Smart Contracts and Decentralized Finance

Kazi Abrar Hossain

The Leonard N. Stern School of Business

Glucksman Institute

Faculty Advisor: Dr. Kose John

April 2024

Abstract

This paper examines decentralized finance (DeFi) and its comparison to traditional financial systems. We analyze DeFi's growth from early experiments to a $120 billion ecosystem measured in total value locked by 2024. The paper first introduces DeFi infrastructure components including blockchains, smart contracts, stablecoins, and oracles. We then explain DeFi primitives that serve as building blocks for complex financial applications.

Our analysis includes detailed case studies of three protocols. We examine Compound (lending), Uniswap (exchange), and MakerDAO (stablecoin issuance). Each case study explores operational structures, target users, and traditional finance equivalents.

We identify significant technical vulnerabilities in DeFi, from smart contract exploits to oracle manipulations. Economic risks including liquidity fragmentation and governance attacks are also analyzed. The paper evaluates computational efficiency and economic trade-offs in DeFi. We assess welfare implications for both individual users and the broader financial system. Despite limitations like overcollateralization and technical complexity, DeFi offers benefits through programmability and permissionless access. The paper concludes by discussing regulatory challenges and identifying key research questions for DeFi's future development.

1. Introduction

Decentralized Finance (DeFi) introduced a fundamental shift in financial services through the application of blockchain technology and smart contracts. Traditional financial (TradFi) systems depend on centralized intermediaries like banks, exchanges, and clearinghouses. On the contrary, the core innovation in DeFi lies in its ability to extend financial services without requiring trusted intermediaries like its traditional counterpart. DeFi applications function through self-executing codes on blockchain networks that automatically enforce predetermined rules without human intervention. This is achieved through smart contracts, which were conceptualized by Szabo (1997) and implemented at scale with the launch of the Ethereum's Turing complete smart contracts in 2015. Since then, DeFi evolved from early experiments like EtherDelta (2017) and 0x Protocol (2017) into a robust ecosystem of Automated Market Makers (AMM), lending pools, and synthetic asset platforms.

DeFi has experienced rapid growth in recent years. Total Value Locked (TVL), which measures the total assets committed to DeFi protocols, grew from under $0.6 billion in January 2020 to over $120 billion by December 2024 (Anon., 2025). This explosive growth reflects increasing confidence in DeFi protocols and their potential to transform financial services. During peak periods in November 2021, DeFi's TVL approached $180 billion which demonstrates the substantial capital allocations to this emerging sector despite its nascent stage.

Despite its impressive growth, DeFi's promise of decentralization faces practical constraints. Complex mechanisms to ensure security and economic viability in the absence of trusted intermediaries can introduce inefficiencies. Blockchain limitations such as throughput constraints create scalability challenges and can generate high transaction costs during periods of network congestion. To address these limitations, Ethereum Layer-2 (L2) blockchains such as rollups and sidechains have emerged critical scaling solutions. The programmable nature of DeFi also introduces novel attack vectors and security vulnerabilities absent in TradFi.

The economic implications of DeFi also extend beyond technological considerations. DeFi protocols can potentially enhance financial inclusion, reduce costs, and increase market efficiency by removing traditional intermediaries. However, such benefits must be balanced against the increased responsibility placed on users and the systemic risks that may emerge from interconnected financial protocols operating with limited regulatory oversight.

In this paper, we will discuss the current landscape of DeFi protocols, evaluate their effectiveness in comparison to traditional financial systems, and assess the various risks and challenges they face. After discussing the DeFi primitives and types of services provided by DeFi protocols, we will examine three categories of DeFi applications:

(i) lending and borrowing protocols (PLFs), (ii) decentralized exchanges (DEXs), and (iii) stablecoins. We will analyze the operational structures, economic implications, and comparative advantages of these applications. We will further discuss the security vulnerabilities, economic risks, and regulatory challenges that could impact DeFi's evolution and acceptance.

2. DeFi Infrastructure

DeFi applications rely on several infrastructure components (Harvey, et al., 2021) that enable decentralized financial services. The following infrastructure components combine to create a robust foundation for the expanding DeFi ecosystem, enabling everything from decentralized exchanges to lending protocols and asset management tools.

2.1. Blockchain

Blockchain is the backbone of all DeFi applications as it allows multiple parties to operate under shared assumptions without requiring mutual trust (John, et al., 2023). The underlying blockchain powering DeFi applications depend on consensus protocols to coordinate agreement across distributed participants. John and Saleh (2025) characterize these protocols as economic mechanisms that enable coordination among an arbitrarily large set of entities regarding transaction settlement. Consensus mechanisms maintain blockchain integrity by determining which blocks become part of the chain. Bitcoin and initially Ethereum used Proof of Work (PoW), where miners solve computational puzzles to validate transactions. Ethereum's transition to Proof of Stake (PoS) marked a shift toward energy efficiency, with validators committing cryptocurrency as collateral to attest block validity (John, et al., 2022). John and Saleh (2025) provide insights into blockchain’s settlement capabilities. They define settlement as consensus on transaction inclusion among validators. This settlement process requires two protocol types. Validation selection protocols determine who proposes blocks whereas chain selection protocols determine which chain is legitimate. Their research suggests that PoS may deliver higher equilibrium security. These settlement mechanisms form the foundation for all DeFi applications. Without the settlement mechanisms, even simple payments would be impossible. Complex financial operations would be entirely unattainable.

2.1.1. Layer-1 Blockchain

Layer-1 (L1) blockchains refer to the base protocol layer of a blockchain network, such as Bitcoin or Ethereum. These networks are responsible for the core functions of consensus, data availability, and transaction settlement. Layer-1 blockchains typically process all transactions directly on-chain, which ensures high security and

decentralization. However, this also results in limited throughput and higher transaction fees during periods of congestion.

2.1.2. Layer-2 Blockchain

Layer-2 (L2) blockchains are protocols or networks built on top of Layer-1 blockchains to improve scalability and reduce transaction costs. Although Ethereum's PoS consensus improves energy efficiency, its L1 throughput remains constrained. Ethereum L2 blockchains address this by processing transactions chain or in bundled batches and periodically settling proofs on Ethereum L1. This approach allows for significantly higher transaction throughput and lower fees, while still inheriting security guarantees of the underlying L1 blockchain. Common L2 architecture includes rollups and sidechains. A discussion of Ethereum's L2 blockchains is provided in section 9.1.

2.2. Smart Contract Platforms

Smart contracts expanded blockchain utility for financial applications. As defined by John, Kogan & Saleh (2023), smart contracts are "computer code uploaded to a blockchain" consisting of state variables and functions. These self-executing programs enable complex financial operations without intermediaries. Ethereum, the predominant smart contract platform for DeFi, requires "gas fees" for transaction execution. These fees compensate validators and prevent system attacks by making resource-intensive operations prohibitively expensive (John, et al., 2024). Standard interfaces like ERC-20 (for fungible tokens) and ERC-721 (for non-fungible tokens) enable seamless interaction between applications, enhancing the composability of the DeFi ecosystem (John, et al., 2023). Smart contracts function as commitment devices for decentralized applications. John and Saleh (2025) analyze smart contracts in the context of blockchain-based business applications. Their analysis explains how validator consensus on deployed code enables credible commitment to programmed terms. This in turn allows DeFi protocols to implement trustless financial arrangements that would be difficult or impossible in TradFi.

2.3. Stablecoins

Stablecoins maintain stable value relative to reference assets like the US dollar to address price volatility of cryptocurrencies. Stablecoins enable users to benefit from DeFi applications without exposure to cryptocurrency volatility (John, et al., 2024). The three main types of stablecoins are:

- **Fiat-Collateralized Stablecoins** (e.g., USDC): Backed by fiat currency reserves held by centralized entities.
- **Crypto-Collateralized Stablecoins** (e.g., DAI): Maintain their peg through overcollateralization with cryptocurrencies, offering greater decentralization but facing scalability limitations.

- **Algorithmic Stablecoins**: Attempt to maintain their peg through algorithmic supply adjustments without direct collateralization, though these have proven vulnerable during market stress.

2.4. Oracles

Since blockchains are isolated from external information, oracles serve as bridges that feed off-chain data into smart contracts. Solutions like Chainlink aggregate multiple data sources to provide reliable information while minimizing trust assumptions (John, et al., 2023). Oracles enable critical DeFi functions like price feeds for lending protocols, settlement data for derivatives, and real-world event outcomes for prediction markets.

2.5. Decentralized Applications (dApps)

The front-end interfaces for most DeFi services are decentralized applications (dApps). dApps operate on smart contract platforms with their logic publicly verifiable on the blockchain. This ensures permissionless access and censorship resistance, allowing anyone to use them without requiring approval from a central authority (Halaburda, et al., 2022).

3. DeFi Primitives

Decentralized Finance (DeFi) applications are constructed from fundamental components or "primitives" that enable complex financial interactions without intermediaries. These primitives serve as the basic building blocks for decentralized financial applications. This section explores the core DeFi primitives, their functionality, and economic implications.

3.1. Transactions

Transactions represent the atoms of DeFi infrastructure and are the fundamental unit of activity on blockchain networks like Ethereum. Every interaction in DeFi from token transfers to complex financial operations begins with a transaction (John, et al., 2023). Ethereum transactions possess two essential properties:

- **Atomicity:** Transactions either complete entirely or revert completely. If any step in a multi-step transaction fails, all prior steps are reversed.
- **Gas Fees:** Users pay fees based on the computational complexity of their transactions. Higher complexity transactions require more gas and thus cost more.

Transactions are initially posted to a memory pool ("mempool") before being included in a block. This creates potential information asymmetries that sophisticated actors can exploit through strategies like front-running

(Capponi, et al., 2024). John, Rivera, and Saleh (2024) suggest that transaction costs will likely decrease as technology improves.

3.2. Fungible Tokens

Fungible tokens represent interchangeable digital assets where each unit is identical. On Ethereum, the ERC-20 standard defines the interface for fungible tokens, enabling applications to interact consistently with any token that implements this standard (John, et al., 2023). Fungible tokens can be categorized into three main types:

- **Equity Tokens:** These tokens represent ownership of an underlying asset or pool of assets. They provide holders with a claim on the value of the underlying assets and potentially their returns. Examples include lending protocol tokens like Compound's cTokens (John, et al., 2023).
- **Utility Tokens:** These tokens provide access to specific functionality within a protocol. These tokens often drive the economics of a system by creating scarcity or incentive mechanisms. Examples include stablecoins like DAI, collateral tokens like SNX, or oracle tokens like LINK. As Roşu and Saleh (2021) note, these tokens can serve as both investment vehicles and functional components of blockchain systems.
- **Governance Tokens:** These tokens confer voting rights over protocol parameters, features, and treasury funds. They allow holders to participate in decentralized governance through a system often referred to as a Decentralized Autonomous Organization (DAO). Prominent examples include MKR for MakerDAO and COMP for Compound. John, Rivera and Saleh (2021) highlight that governance tokens are essential for enabling protocols to adapt to changing economic or technical conditions without relying on centralized control.

3.3. Non-Fungible Tokens (NFTs)

Unlike fungible tokens, non-fungible tokens (NFTs) represent unique assets where each token has distinct characteristics and is not interchangeable with others. On Ethereum, the ERC-721 standard establishes the interface for NFTs (John, et al., 2023). The applications of NFTs in DeFi include ownership of unique financial assets, tokenized real-world assets, and verifiable digital scarcity for collectible assets.

3.4. Custody

Custody in DeFi refers to how assets are held by smart contracts. In TradFi, assets are held by trusted custodians whereas DeFi allows for programmatic control of assets through smart contracts (Saleh, 2021). The custody mechanism enables features like fee retention, incentive distribution, token swaps, market making. When a user transfers tokens to a contract, the contract holds full custody until conditions for release are met. This allows

financial arrangements to get executed automatically without intermediaries. However, current literature suggests the limitation of smart contracts in replacing traditional legal agreements as enforcement requires actions beyond what can be verified on chain (John, et al., 2023).

3.5. Supply Adjustment

Supply adjustment mechanisms allow for dynamic management of token supplies. The two mechanisms of supply adjustment are burning and minting. Minting increases the number of tokens in circulation and burning reduces the supply of tokens in circulation. Minting new tokens to reward users has become a popular strategy known as "yield farming," which incentivizes liquidity provision and platform usage. The mathematical relationship between token supply and price is established by bonding curves. Bonding curves define how token prices change as supply changes. As Halaburda et al. (2022) note, such price mechanisms are essential for providing liquidity in decentralized systems where traditional market makers are absent.

3.6. Incentives

Incentive structures are crucial for guiding user behavior in DeFi systems. These mechanisms encourage desired actions and discourage undesirable ones. Staking rewards provides positive incentives for users who commit capital to a protocol. These rewards can be applied to all staked balances or only those meeting specific criteria. Distribution of staking rewards can also be on a fixed or pro-rata basis with the reward paid in either the same token that was staked or a different token. For example, Compound rewards users who provide liquidity with COMP tokens, while Synthetix rewards SNX stakers with additional SNX from inflation. Inversely, **s**lashing creates negative incentives by removing a portion of a user's staked balance when they violate protocol rules or when certain conditions are met. The most common slashing scenario is a liquidation event due to under-collateralization. Slashing can also be used for supply contractions triggered by market conditions. Saleh (2021) explains that in PoS systems, slashing serves as an important security mechanism by imposing financial costs on those who attempt to undermine the protocol. A third type of incentive is direct rewards, which incentivizes specific user actions without requiring staked balances. Keepers serve as external actors incentivized to perform maintenance functions like liquidating undercollateralized positions. As John et al. (2024) explain, this creates additional economic roles within the ecosystem. Finally, **f**ees provide funding for protocol operations and can influence user behavior. Due to the pseudonymous nature of blockchain addresses, fees in DeFi are typically backed by on-chain collateral to ensure enforcement.

3.7. Swap Mechanisms

Swaps allow users to exchange one token for another. DeFi swaps are atomic (either complete entirely or not at all) and non-custodial (funds remain in user control until the exchange is finalized). Decentralized Exchanges often facilitate non-custodial token swapping. There are two mechanisms of maintaining liquidity in Decentralized Exchanges. Order-book matching systems require parties to agree on exchange rates before executing trades. This approach is like the TradFi exchange model and thus faces challenges around efficiency on blockchains. AMMs can resolve the efficiency challenge by using smart contracts that hold assets on both sides of trading pairs and quote prices based on predetermined formulas. This allows for guaranteed liquidity for smart contract interactions. However, AMMs face a challenge known as impermanent loss. Impermanent loss is the opportunity cost difference between providing liquidity versus holding underlying assets. Park (2021) demonstrates that certain AMM designs can create predictable arbitrage opportunities that must be balanced against trading fees.

3.8. Collateralized Loans

Lending mechanisms enable capital allocation and leverage in DeFi ecosystem. In permissionless systems, loans typically require overcollateralization to mitigate default risk. Collateralized lending relies on collateralization ratios, liquidation mechanisms for undercollateralized positions, and incentives for external keepers to manage risk. John, Kogan, and Saleh (2023) explain that borrowing on a DeFi platform is limited to assets that are directly settled on the blockchain. This restriction exists because blockchains can only verify on-chain assets and off-chain assets must be tokenized before they can be used as collateral. Collateralized loans also help create synthetic assets or tokens backed by collateral that track the price of an underlying asset (for example, MakerDAO's DAI stablecoin).

3.9. Flash Loans

Flash loans are a financial primitive unique to DeFi. They are uncollateralized loans that must be borrowed and repaid within a single transaction. Flash loans eliminate counterparty risk since the transactions revert in case of non-repayment of loans. These loans also do not have any collateral requirements and allow instant execution for efficient financial operation. Flash loans can be used to design sophisticated strategies like arbitrage, liquidations, and collateral swaps without requiring significant initial capital. As Capponi and Jia (2021) note, these innovations have no direct parallel in traditional finance and represent novel financial structures made possible by the atomic transaction properties of blockchain technology.

4. Review of Literature

4.1. Theoretical Foundation

The literature on smart contracts has developed rapidly in recent years. John, Kogan, and Saleh (2023) provide a comprehensive framework for understanding the economic implications of smart contracts. In the paper, the authors highlight that smart contracts can implement certain contingent outcomes that would otherwise be precluded due to credible commitment problems. The authors also note that "a user can overcome an inability to credibly commit to a contingent action by deploying a smart contract with a function that executes the desired action if the desired contingency is realized" (John, et al., 2023, p. 525). However, they also identify crucial limitations of smart contracts, particularly regarding the set of events on which they can condition and the outcomes they can implement. One of the major constraints of smart contracts is the “Oracle Problem.” This relates to smart contracts' inability to directly access external data and need for intermediary mechanisms known as oracles to provide external data to the blockchain. This constraint limits the complexity of conditional agreements that can be effectively implemented through smart contracts without introducing new centralization vectors. Cong and He (2019) expand on these concepts by demonstrating that smart contracts can enable high-quality entrant firms to enter markets when information asymmetry regarding the entrant's type would otherwise preclude such entries. They explain that a high-quality entrant can offer a contract where payment is made only upon successful delivery. This approach helps address information asymmetry (Cong & He, 2019). However, they also emphasize that smart contracts can facilitate anti-competitive behaviors such as collusion between incumbent firms.

4.2. Economics of DeFi Protocols

DeFi represents a practical application of cryptoeconomics, which can be defined as the economic analysis of blockchain technology. John and Saleh (2025) categorize cryptoeconomics into two distinct sub-fields: (i) the study of economic mechanisms ensuring transaction settlement through consensus protocols, and (ii) the analysis of business applications deployed on blockchain infrastructure. Their framework highlights how smart contracts enable commitment to business policies by leveraging the immutability guaranteed by functioning consensus protocols. The economics of DeFi protocols has also been examined from various perspectives. John, O'Hara, and Saleh (2022) explore the economic foundations of blockchain systems with a focus on consensus mechanism. Their analysis highlights how economic incentives shape the security properties of blockchain networks and establish the foundation for understanding the platforms on which DeFi operates. They emphasize a fundamental tension between

security requirements and economic efficiency that underlies many issues addressed in the literature. John, Kogan, and Saleh (2023) also analyze specific DeFi applications with a focus on token issuance, DEXs, and PLFs. Their framework illuminates how these protocols function and the relevant economic trade-offs. For DEXs, they question whether these platforms can sustain as alternatives to centralized exchanges over the long term.

Halaburda et al. (2022) provide a comprehensive framework for analyzing the microeconomics of cryptocurrencies by examining supply and demand sides of cryptocurrency markets. On the supply side, they analyze the process of mining and transaction validation to demonstrate how incentives embedded in protocols influence miner behavior. They emphasize that "a blockchain entails redundant computation by design, and each individual computation entails a nonzero cost so that the redundancy implies a commensurate increase in execution costs" (Halaburda, et al., 2022, p. 982). This inherent cost structure shapes the economics of cryptocurrency networks and impacts the scalability of DeFi applications built on them.

In their microeconomic model of block fee markets, Easley, O'Hara, and Basu (2019) demonstrate how transaction fees emerge as an equilibrium outcome of interactions between users and miners. Huberman, Leshno, and Moallemi (2021) further characterize blockchain fee markets as monopolistic systems despite the absence of a centralized monopolist. Their analysis reveals how congestion is necessary for the economic sustainability of blockchains and the inherent tension between system capacity and fee generation.

Xu and Xu (2021) provide a systematic analysis of DeFi business models. This paper also classifies DeFi protocols according to their service types. They identify that PLFs like Compound and Aave generate revenue through interest rate spreads whereas DEXs like Uniswap earn through transaction fees. Their analysis shows that protocol treasuries have grown alongside market capitalization with varying correlation strengths across protocol types.

John et al. (2024) examine the economic incentives within Ethereum's ecosystem. Their paper focuses particularly on the participants in the transaction lifecycle. They explain how users submit transactions with fees that incentivize inclusion in blocks, and how proposers and attesters coordinate to add these blocks to the blockchain. Their analysis of the Ethereum ecosystem reveals how economic incentives align to maintain the blockchain's integrity while allowing participants to extract value.

4.3. Risks and Limitations

The literature has also identified several limitations and risks associated with DeFi. Security vulnerabilities in smart contracts have received extensive attention in literature. Atzei, Bartoletti, and Cimoli (2017) provide a taxonomy of

vulnerabilities in Ethereum smart contracts by identifying attack vectors that have resulted in financial losses. Qin et al. (2022) document how implementation flaws in DeFi protocols have led to substantial losses through exploitation of flash loan mechanisms. Park (2021) examines design flaws in AMMs to demonstrate how constant product AMMs like Uniswap enable profitable front-running. Capponi and Jia (2021) show that DEXs may experience liquidity freeze during periods of high asset volatility. Extreme exchange rate volatility generates arbitrage opportunities that create losses for liquidity providers and can discourage liquidity provision.

John, Kogan, and Saleh (2023) identify economic limitations arising from the need for collateral and from redundant validator behavior. Implementation of contingent payments through smart contracts creates opportunity costs as they require funds to be held outside the control of both parties until the contingent event occurs. Additionally, the trustless design of blockchains necessitates redundant computation and storage which increases execution costs compared to centralized systems.

4.4. Comparison of TradFi and DeFi Models

Traditional finance models are typically built around trusted intermediaries that centralize risk management, provide liquidity, and enforce contractual agreements. Allen and Santomero (1997) characterize financial intermediaries as risk managers and information processors who reduce transaction costs and information asymmetries. In contrast, DeFi protocols aim to replicate these functions through algorithmic mechanisms and incentive structures embedded in smart contracts. Diamond and Dybvig's (1983) classic model of banking highlights the fundamental economic role of financial intermediaries in maturity transformation and liquidity provision. Traditional banks transform short-term deposits into long-term loans while managing liquidity risk through reserves and institutional support structures. DeFi lending protocols attempt to replicate this function but face unique challenges in managing liquidity without centralized control. The comparative efficiency of DeFi versus TradFi remains an evolving area of research. Barbon and Ranaldo (2021) compare transaction costs between centralized and decentralized exchanges. Their findings indicate that centralized exchanges generally offer lower costs but DEXs can be competitive in certain market segments. They note that the main component of trading costs for DEX arise from fees paid to blockchain validators rather than the direct costs associated with DEX. John et al. (2024) also observe in their analysis of Ethereum economics that the infrastructure supporting DeFi applications introduces economic constraints that do not exist in TradFi. The costs associated with blockchain consensus mechanism and the economic incentives required to maintain security create structural inefficiencies that must be overcome for DeFi to achieve competitive parity with

centralized alternatives. John et al. (2023) also observe that PLFs require all borrowing to be overcollateralized which limits the types of economic activity they can support compared to traditional lending. As physical assets cannot be used as collateral in DeFi, lending is restricted to activities like leveraged trading and short selling of cryptocurrencies rather than traditional small business financing. The research identifies significant barriers to entry including technical requirements, verification processes, and transaction costs that may limit DeFi's ability to serve populations excluded from TradFi.

5. Classification of DeFi Protocol

Decentralized Finance encompasses a diverse ecosystem of financial applications built on blockchain infrastructure. These applications can be categorized based on financial functions traditionally performed by TradFi.

5.1. Lending and Borrowing Protocols

Lending and borrowing protocols, often referred to as Protocols for Loanable Funds (PLFs), enable permissionless lending and borrowing without requiring trust between counterparties. These protocols use smart contracts to manage collateral, interest rates, and liquidations automatically. PLFs operate by creating lending pools for specific assets where lenders provide liquidity in exchange for interest. Borrowers can access these funds by posting collateral. Rather than using credit checks or identity verification used in TradFi, PLFs rely on overcollateralization to manage default risk. Leading protocols in this category include Aave and Compound, which collectively account for a significant portion of DeFi's TVL ($49 billion as of December 2024). These protocols differ in their specific implementations, governance structures, and risk parameters. However, they all share the fundamental approach of using smart contracts to automate lending operations. John and Saleh (2025) analyze decentralized lending protocols as commitment devices for borrowing terms. They note that these protocols enable borrowing and lending without intermediaries by creating credible commitments through immutable smart contract codes. Their frameworks emphasized overcollateralization as a condition given blockchain’s pseudo-anonymous nature which prevents traditional credit assessment. This analysis reinforces why PLFs fundamentally differ from traditional lending institutions not just in operation but in their underlying economic structure.

5.2. Decentralized Exchanges

Decentralized Exchanges enable peer-to-peer trading of digital assets without intermediary custody of funds. DEXs facilitate direct trades between user wallets through AMM. The most prominent DEXs are Uniswap, SushiSwap, and Curve Finance. These DEXs have pioneered various AMM models optimized for different trading scenarios. The

platforms have also transformed cryptocurrency trading by reducing counterparty risk, KYC requirements, and enabling permissionless listing of new assets. DEXs generate revenue through trading fees, typically charging between 0.05% and 0.3% per transaction. These fees are distributed between liquidity providers (who supply the assets that traders exchange) and protocol treasuries (which fund ongoing development and governance). The economic structure of DEXs is analyzed by John and Saleh (2025) where they identify DEXs as sets of smart contracts that custody digital assets as inventory. Their framework distinguishes between order-book model and AMMs with regards to the challenges in providing continuous liquidity without traditional market makers. The analysis also explains why DEXs have innovated beyond traditional exchange models by creating mechanisms like liquidity pools with programmatic pricing formulae.

5.3. Stablecoins and Synthetic Assets

Stablecoins represent the crucial bridge between TradFi and DeFi ecosystem as they provide price stability in an otherwise volatile market. These tokens are designed to maintain a peg to another asset (typically the US dollar) through various stabilization mechanisms. DeFi-native stablecoins include DAI (created by MakerDAO), which maintains its peg through overcollateralized cryptocurrency positions, and algorithmic stablecoins like Frax Finance, which use dynamic mechanisms to balance supply and demand without full collateralization. Synthetic assets extend beyond stablecoins to create blockchain-based representations of real-world assets. This allows investors to gain exposure to stocks, commodities, and other traditional investments without requiring direct ownership. Protocols like Synthetix and Mirror Protocol have pioneered this category although they face ongoing scaling challenges.

5.4. Yield Farming and Staking

Yield farming represents investment strategies to maximize returns from crypto assets through complex interactions with multiple DeFi protocols. Users provide liquidity or stakes to protocols in exchange for rewards (primarily, governance tokens). Notable yield farming platforms include Yearn and Convex Finance. Yearn automates yield optimization strategies across multiple protocols and Convex specializes in optimizing returns from the Curve ecosystem. The mechanics of yield farming frequently involve staking tokens in liquidity pools or governance systems. These mechanisms incentivize network participation by providing returns to asset holders.

5.5. Insurance and Risk Management

As DeFi has matured, specialized insurance and risk management protocols have emerged to address the unique risks of smart contract interactions. These protocols provide coverage against technical failures, hacks, and other

DeFi-specific risks that traditional insurance products do not address. Prominent examples include Nexus Mutual and Unslashed Finance. Nexus offers smart contract cover through a risk-sharing pool and Unslashed provides parametric insurance for specific DeFi failure scenarios. These protocols typically operate through decentralized risk pools where participants stake assets to cover potential claims while earning premiums.

6. Case Study: Analysis of Three DeFi Protocols

To provide deeper insight into the mechanics and economics of DeFi, we analyze three representative protocols: Compound (lending), Uniswap (exchange), and MakerDAO (stablecoin issuance). These protocols exemplify different approaches to DeFi service provision and have established significant market presence.

6.1. Compound: Protocol for Loanable Funds

Service Provided: Compound is a protocol for algorithmic, permissionless interest rate markets. It enables users to supply assets to liquidity pools and earn interest. It also enables users to borrow assets by posting sufficient collateral. Interest rates adjust algorithmically based on the utilization ratio of each asset pool and is correlated to demand-supply gap in borrowing needs.

User Example: A user holds 10 ETH but requires USDC for a temporary expense without selling their ETH position. Using Compound, the user can deposit their 10 ETH as collateral (valued at approximately $30,000 at December 2024 price) and borrow up to 75% of this value in USDC (approximately $22,500), paying a variable interest rate determined by market conditions. The user maintains ownership of their ETH while accessing liquidity. If their collateral value drops below the required threshold, their position may be liquidated.

Target Users: Compound targets the following user segments:

- Asset holders seeking passive income by supplying liquidity to markets
- Traders needing leverage or liquidity without selling their assets
- Arbitrageurs exploiting interest rate differentials across platforms
- Sophisticated DeFi users engaging in complex yield-generating strategies

Blockchain novices are unlikely to use Compound directly due to its technical complexity, gas fees, and lack of user-friendly interfaces. However, they may access it indirectly through centralized services that integrate with Compound's protocols.

TradFi Equivalent: Compound functionally resembles margin lending in traditional finance where securities serve as collateral for loans. However, some of the major differences between Compound and margin lending are:

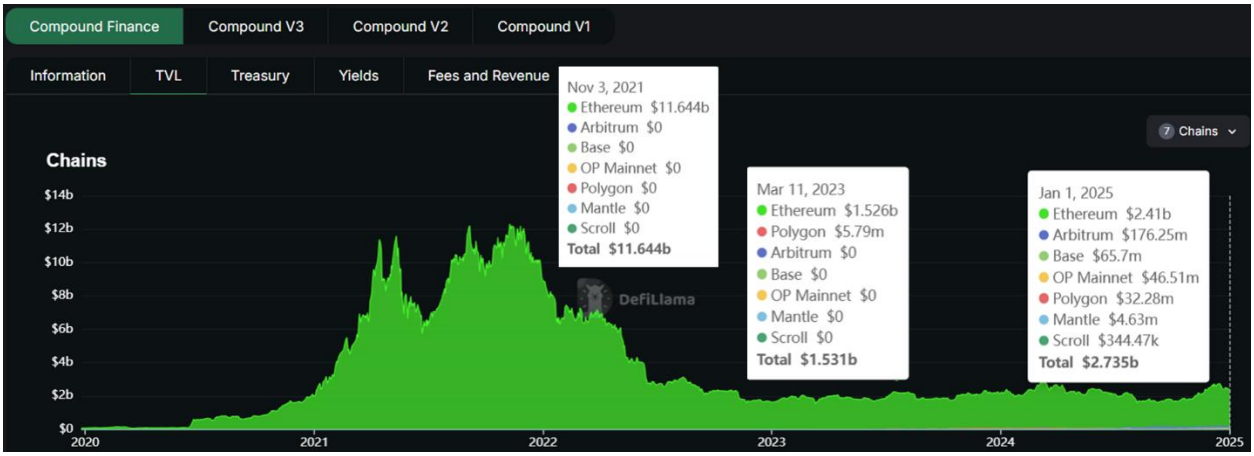
- Permissionless access without credit checks or identity verification
- Overcollateralization requirements (typically 125-175%) versus traditional margin requirements (50-100%)
- Algorithmic interest rate determination without administrative discretion
- Immediate liquidation through smart contracts rather than margin calls with human intervention
- No rehypothecation of collateral in Compound which is allowed in traditional securities lending

Traditional banks operate with reserves supporting uncollateralized lending whereas Compound requires overcollateralization for all loans. This restricts capital efficiency but eliminating credit risk.

TVL Trends: As of December 2024, Compound had approximately $2.7 billion in total value locked. Although this represents some recovery from lows of around $1.5 billion in 2023, it is still below its all-time high of over $11.6 billion reached in November 2021. TVL fluctuations correlate strongly with overall cryptocurrency market conditions as we can observe sharp increases during bull markets and contractions during bear markets.

The distribution of assets within Compound is heavily weighted toward stablecoins. This reflects user preference for borrowing volatile assets against stable collateral to minimize liquidation risk.

Figure 1: TVL of Compound (2020 – 2024)



6.2. Uniswap: Decentralized Exchange

Service Provided: Uniswap is a decentralized exchange protocol that enables permissionless token swaps through AMM. Rather than using order books, Uniswap uses liquidity pools containing pairs of assets, with prices determined by the constant product formula ($x \times y = k$, where x and y represent the quantities of the two assets and k is a constant).

User Example: A user wishes to exchange 1 ETH for USDC. Instead of using a centralized exchange requiring account registration and identity verification, they can connect their wallet to Uniswap's interface and execute the trade directly. The protocol determines the exchange rate based on the ratio of ETH to USDC in the liquidity pool, applies a 0.3% fee, and executes the swap atomically. The user receives approximately 3,000 USDC (assuming December 2024 rates) without custody ever transferring to a third party.

Target Users: Uniswap serves the following user groups:

- Traders seeking to exchange tokens without centralized intermediaries
- Liquidity providers investing in pools to earn trading fees
- Token projects launching new assets without centralized exchange listing requirements
- DeFi applications requiring on-chain liquidity for various operations

Although Uniswap's web interface is relatively user-friendly, blockchain novices still face significant barriers to entry. These barriers include wallet setup, gas fees, and understanding price impact in AMM systems. Integration with more user-friendly front-end applications has expanded accessibility but direct usage remains concentrated among cryptocurrency natives.

TradFi Equivalent: Uniswap most closely resembles electronic communication networks (ECNs) in traditional finance, which facilitate direct trading between market participants. However, following are some of the key differences:

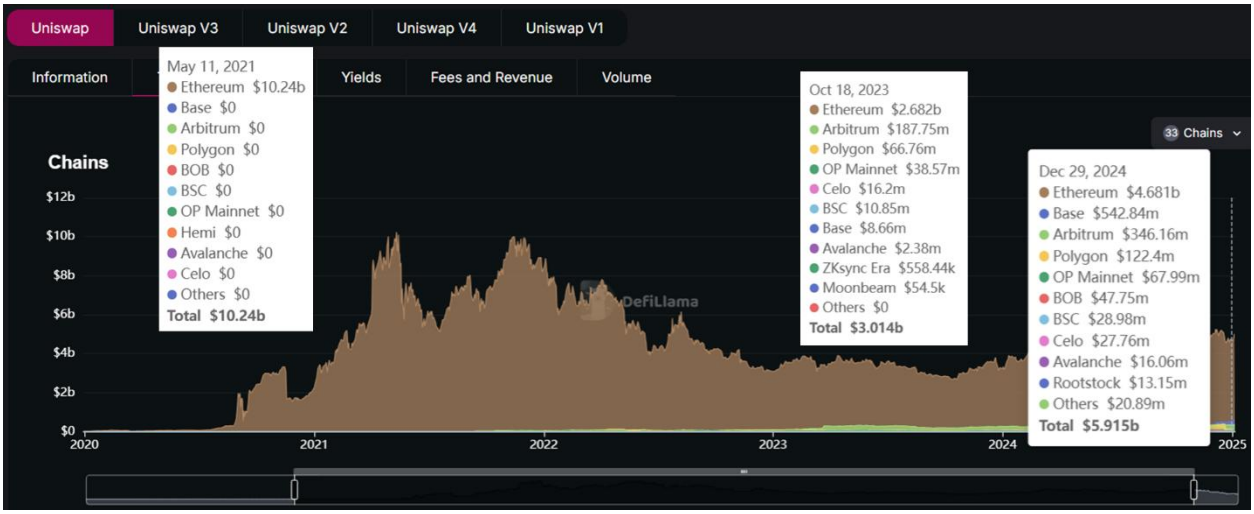
- Uniswap's AMM model versus the order book model of traditional exchanges
- Continuous liquidity availability versus time-limited market operations
- Permission-less asset listing versus rigorous listing requirements
- Absence of KYC/AML requirements that typify traditional exchanges
- Smart contract automation versus human or algorithmic intermediation

Traditional exchanges like NYSE or NASDAQ employ central limit order books with bid-ask matching. On the other hand, Uniswap uses invariant-based pricing that can result in higher slippage for large orders but ensures continuous liquidity.

TVL Trends: As of December 2024, Uniswap had approximately $5.9 billion in total value locked across its various versions. The protocol's TVL peaked at over $10.2 billion in May 2021 but has shown resilience during market downturns compared to other DeFi applications. The distribution of liquidity across Uniswap pools is highly

concentrated with stablecoin and ETH pairs typically accounting for over 70% of total liquidity. This concentration reflects trading volume patterns and the central role of these assets in the broader DeFi ecosystem.

Figure 2: TVL of Uniswap (2020 – 2024)



6.3. MakerDAO: Stablecoin Protocol

Service Provided: MakerDAO enables the creation of DAI, a decentralized stablecoin soft-pegged to the US dollar. Users can mint DAI by depositing collateral into Maker Vaults which mirrors the mechanism of taking out a collateralized debt position. The protocol requires overcollateralization (typically 150-175% depending on the collateral type) to protect against volatility in the underlying assets.

User Example: A user owns 10 ETH (worth approximately $30,000) but needs dollars for expenses without selling their ETH. Using MakerDAO, they can deposit their ETH into a Vault and generate up to 20,000 DAI (at a 150% collateralization ratio). This DAI can then be used like any other cryptocurrency or exchanged for fiat currency. The user maintains exposure to ETH all the while accessing dollar-denominated liquidity. The major requirement is to maintain the minimum collateralization ratio to avoid liquidation.

Target Users: MakerDAO serves the following user segments:

- Cryptocurrency holders seeking dollar-denominated liquidity without selling assets
- DeFi participants requiring a stable medium of exchange
- Investors seeking exposure to crypto governance through the MKR token
- Businesses and individuals seeking stable value storage outside traditional banking systems

Although MakerDAO's direct vault interface requires technical understanding, many users access DAI through simpler interfaces or exchanges. Blockchain novices are unlikely to interact directly with the protocol but frequently use DAI as a stablecoin without understanding its underlying mechanics.

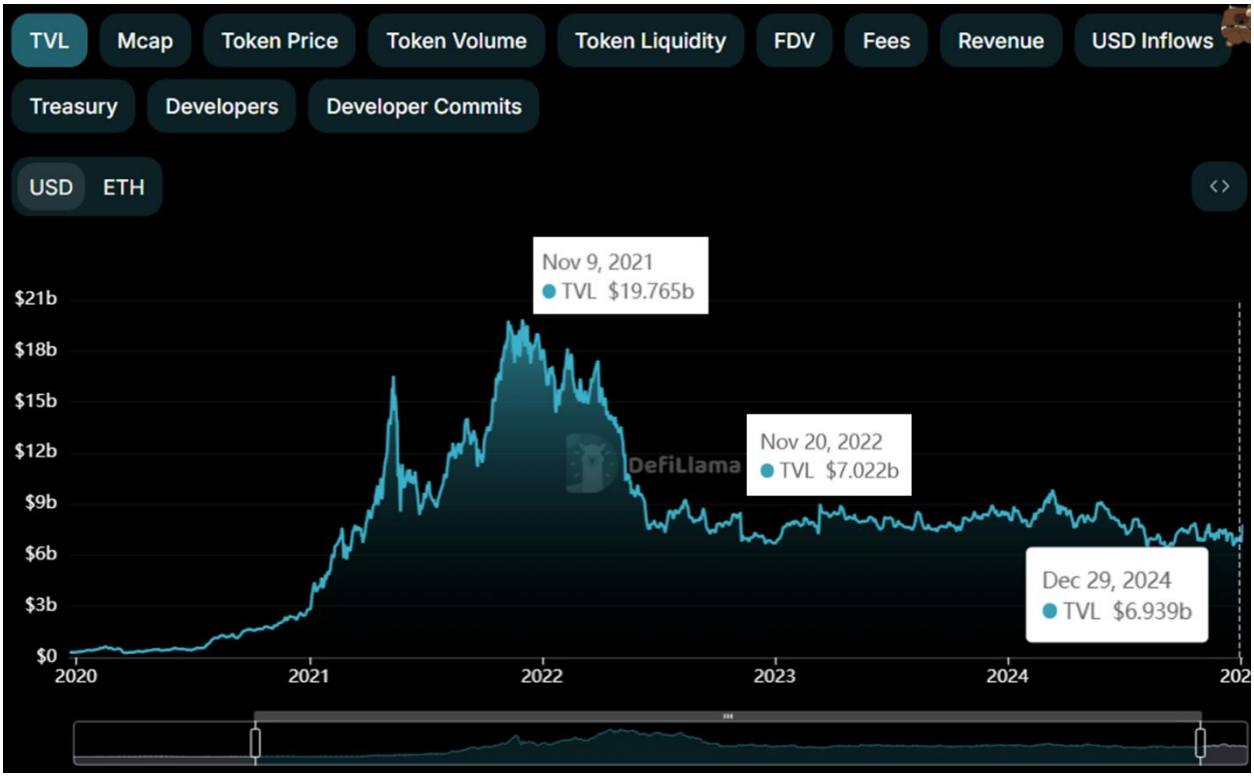
TradFi Equivalent: MakerDAO's closest traditional finance parallel is secured lending, such as home equity loans, where an asset serves as collateral for borrowing. However, following are some of the main differences:

- Programmatic liquidations versus legal foreclosure processes
- Higher collateralization requirements than traditional secured lending
- Creation of a stablecoin rather than lending existing currency
- Decentralized governance versus centralized loan approval

Traditional stablecoins like USDC rely on direct dollar backing in bank accounts whereas DAI achieves stability through overcollateralized crypto positions and algorithmic adjustments to monetary policy.

TVL Trends: As of December 2024, MakerDAO had approximately $7 billion in total value locked, making it one of the largest DeFi protocols. The TVL has shown greater stability than many other protocols during market cycles, reflecting DAI's utility beyond speculative activities.

Figure 3: TVL of MakerDAO (2020 – 2024)



The collateral composition has evolved significantly since MakerDAO's inception. Initially reliant almost exclusively on ETH, the protocol now accepts diverse collateral types including other cryptocurrencies, stablecoins, and real-world assets (RWA) through specialized adapters. This diversification has enhanced stability but introduced new governance challenges and centralization vectors.

7. Security and Economic Risks in DeFi

7.1. Technical Security Risks

DeFi protocols face numerous technical security challenges that differ from those in TradFi systems. DeFi's reliance on smart contract code and the underlying blockchain infrastructure exposes it to certain technical risks.

Smart Contract Vulnerabilities

Smart contract vulnerabilities are one of the most significant security risks in DeFi. Smart contracts are immutable once deployed and operate in a permissionless environment where anyone can interact with them. The immutability of blockchain deployments means that vulnerabilities cannot simply be patched once discovered. This creates a persistent attack surface that can be exploited by adversaries. The common smart contract vulnerabilities include:

- Reentrancy Attacks: These attacks exploit a contract's ability to call external contracts before completing its own state updates. The DAO hack in 2016 exploited a reentrancy vulnerability and resulted in the loss of $60 million.
- Integer Overflow/Underflow: Before Solidity 0.8.0, smart contracts were vulnerable to arithmetic errors where calculations could wrap around to unexpected values when they exceeded the storage capacity of the variable type. The Beauty Chain (BEC) token hack in 2018 exploited an integer overflow vulnerability to create an artificially large number of tokens.
- Access Control Failures: Improper implementation of access controls can allow unauthorized users to execute privileged functions. In August 2021, the Poly Network protocol suffered a $600 million exploit due to a critical access control vulnerability that allowed an attacker to become the owner of the contract.
- Logic Errors: Even correctly implemented contracts may contain logical flaws in their business logic. The October 2022 Mango Markets exploit allowed an attacker to manipulate oracle prices and drain approximately $100 million by taking advantage of a logical flaw in the protocol's liquidation mechanism.
- Oracle Manipulations: DeFi protocols rely on oracles to obtain external data which opens the system to vulnerability from price manipulation attacks. In November 2020, an attacker manipulated the price oracle for flash loans on Compound. This led to approximately $89 million in positions being liquidated.

Consensus and Network Layer Vulnerabilities

DeFi protocols also inherit security risks from the underlying blockchain infrastructure.

- Miner/Validator Extractable Value (MEV): Blockchain validators can manipulate transaction ordering to extract value at users' expense. Research by Qin et al. (2021) documented over $700 million in MEV extracted on Ethereum since 2020 through sandwich attacks, arbitrage, and liquidations.
- 51% Attacks: Although rare on established networks like Ethereum, smaller blockchains are vulnerable to attacks where an entity controlling majority consensus can potentially rewrite transaction history.
- Network Congestion and Front-Running: During periods of high demand, network congestion can lead to transaction failures or excessive fees. Sophisticated actors can exploit these conditions through front-running.
- Cross-Chain Bridge Vulnerabilities: As DeFi expands across multiple blockchains, cross-chain bridges have emerged as a critical vulnerability. In 2022 alone, bridge hacks accounted for over $2 billion in losses. This included major incidents affecting the Ronin Bridge ($624 million), and Wormhole ($326 million).

Implementation and Operational Risks

Practical implementation of DeFi protocols can also introduce security concerns:

- Centralized Points of Failure: Despite claims of decentralization, many DeFi protocols retain centralized components such as admin keys, upgrade mechanisms, or oracle dependencies.
- Composability Risks: DeFi's interconnected nature means that vulnerabilities in one protocol can cascade through the ecosystem. The collapse of Terra/Luna in May 2022 demonstrated how failures in one system can propagate through connected protocols.
- Upgrade Risks: Protocol upgrades can introduce new vulnerabilities or unexpected behaviors. The October 2021 Compound upgrade contained a bug that mistakenly distributed $90 million in COMP tokens to users.

7.2. Economic and Systemic Risks

DeFi faces economic and systemic risks that emerge from its market structures, incentive mechanisms, and interaction with broader financial systems. The economic and regulatory risks represent challenges for DeFi's long-term development. TradFi manages similar risks through regulatory oversight and centralized risk management. Similarly, DeFi must develop novel, decentralized approaches to address these challenges effectively.

Market Structure and Liquidity Risks

DeFi markets exhibit structural characteristics that create unique economic risks.

- Liquidity Fragmentation: Liquidity in DeFi ecosystems is fragmented across numerous protocols and chains. This fragmentation reduces market depth and increases slippage for large trades. Capponi and Jia (2021) demonstrate that DEX liquidity pools can experience complete liquidity freezes during periods of high volatility.
- Impermanent Loss: Liquidity providers in AMMs face impermanent loss when asset prices diverge from initial deposit ratio. This risk discourages liquidity provision during volatile markets when liquidity is most needed.
- Flash Loan Attacks: Flash loans allow for capital-efficient arbitrage by borrowing without collateral within a single transaction but also empowers attackers to temporarily access enormous capital for market manipulation.
- Oracle Failures: DeFi protocols need to rely on price oracles which can create systemic vulnerabilities when these oracles deliver inaccurate data. The Black Thursday event of March 2020 saw MakerDAO suffer $8 million in undercollateralized loans when ETH price oracles failed to update quickly during market volatility.

Incentive Design and Game Theoretic Risks

The economic design of DeFi protocols also create complex game theoretic dynamics with potential for exploitative equilibria:

- Yield Farming Distortions: Protocols offering governance tokens as incentives for liquidity provision often create unsustainable economics where participation is driven by token rewards rather than underlying protocol utility.
- Governance Attacks: Token-based governance systems can be vulnerable to attacks where adversaries accumulate sufficient voting power to extract value. In October 2022, an attacker borrowed large amounts of CRV tokens to influence governance decisions on the Curve protocol.
- MEV Extraction: Although some MEV extraction represents benign arbitrage that improves market efficiency, practices like sandwich attacks directly harm user outcomes by capitalizing on information asymmetry.
- Liquidation Spirals: Overcollateralized lending protocols can experience liquidation spirals where initial price declines trigger liquidations, further depressing collateral prices and triggering additional liquidations.

Regulatory and Legal Risks

The regulatory environment for DeFi remains uncertain, creating significant risks for participants:

- Regulatory Uncertainty: Lack of clear regulatory guidelines creates uncertainty for developers and users. The potential for retroactive enforcement poses existential risks to protocols operating in regulatory uncertain areas.

- AML/KYC Compliance: DeFi's permissionless design conflicts with traditional AML and KYC requirements. Regulatory actions, such as the OFAC sanctions against Tornado Cash demonstrate authorities' willingness to target DeFi protocols that enable anonymous transactions.
- Securities Law Implications: Many DeFi tokens may qualify as securities under regulatory frameworks like the Howey Test, exposing issuers and facilitators to potential enforcement actions.
- Tax Compliance Challenges: DeFi transactions create complex tax reporting obligations that many users struggle to fulfill accurately. The absence of standardized reporting mechanisms increases compliance burdens and potential liability for participants.

8. Computability and Welfare Analysis

8.1. Computational Efficiency of DeFi Protocols

The computational efficiency of DeFi protocols directly impacts their scalability, cost-effectiveness, and practical utility. DeFi protocols operate on public blockchains with inherent computational constraints.

Blockchain Computational Constraints

Public blockchains like Ethereum face fundamental computational limitations. Blockchains have limited capacity to process transactions within each block. On Ethereum, this scarcity is expressed through the gas limit, which constrains the total computational operations possible within each block. As DeFi protocols accumulate data over time, the blockchain state grows, increasing storage requirements for validators and potentially impacting computational efficiency for state-dependent operations. These constraints create a competitive market for block space which allows users to bid through transaction fees to secure inclusion in upcoming blocks. During periods of high demand, this fee market can lead to prohibitively expensive transactions. This undermines DeFi's accessibility and economic viability for smaller participants.

Protocol-Level Efficiency

DeFi protocols vary in their computational efficiency with important implications for user costs and scalability. Well-designed protocols minimize computational requirements through optimized smart contract code. For example, Uniswap V3 introduced significant gas optimizations compared to V2. This reduced the cost of swap transactions by approximately 30% despite the implementation of more complex functionality. Some protocols implement batch processing of operations to amortize fixed computational costs across multiple transactions. For instance, Balancer V2 uses a batch swap mechanism that reduces gas costs for complex multi-hop trades by executing them within a

single transaction. Advanced protocols employ techniques to minimize on-chain state storage. Synthetix's optimized collateralization mechanism reduces state updates, decreasing gas costs for frequent operations. In spite of these optimization mechanisms, fundamental computational constraints of underlying blockchains mean that DeFi protocols remain orders of magnitude less efficient than centralized counterparts in terms of transaction throughput.

8.2. Economic Efficiency Analysis

The economic efficiency of DeFi protocols can be evaluated through the following lenses:

Capital Efficiency

DeFi protocols exhibit varying degrees of capital efficiency.

- Overcollateralization Requirements: Most DeFi lending protocols require overcollateralization where typical collateral ratios range from 125% to 200%. This requirement is necessary for security in a trustless environment but creates substantial capital inefficiency compared to TradFi.
- Liquidity Fragmentation: Liquidity in DeFi protocols is fragmented across multiple platforms and blockchain networks. This fragmentation reduces capital efficiency by preventing optimal allocation of liquidity across markets. Recent innovations like concentrated liquidity in Uniswap V3 allow liquidity providers to target specific price ranges, improving capital efficiency by up to 4000x for equivalent price impact.
- Composability Effects: DeFi's composable nature can enhance capital efficiency by enabling the same assets to be utilized across multiple protocols simultaneously. For example, lending protocol receipt tokens like cTokens in Compound can be used as collateral in other protocols. The recursive lending structure creates capital efficiencies but it also introduces systemic risks when interconnected protocols experience stress events.

Pricing Efficiency

Pricing mechanisms in DeFi exhibit unique characteristics that impact market efficiency:

- AMM Price Discovery: DEXs using AMM models derive prices through a mathematical formula rather than order matching. Research by Park (2021) demonstrates that the conceptual flaws in constant product AMMs can lead to predictable pricing inefficiencies. This can happen mainly for large trades or volatile assets. These inefficiencies manifest as higher slippage compared to centralized alternatives.
- Oracle Dependence: Reliance on price oracles for external data introduces lags and inaccuracies in pricing. For example, Chainlink price feeds typically update every 1% price movement or hourly. This creates potential arbitrage opportunities during periods of high volatility.

- MEV Extraction: As documented by Qin et al. (2021), transaction ordering in public blockchains enables value extraction through front-running, back-running, and sandwich attacks. These practices create systematic pricing inefficiencies that disadvantage ordinary users.

Despite these inefficiencies, research by Barbon and Ranaldo (2021) suggests that pricing on major DEXs has become increasingly competitive with centralized alternatives for commonly traded pairs with deep liquidity.

8.3. Welfare Analysis of DeFi Applications

A comprehensive welfare analysis needs to consider DeFi's impacts at an individual and aggregate level:

User Welfare Impacts

DeFi offers several potential welfare benefits for users:

- Financial Inclusion: DeFi's permissionless nature enables access to financial services for users excluded from traditional banking infrastructure due to geographic, economic, or identity-based barriers. The minimal requirements for participation create opportunities for the approximately 1.7 billion adults globally who lack access to traditional banking services.
- Reduced Intermediation Costs: DeFi can eliminate fees associated with traditional financial intermediaries through disintermediation. For example, remittance services on DeFi platforms typically charge fees of 0.1-0.3%, compared to global averages of 6.5% for traditional remittance providers.
- Continuous Operation: DeFi operates continuously, enabling 24/7 access to financial services and reducing time-dependent friction in global transactions.
- Transparency and Control: DeFi provides transparency into financial operations, allowing users to verify transactions, inspect smart contract code, and maintain custody of their assets. This transparency can enhance trust and reduce information asymmetries that disadvantage users in traditional financial systems.

However, these benefits are offset by several welfare costs:

- Technical Complexity: Technical complexity of DeFi creates barriers to entry for non-technical users. Interacting directly with DeFi protocols requires understanding of blockchain transactions, wallet security, and gas fee mechanics, which exclude many potential users.
- Increased User Responsibility: DeFi shifts responsibility for security from institutions to individual users. Managing private keys, evaluating protocol risks, and protecting against exploits require expertise that most users lack, increasing the risk of catastrophic losses through user error.

- Volatile Transaction Costs: Variable gas fees create unpredictable transaction costs that disproportionately impact smaller users. During periods of network congestion, transaction fees can exceed the value of small transactions, effectively excluding retail users from participation.
- Information Asymmetries: DeFi theoretically offers complete transparency but in practice, sophisticated users and automated bots exploit information asymmetries to extract value from ordinary users through MEV strategies, front-running, and other forms of privileged execution.

Systemic Welfare Impacts

Beyond individual user impacts, DeFi has broader systemic welfare implications:

- Disintermediation of Rent-Seeking: By replacing traditional financial intermediaries with open protocols, DeFi potentially eliminates rent-seeking behavior that extracts value without providing commensurate benefits.
- Reduced Systemic Counterparty Risk: DeFi's reliance on overcollateralization and atomic execution reduces counterparty risk compared to traditional financial systems with fractional reserves and centralized clearing. This design choice trades capital efficiency for system stability.
- Innovation Acceleration: DeFi's open-source nature enables rapid innovation and iteration compared to traditional financial systems constrained by regulatory approval processes and proprietary infrastructure.
- Energy Consumption: PoW blockchains supporting DeFi applications consume significant energy resources and can create negative environmental externalities. Ethereum's transition to PoS has substantially reduced this impact but the environmental costs of blockchain-based systems remain a consideration in welfare analysis.
- Regulatory Arbitrage: DeFi's ability to operate outside traditional regulatory frameworks creates opportunities for regulatory arbitrage that may undermine consumer protections, market integrity, and financial stability measures.

8.4. Programmability Advantages

A distinctive feature of DeFi is the programmability of financial transactions through smart contracts, which enables novel economic arrangements that are difficult or impossible to implement in traditional finance:

- State-Contingent Execution: Smart contracts can automatically execute transactions based on predefined conditions without requiring trust between counterparties. This capability enables complex financial arrangements that would traditionally require extensive legal documentation and enforcement mechanisms.

- Atomic Transactions: DeFi enables atomic execution of multiple operations within a single transaction. This eliminates settlement risk and enables complex multi-step financial operations without counterparty risk. Atomicity creates opportunities for novel financial products that would be impractical in traditional systems.
- Composability: DeFi protocols can seamlessly integrate with one another, creating an ecosystem where financial Lego pieces can be assembled into increasingly complex arrangements. Composability accelerates innovation by allowing developers to build on existing protocol functionality rather than recreating fundamental components.
- Transparent Execution: The public nature of blockchain transactions makes financial operations transparent and auditable, reducing information asymmetries and enabling more effective market discipline. This transparency potentially reduces moral hazard and adverse selection problems that plague traditional financial systems.

Although programmability advantages create significant potential for welfare enhancement, realizing this potential requires overcoming the technical, economic, and regulatory challenges discussed throughout this analysis.

9. Future of DeFi and Open Research Challenges

Future development of DeFi faces challenges that must be addressed to achieve mainstream adoption and long-term sustainability. This section examines key areas of ongoing research and development that will shape DeFi's evolution.

9.1. Ethereum’s L2 Blockchain and Scalability Solutions

Blockchain’s scalability remains a constraint on DeFi adoption with high fees and limited throughput creating barriers to mainstream usage. Layer-2 (L2) solutions can offer improvements in through and cost-efficiency by processing transactions off the main blockchain. L2 protocols may employ the following mechanisms to balance scalability, security, and decentralization:

- Optimistic Rollups: Optimistic Rollups enhance scalability by batching transactions off-chain and submitting compressed data to Ethereum’s L1. These systems assume transactions are legitimate unless challenged during a 7-day dispute window. During this period, validators can submit cryptographic evidence to invalidate fraudulent activity. Arbitrum is a leading implementation in this category with TVL of $3 billion and Bridged TVL of $ 16 billion as of December 2024.. Platforms like Arbitrum can reduce transaction fees by 90-95% while still maintaining compatibility with existing smart contracts. However, there are some trade-offs as central sequencers can introduce single points of failure and delayed withdrawals can create liquidity constraints.

- Zero-Knowledge (ZK) Rollups: ZK-Rollups can optimize for instant finality by validating transactions off-chain using zero-knowledge proofs which cryptographically verify correctness without revealing transaction details. Protocols like zkSync Era and StarkNet demonstrate the potential for high-frequency trading and enterprise scale operation due to their higher TPS. The immediate finality ensures potentially greater throughput than optimistic approaches. Specialized L2 solutions optimized for particular DeFi applications can also achieve greater efficiency improvements. For example, dYdX's L2 implementation achieves thousands of transactions per second for derivatives trading. However, proof-generation costs impose 12 - 18% operational overhead due to specialized hardware requirements and limited Ethereum Virtual Machine compatibility complicates migration for existing dApps.
- Sidechains: Sidechains are independent blockchains connected to L1 networks via two-way bridges to allow for interoperability. Unlike rollups, sidechains employ their own validator set and consensus mechanisms to process transactions. This independence allows sidechains to optimize specific use cases such as low fees or high throughput. One of the leading sidechains is Polygon which can process transactions for less than $0.01 with around 100 validators. In comparison, Ethereum L1 has more than 1 million validators. However, the small validator set can create a single point of failure and undermine decentralization. Sidechains also do not inherit L1 security which exposes them to 51% attacks if validators collude. The cross-chain bridges for asset transfer are also frequently targeted for exploitation.

The rise of Ethereum L2 solutions has resolved critical scalability constraints and reduced transaction fees. However, this success introduces a paradox for Ethereum's economics. As L2s alleviate congestion, they are diverting fee revenue away from Ethereum's base L1 layer. This further weakens Ethereum's deflationary mechanism and value accrual. It is estimated that $2.1 billion of Ethereum's fee revenue was captured by L2 sequencers in 2024, reducing ETH burning and raising concerns about ETH's long-term scarcity. These risks are compounded as centralized sequencers and vulnerable bridges undermine decentralization. L2 solutions also introduce the challenge of cross-layer liquidity fragmentation.

9.2. Regulatory Challenges

In response to regulatory pressures, several approaches to DeFi compliance are emerging. Protocols like Aave Arc and Polymesh implemented permissioned pools that require identity verification. Governance structures specifically designed to address regulatory compliance through decentralized processes are also emerging. This may potentially

enable DeFi protocols to adapt to regulatory requirements while maintaining decentralized operations. The regulatory evolution of DeFi represents a critical area for future research.

9.3. Future Innovations

There are several promising areas of innovation for DeFi's future development. Integration of real-world assets (RWAs) into DeFi represents one such frontier for expansion. Projects like Centrifuge and Maple Finance are pioneering the integration of TradFi assets into DeFi. Platforms like RealT and Lofty AI enable fractional ownership of real estate through tokenization which increases liquidity and accessibility for a traditionally illiquid asset class. DeFi protocols are also beginning to address trade finance and supply chain financing with projects like Tradeshift and Credix connecting real-world commercial activities to DeFi liquidity. Integration of RWAs could exponentially expand DeFi's total addressable market and improve capital efficiency by connecting to cash-flowing assets.

As DeFi matures, identity and reputation systems are emerging as critical infrastructure. The development of privacy-preserving identity systems could help DeFi overcome current limitations in capital efficiency and regulatory compliance while maintaining core values of user sovereignty. Protocols like Ceramic Network and Spruce ID enable users to control their digital identity and selectively disclose attributes without relying on centralized identity providers. Zero-knowledge proof systems like Aztec can potentially enable compliant financial services without comprehensive identity disclosure.

9.4. Open Research Questions

Following are some critical research questions that remain unresolved and represent important areas for future investigation:

- Optimal MEV Distribution: How should value extracted through privileged transaction ordering be distributed to maximize system welfare and align incentives? Current approaches range from complete validator capture to various forms of user rebating.
- Governance Scalability: Can decentralized governance mechanisms scale to support complex, interconnected financial systems while maintaining security, efficiency, and participant alignment? Current approaches struggle with low participation rates and complexity management.
- Privacy vs. Transparency Tradeoffs: How can DeFi balance the benefits of transparency (reduced information asymmetry, verifiable execution) with privacy requirements (personal financial data protection, competitive strategy preservation)?

- Cross-Chain Security Models: What security assumptions and bridge designs minimize cross-chain vulnerability while enabling efficient liquidity transfer? Current cross-chain bridges have proven highly vulnerable to exploitation.
- Sustainable Token Economics: Can tokenomic designs create sustainable incentive alignment without relying on perpetual token appreciation or excessive inflation? Most current models struggle with long-term sustainability once initial growth phases conclude.

Resolution of these research questions would contribute significantly to DeFi's maturation into a robust, accessible financial system capable of serving diverse global users.

10. Conclusion

Our analysis of smart contracts and decentralized finance has examined the current state of DeFi protocols, their economic foundations, security challenges, and future prospect. Several findings emerge from our investigation. First, DeFi represents a genuine innovation in financial architecture by enabling novel financial arrangements through the combination of smart contract programmability, blockchain-based settlement, and permissionless access. These technological capabilities create opportunities for financial inclusion, capital formation, and risk transfer that were previously impractical in TradFi systems. Second, current DeFi implementations face limitations that restrict their practical utility and mainstream adoption. Technical constraints including scalability limitations, security vulnerabilities, and oracle dependencies create friction that undermines user experience and economic efficiency. Economic challenges including capital inefficiency through overcollateralization, liquidity fragmentation, and MEV extraction further constrain DeFi's competitiveness with traditional alternatives. Third, the security landscape of DeFi reveals a complex interplay between technical, economic, and governance factors. While smart contract vulnerabilities receive significant attention, systemic risks arising from protocol interconnection, governance vulnerabilities, and economic design flaws potentially pose greater long-term challenges. The immutable nature of blockchain deployments magnifies the impact of security failures, creating an asymmetric risk profile where defensive measures must anticipate a vast array of potential attack vectors. Fourth, our welfare analysis indicates that DeFi currently offers the greatest benefits to users with technical expertise, substantial capital, and tolerance for experimental financial arrangements. Although permissionless access theoretically enables universal participation, practical barriers including technical complexity, high transaction costs, and information asymmetries limit DeFi's effectiveness in serving traditionally underbanked populations. These limitations suggest that DeFi's current form

may exacerbate rather than resolve existing inequalities in financial access. Fifth, regulatory uncertainty represents both a challenge and an opportunity for DeFi's development. Evolving approaches that focus on outcomes rather than specific entities could potentially enable DeFi innovation while preserving core regulatory objectives like consumer protection and financial stability.

Today, DeFi stands at an inflection point between niche experimentation and mainstream relevance. Addressing current limitations through scalability solutions, improved security practices, user experience enhancements, and regulatory clarity could potentially unlock DeFi's transformative potential. However, these developments require not only technical advancement but also thoughtful integration of economic, governance, and regulatory considerations.

The research challenges identified in this analysis suggest several promising directions for future investigation. Developing more robust security models that address economic and governance vulnerabilities, creating sustainable tokenomic designs that align stakeholder incentives over long-time horizons, and exploring the optimal balance between decentralization and efficiency represent particularly important areas for continuing research.

11. References

Allen, F. & Santomero, A. M., 1997. The Theory of Financial Intermediation.. *Journal of Banking & Finance,* 21(11-12), pp. 1461-1485.

Anon., 2025. *Total Value Locked (TVL) in DeFi.* [Online]
Available at: https://defillama.com/
[Accessed 12 January 2025].

Barbon, A. & Ranaldo, A., 2021. On The Quality Of Cryptocurrency Markets: Centralized Versus Decentralized Exchanges. *Swiss Finance Institute Research,* Issue 22-38.

Bartoletti, M., Cimo, T. & Aztei, N., 2017. A survey of attacks on Ethereum smart contracts. In: *Principles of Security and Trust.* 186: s.n., p. 164.

Capponi, A. & Jia, R., 2021. The Adoption of Blockchain-based Decentralized Exchanges. *Working Paper, Columbia University.*

Capponi, A., Jia, R. & Yu, S., 2024. Price Discovery on Decentralized Exchanges.

Cong, L. W. & He, Z., 2019. Blockchain Disruption and Smart Contracts. *The Review of Financial Studies,* 32(5), pp. 1754-1797.

Diamond, D. W. & Dybvig, P. H., 1983. Bank Runs, Deposit Insurance, and Liquidity. *Journal of Political Economy,* 91(3), pp. 401-419.

Easley, D., O'Hara, M. & Basu, S., 2019. From Mining to Markets: The Evolution of Bitcoin Transaction Fees. *Journal of Financial Economics,* 134(1), pp. 91-109.

Halaburda, H., Haeringer, G., Gans, J. & Gandal, N., 2022. The microeconomics of cryptocurrencies. *Journal of Economic Literature,* 60(3), pp. 971-1013.

Harvey, C. R., Ramachandran, A. & Santoro, J., 2021. *DeFi and the Future of Finance.* New Jersey: John Wiley & Sons, Inc..

Huberman, G., Leshno, J. & Moallemi, C. C., 2021. Monopoly without a Monopolist: An Economic Analysis of the Bitcoin Payment System. *The Review of Economic Studies,* 88(6), pp. 3011-3040.

John, K. et al., 2024. Economics of Ethereum. *Journal of Corporate Finance,* Volume 91.

John, K., Kogan, L. & Saleh, F., 2023. Smart contracts and decentralized finance. *Annual Review of Financial Economics,* Issue 15, pp. 523-542.

John, K., Rivera, T. & Saleh, F., 2021. Equilibrium Staking Levels in a Proof-of-Stake Blockchain.

John, K., Rivera, T. & Saleh, F., 2024. Proof-of-Work versus Proof-of-Stake: A Comparative Economic Analysis. *The Review of Financial Studies.*

John, K. & Saleh, F., Forthcoming 2025. Cryptoeconomics. *Oxford Research Encyclopedia of Economics and Finance.* Oxfod University Press.

John, K., Saleh, F. & O'Hara, M., 2022. Bitcoin and beyond. *Annual Review of Financial Economics,* Issue 14, pp. 95-115.

Park, A., 2021. Conceptual Flaws of Decentralized Automated Market Making. *Working Paper, University of Toronto.*

Qin, K. et al., 2021. *An empirical study of DeFi liquidations: incentives, risks, and instabilities.* s.l., 21st ACM Internet Measurement Conference, pp. 336-350.

Qin, K., Zhou, L. & Gervais, A., 2022. Quantifying Blockchain Extractable Value: How dark is the forest?. *IEEE Symposium on Security and Privacy (SP),* pp. 198-214.

Rosu, I. & Saleh, F., 2021. Evolution of Shares in a Proof-of-Stake Cryptocurrency. *Management Science,* 67(2), pp. 661-672.

Saleh, F., 2021. Blockchain without waste: Proof-of-stake. *The Review of Financial Studies,* 34(3), pp. 1156-1190.

Szabo, N., 1997. Formalizing and Securing Relationships on Public Networks. *First Monday,* 2(9).

Xu, T. & Xu, J., 2021. A Short Survey on Business Models of Decentralized Finance (DeFi) Protocols.