A New Era of Blockchain-Powered Decentralized Finance (DeFi) - A Review

1st Saulo dos Santos
Department of Computer Science
University of Manitoba
Winnipeg, Canada
dossants@myumanitoba.ca

2nd Japjeet Singh
Department of Computer Science
University of Manitoba
Winnipeg, Canada
js5@myumanitoba.ca

3rd Ruppa K. Thulasiram
Department of Computer Science
University of Manitoba
Winnipeg, Canada
tulsi.thulasiram@umanitoba.ca

4th Shahin Kamali
Department of Computer Science
University of Manitoba
Winnipeg, Canada
shahin.kamali@umanitoba.ca

5th Louis Sirico
CTO
Fluidefi
Montreal, Canada
louis@fluidefi.com

6th Lisa Loud
CEO - Fluidefi
IEEE vice-chair on QuADD/WG
Montreal, Canada
lisa@fluidefi.com

2022 IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC) | 978-1-6654-8810-5/22/$31.00 ©2022 IEEE | DOI: 10.1109/COMPSAC54236.2022.00203

***Abstract*—The Bitcoin whitepaper [1] published in 2008 proposed a novel decentralized ledger, later called blockchain, which enabled multiple transacting parties to agree upon the shared state of the ledger without a trusted intermediary. Blockchain technology has been used to implement many decentralized payment systems, with the general term Cryptocurrency coined for the native unit of values. The launch of the Turing-complete Ethereum blockchain [2] in 2015 extended the scope of blockchain-based financial systems beyond cryptocurrencies. The suite of non-custodial financial solutions deployed as Smart Contracts over Turing-complete blockchains is broadly called Decentralized Finance (DeFi). These solutions have gained widespread popularity as investment vehicles in the last two years, with their total value locked (TVL) exceeding USD 100 Billion. This paper reviews the key financial services offered in DeFi and draws a parallel to the corresponding services in the centralized financial industry. Some technical and economic risks associated with the DeFi investments are also discussed in the paper. Most of the existing review papers on DeFi focus on some specific DeFi services, are theoretically inclined, and are intended for academics in computer science or economics. This paper, on the other hand, aims to give an overview of the current state of the DeFi ecosystem. We aim to keep this review lucid to make it accessible to a broader audience without compromising academic rigor. The intended audience for this paper includes anyone with a basic understanding of financial markets and blockchain systems. This work will be specifically helpful for investment professionals to understand the rapidly evolving ecosystem of DeFi services.**

***Index Terms*—DeFi, Blockchain, Financial Services, Smart Contracts, Decentralized Finance**

I. Introduction

Capital investment is a pillar of the modern economic system. Individuals tend to invest their savings as a means to hedge against inflation. There is a broad ecosystem of organizations that manage the investment from numerous individual investors, pool it, and allocate it across various assets throughout the global financial markets. The economy which receives these investments benefits due to the growth and development it brings along, while for the investors, it leads to the growth of their capital and wealth. Many of these investments involve financial instruments like stocks, bonds, and derivatives. These instruments are also traded independently on global financial exchanges, with their prices varying. The world of finance is primarily digitized, with all the information being stored in digital format. In many cases, these assets are traded with very high frequency by large institutions like pension funds that manage their clients' wealth and aim to give them good returns through their trades.

Despite sophisticated risk measures and hedging strategies, these investment institutions may sometimes incur hefty losses (thus affecting their clients). It is especially true at times of extreme events like the 2008 financial crisis and the 2019 pandemic, partly due to the ill effects of a centralized financial system that lacks transparency. Also, economic growth may flatten or decline when capital allocation strategies, controlled by a handful of executives in large institutions, are planned poorly.

A new class of financial assets called cryptocurrency was envisaged in 2008 with the launch of the Bitcoin white paper [1] by a person or a group under the pseudonym Satoshi Nakamoto. The subsequent launch of the Bitcoin peer-to-peer network in a decentralized manner. The key achievement of this white paper was the solution to maintain a distributed ledger of transactions among a set of participants and ensure consensus on the ledgers' state without involving a trusted central party. Blockchain technology is based on well-established cryptographic primitives of hashing and public-key encryption. Another major step in blockchain-powered finance was the launch of the Ethereum blockchain network [2]. Ethereum took the core ideas from Bitcoin and extended these to create a general-purpose platform (not just a currency). Ethereum is a Turing-complete blockchain supporting smart contracts that can be programmed using Solidity [3]. Ethereum Virtual Machine (EVM) uses the consensus mechanism of blockchain to maintain a globally coherent state among its participating

978-1-6654-8810-5/22/$31.00 ©2022 IEEE
DOI 10.1109/COMPSAC54236.2022.00203

nodes.

The consensus mechanism of blockchain can be seen as a public append-only data structure with the following main properties.

1) Persistence: data cannot be altered once written to the blockchain[1].
2) Consensus: All honest participants have the same data[2].
3) Liveliness: All participants can add new transactions.
4) Openness: Any participant can add data to the blockchain.

Smart contracts, in their basic form, are programs in which a set of encoding rules are enforced by a blockchain's consensus mechanism(s). The distributed framework allows trustless economic interactions between parties. The Ethereum blockchain embedded the first working implementation of smart contracts. Following Ethereum, other blockchains such as Binance Smart Chain (BSC) [4], Cardano (ADA) [5], Solana (SOL) [6] and Avalanche (AVAX) [7] with smart-contract capabilities provided other platforms to build decentralized applications using an underlying blockchain as core consensus layer. The concept of decentralized autonomous organizations (DAOs) was subsequently developed along this line. DAOs are companies that are governed by their token holders and use the blockchain to manage token ownership. Another significant development was the introduction of decentralized finance (DeFi) solutions, which involve building a complete financial services ecosystem (mirroring the centralized version, which includes some core institutions like banks and exchanges) over blockchains based on smart contracts. In the past two years, the interest in DeFi has exploded, with total value locked (TVL) reaching more than USD 100 Billion [8]. A key advantage of DeFi over centralized institutions is that all transactions are public and posted on the underlying blockchain. This makes the underlying smart contracts very transparent and auditable. Moreover, to attract investment, the DeFi protocols may have specific incentives to reward the initial investors, making investing in the underlying protocol more appealing. Even though the value locked in DeFi is a tiny portion of the centralized financial institutions, it has the potential to take a significant share of the market. Due to its decentralized, globally accessible 24/7/365, openly auditable nature, and non-custodial architecture that can offer new financial products, DeFi has the potential to resolve the existing inefficiencies of capital allocation in today's centralized financial ecosystem.

The volume of investment in DeFi is growing exponentially, but unlike traditional finance, various statistical measures to quantify investment volatility and risk exposure have not yet been devised. Although the data in the blockchain are public and universally accessible, it is still in a raw format, which needs to be aggregated and extrapolated to provide helpful information and support investment decisions [9]. In this paper, we draw a big picture of DeFi's state of the art and bridge the gap between traditional financial services and DeFi applications.

[1]Assuming honest nodes controls more than 50% of the network

[2]They might diverge for recently added blocks, but the consensus is guaranteed for older blocks

II. Background on Traditional/Crypto Finance

A. Traditional Finance

We will review some of the critical entities of the financial system and the essential services they provide for running today's market-based economies. The key characteristic of these systems is centralized control and the requirement of a trusted intermediary to make financial transactions. The key entities in the traditional financial system and their interconnections are listed below.

- Central Banks: The institution responsible for deciding the overall monetary policy of an economy, from monetary supply to interest rates. Typically, a central bank also supervises commercial banks and non-banking public financial institutions. Examples of central banks are the Bank of England in the UK [10] and the Federal Reserve Board in the USA [11].
- Financial Regulators: These are the authorities typically controlled by the government to oversee the financial activities within their jurisdiction. Different regulators can exist within a jurisdiction, each dedicated to monitoring specific economic activities. Their stated goal is to ensure fairness and prevent fraudulent activities. For example, the Financial Conduct Authority (FCA) [12] is the financial services regulator in the UK and the Securities and Exchange Commission (SEC) [13] is the securities regulator in the USA.
- Exchanges: An exchange is a platform for trading financial instruments like stocks, derivatives, bonds, etc. It also acts as a medium for companies to raise capital from investors by getting listed. The governing body of exchanges also must ensure a fair marketplace for investors. Almost all modern-day exchanges are functioning electronically.
- Commercial Banks: These are the institutions that provide the banking services (like savings, borrowing, etc.) to individuals, companies, and organizations. They make a bridge between the clients having excess capital by accepting deposits through saving services and the clients who need money by offering them lending services.
- Brokers: These individuals or companies act as intermediaries between investors and financial exchanges. They facilitate the individuals to trade assets in exchange for commission/ fees.
- Asset Management Companies: These entities manage their clients' pooled funds. These funds include hedge funds, mutual funds, pension funds, private funds from High Net worth Individuals (HNIs), etc.

Financial services are essential pillars of a modern economy. These services ensure that the global economic system can run and grow, and hence people can improve their living standards by participating in this system. The form of the financial system varies between classes of participants. Generally, individuals aim to build wealth and improve their living

standards, while businesses strive to get resources to invest in productive activities while earning profit from these activities. An ideal financial system ensures efficient resource allocation across the participating actors to achieve these goals. The distribution efficiency among participants is measured in terms of utility derived by each of them. The key components of the financial system are financial contracts that determine how real resources will be allocated among participants. The legal system that enforces these contracts and the regulator that oversees the entire system detect and rectify irregularities by enforcing investor rights and preventing bad actors from using the system by enforcing Know-Your-Customer (KYC) and Anti-Money-Laundering (AML) standards. Also, the financial system performs risk management by mandating specific minimum capital requirements for institutions.

Some of the factors that can undermine a financial system are:

1) Lack of trading opportunities: Inefficacy of the financial system reduces the composability of trading strategies that could increase the utility of counterparties.
2) High systemic risk: a systemic risk is realized when multiple participating entities may collapse one after another, like a domino, due to high interdependence.
3) Inefficient split in the trade benefits resulting in monopolies.

On the contrary, some of the factors that contribute to a healthy financial system are:

1) Allocation: An ideal financial system has resource distribution that optimizes the increase in utility of participants
2) Inclusiveness: Actors willingly participate in an ideal financial system, and the system provides enough opportunities for participation of new actors.
3) Unbiased regulation: Regulators must ensure that the system's spillovers are managed in everyone's best interest.

B. Bitcoin

The standard centralized payment method through government-issued and controlled banknotes has been a norm since it replaced the barter trade system. This norm was questioned by Satoshi Nakamoto (2008) in his seminal paper [1] that advocated for a decentralized system of payment over the traditional intermediate trusted party system (e.g., a central bank). Nakamoto highlighted certain drawbacks of the conventional online transaction systems, such as cost incurred for transactions, minimum transaction limit, and the fact that transactions can be reversible. Subsequently, they proposed a decentralized digital currency, called Bitcoin, that uses cryptography to carry out transactions and securely handle ownership. These transactions are stored in a decentralized system called a blockchain. A blockchain is a list of blocks where the miners record different transactions as blocks, and each block contains a list of validated transactions (after being added to the blockchain). The miners are rewarded with some bitcoins and obtain transaction fees from users once they add a block to the blockchain. Multiple blogs, opinion columns, and articles are published in various conferences and journals ranging from Business to Law and Computer Science to Finance, which discuss Cryptocurrencies at different levels and facets. This paper does not attempt a thorough review of all aspects (business, computing, finance, and law) of cryptocurrencies. We refer to Chohan [14] for a brief thematic review of cryptocurrency markets.

Bitcoin [1] was one of the first payment methods based on a peer-to-peer network that allows transfers without a traditional trusted third party like a central bank or other government institution. It was followed by Ethereum [2] as the first blockchain network with smart-contract capabilities. Commonly used payment systems are based on a trust-based model where a financial institution is responsible for mediating all transactions. Blockchain networks use cryptography algorithms that validate transactions and prevent double-spending transactions using an underlying consensus algorithm [15], [16]. Once a block is inserted into the chain, it cannot be changed unless the majority of the participants agree according to the underlying consensus protocol. This is because, as more and more blocks are inserted into the chain, the amount of network coordination to change becomes a daunting task. Thus, blockchain systems are reliable as long as honest nodes constitute a majority of the network. To guarantee that a majority of the network is honest, an incentive is given for each validated block inserted into the blockchain.

III. SmartContracts

A. Smart Contracts

Nick Szabo introduced the concept of the smart contract [17], and suggested that the terms of a legal contract could be embedded in code, which would execute it autonomously without the requirement of a third party. Szabo used as an example a vending machine, which can handle a simple logic such as "input $\Rightarrow$ selection $\Rightarrow$ authorization $\Rightarrow$ change" without any human intermediary. With the introduction of blockchain technology, smart contracts became popular as complex programs deployed on transaction-based blockchains. They consist of rules verifying, controlling, and self-executing a predefined agreement. As they are executed on a decentralized blockchain network that is transparent, traceable, and irreversible, smart contracts often involve anonymous parties in a trustless setting without the participation of third parties. Smart contracts allow a deterministic, rapid, and cost-efficient execution of contracts between parties.

A smart contract has an address used to call the program, functions which encode its behavior, and data that maintains the state among all the nodes in the network. To execute a smart contract, the users must pay a fee, usually identified in terms of "gas". The amount of gas varies depending on the smart contract's complexity and cost for each operation it executes. Gas is generally paid with the underlying currency of the blockchain on which the smart contract is running. In the case of Ethereum, the denomination is Gwei, while the currency is Ether [18].

B. ERC-20 and ERC-721 Tokens

Smart contracts enable developers to implement tokens, and a variety of complex distributed programs such as lending platforms, e.g. Aave [19], Compound [20], and decentralized exchanges (DEXes), such as Uniswap [21], SushiSwap [22].

Tokens are a standard implementation of smart contracts. The most common tokens constitute ERC-20 and ERC-721 standards for fungible and non-fungible tokens on the Ethereum blockchain. A token can be fungible or non-fungible. Fungible tokens are interchangeable as all the tokens in circulation have the same value, while the non-fungible token (NFT) is unique, and each has its own value [23].

IV. SmartContracts vs Traditional Finance

A. Services

1) Borrowing/Lending: Lending is a vital component of economic machinery. One of the primary mechanisms is to facilitate the capital exchange agreement between parties with excess capital (called lenders) and parties that need money (called borrowers). Lending is a mutually beneficial agreement where the borrowed capital must be returned to the lender along with additional payment in the form of interest as per an agreed-upon timeline [24]. Also, to hedge against the risk of non-repayment of the lent amount, the lender takes custody of some asset called *collateral* from the borrower, which the lender can monetize to cover the unpaid loaned amount. Decentralized lending is a construct like traditional lending for digital assets like cryptocurrencies and tokens hosted on blockchain platforms. But, unlike lending in conventional finance, the decentralized lending platforms cannot accept off-chain assets as collateral [25]. Moreover, as blockchain-based digital assets are more volatile when compared to most traditional financial assets, their lending has to be over-collateralized, i.e., the value of the collateral token at the time of the lending has to be greater than the lent token. The over-collateralized agreements can be seen in the issue of DAI stablecoins by MakerDAO [26] as well as popular decentralized lending platforms like Aave [19] and Compound [20]. Under-collateralized lending protocols such as Alpha Homora [27] also exist, but in such platforms, there are many restrictions on spending of the borrowed funds, and the ownership of the funds stays with the lending pool instead of being transferred to the borrower.

Liquidation is an exciting mechanism associated with decentralized lending, which allows a third party to buy the collateral from the lending pool at a discounted price in case the value of the collateral falls below a certain threshold relative to the borrowed asset [25]. It acts as a risk management mechanism for the borrower while providing liquidators with profit-making opportunities.

Flash loans are a novel risk-free lending mechanism introduced in DeFi, which can only be implemented in blockchain-based settlement systems and is not available in traditional finance. A flash loan involves lending a digital asset and its subsequent repayment within a single atomic transaction [28]. If the borrowed amount is not repaid, the entire transaction is reverted and not included in the block, which is equivalent to the loan event not taking place. One of the most common applications of flash loans is to gather funds for utilizing the arbitrage opportunities between different Decentralized Exchanges to earn risk-free profit [29].

2) Stablecoins: One of the key properties of money in modern economic systems is that it is a "store of value" [30]. A commodity or asset can be considered a value store if it can be reliably saved, retrieved, and exchanged in future times while also being predictably useful as a medium of exchange on retrieval [31]. In other words, its value should remain considerably stable with time. But cryptocurrencies, which are the native medium of exchange on their respective blockchains, are too volatile to be considered a reliable store of value. As the government-backed fiat currencies act as means of payment for all day-to-day financial transactions in the real economy, an equivalent, less volatile store of value is needed for the transactions on the blockchain-powered financial ecosystem. Stablecoins [32] are designed to fill this gap. These are the smart contract-based digital tokens deployed over the blockchain whose value is pegged to the non-volatile assets like fiat currencies. Hence, they act as stable value stores for payments settled on blockchains. Most of the widely used stablecoins are pegged to the US dollar, the most circulated fiat currency in the world. The first stablecoin was Tether, pegged to USD and launched in 2015 [33]. Stablecoins can be custodial or non-custodial. Custodial stablecoins rely on a trusting third party to maintain the stability in prices, generally by off-chain collateral backing of the underlying asset like US Dollars. Non-custodial stablecoins, on the other hand, use economic mechanisms to maintain the peg to stable assets [34]. Tether, USDC, and Binance USD are examples of custodial stablecoins, while MakerDAO is a leading example of non-custodial stablecoins [33].

3) Decentralized Exchanges (DEXes): A financial exchange is a platform on which financial assets, either traditional or blockchain-based digital assets, are traded by different parties. Participating traders enter their quotes to buy or sell a particular asset in the traditional exchange model. The exchange system has two main steps: first, to match the trades which can be executed, and second, the settlement between counterparties. Such an exchange is called an order book and requires a central authority to accept and match quotes and act as an escrow for the financial assets of the counterparties until the trade is executed. The centralized cryptocurrency/token exchanges like Coinbase, Binance, and FTX are also based on an order book model where trade matching and settlement are carried out on the centralized server of the platform service provider. An order book based decentralized exchange can also be set up in the form of smart contracts deployed over the blockchain. EtherDelta is an example of such an approach but suffers from various problems like latency, high gas fees, miner front running, etc. [35], even though it provides certain advantages of decentralized finance in the form of censorship resistance and robustness. Another

class of exchange models more suitable for blockchain-based decentralized financial assets is the Automated Market Makers (AMMs) [36]. The most popular of them is the Constant Function Market Makers (CFMM) [37], which maintain a mathematical invariant (for example, a product of the quantity of assets) during the trade. Unlike order book exchange, in CFMM, transactions happen between a trader and a pool of funds being traded, a smart contract, rather than directly between trading parties. A separate class of investors that provides liquidity in the pool is called Liquidity Providers (LP), which is incentivized by awarding fees accrued on trades in proportion to the ownership of pool reserves. The CFMMs are relatively simple to implement as smart contracts and incur less gas fees than the order book based models. Unfortunately, CFFMs have significant drawbacks when compared to the order book exchange, such as high slippage, impermanent loss, and miner manipulations [35]. However, the trade-off for DEX implementation is mainly in favor of CFMMs.

B. Opportunities

The DeFi sector is still evolving and is a high-risk and high-return investment ecosystem. There exist several investment opportunities in this alternative financial system. The major ones are described below.

1) Liquidity Provider (LP): A liquidity provider (LP) is a key agent that enables the functioning of Automated Market Maker (AMM) based Decentralized Exchanges (DEX) across different blockchain platforms by providing liquidity in the form of digital tokens. A trader, another essential factor, uses the pooled liquidity to trade one pooled token with another. As an incentive to the liquidity provider, most protocols give a fixed fee specified as a percentage of the token being swapped on the platform. In addition to the fixed fee, in some pools, the liquidity providers receive additional reward tokens by either the DEX protocol governance or by the governance of one of the token contracts in the pool to attract liquidity.

2) Arbitrage: In general economic terms, arbitrage is the process of taking advantage of the price difference of an asset in different markets by buying at a lower cost from one market and selling at a higher price to another market, thus making a risk-free profit until the prices in both markets become equal, which is generally a short period. The process of arbitrage ensures the equilibrium of asset prices across all markets. Traditional markets are usually very efficient and with limited arbitrage opportunities, but the DeFi markets are still developing and provide plenty of arbitrage opportunities. The primary modus operandi of executing arbitrage is exploiting a token's price difference across different DEX platforms, which may exist due to market inefficiencies. The decentralized lending platforms' flash loan service can provide collateral-free capital required to book a profit through DEX arbitrage, which involves buying a token at a lower price from one exchange and selling it at a higher price to another exchange.

3) Liquidation Bots: As discussed in Section IV-A1 (Decentralized Borrowing/ Lending), the leading platforms like Compound and Aave have a protective mechanism called *liquidation* in place, which prevents the risk of collateral depreciating below the lent amount. When the collateral value falls below a certain predefined threshold, this mechanism allows the lending contract to sell it to any willing buyer at a discounted price to incentivize the buyer. This discount becomes an investment opportunity for the *liquidators*, as they can buy a token at lower than market prices. As per an analysis conducted by Gudgeon et al. in 2020 [25] on the *Compound* lending protocol, liquidators have become very efficient over time, with over 70 percent of liquidable positions getting immediately liquidated. This efficiency is possible due to specialized computer programs called liquidation bots, which keep parsing the state of the blockchain to look for potentially profitable liquidation opportunities and execute a liquidation transaction. The empirical study by Qin et al. [38] demonstrates algorithmic strategies, which the liquidation bots can use to make profitable liquidations across some popular decentralized lending platforms.

4) HODLing: HODLing is a general term used in cryptocurrency investment to describe a general strategy of holding the digital asset in the long run despite short-term fluctuations in its price. The investor following this strategy is called a *HOLDer*. The strong belief of HODLer is that despite the short-term volatility in price movements, the long-term trend is that price of the asset would go up. This is analogous to *value investing* in traditional finance. To compare investment strategies, one can contrast between HODLing and Liquidity provision. While a HODLer earns returns by the value appreciation in the digital asset in their custody, a liquidity provider holding the same asset can stake it in some liquidity pool and earn fees from the trades executed over the pool. Providing liquidity, however, entails an additional risk of *impermanent loss*, which is briefly explained in the next section.

C. Risks specific to DeFi

As mentioned earlier, DeFi is a high-risk and high-return ecosystem. In addition to the financial risks involved with traditional assets, trading in DeFi assets entails additional risks native to the ecosystem, as described below.

1) Bugs/Hacks: The Decentralized Finance protocols are implemented as smart contracts deployed over a Turing-complete blockchain platform. Like any other piece of code, smart contracts are vulnerable to potential bugs and hacks, and hackers can exploit a bug in a smart contract to drain investors' funds from the contract. The most famous example of a smart contract bug being exploited was *The DAO Hack,* which drained around USD 60 Million worth of Ether from *The DAO* smart contract on the Ethereum blockchain within the month of its launch in 2016. The hackers exploited the *re-entrancy vulnerability*, a design flaw in the smart contract that allowed them to recursively withdraw funds from the smart contract without updating their remaining balance. Different technical bugs might exist in smart contracts and can put the investors' funds in danger of exploitation by malicious actors. Hence, the DeFi protocols hire independent contract auditors

to check for vulnerabilities and make the finding of these audits public to increase investor confidence.

2) Miner Extractable Value (MEV): Miner Extractable Value (MEV) attacks are a risk class associated with transaction order within a block of the underlying blockchain. The risk is based on the premise that ordering transactions within a block can impact the trade returns for the transacting entity. The miner decides the transaction order, and the transactions offering higher gas prices get included on priority in the block to be mined. There are actors called *searchers* which continuously parse the *mempool* of pending transactions to find profit-making opportunities by exploiting MEV. If a profit-making transaction is found, the searcher bots create a new transaction using the identical profit-making strategy and send it to miners with more gas prices than the original transaction. This result in searchers' duplicate transaction getting mined instead of the original transaction, and the profit which was supposed to be earned by the creator of the original transaction is instead taken by the searcher. An even more serious MEV-based attack is *sandwich attack*, in which the searcher earns profit by exploiting the *slippage* in AMM-based DEX at the cost of losses incurred to the originator of the searched transaction.

3) Impermanent Loss: The Liquidity Pools (LPs) bear the risk of impermanent loss in AMM-based Decentralized Exchanges. The LPs can incur a loss due to a change in the reserve ratio of the pool resulting from a divergence in the unit price of the pool tokens. Mathematically, *impermanent loss* is the difference between the current market value of tokens that the LP initially staked in a pool and the current value of pool assets owned by the LP. The impermanent loss incurred by LP can be attributed to the profit of arbitragers who trade out the token with an increasing price in return for the token, which is losing relative value.

4) Liquidations: The liquidation risk is a risk that borrowers face in the decentralized lending protocols due to the liquidation mechanisms in these protocols. Almost all the lending protocols are over-collateralized to counter the risk of the high volatility of crypto assets. Hence, these protocols require the borrower to provide the collateral tokens with a value greater than the borrowed tokens by some minimum ratio called *liquidation threshold*. Suppose the value of collateral relative to the loan falls below this ratio. In that case, liquidation kicks in, and any third party, called a liquidator, can buy the collateral at a discounted price as described in Section IV-B3. The borrower can either add more tokens as collateral to bring it above the liquidation ratio or prepare to lose the collateral to liquidators.

5) Fraudulent Projects/Tokens: Fraudulent Projects and Tokens constitute one of the most common and gravest risks in the decentralized finance investment space. Being permissionless is one of the four key tenets of DeFi; but it is also the reason to be cautious as an investor. Since anyone with Internet access can start a new token on DeFi ecosystem without any KYC requirements and promote it as valuable on social media platforms, an investor must be able to identify frauds from genuine tokens. As per a CNBC report [39], over 10 Billion USD fraud might have occurred in DeFi space in the year 2021 alone. The most common category of DeFi scam is *rug pull,* which accounted for around 37 percent [40] of all cryptocurrency-based scams in 2021. The general scheme in conducting a rug pull starts with launching a token native to a blockchain platform, like an ERC-20 token on Ethereum. The token is then listed on a Decentralized Exchange, such as Uniswap on the Ethereum blockchain. A few days after listing, the token creator (scammer) starts marketing to generate demand for the token. As the token starts appreciating in value, the token creator adds their scam token to one or more liquidity pools and pairs it with a valuable token such as Ethereum or USDC. The marketing campaigns continue, generating demand and increasing token prices. Scammers even use incentive programs to encourage participation. For example, everyone participating in the liquidity pool gets an extra 1000 tokens per week. Once there is sufficient liquidity in the pool for the scammer to profit, the scammer sells all their scam tokens for valuable tokens, leaving other participants with only scam tokens in the pool. Another variation of the scam rug pull involves using a proxy, or upgradable, smart contracts. A scammer creates a token using a smart contract that executes code that is not immutably written on the blockchain but stored on a proxy server under the scammer's control. They follow the same marketing methodology previously described. Instead of using liquidity pools, they sell scam tokens for fiat currencies or swap them for valuable tokens. Then one day, they alter the off-chain code, and the scam token stops working, and existing holdings become worthless. It is complicated to tell a well-executed scam token apart from a genuine token. Smart contract code, publications of an independent audit report, websites, white papers, social media activity, and the individuals and companies that created the token should be thoroughly researched before investing in any new token.

6) Regulatory Risks: In all major jurisdictions worldwide, financial services come under the purview of a strict regulatory framework. This is done to protect investors from getting dumped by financial institutions. Financial regulations are necessary to create trust in the financial ecosystem and keep it running. DeFi is designed to replicate the traditional financial services over blockchain more inclusively and openly. Due to its pseudonymous identity management, it is challenging to target individuals in DeFi-related wrongdoings. Instead, regulators worldwide are increasingly inclined toward bringing DeFi services under their purview and consider developing a separate framework around DeFi services. This is evident from SEC charging Zachary Coburn, founder of EtherDelta, an order book based decentralized exchange on Ethereum, over investor fraud [41]. The primary liability under these regulations will be targeted at founders, developers and contract developers. Still, the secondary liability may come to users of protocols, thus making them potential targets of litigation. Also, in extreme cases, the regulators can choose to ban the system altogether, such as the Chinese government declaring

the use of significant cryptocurrencies and, by extension, all major DeFi services illegal [42].

V. Concluding Remarks

The introduction of new technologies could reshape the entire financial ecosystem by unleashing competitive threats to the existing players and allowing new entrants to thrive. In the future, Cryptocurrencies will further challenge cash and fiat currencies. Narrow banks that hold only liquid government bonds will challenge traditional banks built on the fractional-reserve model. Distributed payment systems like those that allow individuals to make payments through blockchains will compete with existing centralized systems anchored in physical public and private banks. Decentralized finance that removes intermediaries will test the role of traditional Wall Street giants and their law firms. To conclude, the financial ecosystem is undergoing a frenetic evolution, and when the dust settles, it could be changed beyond recognition.

Acknowledgements

The first and second authors acknowledge the Mitacs Accelerate program with Fluidefi for the internship and financial support.

References

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008, [Online]. Available: https://bitcoin.org/bitcoin.pdf, last accessed 10 May 2020.

[2] V. Buterin. Ethereum whitepaper — ethereum.org. Ethereum.org. [Online]. Available: https://ethereum.org/en/whitepaper/, last accessed 8 December 2021.

[3] S. Team. Solidity programming language. https://soliditylang.org/. [Online]. Available: https://soliditylang.org/, last accessed 8 December 2021.

[4] Binance smart chain - bsc. Binance. [Online]. Available https://dex-bin.bnbstatic.com/static/Whitepaper_\%20Binance\%20Smart\%20Chain.pdf, last accessed 8 December 2021.

[5] Cardano project. Cardano.org. [Online]. Available https://cardano.org/, last accessed 8 December 2021.

[6] Solana project. Solana. [Online]. Available https://solana.com/, last accessed 8 December 2021.

[7] Avalanche project. Avalanche. [Online]. Available https://www.avax.network/, last accessed 8 December 2021.

[8] Defi pulse - the decentralized finance leaderboard. DefiPulse. [Online]. Available https://defipulse.com/, last accessed 8 December 2021.

[9] "Fluidefi - defi investments for institutional investors." [Online]. Available: https://fluidefi.com/

[10] Governance and funding — bank of england. [Online]. Available https://www.bankofengland.co.uk/about/governance-and-funding, last accessed 8 December 2021.

[11] Federal reserve board - the fed explained. [Online]. Available https://www.federalreserve.gov/aboutthefed/the-fed-explained.htm, last accessed 8 December 2021.

[12] Financial conduct authority. FCA. [Online]. Available https://www.fca.org.uk/about, last accessed 8 December 2021.

[13] Sec.gov — what we do. U.S Securities and Exchange Commission. [Online]. Available https://www.sec.gov/about/what-we-do, last accessed 8 December 2021.

[14] U. W. Chohan, "Cryptocurrencies: A brief thematic review," *Available at SSRN 3024330*, 2017.

[15] S. Bano, A. Sonnino, M. Al-Bassam, S. Azouvi, P. McCorry, S. Meiklejohn, and G. Danezis, "Sok: Consensus in the age of blockchains," in *Proceedings of the 1st ACM Conference on Advances in Financial Technologies*, 2019, pp. 183–198.

[16] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, "Sok: Research perspectives and challenges for bitcoin and cryptocurrencies," in *2015 IEEE symposium on security and privacy*. IEEE, 2015, pp. 104–121.

[17] N. Szabo, "Formalizing and securing relationships on public networks," *First Monday*, vol. 2, no. 9, 1997.

[18] Gas and fees — ethereum.org. [Online]. Available https://ethereum.org/en/developers/docs/gas/#top, last accessed 8 December 2021.

[19] "Aave v2 whitepaper," Dec 2020. [Online]. Available: https://github.com/aave/protocol-v2/blob/master/aave-v2-whitepaper.pdf

[20] R. Leshner and G. Hayes, "Compound:the money market protocol," Feb 2019. [Online]. Available: https://compound.finance/documents/Compound.Whitepaper.pdf

[21] H. Adams, N. Zinsmeister, M. Salem, R. Keefer, and D. Robinson, "Uniswap v3 core," 2021.

[22] "Sushiswap, 2020. sushiswap staking," Dec 2020. [Online]. Available: https://docs.sushi.com/

[23] L. Kugler, "Non-fungible tokens and the future of art," *Communications of the ACM*, vol. 64, no. 9, pp. 19–20, 2021.

[24] S. Mishkin Frederic, "The economics of money, banking and financial markets," *Mishkin Frederic–Addison Wesley Longman*, 2004.

[25] L. Gudgeon, S. Werner, D. Perez, and W. J. Knottenbelt, "Defi protocols for loanable funds: Interest rates, liquidity and market efficiency," in *Proceedings of the 2nd ACM Conference on Advances in Financial Technologies*, ser. AFT '20. New York, NY, USA: Association for Computing Machinery, 2020, p. 92–112.

[26] M. Foundation, "The maker protocol: Makerdao's multi-collateral dai (mcd) system." [Online]. Available: \url{https://makerdao.com/da/whitepaper/}

[27] A. Finance, "Alpha homora v2." [Online]. Available: https://alphafinancelab.gitbook.io/alpha-finance-lab/alpha-products/3.-alpha-homora-v2-on-ethereum

[28] D. Wang, S. Wu, Z. Lin, L. Wu, X. Yuan, Y. Zhou, H. Wang, and K. Ren, "Towards a first step to understand flash loan and its applications in defi ecosystem," in *Proceedings of the Ninth International Workshop on Security in Blockchain and Cloud Computing*, 2021, pp. 23–28.

[29] D. e. a. Wang, "Towards a first step to understand flash loan and its applications in defi ecosystem," in *Proceedings of the Ninth International Workshop on Security in Blockchain and Cloud Computing*, ser. SBC '21. New York, NY, USA: Association for Computing Machinery, 2021, p. 23–28.

[30] N. G. Mankiw, *Essentials of economics*. Cengage learning, 2020.

[31] P. Tasca, "The dual nature of bitcoin as payment network and money," in *VI Chapter SUERF Conference Proceedings*, vol. 1, 2016.

[32] G. Hileman, "State of stablecoins (2019)," *Available at SSRN 3533143*, 2019.

[33] e. a. Klages-Mundt, "Stablecoins 2.0: Economic foundations and risk-based models," in *Proceedings of the 2nd ACM Conference on Advances in Financial Technologies*, 2020, pp. 59–79.

[34] D. e. a. Bullmann, "In search for stability in crypto-assets: are stablecoins the solution?" *ECB Occasional Paper*, no. 230, 2019.

[35] A. Gervais, "Decentralized exchanges (dex)," Sep 2021. [Online]. Available: https://berkeley-defi.github.io/assets/material/Updated\%20Lecture\%205\%20Slides.pdf

[36] A. M. Othman, "Automated market making: Theory and practice," Jun 2018. [Online]. Available: https://kilthub.cmu.edu/articles/thesis/Automated_Market_Making_Theory_and_Practice/6714920/1

[37] G. Angeris and T. Chitra, "Improved price oracles," *Proceedings of the 2nd ACM Conference on Advances in Financial Technologies*, Oct 2020. [Online]. Available: http://dx.doi.org/10.1145/3419614.3423251

[38] K. Qin, L. Zhou, P. Gamito, P. Jovanovic, and A. Gervais, "An empirical study of defi liquidations: Incentives, risks, and instabilities," *arXiv preprint arXiv:2106.06389*, 2021.

[39] T. Locke, "Over $10 billion was stolen in defi-related theft this year. here's how to protect yourself from common crypto scams," Dec 2021. [Online]. Available: https://www.cnbc.com/2021/12/14/common-defi-crypto-related-scams-and-how-to-protect-your-wallet.html

[40] S. Malwa, "Defi 'rug pull' scams pulled in $2.8b this year: Chainalysis," Dec 2021. [Online]. Available: https://www.coindesk.com/markets/2021/12/17/defi-rug-pull-scams-pulled-in-28b-this-year-chainalysis/

[41] "In the matter of zachary coburn, respondent. administrative proceeding file no. 3-18888," *Release No. 84553 / November 8, 2018*. [Online]. Available: https://www.sec.gov/litigation/admin/2018/34-84553.pdf

[42] J. Riley, "The current status of cryptocurrency regulation in china and its effect around the world," *China and WTO Review*, vol. 7, no. 1, pp. 135–152, 2021.