Complex Systems Informatics and Modeling Quarterly (CSIMQ)
eISSN: 2255-9922
Published online by RTU Press, https://csimq-journals.rtu.lv
Article 150, Issue 26, March/April 2021, Pages 46–54
https://doi.org/10.7250/csimq.2021-26.03

An Introduction to Decentralized Finance (DeFi)

Johannes Rude Jensen[1,2*], Victor von Wachter[1], and Omri Ross[1,2]

[1] Department of Computer Science, University of Copenhagen, Copenhagen, Denmark
[2] eToroX Labs, Copenhagen, Denmark

johannesrudejensen@gmail.com, victor.vonwachter@di.ku.dk, omri@di.ku.dk

Abstract. Decentralized financial applications (DeFi) are a new breed of consumer-facing financial applications composed as smart contracts, deployed on permissionless blockchain technologies. In this article, we situate the DeFi concept in the theoretical context of permissionless blockchain technology and provide a taxonomical overview of agents, incentives and risks. We examine the key market categories and use-cases for DeFi applications today and identify four key risk groups for potential stakeholders contemplating the advantages of decentralized financial applications. We contribute novel insights into a rapidly emerging field, with far-reaching implications for the financial services.
Keywords: Blockchain, Decentralized Finance, DeFi, Smart Contracts.

1 Introduction

Decentralized financial applications, colloquially referred to as 'DeFi', are a new type of open financial applications deployed on publicly accessible, permissionless blockchains. A rapid surge in the popularity of these applications saw the total value of the assets locked in DeFi applications (TVL) grow from $675mn at the outset of 2020 to an excess of $40bn towards the end of first quarter in the following year[†]. While scholars within the information systems and management disciplines recognize the novelty and prospective impact of blockchain technologies, theoretical or empirical work on DeFi remains scarce [1]. In this short article, we provide a conceptual introduction to 'DeFi' situated in the theoretical context of permissionless blockchain technology. We introduce a taxonomy of agents, roles, incentives, and risks in DeFi applications and present four potential sources of complexity and risk.

This article extends the previous publication on managing risk in DeFi[‡] and is structured as follows. Section 2 introduces the permissionless blockchain technology and decentralized finance. Section 3 presents DeFi application taxonomy. An overview of popular DeFi application

* Corresponding author

Reference: J. R. Jensen, V. von Wachter, and O. Ross, "An Introduction to Decentralized Finance (DeFi)," Complex Systems Informatics and Modeling Quarterly, CSIMQ, no. 26, pp. 46–54, 2021. Available: https://doi.org/10.7250/csimq.2021-26.03

Additional information. Author ORCID iD: J. R. Jensen – https://orcid.org/0000-0002-7835-6424, V. von Wachter – https://orcid.org/0000-0003-4275-3660, and O. Ross – https://orcid.org/0000-0002-0384-1644. PII S225599222100150X. Received: 18 February 2021. Accepted: 15 April 2021. Available online: 30 April 2021.

[†] https://defipulse.com/
[‡] http://ceur-ws.org/Vol-2749/short3.pdf

categories is given in Section 4. The risks in decentralized finance are discussed in Section 5. Section 6 concludes the paper.

2 Permissionless Blockchain Technology and Decentralized Finance

The implications and design principles for blockchain and distributed ledger technologies have generated a growing body of literature in the information systems (IS) genre [2]. Primarily informed by the commercial implications of smart contract technology, scholars have examined the implications for activities in the financial services such as the settlement and clearing of 'tokenized' assets [3] the execution and compilation of financial contracts [4]–[6], complexities in supply-chain logistics [7] and beyond. A blockchain is a type of distributed database architecture in which a decentralized network of stakeholders maintains a singleton state machine. Transactions in the database represent state transitions disseminated amongst network participants in 'blocks' of data. The correct order of the blocks containing the chronological overview of transactions in the database is maintained with the use of cryptographical primitives, by which all stakeholders can manually verify the succession of blocks.

A network consensus protocol defines the rules for what constitutes a legitimate transaction in the distributed database. In most cases, consensus protocols are rigorous game-theoretical mechanisms in which network participants are economically incentivized to promote network security through rewards and penalties for benevolent or malicious behavior [8]. Scholars typically differentiate between 'permissioned' and 'permissionless' blockchains. Permissionless blockchains are open environments accessible by all, whereas permissioned blockchains are inaccessible for external parties not recognized by a system administrator [2]. Recent implementations of the technology introduces a virtual machine, the state of which is maintained by the nodes supporting the network. The virtual machine is a simple stack-based architecture, in which network participants can execute metered computations denominated in the native currency format. Because all 'nodes' running the blockchain 'client' software must replicate the computations required for a program to run, computational expenditures are priced on the open market. This design choice is intended to mitigate excessive use of resources leading to network congestion or abuse.

Network participants pass instructions to the virtual machine in a higher-level programming language, the most recent generations of which is used to write programs, referred to as *smart contracts*. Because operations in the virtual machine are executed in a shared state, smart contracts are both transparent and *stateful*, meaning that any application deployed as a smart contract executes deterministically. This ensures that once a smart contract is deployed, it will execute exactly as instructed.

3 DeFi Agent Taxonomy

We denote the concept: 'DeFi application' as an arrangement of consumer-facing smart contracts, executing a predefined business logic within the transparent and deterministic computational environment afforded by a permissionless blockchain technology. Blockchain technology is the core infrastructure layer (see Figure 1) storing transactions securely and providing game-theoretic consensus through the issuance of a native asset. As a basic financial function, standardized smart contracts are utilized to create base assets in the asset layer. These assets are utilized as basis for more complex financial instruments in the application layer. In the application layer, DeFi applications are deployed as sophisticated smart contracts and thus execute a given business logic deterministically. Contemporary DeFi applications provide a range of financial services within trading, lending, derivatives, asset management and insurance services. Aggregators source services from multiple applications, largely to provide the best rates across the ecosystem. Finally, user friendly frontends combine the applications and build a service similar to today's banking apps. In contrast to traditional banking services, in a

blockchain-based technology stack, users interact directly with the application independent of any intermediary service provider.

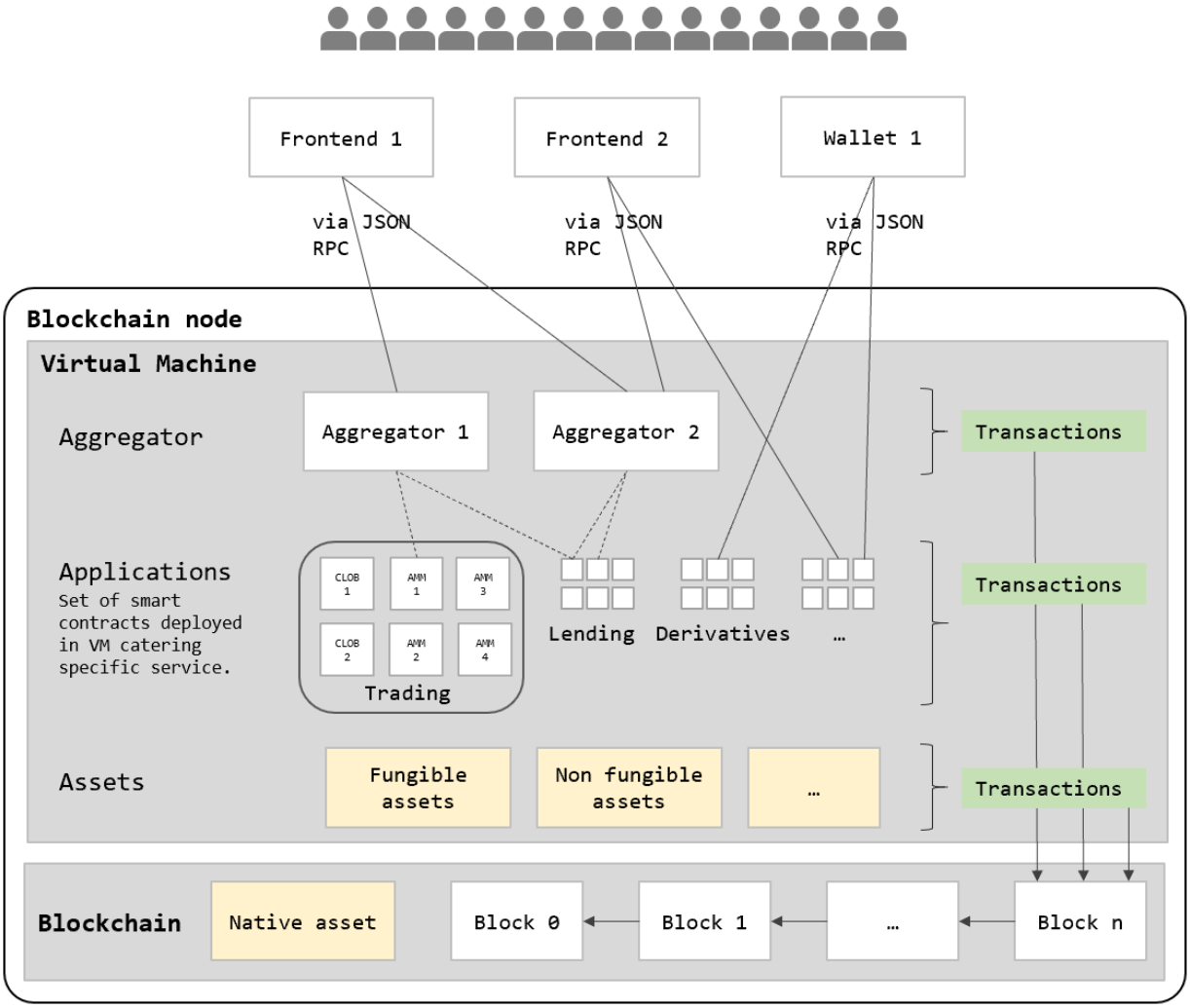

Figure 1. DeFi applications on permisionless blockchain

The metered pricing of computational resources on permissionless blockchains means that DeFi applications are constrained by the computational resources they can use. Application designers seek to mitigate the need for the most expensive operations, such as storing big amounts of data or conducting sophisticated calculations, in the effort of reducing the level of complexity required to execute the service that their application provides.

Because the resources required for interacting with a smart contract are paid by the user, DeFi application designers employ an innovative combination of algorithmic financial engineering and game theory to ensure that all stakeholders of their application are sufficiently compensated and incentivized. In Table 1, we introduce a taxonomy for the different types of agents and their roles in contemporary DeFi applications. We highlight the incentives for participation and key risks associated with each role.

Owing to the original open-source ethos of blockchain technology, application designers are required to be transparent and build ‘open’ and accessible applications, in which users can take ownership and participate in decision-making processes, primarily concerning new features or changes to the applications. As a reaction to these demands, application designers often issue and distribute so-called *governance tokens*. Governance tokens are fungible units held by users, which allocates voting power in majority voting-schemes [9]. Much like traditional equities, governance tokens trade on secondary markets which introduces the opportunity for capital

formation for early stakeholders and designers of successful applications. By distributing governance tokens, application designers seek to disseminate value to community members while retaining enough capital to scale development of the application by selling inventory over multiple years.

Table 1. Agent classification, incentives, and key risks

Agent:	**Role:**	**Incentives for participation:**	**Key risk:**
Users	Utilizing the application	Profits, credit, exposure and governance token	Market risk, technical risk
Liquidity Providers	Supply capital to the application in order to ensure liquidity for traders or borrowers	Protocol fees, governance token	Systemic economic risk, technical risk, regulatory risk, opportunity costs of capital
Arbitrageurs	Return the application to an equilibrium state through strategic purchasing and selling of assets	Arbitrage profits	Market risk, network congestion and transaction fees
Application Designers (Team and Founders)	Design, implement and maintain the application	Governance token appreciation	Software bugs

The generalized agent classification demonstrated in Table 1 is applicable to a wide area of DeFi applications providing peer-to-peer financial services on blockchain technology including, trading, lending, derivatives and asset management. In the following section, we dive into a number of recent use cases, examining the most recently popular categories of applications.

4 An Overview of Popular DeFi Application Categories

The development principles presented above have been implemented in a number of live applications to date. In this section, we provide a brief overview of the main categories of DeFi applications.

4.1 Decentralized Exchanges and Automated Market Makers

Facilitating the decentralized exchange of assets requires an efficient solution for matching counterparties with the desire to sell or purchase a given asset for a certain price, a process known as *price-discovery*. Early implementations of decentralized exchanges on permissionless blockchain technologies successfully demonstrated the feasibility of executing decentralized exchange of assets on permissionless blockchain technology, by imitating the conventional central limit order book (CLOB) design. However, for reasons stipulated below, this proved infeasible and expensive at scale.

First, in the unique cost structure of the blockchain based virtual machine format [10], traders engaging with an application, pay fees corresponding to the complexity of the computation and the amount of storage required for the operation they wish to compute. Because the virtual machine is replicated on all active nodes, storing even small amounts of data is exceedingly expensive. Combined with a complex matching logic required to maintain a liquid orderbook, computing fees rapidly exceeded users' willingness to trade.

Second, as 'miners' pick transactions for inclusion in the next block by the amount of computational fees attached to the transaction, it is possible to front-run state changes to the decentralized orderbook by attaching a large computational fee to a transaction including a trade,

which pre-emptively exploits the next state change of the orderbook, thus profiting through arbitrage on a deterministic future state [11].

Subsequent iterations of decentralized exchanges addressed these issues by storing the state of the orderbook separately, using the blockchain only to compute the final settlement [12]. Nevertheless, problems with settlement frequency persisted, as these implementations introduced complex coordination problems between orderbook storage providers, presenting additional risk vectors to storage security. Motivated by the shortcomings of the established CLOB design a generation of blockchain specific 'automated' market makers (AMMs) presents a new approach to blockchain enabled market design.

By pooling available liquidity in trading pairs or groups, AMMs eliminate the need for the presence of buyers and sellers at the same time, facilitating relatively seamless trade execution without compromising the deterministic integrity of the computational environment afforded by the blockchain. Trading liquidity is provided by 'liquidity providers' which lock crypto assets in the pursuit of trading fee returns.

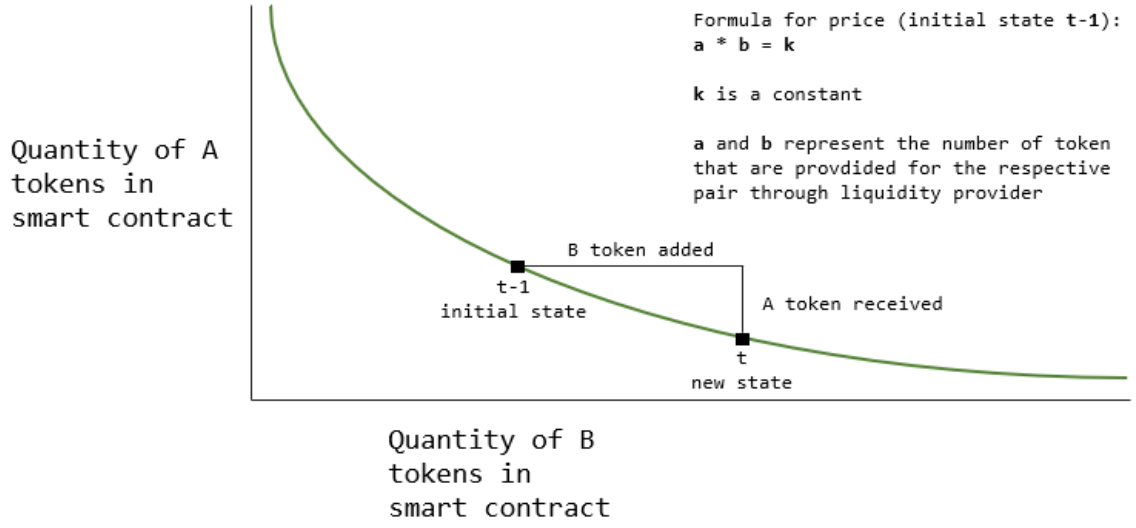

Figure 2. AMM Price Discovery Function

While the primary context for the formal literature on blockchain based AMM has been provided by Angeris and Chitra *et al.* [13]–[15] the field has attracted new work on adjacent topics such as liquidity provisioning [16]–[18] and token weighted voting systems [19].

4.2 Peer-to-Peer Lending and Algorithmic Money Markets

The 'money markets' to borrow and lend capital with corresponding interest payments occupy an important role in the traditional financial service. Within DeFi, borrowing and lending applications are amongst the largest segments of financial applications with $7bn total value locked[§] at the end of 2020. In borrowing/lending protocols agents with excess capital can lend crypto assets ('liquidity providers') to a peer-to-peer protocol receiving continuous interest payments. Consequently, a borrower can borrow crypto assets and pays an interest rate. Given the pseudonymous nature of blockchain technology, it is not possible to borrow funds purely on credit. To borrow funds, the borrowing agent has to 'overcollateralize' a loan, by providing another crypto assets exceeding the dollar value of the loan to the smart contract. The smart contract then issues a loan relative to 70–90% of the value of the collateral assets. Should the

[§] https://defipulse.com/

value of the collateral assets drop below the value of the outstanding loan, the smart contract automatically auctions away the collateral on a decentralized exchange at a profit. The interest rate is algorithmically set by the relative supply and demand for each specific crypto asset. Initially pioneered by the MakerDAO [**] application, several protocols are now accessible providing similar services with novel interests rate calculations or optional insurance properties, currently presiding over a $7bn crypto assets under management.

4.3 Derivatives

Blockchain-based financial contracts (derivatives) are one of the fastest growing market segments in DeFi. Here, application designers seek to make traditional financial derivatives such as *options, futures* and other kinds of *synthetic* contracts available to the broader DeFi ecosystem. A futures contract stipulates a sale of an asset at a specified price with an expiry date, an option contract stipulates the *right* but not the obligation to sell or purchase an asset at a specific price.

As in traditional finance both financial services can be used as insurance against market movements as well as speculation on prices. Recently, a new segment of 'synthetic' assets has entered the market in the form of tokens pegged to an external price, commonly tracking the price of commodities (e.g., gold) or stocks (e.g., Tesla). A user can create such synthetic asset by collateralized crypto assets in a smart contract similar to how a decentralized lending is computed. The synthetic asset tracks an external price feed ('oracle') which is provided to the blockchain. However, external price feeds are prone to technical issues and coordination problems leading to staleness in case of network congestions or fraudulent manipulation [20].

4.4 Automated Asset Management

The traditional practice of 'asset management' in the financial services industry consists primarily of the practice of allocating financial assets such as to satisfy the long-term financial objectives of an institution or an individual. As the reader will have noted above, there are an increasing number of DeFi applications, all of which operate algorithmically without human intervention. This means that the DeFi markets operate around the clock and are impossible to manage

The two main use cases for automated asset managers are 'yield aggregators' and traditional crypto asset indices. Utilizing the interoperability and automation of blockchain technology, 'yield aggregators' are smart contract protocols allocating crypto assets according to predefined rules, often with the goal of maximizing yield whilst controlling risk. Users typically allocate assets to a protocols, which automatically allocates assets across applications in order to optimize the aggregate returns, while rebalancing capital allocations on an ongoing basis.

Indices, on the other hand, offer a broad exposure to crypto assets akin to the practice of 'passive' investing. These applications track a portfolio of crypto assets by automatically purchasing these assets and holding them within the smart contract. Equivalent to exchange traded funds (ETFs), stakeholders purchase ownership of the indices by buying a novel token, granting them the algorithmic rights over a fraction of the total assets held within the smart contract[††].

5 Identifying and Managing Risk in Decentralized Finance

In this section, we identify and evaluate four risk factors which are likely to introduce new complexities for stakeholders involved with DeFi applications.

[**] https://makerdao.com/

[††] blockchain-in-asset-management.pdf (pwc.co.uk)

5.1 Software Integrity and Security

Owing to the deterministic nature of permissionless blockchain technology, applications deployed on as smart contracts are subject to excessive security risks, as any signed transaction remains permanent once included in a block. The irreversible or, 'immutable' nature of transactions in a blockchain network has led to significant loss of capital on multiple occasions, most frequently as a result of coding errors, sometimes relating to even the most sophisticated aspects virtual machine and programming language semantics [21]. DeFi applications rely on the integrity of smart contracts and the underlying blockchain. Risk is further enforced through uncertainties in future developments and the novelty of the technology.

5.2 Transaction Costs and Network Congestion

To mitigate abusive or excessive use of the computational resources available on the network, computational resources required to interact with smart contracts are metered. This creates a secondary market for transactions, in which users can outbid each other by attaching transaction fees in the effort of incentivizing miners to select their transaction for inclusion in the next block [11]. In times of network congestion, transactions can remain in a pending state, which ultimately results in market inefficiency and information delays.

Furthermore, in these times, complex transactions can cost up to hundreds of dollars, making potential adjustments to the state costly.[‡‡] While intermediary service providers occasionally choose to subsidize protocol transaction fees[§§], application fees are in near all cases paid by the user interacting with the DeFi application.

Because application designers seek to lower the aggregate transaction costs, protocol fees, slippage or impermanent loss through algorithmic financial modelling and incentive alignment, stakeholders must carefully observe the state of the blockchain network. If a period of network congestion coincides with a period of volatility, the application design may suddenly impose excessive fees or penalties on otherwise standard actions such as withdrawing or adding funds to a lending market [20].

5.3 Participation in Decentralized Governance

Responding to implications of the historically concentrated distribution of native assets amongst a small minority of stakeholders, DeFi application designers increasingly rely on a gradual distribution of fungible governance-tokens in the attempt at adequately 'decentralizing' decision-making processes [9].

While the distribution of governance tokens remains fairly concentrated amongst a small group of colluding stakeholders, the gradual distribution of voting-power to liquidity providers and users will result in an increasingly long-tailed distribution of governance tokens. Broad distributions of governance tokens may result in adversarial implications of a given set of governance outcomes, for stakeholders who are not sufficiently involved in monitoring the governance process [19].

5.4 Application Interoperability and Systemic Risks

A key value proposition for DeFi applications is the high level of interoperability between applications. As most applications are deployed on the Ethereum blockchain, users can transact seamlessly between different applications with settlement times rarely exceeding a few minutes. This facilitates rapid capital flows between old and new applications on the network. While interoperability is an attractive feature for any set of financial applications, tightly coupled and

[‡‡] https://etherscan.io/gastracker
[§§] Coinbase.com

complex liquidity systems can generate an excessive degree of financial integration, resulting in systemic dependencies between applications [22].

This factor is exacerbated by the often complex and heterogeneous methodologies for the computation of exposure, debt, value, and collateral value that DeFi application designers have used to improve their product. An increasing degree of contagion between applications may introduce systemic risks, as a sudden failure or exploit in one application could ripple throughout the network, affecting stakeholders across the entire ecosystem of applications.

The primary example of this dynamic can be demonstrated by the computation of ownership in so-called liquidity pools used by traders utilizing AMM smart contracts. When providing liquidity in the form of crypto assets to a decentralized exchange, liquidity providers receives 'liquidity shares' redeemable for a proportional share of the liquidity pool, together with the accumulated fees generated through trading.

As liquidity shares are typically transferable and fungible IOU tokens representing fractional ownership of a liquidity pool, this has led to the emergence of secondary markets for liquidity shares. Providing liquidity in the form of IOU tokens, to these secondary market creates additional (3rd generation) liquidity shares, generating additional fees for the liquidity provider. As a consequence of the increasingly integrated market for liquidity shares, a rapid depreciation of the source asset for the liquidity shares may trigger a sequence of cascading liquidations, as the market struggles to price in any rapid changes in the price of the source asset [20], [22], [23].

6 Conclusion: Is DeFi The Future of Finance?

In this article, we have examined the potential implications, complexities and risks associated with the proliferation of consumer facing DeFi applications. While DeFi applications deployed on permissionless blockchains present a radical potential for transforming consumer facing financial services, the risks associated with engaging with these applications remain salient. Future stakeholder contemplating an engagement with these applications ought to consider and evaluate key risks prior to committing or allocating funds to DeFi applications.

Scholars interested in DeFi applications may approach the theme from numerous angles, extending early research on the market design of DeFi applications [14] or issues related to governance tokens [9], [19] and beyond.

Acknowledgments

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Sklodowska-Curie grant agreement No 801199.

References

[1] J. Kolb, M. Abdelbaky, R. H. Katz, and D. E. Culler, "Core Concepts, Challenges, and future Directions in Blockchain: A centralized Tutorial," *ACM Comput. Surv.*, vol. 53, no. 1, pp. 1–39, 2020. Available: https://doi.org/10.1145/3366370

[2] O. Labazova, "Towards a Framework for Evaluation of Blockchain Implementations," in *Conference Proceedings of ICIS (2019)*, 2019.

[3] O. Ross, J. Jensen, and T. Asheim, "Assets under Tokenization: Can Blockchain Technology Improve Post-Trade Processing?" in *Conference Proceedings of ICIS (2019)*, 2019. Available: https://doi.org/10.2139/ssrn.3488344

[4] J. R. Jensen and O. Ross, "Settlement with Distributed Ledger Technology," in *Conference Proceedings of ICIS (2020)*, 2020.

[5] B. Egelund-Müller, M. Elsman, F. Henglein, and O. Ross, "Automated Execution of Financial Contracts on Blockchains," *Bus. Inf. Syst. Eng.*, vol. 59, no. 6, pp. 457–467, 2017. Available: https://doi.org/10.1007/s12599-017-0507-z

[6] O. Ross and J. R. Jensen, “Compact Multiparty Verification of Simple Computations,” in *CEUR Workshop Proceedings*, 2018. Available: https://doi.org/10.2139/ssrn.3745627

[7] B. Düdder and O. Ross, “Timber Tracking: reducing Complexity of Due Diligence by using Blockchain Technology,” *SSRN*, 2017. Available: https://doi.org/10.2139/ssrn.3015219

[8] A. Antonopoulos and G. Wood, *Mastering Ethereum: Building Smart Contracts and DApps*. Sebastopol, CA: O’Reilly Media, 2018.

[9] V. von Wachter, J. R. Jensen, and O. Ross, “How Decentralized is the Governance of Blockchain-based Finance? Empirical Evidence from four Governance Token Distributions,” 2020. Available: https://arxiv.org/abs/2102.10096

[10] G. Wood, “Ethereum: A secure decentralized generalized Transaction Ledger EIP 150,” in *Ethereum Project Yellow Paper*, 2014, pp. 1–32.

[11] P. Daian *et al.*, “Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges,” 2019. Available: https://arxiv.org/abs/1904.05234

[12] W. Warren and A. Bandeali, “0x : An open Protocol for decentralized Exchange on the Ethereum Blockchain.” Available: https://github.com/0xProject

[13] G. Angeris, A. Evans, and T. Chitra, “When does the Tail wag the Dog? Curvature and Market Making,” 2020. Available: https://arxiv.org/abs/2012.08040

[14] G. Angeris, H.-T. Kao, R. Chiang, C. Noyes, and T. Chitra, “An Analysis of Uniswap Markets,” *Cryptoeconomic Systems*, vol. 1, no. 1, 2019. Available: https://doi.org/10.21428/58320208.c9738e64

[15] T. Chitra, “Competitive Equilibria between Staking and on-chain Lending,” *Cryptoeconomic Systems*, vol. 1, no. 1, 2021. Available: https://doi.org/10.21428/58320208.9ce1cd26

[16] J. Aoyagi, “Liquidity Provision by Automated Market Makers,” *SSRN*, 2020. Available: https://doi.org/10.2139/ssrn.3674178

[17] M. Tassy and D. White, “Growth Rate of A Liquidity Provider’s Wealth in XY = c Automated Market Makers,” 2020. Available: https://math.dartmouth.edu/~mtassy/articles/AMM_returns.pdf

[18] M. Bartoletti, J. H. Chiang, and A. Lluch-Lafuente, “SoK: Lending Pools in Decentralized Finance,” 2020. Available: https://arxiv.org/abs/2012.13230

[19] G. Tsoukalas and B. H. Falk, “Token-Weighted Crowdsourcing,” *Manag. Sci.*, vol. 66, no. 9, pp. 3843–3859, 2020. Available: https://doi.org/10.1287/mnsc.2019.3515

[20] D. Perez, S. M. Werner, J. Xu, and B. Livshits, “Liquidations: DeFi on a Knife-edge,” 2020. Available: https://arxiv.org/abs/2009.13235

[21] L. Luu, D.-H. Chu, H. Olickel, P. Saxena, and A. Hobor, “Making Smart Contracts Smarter,” in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS’16)*, pp.254–269, 2016. Available: https://doi.org/10.1145/2976749.2978309

[22] L. Gudgeon, D. Perez, D. Harz, B. Livshits, and A. Gervais, “The Decentralized Financial Crisis,” *Crypto Valley Conference on Blockchain Technology (CVCBT)*, pp. 1–15, 2020. Available: https://doi.org/10.1109/CVCBT50464.2020.00005

[23] V. von Wachter, J. R. Jensen, and O. Ross, “Measuring Asset Composability as a Proxy for Ecosystem Integration,” in *DeFi Workshop Proceedings of FC'21*, 2021. Available: https://arxiv.org/abs/2102.04227