Decentralized Finance: Protocols, Risks, and Governance

Other titles in Foundations and Trends® in Privacy and Security

Proofs, Arguments, and Zero-Knowledge
Justin Thaler
ISBN: 978-1-63828-124-5

Assured Autonomy Survey
Christopher Rouff and Lanier Watkins
ISBN: 978-1-63828-038-5

Hardware Platform Security for Mobile Devices
Lachlan J. Gunn, N. Asokan, Jan-Erik Ekberg, Hans Liljestrand, Vijayanand Nayani and Thomas Nyman
ISBN: 978-1-68083-976-0

Cloud Computing Security: Foundations and Research Directions
Anrin Chakraborti, Reza Curtmola, Jonathan Katz, Jason Nieh, Ahmad-Reza Sadeghi, Radu Sion and Yinqian Zhang
ISBN: 978-1-68083-958-6

Expressing Information Flow Properties
Elisavet Kozyri, Stephen Chong and Andrew C. Myers
ISBN: 978-1-68083-936-4

Decentralized Finance: Protocols, Risks, and Governance

Agostino Capponi
Columbia University
ac3827@columbia.edu

Garud Iyengar
Columbia University
garud@ieor.columbia.edu

Jay Sethuraman
Columbia University
jay@ieor.columbia.edu

now
the essence of knowledge
Boston — Delft

Foundations and Trends® in Privacy and Security

Published, sold and distributed by:
now Publishers Inc.
PO Box 1024
Hanover, MA 02339
United States
Tel. +1-781-985-4510
www.nowpublishers.com
sales@nowpublishers.com

Outside North America:
now Publishers Inc.
PO Box 179
2600 AD Delft
The Netherlands
Tel. +31-6-51115274

The preferred citation for this publication is

A. Capponi *et al.*. *Decentralized Finance: Protocols, Risks, and Governance*. Foundations and Trends® in Privacy and Security, vol. 5, no. 3, pp. 144–188, 2023.

ISBN: 978-1-63828-271-6

Foundations and Trends® in Privacy and Security
Volume 5, Issue 3, 2023

Editorial Board

Editorial Scope

Topics

Foundations and Trends® in Privacy and Security publishes survey and tutorial articles in the following topics:

- Access control
- Accountability
- Anonymity
- Application security
- Artifical intelligence methods in security and privacy
- Authentication
- Big data analytics and privacy
- Cloud security
- Cyber-physical systems security and privacy
- Distributed systems security and privacy
- Embedded systems security and privacy
- Forensics
- Hardware security
- Human factors in security and privacy
- Information flow
- Intrusion detection
- Malware
- Metrics
- Mobile security and privacy
- Language-based security and privacy
- Network security
- Privacy-preserving systems
- Protocol security
- Security and privacy policies
- Security architectures
- System security
- Web security and privacy

Information for Librarians

Foundations and Trends® in Privacy and Security, 2023, Volume 5, 4 issues. ISSN paper version 2474-1558. ISSN online version 2474-1566. Also available as a combined paper and online subscription.

Contents

Decentralized Finance: Protocols, Risks, and Governance

Agostino Capponi, Garud Iyengar and Jay Sethuraman

Department of Industrial Engineering and Operations Research, Columbia University, USA; ac3827@columbia.edu, garud@ieor.columbia.edu, jay@ieor.columbia.edu

ABSTRACT

Financial markets are undergoing an unprecedented transformation. Technological advances have brought major improvements to the operations of financial services. While these advances promote improved accessibility and convenience, traditional finance shortcomings like lack of transparency and moral hazard frictions continue to plague centralized platforms, imposing societal costs.

In this monograph, we argue how these shortcomings and frictions may be mitigated by the decentralized finance (DeFi) ecosystem. We delve into the workings of smart contracts, the backbone of DeFi transactions, with an emphasis on those underpinning token exchange and lending services.

We highlight the pros and cons of the novel form of decentralized governance introduced via the ownership of governance tokens. We argue that the current DeFi infrastructure introduces operational risks to users, which we segment into five primary categories: consensus mechanisms, protocol, oracle, frontrunning, and systemic risks.

We conclude by emphasizing the need for future research to focus on the scalability of existing blockchains, the im-

Agostino Capponi, Garud Iyengar and Jay Sethuraman (2023), "Decentralized Finance: Protocols, Risks, and Governance", Foundations and Trends® in Privacy and Security: Vol. 5, No. 3, pp 144–188. DOI: 10.1561/3300000036.

proved design and interoperability of DeFi protocols, and the rigorous auditing of smart contracts.

1

Introduction

Financial services have traditionally been provided through centralized platforms. Notable instances include Visa and Mastercard, the world's leading payment processing networks; Nasdaq, the globe's premier stock exchange; Vanguard and Blackrock, renowned for their investment and brokerage services; and JP Morgan Chase, offering a spectrum of banking services. While the centralized financial system is essential to provide intermediation services to the real economy, it can also be exclusionary and impose hefty costs on users. Take credit card companies as an example: they impose processing fees ranging from 2% to 4.35% of the transaction's value. Moreover, commercial banks frequently apply considerable service charges and loan interest rates, yet offer low interest rates on customer deposits. The cost of financing can be prohibitive for small borrowers who may find loans or mortgages inaccessible, leading them to depend on credit cards that demand high interest rates. Even access to basic financial services, such as payment services, can be uncertain, particularly in less developed regions where a significant portion of the population remains unbanked.

The integration of technology into finance has sparked the rise of alternative service providers that alleviate some of these concerns.

Emergent payment systems, like Square and Venmo, utilize mobile devices and internet technology to provide affordable, user-friendly payment solutions. These services are accessible to individuals and small businesses alike, democratizing access to financial systems

Peer-to-peer lending platforms, like Prosper and LendingClub, harness the power of technology to develop innovative lending marketplaces. These platforms offer an alternative to traditional credit sources by facilitating loans, primarily funded by institutional investors, to borrowers. Fintech brokerage platforms, such as Robinhood, enable users to execute commission-free trades of stocks, exchange-traded funds, and cryptocurrencies via mobile applications.

While these financial technology advancements offer increased convenience, inclusivity, and cost reductions, they also inherit several drawbacks associated with traditional centralized finance (CeFi). Firstly, decreases in transaction costs and enhancements in execution speed are not necessarily a given, as these fintech applications are constructed on the existing financial infrastructure. For instance, when receiving a payment through Venmo followed by a deposit into your bank account, a bank transfer must be initiated. Such transfers may take up to three business days to complete. Even though an instant transfer option exists, it remains a costly alternative, imposing a 1.75% fee.

Most extant fintech platforms still function as centralized, profit-driven entities, which often leads to moral hazard issues and societal costs. Several of these platforms have faced criticisms for prioritizing their own profitability over customer interests. A notable example is Robinhood Markets, a firm offering commission-free investment services, which was found to have routed customer order flows to high-frequency trading firms rather than stock exchanges, as indicated in Levine (2021).

Similarly, the lack of transparency in some peer-to-peer (P2P) lending platforms' credit assessment methodologies can lead to defaults and investor losses. As profit-oriented entities, P2P companies primarily aim to enhance their profits. Consequently, despite lenders' desire to steer clear of high-risk borrowers, P2P platforms may entice borrowers to take larger loans by offering appealing interest rates and neglecting credit risk. This moral hazard dilemma contributed to the downfall of numerous P2P lending firms, particularly in China, as reported in Liu (2021).

The advent of distributed ledger technologies presents an opportunity to alleviate some of the issues raised by centralized financial platforms, regardless of their integration of fintech enhancements. These technologies have the potential to further disrupt the financial service industry by facilitating the transition to a decentralized trading environment, also referred to as *decentralized finance* (DeFi). DeFi enables the provision of services such as exchanges, lending, derivatives trading, and insurance without the need for a centralized intermediary. The rest of the monograph is organized as follows. Section 2 provides an overview of the DeFi ecosystem, with a focus on exchanges, lending protocols, and the decentralized governance structure in place. Section 3 discusses the operational risks inherent in the design of smart contracts and the DeFi ecosystem. We provide concluding remarks and directions for future research in Section 4.

References

Aave. (2020). "Aave Protocol White Paper V1.0". *Tech. rep.* URL: https://github.com/aave/aave-protocol/blob/master/docs/Aave_Protocol_Whitepaper_v1_0.pdf.

Abad, J., P. Bains, Y. Chen, T. Ehlers, A. Pascual, F. Melo, J. Mok, N. Sugimoto, T. Tsuruga, Z. Yuan, and X. Zheng. (2022). "The rapid growth of fintech: vulnerabilities and challenges for financial stability". *Global Financial Stability Report*. Apr.

Adams, H., N. Zinsmeister, and D. Robinson. (2020). "Uniswap v2 Core". *Tech. rep.* URL: https://uniswap.org/whitepaper.pdf.

Akansha. (2022). "Everything you need to know about LUNA/Terra collapse: Oracle manipulation, lawsuits, supporters and hard fork". en-US. URL: https://blockmagnates.com/everything-you-need-to-know-about-luna-terra-collapse-oracle-manipulation-lawsuits-supporters-and-hard-fork/.

Aoyagi, J. and Y. Ito. (2021). "Coexisting Exchange Platforms: Limit Order Books and Automated Market Makers". *Working Paper*. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3808755.

Auer, R., J. Frost, and J. M. V. P. (2022). "Miners as intermediaries: extractable value and market manipulation in crypto and DeFi". *Tech. rep.* URL: https://www.bis.org/publ/bisbull58.pdf.

Aune, R., M. O'Hara, and S. Ouziel. (2017). "Footprints on the blockchain: Information leakage in distributed ledgers". *Working Paper, Cornell University*.

Bains, P., M. Diaby, D. Drakopoulos, J. Faltermeier, F. Grinberg, E. Papageorgiou, D. Petrov, P. Schneider, and N. Sugimoto. (2021). "The Crypto Ecosystem and Financial Stability Challenge". *Tech. rep.* International Monetary Fund.

Breidenbach, L., C. Cachin, B. Chan, A. Coventry, S. Ellis, A. Juels, F. Koushanfar, A. Miller, B. Magauran, D. Moroz, S. Nazarov, A. Topliceanu, F. Tramer, and F. Zhang. (2020). "Chainlink 2.0: Next Steps in the Evolution of Decentralized Oracle Networks". *Tech. rep.* URL: https://research.chain.link/whitepaper-v2.pdf?_ga=2.41628002.1737410159.1678218527-463163097.1677192019.

Brogaard, J., T. Hendershott, and R. Riordan. (2021). "Price discovery without trading: Evidence from limit orders". *Journal of Finance*. 74(4): 1621–1658.

Budish, E., P. Cramton, and J. Shim. (2015). "The High-Frequency Trading Arms Race: Frequent Batch Auctions as a Market Design Response". *The Quarterly Journal of Economics*. 130(4): 1547–1621.

Buterin, V. (2014). "A next generation smart contract & decentralized application platform". *Ethereum white paper*.

Canidio, A. and V. Danos. (2023). "Commitment Against Front Running Attacks". *Working Paper*.

Capponi, A. (2016). "Systemic Risk, Policies, and Data Needs". *INFORMS Tutorial in Operations Research*.

Capponi, A. and R. Jia. (2021). "The adoption of blockchain based decentralized exchanges". *Working Paper, Columbia University*. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3805095.

Capponi, A., R. Jia, and Y. Wang. (2022). "Allocative Inefficiencies in Public Distributed Ledgers". *Working Paper, Columbia University*. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3997796.

Capponi, A., R. Jia, and S. Yu. (2023). "Price Discovery on decentralized exchanges". *Working Paper, Columbia University*. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4236993.

Cong, L. and Z. He. (2019). "Blockchain Disruption and Smart Contracts". *The Review of Financial Studies*. 32(5): 1754–1797.

Cong, L., K. Tang, Y. Wang, and X. Zhao. (2022). "Inclusion and Democratization Through Web3 and DeFi? Initial Evidence from the Ethereum Ecosystem". *Working Paper*.

Daian, P., S. Goldfeder, T. Kell, Y. Li, X. Zhao, I. Bentov, L. Breidenbach, and A. Juels. (2020). "Flash Boys 2.0: Frontrunning in Decentralized Exchanges, Miner Extractable Value, and Consensus Instability". In: *2020 IEEE Symposium on Security and Privacy (SP)*. 910–927.

ECB Crypto-Assets Task Force. (2020). "Stablecoins: Implications for monetary policy, financial stability, market infrastructure and payments, and banking supervision in the euro area". *Tech. rep.* No. 247. European Central Bank.

Eskandari, S., S. Moosavi, and J. Clark. (2019). "Sok: Transparent dishonesty: front-running attacks on blockchain". In: *International Conference on Financial Cryptography and Data Security*. Springer. 170–189.

Ferreira, M. and D. Parkes. (2023). "Credible Decentralized Exchange Design via Verifiable Sequencing Rules". In: *Proceedings of the 55th Annual ACM Symposium on Theory of Computing*. 723–736.

Goldreich, O., S. Micali, and A. Wigderson. (1987). "How to play ANY mental game". In: *Proceedings of the 19th annual ACM symposium on Theory of computing*. 218–229.

Haber, S. and W. Stornetta. (1990). "How to time-stamp a digital document". In: *Conference on the Theory and Application of Cryptography*. 437–455.

Halaburda, H. and Y. Bakos. (2021). "Blockchains, Smart Contracts and Connected Sensors: Substitutes or Complements?" *Working paper*.

Hasbrouck, J. and R. Levich. (2021). "Network structure and pricing in the FX market". *Journal of Financial Economics*. 141(2): 705–729.

Hasbrouck, J., T. Rivera, and F. Saleh. (2022). "The Need for Fees at a DEX: How Increases in Fees Can Increase DEX Trading Volume". *Working Paper*. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4192925.

Lehar, A. and C. Parlour. (2021). "Decentralized Exchanges". *Working Paper*. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3905316.

Lehar, A. and C. Parlour. (2022). "Systemic Fragility in Decentralized Markets". *Working Paper*.

Levine, M. (2021). "Does Robinhood Need Payment for Order Flow?" *Bloomberg*. 14(1): 71–100.

Liu, J. (2021). "The rise and fall of China's online P2P lending". *Bloomberg*. URL: https://technode.com/2018/08/02/the-rise-and-fall-of-chinas-online-p2p-lending/.

Ma, Y., Y. Zheng, and A. Zhang. (2022). "Stablecoin Runs and the Centralization of Arbitrage". URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4398546.

Makarov, I. and A. Schoar. (2023). "Anatomy of a Run: The Terra Luna Crash". *NBER Working Paper Series*. (31160).

MakerDAO. (2022). "The Maker Protocol: MakerDAO's Multi-Collateral Dai (MCD) System". *White Paper*. URL: https://makerdao.com/en/whitepaper/.

Mercy Corps Ventures. (2022). "Pilot Launch | Savings for low-income users in Cameroon through DeFi bond tokenization". *Technical Report*.

Milionis, J., C. Moallemi, T. Roughgarden, and A. Zhang. (2022). "Automated Market Making and Loss-Versus-Rebalancing". *Working Paper*. URL: https://moallemi.com/ciamac/papers/lvr-2022.pdf.

Milionis, J., C. Moallemi, and T. Roughgarden. (2023). "Complexity-Approximation Trade-offs in Exchange Mechanisms: AMMs vs. LOBs". arXiv: /2302.11652 [q-fin.TR].

Nakamoto, S. (2008). "Bitcoin: A Peer-to-Peer Electronic Cash System". *Unpublished Manuscript*.

Park, A. (2021). "Conceptual Flaws of Decentralized Automated Market Making". *Working Paper*. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3805750.

President's Working Group. (2021). "Report on Stablecoins". *Working Paper*. Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency.

Qin, K., L. Zhou, Y. Afonin, L. Lazzaretti, and A. Gervais. (2021a). "CeFi vs. DeFi - Comparing Centralized to Decentralized Finance". arXiv: 2106.08157 [q-fin.TR].

Qin, K., L. Zhou, and A. Gervais. (2021b). "Quantifying Blockchain Extractable Value: How dark is the forest?" *arXiv preprint arXiv:2101.05511*.

Qin, K., L. Zhou, B. Livshits, and A. Gervais. (2021c). "Attacking the DeFi ecosystem with flash loans for fun and profit". In: *International Conference on Financial Cryptography and Data Security*. 3–32.

Saleh, F. (2021). "Blockchain without Waste: Proof-of-Stake". *Review of Financial Studies*. 34(3): 1156–1190.

Tomach, P., L. Yi, L. Shang-Wei, Y. Liu, and L. Zengxiang. (2021). "A Survey of Smart Contract Formal Specification and Verification". *ACM Computing Surveys*. 54(7): 1–38.

Torres, C. F., R. Camino, and R. State. (2021). "Frontrunner Jones and the Raiders of the Dark Forest: An Empirical Study of Frontrunning on the Ethereum Blockchain". In: *30th USENIX Security Symposium (USENIX Security 21)*. 1343–1359.

Uhlig, H. (2023). "A Luna-Tic Stablecoin Crash". *NBER Working Paper Series*. (30256).

Walch, A. (2019). "Deconstructing 'Decentralization': Exploring the Core Claim of Crypto Systems". In: *CRYPTOASSETS: LEGAL, REGULATORY, AND MONETARY PERSPECTIVES*. Ed. by C. Brummer. Oxford University Press.

Xu, J., N. Vavryk, K. Paruch, and S. Cousaert. (2021). "SoK: Decentralized Exchanges (DEX) with Automated Market Maker (AMM) protocols". arXiv: 2103.12732 [q-fin.TR].

Yao, A. (1982). "Protocols for secure computations". In: *Proceedings of the 23rd Annual IEEE Symposium on Foundations of Computer Science*. 160–164.

Zhang, F., D. Maram, H. Malvai, S. Goldfeder, and A. Juels. (2020). "DECO: Liberating Web Data Using Decentralized Oracles for TLS". In: *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*. 1919–1938.

Zhang, L. (2022). "Robust (Decentralized) Oracle Design". *Working Paper, Chicago Booth School of Business*.

Zhou, L., X. Xiong, J. Ernstberger, S. Chaliasos, Z. Wang, Y. Wang, K. Qin, R. Wattenhofer, D. Song, and A. Gervais. (2023). "SoK: Decentralized Finance (DeFi) Attacks". In: *The 44th IEEE Symposium on Security and Privacy*. IEEE.