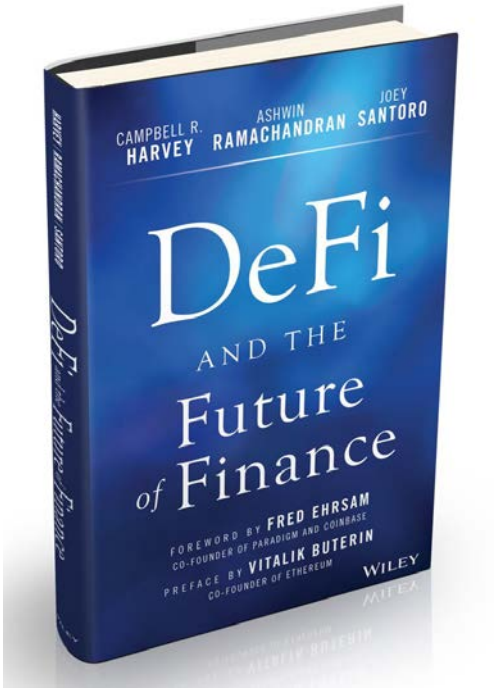
DeFi and the Future of Finance*

Available for Pre-Order at:
https://www.amazon.com/DeFi-Future-Finance-Campbell-Harvey/dp/1119836018/ref=sr_1_3



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.

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*

*Excerpt from book based on an early April 5, 2021 manuscript draft. 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, and Daniel Liebau on an earlier draft. Lucy Pless created the graphics and Kay Jaitly provided editorial assistance.

Table of Contents [Excerpt omits chapters 3-6]

1. Introduction **4**

2. The Origins of Modern Decentralized Finance 9
2.1 A Brief History of Finance 9
2.2 Fintech 9
2.3 Bitcoin and Cryptocurrency 11
2.4 Ethereum and DeFi 13

3. DeFi Infrastructure 14
3.1 Blockchain 15
3.2 Cryptocurrency 15
3.3 The Smart Contract Platform 15
3.4 Oracles 15
3.5 Stablecoins 15
3.6 Decentralized Applications 15

4. DeFi Primitives 15
4.1 Transactions 16
4.2 Fungible Tokens 16
4.2.1 Equity Token 16
4.2.2 Utility Tokens 16
4.2.3 Governance Tokens 16
4.3 Nonfungible Tokens 16
4.3.1 NFT Standard 16
4.3.2 Multi-Token Standard 16
4.4 Custody 16
4.5 Supply Adjustment 16
4.5.1 Burn - Reduce Supply 16
4.5.2 Mint - Increase Supply 16
4.5.3. Bonding Curve - Pricing Supply 16
4.6 Incentives 16
4.6.1 Staking Rewards 16
4.6.2 Slashing (Staking Penalties)
4.6.3 Direct Rewards and Keepers 16
4.6.4 Fees 16

4.7 Swap 16

4.7.1 Order Book Matching 16
4.7.2 Automated Market Makers (AMMs) 16
4.8 Collateralized Loans 16
4.9 Flash Loan (Uncollateralized Loan) 16

5. Problems DeFi Solves 16
5.1 Inefficiency 17
5.1.1 Keepers 17
5.1.2 Forking 17
5.2 Limited Access 17
5.2.1 Yield Farming 17
5.2.1 Initial DeFi Offering 17
5.3 Opacity 17
5.3.1 Smart Contracts 17
5.4 Centralized Control 17
5.4.1 Decentralized Autonomous Organization 17
5.5 Lack of Interoperability 17
5.5.1 Tokenization 17
5.5.2 Networked Liquidity 17

6. DeFi Deep Dive 17
6.1 Credit/Lending 18
6.1.1 MakerDAO 18
6.1.2 Compound 18
6.1.3 Aave 18
6.2 Decentralized Exchange 18
6.2.1 Uniswap 18
6.3 Derivatives 18
6.3.1 Yield Protocol 18
6.3.2 dYdX 18
6.3.3 Synthetix 18
6.4 Tokenization 18
6.4.1 Set Protocol 18
6.4.2 wBTC 18

7. Risks 18
7.1 Smart-Contract Risk 19
7.2 Governance Risk 21

7.3 Oracle Risk 22
7.4 Scaling Risk 23
7.5 DEX Risk 25
7.6 Custodial Risk 26
7.7 Regulatory Risk 27

8. Conclusions: The Losers and the Winners 28

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.

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 a financial 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 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

[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

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 adopt. 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

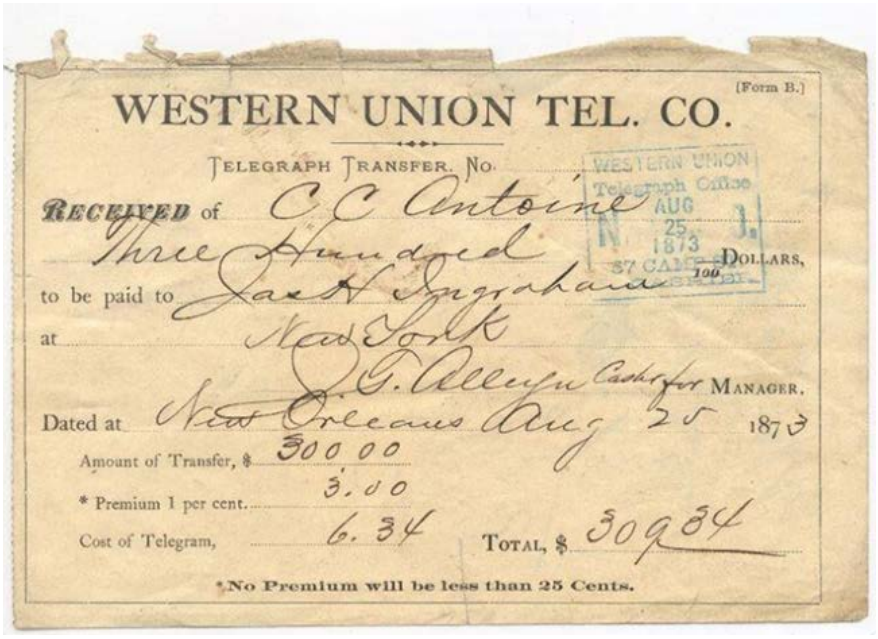
2.1 A brief history of finance

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 H Ingraham

at New York

J. G. Allen 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 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.

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

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, 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

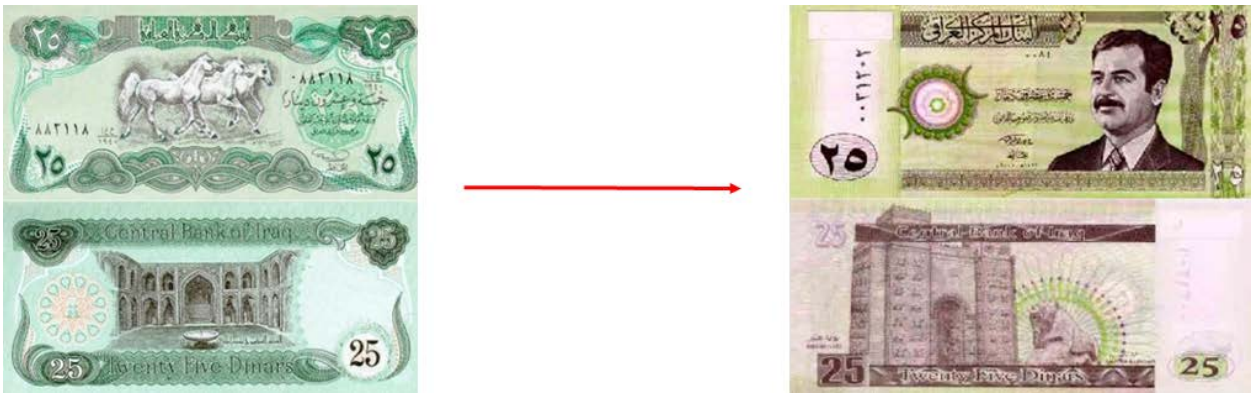
[5] PayPal founded as Confinity in 1998 did not begin offering a payments function until it merged with X.com in 2000.
[6] Other examples include: Cash App, Braintree, Venmo, and Robinhood.
[7] See Harvey, C. R., The history of digital money (2020), https://faculty.fuqua.duke.edu/~charvey/Teaching/697_2020/Public_Presentations_697/History_of_Digital_Money_2020_6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

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 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

[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.

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.

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

[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.

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 [See book]

3.1 Blockchain

3.2 Cryptocurrency

3.3 The Smart Contract Platform

3.4 Oracles

3.5 Stablecoins

3.6 Decentralized Applications

4. DeFi Primitives [See book]

4.1 Transactions

4.2 Fungible Tokens

4.2.1 Equity Token
4.2.2 Utility Tokens
4.2.3 Governance Tokens

4.3 Nonfungible Tokens

4.3.1 NFT Standard
4.3.2 Multi-Token Standard

4.4 Custody

4.5 Supply Adjustment

4.5.1 Burn - Reduce Supply
4.5.2 Mint - Increase Supply
4.5.3. Bonding Curve - Pricing Supply

4.6 Incentives

4.6.1 Staking Rewards
4.6.3 Direct Rewards and Keepers
4.6.4 Fees

4.7 Swap

4.7.1 Order Book Matching
4.7.2 Automated Market Makers (AMMs)

4.8 Collateralized Loans

4.9 Flash Loan (Uncollateralized Loan)

5. Problems DeFi Solves [See book]

5.1 Inefficiency

5.1.1 Keepers
5.1.2 Forking

5.2 Limited Access

5.2.1 Yield Farming
5.2.2 Initial DeFi Offering

5.3 Opacity

5.3.1 Smart Contracts

5.4 Centralized Control

5.4.1 Decentralized Autonomous Organization

5.5 Lack of Interoperability

5.5.1 Tokenization
5.5.2 Networked Liquidity

6. DeFi Deep Dive [See book]

6.1 Credit/Lending

6.1.1 MakerDAO
6.1.2 Compound
6.1.3 Aave

6.2 Decentralized Exchange

6.2.1 Uniswap

6.3 Derivatives

6.3.1 Yield Protocol
6.3.2 dYdX
6.3.3 Synthetix

6.4 Tokenization

6.4.1 Set Protocol
6.4.2 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[11] 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.

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

[11] 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

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 purchase heavily on the oracle exchange to manipulate the price, then proceed to purchase far more on the primary exchange in the opposite direction 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.[12] 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[13] 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 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.

[12] https://bzx.network/blog/postmortem-ethdenver
[13] Ethereum block 1428757.

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."[14]

A smaller but fascinating attack occurred in February 2021 and the target was Yearn.finance.[15] 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.[16] 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 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.[17] 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

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

[17] https://medium.com/dragonfly-research/decentralized-governance-innovation-or-imitation-ad872f37b1ea

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. While we have yet to see a true governance attack in practice, new projects like Automata[18] allow users to buy governance votes directly, and will likely accelerate the threat of malicious/hostile governance.

The founders often control traditional fintech companies, which reduces the risk of an external party influencing or changing the company's direction or product. DeFi protocols, however, are vulnerable to attack as soon as the governance system launches. Any financially equipped adversary can simply acquire a majority of liquid governance tokens to gain control of the protocol and steal funds.

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.[19]

We have not yet experienced a successful governance attack on any Ethereum-based DeFi project, but little doubt exists that a financially equipped adversary will eventually attack a protocol if the potential profit exceeds the cost of attack.

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.

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.

[18] https://automata.fi/
[19] https://twitter.com/trueseigniorage/status/1370956726489415683?lang=en

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[20] 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 (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.

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

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.[21] 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.

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.

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

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.[22] 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.[23] 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.

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

7.7 Environmental Risk [See book]

7.8 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[24]).

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 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

[24] https://basis.cash/

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 if you received any cryptocurrency for work, that must be reported on form W2.[25]

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.

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

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

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.

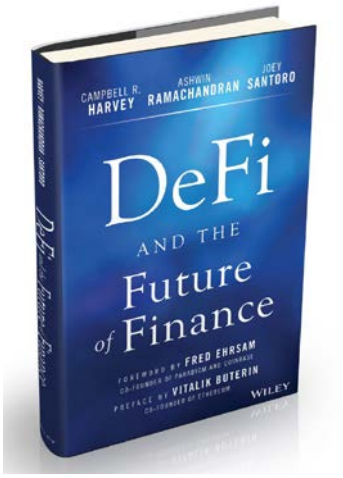
As a caution to dApps that blindlessly integrate and stack on top of each other without proper due diligence, the weakest link in the chain will bring down the entire house. The severity of smart contract risk grows directly in proportion to the natural tendency to innovate and integrate with new technologies. 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.

Available for Pre-Order at:
https://www.amazon.com/DeFi-Future-Finance-Campbell-Harvey/dp/1119836018/ref=sr_1_3



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).

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.[26]

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 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

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

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 16^{th} (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.