each may have over its centralized counterparts.

4.1 Transactions

Ethereum transactions are the atoms of DeFi (and Ethereum as a whole). Transactions involve sending data and/or ETH (or other tokens) from one address to another. All Ethereum interactions, including each of the primitives discussed in this section, begin with a transaction. Therefore, good comprehension of the mechanics of transactions is crucial to understanding Ethereum, in particular, and DeFi, in general.

An Ethereum user can control addresses through an *externally owned account* (EOA) or by using smart contract code (*contract account*). When data is sent to a contract account, the data are used to execute code in that contract. The transaction may or may not have an accompanying ETH payment for use by the contract. Transactions sent to an EOA can only transfer ETH.[15]

---

[14] See, e.g., Financial Stability Board, "Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements", October 2020.

[15] Technically, a transaction sent to an EOA can also send data, but the data have no Ethereum-specific functionality.

A single transaction starts with an end-user from an EOA, but can interact with a large number of dApps (or any Ethereum smart contract) before completing. The transaction starts by interacting with a single contract, which will enumerate all of the intermediate steps in the transaction required within the contract body.

Clauses in a smart contract can cause a transaction to fail and thereby revert all previous steps of the transaction; as a result, transactions are *atomic*. Atomicity is a critical feature of transactions because funds can move between many contracts (i.e., "exchange hands") with the knowledge and security that if one of the conditions is not met, the contract terms reset as if the money never left the starting point.

As we mentioned in Section 3, transactions have a gas fee, which varies based on the complexity of the transaction. When, for example, ETH is used to compensate a miner for including and executing a transaction, the gas fee is relatively low. Longer or more data-intensive transactions cost more gas. If a transaction reverts for any reason, or runs out of gas, the sender forfeits all gas used until that point. Forfeiture protects the miners who, without this provision, could fall prey to large volumes of failed transactions for which they would not receive payment.

The gas price is determined by the market and effectively creates an auction for inclusion in the next Ethereum block. Higher gas fees signal higher demand and therefore generally receive higher priority for inclusion.

A technical aside about transactions is that they are posted to a *memory pool*, or *mempool*, before they are added to a block. Miners monitor these posted transactions, add them to their own mempool, and share the transaction with other miners to be included in the next available block. If the gas price offered by the transaction is uncompetitive relative to other transactions in the mempool, the transaction is deferred to a future block.

Any actor can see transactions in the mempool by running or communicating with mining nodes. This visibility can even allow for advanced front-running and other competitive techniques that aid the miner in profiting from trading activity. If a miner sees a transaction in the mempool she could profit from by either executing herself or front-running it, the miner is incentivized to do so if lucky enough to win the block. Any occurrence of direct execution is known as *miner extractable value* (MEV). MEV is a drawback to the proof-of-work model. Certain strategies, such as obfuscating transactions, can mitigate MEV, thus hiding from miners how they might profit from the transactions.

4.2 Fungible Tokens

Fungible tokens are a cornerstone of the value proposition of Ethereum and DeFi. Any Ethereum developer can create a token divisible to a certain decimal granularity and with units that are all identical and interchangeable. By way of example, USD is a fungible asset because

one $100 bill is equivalent to one hundred $1 bills. As we mentioned in Section 3, the Ethereum blockchain token interface is ERC-20. An interface from an application developer's perspective is the minimum required set of functionality. When a token implements the ERC-20 interface, any application that generically handles the defined functionality can instantly and seamlessly integrate with the token. Using ERC-20 and similar interfaces, application developers can confidently support tokens that do not yet exist.

The ERC-20 interface defines the following core functionality:

- totalSupply()—read the token's total supply;
- balanceOf(account)—read the balance of the token for a particular account;
- transfer(recipient address, amount)—send "amount" tokens from the transaction sender to "recipient address";
- transferFrom(sender address, recipient address, amount)—send "amount" tokens from the balance of tokens held at "sender address" to "recipient address";
- approve(spender, amount)—allows "spender" to spend "amount" tokens on behalf of the account owner;
- allowance(owner address, spender address)—returns the amount of tokens the "spender address" can spend on behalf of the "owner address".

The contract will reject transfers involving insufficient balances or unauthorized spending. The first four functions are intuitive and expected (reading supply, balances, and sending tokens). The last two functions, approve and allowance, are critical to understanding the power of the ERC-20 interface. Without this function, users would be limited to directly transferring tokens to and from accounts. With approval functionality, contracts (or trusted accounts) can be whitelisted to act as custodians for a user's tokens without directly holding the token balance. This functionality widens the scope of possible applications because users retain full custody before an approved spender executes a transaction.

We will now define three main categories of ERC-20 tokens. An ERC-20 token can simultaneously be in more than one category.

4.2.1 Equity Token

An equity token, not to be confused with equities or stocks in the traditional finance sense, is simply a token that represents ownership of an underlying asset or pool of assets. The units must be fungible so that each corresponds to an identical share in the pool. For example, suppose a token, TKN, has a total fixed supply of 10,000, and TKN corresponds to an ETH pool of 100 ETH held in a smart contract. The smart contract stipulates that for every unit of TKN it receives, it will return a pro rata amount of ETH, fixing the exchange ratio at 100 TKN/1 ETH.

We can extend the example so the pool has a variable amount of ETH. Suppose the ETH in the pool increases at 5% per year by some other mechanism. Now 100 TKN would represent 1 ETH

plus a 5% perpetuity cash flow of ETH. The market can use this information to accurately price the value of TKN.

In actual equity tokens, the pools of assets can contain much more complex mechanics, going beyond a static pool or fixed rates of increase. The possibilities are limited only by what can be encoded into a smart contract. We will examine a contract with variable interest-rate mechanics in Section 6.1.2, when discussing Compound, and a contract that owns a multi-asset pool with a complex fee structure in Section 6.2.1 when discussing Uniswap. In Section 6.4.1 we explain Set Protocol, which defines a standard interface for creating equity tokens with static or dynamic holdings.

4.2.2 Utility Tokens

Utility tokens are in many ways a catchall bucket, although they do have a clear definition. Utility tokens are fungible tokens that are required to utilize some functionality of a smart contract system or that have an intrinsic value proposition defined by its respective smart contract system. In many cases, utility tokens drive the economics of a system, creating scarcity or incentives where intended by the developers. In some cases, ETH could be used in place of a utility token, but utility tokens allow systems to accrue and maintain decoupled economic value from Ethereum as a whole. A use case that requires a distinct utility token would include a system with algorithmically varied supply. We will discuss the mechanics in more depth in Section 4.5.

The following are examples of use cases for utility tokens:

- To be collateral (e.g., SNX)
- To represent reputation or stake (e.g., REP, LINK)
- To maintain stable value relative to underlying or peg (e.g., DAI, Synthetix Synth)
- To pay application-specific fees (e.g., ZRX, DAI, LINK)

The last example includes all stablecoins, regardless of whether the stablecoin is fiat collateralized, crypto-collateralized, or algorithmic. In the case of USDC, a fiat-collateralized stablecoin, the utility token operates as its own system without any additional smart-contract infrastructure to support its value. The value of USDC arises from the promise of redemption for USD by its backing companies, including Coinbase.

Far more possibilities exist for utility tokens than the few we have mentioned here. Innovation will expand this category as novel economic and technical mechanisms emerge.

4.2.3 Governance Tokens

Governance tokens are similar to equity tokens in the sense they represent percentage ownership. Instead of asset ownership, governance token ownership applies to voting rights, as the name suggests. We start by motivating the types of changes on which owners can vote.

Many smart contracts have embedded clauses stipulating how the system can change; for instance, allowed changes could include adjusting parameters, adding new components, or even altering the functionality of existing components. The ability of the system to change is a powerful proposition given the possibility that the contract a user interacts with today could change tomorrow. In some cases, only developer admins, who encode special privileges for themselves, can control changes to the platform.

Any platform with admin-controlled functionality is not truly DeFi because of the admins' centralized control. A contract without the capacity for change is necessarily rigid, however, and has no way to adapt to bugs in the code or changing economic or technical conditions. For this reason, many platforms strive for a decentralized upgrade process, often mediated by a governance token.

The owners of a governance token would have pro-rata voting rights for implementing any change allowed by the smart contracts that govern the platform. We will discuss the voting mechanisms in Section 5 when we discuss *decentralized autonomous organizations* (DAOs).

A governance token can be implemented in many ways—with a static supply, an inflationary supply, or even a deflationary supply. A static supply is straightforward: purchased shares would correspond directly to a certain percentage control of the vote. The current implementation of the MKR token for MakerDAO has a generally static supply. In Section 6.1 we will take a deep dive on MakerDAO and discuss its implementation in more detail.

Many platforms issue the governance token via an inflation schedule that incentivizes users to utilize particular features of the platform, ensuring the governance token is distributed directly to users. Compound, for example, uses an inflationary implementation approach with its COMP token, which we will discuss in Section 6.2. A deflationary approach would likely consist of using the governance token also as a utility token to pay fees to the platform. These fees would be burned, or removed, from the supply rather than going to a specific entity. The MKR token of MakerDAO used to be burned in this manner in an older version of the platform. We will discuss burning mechanics further in Section 4.5.

4.3 Nonfungible Tokens

As the name suggests, a nonfungible token's units are not equal to the units of other tokens.

4.3.1 NFT Standard

On Ethereum, the ERC-721 standard defines nonfungibility. This standard is similar to ERC-20, except each unit has its own unique ID, rather than all units being stored as a single balance. This unique ID can be linked to additional metadata that differentiate the token from others' stemming from the same contract. Under the balanceOf(address) method, the total number of nonfungible tokens (NFTs) in the given contract that the address owns is returned. An additional method, ownerOf(id), returns the address of the owner of a specific token, referenced by its ID. Another important difference is that ERC-20 allows for the partial approval of an operator's token balances, whereas ERC-721 uses an all-or-nothing approach. An operator approved to use the NFTs can move any of them.

NFTs have interesting applications in DeFi. Their alternate name, *deeds*, implies their use case as representing unique ownership of unitary assets; an example could be ownership of a particular P2P loan with its own rates and terms. The asset could then be transferred and sold via the ERC-721 interface. Another use case might be to represent a share in a lottery. Lottery tickets could be considered nonfungible because only one or a limited number will be winning tickets and the remainder are worthless. NFTs also have a strong use case in their ability to bridge financial and nonfinancial use cases via *collectibles* (e.g., a token could represent ownership in a piece of art). NFTs can also represent scarce items in a game or other network and retain economic value in secondary markets for NFTs.

4.3.2 Multi-Token Standard

ERC-20 and ERC-721 tokens require an individual contract and address deployed to the blockchain. These requirements can be cumbersome for systems that have many tokens, which are closely related, possibly even a mix of fungible and nonfungible token types. The ERC-1155 token standard resolves this complexity by defining a multi-token model in which the contract holds balances for a variable number of tokens, which can be fungible or nonfungible. The standard also allows for batch reading and transfers, which saves on gas costs and leads to a smoother user experience. Under ERC-1155 and similar to ERC-721, operators are approved for all supported tokens in a binary all-or-none fashion.

4.4 Custody

A critical DeFi primitive is the ability to escrow or custody funds directly in a smart contract. This is distinct from the situation in ERC-20 when operators are approved to transfer a user's balance. In that case, the user still retains custody of his funds and could transfer the balance at any time or revoke the contract's approval. When a smart contract has full custody over funds, new capabilities (and additional primitives) are possible:

- Retaining fees and disbursing incentives (Section 4.6)
- Facilitation of token swaps (Section 4.7)
- Market making of a bonding curve (Section 4.5)
- Collateralized Loans (Section 4.8)
- Auctions
- Insurance funds

In order to effectively custody tokens, a contract must be programmed to handle the token interface of the corresponding type of token, which would be ERC-20 for fungible tokens and ERC-721 for nonfungible tokens. The contract could generically handle all tokens of that interface or of a specific subset only. Users must exercise caution when sending tokens to contracts because the tokens could become permanently custodied if the contract has no encoded mechanism for releasing the funds of that particular token. Safety checks are often embedded in the token transfer to verify if the contract is registered to support a given token interface as a means to mitigate this potential problem.

4.5 Supply Adjustment

Supply adjustment applies specifically to fungible tokens and the ability to create (*mint*) and reduce (*burn*) supply via a smart contract. We will explore the basic primitives of burning and minting, and a more complex system known as a *bonding curve*.

4.5.1 Burn - Reduce Supply

To burn a token means to remove it from circulation. Burning a token can take two forms. One method is to manually send a token to an unowned Ethereum address. Another, and even more efficient, method is to create a contract that is incapable of spending them. Either approach renders the burned tokens unusable, although the decrease in circulating supply would not be "known" by the token contract. Burning is analogous to the destruction or irreversible loss of currency in the traditional finance world, which is unknown to the issuing government. In practice, ETH or ERC-20 tokens have frequently and accidently been burned using both forms. Mechanisms are in place to protect against accidental burning, such as checksumming addresses [16] and registering contracts[17] as being able to handle certain tokens.

---

[16] Checksums in general are cryptographic primitives used to verify data integrity. In the context of Ethereum addresses, EIP-55 proposed a specific checksum encoding of addresses to stop incorrect addresses' receiving token transfers. If an address used for a token transfer does not include the correct checksum metadata, the contract assumes the address was mistyped and the transaction would fail. Typically, these checks are added by code compilers before deploying smart contract code and by client software used for interacting with Ethereum.

[17] Registry contracts and interfaces allow a smart contract on chain to determine if another contract it interacts with is implementing the intended interface. For example, a contract may register itself as being able to handle specific ERC-20 tokens if unable to handle all ERC-20 tokens. Sending contracts can verify that the recipient does support ERC-20 tokens as a precondition for clearing the transfer. EIP-165 proposes a standard solution in which each contract declares which interfaces they implement.

More common and useful is the ability to intentionally burn tokens as a part of the smart contract design. Here are some example use cases for burning tokens algorithmically:

- Represent exiting of a pool and redemption of underlying (common in equity tokens like cTokens for Compound discussed in Section 6.1.2)
- Increase scarcity to drive the price upward (e.g., AAVE in Section 6.1.3, Seigniorage Stablecoin models like Basis/ESD)
- Penalize bad acting (discussed further in Section 4.7)

4.5.2 Mint - Increase Supply

The flip side of burning is *minting* tokens. Minting increases the number of tokens in circulation. Contrary to burning, there is no mechanism for accidentally or manually minting tokens. Any mint mechanics have to be directly encoded into the smart contract mechanism. There are many use cases for minting as it can incentivize a wider range of user behavior. Here are some examples:

- Represent entering a pool and acquiring corresponding ownership share (common in equity tokens like cTokens for Compound)
- Decrease scarcity (increase supply) to drive the price downward (seigniorage Stablecoin models like Basis/ESD)
- Reward user behavior

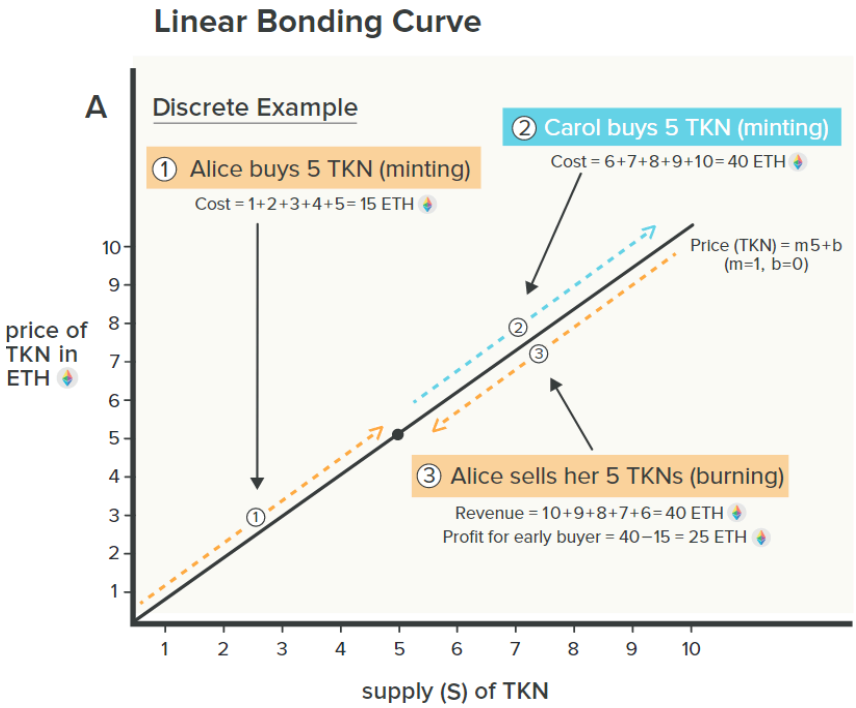
Rewarding user behavior with increases in supply (*inflationary rewards*) has become a common practice to encourage actions such as supplying liquidity or using a particular platform. Consequently, many users engage in *yield farming*, taking actions to seek the highest possible rewards. Platforms can bootstrap their networks by issuing a token with an additional value proposition in the network. Users can keep the token and use it in the context of the network or sell it for a profit. Either way, utilization of the token benefits the platform by increasing activity.

4.5.3. Bonding Curve - Pricing Supply

One advantage of being able to adjust supply up and down on a contractual basis is being able to define a bonding curve. A bonding curve is the price relationship between the token supply and a corresponding asset used to purchase the token(s). In most implementations investors sell back to the curve using the same price relationship. The relationship is defined as a mathematical function or as an algorithm with several clauses.

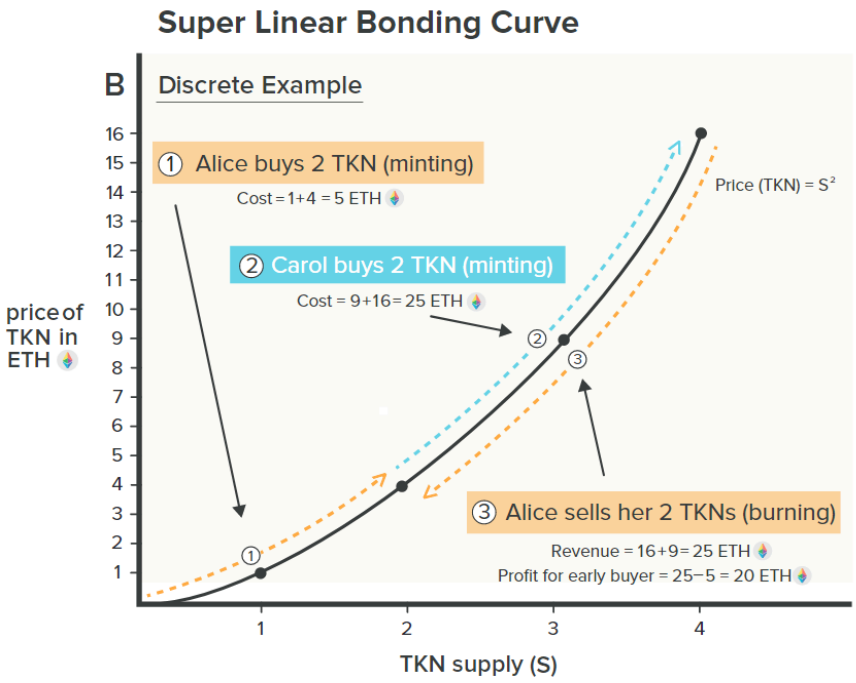
To illustrate, we can use TKN to denote the price of a token denominated in ETH (which could be any fungible cryptoasset) and use S to represent the supply. The simplest possible bonding curve would be $TKN = 1$ (or any constant). This relationship—TKN backed by a constant ratio of ETH—enforces that TKN is pegged to the price of ETH. The next-level bonding curve could be a simple linear bonding curve, where m and b represent the slope and intercept, respectively, in a standard linear function. If $m = 1$ and $b = 0$, the first TKN would cost 1 ETH, the second would cost 2 ETH, and so on. A monotonically increasing bonding curve rewards early investors,

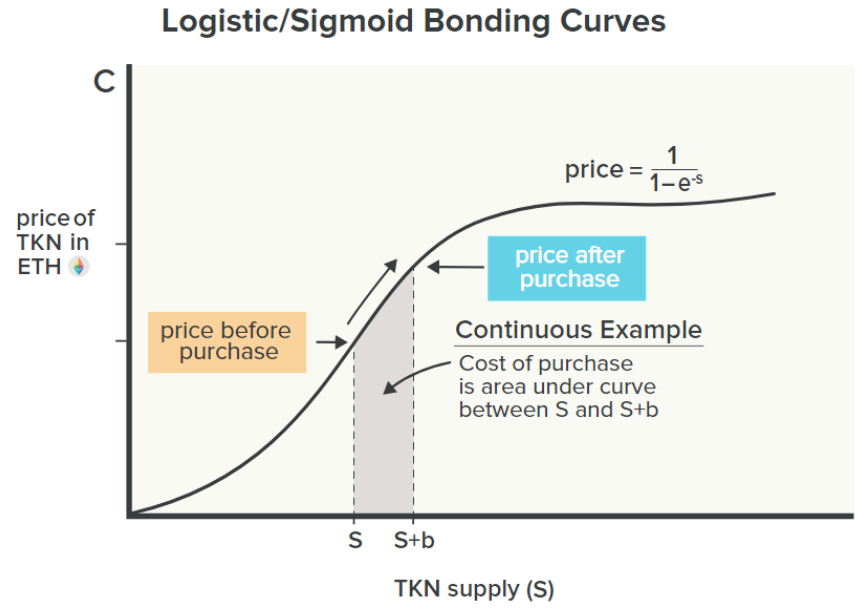
because any incremental demand beyond their purchase price would allow them to sell back against the curve at a higher price point.



The mechanics of a bonding curve are relatively straightforward. The curve can be represented as a single smart contract with options for purchasing and selling the underlying token. The token to be sold can have either an uncapped supply with the bonding curve as an authorized minter or a predetermined maximum supply that is escrowed in the bonding curve contract. As users purchase the token, the bonding curve escrows the incoming funding for the point in the future when a user may want to sell back against the curve.

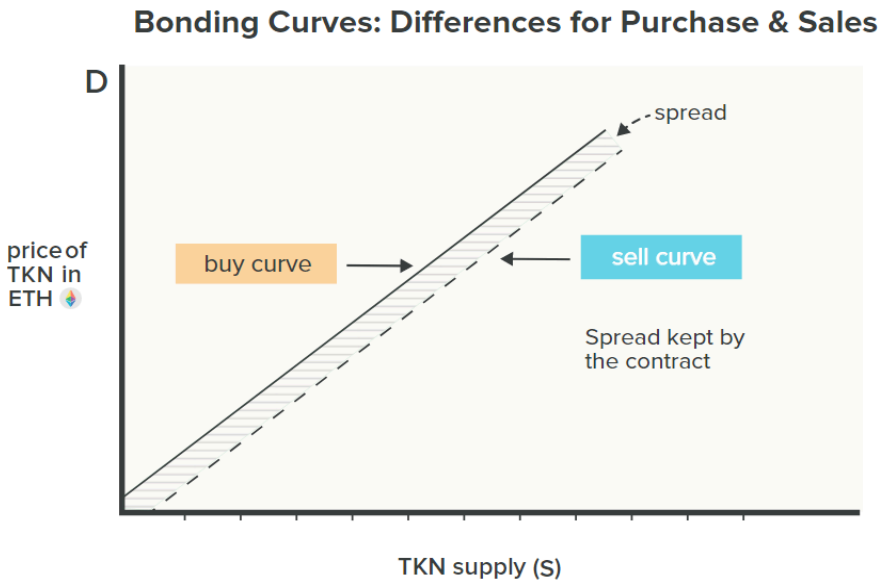
The growth rate of the bonding curve is important in determining users' performance. A linear growth rate would generously reward early users if the token grows to a sufficiently large supply. An even more extreme return could result from a superlinear growth rate, such as $TKN = S^2$. The first token would cost 1 ETH and the 100th would cost 10,000 ETH. In practice, most projects would use a sublinear growth rate or a logistic function that converges on an upper bounded price.





A bonding curve can have a different price curve for buyers and for sellers. The selling curve could have a lower growth rate or intercept than the buying curve. The spread between the curves would be the value (in this case ETH) accrued to the smart contract and could represent a fee for usage or used to finance more-complex functionality within the system. As long as the

contract maintains sufficient collateral to sell back down the entire sell curve, the contract is capitalized and able to fulfill any sell demand.



4.6 Incentives

Incentives within cryptoeconomic systems including DeFi are extremely important in encouraging desired (positive incentive) and discouraging undesired (negative incentive) user behaviors. The term *incentive* is quite broad, but we narrow our discussion to direct token payments or fees. We will look at two different categories of incentives: *staked incentives* and *direct incentives*. Staked incentives apply to a balance of tokens custodied in a smart contract. Direct incentives apply to users within the system who do not have a custodied balance.

Mechanisms in the contract determine the source of any reward funds and the destination for fees. Reward funds can be issued through inflation or by minting (Section 4.5.2) as well as custodied in the smart contract (Section 4.4). Funds removed as a fee can be burned (Section 4.5.1) or can be retained in the smart contract's custody. Reward funds can also be issued as a direct incentive to the platform's participants or can be raised through an auction to repay a debt. A mechanism might instigate a burn to reduce the supply of a particular token in order to increase price pressure.

4.6.1 Staking Rewards

A *staking reward* is a positive staked incentive by which a user receives a bonus in his token balance based on the stake he has in the system. Several verticals of incentive customization are possible:

- Stake requirement options:
    - minimum threshold or applied to all staked balances on a pro rata basis
- Reward options:
    - Fixed payout or pro rata payout
    - Same token type as staked or a distinct token

The Compound protocol (Section 6.1.2) issues staking rewards on user balances that are custodied in a borrowing or lending position. These rewards are paid in a separate token (COMP) funded by custodied COMP, which has a fixed supply, and applied to all staked balances on a pro rata basis. The Synthetix protocol (Section 6.3.3) issues staking rewards on staked SNX, its protocol token which has unlimited supply. The rewards are paid in SNX, funded by inflation, and issued only if the user meets a minimum-collateralization-ratio threshold.

4.6.2 Slashing (Staking Penalties)

Slashing is the removal of a portion of a user's staked balance, thereby creating a negative staked incentive. Slashing occurs as the result of an undesirable event. A *slashing condition* is a mechanism that triggers a slashing. As with staking rewards, several verticals of slashing customization are possible:

- Removed funds options:
    - Complete or partial slashing
- Slashing condition options:
    - Undercollateralization triggers liquidation
    - Detectable malicious behavior by user
    - Change in market conditions triggers necessary contraction

In Section 4.8 on collateralized loans, we will illustrate the common slashing mechanism of *liquidation*. In a liquidation, potential liquidators receive a direct incentive to execute the liquidation through auctioning or directly selling the collateral; the balance of funds remaining after the liquidation stays with the original owner. An example of slashing due to market changes not related to debt is an algorithmic stablecoin. This system might directly reduce a user's token balance when the price depreciates in order to return the supply-weighted price to, say, $1.

4.6.3 Direct Rewards and Keepers

Direct rewards are positive incentives that include payments or fees associated with user actions. As we mentioned in Section 4.1, all Ethereum interactions begin with a transaction, and all transactions begin with an externally owned account. An EOA, whether controlled by a human user or an off-chain bot, is (importantly) off chain, and thus autonomous response to market conditions is either expensive (costs gas) or technically infeasible. As a result, no transaction happens automatically on Ethereum without being purposely set in motion.

The classic example of a transaction that must be set in motion is when a collateralized debt position becomes undercollateralized. This use case does not automatically trigger a liquidation; the EOA must trigger the liquidation. For this use case and others, EOAs generally receive a direct incentive to trigger the contract. The contract then evaluates the conditions and liquidates or updates if everything is as expected. We will discuss the mechanics of liquidation in more depth in Section 4.8 on collateralized loans.

A *keeper* is a class of EOA incentivized to perform an action in a DeFi protocol or other dApp. A keeper is rewarded by receiving a fee, either flat or percentage of the incented action. With sufficient incentivization, autonomous monitoring can be outsourced off chain, thus creating robust economies and new profit opportunities. Keeper rewards may also be structured as an auction to ensure competition and best price. Keeper auctions are very competitive because the information available in the system is almost entirely public. A side effect of direct rewards for keepers is that gas prices can inflate due to the competition for these rewards. That is, more keeper activity generates additional demand for transactions, which in turn increases the price of gas.

4.6.4 Fees

Fees are typically a funding mechanism for the features of the system or platform. They can be flat or percentage based, depending on the desired incentive. Fees can be imposed as a direct negative incentive or can be accrued on staked balances. Accrued fees must have an associated staked balance to ensure the user pays them. Because of the pseudonymous anonymous nature of Ethereum accounts—all that is known about an Ethereum user is his wallet balance and interactions with various contracts on Ethereum—the imposition of fees is a design challenge. If the smart contract is open to any Ethereum account, the only way to guarantee enforcementis for all debts to be backed by staked on-chain collateral. The challenges created by anonymity make other mechanisms, such as reputation, unreliable compared to staked balances.

4.7 Swap

A swap is simply the exchange of one type of token for another. The key benefit of swapping in DeFi is that it is atomic and noncustodial. Funds can be custodied in a smart contract with

withdrawal rights that can be exercised at any time before the swap is completed. If the swap does not complete, all parties involved retain their custodied funds. The swap only executes when the exchange conditions are agreed to and met by all parties, and are enforced by the smart contract. If any condition is not met, the entire transaction is cancelled. A platform that facilitates token swapping on Ethereum in a noncustodial fashion is a *decentralized exchange* (DEX). There are two primary mechanisms for DEX liquidity: one is an order-matching approach and the other is an *Automated Market Maker*.

4.7.1 Order Book Matching

Order-book matching is a system in which all parties must agree on the swap exchange rate. Market makers can post bids and asks to a DEX and allow takers to fill the quotes at the pre-agreed-upon price. Until the offer is taken, the market maker retains the right to remove the offer or update the exchange rate as market conditions change.

The order-matching approach is expensive and inefficient because each update requires an on-chain transaction. An insurmountable inefficiency with an order-book matching is that both counterparties must be willing and able to exchange at the agreed-upon rate for the trade to execute. This requirement creates limitations for many smart contract applications in which demand for exchange liquidity cannot be dependent on a counterparty's availability. An innovative alternative is an Automated Market Maker.

4.7.2 Automated Market Makers (AMMs)

An Automated Market Maker (AMM) is a smart contract that holds assets on both sides of a trading pair and continuously quotes a price for buying and for selling. Based on executed purchases and sales, the contract updates the asset size behind the bid and the ask and uses this ratio to define its pricing function. The contract can also take into account more complex data than relative bid/ask size when determining price. From the contract's perspective, the price should be risk-neutral where it is indifferent to buying or selling.

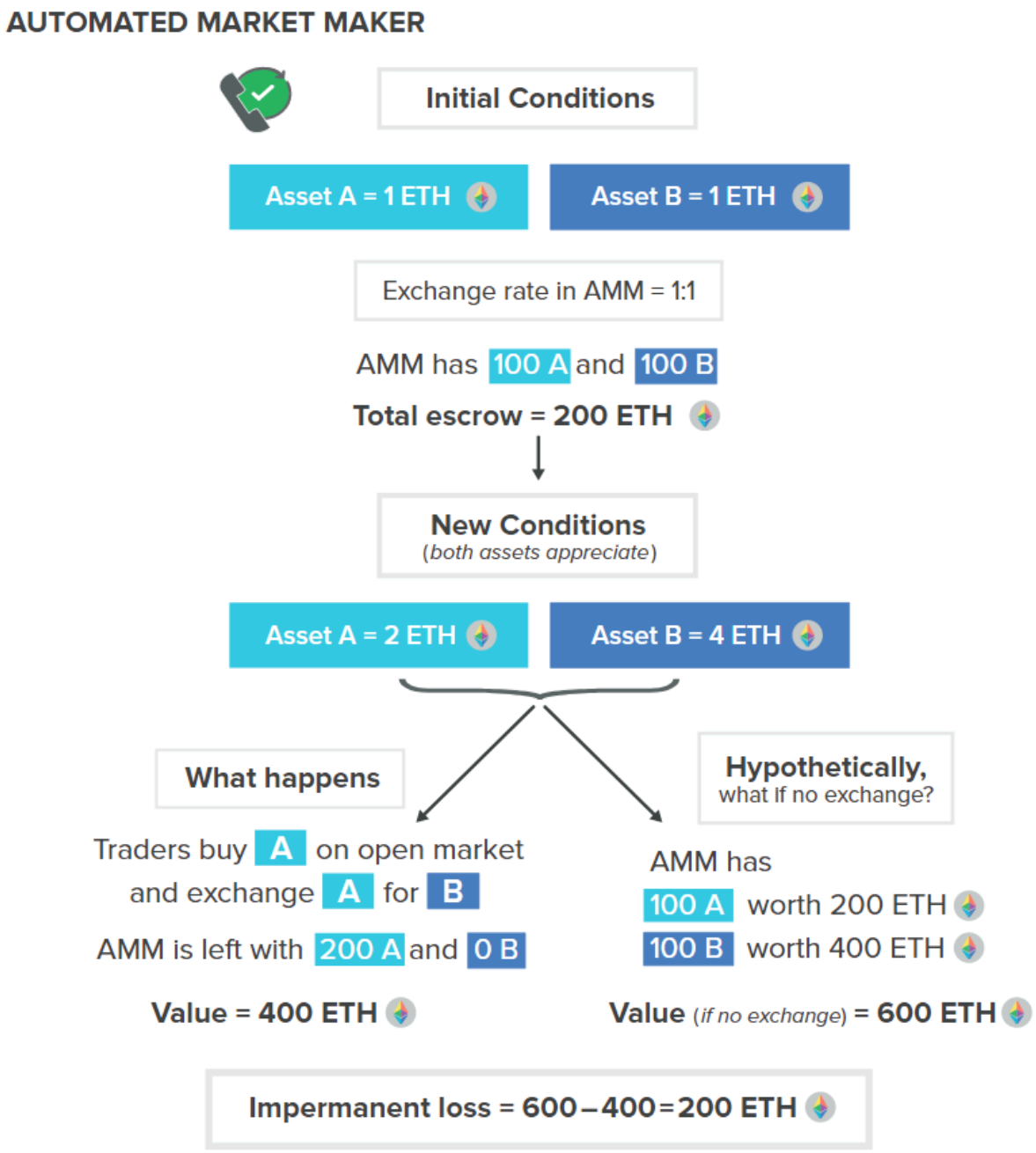
A naive AMM might set a fixed price ratio between two assets. With a fixed price ratio, when the market price shifts between the assets, the more valuable asset would be drained from the AMM and arbitraged on another exchange where trading is occurring at the market price. The AMM should have a pricing function that can converge on the market price of an asset so that it becomes more expensive to purchase an asset from the trading pair as the ratio of that asset to the others in the contract decreases.

The major benefits of an AMM are constant availability and that a traditional counterparty is not necessary to execute a trade. These provisions are very important for smart contracts and DeFi development because of the guarantee that a user can exchange assets at any moment if necessary. A user maintains custody of her funds until she completes the trade, hence, counterparty risk is zero. An additional benefit is *composable liquidity*, which means any

exchange contract can plug into the liquidity and exchange rates of any other exchange contract. AMMs make this particularly easy because of their guaranteed availability and their allowing one-sided trading against the contract. Composable liquidity correlates comfortably with the concept of DeFi Legos.

One drawback to an AMM is the concept of *impermanent loss*, the opportunity-cost dynamic between offering assets for exchange and holding the underlying assets to potentially profit from the price movement. The loss is impermanent because it can be recovered if the price reverts to its original level. To illustrate, consider two assets, A and B, each initially worth 1 ETH as in Exhibit X. The AMM contract holds identical quantities of 100 of each asset and naively offers both at a fixed exchange rate of 1:1. We use ETH as the unit of account to track the contract's return on its holdings and any impermanent loss. At the given balances and market exchange rates, the contract has 200 ETH in escrow. Suppose asset B's price appreciates to 4 ETH in the wider market and asset A's price appreciates to 2 ETH. Arbitrageurs exchange all of asset B in the contract for asset A because asset B is more valuable. The contract then holds 200 of asset A worth 400 ETH. In this case, the contract's real return is 100%.

If, however, the contract does not sell asset B, the contract's value would be 600 ETH. The contract has an impermanent loss equal to 200 ETH, the difference between 600 ETH and 400 ETH. If the contract's holdings return to parity between assets A and B, the impermanent loss disappears. If the goal for liquidity held in the contract is profit, any fees charged must exceed the amount of the impermanent loss.



Impermanent loss occurs for any shift in price and liquidity, because the contract is structured to sell the appreciating asset and to buy the depreciating asset. An important feature of impermanent loss is *path independence*. In our example, it is irrelevant whether 1 or 100 traders consumed all the liquidity. The final exchange rate and contract asset ratios yield the same impermanent loss regardless of the number of trades or the direction of the trades. Because of path independence, impermanent loss is minimized on trading pairs that have correlated prices (*mean-reverting pairs*). Thus, stablecoin trading pairs are particularly attractive for AMMs.

4.8 Collateralized Loans

Debt and lending are perhaps the most important financial mechanisms that exist in DeFi, and more generally, in traditional finance. On the one hand, these mechanisms are a powerful tool for efficiently allocating capital, increasing return-bearing risk exposure, and expanding economic growth. On the other hand, excess debt in the system can cause instability, leading to large economic and market contractions. These benefits and risks are amplified in DeFi, because the counterparties share an adversarial and integrated environment. Platforms are increasingly interdependent, and a debt-fueled collapse in one part of the system can quickly contaminate all connected protocols—and expand outward.

Any loan of non-zero duration (e.g., foreshadowing flash loan, as we discuss in Section 4.9) must be backed by an equivalent or excess amount of collateral. Requiring collateral contractually prevents a counterparty from defaulting. An uncollateralized mechanism raises the risk that a counterparty could steal funds, especially in an open and anonymous system such as Ethereum. A risk of overcollateralized positions is that the collateral becomes less valuable than the debt, leading to a foreclosure without an option for recovery. Therefore, more-volatile types of collateral require larger collateralization ratios in order to mitigate this risk.

We have already mentioned the mechanism of liquidation and now we will explain it in detail. To avoid liquidation it is imperative that debt remain overcollateralized by a margin sufficiently large that moderate price volatility does not place the collateral value in jeopardy. Smart contracts commonly define a minimum collateralization threshold below which the collateral can be liquidated and the position closed. The collateral could be auctioned or directly sold on a DEX, likely with an AMM, at the market price.

As stated in Section 4.6, positions in the Ethereum blockchain cannot be liquidated automatically, so an incentive is needed. The incentive often takes the form of a percentage fee allocated to an external keeper who is able to liquidate the position and collect the reward. Any remaining collateral is left to the original holder of the position. In some cases, the system will leave all remaining collateral to the keeper as a stronger incentive. Because the penalty for liquidation is high and most collateral types are volatile, platforms generally allow users to top up their collateral to maintain healthy collateralization ratios.

An interesting implication of collateralized loans and token supply adjustment (Section 4.5) is that collateralization can back the value of a synthetic token. The synthetic token is an asset created and funded by a debt, which has the requirement to repay the synthetic token in order to reclaim the collateral. The synthetic token can have a utility mechanism or represent a complex financial derivative, such as an option or bond (e.g., Synthetix Synth, discussed in Section 6.3.3 and Yield yToken, discussed in Section 6.3.1). A stablecoin that tracks the price of an underlying asset can also be a synthetic token of this type (e.g., MakerDAO DAI, discussed in Section 6.1.1).

4.9 Flash Loan (Uncollateralized Loan)

A financial primitive that uniquely exists in DeFi and dramatically broadens certain types of financial access is a *flash loan*. In traditional finance, a loan is an instrument designed to efficiently allocate excess capital from a person or entity who wishes to employ it (lender) to a person or entity who needs capital to fund a project or to consume (borrower). A lender is compensated for providing the capital and bearing the risk of default by the interest amount charged over the life of the loan. The interest rate is typically higher the longer the duration of the loan, because the longer time to repay exposes the lender to greater risk that the borrower may default.

Reversing the concept leads to the conclusion that shorter-term loans should be less risky and therefore require less compensation for the lender. A flash loan is an instantaneous loan paid back within the same transaction. A flash loan is similar to an overnight loan in traditional finance, but with a crucial difference—repayment is required within the transaction and enforced by the smart contract.

A thorough understanding of an Ethereum transaction is important for understanding how flash loans work. One clause in the transaction is vital: if the loan is not repaid with required interest by the end of the transaction, the whole process reverts to the state before any money ever left the lender's account. In other words, either the user successfully employs the loan for the desired use case and completely repays it in the transaction or the transaction fails and everything resets as if the user had not borrowed any money.

Flash loans essentially have zero counterparty risk or duration risk. However, there is always smart contract risk (e.g., a flaw in the contract design, see Section 7.1). They allow a user to take advantage of arbitrage opportunities or refinance loans without pledging collateral. This capability allows anyone in the world to have access to opportunities that typically require very large amounts of capital investment. In time, we will see similar innovations that could not exist in the world of traditional finance.

5. Problems DeFi Solves

In this chapter, we will address the concrete solutions that DeFi presents to the five flaws of traditional finance: inefficiency, limited access, opacity, centralized control, and lack of interoperability.

5.1 Inefficiency

The first of the five flaws of traditional finance is inefficiency. DeFi can accomplish financial transactions with high volumes of assets and low friction that would generally be a large organizational burden for traditional finance. DeFi creates reusable smart contracts in the form of dApps designed to execute a specific financial operation. These dApps are available to any user who seeks that particular type of service, for example, to execute a put option, regardless of the size of the transaction. A user can largely self-serve within the parameters of the smart contract and of the blockchain the application lives on. In the case of Ethereum-based DeFi, the contracts can be used by anyone who pays the flat gas fee, usually around $15.00 for a transfer and $25.00 for a dApp feature such as leveraging against collateral. Once deployed, these contracts continually provide their service with near-zero organizational overhead.

5.1.1 Keepers

We introduced the concept of a keeper in Section 4.6.3. Keepers are external participants directly incentivized to provide a service to DeFi protocols, such as monitoring positions to safeguard that they are sufficiently collateralized or triggering state updates for various functions. To ensure that a dApp's benefits and services are optimally priced, keeper rewards are often structured as an auction. Pure, open competition provides value to DeFi platforms by guaranteeing users pay the market price for the services they need.

5.1.2 Forking

Another concept that also incentivizes efficiency is a *fork*. A fork, in the context of open source code, is a copy and reuse of the code with upgrades or enhancements layered on top. A common fork of blockchain protocols is to reference them in two parallel currencies and chains. Doing so creates competition at the protocol level and creates the best possible smart contract platform. Not only is the code of the entire Ethereum blockchain public and forkable, but each DeFi dApp built on top of Ethereum is as well. Should inefficient or suboptimal DeFi applications exist, the code can be easily copied, improved, and redeployed through forking. Forking and its benefits arise from the open nature of DeFi and blockchains.

Forking creates an interesting challenge to DeFi platforms, namely, *vampirism*. Vampirism is an exact or near-carbon copy of a DeFi platform designed to poach liquidity or users by offering larger incentives than the platform it is copying. The larger incentives usually take the form of inflationary rewards offered at a far higher rate than the original platform offers. Users might be attracted to the higher potential reward for the same functionality, which would cause a reduction in usage and liquidity on the initial platform.

If the inflationary rewards are flawed, over long-term use the clone could perhaps collapse after a large asset bubble. The clones could also select closer to optimal models and replace the

original platform. Vampirism is not an inherent risk or flaw, but rather a complicating factor arising from the pure competition and openness of DeFi. The selection process will eventually give rise to more robust financial infrastructure with optimal efficiency.

5.2 Limited Access

As smart contract platforms move to more-scalable implementations, user friction falls, enabling a wide range of users, and thus mitigates the second flaw of traditional finance: limited access. DeFi gives large underserved groups, such as the global population of the unbanked as well as small businesses that employ substantial portions of the workforce (for example, nearly 50% in the United States) direct access to financial services. The resulting impact on the entire global economy should be strongly positive. Even consumers who have access to financial services in traditional finance, such as bank accounts, mortgages, and credit cards, do not have access to the financial products with the most competitive pricing and most favorable terms; these products and structures are restricted to large institutions. DeFi allows any user access to the entirety of its financial infrastructure, regardless of her wealth or geographic location.

5.2.1 Yield Farming

Yield farming, mentioned in Section 4.5.2, provides access to many who need financial services but whom traditional finance leaves behind. To summarize, yield farming provides inflationary or contract-funded rewards to users for staking capital or utilizing a protocol. These rewards are payable in the same underlying asset the user holds or in a distinct asset such as a governance token. Any user can participate in yield farming. A user can stake an amount of any size, regardless of how small, and receive a proportional reward. This capability is particularly powerful in the case of governance tokens. A user of a protocol that issues a governance token via yield farming becomes a partial owner of the platform through the issued token. A rare occurrence in traditional finance, this process is a common and celebrated way to give ownership of the platform to the people who use and benefit from it.

5.2.2 Initial DeFi Offering

An interesting consequence of yield farming is that a user can create an *Initial DeFi Offering* (IDO) by market making his own Uniswap (section 6.2.1) trading pair. The user can set the initial exchange rate by becoming the first liquidity provider on the pair. Suppose the user's token is called DFT and has a total supply of 2 million. The user can make each DFT worth 0.10 USDC by opening the market with 1 million DFT and 100,000 USDC. Any ERC-20 token holder can purchase DFT, which drives up the price. As the only liquidity provider, the user also receives all of the trading fees. In this way, the user is able to get his token immediate access to as many users as possible. The method sets an artificial price floor for the token if the user controls the supply outside of the amount supplied to the Uniswap market, and as such, inhibits

price discovery. The trade-offs of an IDO should be weighed as an option, or strategy, for a user's token distribution.

IDOs democratize access to DeFi in two ways. First, an IDO allows a project to list on high-traffic DeFi exchanges that do not have barriers to entry beyond the initial capital. Second, an IDO allows a user access to the best new projects immediately after the project lists.

5.3 Opacity

The third drawback of traditional finance is opacity. DeFi elegantly solves this problem through the open and contractual nature of agreements. We will explore how smart contracts and tokenization improve transparency within DeFi.

5.3.1 Smart Contracts

Smart contracts provide an immediate benefit in terms of transparency. All parties are aware of the capitalization of their counterparties and, to the extent required, can see how funds will be deployed. The parties can read the contracts themselves to determine if the terms are agreeable to eliminate any ambiguity as to what will happen when they interact under the contract terms. This transparency substantially eases the threat of legal burdens and brings peace of mind to smaller players who, in the current environment of traditional finance, could be abused by powerful counterparties through delaying or even completely withholding their end of a financial agreement. Realistically, the average consumer does not understand the contract code, but can rely on the open-source nature of the platform, the existence of code audits (discussed in section 7) and the wisdom of the crowd to feel secure. Overall, DeFi mitigates counterparty risk and thus creates a host of efficiencies not present under traditional finance.

DeFi participants are accountable for acting in accordance with the terms of the contracts they use. One mechanism for ensuring the appropriate behavior is staking. Staking is escrowing a cryptoasset into a contract, so that the contract releases the cryptoasset to the appropriate counterparty only after the contract terms are met; otherwise, the asset reverts to the original holder. Parties can be required to stake on any claims or interactions they make. Staking enforces agreements by imposing a tangible penalty for the misbehaving side and a tangible reward for the counterparty. The tangible reward should be as good as or even better than the outcome of the original terms of the contract. These transparent incentive structures provide much securer and more obvious guarantees than traditional financial agreements.

Another type of smart contract in DeFi that improves transparency is a token contract. Tokenization allows for transparent ownership and economics within a system. Users can know exactly how many tokens are in the system as well as the inflation and deflation parameters.

5.4 Centralized Control

The fourth flaw of traditional finance is the strong control exerted by governments and large institutions that hold a virtual monopoly over elements such as the money supply, rate of inflation, and access to the best investment opportunities. DeFi upends this centralized control by relinquishing control to open protocols having transparent and immutable properties. The community of stakeholders or even a predetermined algorithm can control a parameter, such as the inflation rate, of a DeFi dApp. If a dApp contains special privileges for an administrator, all users are aware of the privileges, and any user can readily create a less-centralized counterpart.

The open-source ethos of blockchain and the public nature of all smart contracts assures that flaws and inefficiencies in a DeFi project can be readily identified and "forked away" by users who copy and improve the flawed project. Consequently, DeFi strives to design protocols that naturally and elegantly incentivize stakeholders and maintain a healthy equilibrium through careful mechanism design. Naturally, trade-offs exist between having a centralized party and not having one. Centralized control allows for radically decisive action in a crisis, sometimes the necessary approach but also perhaps an overreaction. The path to decentralizing finance will certainly encounter growing pains because of the challenges in pre-planning for every eventuality and economic nuance. Ultimately, however, the transparency and security gained through a decentralized approach will lead to robust protocols that can become trusted financial infrastructure for a global user base.

5.4.1 Decentralized Autonomous Organization

A *decentralized autonomous organization* (*DAO*) has its rules of operation encoded in smart contracts that determine who can execute what behavior or upgrade. It is common for a DAO to have some kind of *governance token*, which gives an owner some percentage of the vote on future outcomes. We will explore governance in much more detail later.

5.5 Lack of Interoperability

We will now touch on the lack-of-interoperability aspect of traditional finance that DeFi solves. Traditional financial products are difficult to integrate with each other, generally requiring at minimum a wire transfer, but in many cases cannot be recombined. The possibilities for DeFi are substantial and new innovations continue to grow at a non-linear rate. This growth is fueled by the ease of composability of DeFi products. Once one has some base infrastructure to, for example, create a synthetic asset, any new protocols allowing for borrowing and lending can be applied. A higher layer would allow for attainment of leverage on top of borrowed assets. Such composability can continue in an increasing number of directions as new platforms arise. For this reason, *DeFi Legos* is an analogy often used to describe the act of combining existing protocols into a new protocol. We will discuss below a few advantages to this composability, namely tokenization and networked liquidity.

5.5.1 Tokenization

Tokenization is a critical way in which DeFi platforms integrate with each other. Take for example a percentage ownership stake in a private commercial real estate venture. In traditional finance to use this asset as collateral for a loan or as margin to open a levered derivative position would be quite difficult. Because DeFi relies on shared interfaces, applications can directly plug into each other's assets, repackage, and subdivide positions as needed. DeFi has the potential to unlock liquidity in traditionally illiquid assets through tokenization. A simple use case would be creating fractional shares from a unitary asset such as a stock. We can extend this concept to give fractional ownership to scarce resources such as rare art. The tokens can be used as collateral for any other DeFi service, such as leverage or derivatives.

We are able to invert this paradigm to create token bundles of groups of real-world or digital assets and trade them like an ETF. Imagine a dApp similar to a real estate investment trust (REIT), but with the added capability of allowing the owner to subdivide the REIT into the individual real estate components to select a preferred geographic distribution and allocation within the REIT. Ownership of the token provides direct ownership of the distribution of the properties. The owner can trade the token on a decentralized exchange to liquidate the position.

Tokenizing hard assets, such as real estate or precious metals, is more difficult than tokenizing digital assets because the practical considerations related to the hard assets, such as maintenance and storage, cannot be enforced by code. Legal restrictions across jurisdictions are also a challenge for tokenization; nevertheless, the utility of secure, contractual tokenization for most use cases should not be underestimated.

A tokenized version of a position in a DeFi platform is a pluggable derivative asset that is usable in another platform. Tokenization allows the benefits and features of one position to be portable. The archetypal example of portability through tokenization is Compound, which we will discuss in Section 6.2. Compound allows for robust lending markets in which a position can accrue variable-rate interest denominated in a given token, and the position itself is a token. If, for example, the base asset is ETH, the ETH deposit wrapper known as cETH (cToken) can be used in place of the base asset. The result is an ETH-backed derivative that is also accruing variable-rate interest per the Compound protocol. Tokenization, therefore, unlocks new revenue models for dApps because they can plug asset holdings directly into Compound or use the cToken interface to gain the benefits of Compound's interest rates.

5.5.2 Networked Liquidity

The concept of interoperability extends easily to liquidity in the exchange use case. Traditional exchanges, in particular those that retail investors typically use, cannot readily share liquidity with other exchanges. In DeFi, as a subcomponent of the contract, any exchange application can leverage the liquidity and rates of any other exchange on the same blockchain. This capability

allows for networked liquidity and leads to very competitive rates for users within the same application.

6. DeFi Deep Dive

DeFi can be loosely broken into sectors based on the functionality type of the dApp. Many dApps could fit into multiple categories, so we attempt to place them into the most relevant category. We examine DeFi platforms in the taxonomy of lending/credit facilities, DEXes, derivatives, and tokenization.[18] We mainly focus on the Ethereum network due to its popularity, but DeFi innovations are occurring on many blockchains including Stellar and EOS. Polkadot is another platform that employs a type of Proof of Stake consensus.

6.1 Credit/Lending

6.1.1 MakerDAO

MakerDAO (DAO is a decentralized autonomous organization) is often considered an exemplar of DeFi. In order for a series of applications to build on each other, there must necessarily be a foundation. The primary value-add of MakerDAO is the creation of a crypto-collateralized stablecoin, pegged to USD. This means the system can run completely from within the Ethereum blockchain without relying on outside centralized institutions to back, vault and audit the stablecoin. MakerDAO is a two-token model where a governance token MKR yields voting rights on the platform and participates in value capture. The second token is the stablecoin, called DAI, and is a staple token in the DeFi ecosystem with which many protocols integrate - including a few we will discuss later.

DAI is generated as follows. A user can deposit ETH or other supported ERC-20 assets into a *Vault*. A Vault is a smart contract that escrows collateral and keeps track of the USD-denominated value of the collateral. The user can then mint DAI up to a certain collateralization ratio on their assets. This creates a "debt" in DAI that must be paid back by the Vault holder. The DAI is the corresponding asset that can be used any way the Vault holder wishes. For example, the user can sell the DAI for cash or lever it into more of the collateral asset,[19] and repeat the process. Due to the volatility of ETH and most collateral types, the collateralization requirement is far in excess of 100% and usually in the 150-200% range.

[18] A large number of DeFi resources are available. For example, see https://defipulse.com/defi-list/ and https://github.com/ong/awesome-decentralized-finance. We do not cover all applications. For example, insurance is a growing area in DeFi that offers to reinvent traditional insurance markets.
[19] It is possible to deposit ETH into the contract and receive DAI. An investor could use that DAI to buy more ETH and repeat the process, allowing the investor to create a leveraged ETH position.

The basic idea is not new; it is simply a collateralized debt position. For example, a homeowner in need of some liquidity can pledge their house as collateral to a bank and receive a mortgage loan structured to include a cash takeout. The price volatility of ETH is much greater than for a house and, as such, collateralization ratios for the ETH-DAI contract are higher. In addition, no centralized institution is necessary as everything happens within the Ethereum blockchain.

Let's consider a simple example. Suppose an ETH owner needs liquidity but does not want to sell her ETH because she thinks it will appreciate. The situation is analogous to the homeowner who needs liquidity but does not want to sell her house. Let's say an investor has 5 ETH at a market price of $200 (total value of $1,000). If the collateralization requirement is 150%, then the investor can mint up to 667 DAI ($1,000/1.5 with rounding). The collateralization ratio is set high to reduce the probability that the loan debt exceeds the collateral value, and for the DAI token to be credibly pegged to the USD, the system needs to avoid the risk that the collateral is worth less than $1=1 DAI.

Given the collateralization ratio of 1.5, it would be unwise to mint the 667 DAI because if the ETH ever dropped below $200, the contract would be undercollateralized, the equivalent of a "margin call". We are using traditional finance parlance, but in DeFi there is no communication from your broker about the need to post additional margin or to liquidate the position and also no grace period. Liquidation can happen immediately.

As such, most investors choose to mint less than 667 DAI to give themselves a buffer. Suppose the investor mints 500 DAI, which implies a collateralization ratio of 2.0 ($1,000/2.0 =500). Let's explore two scenarios. First, suppose the price of ETH rises by 50% so that the collateral is worth $1,500. Now, the investor can increase the size of his loan. To maintain the collateralization of 200%, the investor can mint an extra 250 DAI.

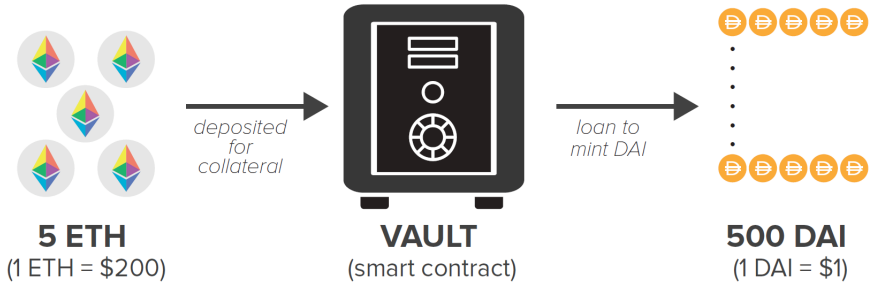
A more interesting scenario is when the value of the collateral drops. Suppose the value of the ETH drops by 25% from $200 to $150. In this case, the value of the collateral drops to $750 and the collateralization ratio drops to 1.5 ($750/1.5 = 500).

The Vault holder faces three scenarios. First, he can increase the amount of collateral in the contract (by, for example, adding 1 ETH). Second, he can use the 500 DAI to pay back the loan and repatriate the 5 ETH. These ETH are now worth $250 less, but the depreciation in value would have happened irrespective of the loan. Third, the loan is liquidated by a *keeper* (any external actor). A keeper is incentivized to find contracts eligible for liquidation. The keeper auctions the ETH for enough DAI to pay off the loan. In this case, 3.33 ETH would be sold and 1.47 would be returned to the Vault holder (the keeper earns an incentive fee of 0.2 ETH). The Vault holder then has 500 DAI worth $500 and 1.47 ETH worth $220. This analysis does not include gas fees.

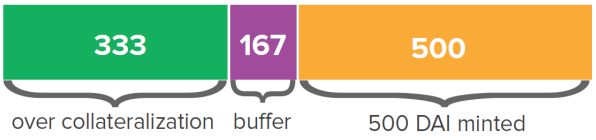
Two forces in this process reinforce the stability of DAI. The first is the overcollateralization. The second is the market actions. In the liquidation, ETH are sold and DAI are purchased, which

exerts positive price pressure on DAI. This simple example does not address many features in the MakerDAO ecosystem, in particular, the fee mechanisms and the debt limit, which we will now explore.

EXHIBIT A



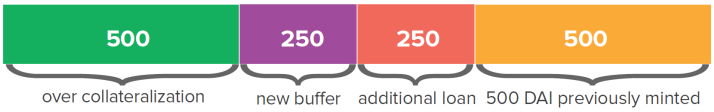
VALUE of COLLATERAL (5 ETH) = $1000



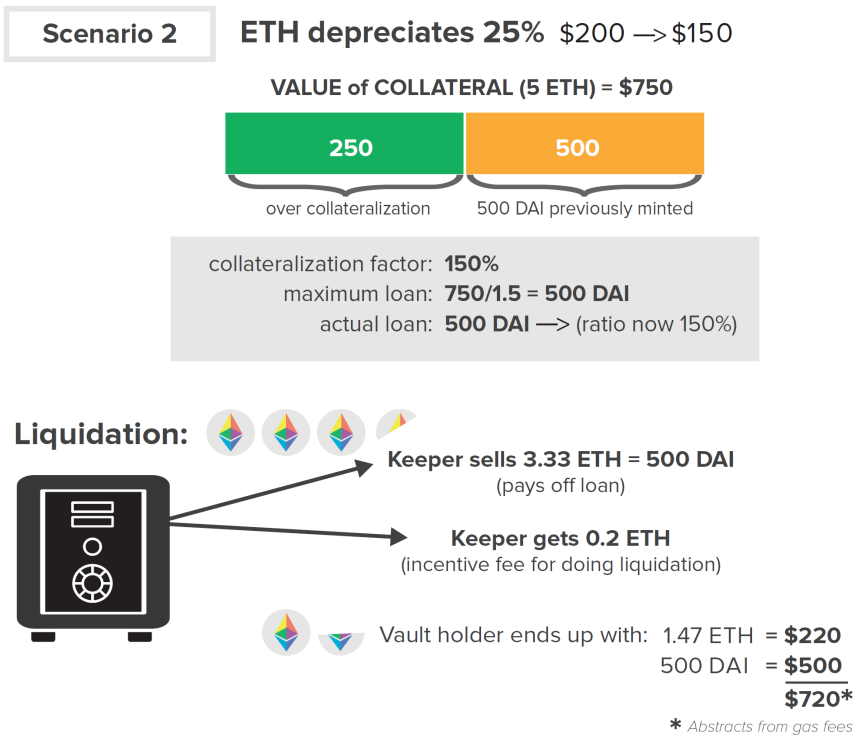
collateralization factor: **150%**
maximum loan: **1000/1.5 = 667 DAI**
actual loan: **500 DAI**

Scenario 1 **ETH appreciates 50%** $200 —> $300

VALUE of COLLATERAL (5 ETH) = $1500



collateralization factor: **150%**
maximum loan: **1500/1.5 = 1000 DAI**
actual loan: **500 DAI** —> (ratio now 300%)
additional loan: **250 DAI**
new loan: **750 DAI** —> (ratio 200%)



The viability of the MakerDAO ecosystem critically depends on DAI maintaining a 1:1 peg to the USD. Various mechanisms are in place to incentivize demand and supply in order to drive the price toward the peg. The primary mechanisms for maintaining the peg are the debt ceiling, stability fee, and DAI Savings Rate (DSR). These parameters are controlled by holders of the governance token Maker (MKR) and MakerDAO governance, which we will discuss toward the end of this section.

The Stability Fee is a variable interest rate paid in DAI by Vault holders on any DAI debt they generate. The interest rate can be raised or lowered (even to a negative value) to incentivize the generation or repayment of DAI to drive its price toward the peg. The Stability Fee funds the DSR, a variable rate any DAI holder can earn on their DAI deposit. The DSR compounds on a per-block basis. The Stability Fee, which must always be greater or equal to the DSR, is enforced by the smart contracts powering the platform. Lastly, a smart contract–enforced DAI debt ceiling can be adjusted to allow for more or less supply to meet the current level of demand. If the protocol is at the debt ceiling, no new DAI is able to be minted in new Vaults until the old debt is paid or the ceiling is raised.

To stay above the liquidation threshold, a user can deposit more collateral into the Vault to keep the DAI safely collateralized. When a position is deemed to be under the liquidation ratio, a keeper can initiate an auction (sell some of the ETH collateral[20]) to liquidate the position and

[20] The amount of ETH available for sale depends on the collateralization. Any unneeded collateral remains in the contract for the Vault holder to withdraw.

close the Vault holder's debt. The *Liquidation Penalty* is calculated as a percentage of the debt and is deducted from the collateral in addition to the amount needed to close the position.

After the auction, any remaining collateral reverts to the Vault owner. The Liquidation Penalty acts as an incentive for market participants to monitor the Vaults and trigger an auction when a position becomes undercollateralized. If the collateral drops so far in value that the DAI debt cannot be fully repaid, the position is closed, and the protocol accrues what is known as *Protocol Debt*. A buffer pool of DAI exists to cover Protocol Debt, but in certain circumstances the debt can be too great for even the buffer pool to cover. The solution involves the governance token MKR and the governance system.

The MKR token controls MakerDAO. Holders of the token have the right to vote on protocol upgrades, including supporting new collateral types and tweaking parameters such as collateralization ratios. MKR holders are expected to make decisions in the best financial interest of the platform. Their incentive is that a healthy platform should increase the value of their share in the platform's governance. For example, poor governance could lead to a situation as described earlier in which the buffer pool is not sufficient to pay back the Protocol Debt. In this case, newly minted MKR tokens are auctioned off in exchange for DAI and the DAI are used to pay back the Protocol Debt. This process is *Global Settlement*, a safety mechanism intended for use only when all other measures have failed. Global Settlement dilutes the MKR share, which is why stakeholders are incentivized to avoid it and keep Protocol Debt to a minimum.

MKR holders are collectively the owners of the future of MakerDAO. A proposal and corresponding approved vote can change any of the parameters available on the platform. Other possible parameter changes include supporting new collateral types for Vaults and adding upgrades to functionality. MKR holders could for instance vote to pay themselves a dividend funded by the spread between the interest payments paid by Vault holders and the DAI Savings Rate. The reward of receiving this dividend would need to be weighed against any negative community response (e.g., a backlash against rent seeking from a previously no-rent protocol) that might decrease the value of the protocol and the MKR token.

A number of features make DAI attractive to users. Importantly, users can purchase and utilize DAI without having to go through the process of generating it in a Vault—they can simply purchase DAI on an exchange. Therefore, users do not need to know the underlying mechanics of how DAI are created. Holders can easily earn the DAI Savings Rate by using the protocol. More technologically and financially sophisticated users can use the MakerDAO web portal to generate Vaults and create DAI to get liquidity from their assets without having to sell them. It is easy to sell DAI and purchase an additional amount of the collateral asset to get leverage.

A noteworthy drawback to DAI is that its supply is always constrained by demand for ETH-collateralized debt. No clear arbitrage loop exists to maintain the peg. For example, the stablecoin USDC is always redeemable by Coinbase for $1, with no fees. Arbitrageurs have a guaranteed (assuming solvency of Coinbase) strategy in which they can buy USDC at a discount or sell it at a premium elsewhere and redeem on Coinbase. This is not true for DAI. Irrespective

of any drawbacks, the simplicity of DAI makes it an essential building block for other DeFi applications.

Traditional Finance Problem	**MakerDAO Solution**
Centralized Control: Interest rates are influenced by the US Federal Reserve and access to loan products controlled by regulation and institutional policies.	MakerDAO platform is openly controlled by the MKR holders.
Limited Access: Obtaining loans is difficult for a large majority of the population.	Open ability to take out DAI liquidity against an overcollateralized position in any supported ERC-20 token. Access to a competitive USD-denominated return in the DSR.
Inefficiency: Acquiring a loan involves costs of time and money.	Instant liquidity at the push of a button with minimal transaction costs.
Lack of Interoperability: Cannot trustlessly use USD or USD-collateralized token in smart contract agreements.	Issuance of DAI, a permissionless USD-tracking stablecoin backed by cryptocurrency. DAI can be used in any smart contract or DeFi application.
Opacity: Unclear collateralization of lending institutions.	Transparent collateralization ratios of vaults visible to entire ecosystem.

6.1.2 Compound

Compound is a lending market that offers several different ERC-20 assets for borrowing and lending. All the tokens in a single market are pooled together so every lender earns the same variable rate and every borrower pays the same variable rate. The concept of a credit rating is irrelevant, and because Ethereum accounts are pseudonymous, enforcing repayment in the event of a loan default is virtually impossible. For this reason, all loans are overcollateralized in a collateral asset different from the one being borrowed. If a borrower falls below their collateralization ratio, their position is liquidated to pay back their debt. The debt can be liquidated by a keeper, similar to the process used in MakerDAO Vaults. The keeper receives a bonus incentive for each unit of debt they close out.

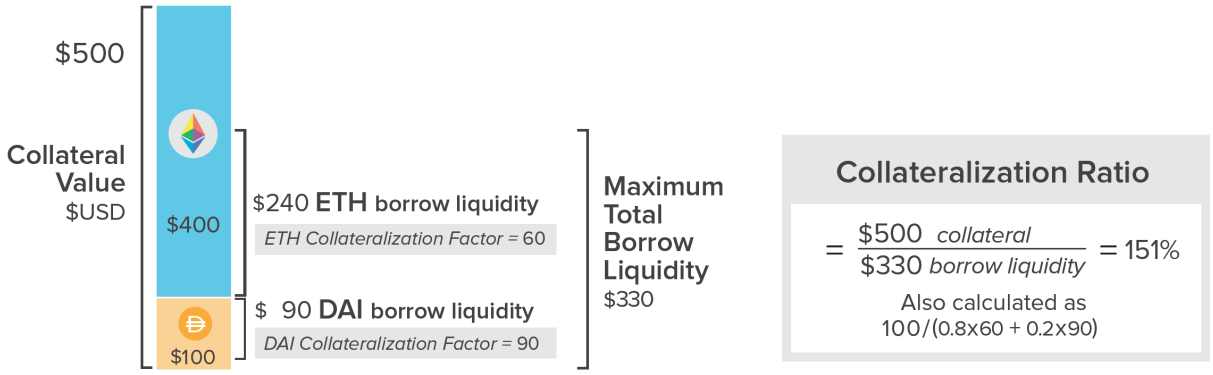
The collateralization ratio is calculated via a *collateral factor*. Each ERC-20 asset on the platform has its own collateral factor ranging from 0-90%. A collateral factor of zero means an asset cannot be used as collateral. The required collateralization ratio for a single collateral type

is calculated as 100 divided by the collateral factor. Volatile assets generally have lower collateral factors, which mandate higher collateralization ratios due to increased risk of a price movement that could lead to undercollateralization. An account can use multiple collateral types at once, in which case the collateralization ratio is calculated as 100 divided by the weighted average of the collateral types by their relative sizes (denominated in a common currency) in the portfolio.

The collateralization ratio is similar to a reserve multiplier in traditional banking, constraining the amount of "borrowed" dollars that can be in the system relative to the "real" supply. For instance, there is occasionally more DAI in Compound than is actually supplied by MakerDAO, because users are borrowing and resupplying or selling to others who resupply. Importantly, all MakerDAO supply is ultimately backed by real collateral and there is no way to borrow more collateral value than has been supplied.

For example, suppose an investor deposits 100 DAI with a collateral factor of 90. This transaction alone corresponds to a required collateralization ratio of 111%. Assuming 1 DAI = $1, the investor can borrow up to $90 worth of any other asset in Compound. If she borrows the maximum, and the price of the borrowed asset increases at all, the position is subject to liquidation. Suppose she also deposits two ETH with a collateral factor of 60 and a price of $200/ETH. The total supply balance is now $500, with 80% being ETH and 20% being DAI. The required collateralization ratio is 100/(0.8*60 + 0.2*90) = 151%.

EXHIBIT B



The supply and borrow interest rates are compounded every block (approximately 15 seconds on Ethereum producing approximately continuous compounding) and are determined by the utilization percentage in the market. Utilization is calculated as total borrow/total supply. The utilization rate is used as an input parameter to a formula that determines the interest rates. The remaining parameters are set by *Compound Governance* which we describe near the end of this section.

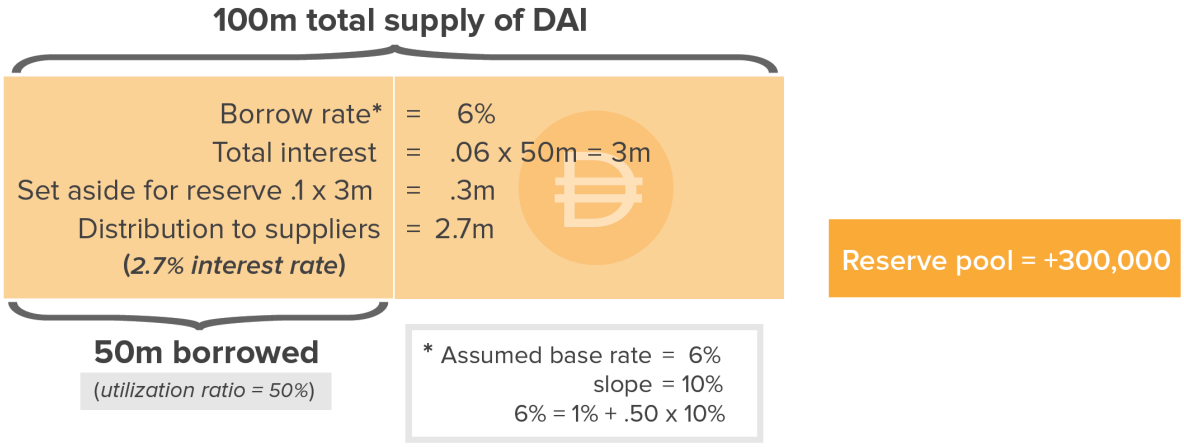
The formula for the borrow rate generally is an increasing linear function with a y-intercept known as the *base rate* that represents the borrow rate at 0% borrow demand and a *slope* representing the rate of change of the rates. These parameters are different for each ERC-20 asset supported by the platforms. Some markets have more advanced formulas that include a *kink*. A kink is a utilization ratio beyond which the slope steepens. These formulas can be used to reduce the cost of borrowing up to the kink and then increase the cost of borrowing after the kink to incentivize a minimum level of liquidity.

The supply interest rate is the borrow rate multiplied by the utilization ratio so borrow payments can fully cover the supplier rates. The *reserve factor* is a percentage of the borrow payments not given to the suppliers and instead set aside in a reserve pool that acts as insurance in the case a borrower defaults. In an extreme price movement, many positions may become undercollateralized in that they have insufficient funds to repay the suppliers. In the event of such a scenario, the suppliers would be repaid using the assets in the reserve pool.

Here is a concrete example of the rates: In the DAI market, 100 million is supplied and 50 million is borrowed. Suppose the base rate is 1% and the slope is 10%. At 50 million borrowed, utilization is 50%. The borrow interest rate is then calculated to be 0.5*0.1 + 0.01 = 0.06 or 6%. The maximum supply rate (assuming a reserve factor of zero) would simply be 0.5*0.06 = 0.03 or 3%. If the reserve factor is set to 10, then 10% of the borrow interest is diverted to a DAI reserve pool, lowering the supply interest rate to 2.7%. Another way to think about the supply interest rate is that the 6% borrow interest of 50 million is equal to 3 million of borrow payments. Distributing 3 million of payments to 100 million of suppliers implies a 3% interest rate to all suppliers.

For a more complicated example involving a kink, suppose 100 million DAI is supplied and 90 million DAI is borrowed, a 90% utilization. The kink is at 80% utilization, before which the slope is 10% and after which the slope is 40%, which implies the borrow rate will be much higher if the 80% utilization is exceeded. The base rate remains at 1%. The borrow interest rate = 0.01 (base) + 0.8*0.1 (pre-kink) + 0.1*0.4 (post-kink) = 13%. The supply rate (assuming a reserve factor of zero) is 0.9*0.13 = 11.7%.

EXHIBIT C



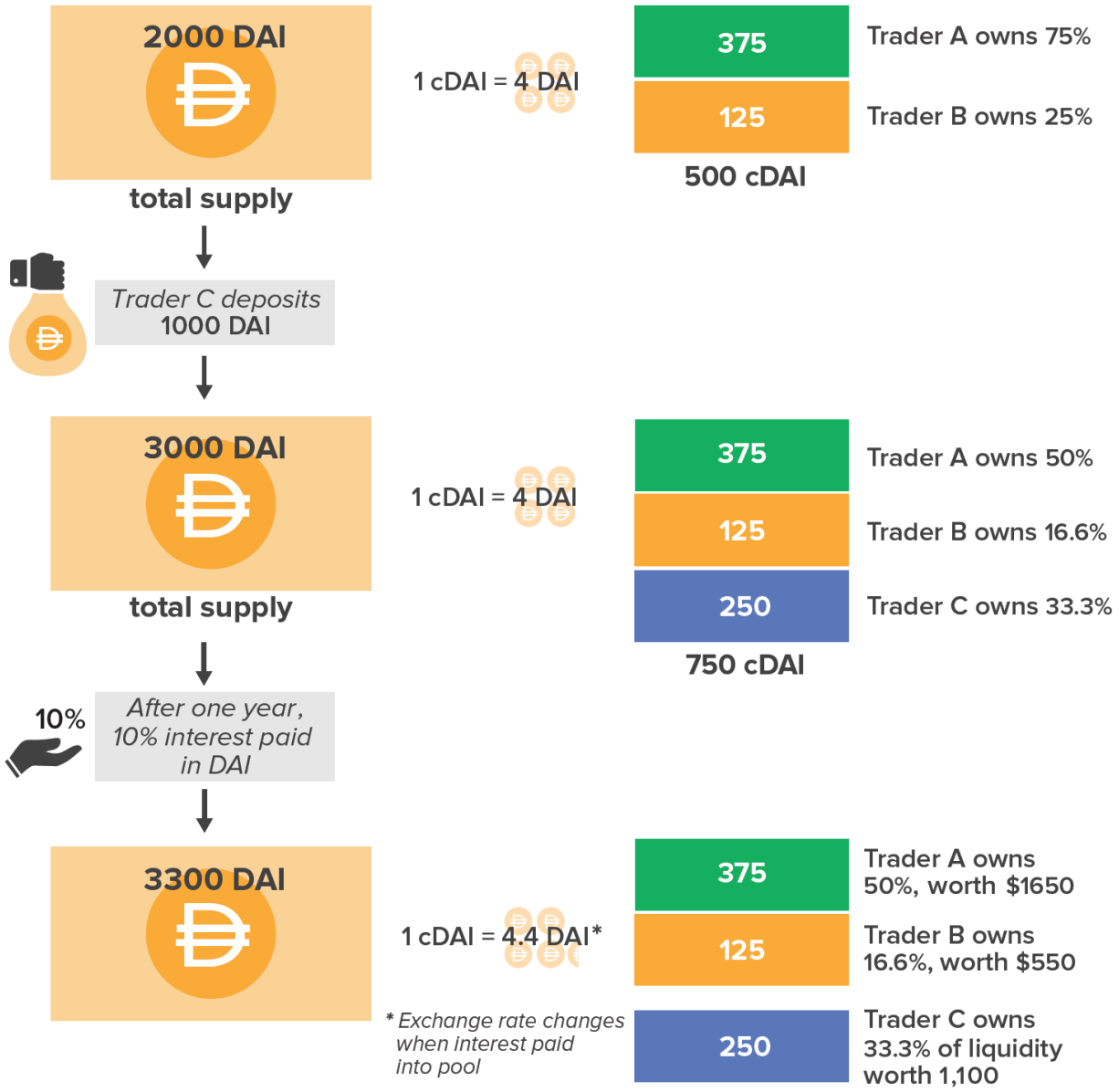
The utility of the Compound lending market is straightforward: it allows users to unlock the value of an asset without selling it and incurring a taxable event (at least under today's rules), similar to a home equity line of credit. Additionally, they can use the borrowed assets to engineer leveraged long or short positions, with competitive pooled rates and no approval process. For instance, if an investor is bearish on the price of ETH, he can simply deposit a stablecoin, such as DAI or USDC, as collateral, then borrow ETH and sell it for more of the stablecoin. If the price of ETH falls, the investor uses some of the DAI to purchase (cheaply) ETH to repay the debt. Compound offers several volatile and stable tokens to suit the risk preferences of the investor, and new tokens are continually added.

The Compound protocol must escrow tokens as a depositor in order to maintain that liquidity for the platform itself and to keep track of each person's ownership stake in each market. A naive approach would be to keep track of the number inside a contract. A better approach would be to tokenize the user's share. Compound does this using a cToken, and this is one of the platform's important innovations.

Compound's cToken is an ERC-20 in its own right that represents an ownership stake in the underlying Compound market. For example, cDAI corresponds to the Compound DAI market and cETH corresponds to the Compound ETH market. Both tokens are minted and burned in proportion to the funds added and removed from the underlying market as a means to track the amount belonging to a specific investor. Because of the interest payments that continually accrue to suppliers, these tokens are always worth more than the underlying asset. The benefit of designing the protocol in this way is that a cToken can be traded on its own like a normal ERC-20 asset. This trait allows other protocols to seamlessly integrate with Compound simply by holding cTokens and allows users to deploy their cTokens directly into other opportunities, such as using a cToken as collateral for a MakerDAO Vault. Instead of using ETH only as collateral, an investor can use cETH and earn lending interest on the ETH collateral.

For example, assume there are 2,000 DAI in the Compound DAI market and a total 500 cDAI represents the ownership in the market; this ratio of cDAI to DAI is not determinative and could just as easily be 500,000 cDAI. At that moment in time, 1 cDAI is worth 4 DAI, but after more interest accrues in the market the ratio will change. If a trader comes in and deposits 1,000 DAI, the supply increases by 50% (see Exhibit D). Therefore, the Compound protocol mints 50%, or 250, more cDAI and transfers this amount to the trader's account. Assuming an interest rate of 10%, at year end there will be 3,300 DAI, and the trader's 250 cDAI can be redeemed for one-third, or 1,100, of the DAI. The trader can deploy cDAI in the place of DAI so the DAI is not sitting idle but earning interest via the Compound pool. For example, the trader could deploy cDAI as the necessary collateral to open a perpetual futures position on dYdX or she could market make on Uniswap using a cDAI trading pair. (dYdX and Uniswap will be discussed later in the paper.)

EXHIBIT D



The many different parameters of Compound's functionality, such as the *collateral factor, reserve factor, base rate, slope,* and *kink*, can all be tuned. The entity capable of tuning these parameters is *Compound Governance*. Compound Governance has the power to change parameters, add new markets, freeze the ability to initiate new deposits or borrows in a market, and even upgrade some of the contract code itself. Importantly, Compound Governance cannot steal funds or prevent users from withdrawing. In the early stages of Compound's growth, governance was controlled by developer admins, similar to any tech startup. A strong development goal of Compound, as with most DeFi protocols, was to remove developer admin

access and release the protocol to the leadership of a DAO via a governance token. The token allowed shareholders and community members to collectively become Compound Governance and propose upgrades or parameter tuning. A quorum agreement was required for any change to be implemented.[21]

Compound implemented this new governance system in May 2020 via the COMP token. COMP is used to vote on protocol updates such as parameter tuning, adding new asset support, and functionality upgrades (similar to MKR for MakerDAO). On June 15, 2020, the 7th governance proposal passed which provided for distributing COMP tokens to users of the platform based on the borrow volume per market. The proposal offered an experience akin to a tech company giving its own stock to its users. The COMP token is distributed to both suppliers and borrowers, and acts as a subsidization of rates. With the release of the token on public markets, COMP's market cap spiked to over $2 billion. The price point of the distribution rate is so high that borrowing in most markets turned out to be profitable. This arbitrage opportunity attracted considerable volume to the platform, and the community governance has made and passed several proposals to help manage the usage.

The Compound protocol can no longer be turned off and will exist on Ethereum as long as Ethereum exists. Other platforms can easily escrow funds in Compound to provide additional value to their users or enable novel business models. An interesting example of this is PoolTogether. PoolTogether is a no-loss lottery[22] that deposits all user's funds into Compound, but pays the entire pool's earned interest to a single random depositor at fixed intervals. Easy, instant access to yield or borrow liquidity on different Ethereum tokens makes Compound an important platform in DeFi.

Traditional Finance Problem	**Compound Solution**
Centralized Control: Borrowing and lending rates are controlled by institutions.	Compound rates are determined algorithmically and give control of market parameters to COMP stakeholders incentivized to provide value to users.
Limited Access: Difficulty in accessing high-yield USD investment opportunities or competitive borrowing.	Open ability to borrow or lend any supported assets at competitive algorithmically determined rates (temporarily subsidized by COMP distribution).
Inefficiency: Suboptimal rates for borrowing and lending due to inflated costs.	Algorithmically pooled and optimized interest rates.

[21] The quorum rule for Compound is a majority of user each of whom holds with a minimum of 400,000 COMP (~4% of total eventual supply)

[22] In most lotteries, 30-50% of the lottery sales are tagged for administrative costs and government or charitable use; hence, the expected value of investing $1.00 in a lottery is $0.50-$0.70. In a no-loss lottery, all sales are paid out and the expected value is $1.00.

Lack of Interoperability: Cannot repurpose supplied positions for other investment opportunities.	Tokenized positions via cTokens can be used to turn static assets into yield-generating assets.
Opacity: Unclear collateralization of lending institutions.	Transparent collateralization ratios of borrowers visible to entire ecosystem.

6.1.3 Aave

Aave (launched in 2017) is a lending market protocol similar to Compound and offers several enhanced features. Aave offers many additional tokens to supply and borrow beyond what Compound offers. At the time of writing, Compound offers eight distinct tokens (different ERC-20 Ethereum-based assets) and Aave offers these eight plus an additional nine not offered on Compound. Importantly, the Aave lending and variable borrowing rates are more predictable, because unlike the volatile COMP token in Compound, no subsidy is involved.

The Aave protocol supports the ability to create entirely new markets. Each market consists of its own group of token pools with their corresponding supply and borrow interest rates. The benefit of creating a separate market is that the market's supported tokens act as collateral solely in that market and cannot affect other markets, thus mitigating any potential contagion.

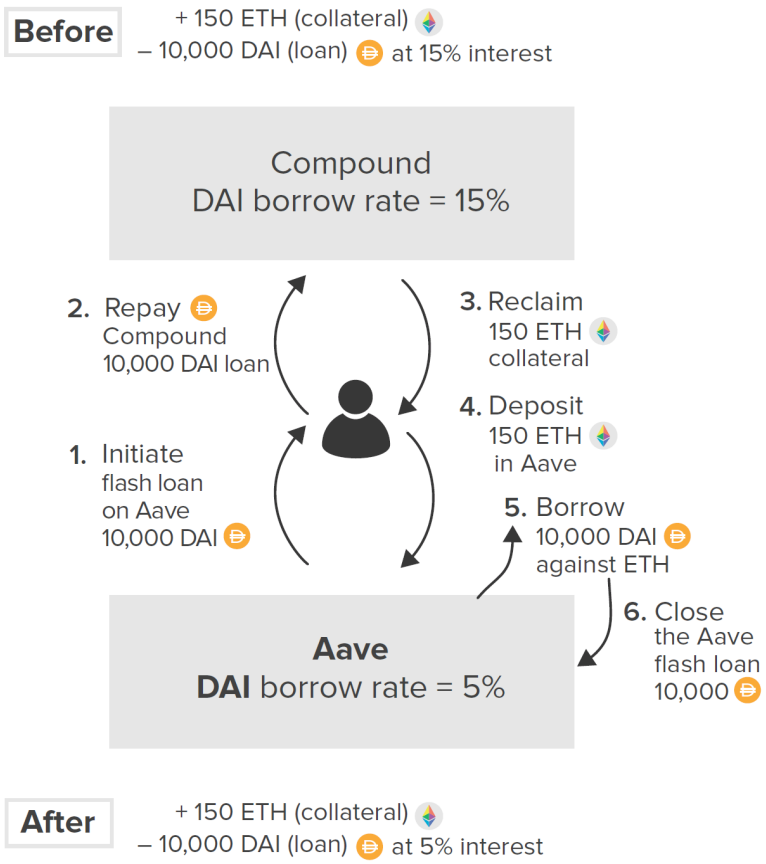
Aave currently has two main markets. The first is for more-conventional ERC-20 tokens similar to those of Compound, supporting assets such as ETH, USDC, and DAI. The second is specific to Uniswap LP tokens. For example, when a user deposits collateral into a Uniswap market, she receives an LP token that represents her ownership in the market. The LP tokens can be deposited in the Uniswap market on Aave to generate additional returns.

Aave also supports flash loans (discussed in section 5) in all of its markets and is the only source of flash liquidity for many smaller-cap tokens. Aave charges a fee of 9 basis points (bps) on the loan amount to execute a flash loan. The fee is paid to the asset pool and provides an additional return on investment to suppliers, because they each own a pro rata share of the pool. An important use case for flash loans is that they allow users quick access to capital as a means to refinance positions. This functionality is crucial to DeFi, both as general infrastructure and as a component of a positive user experience (UX).

To provide an example, assume the price of ETH is 200 DAI. A user supplies 100 ETH in Compound and borrows 10,000 DAI to lever up and purchase an additional 50 ETH, which the user also supplies to Compound. Suppose the borrow interest rate in DAI on Compound is 15% but only Aave is 5%. The goal is to refinance the borrowing to take advantage of the lower rate offered on Aave, which is analogous to refinancing a mortgage, a long and costly process in centralized finance.

One option is to manually unwind each trade on Compound and re-do both trades on Aave to reconstruct the levered position, but this option is wasteful in terms of exchange fees and gas fees. The easier action is to take out a flash loan from Aave for 10,000 DAI, use it to pay the debt on Compound, withdraw the full 150 ETH, resupply to Aave, and trigger a normal Aave borrow position (at 5% APR) against that collateral to repay the flash loan. The latter approach effectively skips the steps of exchanging ETH for DAI to unwind and rewind the leverage.

EXHIBIT G



As shown in the preceding example, a flash loan used to refinance a position allows for DeFi client applications that let users migrate a levered position from one dApp to another with the single push of a button. These applications can even optimize portfolios for APR among several competing offerings including Maker DSR (Dai Savings Rate), Compound, dYdX, and Aave.

An Aave innovation (and as of this writing only available on Aave) is a “stable” rate loan. The choice of “stable” intentionally avoids the use of “fixed rate.” A borrower has the option to switch between the variable rate and the current stable rate. The supply rate is always variable, because under certain circumstances, such as if all borrowers left the market, it would be impossible to

fund a fixed supply rate. The suppliers always collectively earn the sum of the stable and variable borrow interest payments minus any fees to the platform.

The stable rate is not a fixed rate, because the rate is adjustable in extreme liquidity crunches and can be refinanced to a lower rate if market conditions allow. Also, some constraints exist around how much liquidity can be removed at a specific stable rate. Algorithmic stable borrowing rates provide value to risk-averse investors who wish to take on leverage without the uncertainty of a variable-rate position.

Aave is developing a *Credit Delegation* feature in which users can allocate collateral to potential borrowers who can use it to borrow a desired asset. The process is unsecured and relies on trust. This process allows for uncollateralized loan relationships, such as in traditional finance, and potentially opens the floodgates in terms of sourcing liquidity. The credit delegation agreements will likely have fees and credit scores to compensate for the risk of unsecured loans. Ultimately, the delegator has sole discretion to determine who is an eligible borrower and what contract terms are sufficient. Importantly, credit delegation terms can be mediated by a smart contract. Alternatively, the delegated liquidity can be given to a smart contract, and the smart contract can use the liquidity to accomplish its intended function. The underlying benefit of credit delegation is that all loans in Aave are ultimately backed by collateral, regardless of whose collateral it is.

For example, a supplier may have a balance of 40,000 DAI in Aave earning interest. The supplier wants to increase their expected return via an unsecured delegation of their collateral to a trusted counterparty. The supplier likely knows the counterparty through an off-chain relationship, perhaps it is a banking client. The counterparty can proceed to borrow, for instance, 100 ETH with the commitment to repay the asset to the supplier plus an agreed-upon interest payment. The practical impact is that the external relationship is unsecured because no collateral is available to enforce payment; the relationship is based essentially on trust.

In summary, Aave offers several innovations beyond the lending products offered by Compound and other competitors. Aave's flash loans, although not unique among competitors, provide additional yield to investors, making them a compelling mechanism to provide liquidity. These utilities also attract to the platform arbitrageurs and other applications that require flash liquidity for their use cases. Stable borrow rates are a key innovation, and Aave is the only platform currently with this offering. This feature could be important for larger players who cannot operate under the potential volatility of variable borrow rates.

Finally, *Credit Delegation* allows users to unlock the value of supplied collateral in novel ways, including through traditional markets and contracts and even via additional layers of smart contracts that charge a premium rate to compensate for risk. Credit delegation allows loan providers to take their own collateral in the form of nonfungible Ethereum assets, perhaps tokenized art or real estate not supported by the main Aave protocol. As Aave continues to

innovate, the platform will continue to amass more liquidity and cover a wider base of potential use cases.

Traditional Finance Problem	**Aave Solution**
Centralized Control: Borrowing and lending rates controlled by institutions.	Aave interest rates are controlled algorithmically.
Limited Access: Only select groups have access to large quantities of money for arbitrage or refinancing.	Flash loans democratize access to liquidity for immediately profitable enterprises.
Inefficiency: Suboptimal rates for borrowing and lending due to inflated costs.	Algorithmically pooled and optimized interest rates.
Lack of Interoperability: Cannot monetize or utilize excess collateral in a lending position.	Credit delegation allows parties to use deposited collateral when they do not need borrowing liquidity.
Opacity: Unclear collateralization of lending institutions.	Transparent collateralization ratios of borrowers visible to the entire ecosystem.

6.2 Decentralized Exchange

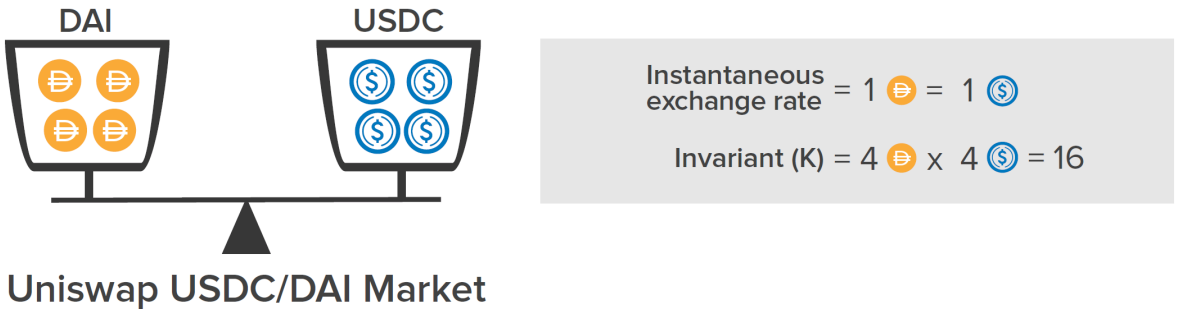
6.2.1 Uniswap

The primary example of an AMM on Ethereum is Uniswap. Currently, Uniswap uses a constant product rule to determine the trading price, using the formula $k = x*y$, where x is the balance of asset A, and y the balance of asset B. The product k is the *invariant* and is required to remain fixed at a given level of liquidity. To purchase (withdraw) some x, some y must be sold (deposited). The implied price is x/y and is the *risk-neutral* price, because the contract is equally willing to buy or sell at this rate as long as invariant k is constant.

Consider a concrete example. For simplicity, we will ignore transaction fees (gas) in all of the examples. Assume an investor in the Uniswap USDC/DAI market has 4 DAI (Asset A) and 4 USDC (Asset B). This sets the instantaneous exchange rate at 1 DAI:1 USDC and the invariant at 16 (= $x*y$). To sell 4 DAI for USDC, the investor deposits 4 DAI to the contract and withdraws 2 USDC. Now the USDC balance is $4 - 2 = 2$ and the DAI balance is $4 + 4 = 8$. The invariant remains constant at 16. Notice that the effective exchange rate is now 2 DAI: 1 USDC. The change in the exchange rate is due to slippage because of the low level of liquidity in the market. The magnitude of the invariant determines the amount of slippage. To extend the example, assume the balance is 100 DAI and 100 USDC in the contract. Now the invariant is 10,000, but

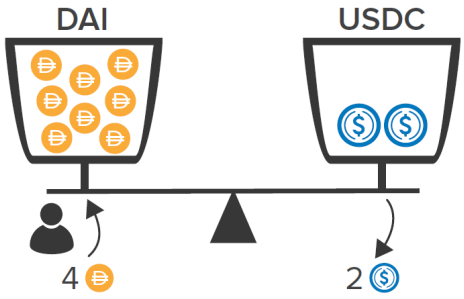
the exchange rate is the same. If the investor sells 4 DAI for USDC, now 3.85 USDC can be withdrawn to keep the invariant constant and results in much lower slippage at an effective rate of 1.04 DAI: 1 USDC.

EXHIBIT E



Scenario A

Exchange 4 DAI



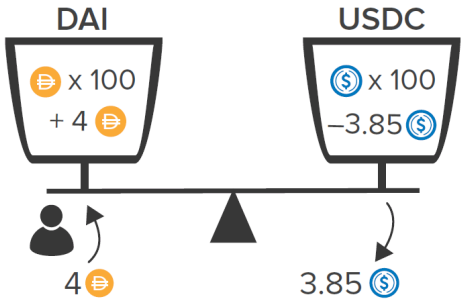
Invariant = K = 8 x 2 = 16

Hence, **4 DAI** exchanged for **2 USDC**

Scenario B

Exchange 4 DAI

but contract has more liquidity, 100 DAI, 100 USDC



Instantaneous exchange rate = 1 = 1

Before K = 100 x 100 = 10,000

After K = 104 x 96.15 = 10,000

Implied price = 1.04 = 1

Deep liquidity helps minimize slippage. Therefore, it is important that Uniswap incentivizes depositors to supply capital to a given market. Anyone can become a liquidity provider by supplying assets on both sides of a market at the current exchange rate.[23] Supplying both sides increases the product of the amount of assets held in the trading pair (i.e., increases the invariant as mentioned in the formula for the market maker). Per the preceding example, higher invariants lead to lower slippage and therefore an increase in effective liquidity. We can think of the invariant as a direct measure of liquidity. In summary, liquidity providing increases the invariant with no effect on price, whereas trading against a market impacts the price with no effect on the invariant.

Each trade in a Uniswap market has an associated 0.3% fee that is paid back into the pool. Liquidity providers earn these fees based on their pro rata contribution to the liquidity pool.

[23] A liquidity provider adds to both sides of the market, thereby increasing total market liquidity. If a user exchanges one asset for another, the total liquidity of the market as measured by the invariant does not change.

They therefore prefer high-volume markets. This mechanism of earning fees is identical to the *cToken* model of Compound. The ownership stake is represented by a similar token called a *Uni* token. For example, the token representing ownership in the DAI/ETH pool is Uni DAI/ETH.

Liquidity providers in Uniswap essentially earn passive income in proportion to the volume on the market they are supplying. Upon withdrawal, however, the exchange rate of the underlying assets will almost certainly have changed. This shift creates an opportunity-cost dynamic (*impermanent loss*) that arises because the liquidity provider could simply hold the underlying assets and profit from the price movement. The fees earned from trading volume must exceed impermanent loss in order for liquidity provision to be profitable. Consequently, stablecoin trading pairs such as USDC/DAI are attractive for liquidity providers because the high correlation of the assets minimizes the impermanent loss.

Uniswap's $k = x*y$ pricing model works well if the correlation of the underlying assets is unknown. The model calculates the exact same slippage at a given liquidity level for any two trading pairs. In practice, however, we would expect much lower slippage for a stablecoin trading pair than for an ETH trading pair, because we know by design that the stablecoin's price should be close to $1. The Uniswap pricing model leaves money on the table for arbitrageurs on high correlation pairs such as stablecoins, because it does not adjust default slippage lower (change the shape of the bonding curve), as would be expected; the profit is subtracted from the liquidity providers. For this reason, competitor AMMs, such as Curve, that specialize in high-correlation trading pairs may cannibalize liquidity in these types of Uniswap markets.

Anyone can start an ERC-20/ERC-20 or ETH/ERC-20 trading pair on Uniswap, if the pair does not already exist, by simply supplying capital on both sides.[24] The user determines the initial exchange rate, and arbitrageurs should drive that price to the true market price if it deviates at all. Users of the platform can effectively trade any two ERC-20 tokens supported by using *router contracts* that determine the most efficient path of swaps in order to get the lowest slippage, if no direct trading pair is available.

A drawback of the AMM model is that it is particularly susceptible to "front-running". This is not to be confused with illegal front-running which plagues centralized finance. One of the features of blockchain is that all transactions are public. That is, when an Ethereum user posts a transaction to the memory pool, it is publicly visible to all Ethereum nodes. Front-runners can see this transaction which is public information and post a higher gas-fee transaction to trade against the pair before the user's transaction is added to a block, and then immediately trade in the reverse direction against the pair. Estimates of front-running revenues, which come directly at the expense of the users, grew from hundreds of thousands of dollars when front-running was

[24] ETH, although fungible, is not an ERC-20. Many platforms, including Uniswap, instead use WETH, an ERC-20-wrapped version of ETH to get around this. Uniswap allows a user to directly supply and trade with ETH and it converts to WETH behind the scenes.

first publicly demonstrated in 2017[25], to hundreds of millions of dollars as of mid-2021[26]. Large transactions, especially in illiquid markets with high slippage, are particularly susceptible to front-running. For this reason, Uniswap allows users to set a maximum slippage as a clause in the transaction. If the acceptable level of slippage is exceeded, the trade will fail to execute.[27] This provides a limit to the profit front-runners can make, but does not completely remove the problem.

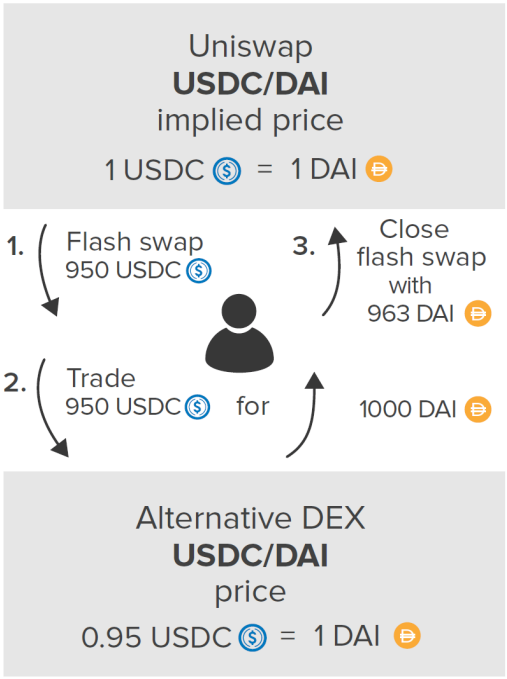
Another drawback is that arbitrage profits go only to arbitrageurs, who do not have a vested interest in the platform. The arbitrageurs profit at the expense of liquidity providers, who should not be losing the potential spread they would earn in a normal market-making scenario. Competing platforms, such as Mooniswap, propose to solve this issue by supplying virtual prices that slowly approach the true price, leaving tighter time windows and lower spreads for arbitrageurs to capitalize on. The additional spread remains in the pool for the liquidity providers.

Uniswap offers an interesting feature, similar to a flash loan, (described in Section 5) called *flash swaps*. In a flash swap, the contract sends the tokens *before* the user pays for them with assets on the other side of the pair. A flash swap unlocks many opportunities for arbitrageurs. The user can deploy this instant liquidity to acquire the other asset at a discount on another exchange before repaying it; the corresponding amount of the alternate asset must be repaid in order to maintain the invariant. This flexibility in a flash swap is different from the provision in a flash loan, which requires that repayment occur with the same asset. A key aspect of a flash swap is that all trades must take place during a single Ethereum transaction and that the trade must be closed with the corresponding amount of the complementary asset in that market.

Consider this example in the DAI/USDC market with a supply of 100,000 each. This implies a 1:1 exchange rate and an invariant of 10 billion. A trader who has no starting capital spots an arbitrage opportunity to buy DAI on a DEX for 0.95 USDC. The trader can capitalize on this arbitrage via a flash swap by withdrawing 950 USDC of flash liquidity (liquidity derived from a flash loan) from the DAI/USDC market, purchase 1,000 DAI via the described arbitrage trade, and repay 963 DAI for a profit of 37 DAI—all consummated with no initial capital. The figure of 963 is calculated as 960 (with rounding for ease of illustration) to maintain the 10 billion invariant, and to account for some slippage, plus a 0.30%*960 = 3 DAI transaction fee paid into the pool owned by the liquidity providers.

[25] https://github.com/bogatyy/bancor
[26] https://explore.flashbots.net/
[27] This is a smart contract level check. In other words, before finalizing the trade, the contract checks the total slippage from the initially posted price to the effective execution price (which could have changed if other transactions made it in first like the described front running attempt). If this slippage exceeds the pre-defined user tolerance, the entire trade is cancelled and the contract execution fails.

EXHIBIT F



4. **Slippage** = 10 DAI, so 960 DAI
Fee = .003 x 960 = 3 DAI
Swap done at 960 + 3 = 963 DAI
Profit = 1000 – 963 = 37 DAI

Lastly, an important point about Uniswap is the release of a governance token in September 2020 called UNI. Like COMP, the Compound governance token, UNI is distributed to users to incentivize liquidity in key pools including ETH/USDC and ETH/DAI. The UNI governance even has some control over its own token distribution because 43% of the supply will be vested over four years to a treasury controlled by UNI governance. Importantly, each unique Ethereum address that had used Uniswap before a certain cutoff date (over 250,000 addresses) was given 400 UNI tokens as a free airdrop. At the same time as the airdrop, UNI was released on Uniswap and the Coinbase Pro exchange for trading. The price per token opened around $3 with a total market cap of over $500 million, amounting to $1,200 of liquid value distributed directly to each user. This flood of supply could have led to selling pressure that tanked the token price. Instead, the token price spiked to over $8 before settling in the $4–5 range. Through UNI, Uniswap effectively crowdsourced capital to build and scale its business, which attained a unicorn valuation for a short time. This demonstrates the value the community places in the token and the platform, because the majority of supply is still held by those who received the airdrop.

As evidence that Uniswap is a good idea, it has been largely copied by Sushiswap. Furthermore, the CFMM has been generalized by Balancer. With Balancer, more than two markets can be supported in a liquidity pool. In addition, the assets can be arbitrarily weighted (currently, Uniswap requires equal value).[28] Further, the liquidity pool creator sets the transactions fees.

As of March 2021, the Uniswap team released a timeline and upgrade plan for the Uniswap protocol. Termed Uniswap v3, the Uniswap team proposed several changes to the protocol's liquidity provisioning model, moving away from the constant product formula described earlier and towards a model that resembles an on-chain, limit order book.[29] This change increases Uniswap's flexibility, allowing users and liquidity providers to customize curves and more actively manage their liquidity positions/control their return profiles.

Uniswap is critical infrastructure for DeFi applications; it is important to have exchanges operational whenever it is needed. Uniswap offers a unique approach for generating yield on users' assets by being a liquidity provider. The platform's flash swap functionality aids arbitrageurs in maintaining efficient markets and unlocks new use cases for users. Users can access any ERC-20 token listed, including creating completely new tokens through an IDO. As AMM volume grows on Ethereum and new platforms arise with competing models, Uniswap will continue to be a leader and an example of critical infrastructure going forward.

Traditional Finance Problem	**Uniswap Solution**
Centralized Control: Exchanges that control which trading pairs are supported.	Allows anyone to create a new trading pair if it does not already exist and automatically routes trades through the most efficient path if no direct pair exists.
Limited Access: The best investment opportunities and returns from liquidity providing are restricted to large institutions.	Anyone can become a liquidity provider and earn fees for doing so. Any project can list its token on Uniswap to give anyone access to an investor.
Inefficiency: Trades generally require two parties to clear.	An AMM that allows constant access for trading against the contract.
Lack of Interoperability: Ability to exchange assets on one exchange is not easily used	Any token swap needed for a DeFi application can utilize Uniswap as an embedded feature.

[28] The bonding surface in Balancer is given by V = PI_t=0^n B_t^W^t where V is the value function (analogous to k), n is the number of assets in the pool, B is the balance of the token t in the pool and W is the normalized weight of token t. See: https://medium.com/balancer-protocol/bonding-surfaces-balancer-protocol-ff6d3d05d577

[29] https://uniswap.org/blog/uniswap-v3/

within another financial application.	
Opacity: Unknown if the exchange truly owns all user's entire balance.	Transparent liquidity levels in the platform and algorithmic pricing.

6.3 Derivatives

6.3.1 Yield Protocol

Yield Protocol proposes a derivative model for secured, zero-coupon bonds. Essentially, the protocol defines a *yToken* to be an ERC-20 (fungible) token that settles in some fixed quantity of a target asset at a specified date. The contract will specify that the tokens, which have the same expiry, target asset, collateral asset, and collateralization ratio, are fungible. The tokens are secured by the collateral asset and have a required maintenance collateralization ratio similar to, for example, MakerDAO, as well as to other DeFi platforms we have discussed. If the collateral's value dips below the maintenance requirement, the position can be liquidated with some or all of the collateral sold to cover the debt.

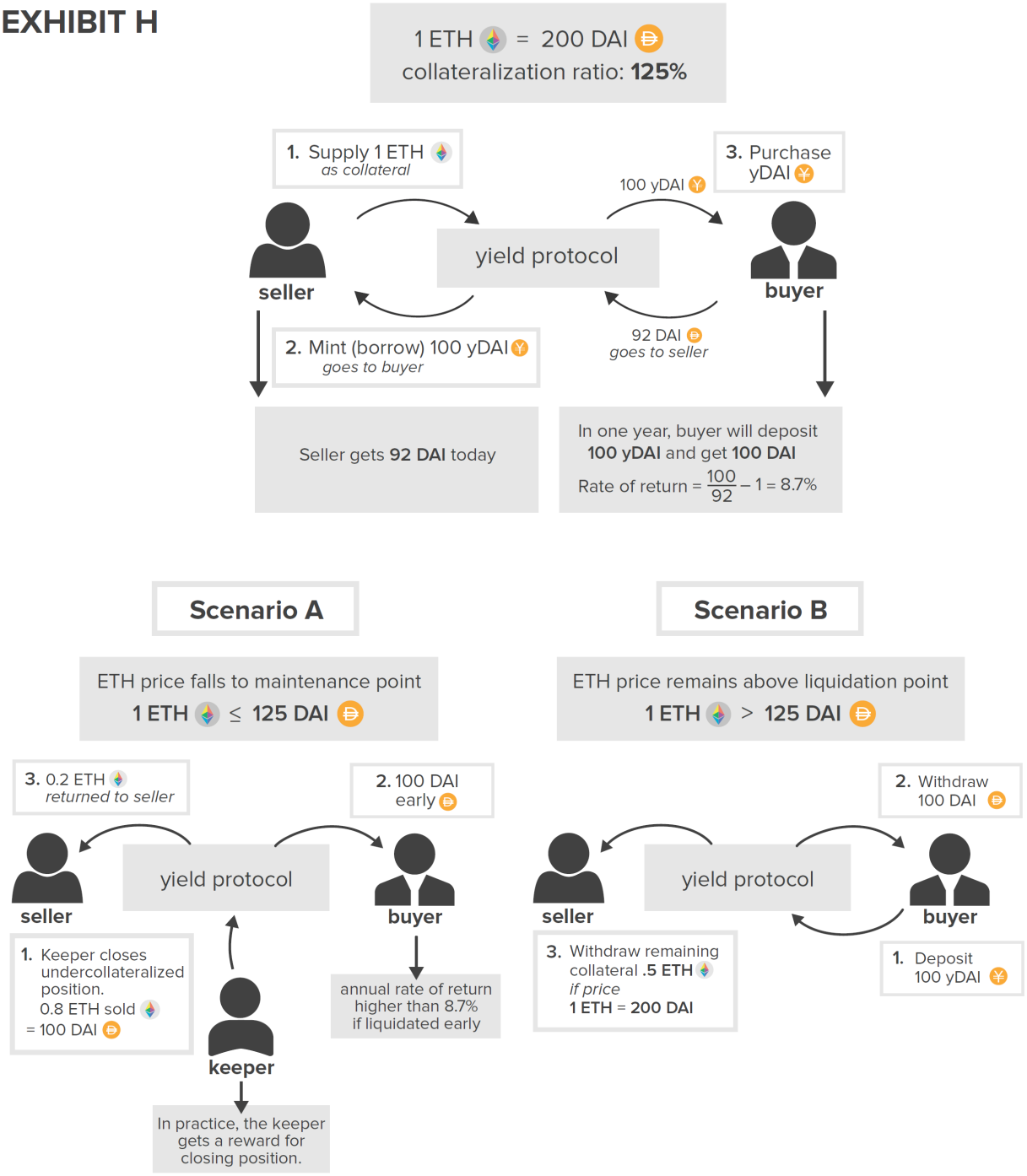
The mechanism for yToken settlement is still undecided, but one proposed solution is "cash" settlement, which means paying an equivalent amount of the collateral asset worth the specified amount of the target asset. For example, if the target asset is 1 ETH secured by 300 DAI, and at expiry 1 ETH = 200 DAI, a cash settlement would pay out 200 DAI and return the 100 DAI excess collateral to the seller of the yToken.

The other commonly proposed solution is "physical" settlement, which automatically sells collateral for the target asset upon expiry (perhaps on Uniswap) to pay out in the target asset. Using the same numbers as in the previous example, the owner of the yToken would receive 1 ETH and the seller would receive slightly less of the remaining collateral, likely around 95 DAI, after subtracting exchange fees.

The yToken effectively allows for fixed-rate borrowing and lending, using the implied return on the discounted price of the token versus the target amount.

We can illustrate as follows: assume a user has a yToken with the target asset of 1 DAI backed by ETH. The maturity date is one year ahead and the yToken is trading at 0.92 DAI. A purchase of the yToken effectively secures an 8.7% fixed interest rate, even in the case of a liquidation. In the event of a normal liquidation, the collateral would be sold to cover the position, as shown in Exhibit H.

EXHIBIT H



A compelling third option for settlement (in addition to cash and physical) is "synthetic" settlement. Here, the underlying asset is not directly repaid, but instead rolled into an equivalent amount of that asset pool on a lending platform such as Compound. Synthetic

settlement means that yDAI could settle in cDAI, converting the fixed rate into a floating rate. The buyer could close the position and redeem cDAI for DAI at her leisure. The Yield Protocol handles all of these conversions for the user so that UX simply revolves around the target asset.

In the Yield Protocol white paper, the authors discuss interesting applications from the investor's perspective. An investor can purchase yTokens to synthetically lend the target asset. The investor would be paying X amount of the asset now to purchase the yTokens. Upon settlement, the investor receives X + interest. This financial transaction in total is functionally a lend of the target asset. Note that the interest is implied in the pricing and not a directly specified value. Alternatively one can mint and sell yTokens to synthetically borrow the target asset. By selling a yToken, you are receiving X amount of the asset now (the face value) and promising to pay X + interest in the future. This financial transaction is functionally a borrow of the target asset.

Additional applications include a perpetual product on top of yTokens that maintains a portfolio of different maturities and rolls short-term profits into long-term yToken contracts. For example, the portfolio may include 3-month, 6-month, 9-month, and 1-year maturity yTokens, and once the 3-month tokens mature the smart contract can reinvest the balance into 1-year maturity yTokens. Token holders in this fund would essentially be experiencing a floating rate yield on the underlying asset with rate updates every three months.

The yTokens also allow for the construction of yield curves by analyzing the implied yields of short and longer term contracts. This can allow observers to get insights into investor sentiment among the various supported target assets.

The Yield Protocol can even be directly used to speculate on interest rates. There exist a few DAI derivative assets that represent a variable interest rate (Compound cDAI, Aave aDAI, Chai). One can imagine a seller of yDAI using one of these DAI derivative assets as collateral. The effect of this transaction is that the seller is paying the fixed rate on the yDAI while receiving the variable rate on the collateral. This is a bet that rates will increase. Likewise purchasing yDAI (of any collateral type) is a bet that variable rates will NOT increase beyond the fixed rate received.

Yield is an important protocol that supplies fixed rate products to Ethereum. It can be tightly integrated with other protocols like MakerDAO and Compound to create robust interest-bearing applications for investors. Demand for fixed income components will grow as mainstream investors begin adopting DeFi with portfolios in need of these types of assets.

Traditional Finance Problem	**Yield Solution**
Centralized Control: Fixed income instruments largely restricted to governments and large corporations.	Yield protocol is open to parties of any size.
Limited Access: Many investors have limited	Yield allows any market participant to buy or

access to buy or sell sophisticated fixed income investments.	sell a fixed income asset that settles in a target asset of their choosing.
Inefficiency: Fixed income rates are lower due to layers of fat in traditional finance.	Lean infrastructure running on Ethereum allows for more competitive rates and diverse liquidity pools due to the elimination of middlemen.
Lack of Interoperability: Fixed income instruments generally settle in cash which the investor must determine how to allocate.	yTokens can settle in any Ethereum target asset and even settle synthetically into a floating-rate lending protocol to preserve returns.
Opacity: Risk and uncertainty of counterparty in traditional agreements.	Clear collateralization publicly known on Ethereum blockchain backing the investment.

6.3.2 dYdX

dYdX is a company that specializes in margin trading and derivatives. The margin trading protocol supports USDC, DAI, and ETH. The company has a spot DEX that allows investors to exchange these assets against the current bid–ask on the order book. The DEX uses a hybrid on–off chain approach. Essentially dYdX stores *signed* or pre-approved orders without submitting to Ethereum. These orders use cryptography to guarantee they are only used to exchange funds for the desired asset at the desired price. The DEX supports limit orders and a *maximum slippage* parameter for market orders in an effort to mitigate the slippage associated with price moves or front running.

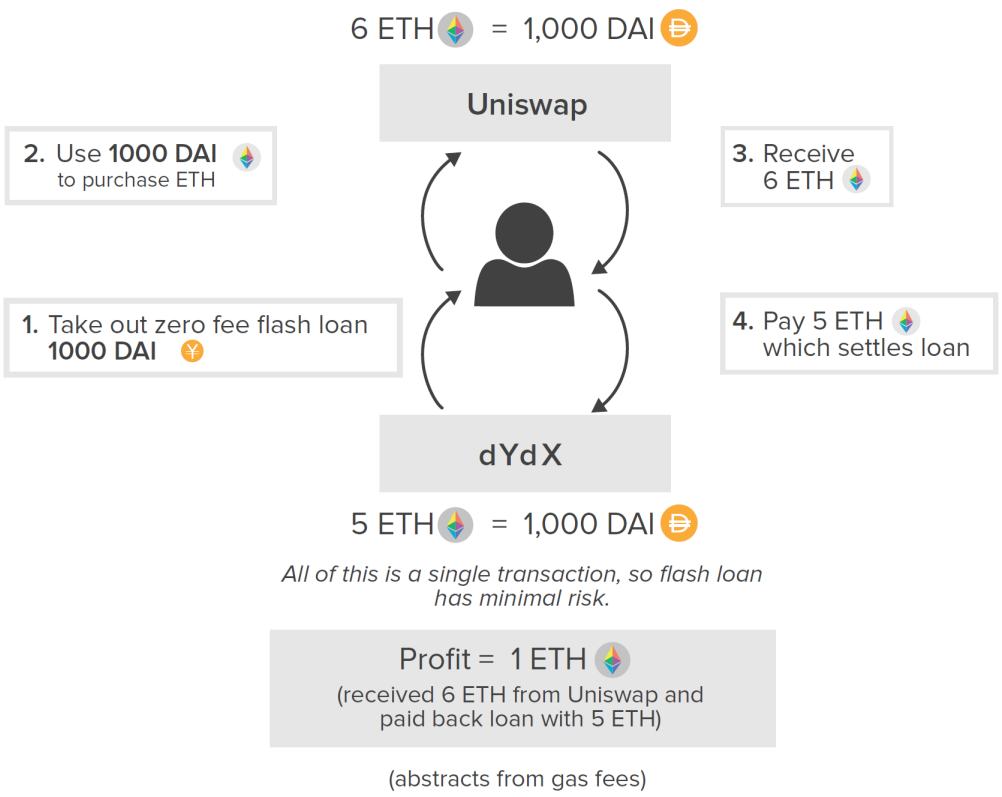
dYdX provides market makers and traders the open-source software required to interact with the DEX; alternatively, users can simply use the user interface (UI). Having dYdX do the order matching introduces a certain element of trust, because the infrastructure could be in downtime or not posting transactions for some reason. Allowing dYdX to match the orders holds little or no risk that the company could steal user funds, because the signed orders can only be used as intended per the smart contract. When the orders are matched, they are submitted to the Ethereum blockchain, where the smart contract facilitates settlement.

In addition, an investor can take a levered long or short position using margined collateral. The maximum leverage dYdX allows is 10 times. The positions can be isolated so that a single collateral deposit is used or cross-margined so that all of the investor's balances are pooled to serve as collateral. As in other protocols, dYdX has a maintenance margin requirement that if not maintained triggers liquidation of the collateral to close the position. The liquidations can be performed by external keepers who are paid to find and liquidate underwater positions, similar to the process followed by MakerDAO.

dYdX offers borrowing and lending similar to Compound and Aave. The dYdX markets also feature flash loans. Unlike Aave, the flash loans are free, so that dYdX is a popular choice for DAI, ETH, and USDC flash liquidity. In the world of open smart contracts, it makes sense that flash loans rates would be driven to zero given that they are near risk free. Lending rates are determined by the loan's duration and relative risk of default. For flash loans, repayment is algorithmically enforced and time is infinitesimal: in a single transaction, only the user can make any function calls or transfers. No other Ethereum users can move funds or make any changes while a particular user's transaction is in flight, resulting in no opportunity cost for the capital. Hence, as expected, a market participant offering free flash loans will attract more usage to their platform. Because flash loans do not require any upfront capital, they democratize access to funds for various use cases. In the Aave example, we showed how flash loans can be used to refinance a loan. We will now illustrate the use of flash loans to capitalize on an arbitrage opportunity.

Suppose the effective exchange rate for 1,000 DAI for ETH on Uniswap is 6 ETH/1,000 DAI. (The instantaneous exchange rate would be different, due to slippage.) Also, suppose the dYdX DEX has a spot ask price of 5 ETH for 1,000 DAI (i.e., the ETH are much more expensive on dYdX than Uniswap). To capitalize on this arbitrage opportunity, without any capital beyond the gas fee, an investor can execute a flash loan to borrow 1,000 DAI, exchange it on Uniswap for 6 ETH, and use 5 of those ETH to trade for 1,000 DAI on dYdX. Finally, the investor can repay the flash loan with the 1,000 DAI and pocket the 1 ETH profit. This all happens in a single transaction; multiple contract executions can happen in a single transaction on the Ethereum blockchain. See Exhibit I.

EXHIBIT I



The main derivative product dYdX offers is a BTC perpetual futures contract. Perpetual futures are a popular derivative product similar to traditional futures but without a settlement date. By entering into a perpetual futures contract, the investor is simply betting on the future price of an asset. The contract can be long or short, with or without leverage. The perpetual futures contract uses an Index Price based on the average price of the underlying asset across the major exchanges.[30] The investor deposits margin collateral and chooses a direction and amount of leverage. The contract can trade at a premium or discount to the Index Price depending on whether more traders are long or short the underlying, in this case BTC.

A funding rate, paid from one side to the other, keeps the futures price close to the Index. If the futures contract is trading at a premium to the Index, the funding rate would be positive, and longs would pay shorts. The magnitude of the funding rate is a function of the difference in price compared to the Index. Likewise, if the contract is trading at a discount, the shorts pay the long positions. The funding rate incentivizes investors to take up the opposing side from the majority in order to keep the contract price close to the Index.[31] As long as the required margin is

[30] BTC-USD Perpetual uses the MakerDAO BTCUSD Oracle V2, an oracle that reports in on-chain fashion the bitcoin prices from the cryptocurrency exchanges of Binance, Bitfinex, Bitstamp, Bittrex, Coinbase Pro, Gemini, and Kraken. See https://defiprime.com/perpetual-dydx

[31] Each protocol in DeFi can only update balances when a user interacts with the protocol. In the example of Compound, the interest rate is fixed until supply enters or leaves the pool which changes the utilization. The contract simply keeps track of the current rate and the last timestamp when the balances updated.

maintained, the investor can always close the position at the difference in the price of the notional position minus any negative balance held on margin.

Like a traditional futures contract, the perpetual futures contract has two margins: initial and maintenance. Suppose the initial margin is 10%. This means the investor needs to post collateral (or equity) worth 10% of the underlying asset. A long futures contract allows the investor to buy the asset at a set price in the future. If the market price rises, the investor can buy the asset at a price cheaper than the market price and the profit is the difference between the market price and the contract price. A short position works similarly except that the investor agrees to sell the asset at a fixed price. If the market price falls, the investor can purchase the asset in the open market and sell at the higher price stipulated in the contract. The profit is the difference between the contract price and the market price.

The risk is that the price moves against the investor. For example, if the investor is long with a 10% margin and the market price drops by 10%, the collateral is gone because the difference between purchasing at the contract price and selling in the open market (at a loss) wipes out the value of the collateral. Importantly, futures are different from options. If the underlying asset's price moves the wrong way in an option contract, the option holder can walk away: The exercise of the option is discretionary—that's why it is called an option—and no trader would exercise an option to guarantee a loss. Futures, however, are obligations. As such, traditional exchanges have mechanisms that seek to minimize the chance the contract holder does not default on a losing position.

The maintenance margin is the main tool to minimize default. Suppose the maintenance margin is 5%. On a traditional futures exchange, if the price drops by 5% the investor is required to replenish the collateral to bring it back up to 10%. If the investor fails to do this, the exchange liquidates the position. A similar mechanism exists on dYdX, but with important differences. First, if any position falls to 5%, keepers will trigger liquidation. If any collateral remains, they may keep it as a reward. Second, the liquidation is almost instantaneous. Third, no centralized exchange exists. Fourth, dYdX contracts are perpetual, whereas traditional exchange contracts usually have a fixed maturity date.

Consider the following example. Suppose the BTC price index is 10,000 USDC/BTC. An investor initiates a long position by depositing 1,000 USDC as margin (collateral), creating a levered bet on the price of BTC. If the price rises by 5%, the profit is 500. Given the investor has only deposited 1,000, the investor's rate of return is 50%, or (1,000 – 500)/1,000.

We can also think about the mechanics another way. Taking a long position at 10,000, the investor is committing to buying at 10,000 and the obligation is 10,000. Think of the obligation as a "negative balance" because the investor must pay 10,000 according to the contract. The

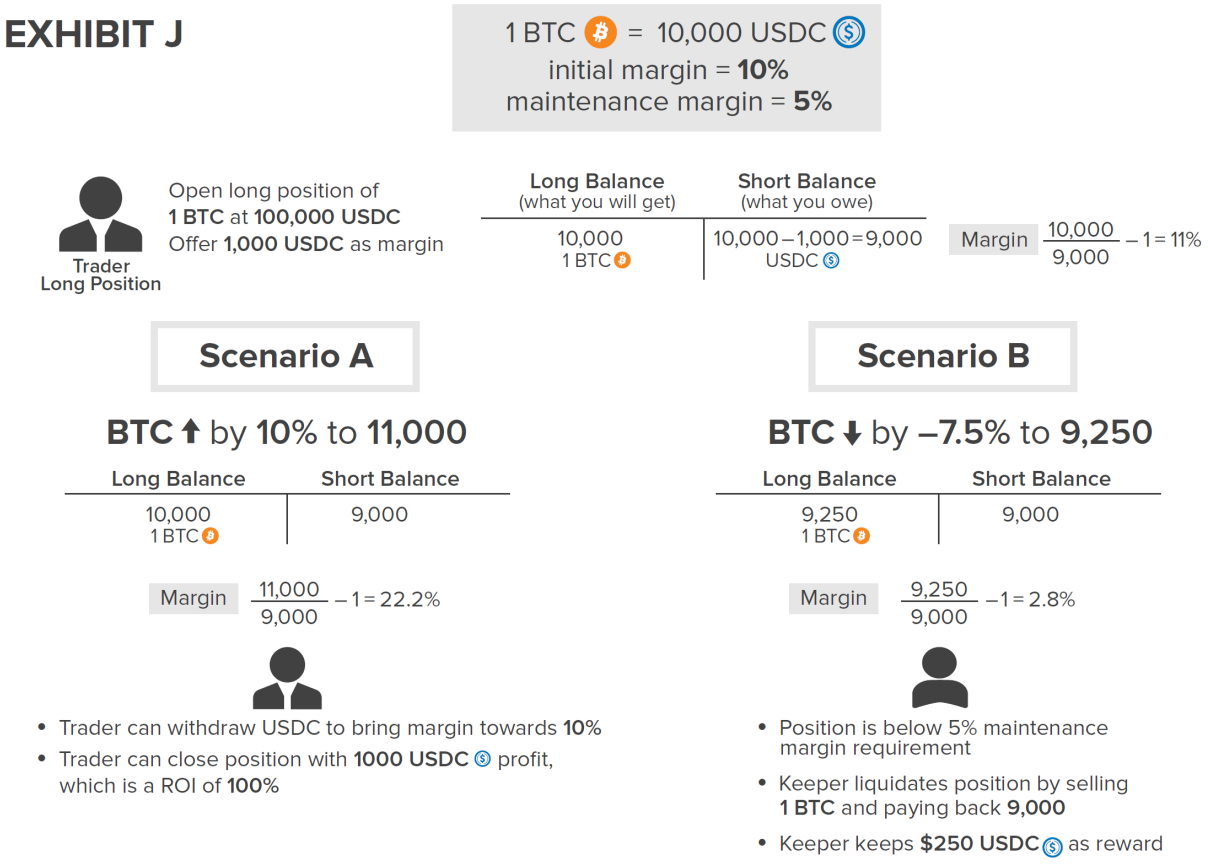
---

When a new user borrows or supplies, that transaction updates the rates for the entire market. Similarly, whereas the dYdX's Funding Rate is updated every second, it is only applied at the time a user opens, closes, or edits a position. The contract calculates the new values based on what the rates were and how long the futures position has been open.

investor has already committed collateral of 1,000 and owes 9,000. On the other side, the investor has committed those funds to purchase an asset, 1 BTC. The investor thus has a positive balance of 10,000, the current price. The collateralization ratio is 10,000/9,000 = 111%, which is a margin percentage of 11% and is nearly the maximum amount of allowed leverage (10% margin).

This intuition works similarly for a short position. The investor has committed to sell at 10,000, which is a positive balance and is supplemented by the margin deposit of 1,000 (so total of 11,000). The investor's negative balance is the obligation to buy 1 BTC, currently worth 10,000. The collateralization ratio is 11,000/10,000, which corresponds to a margin of 10%.

Let's now follow the mechanics of a short position when the underlying asset (BTC) increases in value by 5%. If the price of BTC increases to 10,500 (a 5% increase), the margin percentage becomes (11,000/10,500) – 1 = 4.76% and the short position becomes subject to liquidation. The paper net balance of the position is $500, the incentive for the liquidator to close the position collect the balance. Exhibit J reviews the mechanics of a long position.



The dYdX BTC perpetual futures contract allows investors to access BTC returns natively on the Ethereum blockchain, while being able to supply any ERC-20 asset as collateral. Perpetual

futures are rising in popularity, and this functionality may continue to attract liquidity over time.

Traditional Finance Problem	**dYdX Solution**
Centralized Control: Borrowing and lending rates controlled by institutions.	dYdX rates are determined algorithmically based on clearly outlined, transparent formulas (often asset pool utilization rates).
Limited Access: Difficulty in accessing high yield USD investment opportunities or competitive borrowing as well as futures and derivative products. Access to capital for immediately profitable enterprises is limited.	Open ability to borrow or lend any supported assets at competitive algorithmically determined rates. Includes a perpetual futures contract that could synthetically support any asset. Free flash loans give developers access to large amounts of capital to capitalize on arbitrage or other profitable opportunities.
Inefficiency: Suboptimal rates for borrowing and lending due to inflated costs.	Algorithmically pooled and optimized interest rates. Free flash loans offered for immediate use cases.
Lack of Interoperability: Difficult to repurpose funds within a financial instrument.	Flash loans can immediately utilize the entirety of the AUM for outside opportunities without risk or loss to investors.
Opacity: Unclear collateralization of lending institutions.	Transparent collateralization ratios of borrowers are visible to the entire ecosystem.

6.3.3 Synthetix

Many traditional derivative products have a decentralized counterpart. DeFi, however, allows new types of derivatives because of smart contracts. Synthetix is developing such a new type of derivative.

Imagine creating a derivative cryptoasset, whose value is based on an underlying asset that is neither owned nor escrowed. Synthetix is one group whose primary focus is creating a wide variety of liquid synthetic derivatives. Its model is, at a high level, straightforward and novel. The company issues *Synths*, tokens whose prices are pegged to an underlying price feed and are backed by collateral. MakerDAO's DAI is also a synthetic asset. The price feeds come from the Chainlink's decentralized oracles.[32] Synths can theoretically track any asset, long or short, and

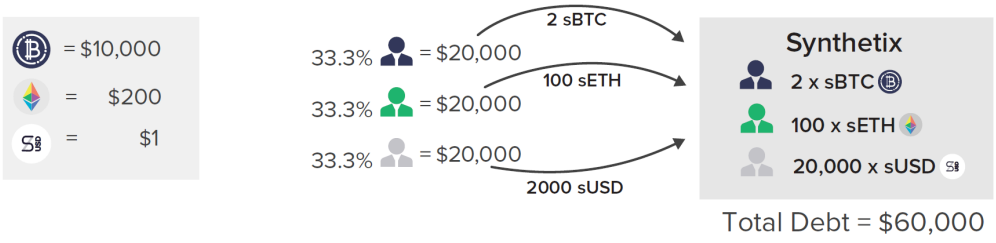
[32] See https://blog.synthetix.io/all-synths-are-now-powered-by-chainlink-decentralised-oracles/

even levered positions. In practice, there is no leverage, and the main tracked assets are cryptocurrencies, fiat currencies, and gold.

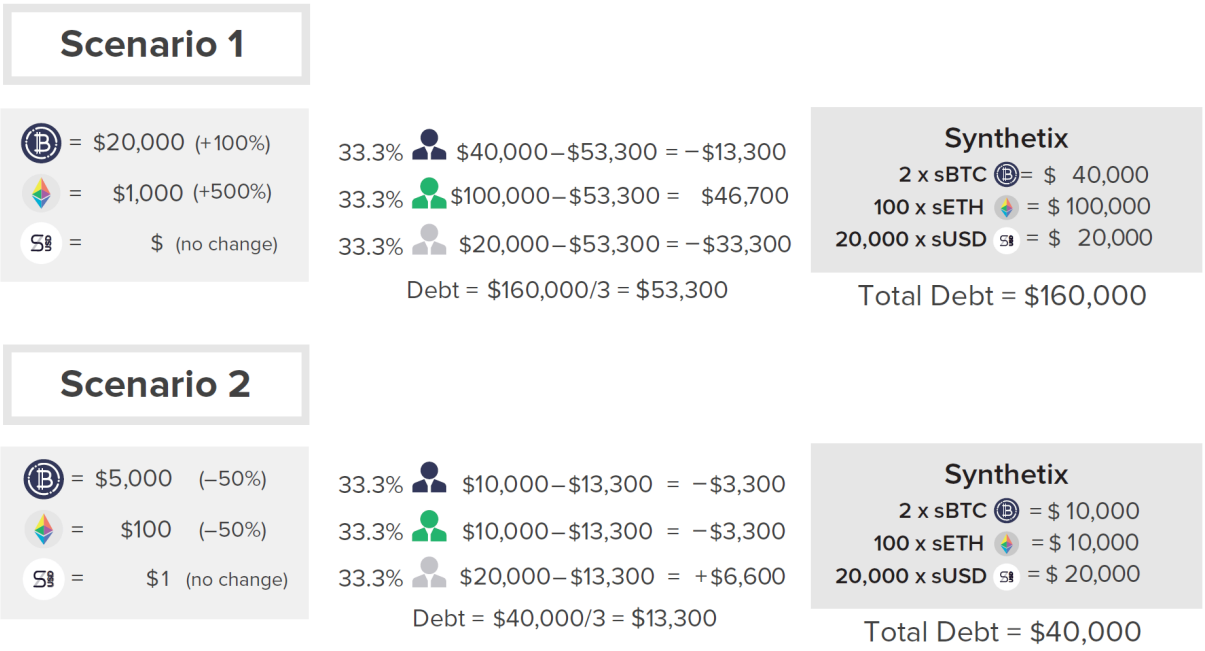
A long Synth is called an *sToken*, for example, a sUSD or a sBTC. The sUSD is a synthetic because its value is based on a price feed. A short Synth is called an *iToken*, for example, an iETH or an iMKR. Synthetix also has a platform token called SNX. SNX is not a governance token like MKR and COMP, but is a *utility token* or a *network token*, which means it enables the use of Synthetix functionality as its only feature. SNX serves as the unique collateral asset for the entire system. When users mint Synths against their SNX, they incur a debt proportioned to the total outstanding debt denominated in USD. They become *responsible* for this percentage of the debt in the sense that to unlock their SNX collateral they need to return the total USD value of their debt. The global debt of all Synths is thus shared collectively by the Synth holders based on the USD-denominated percentage of the debt they owned when they opened their positions. The total outstanding USD-denominated debt changes when any Synth's price fluctuates, and each holder remains responsible for the same percentage they were responsible for when they minted their Synths. Therefore, when a SNX holder's Synths outperform the collective pool, the holder effectively profits, and vice versa, because their asset value (their Synth position) outpaced the growth of the debt (sum of all sUSD debt).

As an example, three traders each have $20,000 for a total debt of $60,000: one holds 2 sBTC priced at $10,000 each, one holds 100 sETH priced at $200 each, and one holds 20,000 sUSD priced at $1 each. Each has a debt proportion of 33.3%. If the price of BTC doubles to $20,000 and the price of ETH spikes to $1,000, the total debt becomes $160,000 = $40,000 (sBTC) + $100,000 (sETH) + $20,000 (sUSD).[33] Because each trader is responsible for 33.3%, about $53,300, only the sETH holder is profitable even though the price of BTC doubled. If the price of BTC falls to $5,000 and ETH to $100, then the total debt falls to $40,000 and the sUSD holder becomes the only profiting trader. Exhibit K details this example.

EXHIBIT K



[33] In any Synthetix position, the trader is effectively "long" his personal portfolio against the entire pool's portfolio. In other words, the trader is betting his returns will exceed the pool's returns. For example, by holding sUSD only, the trader is effectively shorting the entire composition of all other traders' Synthetix portfolios and betting that USD will outperform all other assets held. The trader's goal is to own Synths that he thinks will outperform the rest of the market, because it is the only way to profit.



The platform has a native DEX that will exchange any two Synths at the rate quoted by the oracle. Traders pay the exchange fees to a fee pool redeemable by SNX holders in proportion to their percentage of the debt. The contracts enforce that SNX holders can only redeem their fees if they maintain a sufficient collateralization ratio relative to their portion of the debt. The required collateralization ratio to mint Synths and participate in staking rewards is high, currently 800%. The Synthetix protocol also mints new SNX tokens via inflation to reward various stakeholders in the ecosystem for contributing value. The protocol distributes the rewards as a bonus incentive for maintaining a high collateralization ratio or increasing the liquidity of SNX.

Synthetix has branched into products that track real-world equities with the release of sNIKKEI and sFTSE. The protocol is also beginning to offer a binary options trading interface, further expanding its capabilities. The platform could easily gain popularity because there is no slippage against the price feed, however, the pooled liquidity and shared debt models offer interesting challenges.

Traditional Finance Problem	**Synthetix Solution**
Centralized Control: Assets can generally only be bought and sold on registered exchanges.	Offer synthetic assets in one place that can track any real world asset.
Limited Access: Access to certain assets is geographically limited.	Anyone can access Synthetix to buy and sell Synths. Some restrictions may eventually apply to thoses Synths that are securities.

Inefficiency: Large asset purchases suffer from slippage as traders eat into the liquidity pool.	Synths exchange rates are backed by a price feed, which eliminates slippage.
Lack of Interoperability: Real-world assets such as stocks can't be easily represented directly on a blockchain	Synth representations of real assets are totally compatible with Ethereum and other DeFi protocols.
Opacity: Lack of transparency in traditional derivative markets.	All protocol-based projects and features are transparently funded and voted upon by a DAO

6.4 Tokenization

Tokenization refers to the process of taking some asset or bundle of assets, either on or off chain, and

1. representing that asset on chain with possible fractional ownership, or
2. creating a composite token that holds some number of underlying tokens.

A token can conform to different specifications based on the type of properties a user wants the token to have. As mentioned earlier, the most popular token standard is ERC-20, the fungible token standard. This interface defines abstractly how a token, which has units that are non-unique and interchangeable (such as USD), should behave. An alternative is the ERC-721 standard, which defines nonfungible tokens (NFTs). These tokens are unique, such as a token representing ownership of a piece of fine art or a specific digital asset from a game. DeFi applications can take advantage of these and other standards to support any token using the standard simply by coding for the single standard.

6.4.1 Set Protocol

Set Protocol offers the "composite token" approach to tokenization. Instead of tokenizing assets non-native to Ethereum, Set Protocol combines Ethereum tokens into composite tokens that function more like traditional exchange traded funds (ETFs). Set Protocol combines cryptoassets into *Sets*, which are themselves ERC-20 tokens and fully collateralized by the components escrowed in a smart contract. A Set token is always redeemable for its components. Sets can be static or dynamic, based on a trading strategy. Static Sets are straightforward to understand and are simply bundled tokens the investor cares about; the resulting Set can be transferred as a single unit.

Dynamic Sets define a trading strategy that determines when reallocations can be made and at what times. Some examples include the "Moving Average" Sets that shift between 100% ETH

and 100% USDC whenever ETH crosses its X-day simple or exponentially weighted moving average. Similar to normal ETFs, these Set tokens have fees and sometimes performance-related incentives. At the Set's creation, the manager pre-programs the fees, which are paid directly to the manager for that particular Set. The available fee options are a buy fee (front-end load fee), a streaming fee (management fee), and a performance fee (percentage of profits over a high-water mark). The Set Protocol currently takes no fee for itself, although it may add a fee in the future. The prices and returns for Set Protocol are calculated via MakerDAOs' publicly available oracle price feeds, which are also used by Synthetix. The main value-add of dynamic Sets is that the trading strategies are publicly encoded in a smart contract so users know exactly how their funds are being allocated and can easily redeem at any time.

Set Protocol also has a *Social Trading* feature in which a user can purchase a Set whose portfolio is restricted to certain assets with reallocations controlled by a single trader. Because these portfolios are actively managed, they function much more like mutual funds. The benefits are similar in that the portfolio manager has a predefined set of assets to choose from, and the users benefit from this contract-enforced transparency.

For example, a portfolio manager for a Set has a goal to "buy low and sell high" on ETH. The only assets she can use are ETH and USDC, and the only allocations she is allowed are 100% ETH and 100% USDC. At her sole discretion, she can trigger a contract function to rebalance the portfolio entirely into one asset or the other; this is the only allocation decision she can make. Assume she starts with 1,000 USDC. The price of ETH dips to 100 USDC/ETH and she decides to buy. She can trigger a rebalance to have 10 ETH in the Set. If the price of ETH doubles to $200, the entire Set is now worth $2,000. A shareholder who owns 10% of the Set can redeem her shares for 1 ETH.

Sets could democratize wealth management in the future by being more peer to peer, allowing fund managers to gain investment exposures through nontraditional channels and giving all investors access to the best managers. A further enhancement many Sets take advantage of is that their components use cTokens, the Compound-invested version of tokens. Between rebalances, tokens earn interest through the Compound protocol. This is one example of DeFi platforms being composed to create new products and value for investors.

Traditional Finance Problem	**Set Protocol Solution**
Centralized Control: Fund managers can control their funds against the will of investors.	Enforces sovereignty of the investor over their funds at the smart contract level.
Limited Access: Talented fund managers often are unable to gain exposures and capital to run a successful fund.	Allows anyone to become a fund manager and display their skills using social trading features.

Inefficiency: Many arising from antiquated practices.	Trading strategies encoded in smart contracts lead to optimal execution.
Lack of Interoperability: Difficult to combine assets into new packages and incorporate the combined assets into new financial products.	Set tokens are ERC-20 compliant tokens that can be used on their own in other DeFi protocols. For example, Aave allows Set token borrowing and lending for some popular Sets.
Opacity: Difficult to know the breakdown of assets in an ETF or mutual fund at any given time.	Total transparency into strategies and allocations of Set tokens.

6.4.2 wBTC

The wBTC application takes the *representing off-chain assets on chain* approach to tokenization, specifically for BTC. Abstractly, wBTC allows BTC to be included as collateral or liquidity on all of the Ethereum-native DeFi platforms. Given that BTC has comparatively low volatility and is the most well-adopted cryptocurrency by market-cap, this characteristic unlocks a large potential capital pool for DeFi dApps.

The wBTC ecosystem contains three key stakeholders: users, merchants, and custodians. Users are simply the traders and DeFi participants who generate demand for the value proposition associated with wBTC, namely, Ethereum-tokenized BTC. Users can purchase wBTC from merchants by transferring BTC and performing the requisite KYC/AML, thus making the entry and exit points of wBTC centralized and reliant on off-chain trust and infrastructure. Merchants are responsible for transferring BTC to the custodians. At the point of transfer, the merchant signals to an on-chain Ethereum smart contract that the custodian has taken custody of the BTC and is approved to mint wBTC. Custodians use industry-standard security mechanisms to custody the BTC until it is withdrawn from the wBTC ecosystem. Once the custodians have confirmed receipt, they can trigger the minting of wBTC that releases wBTC to the merchant. Finally, closing the loop, the merchant transfers the wBTC to the user.

No single participant can control the minting and burning of wBTC, and all BTC entering the system is audited via transaction receipts that verify custody of on-chain funds. These safeguards increase the system's transparency and reduce the risk to users that is inherent in the system. Because the network consists of merchants and custodians, any fraud is quickly expungeable from the network at only a small overall cost versus the cost that would be incurred in a single centralized entity. The mechanism by which merchants and custodians enter and leave the network is a multi-signature wallet controlled by the wBTC DAO. In this case, the DAO does not have a governance token; instead, a set of owners who can add and remove owners controls the DAO. The contract currently allows a maximum of 50 owners, with a minimum threshold of 11 to invoke a change. The numbers 50 and 11 can be changed, if a number of conditions are met. This system is more centralized than other governance mechanisms we have

discussed, but is still more decentralized than allowing a single custodian to control all of the wBTC.

7. Risks

As we have emphasized in previous sections, DeFi allows developers to create new types of financial products and services, expanding the possibilities of financial technology. While DeFi can eliminate counterparty risk, cutting out middlemen and allowing financial assets to be exchanged in a trustless way, as with any innovative technology, the innovations introduce a new set of risks. In order to provide users and institutions with a robust and fault-tolerant system capable of handling new financial applications at scale, we must confront these risks. Without proper risk mitigation, DeFi will remain an exploratory technology, restricting its use, adoption, and appeal.

The principal risks DeFi faces today are smart contract, governance, oracle, scaling, exchange, custodial and regulatory risks.

7.1 Smart-Contract Risk

Over the past decade, crypto-focused products, primarily exchanges, have repeatedly been hacked. Whereas many of these hacks happened because of poor security practices, they demonstrate an important point: software is uniquely vulnerable to hacks and developer malpractice. Blockchains can remove traditional financial risks, such as counterparty risk, with their unique properties, but DeFi is built on code. This software foundation gives attackers a larger attack surface than the threat vectors of traditional financial institutions. As we discussed previously, public blockchains are open systems. Anyone can view and interact with code on a blockchain after the code is deployed. Given that this code is often responsible for storing and transferring blockchain native financial assets, it introduces a new, unique risk. This new attack vector is termed *smart contract risk*.

So what does smart contract risk mean?

DeFi's foundation is public computer code known as a smart contract. While the concept of a smart contract was first introduced by Nick Szabo in his 1997 paper, the implementation is new to mainstream engineering practice. Therefore, formal engineering practices that will help reduce the risk of smart contract bugs and programming errors are still under development. The recent hacks of DForce and bZx[34] demonstrate the fragility of smart contract programming, and auditing firms, such as Quantstamp, Trail of Bits, and Peckshield, are emerging to fill this gap in best practices and smart contract expertise.

[34] See https://cointelegraph.com/news/dforce-hacker-returns-stolen-money-as-criticism-of-the-project-continues and https://cointelegraph.com/news/decentralized-lending-protocol-bzx-hacked-twice-in-a-matter-of-days

Smart Contract risk can take the form of a logic error in the code or an economic exploit in which an attacker can withdraw funds from the platform beyond the intended functionality. The former can take the form of any typical software bug in the code. For example, let's say we have a smart contract which is intended to be able to escrow deposits from a particular ERC-20 from any user and transfer the entire balance to the winner of a lottery. The contract keeps track of how many tokens it has internally, and uses that internal number as the amount when performing the transfer. The bug will belong here in our hypothetical contract. The internal number will, due to a rounding error, be slightly higher than the actual balance of tokens the contract holds. When it tries to transfer, it will transfer "too much" and the execution will fail. If there was no failsafe put into place, the tokens are functionally locked within the protocol. Informally these are known as "bricked" funds and cannot be recovered.

An economic exploit would be more subtle. There would be no explicit failure in the logic of the code, but rather an opportunity for an economically equipped adversary to influence market conditions in such a way as to profit inappropriately at the contract's expense. For example, let's assume a contract takes the role of an exchange between two tokens. It determines the price by looking at the exchange rate of another similar contract elsewhere on chain and offering that rate with a minor adjustment. We note here that the other exchange is playing the role of a price oracle for this particular contract. The possibility for an economic exploit arises when the oracle exchange has significantly lower liquidity when compared to the primary exchange in our example. A financially equipped adversary can sell heavily on the oracle exchange to manipulate the price, then proceed to purchase far more on the primary exchange to capitalize on the price movement. The net effect is that the attacker was able to manufacture a discounted price on a high liquidity exchange by manipulating a low liquidity oracle.

Economic exploits become even trickier when considering that flash loans essentially allow any Ethereum user to become financially equipped for a single transaction. Special care must be used when designing protocols such that they cannot be manipulated by massive market volatility within a single transaction. An economic exploit which utilizes a flash loan can be referred to as a *flash attack*. A series of high profile flash attacks were executed in Feb 2020 on bZx Fulcrum, a lending market similar to Compound.[35] The attacker utilized a flash loan and diverted some of the funds to purchase a levered short position, with the remainder used to manipulate the price of the oracle exchange which the short position was based on. The attacker then closed the short at a profit, unwound the market trade and paid back the flash loan. The net profit was almost $300,000 worth of funds previously held by bZx, for near zero upfront cost.

The most famous smart contract attack occurred in 2016. A smart contract was designed by Slock.it to act as the first decentralized venture capital fund for blockchain ventures. It was launched in April 2016[36] and attracted about 14% of all the ether available at the time. The DAO tokens began trading in May. However, there was a crucial part of the code with two lines in the

[35] https://bzx.network/blog/postmortem-ethdenver
[36] Ethereum block 1428757.

wrong order allowing the withdrawal of ether repeatedly - before checking to see if the hacker was entitled to withdraw. This flaw is known as the reentrancy bug. On June 17, a hacker drained 30% of the value of the contract before another group, the Robin Hood Group, drained the other 70%. The Robin Hood Group promised to return all the ether to the original owners.

The original contract had a 28-day hold period before the funds could be withdrawn. The Ethereum community debated whether they should rewrite history by creating a hard fork (which would eliminate the hack). In the end, they decided to do the hard fork and returned the ether to the original investors. The old protocol became Ethereum Classic (ETC) which preserved the immutable record. The initiative halted in July when the SEC declared that DAO tokens were securities.

There have been many exploits like this. In April 2020, hackers exploited $25m from dForce's Lendf.Me lending protocol. Interestingly, the Lendf.Me code was largely copied from Compound. Indeed, the word "Compound" appears four times in dForce's contract. The CEO of Compound remarked: "If a project doesn't have the expertise to develop its own smart contracts, … it's a sign that they don't have the capacity or intention to consider security."[37]

A smaller but fascinating attack occurred in February 2021 and the target was Yearn.finance.[38] Yearn is a yield aggregator. Users deposit funds into pools and these funds are allocated to other DeFi protocols to maximize the yield for the original investors. The transaction included 161 token transfers using Compound, dYdX, Aave, Uniswap and cost over $5,000 in gas fees.[39] It involved flash loans of over $200m.

Smart-contract programming still has a long way to go before best practices are developed and complex smart-contracts have the resilience necessary to handle high-value transactions. As long as smart-contract risk threatens the DeFi landscape, application adoption and trust will suffer as users hesitate to trust the contracts they interact with and that custody their funds.

7.2 Governance Risk

Programming risks are nothing new. In fact, they have been around since the dawn of modern computing more than half a century ago. For some protocols, such as Uniswap, programming risk is the sole threat to the protocol because the application is autonomous and controlled by smart contracts. Other DeFi applications rely on more than just autonomous computer code. For example, MakerDAO, the decentralized credit facility described earlier, is reliant on a human-controlled governance process that actively adjusts protocol parameters to keep the system solvent. Many other DeFi protocols use similar systems and rely on humans to actively

[37] https://decrypt.co/26033/dforce-lendfme-defi-hack-25m
[38] https://www.theblockcrypto.com/linked/93818/yearn-finance-dai-pool-defi-exploit-attack
[39] https://etherscan.io/tx/0x6dc268706818d1e6503739950abc5ba2211fc6b451e54244da7b1e226b12e027

manage protocol risk. This introduces a new risk, *governance risk*, which is unique to the DeFi landscape.

Protocol governance refers to the representative or liquid democratic mechanisms that enable changes in the protocol.[40] To participate in the governance process, users and investors must acquire a token that has been explicitly assigned protocol governance rights on a liquid marketplace. Once acquired, holders use these tokens to vote on protocol changes and guide future direction. Governance tokens usually have a fixed supply that assists in resisting attempts by anyone to acquire a majority (51%), nevertheless they expose the protocol to the risk of control by a malicious actor. New projects like Automata[41] allow users to buy governance votes directly, and will likely accelerate the threat of malicious/hostile governance.

In traditional companies, activist investors can buy shares and vote to tilt the company's direction as they desire. DeFi protocols with governance tokens are similar, except governance systems are launched much earlier into a protocol's life, which can create greater risks. Furthermore, in traditional companies, even activist investors are bound by a legally-enforceable fiduciary "duty of loyalty" to minority shareholders, whereas in DeFi this does not exist.

On March 13, 2021 there was a governance attack on True Seigniorage Dollar. In this particular situation, the developers controlled only 9% of the DAO. The attacker gradually bought $TSD until he had 33% of the DAO. The hacker then proposed an implementation and voted for it. The attacker added code to mint himself 11.5 quintillion $TSD and then sold 11.8b $TSD tokens on Pancakeswap.[42]

7.3 Oracle Risk

Oracles are one of the last unsolved problems in DeFi and are required by most DeFi protocols in order to function correctly. Fundamentally, oracles aim to answer the simple question: How can off-chain data be securely reported on chain? Without oracles, blockchains are completely self-encapsulated and have no knowledge of the outside world other than the transactions added to the native blockchain. Many DeFi protocols require access to secure, tamper-resistant asset prices to ensure that routine actions, such as liquidations and prediction market resolutions, function correctly. Protocol reliance on these data feeds introduces *oracle risk*.

Oracles represent significant risks to the systems they help support. If an oracle's *Cost of Corruption* is ever less than an attacker's potential *Profit from Corruption*, the oracle is extremely vulnerable to attack.

[40] https://medium.com/dragonfly-research/decentralized-governance-innovation-or-imitation-ad872f37b1ea
[41] https://automata.fi/
[42] https://twitter.com/trueseigniorage/status/1370956726489415683?lang=en

To date, three types of oracle solutions have been introduced, developed, and used. The first is a *Schelling-point oracle*. This oracle relies on the owners of a fixed-supply token to vote on the outcome of an event or report the price of an asset. Examples of this type of oracle include Augur and UMA. While Schelling-point oracles preserve the decentralization components of protocols that rely on them, they suffer from slow times to resolution.

The second type of oracle solution an *API oracle*. These oracles are centralized entities that respond asynchronously to requests for data or prices. Examples include Provable, Oraclize, and Chainlink. All systems relying on API-based oracles, must trust the data provider to respond accurately to all queries.

The third type of oracle is a custom, application-specific oracle service. This type of oracle is used by Maker and Compound. Its design differs based on the requirements of the protocol it was developed for. For example, Compound relies on a single data provider that the Compound team controls to provide all on-chain price data to the Compound oracle.

Oracles, as they exist today, represent the highest risk to DeFi protocols that rely on them. All on-chain oracles are vulnerable to front-running, and millions of dollars have been lost due to arbitrageurs. Additionally, oracle services, including Chainlink and Maker, have suffered crippling outages with catastrophic downstream effects.

Until oracles are blockchain native, hardened, and proven resilient, they represent the largest systemic threat to DeFi today.

7.4 Scaling Risk

As we have discussed, Ethereum and other "Proof of Work" (the consensus mechanism) blockchains have a fixed block size. For a block to become part of the chain, every Ethereum miner must execute all of the included transactions on their machine. To expect each miner to process all of the financial transactions for a global financial market is unrealistic. Ethereum is currently limited to a maximum of 15 TPS. Yet, almost all of DeFi today resides on this blockchain. Compared to Visa, which can handle upward of 65,000 transactions per second, Ethereum is capable of handling less than 0.1% of the throughput. Ethereum's lack of scalability places DeFi at risk of being unable to meet requisite demand. Much effort is focused on increasing Ethereum's scalability or replacing Ethereum with an alternative blockchain that can more readily handle higher transaction volumes. To date, all efforts have proven unsuccessful for Ethereum. However, some new platforms such as Polkadot, Zilliqa and Algorand offer some solutions for this scaling risk.

One actively pursued solution to the problem is a new consensus algorithm, *Proof of Stake*. Proof of Stake simply replaces mining of blocks (which requires a probabilistic wait time), with staking an asset on the next block, with majority rules similar to PoW.

Staking, an important concept in cryptocurrencies and DeFi, means a user escrows funds in a smart contract and is subject to a penalty (*slashed funds*) if they deviate from expected behavior.

An example of malicious behavior in Proof of Stake includes voting for multiple candidate blocks. This action shows a lack of discernment and skews voting numbers, and thus is penalized. The security in Proof of Stake is based on the concept that a malicious actor would have to amass more of the staked asset (ether in the case of Ethereum) than the entire rest of the stakers on that chain. This goal is infeasible and hence results in strong security properties similar to PoW.

Vertical and horizontal scaling are two additional general approaches to increasing blockchain throughput. Vertical scaling centralizes all transaction processing to a single large machine. This centralization reduces the communication overhead (transaction/block latency) associated with a PoW blockchain such as Ethereum, but results in a centralized architecture in which one machine is responsible for a majority of the system's processing. Some blockchains, such as Solana, follow this approach and can achieve upward of 50,000 TPS.

Horizontal scaling, however, divides the work of the system into multiple pieces, retaining decentralization but increasing the throughput of the system through parallelization. *Ethereum 2.0* takes this approach (called *sharding*) in combination with a Proof of Stake consensus algorithm.

Ethereum 2.0's technical architecture[43] differs drastically from vertically scaled blockchains such as Solana, but the improvements are the same. Ethereum 2.0 uses horizontal scaling with multiple blockchains and can achieve upward of 50,000 transactions per second.

The development of Ethereum 2.0 has been delayed for several years, but its mainnet, which will contain a basic blockchain without any smart contract support, may go live in 2021. Ethereum 2.0 has not yet finalized a functional specification for sending transactions between its horizontally scaled blockchains.

Another competitor with the potential to reduce scaling risk is the Ethereum layer-2 landscape. *Layer 2* refers to a solution built on top of a blockchain that relies on cryptography and economic guarantees to maintain desired levels of security. Transactions can be signed and aggregated in a form resistant to malicious actors, but are not directly posted to the blockchain unless there is a discrepancy of some kind. This removes the constraints of a fixed block size and block rate, allowing for much higher throughput. Some layer-2 solutions are live today.

As Ethereum's transaction fees have risen to record levels, layer-2 usage has remained stagnant. The space has been developing slowly and many live solutions lack support for smart contracts or decentralized exchanges. One solution in development is an *Optimistic Rollup*. An optimistic rollup is a process in which transactions are aggregated off-chain into a single digest that is periodically submitted to the chain over a certain interval. Only an aggregator who has a bond

[43] See https://docs.ethhub.io/ethereum-roadmap/ethereum-2.0/eth-2.0-phases/

(stake) can combine and submit these summaries. Importantly, the state is assumed to be valid unless someone challenges it. If a challenge occurs, cryptography can prove if the aggregator posted a faulty state. The prover is then rewarded with a portion of the malicious aggregator's bond as an incentive (similar to a Keeper mechanism). Optimistic rollups have yet to deliver functional mainnets and require expensive fraud proofs as well as frequent rollup transaction posting, limiting their throughput and increasing their average transaction costs.

Many approaches aim to decrease the scalability risks facing DeFi today, but the field lacks a clear winner. As long as DeFi's growth is limited by blockchain scaling, applications will be limited in their potential impact.

7.5 DEX Risk

The most popular DeFi products today mirror those we observe in traditional finance. The main uses for DeFi are gaining leverage, trading, and acquiring exposure to synthetic assets. Trading, as might be expected, accounts for the highest on-chain activity, while the introduction of new assets (ERC-20 tokens, Synthetics, and so forth) has led to a Cambrian explosion in DEXs. These decentralized exchanges vary considerably in design and architecture, but all are attempts to solve the same problem—how to create the best decentralized venue to exchange assets?

The DEX landscape on Ethereum consists of two dominant types, Automated Market Makers (AMMs) and order-book exchanges. Both types of DEXs vary in architecture and have differing risk profiles. AMMs, however, are the most popular DEX to date, because they allow users to trustlessly and securely exchange assets, while removing traditional counterparty risk. By storing exchange liquidity in a trustless smart contract, AMMs give users instant access to quotes on an exchange pair. Uniswap is perhaps the best-known example of an AMM, also known as a Constant-Function Market Maker (CFMM). Uniswap relies on the product of two assets to determine an exchange price (see section 7.3). The amount of liquidity in the pool determines the slippage when assets are exchanged during a transaction.

CFMMs such as Uniswap optimize for user experience and convenience, but sacrifice absolute returns. CFMM liquidity providers (LPs) earn yield by depositing assets into a pool, because the pool takes a fee for every trade (LPs benefit from high trading volume). This allows the pool to attract liquidity, but exposes LPs to smart contract risk and impermanent loss. Impermanent loss occurs when two assets in a pool have uncorrelated returns and high volatilities.[44] These properties allow arbitrageurs to profit from the asset volatilities and price differences, reducing the temporary returns for LPs and exposing them to risk if an asset moves sharply in price. Some AMMs, such as Cap, are able to reduce impermanent loss by using an oracle to determine exchange prices and dynamically adjusting a pricing curve to prevent arbitrageurs from exploiting LPs, but impermanent loss remains a large problem with most AMMs used today.

[44] For more on this topic, see Qureshi (2020).

On-chain order-book DEXs have a different but prevalent set of risks. These exchanges suffer from the scalability issues inherited from the underlying blockchain they run atop of, and are often vulnerable to front running by sophisticated arbitrage bots. Order-book DEXs also often have large spreads due to the presence of low-sophistication market makers. Whereas traditional finance is able to rely on sophisticated market makers including Jump, Virtu, DRW, Jane Street and more, order-book DEXs are often forced to rely on a single market maker for each asset pair. This reliance is due to the nascency of the DeFi market as well as the complex compute infrastructure required to provide on-chain liquidity to order-book DEXs. As the market evolves, we expect these barriers to break down and more traditional market makers to enter the ecosystem; for now, however, these obstacles create a significant barrier to entry. Regardless, both AMM and order-book DEXs are able to eliminate counterparty risk while offering traders a noncustodial and trustless exchange platform.

Several decentralized exchanges use an entirely off-chain order book, retaining the benefits of a noncustodial DEX, while circumventing the market making and scaling problems posed by on-chain order-book DEXs. These exchanges function by settling all position entries and exits on chain, while maintaining a limit-order book entirely off chain. This allows the DEX to avoid the scaling and UX issues faced by on-chain order-book DEXs, but also presents a separate set of problems around regulatory compliance.

Although risks abound in the DEX landscape today, they should shrink over time as the technology advances and market players increase in sophistication.

7.6 Custodial Risk

There are three types of custody: self, partial, and third-party custody. With self custody, a user develops their own solution which might be a flash drive not connected to the internet, a hard copy, or a vaulting device. With partial custody, there is a combination of self custody and external solution (e.g., Bitgo). Here, a hack on the external provider provides insufficient information to recreate the private key. However, if the user loses their private key, the user combined with the external solution, can recreate the key. The final option is third-party custody. There are many companies that have traditionally focused on custody in centralized finance that are now offering solutions in decentralized finance (e.g., Fidelity Digital Assets).

Retail investors generally face two options. The first is self custody where users have full control over their keys. This includes a hardware wallet, web wallet (e.g., MetaMask where keys are stored in a browser), desktop wallet, or even a paper wallet. The second is a custodial wallet. Here a third party holds your private keys. Examples are Coinbase and Binance.

The most obvious risk for self custody is that the private keys are lost or locked. In January 2021, The New York Times ran a story about a programmer who used a hardware wallet but

forgot the password.[45] The wallet contains $220m of bitcoin. The hardware wallet allows 10 password attempts before all data are destroyed. The programmer has only two tries to go.

Delegated custody also involves risks. For example, if an exchange holds your private keys, the exchange could be hacked and your keys lost. Most exchanges keep the bulk of private keys in "cold storage" (on a drive not connected to the internet). Nevertheless, there is a long history of exchange attacks including: Mt Gox (2011-2014) 850,000 bitcoin, Bitfloor (2012) 24,000 bitcoin, Bitfinex (2016) 120,000 bitcoin, Coincheck (2018) 523m NEM worth $500m at the time, and Binance (2019) 7,000 bitcoin.[46] The attacks have become less frequent. Some exchanges, such as Coinbase, even offer insurance. All of these attacks were on centralized exchanges. We have already reviewed some of the attacks on DEXs.

7.7 Regulatory Risk

As the DeFi market increases in size and influence, it will face greater regulatory scrutiny. Major centralized spot and derivatives exchanges, previously ignored by the CFTC, have recently been forced to comply with KYC/AML compliance orders, and DEXs appear to be next. Already, several decentralized derivatives exchanges, such as dYdX, must geoblock US customers from accessing certain exchange functionalities. Whereas the noncustodial and decentralized nature of DEXs presents a legal grey area with an uncertain regulatory future, little doubt exists that regulation will arrive once the market expands.

A well known algorithmic stablecoin project known as Basis was forced to shut down in December of 2018 due to regulatory concerns. A harrowing message remains on their home page for future similar companies: "Unfortunately, having to apply US securities regulation to the system had a serious negative impact on our ability to launch Basis…As such, I am sad to share the news that we have decided to return capital to our investors. This also means, unfortunately, that the Basis project will be shutting down." In response to regulatory pressure, DeFi has seen an increasing number of anonymous protocol founders. Earlier this year, an anonymous team launched a fork of the original Basis project (Basis Cash[47]).

Governance tokens, released by many DeFi projects, are also facing increasing scrutiny as the SEC continues to evaluate if these new assets will be regulated as securities. For example, Compound, the decentralized money market on Ethereum, recently released a governance token with no intrinsic value or rights to future cash flows. Doing so allowed Compound to avoid the SEC's securities regulation, freeing the company from security issuance responsibilities. We predict more projects will follow Compound's example in the future, and we expect most to

[45] https://www.nytimes.com/2021/01/12/technology/bitcoin-passwords-wallets-fortunes.html
[46] https://blog.idex.io/all-posts/a-complete-list-of-cryptocurrency-exchange-hacks-updated
[47] https://basis.cash/

exercise caution before issuing new tokens; many projects learned from the harsh penalties the SEC issued following the ICO boom in 2017.

Many major market-cap cryptocurrencies have been ruled commodities by the CFTC, exempting them from money-transmitter laws. Individual states, such as New York, however, have regulation that targets brokerages facilitating the transfer and exchange of cryptocurrencies. As DeFi continues to grow and the total number of issued assets continues to expand, we expect to see increasingly specific and nuanced regulation aimed at DeFi protocols and their users.

Cryptocurrency taxation has yet to be fully developed from a regulatory standpoint, and accounting software/on-chain monitoring is just starting to reach mainstream retail audiences. For example, as of December 31, 2020, the IRS draft proposal requires reporting on form 1040 of: any receipt of cryptocurrency (for free) including airdrop or hard fork; exchange of cryptocurrency for goods or services; purchase or sale of cryptocurrency; exchange of virtual currency for other property, including for another virtual currency; and acquisition or disposition of a financial interest in a cryptocurrency. Moving virtual currency from one wallet to another is not included. The regulations also make it clear that a form W2 is required for cryptocurrency payments made in exchange for work.[48]

While the DeFi regulatory landscape continues to be actively explored, with new regulatory decisions being made daily such as that allowing banks to custody cryptocurrency, the market outlook is hazy with many existing problems yet to be navigated.

8. Conclusions: The Losers and the Winners

Decentralized finance provides compelling advantages over traditional finance along the verticals of decentralization, access, efficiency, interoperability, and transparency. Decentralization allows financial products to be owned collectively by the community without top-down control, which could be hazardous to the average user. Access to these new products for all individuals is of critical importance in preventing widening wealth gaps.

Traditional finance exhibits layers of fat and inefficiency that ultimately remove value from the average consumer. The contractual efficiency of DeFi brings all of this value back. As a result of its shared infrastructure and interfaces, DeFi allows for radical interoperability beyond what could ever be achieved in the traditional-finance world. Finally, the public nature of DeFi fosters trust and security where there may traditionally exist opacity.

[48] https://www.irs.gov/pub/irs-dft/i1040gi--dft.pdf

DeFi can even directly distribute value to users to incentivize its growth, as demonstrated by Compound (via COMP) and Uniswap (via UNI). *Yield farming* is the practice of seeking rewards by depositing into platforms that incentivize liquidity provisioning. Token distributions and yield farming have attracted large amounts of capital to DeFi over incredibly short time windows. Platforms can engineer their token economics to both reward their innovation and foster a long-term sustainable protocol and community that continues to provide value.

Each DeFi use case embodies some of these benefits more than others and has notable drawbacks and risks. For example, a DeFi platform, which heavily relies on an oracle that is more centralized, can never be as decentralized as a platform that needs no external input to operate, such as Uniswap. Additionally, a platform such as dYdX with some off-chain infrastructure in its exchange cannot have the same levels of transparency and interoperability.

Certain risks plague all of DeFi and overcoming them is crucial to DeFi's achieving mainstream adoption. Two risks, in particular, are scaling risk and smart contract risk. The benefits of DeFi will be limited to only the wealthiest parties if the underlying technology cannot scale to serve the population at large. Inevitably, the solutions to the scaling problem will come at the price of some of the benefits of a "pure" DeFi approach, such as decreased interoperability on a "sharded" blockchain. Similar to the internet and other transformational technologies, the benefits and scale will improve over time. Smart contract risk will never be eliminated, but wisdom gained from experience will inform best practices and industry trends going forward.

As a caution to dApps that blindly integrate and stack on top of each other without proper due diligence, the weakest link in the chain will bring down the entire house. The severity of smart contract risk grows directly in proportion to the natural tendency to innovate and integrate with new technologies. For this reason, it is inevitable that high-profile vulnerabilities will continue to jeopardize user funds as they have in the past. If DeFi cannot surmount these risks, among others, its utility will remain a shadow of its potential.

The true potential of DeFi is transformational. Assuming DeFi realizes its potential, the firms that refuse to adapt will be lost and forgotten. All traditional finance firms can and should begin to integrate their services with crypto and DeFi as the regulatory environment gains clarity and the risks are better understood over time. This adoption can be viewed as a "DeFi front end" that abstracts away the details to provide more simplicity for the end user.

Startups, such as Dharma, are leading this new wave of consumer access to DeFi. This approach will still suffer from added layers of inefficiency, but the firms that best adopt the technology and support local regulation will emerge as victors while the others fade away. The DeFi protocols that establish strong liquidity moats and offer the best utility will thrive as the key backend to mainstream adoption.

We see the scaffolding of a shiny new city. This is not a renovation of existing structures; it is a complete rebuild from the bottom up. Finance becomes accessible to all. Quality ideas are funded no matter who you are. A $10 transaction is treated identically to a $100m transaction.

Savings rates increase and borrowing costs decrease as the wasteful middle layers are excised. Ultimately, we see DeFi as the greatest opportunity of the coming decade and look forward to the reinvention of finance as we know it.

9. References

Chetty, Raj, Nathaniel Hendren, Patrick Kline, and Emmanuel Saez. 2014. "Where Is the Land of Opportunity? The Geography of Intergenerational Mobility in the United States." *Quarterly Journal of Economics,* vol. 129, no. 4 (November): 1553–1623.

Corbae, Dean, and Pablo D'Erasmo. 2020. "Rising Bank Concentration," Staff Paper 594, Federal Reserve Bank of Minneapolis (March). Available at https://doi.org/10.21034/sr.594

Ellis, Steve, Ari Juels, and Sergey Nazarov. 2017. "Chainlink: A Decentralized Oracle Network." Working paper (September 4). Available at https://link.smartcontract.com/whitepaper

Euromoney. 2001. "Forex Goes into Future Shock." (October). Available at https://faculty.fuqua.duke.edu/~charvey/Media/2001/EuromoneyOct01.pdf

Haber, Stuart, and Scott Stornetta. 1991. "How to Time-Stamp a Digital Document." *Journal of* Cryptology (January). Available at https://dl.acm.org/doi/10.1007/BF00196791

Nakamoto, Satoshi. 2008. "Bitcoin: A Peer-to-Peer Electronic Cash System." Bitcoin.org.

Narayan, Amber, Roy Van der Weide, Alexandru Cojocaru, Christoph Lakner, Silvia Redaelli, Daniel Mahler, Rakesh Ramasubbaiah, and Stefan Thewissen. 2018. *Fair Progress? Economic Mobility across Generations around the World,* Equity and Development Series. Washington, DC: World Bank.

Qureshi, Haseeb. 2020. "What Explains the Rise of AMMs?" Dragonfly Research (July 22).

Ramachandran, Ashwin, and Haseeb Qureshi. 2020. "Decentralized Governance: Innovation or Imitation?" Dragonfly Research.com (August 5). Available at https://medium.com/dragonfly-research/decentralized-governance-innovation-or-imitation-ad872f37b1ea

Robinson, Dan, and Allan Niemerg. 2020. "The Yield Protocol: On-Chain Lending with Interest Rate Discovery." White paper (April). Available at https://research.paradigm.xyz/Yield.pdf

Shevchenko, Andrey. 2020. "Dforce Hacker Returns Stolen Money as Criticism of the Project Continues." Cointelegraph.com (April 22).

Szabo, Nick. 1997. "Formalizing and Securing Relationships on Public Networks." Satoshi Nakamoto Institute. Available at https://nakamotoinstitute.org/formalizing-securing-relationships/

Zmudzinski, Adrian. 2020. "Decentralized Lending Protocol bZx Hacked Twice in a Matter of Days." Cointelegraph.com (February 18).

Bogatyy, Ivan. 2017. "Implementing Ethereum trading front-runs on the Bancor exchange in Python." Hackernoon (October 10)

10. Glossary

The italicized terms in the glossary definitions are themselves defined in the glossary.

Address. The address is the identifier where a transaction is sent. The address is derived from a user's public key. The public key is derived from the private key by *asymmetric key cryptography*. In Ethereum, the public key is 512 bits or 128 *hexadecimal* characters. The public key is hashed (i.e., uniquely represented) with a Keccak-256 algorithm, which transforms it into 256 bits or 64 hexadecimal characters. The last 40 hexadecimal characters are the public key. The public key usually carries the pre-fix "0x." Also known as public address.

Airdrop. Refers to a free distribution of tokens into wallets. For example, Uniswap governance airdropped 400 tokens into every Ethereum address that had used their platform.

AML (Anti-Money Laundering). A common compliance regulation designed to detect and report suspicious activity related to illegally concealing the origins of money.

AMM. See **Automated market maker**.

Asymmetric key cryptography. A means to secure communication. Cryptocurrencies have two keys: public (everyone can see) and private (secret and only for the owner). The two keys are connected mathematically in that the private key is used to derive the public key. With current technology, it is not feasible to derive the private key from the public key (hence, the description "asymmetric"). A user can receive a payment to their public address and spend it with their private key. Also, see *symmetric key cryptography*.

Atomic. A provision that causes contract terms to revert as if tokens never left the starting point, if any contract condition is not met. This provision is an important feature of a *smart contract*.

Automated market maker (AMM). A *smart contract* that holds assets on both sides of a trading pair and continuously quotes a price for buying and for selling. Based on executed purchases and sales, the contract updates the asset size behind both the bid and the ask and uses this ratio to define a pricing function.

Barter. A peer-to-peer exchange mechanism in which two parties are exactly matched. For example, A has two pigs and needs a cow. B has a cow and needs two pigs. There is some debate as to whether barter was the first method of exchange. For example, David Graeber argues that the earliest form of trade was in the form of debit/credit. People living in the same village gave each other "gifts" which by social consensus had to be returned in future by another gift that is

usually a little more valuable (interest). People kept track of exchanges in their minds as it was only natural and convenient to do so since there is only a handful sharing the same village. Coinage comes into play many, many years later with the rise of migration and war with war tax being one of the very first use cases.[49]

Blockchain. A decentralized ledger invented in 1991 by Haber and Stornetta. Every *node* in the ledger has a copy. The ledger can be added to through *consensus protocol*, but the ledger's history is immutable. The ledger is also visible to anyone.

Bonding curve. A *smart contract* that allows users to buy or sell a token using a fixed mathematical model. For example, consider a simple linear function in which the token = supply. In this case, the first token would cost 1 ETH and the second token 2 ETH, thereby rewarding early participants. It is possible to have different bonding curves for buying and selling. A common functional form is a logistic curve.

Bricked funds. Funds trapped in a *smart contract* due to a bug in the contract.

Burn. The removal of a token from circulation, which thereby reduces the supply of the token. Burning is achieved by sending the token to an unowned *Ethereum* address or to a contract that is incapable of spending. Burning is an important part of many *smart contracts*. For example, burning occurs when someone exits a pool and redeems the underlying assets.

Collateralized currency. Paper currency backed by collateral such as gold, silver, or other assets.

Collateralized debt obligation. In traditional finance, this represents a debt instrument such as a mortgage. In *DeFI*, an example would be a *stablecoin* overcollateralized with a cryptoasset.

Consensus protocol. The mechanism whereby parties agree to add a new block to the existing *blockchain*. Both *Ethereum* and *bitcoin* use *proof of work*, but many other mechanisms exist, such as *proof of stake*.

Contract account. A type of account in *Ethereum* controlled by a *smart contract*.

Credit delegation. A feature whereby users can allocate collateral to potential borrowers who can use the collateral to borrow the desired asset.

Cryptocurrency. A digital token that is cryptographically secured and transferred using blockchain technology. Leading examples are *bitcoin* and *Ethereum*. Many different types of

[49] See https://www.creditslips.org/creditslips/2020/06/david-graebers-debt-the-first-5000-years.html

cryptocurrencies exist, such as *stablecoin* and tokens that represent digital and non-digital assets.

Cryptographic hash. A one-way function that uniquely represents the input data. It can be thought of as a unique digital fingerprint. The output is a fixed size even though the input can be arbitrarily large. A hash is not encryption because it does not allow recovery of the original message. A popular hashing algorithm is the SHA-256, which returns 256 bits or 64 *hexadecimal* characters. The *bitcoin blockchain* uses the SHA-256. *Ethereum* uses the Keccak-256.

DAO. See **Decentralized autonomous organization**.

dApp. A decentralized application that allows direct interactions between peers (i.e., removing the central clearing). These applications are permissionless and censorship resistant. Anyone can use them and no central organization controls them.

Decentralized autonomous organization (DAO). An algorithmic organization that has a set of rules encoded in a *smart contract* that stipulates who can execute what behavior or upgrade. A DAO commonly includes a *governance token*.

Decentralized exchange (DEX). A platform that facilitates token swaps in a noncustodial fashion. The two mechanisms for DEX liquidity are *order book matching* and *automated market maker*.

Decentralized finance (DeFi). A financial infrastructure that does not rely on a centralized institution such as a bank. Exchange, lending, borrowing, and trading are conducted on a peer-to-peer basis using *blockchain* technology and *smart contracts*.

Defi. See **Decentralized finance**.

Defi Legos. The idea that combining protocols to build a new protocol is possible. Sometimes referred to as DeFi Money Legos or composability.

DEX. See **Decentralized exchange**.

Digest. See **Cryptographic hash**. Also known as message digest.

Direct incentive. A payment or fee associated with a specific user action intended to be a reward for positive behavior. For example, suppose a *collateralized debt obligation* becomes undercollateralized. The condition does not automatically trigger liquidation. An *externally owned account* must trigger the liquidation, and a reward (direct incentive) is given for triggering the liquation.

Double spend. A problem that plagued digital currency initiatives in the 1980s and 1990s: perfect copies can be made of a digital asset, so it can be spent multiple times. The *Satoshi*

Nakamoto white paper in 2008 solved this problem using a combination of *blockchain* technology and *proof of work*.

Equity token. A type of cryptocurrency that represents ownership of an underlying asset or a pool of assets.

EOA. See **Externally owned account**.

ERC-20. Ethereum Request for Comments (ERC) related to defining the interface for fungible tokens. Fungible tokens are identical in utility and functionality. The US dollar is fungible currency in that all $20 bills are identical in value and 20 $1 bills are equal to the $20 bill.

ERC-721. Ethereum Request for Comments (ERC) related to defining the interface for nonfungible tokens. Nonfungible tokens are unique and are often used for collectibles or specific assets, such as a loan.

ERC-1155. Ethereum Request for Comments (ERC) related to defining a multi-token model in which a contract can hold balances of a number of tokens, either fungible or non-fungible.

Ethereum. Second-largest cryptocurrency/*blockchain*, which has existed since 2015. The currency is known as ether (ETH). Ethereum has the ability to run computer programs known as *smart contracts*. Ethereum is considered a distributed computational platform.

Ethereum 2.0. A proposed improvement on the *Ethereum blockchain* that uses *horizontal scaling* and *proof-of-stake* consensus.

Externally owned account (EOA). An *Ethereum* account controlled by a specific user.

Fiat currency. Uncollateralized paper currency, which is essentially an IOU by a government.

Fintech (Financial Technology). A general term that refers to technological advances in finance. It broadly includes technologies in the payments, trading, borrowing, and lending spaces. Fintech often includes big data and machine learning applications.

Flash loan. An uncollateralized loan with zero counterparty risk and zero duration. A flash loan is used to facilitate arbitrage or to refinance a loan without pledging collateral. A flash loan has no counterparty risk because, in a single transaction, the loan is created, all buying and selling using the loan funding is completed, and the loan is paid in full.

Flash swap. Feature of some *DeFi* protocols whereby a contract sends tokens before the user pays for them with assets on the other side of the pair. A flash swap allows for near-instantaneous arbitrage. Whereas a *flash loan* must be repaid with the same asset, a flash swap allows the flexibility of repaying with a different asset. A key feature is that all trades occur within a single *Ethereum* transaction.

Fork. In the context of open source code, an upgrade or enhancement to an existing protocol that connects to the protocol's history. A user has the choice of using the old or the new protocol. If the new protocol is better and attracts sufficient mining power, it will win. Forking is a key mechanism to assure efficiency in *DeFi*.

Gas. A fee required to execute a transaction and to execute a *smart contract*. Gas is the mechanism that allows *Ethereum* to deal with the *halting problem*.

Geoblock. Technology that blocks users from certain countries bound by regulation that precludes the application.

Governance token. The right of an owner to vote on changes to the protocol. Examples include the MakerDAO MKR token and the Compound COMP token.

Halting problem. A computer program in an infinite loop. *Ethereum* solves this problem by requiring a fee for a certain amount of computing. If the *gas* is exhausted, the program stops.

Hash. See **Cryptographic hash.**

Hexadecimal. A counting system in base-16 that includes the first 10 numbers 0 through 9 plus the first six letters of the alphabet, a through f. Each hexadecimal character represents 4 bits, where 0 is 0000 and the 16th (f) is 1111.

Horizontal scaling. An approach that divides the work of the system into multiple pieces, retaining decentralization but increasing the throughput of the system through parallelization. This is also known as *sharding*. Ethereum 2.0 takes this approach in combination with a *proof-of-stake* consensus algorithm.

IDO. See **Initial DeFi Offering**.

Impermanent loss. Applies to *automated market makers (AMM)*, where a contract holds assets on both sides of a trading pair. Suppose the AMM imposes a fixed exchange ratio between the two assets, and both assets appreciate in market value. The first asset appreciates by more than the second asset. Users drain the first asset and the contract is left holding only the second asset. The impermanent loss is the value of the contract if no exchange took place (value of both tokens) minus the value of the contract after it was drained (value of second token).

Incentive. A broad term used to reward productive behavior. Examples include *direct incentives* and *staked incentives*.

Initial DeFi Offering (IDO). A method of setting an initial exchange rate for a new token. A user can be the first liquidity provider on a pair, such as, for example, the new token and a *stablecoin* such as USDC. Essentially, the user establishes an artificial floor for the price of the new token.

Invariant. The result of a constant product rule. For example, invariant = S_A * $S_{B,}$ where S_A is the supply of asset A, and S_B is the supply of asset B. Suppose the instantaneous exchange rate is 1A:1B. The supply of asset A = 4 and the supply of asset B = 4. The invariant = 16. Suppose the investor wants to exchange some A for some B. The investor deposits 4 of A so that the contract has 8 A (S_A = 4 + 4 = 8). The investor can withdraw only 2 of asset B as defined by the invariant. The new supply of B is therefore 2 (S_B = 4 – 2 = 2). The invariant does not change, remaining at 16 = 2 * 8. The exchange rate does change, however, and is now 2A:1B.

Keeper. A class of *externally owned accounts* that is an incentive to perform an action in a *DeFi* protocol of a *dApp*. The keeper receives a reward in the form of a flat fee or a percentage of the incented action. For example, the keeper receives a fee for liquidating a *collateralized debt obligation* when it becomes undercollateralized.

KYC (Know Your Customer). A provision of US regulation common to financial services regulation requiring that users must identify themselves. This regulation has led to *geoblocking* of US customers from certain *decentralized exchange* functionalities.

Layer 2. A *scaling* solution built on top of a *blockchain* that uses cryptography and economic guarantees to maintain desired levels of security. For example, small transactions can occur using a multi-signature payment channel. The *blockchain* is only used when funds are added to the channel or withdrawn.

Liquidity provider (LP). A user that earns a return by depositing assets into a pool or a *smart contract*.

Mainnet. The fully-operational, production *blockchain* behind a token, such as the *Bitcoin* blockchain or the *Ethereum* blockchain. Often used to contrast with *testnet*.

Miner. Miners cycle through various values of a *nonce* to try to find a rare *cryptographic hash* value in a *proof-of-work blockchain*. A miner gathers candidate transactions for a new block, adds a piece of data called a *nonce*, and executes a *cryptographic hashing function***.** The nonce is varied and the hashing continues. If the miner "wins" by finding a hash value that is very small, the miner receives a direct reward in newly minted cryptocurrency. A miner also earns an indirect reward, collecting fees for the transactions included in their block.

Miner extractable value. The profit derived by a miner. For example, the miner could front run a pending transaction they believe will increase the price of the cryptocurrency (e.g., a large buy).

Mint. An action that increases the supply of tokens and is the opposite of *burn*. Minting often occurs when a user enters a pool and acquires an ownership share. Minting and burning are essential parts of noncollateralized *stablecoin* models (i.e., when stablecoin gets too expensive more are minted, which increases supply and reduces prices). Minting is also a means to reward user behavior.

Networked liquidity. The idea that any exchange application can lever the liquidity and rates of any other exchange on the same *blockchain*.

Node. A computer on a network that has a full copy of a *blockchain*.

Nonce (Number Only Once). A counter mechanism for *miners* as they cycle through various values when trying to discover a rare *cryptographic hash* value.

Optimistic rollup. A scaling solution whereby transactions are aggregated off-chain into a single *digest* that is submitted to the chain on a periodic basis.

Oracle. A method whereby information is gathered outside of a *blockchain*. Parties must agree on the source of the information.

Order book matching. A process in which all parties must agree on the swap exchange rate. Market makers can post bids and asks to a *decentralized exchange (DEX)* and allow takers to fill the quotes at the pre-agreed price. Until the offer is taken, the market maker has the right to withdraw the offer or update the exchange rate.

Perpetual futures contract. Similar to a traditional futures contract, but without an expiration date.

Proof of stake. An alternative consensus mechanism, and a key feature of Ethereum 2.0, in which the staking of an asset on the next block replaces the mining of blocks as in *proof of work*. In *proof of work,* miners need to spend on electricity and equipment to win a block. In proof of stake, validators commit some capital (the stake) to attest that the block is valid. Validators make themselves available by staking their cryptocurrency and then they are randomly selected to propose a block. The proposed block needs to be attested by a majority of the other validators. Validators profit by both proposing a block as well as attesting to the validity of others' proposed blocks. If a validator acts maliciously, there is a penalty mechanism whereby their stake is *slashed*.

Proof of work (PoW). Originally advocated by Back in 2002, PoW is the consensus mechanism for the two leading *blockchains*: *Bitcoin* and *Ethereum*. *Miners* compete to find a rare *cryptographic hash*, which is hard to find but easy to verify. Miners are rewarded for finding the cryptographic hash and using it to add a block to the *blockchain*. The computing difficulty of finding the hash makes it impractical to go backward to rewrite the history of a leading blockchain.

Router contracts. In the context of *decentralized exchange,* a contract that determines the most efficient path of swaps in order to get the lowest slippage, if no direct trading pair is available e.g., on Uniswap.

Scaling risk. The limited ability of most current blockchains to handle a larger number of transactions per second. See *vertical scaling* and *horizontal scaling*.

Schelling-point oracle. A type of *oracle* that relies on the owners of a fixed supply of tokens to vote on the outcome of an event or report a price of an asset.

Sharding. A process of horizontally splitting a database, in our context, a blockchain. It is also known as *horizontal scaling*. This divides the work of the system into multiple pieces, retaining decentralization but increasing the throughput of the system through parallelization. *Ethereum 2.0* takes this approach with the goal of reducing network congestion and increasing the number of transactions per second..

Slashing. A mechanism in *proof of stake blockchain* protocols intended to discourage certain user misbehavior.

Slashing condition. The mechanism that triggers a *slashing*. An example of a slashing condition is when undercollateralization triggers a liquidation.

Smart contract. A contract activated when it receives ETH, or *gas*. Given the distributed nature of the *Ethereum blockchain*, the program runs on every *node*. A feature of the *Ethereum blockchain*, the main blockchain for *DeFi* applications.

Specie. Metallic currency such as gold or silver (or nickel and copper) that has value on its own (i.e., if melted and sold as a metal).

Stablecoin. A token tied to the value of an asset such as the US dollar. A stablecoin can be collateralized with physical assets (e.g., US dollar in USDC) or digital assets (e.g., DAI) or can be uncollateralized (e.g., AMPL and ESD).

Staking. The escrows of funds in a smart contract by a user who is subject to a penalty (*slashed* funds) if they deviate from expected behavior.

Staked incentive. A token balance custodied in a *smart contract* whose purpose is to influence user behavior. A staking reward is designed to encourage positive behavior by giving the user a bonus in their token balance based on the stake size. A staking penalty (*slashing*) is designed to discourage negative behavior by removing a portion of a user's token balance based on the stake size.

Swap. The exchange of one token for another. In *DeFi*, swaps are *atomic* and noncustodial. Funds can be custodied in a *smart contract* with withdrawal rights exercisable at any time before the swap is completed. If the swap is not completed, all parties retain their custodied funds.

Symmetric key cryptography. A type of cryptography in which a common key is used to encrypt and decrypt a message.

Testnet. An identically functioning *blockchain* to a *mainnet*, whose purpose is to test software. The tokens associated with the testnet when testing Ethereum, for example, are called test ETH. Test ETH are obtained for free from a smart contract that mints the test ETH (known as a faucet).

Transparency. The ability for anyone to see the code and all transactions sent to a *smart contract*. A commonly used blockchain explorer is etherscan.io.

Utility token. A fungible token required to utilize some functionality of a smart contract system or that has an intrinsic value defined by its respective smart contract system. For example, a *stablecoin***,** whether collateralized or algorithmic, is a utility token.

Vampirism. An exact or near-exact copy of a *DeFi* platform designed to take liquidity away from an existing platform often by offering users *direct incentives*.

Vault. A smart contract that escrows collateral and keeps track of the value of the collateral.

Vertical scaling. The centralization of all transaction processing to a single large machine, which reduces the communication overhead (transaction/block latency) associated with a *proof-of-work blockchain*, such as *Ethereum*, but results in a centralized architecture in which one machine is responsible for a majority of the system's processing.

Yield farming. A means to provide contract-funded rewards to users for staking capital or using a protocol.