CHAPTER 20 A CLOSER LOOK INTO DECENTRALIZED FINANCE

HUGO BENEDETTI
Assistant Professor, ESE Business School, Universidad de los Andes, Chile

SEBASTIÁN LABBÉ
Doctoral Research Assistant, Karlsruhe Institute of Technology, Germany

KEYWORDS: Decentralized finance (DeFi), stablecoins, decentralized exchanges, automated market makers, liquidity pools, decentralized lending, synthetic instruments.

ABSTRACT

Decentralized finance (DeFi) is a technological infrastructure built on a blockchain networking environment that supplies transparent, uncensorable, and decentralized financial services and products. This infrastructure offers the opportunity to replicate traditional financial instruments on a decentralized platform and incorporate added features provided by blockchain technology. It also allows creating new instruments native to blockchain technology unavailable through traditional financial institutions. This chapter presents an in-depth analysis of the inner workings of stablecoins, decentralized exchanges, automated market makers, liquidity pools, decentralized lending, synthetic instruments, and asset management. It also provides specific examples for each application and presents some current challenges the sector faces.

INTRODUCTION

Decentralized finance (DeFi) has evolved rapidly in recent years with the promise of using the internet, cryptography, and code to optimize the efficiency and transparency of people's finances using decentralized blockchain networks. This area consists of different blockchains in the form of applications that together enable functions that until a few years ago were only possible through the traditional finance system, with barriers to entry difficult to overcome depending on an individual’s economic or geographic situation.

Free access to this new form of finance has also propelled its growth. Economists and others often ignore concerns about inflation for developed countries with strong currencies because it is low, or alternative financial instruments that protect against it are readily available. On the contrary, if one explores the context of developing countries with domestic currencies with high inflation due to negligent economic measures, a sustained pressure exists to sell domestic currencies for foreign currency, resulting in governments restricting access to these currencies. Access to these new instruments that only require an internet connection allows people to access free markets of stable currencies and digital assets safely, without needing intermediaries to restrict the free circulation of money. This new form of digital finance has a bright future in an increasingly connected world, given the rapid spread of the internet and smart devices capable of storing the cryptographic keys needed to make transactions.

DeFi is a technological infrastructure based on a blockchain networking environment built to provide financial services and products without a central authority (Schär 2020; Deshmukh et al. 2021; Gogel 2021). This infrastructure has different foundational pieces, which here are decentralized applications (DApps) using smart contracts to replicate services of traditional finance.

First appearing in the 1990s, a *smart contract* is “a set of promises, specified in digital form, which includes the same protocols where actors execute these promises” (Szabo 1996, p. 1). Additionally, a smart contract is a program or protocol devised to execute, control, or automatically document events or actions if certain conditions are met (Fries and Paal 2019). Blockchain’s emergence as a solution for peer-to-peer (P2P) transfers of value and a method of decentralized execution of contracts allowed this idea to come to life in 2015, with Ethereum as the first blockchain network compatible with executing smart contracts (Buterin 2014).

Among the fundamental building blocks of DeFi's exponential growth are overcollateralized stablecoin projects, such as MakerDAO (DAI), Synthetix (sUSD), and Liquity (LUSD). These stablecoins are debt instruments backed by volatile cryptoassets held in an over-collateralized reserve, with a dynamic interest rate adjusted algorithmically by predetermined formulas or according to decisions made by decentralized autonomous organizations (DAOs). Stablecoin’s creation allows for a decentralized, digital, and self-custodial alternative to traditional fiat currencies or fiat-backed stablecoins.

A second relevant DeFi application is decentralized exchanges (DEXs). These markets differ from their centralized counterparts. Users do not delegate the custody of their assets to a third party, enabling them to trade on a P2P in a secure and trustless format through a smart contract-based order book. These markets function 24/7 and are accessible ubiquitously to any user with a compatible wallet interface. Moreover, some web-based crypto wallets have embedded DEXs functionalities into their user interface, allowing users to trade directly from their wallet application, bypassing the need to connect to a DEX protocol. As DEXs rely on blockchain infrastructure, they can only trade blockchain-compatible assets. Therefore, using fiat currencies is limited to fiat-backed cryptocurrencies or fiat-based stablecoins.

Besides P2P trading, some DEXs have also implemented the concept of an *automatic market maker* (AMM), a smart contract that groups sellers and buyers of cryptocurrencies without needing preset market orders. People participate in these markets through so-called *liquidity pools* (LP), consisting of dynamically adjusted portfolios of tradable tokens. Users who contribute liquidity to the pools usually receive returns from trading fees and additional rewards in the form of newly issued tokens. Examples of DEX are Uniswap, Sushiswap, Balancer, Kyber, and Bancor.

Another fundamental building block is P2P lending, such as Compound and Aave. These protocols allow for overcollateralized lending through dynamic interest rates based on the demand for the protocol's liquidity pool. These overcollateralized loans theoretically have no risk of bad debt because they have sufficient backing or collateral to be repaid in the event of liquidation. Settlement mechanisms are open and rely on information provided by “oracles.” An *oracle* is an interface providing information from a blockchain network to smart contracts. Oracles can deliver different types of information depending on the smart contract’s requirements (Beniiche 2020). Some P2P protocols allow a flash loan instrument, which is a loan issued, settled, and repaid in the same blockchain block, allowing for instantaneous arbitrage and debt swaps from one blockchain protocol to another.

Decentralized insurers acting as mutuals allow mitigating the risks of blockchain-related events such as hackings, smart contract malfunctions, and events external to blockchain networks. Armor, Nexus Mutual, and Unslashed are examples of decentralized insurance projects that provide insurance to DeFi protocols. Other projects have gone beyond ensuring blockchain-based application providing insurance on more traditional events like flight delays or catastrophic weather, such as floods, hurricanes, and tornados.

Another DeFi product is a derivative instrument. Some protocols allow exposure to traditional asset types external to blockchain technologies, such as market indexes, stocks, and commodities. Applications including Synthethix, Mirror, and Uma use market information from oracles and algorithms from betting markets to generate synthetic tokens. A *synthetic token* tracks an external asset’s price without possessing the underlying asset or any related traditional instrument (Brooks, Jurisevic, Spain, and Warwick 2020). Markets, where buyers take a long or short position depending on market conditions, make this situation possible. Users can also exchange these synthetic tokens in decentralized markets.

Lastly, decentralized asset managers allow users to manage their cryptoassets automatically according to specific investment and portfolio optimization algorithms. The core premise is searching for the best investment strategies through decentralized governance. Some examples are Yearn Finance and Beefy Finance, which focus on the growth of digital assets, regardless of their volatility. Within this category, investors can buy index portfolios in a decentralized market. These portfolios can be pure indexes or actively managed by the community and developers. Set Protocol, Index Coop, Basket Dao, and Indexed Finance are examples of decentralized asset managers.

Composability is a crucial property of these applications. It allows creating higher complexity services or applications by assembling and combining a different set of smart contracts and decentralized applications, potentially from different blockchain networks. A smart contract creates a volume-weighted price on each collateral asset using prices obtained from several DEXs to algorithmically determine the collateralization ratios of stablecoins. In turn, each DEX can use the stablecoin as a price denominator in the exchange. If price differences exist between different DEXs, an AMM contract can arbitrage away the price differences, creating a more efficient price and greater liquidity across markets. Several blockchains with smart contract capabilities are available. Thus, each can host its stablecoins, DEXs, and AMM projects. Smart contracts can interconnect (bridge) different blockchains and allow interaction across stablecoins, DEXs, and AMMs. Lastly, as the interconnection between smart contracts and blockchains increases, dependency and reliance also increase. Therefore, if a hack, an exploit, or a bug occurs in a smart contract, its impact is likely to spread through the network and affect other ecosystem components.

The chapter proceeds as follows. The next section presents the economic dynamics of the three main stablecoin issuance mechanisms: asset-backed, cryptoasset-backed, and algorithmic/seigniorage-based. The following section describes DEXs, AMMs, and their interrelation. The subsequent section presents decentralized lending, derivatives, and asset managers, followed by a section on the current DeFi challenges. The final section contains a summary and conclusions.

STABLECOINS

Most agree that money should be a store of value, a medium of exchange, accountable, and recognizable (Mankiw 2019; Moin, Sekniqi, and Sirer 2020;). Smart contracts allow physical and digital assets to have these characteristics by representing them in the form of tokens. However, native cryptoassets are known for their price volatility, reducing their capacity as a store of value. Stablecoins reduce price volatility by formulating smart contracts to follow a reference price or peg. Although different types of stablecoins are available, the most common mechanism design involves those of asset-backed reserves, mainly fiat currencies such as the U.S. dollar, Euro, or Yen, overcollateralized cryptoasset-backed, such as bitcoin, ethereum, or another broadly used cryptoasset, and dual seignorage algorithmic tokens. These mechanism designs attempt to maintain the stablecoin price equal to its peg or redemption price. The following subsections present and compare these stablecoin economic mechanisms.

Asset-Backed Stablecoins

In this system, a traditional asset fully backs each stablecoin. The creating and destructing (“burning”) stablecoins result from an increase or reduction in the asset reserve. Most commonly, the reserve is U.S. dollars, held in custody by an intermediary, which may or may not be a regulated custodian. Some companies have caused controversy by using fixed income securities considered “cash and cash equivalent” instead of U.S. dollars directly (Grant Thornton LLP 2021).

The asset-backed reserve mechanism was the first stablecoin design, having its origins in 2012, when the Mastercoin project described the possibility of issuing digital assets on the Bitcoin network, operating on a second layer (Willet 2013). Subsequently, part of the Mastercoin team founded Realcoin in 2014 (Casey 2014). This project, later renamed "Tether," managed different digital assets operating on the Mastercoin Project's Omni network. Different cryptocurrency exchanges and blockchain networks later used the stablecoin "USDT," issued by Tether. It was a primary instrument to store and safeguard liquidity in the different cryptocurrency markets (Griffin and Shams 2020). Despite this stablecoin's success, doubts arose about the integrity of Tether reserves. In March 2021, after a ruling by the New York courts, authorities forced Tether to disclose publicly its detailed reserve instruments.

Newer projects sought greater transparency with regular audits, institutional-grade custody, and fully insured reserves. In 2018, the U.S.-based companies Circle and Coinbase created USDC, a stablecoin fully backed by U.S. dollar reserves. In 2018, Stasis launched EURS, a stablecoin fully backed by Euro reserves. Also, in 2018, Paxos launched a white-label stablecoin, providing stablecoin issuance to third parties. Its most relevant stablecoin is BUSD, used by the leading crypto exchange Binance as its proprietary stablecoin. At the end of 2021, Tether represented 45.99 percent ($78.12 billion) of the dollar-denominated stablecoin market, followed by USDC with 29.32 percent ($49.66 billion) and BUSD with 8.82 percent ($15.02 billion) (Gecko Labs Pte. Ltd 2022).

Overcollateralized Crypto-Backed Stablecoins

MakerDAO was one of the first projects to propose creating decentralized stablecoins pegged to the dollar by generating debt-collateralized positions (CDP). Users deposit cryptoassets, such as bitcoin, ether, and liquidity pool tokens, into a smart contract "vault" and use them as collateral to generate a debt instrument. This instrument equals a certain number of tokens, "DAI," each with a value pegged to $1. Users can issue any amount between 25 and 75 percent of the collateral value, with a dynamically agreed interest rate ("stability rate"). Adjustment of a DAI's price occurs through the market, with the stability rate being the mechanism to incentivize the token's price to tend to the peg. The collateral can be unlocked at any time if the full borrowed value of DAI plus the stability rate is paid (Moin et al. 2020). Control of a protocol's stability rate occurs through constituents voting on a decentralized autonomous organization (DAO). The DAO's constituents must deposit their governance tokens in a smart contract to vote on protocol decisions. These decisions can be executive, such as adding or removing collateral types and vaults, adjusting global protocol parameters, replacing smart contracts, or polls designed to assess the DAO's sentiment, regarding possible changes in the protocol (MakerDAO 2021).

As opposed to asset-backed stablecoins, decentralized cryptoasset-backed stablecoins do not require a central controlling and issuing authority, a custodian to hold reserves, or an auditor to verify the integrity and value of reserves. The smart contract performs all these processes. Holders of the protocol's token determine changes to the smart contract.

A criticism of this decentralized stablecoin model is that it still suffers from the problem of tracking the peg's value. This value is usually a traditional currency subject to inflation, despite working well as a store of value, unit of account, and medium of exchange. Additionally, some newly accepted collaterals are centralized asset-backed stablecoins, like USDC, PAX, TUSD, GUSD, and USDT), increasing regulatory risk if those assets become regulated. On the other hand, the governance model has barriers to entry due to the fluctuating cost of blockchain transactions. During specific periods of high demand for blockchain transactions, the dynamically adjusted transaction cost has made participating in governance voting economically unfeasible for retail token holders. This situation is detrimental to the protocol's decentralization.

Liquidity is a decentralized cryptoasset-backed stablecoin project, holding overcollateralized reserves of ether to issue its stablecoin LUSD. The project minimizes potential regulatory risks by not having a front-end interface and only interacting with smart contracts. Any website or app-based interface can connect to the smart contract and function as an intermediary between users and the liquidity protocol. Besides this back-end-only infrastructure, the protocol offers a 0 percent interest rate on loans, a collateral requirement of only 110 percent, and a one-time issuance rate of 0.5 percent, charged at debt repayment.

Figure 20.1 presents the price evolution of LUSD and ether. The figure shows that while the price of ether in U.S. dollars fluctuated wildly, a 100 percent increase followed by a 25 percent decrease, closely maintaining the peg of LUSD ($1r).

(Insert Figure 20.1 about here)

Algorithmic Seignorage Stablecoins

The third stablecoin mechanism relies on the issuance and destruction of monetary units or reserves to maintain the stablecoin's peg value. The most common framework relies on using two tokens simultaneously. One token acts as a stablecoin and backs its value on reserves of the other token, usually a utility and governance token. The most representative example of this type of token is UST, a stablecoin backed by Luna, the native token of the Terra blockchain. In this case, the protocol controls the issuance and burning of UST tokens (Kereiakes, Kwon, Di Maggio, and Platias 2019). When UST's value exceeds the dollar value in a set of markets monitored by an oracle, the protocol creates more UST. It simultaneously burns part of Luna token reserves, balancing the total issued value of UST and LUNA. When UST's value drops below $1, the system sells LUNA and buys UST tokens in the open market.

Figure 20.2 presents the price evolution of UST and LUNA. UST's price remains close to the peg, while reserve token's price varies widely, from around $0.40 in the last quarter of 2020 to $25.00 in the last quarter of 2021, after reaching highs near $45.

(Insert Figure 20.2 about here)

A less traditional project, Ampleforth, developed a single token algorithmic stablecoin. The AMPL tokens follow a continuous rebasing, meaning that the number of tokens in circulation can increase or decrease automatically according to the token's price evolution in the monitored markets. The number of tokens in any crypto wallet containing AMPL increases when AMPL's price increases, aiming to return to the peg price equal to the 2019 inflation-adjusted $1 benchmark. The increase in the total circulating supply of AMPL delivered directly to all current holders of the token should decrease the market price by increasing the selling pressure due to the inflation of tokens in circulation. At the same time, when AMPL's value decreases, the number of tokens in the wallet also decreases, removing market liquidity and potentially bringing the token's price back to the inflation-adjusted $1. This mechanism, called "rebasing," occurs every 24 hours. A smart contract oracle calculates AMPL's time-weighted average price from the main marketplaces. It then gradually increases or decreases the total amount of tokens in circulation. The rebasing mechanism has not been as effective as initially intended, leading to a large price disparity relative to the target peg. As Figure 20.3 shows, AMPL's price reached lows below $0.50 and highs of over $3.50.

(Insert figure 20.3 about here)

Lastly, the FRAX project proposed a hybrid solution to stablecoin design (Frax 2020). It combines collateralized issuance with algorithmic rebasing. A potential problem with collateralized stablecoins is that the collateral base does not increase by the same magnitude during positive demand shocks. FRAX proposes a dual reserve, with a fraction of reserves held in a stablecoin and the rest in a proprietary token (FXS). The share of collateral held on each adjusts algorithmically. If FRAX's price exceeds the peg, in this case a $1, FXS held in reserve is burned, reducing the share of collateral backed by FXS and increasing the share backed by stablecoins. If FRAX's price is below the peg, additional FXS are minted and held in reserves, increasing the share of reserves backed by FXS and reducing the share backed by stablecoins.

DECENTRALIZED EXCHANGES

Before 2014, users mostly exchanged cryptocurrencies on centralized exchanges (CEXs). This approach went against Bitcoin's original ethos regarding exchanging fiat currencies for cryptocurrencies. Thus, a need existed to relinquish direct control of the cryptocurrency and transfer ownership to a centralized intermediary, the CEX. Hackers targeted many CEXs between 2014 and 2020 (Crystal Analytics Team 2021). For example, Mt. Gox's hack in February 2014 accounted for about 6 percent of bitcoin's total supply.

To bring bitcoin's ethos to the cryptocurrency markets, different developers created DEXs that operated on top of Bitcoin as a second layer, such as Bitshares, NXT, Mastercoin, and Counterparty. Developers designed these platforms to abstract the marketplace's complexity while using the security of the Bitcoin blockchain when settling transactions. However, the Bitcoin programming system's limitations, in addition to the limitations on the size and type of information stored in the Bitcoin blockchain, made these solutions complex to program, use, and isolated from each other.

In 2016, Vitalik Buterin proposed a DEX based on an automated market maker (AMM) (Buterin 2016). With this approach, any user could participate in an AMM smart contract by depositing two equal-valued amounts of tokens in a liquidity pool. When a counterparty trades against the AMM, it removes a certain amount of one token and increases the amount of the other. The relative value of each token held in the LP changes and reflects the new relative price of each token. In addition, users pay a liquidity fee, which goes to the liquidity providers.

In 2018 Hayden Adams implemented this idea in a project called Uniswap (Adams, Zinsmeister, and Robinson 2020). Two years later, during the so-called DeFi summer, it became the first DEX to hold over $1 billion in assets and outperform Coinbase Pro (a US-based CEX) in daily volume. Uniswap's success shows that a DEX can provide liquidity levels similar to world-class CEXs. Additionally, without regard for its potential market cap or liquidity levels, any token can be "listed" using an AMM smart contract. The latter led to creating initial decentralized offerings (IDOs) instead of initial exchange offerings (IEOs) by funding liquidity pools on an AMM. This feature enables token issuers to distribute primary issuance tokens to users and provide liquidity to current token holders.

During the Uniswap boom in late August 2020, an anonymous developer, known by the pseudonym Chef Nomi, copied the code, named the copy Sushiswap and executed what came to be known as a *vampire attack*, draining liquidity from the victim and transferring it to the attacker. Sushiswap distributed its token (Sushi) to users who deposited Uniswap liquidity pool tokens into a smart contract. The value of newly issued Sushi tokens offered liquidity providers an annual percentage yield equivalent to over 1000 percent. During the attack, over $800 million moved from Uniswap to Sushiswap.

The project Balancer aspires to be an AMM based on a market value-weighted portfolio index. Liquidity providers deposit multiple tokens into a liquidity pool, creating a portfolio of tokens available for trading. As users trade against the portfolio, the weights of each asset and their relative prices change, effectively rebalancing the portfolio. With each trade, the portfolio receives trading fees. Therefore, liquidity providers who deposit into Balancer's liquidity pool participate in a self-rebalancing market portfolio and get a share of all fees received from trader interactions.

A drawback of AMM is *impermanent loss*, which refers to the temporary losses occurring in liquidity pools due to large and sudden price changes that generate an imbalance in the value of the token reserves. Most smart contract AMMs are passive traders, not initiating transactions on behalf of the liquidity pool. The smart contract waits for external traders to interact and trade against the liquidity pool. This feature creates a dependency on external traders to arbitrage price differences between the relative prices within the liquidity pool and the relative prices in other markets (DEXs, CEXs, or other AMMs).

Suppose an initial price of 2,000 UST per ETH. A liquidity pool should have in reserve 2,000 UST per ETH. Therefore, if the contract initially had 20,000 UST and 10 ETH, it would have a total value locked (TVL) of 40,000 UST. If the price of ETH doubles to 4,000 UST in external markets, traders could still buy 1 ETH by depositing 2,000 UST into the contract. After one transaction of 1 ETH, the contract would have 22,000 UST and 9 ETH. ETH's internal relative price would now be 2,444 UST (22,000 UST divided by 9 ETH). This process would continue until the internal relative price equals the external relative price. A smart contract predetermines the price impact of each trade to prevent users from withdrawing (purchasing) large amounts of tokens and taking unfair advantage of the protocol. However, it is vulnerable to large price changes. The *impermanent loss* is the difference in the portfolio's value to the value of a buy-and-hold strategy on the same assets. To compensate for this potential loss, liquidity providers receive compensation in the form of trading fees charged on each transaction.

DECENTRALIZED LENDING, DERIVATIVES, AND ASSET MANAGEMENT

The idea of a P2P credit market is not new. Since 2005 companies have operated solutions using the internet to enable direct lending between retail customers (Lee and Lee 2012). The emergence of smart contracts permitted creating protocols that allow this kind of P2P transactions in a decentralized manner.

In 2018, a protocol called ETHLend and later renamed Aave created a lending marketplace on Ethereum. Due to the pseudo-anonymous nature of blockchain networks, which limits reputation building and legally enforces delinquent debt, lending markets have only been collateral-based. Collateralized loans reduce or eliminate debt repayment risk and allow using the collateral for low-risk investments such as staking, offsetting part of a debtor's interest cost. Interest rates adjust dynamically and depend on the usability of the deposited assets. These markets also enable leveraged long and short investing. In a leveraged long position, a debtor uses the newly acquired debt, usually a stablecoin, to purchase additional amounts of the collateral asset token. In leveraged shorts, users deposit stablecoins as collateral and borrow the volatile cryptocurrency they expect to decrease in price. If the price decreases, their collateralization ratio increases, allowing additional debt issuance and increasing the short position.

Another application that emerged with a similar idea is Compound. This application uses collateral deposits to provide liquidity to AMMs. Hence collateral receives additional revenue from trading fees, further reducing the cost of borrowing. The yield received from trading fees surpassed the interest charge during specific periods, leading to a negative borrowing cost in some cryptoassets.

Smart contracts can also create derivative instruments by holding collateral reserves and distributing future flows derived from them according to a predetermined set of rules. As presented in the previous sections, users can deposit volatile cryptoassets and create a new asset of stable value. The same mechanism allows protocols to transform volatile assets into new tokens, which could track the price of volatile non-blockchain-related assets such as commodities, stocks, bonds, and exchange rates.

In the case of the Synthethix protocol, individuals can deposit the protocol token (SNX) to generate synthetic dollars, which serve as collateral in the synthetic stock and derivatives market. Any synthetic derivative's value in the platform derives from markets where people favoring an outcome take a long position on the token, while people are against take a short position. The platforms support contracts on synthetics stocks, fiat currencies, indices, options, and perpetual futures, among others.

An implementation that best demonstrates DeFi's composability is asset management Dapps. The segment started with Yearn Finance, a dApp launched in 2020 in response to the difficulties observed by users on choosing the most profitable investment option among different protocols. As investment returns fluctuate based on the supply and demand of liquidity on a particular token in each market, Yearn Finance automatically tracks returns on each market and deploys funds to the highest paying market. As token transactions have fixed fees, pooling funds reduces the average transaction cost per user, increasing returns compared to individual strategies. Yearn Finance currently employs multiple strategies per token. In the case of Ethereum, the protocol employs seven different strategies to generate returns. A team of developers actively updates and monitors these strategies.

CHALLENGES

Although DeFi has many advantages over traditional finance, it still has several unresolved issues. Exponential project growth occurred during 2021, reflecting developer and user interest in this new form of finance. However, developers do not yet have enough experience to create robust and secure code in such immature fields, leading to security flaws overlooked by developers, auditors, and users.

A leading area of uncertainty concerns an applicable legal and tax framework. Different jurisdictions have not adapted regulations for digital assets. This legal limbo generates distrust in investors. Consequently, some refrain from investing due to unclear legal and tax implications. By contrast, other jurisdictions take advantage of this situation. They strategically adopt a less restrictive attitude to attract investors from other countries. For example, El Salvador legalized using bitcoin as legal tender. For El Salvador, a dollarized country, without a domestic fiat currency and an economy dependent on remittances in foreign currency (Anzoategui, Demirgüç-Kunt, and Martínez Pería 2014), DeFi expands access to international capital markets without the limitations of traditional intermediaries, remittances, and payment systems. Some European countries adopted much lower taxes on profits from cryptoasset investments.

The transparency in code execution in most blockchain protocols allows for front running by competing agents and transaction reordering by miners. Daian et al. (2019) and Obadia (2021) discuss and measure the total value that can be extracted through the reordering, inclusion, or censorship of transactions within the blocks when included in the blockchain. This problem is like that observed in traditional finance with free trading applications. In this instance, some market participants sell information about the volume of orders from retail investors to generate profits from arbitrage, a phenomenon called *payment for order flow* (PFOF). Proposals are available to solve this problem, such as *fair sequencing order* (FSS), which attempts to order transactions fairly across blocks.

Another problem is the safekeeping of digital assets. Although sufficient education about computer security is available, the risk of losing digital assets due to phishing techniques or lack of risk prevention is still common. Fraud frequently occurs in this space. According to Chainanalysis (Chainanalysis Team 2021), scams represent the most prominent form of cryptocurrency-based crime by transaction volume, with over $7.7 billion worth of cryptocurrency taken from victims worldwide in 2021. Also, the basis of the programming language for most of these apps is still novel. Therefore, developers who lack sufficient experience may be unaware of all possible issues.

In 2021, DeFi-related hacks accounted for about 75 percent of the major hacks related to cryptocurrencies, totaling almost $1.3 billion (CipherTrace 2021; CertiK 2022). This situation further strengthens the position that DeFi is still a novel ecosystem, with potential, but faces many challenges to overcome before mainstream adoption.

SUMMARY AND CONCLUSIONS

This chapter presents some DeFi building blocks, namely stablecoins, DEXs, AMMs, decentralized lending, smart contract-based synthetic instruments, and automated asset managers. The chapter briefly explains the mechanics behind code execution and discusses some currently available protocols and projects for each element. It ends by reviewing some challenges faced by the DeFi industry.

DISCUSSION QUESTIONS

1. Identify and explain three stablecoin implementation designs.
2. Explain the arbitrage process that allows liquidity pools to reach market prices without relying on oracles or market price feeds.
3. Describe the term impermanent loss.
4. Discuss the mechanisms that allow negative interest rates on crypto asset collateralized loans.

REFERENCES

Adams, Hayden, Noah Zinsmeister, and Dan Robinson. 2020. "Uniswap v2 Core." Uniswap.org. March. Available at https://uniswap.org/whitepaper.pdf.

Anzoategui, Diego, Asli Demirgüç-Kunt, and María Soledad Martínez Pería. 2014. "Remittances and Financial Inclusion: Evidence from El Salvador." *World Development* 54:C, 338–349.

Beniiche, Abdeljalil. 2020. "A Study of Blockchain Oracles." arXiv:2004.07140. Cornell University. March 19. Available at https://arxiv.org/abs/2004.07140v2.

Brooks, Samuel, Anton Jurisevic, Michael Spain, and Kain Warwick. 2020. "Synthetix Litepaper." Available at https://synthetix.io/.

Buterin, Vitalik. 2014. “A Next-Generation Smart Contract and Decentralized Application Platform.” Ethereum White Paper. Available at http://buyxpr.com/build/pdfs/EthereumWhitePaper.pdf.

Buterin, Vitalik. 2016. “Let’s Run On-Chain Decentralized Exchanges the Way We Run Prediction Markets.” Reddit.com. October 3. Available at https://www.reddit.com/r/ethereum/comments/55m04x/lets_run_onchain_decentralized_exchanges_the_way/.

Casey, Michael J. 2014. “Dollar-Backed Digital Currency Aims to Fix Bitcoin’s Volatility Dilemma.” *The Wall Street Journal*. July 8. Available at https://www.wsj.com/articles/BL-MBB-23780.

CertiK. 2022. “State of DeFi Security 2021.” Available at https://certik-2.hubspotpagebuilder.com/the-state-of-defi-security-2021.

Chainanalysis Team. 2021. “The Biggest Threat to Trust in Cryptocurrency: Rug Pulls Put 2021 Scam Revenue Close to All-Time High.” Chainanalysis.com. December 16. Available at https://blog.chainalysis.com/reports/2021-crypto-scam-revenues/.

CipherTrace. 2021. “Cryptocurrency Crime and Anti-Money Laundering Report, August 2021.” Ciphertrace.com. August. Available at https://ciphertrace.com/cryptocurrency-crime-and-anti-money-laundering-report-august-2021/.

Crystal Analytics Team. 2021. “The 10 Biggest Crypto Exchange Hacks in History.” Crystalblockchain.com. June 25. Available at https://crystalblockchain.com/articles/the-10-biggest-crypto-exchange-hacks-in-history/.

Daian, Philip, Steven Goldfeder, Tyler Kell, Yunqi Li, Xueyuan Zhao, Iddo Bentov, Lorenz Breidenbach, and Ari Juels. 2019. “Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges.” Arxiv.org. April 10. Cornell University. Available at https://arxiv.org/abs/1904.05234v1.

Deshmukh, Sumedha, André Geest, David Gogel, Daniel Resas, and Christian Sillaber. 2021. “Decentralized Finance (DeFi) Policy-Maker Toolkit.” Weforum.org. June 8. Available at https://www.weforum.org/whitepapers/decentralized-finance-defi-policy-maker-toolkit.

Frax. 2020. "Frax: Fractional-Algorithmic Stablecoin Protocol." Available at https://docs.frax.finance/overview.

Fries, Martin, and Boris P Paal (eds.). 2019. *Smart Contracts*. Germany: Mohr Siebeck. Available at https://library.oapen.org/handle/20.500.12657/24858.

Gecko Labs Pte. Ltd. 2022. “Stablecoins by Market Capitalization.” Available at https://www.coingecko.com/en/categories/stablecoins.

Gogel, David. 2021. “DeFi Beyond the Hype – The Emerging World of Decentralized Finance.” Wharton, University of Pennsylvania. June. Available at https://wifpr.wharton.upenn.edu/wp-content/uploads/2021/05/DeFi-Beyond-the-Hype.pdf.

Grant Thornton LLP. 2021. “Circle Reserve Account Report.” September 1. Available at https://www.centre.io/hubfs/pdfs/attestation/2021 Circle Examination Report July 2021 Final.pdf?hsLang=en.

Griffin, John M., and Amin Shams. 2020. “Is Bitcoin Really Untethered?” *Journal of Finance* 75:4, 1913–1964.

Kereiakes, Evan, Do Kwon, Marco Di Maggio, and Nicholas Platias. 2019. “Terra Money: Stability and Adoption.” Available at https://www.terra.money/Terra_White_paper.pdf.

Lee, Eunkyoung, and Byungtae Lee. 2012. “Herding Behavior in Online P2P Lending: An Empirical Investigation.” *Electronic Commerce Research and Applications* 11:5, 495–503.

MakerDAO. 2021. “Learn About MakerDAO.” Available at https://makerdao.world/en/learn/MakerDAO.

Mankiw, N. Gregory. 2019. *Macroeconomics,* Tenth Edition. New York, NY: Worth Publishers.

Moin, Amani, Kevin Sekniqi, and Emin Gun Sirer. 2020. “SoK: A Classification Framework for Stablecoin Designs.” In Joseph Bonneau and Nadia Heninger (eds.), *Financial Cryptography and Data Security. FC 2020. Lecture Notes in Computer Science*, vol 12059, 174−200. Cham: Springer.

Obadia, Alex. 2021. “Quantifying MEV: Introducing MEV-Explore V0.” Medium.com. February 22. Available at https://medium.com/flashbots/quantifying-mev-introducing-mev-explore-v0-5ccbee0f6d02.

Schär, Fabian. 2020. “Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets.” *Review*, *Federal Reserve of Saint Louis* 103:2, 153−174.

Szabo, Nick. 1996. “Smart Contracts: Building Blocks for Digital Markets.” *Extropy* 16. Available at https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html.

Willet, Jr. 2013. “MasterCoin Complete Specification vs. 1.1 (Smart Property Edition).” Available at https://sites.google.com/site/2ndbtcwpaper/.

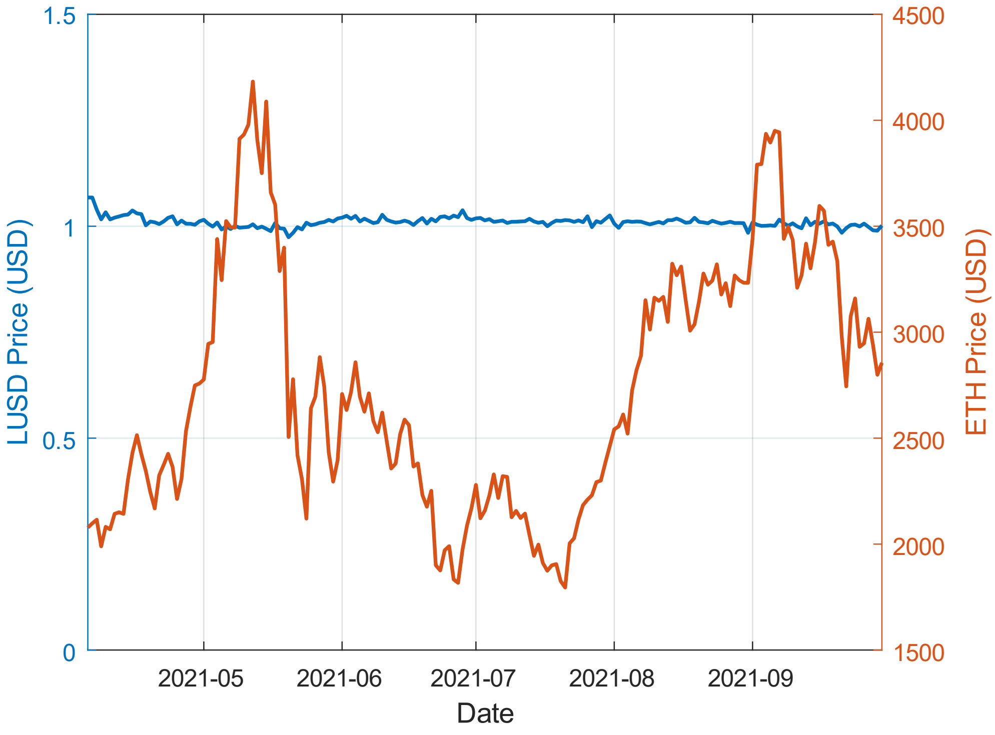
ABOUT THE AUTHORS

Hugo Benedetti is an Assistant Professor and the Academic Director of the Executive Master’s in Finance and Investments Program at ESE Business School, Universidad de Los Andes, Chile. His research focuses on entrepreneurial finance, venture capital, and FinTech, particularly blockchain technology and blockchain-enabled assets. *The Economist*, *Bloomberg*, *The Wall Street Journal*, Nasdaq, and several crypto-industry publications have featured his research. Professor Benedetti often delivers workshops on entrepreneurial finance, venture capital, and FinTech to incubators, angel investor networks, and venture capital funds. He has advised and mentored several FinTech and blockchain projects. Before joining academia, he co-founded a financial advisory boutique and held leadership roles in corporate finance, financial advisory, and venture capital at world-class firms. Professor Benedetti is a Fulbright scholar and received a PhD in finance from Boston College.

Sebastián Labbé is a Research Assistant at the Institute of Concrete Structures and Building Materials at Karlsruhe Institute of Technology. His research focuses on structural dynamics, concrete technologies, and modeling impact loads due to railway traffic. *Building and Construction Materials* and *The German Federal Railway Authority* Have featured his research. Mr. Labbé is a blockchain enthusiast due to his experience with personal finance while living abroad, focusing on the technology, applications, and teaching of DeFi. He is a CHILFITEC and DAAD Alumni and received a Civil Engineering and Master of Engineering degree at Pontificia Universidad Católica de Chile and an MS at École Centrale Paris.

Figure 20.1 Price Evolution of LUSD and Ether: April 1, 2021, to September 30, 2021

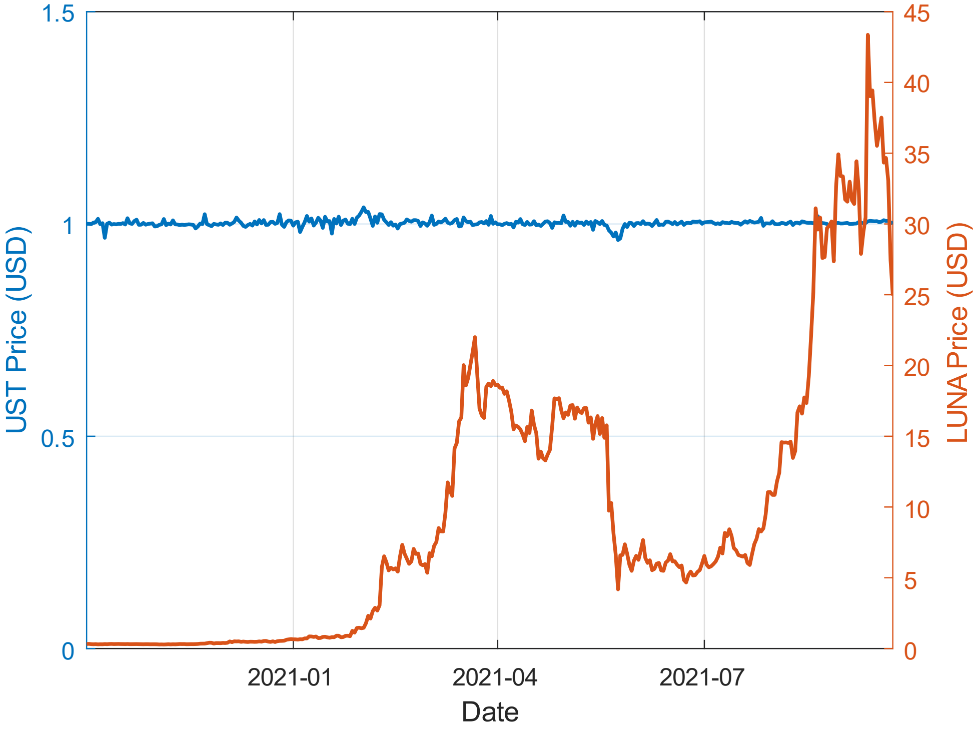
This table shows LUSD and ether prices in U.S. dollars between April 1, 2021, and September 30, 2021, using price data from coinmarketcap.com.



Source: Coinmarketcap.com.

Figure 20.2 Price Evolution of UST and LUNA: November 1, 2020, to September 30, 2021.

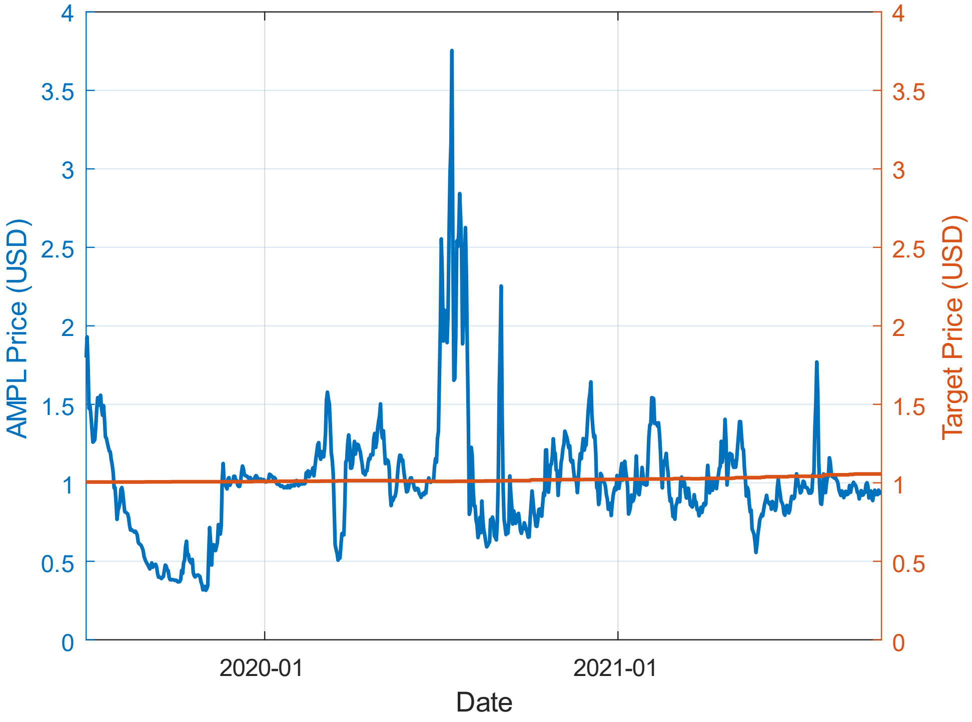
This table shows UST and LUSD prices in U.S. dollars between November 1, 2020, and September 30, 2021, using price data from coinmarketcap.com.



Source: Coinmarketcap.com.

Figure 20.3 Price Evolution of AMPL and Its Target Price: July 1, 2019, to September 30, 2021

This table shows the evolution of AMPL and its target prices, 2019 inflation-adjusted $1 US, both expressed in US dollars, between July 1, 2019, and September 30, 2021, using price data from coinmarketcap.com



Source: Coinmarketcap.com.