

Agenda: Frontiers in DeFi

CSH Workshop, May 27th, 2024

Complexity Science Hub, Josefstädterstraße 39, 1080, Vienna

08:30 - 09:00 Arrival & Welcome

09:00 - 10:30

- *Contagion in Decentralized Lending Protocols* (Julien Prat)
- *Liquid Staking and Roll-ups: Enhancing or Challenging Ethereum DeFi?* (Krzysztof Gogol)
- *Secure contract composition in DeFi* (Riccardo Marchesin)
- *Non-Atomic Arbitrage in Decentralized Finance* (Vabuk Pahari)

10:30 - 11:00 Coffee break

11:00 - 12:00

- *Arbitrageurs' profits, LVR, and sandwich attacks: batch trading as an AMM design response* (Robin Fritsch / Andrea Candido)
- *The governance of decentralized autonomous organizations: A study of contributors' influence, networks, and shifts in voting power* (Pietro Saggese)
- *Strategic Vote Timing in Online Elections With Public Tallies* (Svetlana Abramova)

12:00 - 13:30 Lunch Break

13:30 - 15:00

- *Risk Premiums in the Bitcoin Market* (Maria Grith)
- *Testing a rational Crypto Bubble* (Christoph Wegener)
- *The Economics of Non-Fungible Tokens* (Nicola Borri)
- *Quantinar: A Blockchain p2p Ecosystem for Scientific Research* (Wolfgang Härdle)

15:00 - 15:30 Coffee break

15:30 - 17:00

- *The DeFi dilemma* (Stefan Voigt)
- *Automated Market Makers Designs Beyond Constant Functions* (Fayçal Drissi)
- *Cryptocurrency Pair Trading* (Ronald Hochreiter)
- *Would Friedman burn your Tokens?* (Jan Schlegel)

Title: Contagion in Decentralized Lending Protocols

Speaker: Julien Prat

Abstract: We study financial contagion in Compound V2, a decentralized lending protocol deployed on the Ethereum blockchain. We explain how to construct the balance sheets of Compound's liquidity pools and use our methodology to characterize the financial network. Our analysis reveals that most users either borrow stablecoins or engage in liquidity mining. We then study the robustness of Compound through a series of stress tests, identifying the pools that are most likely to set off a cascade of defaults.

Short Bio: Julien Prat is a CNRS director of research and an associate professor of economics at Ecole Polytechnique. He is an expert in information economics, contract theory and labor economics. His current projects focus on the optimal design and financial implications of decentralized systems.

Title: Liquid Staking and Roll-ups: Enhancing or Challenging Ethereum DeFi?

Speaker: Krzysztof Gogol

Abstract: Liquid staking tokens (LSTs) and roll-ups represent novel approaches to Decentralizing Finance (DeFi). LSTs simplify staking by tokenizing assets staked at validators. Roll-ups, new forms of layer-2 blockchain, enhance DeFi scalability and efficiency while still relying on Ethereum security. Nevertheless, both solutions introduce new complexities. Liquid staking, and related re-staking, alter the assumptions behind the PoS blockchain's security, while roll-ups expose users to liquidity fragmentation and bridging risks. Although roll-ups mitigate MEV attacks, relying on centralized aggregators (sequencers) also brings centralization risks.

Short Bio: Krzysztof is a tech entrepreneur with expertise in the field of blockchain, Decentralized Finance (DeFi), and FinTech. Currently serving as a PhD Candidate at the University of Zurich, Krzysztof is involved in researching a layer-2 blockchain approach for the security and scalability of DeFi protocols. He has been actively engaged in supporting and advising projects in the areas of DeFi, CBDCs, and digital asset management. Furthermore, Krzysztof brings experience as the Founder and CEO of a successful fintech company in the wealth management space.

<https://arxiv.org/abs/2403.10226> Liquid Staking Tokens in Automated Market Makers

<https://arxiv.org/abs/2401.16353> Empirical and Theoretical Analysis of Liquid Staking Protocols

Title: Secure Contract Composition in DeFi

Speaker: Riccardo Marchesin

Complexity Science★Hub

Abstract: In the context of DeFi, complex financial services are often constructed by composing a variety of simple smart contracts. This exposes them to risk: an adversary may target any of the underlying contracts to economically damage the compound service. This talk will present the notion of MEV non-interference, proposing it as a way to define secure composability for smart contracts. The talk will also draw comparisons between MEV non-interference and the notion of ϵ -composability, introduced by Babel et al in 2021.

Short Bio: Riccardo Marchesin is a PhD student in Mathematics at the University of Trento. His research focuses on the security of smart contracts.

Link Paper: <https://arxiv.org/abs/2309.10781>

Link Personal Page: <https://r-marche.github.io/>

Title: Non-Atomic Arbitrage in Decentralized Finance

Speaker: Vabuk Pahari

Abstract: The prevalence of Maximal Extractable Value (MEV) in the Ethereum ecosystem has led to a characterization of the latter as a Dark Forest. Studies of MEV have thus far largely been restricted to purely on-chain MEV, i.e., sandwich attacks, cyclic arbitrage, and liquidations. In this work, we shed light on the prevalence of non-atomic arbitrage on decentralized exchanges (DEXes) on the Ethereum blockchain. Importantly, non-atomic arbitrage exploits price differences between DEXes on the Ethereum blockchain as well as exchanges outside the Ethereum blockchain (i.e., centralized exchanges or DEXes on other blockchains). Thus, non-atomic arbitrage is a type of MEV that involves actions on and off the Ethereum blockchain.

In our study of non-atomic arbitrage, we uncover that more than a fourth of the volume on Ethereum's biggest five DEXes from the merge until 31 October 2023 can likely be attributed to this type of MEV. We further highlight that only eleven searchers are responsible for more than 80% of the identified non-atomic arbitrage volume sitting at a staggering \$132 billion and draw a connection between the centralization of the block construction market and non-atomic arbitrage. Finally, we discuss the security implications of these high-value transactions that account for more than 10% of Ethereum's total block value and outline possible mitigations.

Short Bio: Vabuk Pahari is a PhD student at the Max-Planck-Institute for Software Systems (MPI-SWS), where Prof. Krishna P. Gummadi advises me. His research focuses on blockchain protocols, cryptocurrencies, and DeFi, with a focus on studying the transparency and decentralization of these systems. During his Ph.D., he studied the lack of transparency in transaction prioritization in blockchains and the effects of MEV on transaction prioritization. He is also interested in understanding the existing mechanisms for decentralized governance across DAOs, as well as ways to enable more decentralization in DAOs.

Profile Link: <https://vpahari.github.io/>

Paper Link: <https://arxiv.org/pdf/2401.01622.pdf>. (To appear at S&P 2024)

Title: Arbitrageurs' profits, LVR, and sandwich attacks: batch trading as an AMM design response

Speaker: Robin Fritsch / Andrea Candido

Abstract: We study a novel automated market maker design: the function maximizing AMM (FM-AMM). Our central assumption is that trades are batched before execution. Because of competition between arbitrageurs, the FM-AMM eliminates arbitrage profits (or LVR) and sandwich attacks, currently the two main problems in decentralized finance and blockchain design more broadly. We then consider 11 token pairs and use Binance price data to simulate the lower bound to the return of providing liquidity to an FM-AMM. Such a lower bound is, for the most part, slightly higher than the empirical returns of providing liquidity on Uniswap v3 (currently the dominant AMM)

Short Bio: Andrea Canidio is a senior research economist at CoW Protocol. Before that, he taught at Central European University, INSEAD, and IMT School for Advanced Studies. Robin Fritsch is completing his PhD in Computer Science at ETH Zurich."

Paper Link: <https://arxiv.org/abs/2307.02074>

Title: The governance of decentralized autonomous organizations: A study of contributors' influence, networks, and shifts in voting power.

Speaker: Pietro Saggese

Abstract: We present a study analyzing the voting behavior of contributors, or vested users, in Decentralized Autonomous Organizations (DAOs). We evaluate their involvement in decision-making processes, discovering that in at least 7.54% of all DAOs, contributors, on average, held the necessary majority to control governance decisions. Furthermore, contributors have singularly decided at least one proposal in 20.41% of DAOs. Notably, contributors tend to be centrally positioned within the DAO governance ecosystem, suggesting the presence of inner power circles. Additionally, we observed a tendency for shifts in governance token ownership shortly before governance polls take place in 1202 (14.81%) of 8116 evaluated proposals. Our findings highlight the central role of contributors across a spectrum of DAOs, including Decentralized Finance protocols. Our research also offers important empirical insights pertinent to ongoing regulatory activities aimed at increasing transparency to DAO governance frameworks.

Short Bio: Pietro Saggese has been an Assistant Professor at IMT School for Advanced Studies Lucca, Italy, since November 2023. He was a postdoctoral researcher at the Complexity Science Hub and the AIT Austrian Institute of Technology from May 2021 until October 2023. Pietro obtained his PhD at the Economics and Data Science department, IMT School for Advanced Studies in Lucca, in July 2021. He started delving into complex systems and economics during his university studies at the University of Turin, where he obtained both his bachelor's and master's degrees in physics. During his PhD studies, he worked on the identification of the arbitrage activity within the Bitcoin ecosystem – and of the investors who conducted it. The goal of these studies is to provide empirical evidence (yet lacking in the literature) of the nature of the arbitrageurs, showing that such investors are few, sophisticated, and specialized users, in contrast with theoretical assumptions from traditional finance. In his current research, Pietro is focusing mainly on crypto asset analytics, and in

Complexity Science*Hub

particular on investigating the interplay between Decentralised Finance (DeFi) protocols deployed in Ethereum, to gain insights into the potential risks and opportunities associated with them. His research interests include crypto-finance, crypto asset analytics, CBDCs, and their socio-economic implications.

Profile Link: <https://www.linkedin.com/in/pietro-saggese-519718166/>

Paper Link: <https://arxiv.org/abs/2309.14232>

Title: Strategic Vote Timing in Online Elections With Public Tallies

Speaker: Svetlana Abramova

Abstract: Many online elections are conducted sequentially, where interim results are known to the electorate and can be used by voters to inform their decisions. One example of such voting schemes is blockchain governance mechanisms, in which token holders publicly vote on protocol changes on a blockchain. When votes are public and costly, the strategic importance of choosing when to cast a vote arises. In particular, there is a tension between voting early to influence future votes and waiting to observe interim results and avoid voting costs if the outcome has already been decided. Against this background, this talk will present a novel game-theoretical model, where the electorate consists of informed voters who have a preferred candidate, and uninformed swing voters who can be swayed according to the interim outcome at the time of voting. For a three-player game with two strategic and one non-strategic voters, different equilibrium behaviors emerge depending on the parameter constraints.

Short bio: Svetlana Abramova has been a scientist at the Austrian Institute of Technology since May 2024. She obtained her Ph.D. at the Department of Computer Science of the University of Innsbruck, where she afterward worked as a postdoctoral researcher and assistant professor. Her research interests span empirical and theoretical perspectives on security, privacy, digital money, and decentralized systems, with a strong focus on economic, human, behavioral, and social aspects. She is particularly interested in interdisciplinary and multi-method research, at the frontier between computer science, information systems, economics, and social sciences.

Paper Link: <https://arxiv.org/abs/2402.09776>

Title: Risk Premiums in the Bitcoin Market

Speaker: Maria Grith

Abstract: We adopt options and realized returns to analyze risk premiums in the Bitcoin market. By decomposing the index risk premium into different parts of the return space, we find that negative returns explain one-third of the total Bitcoin equity premium (EP). This is not only in contrast to results for the S&P 500 market, for which moderately negative returns explain 70% of the EP (Beason and Schreindorfer, 2022), but also challenges conventional macrofinance models based on habit, disasters, and long-run risk explanations. To verify if risk premium is time-varying and dependent on market conditions, we identify data clusters

Complexity Science*Hub

based on the sequence of risk-neutral densities estimated from option prices. The risk-neutral variance arises as the leading state variable characterizing these clusters. During low-volatility market states, the returns of at-the-money options suggest that investors are mainly concerned with variance risk. By investigating the out-of-the-money option returns, we find that losses are more painful, and leveraged bets are more attractive for investors during periods of low volatility.

Short bio: Dr. Maria Grith is an Assistant Professor of Econometrics at Erasmus University Rotterdam, with a Ph.D. in Economics from Humboldt University of Berlin. Her research focuses on statistical methods for analyzing high-dimensional data settings in finance, using nonparametric, semiparametric, functional data analysis, and machine learning approaches. She has co-authored articles in statistics, econometrics, and finance journals and coordinates the Erasmus School of Economics Female Network, promoting gender diversity in economics. Dr. Grith also collaborates with IDA - the Institute of Digital Assets.

Profile Link: <https://www.eur.nl/people/maria-grith>

Title: Testing a rational Crypto Bubble (co-authored by Simon Trimborn)

Speaker: Christoph Wegner

Abstract: The meteoric rise of Bitcoin has captivated the attention of market participants and researchers alike, sparking debates regarding the underlying drivers of its price fluctuations. A central inquiry revolves around whether these movements are driven by speculative fervor, potentially indicative of rational bubbles. However, assessing such hypotheses poses a significant challenge, given the elusive nature of defining Bitcoin's fundamental value, which lacks consensus among scholars. In response, our study uses a novel approach to investigate rational bubbles in the Bitcoin market. Rather than relying on proxies for Bitcoin's fundamental value, we employ a robust methodology centered on futures prices. By integrating a trending risk premium component within the futures price, our method demonstrates resilience and offers valuable insights into the dynamics of rational bubbles in the crypto ecosystem.

Short Bio: Christoph Wegner holds the Junior Professorship for Quantitative Methods in Economics at the Center for Methodology, Leuphana University, Lüneburg., Lüneburg. His academic journey culminated in the attainment of a doctoral degree (Dr. rer. pol.) in Economics from Leibniz University, Hannover, in 2016. His research interests span various domains, encompassing applied and financial econometrics, energy economics, and (corporate) finance. Notably, he is deeply engaged in exploring carbon finance and rigorously testing the Efficient Market Hypothesis. In addition to his academic endeavors, he has the privilege of serving as an associate editor on the editorial board of Finance Research Letters.

Profile Link: www.christoph-wegener.info

Title: The Economics of Non-Fungible Tokens

Speaker: Nicola Borri

Abstract: We construct a comprehensive dataset of NFT transactions, analyze their properties and create indices for the overall market. Individual collections misrepresent the broader market, highlighting the importance of a holistic perspective. Our data granularity allows high-resolution testing of theories of blockchain economics and more broadly markets with frictions. Firstly, we highlight the significance of unique NFT characteristics, particularly visual attributes extracted via machine-learning, in valuation, establishing their substantial non-fungible nature. Second, we establish that the market is strongly segmented and has no clear dominant players. Third, we determine the implications of the frictional market structure on returns and investor performance.

Short Bio: I am an Associate Professor of Finance in the Department of Economics and Finance at LUISS University, Rome. I joined the faculty at LUISS in 2009, after completing my Ph.D. in economics at Boston University. I also hold a BA and a MA in economics from Bocconi University, Milan. My research interests are primarily at the intersection of finance and macroeconomy, with a focus on quantitative asset pricing and fintech. I am an Associate Editor at *Economics Letters*. Some of my recent papers appeared in the *Review of Asset Pricing Studies*, *Journal of Banking & Finance*, *Review of Economic Dynamics*, and *Journal of Empirical Finance*.

Profile Link: <https://www.nicolaborri.com>

Title: Quantinar: A Blockchain p2p Ecosystem for Scientific Research

Speaker: Wolfgang Härdle

Abstract: Living in the Information Age, the power of data and correct statistical analysis has never been more prevalent. Academics and practitioners nowadays require an accurate application of quantitative methods. Yet many branches are subject to a crisis of integrity, which is shown in an improper use of statistical models, \$p\$-hacking, HARKing, or failure to replicate results. We propose the use of a Peer-to-Peer (P2P) ecosystem based on a blockchain network, Quantinar (quantinar.com), to support quantitative analytics knowledge paired with code in the form of Quantlets (quantlet.com) or software snippets. The integration of blockchain technology makes Quantinar a decentralized autonomous organization (DAO) that ensures fully transparent and reproducible scientific research.

Short Bio: Wolfgang Karl Härdle's research focus is on quantitative finance, in particular on multivariate methods in finance, as well as on methods for dimension reduction and computer-based statistics. Prof. Härdle is a co-founder of the BRC Blockchain Research Center (2020-). The BRC serves as a platform for academics and industry practitioners for scientific discussions and collaborations on blockchain technology. He managed the Collaborative Research Center CRC649 „Economic Risk“ (2005-2016) which researched multiple forms of risks in a global context. He is head of the Sino-German Research Training Group IRTG1792 “High Dimensional Non-Stationary Time Series” (2013-2023). WK Härdle is known for paradigm-shifting research directions. He develops new research technologies like machine learning, explainable AI, digital art, and crypto indices that are based on

Complexity Science★Hub

statistical analysis of ultra-high dimensional data structures. Since 2019 he has been a Yushan Scholar 玉山學者 in Taiwan. He also is a senior advisor to the Sim Lee Boon Institute for Financial Economics, SMU, Singapore. He invented CRIX the CRyptocurrency IndeX. He is affiliated as a Senior Advisor with the Asian Competitiveness Institute, NUS, Singapore. He has created IDA (2023-), the Institute Digital Assets, Bucharest University of Economic Sciences, Romania. He is a board member of the AIFM royalton-partners.com Luxembourg.

Profile Link: <https://www.linkedin.com/in/wolfgang-karl-h%C3%A4rdle-499739287/>

Paper Link: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4275797

Title: The DeFi Dilemma

Speaker: Stefan Voigt

Abstract: Blockchain technology enables financial interactions without central counterparties by distributing pending transactions in an open network {and} offering compensation fees to validators in order to ensure a reliable record of transaction histories. We show that these essential building blocks of decentralized settlement make decentralized finance (DeFi) applications inherently inefficient: Front-running risk causes a wasteful arms race for transaction fees and renders arbitrage prohibitively costly. Exploiting a novel, granular dataset of prices and transactions on decentralized exchanges, we show that cross-exchange price differences are substantial and persistent, while transaction fees almost entirely consume arbitrage profits. Overcoming these inefficiencies is possible only by reinstalling central counterparties, thus undermining the fundamental principle of DeFi.

Bio: Stefan is a tenure-track assistant professor of Finance at the Department of Economics at the University of Copenhagen and a research fellow at the Danish Finance Institute. His research is anchored in the intersection of market microstructure, asset pricing, and financial econometrics. Stefan has a deep interest in the economic implications and evolution of blockchain-based settlement in financial markets. He is also co-author of the books Tidy Finance with R and Tidy Finance with Python.

Profile Link: www.voigtstefan.me

Title: Automated Market Makers Designs Beyond Constant Functions

Speaker: Fayçal Drissi

Abstract: Popular automated market makers (AMMs) use constant function markets (CFMs) to clear demand and supply of liquidity. A key drawback in the implementation of CFMs is that liquidity providers (LPs) provide liquidity at a loss. We propose a new design for decentralized venues called the arithmetic liquidity pool (ALP). In the ALP, LPs decide whether or not to commit their liquidity, and the protocol (i) specifies impact functions that determine how orders impact the exchange rate in the pool, and (ii) sets the price of liquidity in the form of dynamic quotes around the exchange rate. We show that CFMs are a subset of ALP; specifically, there are impact functions and quotes in the ALP that replicate the price

Complexity Science*Hub

dynamics and execution costs of any CFM. We show that the price of liquidity in CFMs is suboptimal in the ALP for LPs that maximize wealth. Finally, we propose a family of ALPs where the dynamic quotes incorporate tolerance to risk and views on the demand for liquidity to maximize the expected profit of LPs. Our quotes are obtained in closed form and we use transaction data from Binance and Uniswap v3 to show that liquidity provision is not a loss-leading activity in an ALP that implements our quotes.

Short Bio: Fayçal Drissi is a postdoctoral researcher at the Oxford-Man Institute, University of Oxford. Holding a Ph.D. in Mathematics from Université Paris 1 Panthéon-Sorbonne, Fayçal's academic journey has been enriched by prior experience in the hedge-fund industry, where he spent five years engaged in research and development concerning derivatives pricing and systematic trading. Fayçal's research is centered on the integration of Mathematics and Machine Learning to address financial decision problems across both traditional finance and decentralized finance sectors. His interests span transfer learning, deep partial differential equation (PDE) solving, optimal execution, and market-making strategies. Notably, Fayçal is an active member of the organizing committee for the OMI Finance seminar at the University of Oxford. This seminar serves as a platform to discuss and promote academic and industrial research addressing emerging challenges in finance. Covering topics such as economics, microstructure, monetary policy, decentralized finance, and financial technology, the seminar aims to showcase recent and cutting-edge contributions in the field. For those interested in attending or presenting at the seminar, Fayçal is the point of contact.

Paper Link: https://www.faycaldrissi.com/workingpapers/amm_alp

Title: Cryptocurrency Pair Trading

Speaker: Ronald Hochreiter

Abstract: Pair trading is a strategy that relies on betting on the relative mispricing of the spread between two securities that share a long-term relationship. These strategies have shown to perform well with equities, however, not much research has been conducted in the field of cryptocurrencies, even though this asset class has shown characteristics suggesting suitability for pair trading. Various classical and contemporary methods including machine learning are compared and analyzed.

Bio: Ronald Hochreiter is a Senior Scientist at the Research Department of Computational Methods at the WU Vienna University of Economics and Business. He is the president of the Academy of Data Science in Finance, vice president of the Austrian Society of Operations Research, and senior member of the Association for Computing Machinery. He leads various European research projects, e.g. the WP "AI for Financial Markets" of the EU MSCA Doctoral Network on Digital Finance. Furthermore, he is actively providing consulting on AI for business and management for various companies.

Website Link: <https://hochreiter.net/>

Paper Link: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4433530

Title: Would Friedman burn your Tokens?

Speaker: Jan Christoph Schlegel

Abstract: Cryptocurrencies come with a variety of tokenomic policies as well as aspirations of desirable monetary characteristics that have been described by proponents as “sound money” or even “ultra sound money.” These propositions are typically devoid of economic analysis so

it is a pertinent question how such aspirations fit in the wider context of monetary economic theory. In this work, we develop a framework that determines the optimal token supply policy of a cryptocurrency, as well as investigate how such a policy may be algorithmically implemented. Our findings suggest that the optimal policy complies with the Friedman rule and it is dependent on the risk-free rate, as well as the growth of the cryptocurrency platform. Furthermore, we demonstrate a wide set of conditions under which such policy can be implemented via contractions and expansions of token supply that can be realized algorithmically with block rewards, taxation of consumption and burning the proceeds, and blockchain oracles.

Short Bio: Christoph works on questions of mechanism design in blockchain systems. He has worked on several projects on problems such as the design of transaction ordering policies, transaction fee mechanisms, AMMs, and auctions in a blockchain context. Currently, Christoph is interested in understanding competition between mechanisms deployed on blockchains, auctions in the MEV supply chain, and questions of distribution and decentralization.

Website Link: christophschlegel.com