IJTCS 2022, Game Theory in Blockchain

Aug. 17, Beijing time

**Speaker contacts information: Do NOT post online**

Christian Catalini [catalini@mit.edu](mailto:catalini@mit.edu), [christian@catalini.com](mailto:christian@catalini.com)

Ye Li [liye@uw.edu](mailto:liye@uw.edu)

Ravi Jagadeesan [ravi.jagadeesan@gmail.com](mailto:ravi.jagadeesan@gmail.com)

Yuqing Kong [yuqing.kong@pku.edu.cn](mailto:yuqing.kong@pku.edu.cn)

Mengqian Zhang [mengqian@sjtu.edu.cn](mailto:mengqian@sjtu.edu.cn)

Hongyin Chen [chenhongyin@pku.edu.cn](mailto:chenhongyin@pku.edu.cn)

Stefanos Leonardos [sleonardos@outlook.de](mailto:sleonardos@outlook.de)

Vassilis Zikas [vassilis.zikas@gmail.com](mailto:vassilis.zikas@gmail.com)

Zhanghao Yao [zhyao@post.usts.edu.cn](mailto:zhyao@post.usts.edu.cn)

**Invited Speakers**

Keynote: Christian Catalini. Founder, MIT Cryptoeconomics Lab and Research Scientist, MIT

Ye Li, University of Washington

Ravi Jagadeesan, Stanford University

Yuqing Kong, Peking University

Mengqian Zhang, Shanghai Jiao Tong University

Hongyin Chen, Peking University

Stefanos Leonardos, King's College London

Vassilis Zikas, Purdue University

**Accepted Paper**

Zhanghao Yao, Suzhou University of Science and Technology

**Program**

9am-9:55am Keynote: Christian Catalini, Massachusetts Institute of Technology

10am-10:25am Ye Li, University of Washington

10:30am-10:55am Ravi Jagadeesan, Stanford University

11am-11:25am Yuqing Kong, Peking University

11:30am-11:55am Mengqian Zhang, Shanghai Jiao Tong University

12pm-1pm Lunch break

1pm-1:25pm Zhanghao Yao, Suzhou University of Science and Technology

1:30pm-1:55pm Hongyin Chen, Peking University

2pm-2:25pm Stefanos Leonardos, King's College London

2:30pm-2:55pm Vassilis Zikas, Purdue University

**Talk Information**

9am-9:55am Christian Catalini

Founder, MIT Cryptoeconomics Lab and Research Scientist, MIT

**Keynote: How Crypto, Stablecoins, CBDCs and Web3 Will Reshape Competition**

**Abstract:** The talk will explore some of the recent developments in the crypto, payments and web3 space, as well as implications for competition and innovation.

**Bio:** Christian Catalini is the Co-Founder and Chief Strategy Officer of Lightspark. Christian is also the founder of the MIT Cryptoeconomics Lab, and a Research Scientist at MIT. Previously, he was a co-creator of Diem (formerly Libra), Chief Economist of the Diem Association, and Head Economist of Meta FinTech. While a Professor at MIT, Christian designed the MIT Digital Currency Research Study. In 2018, Christian was appointed as a Faculty Research Fellow in the Productivity, Innovation and Entrepreneurship Program at the National Bureau of Economic Research. Christian's academic research focuses on blockchain technology and cryptocurrencies, and he previously worked on the economics of equity crowdfunding and startup growth, and the economics of scientific collaboration. He holds a PhD from the University of Toronto (Rotman School of Management), and MSc (summa cum laude) in Economics and Management of New Technologies from Bocconi University, Milan. Christian’s research has been featured in Nature, Science, the New York Times, the Wall Street Journal, the Economist, WIRED, NPR, Forbes, Bloomberg, TechCrunch, the Chicago Tribune, the Boston Globe, VICE news and the Washington Post among others. Christian has presented his work at a variety of institutions including Harvard University, MIT, Yale University, London Business School, New York University, UC Berkeley, Stanford University, the Federal Reserve Bank, the US Treasury, the U.S. Securities and Exchange Commission, the Commodity Futures Trading Commission, the World Bank, the IMF, the White House OSTP, and a number of central banks and regulators.

10am-10:25am Ye Li, University of Washington

**Token Design and Economic Incentives**

**Abstract:** We develop a dynamic model of platform economy where tokens serve as a means of payments among platform users and are issued to finance investment in platform productivity. Tokens are optimally issued to reward platform owners when the productivity-normalized token supply is low and burnt to boost the franchise value when the productivity-normalized normalized supply is high. Although token price is determined in a liquid market, the platform's financial constraint generates an endogenous token issuance cost, causing underinvestment through the conflict of interest between insiders (platform owners) and outsiders (users). Blockchain technology mitigates underinvestment by addressing the platform's time-inconsistency problem.

**Bio:** Ye Li - PhD in Finance and Economics from Columbia University and Assistant Professor of Finance (William W. Alberts Endowed Professor in Finance) at University of Washington. Ye Li is also an advisor to the Bank of Canada in the area of digital currency, a Lamfalussy Research Fellow at the European Central Bank, an elected member of the Finance Theory Group, an invited member of the Macron Finance Society, and a research affiliate of CESifo in Germany. Ye Li has published papers on the top economics and finance journals, such as the American Economic Review, Review of Financial Studies, and Journal of Financial Economics, in the area of monetary economics, blockchain and cryptocurrency, and token-financed platform development. He collaborated with researchers from the leading academic institutions and central banks around the world, such as the Federal Reserve System of the U.S. and Bank of England, and his research has been presented at leading academic conferences in Asia, Europe, and the U.S.

10:30am-10:55am Ravi Jagadeesan, Economics Department, Stanford University

**Markets for Crypto Tokens, and Security under Proof of Stake**

**Abstract:** Cryptocurrency systems based on proof of stake (PoS) grant governance rights to the holders of currency tokens and therefore are vulnerable to attack by adversaries who buy tokens in order to gain control. To evaluate the robustness of PoS cryptocurrencies to such attacks, we model the market for tokens and determine how the cost of attacking the system depends on the level and shape of token supply and demand. We show that, contrary to popular belief, the appreciation of tokens in response to demand by attackers plays a small role in securing the system. In particular, stablecoins can be less vulnerable to attack than cryptocurrencies that are freely floating. Moreover, PoS cryptocurrencies that primarily function as mediums of exchange are vulnerable to attack if the velocity of money is high.

**Bio:** Ravi Jagadeesan is an Assistant Professor of Economics at Stanford University. His research interests are in market design, economic theory, and public economics. He received a Ph.D. in Business Economics from Harvard University in 2020.

11am-11:25am Yuqing Kong, Center on Frontiers of Computing Studies, Peking University

**Eliciting Information without Verification**

**Abstract:** When we use the wisdom of the crowds, we usually rank the answers according to their popularity, especially when we cannot verify the answers. However, this can be very dangerous when the majority make systematic mistakes. A fundamental question arises: can we build a hierarchy among the answers without any prior where the higher-ranking answers, which may not be supported by the majority, are from more sophisticated people? To address the question, we propose 1) a novel model to describe people's thinking hierarchy; 2) two algorithms to learn the thinking hierarchy without any prior; 3) a novel open-response based crowdsourcing approach based on the above theoretic framework. In addition to theoretic justifications, we conduct four empirical crowdsourcing studies and show that a) the accuracy of the top-ranking answers learned by our approach is much higher than that of plurality voting (In one question, the plurality answer is supported by 74 respondents but the correct answer is only supported by 3 respondents. Our approach ranks the correct answer the highest without any prior); b) our model has a high goodness-of-fit, especially for the questions where our top-ranking answer is correct. To the best of our knowledge, we are the first to propose a thinking hierarchy model with empirical validations in the general problem-solving scenarios; and the first to propose a practical open-response based crowdsourcing approach that beats plurality voting without any prior.

**Bio:** Yuqing Kong is currently an assistant professor at The Center of Frontier Computing Science (CFCS), Peking University. She obtained her Ph.D. degree from the Computer Science and Engineering Department at University of Michigan in 2018 and her bachelor degree in mathematics from University of Science and Technology of China in 2013.

Her research interests lie in the intersection of theoretical computer science and the areas of economics: information elicitation, prediction markets, mechanism design, and the future applications of these areas to crowdsourcing and machine learning. Her papers were published in several conferences include WINE, ITCS, EC, SODA, AAAI, NeurIPS, ICLR, ECCV, IJCAI, WWW.

11:30am-11:55am Mengqian Zhang, Shanghai Jiao Tong University

**Insightful Mining Equilibria**

**Abstract:** The selfish mining attack, arguably the most famous game-theoretic attack in blockchain, indicates that the Bitcoin protocol is not incentive-compatible. Most subsequent works mainly focus on strengthening the selfish mining strategy, thus enabling a single strategic agent more likely to deviate. In sharp contrast, little attention has been paid to the resistant behavior against the selfish mining attack, let alone further equilibrium analysis for miners and mining pools in blockchain as a multi-agent system.

In this talk, first, we propose a strategy called insightful mining to counteract selfish mining. By infiltrating an undercover miner into the selfish pool, the insightful pool could acquire the number of its hidden blocks. We prove that, with this extra insight, the utility of the insightful pool could be strictly greater than the selfish pool’s when they have the same mining power. Then we investigate the mining game where all pools can either choose to be honest or take the insightful mining strategy. We characterize the Nash equilibrium of this mining game and derive three corollaries: (a) each mining game has a pure Nash equilibrium; (b) there are at most two insightful pools under equilibrium no matter how the mining power is distributed; (c) honest mining is a Nash equilibrium if the largest mining pool has a fraction of mining power no more than 1/3.

Based on joint work with Yuhao Li, Jichen Li, Chaozhe Kong, and Xiaotie Deng.

**Bio:** Mengqian Zhang is a Ph.D. student in the Department of Computer Science and Engineering at Shanghai Jiao Tong University. Before this, she got the B.E. degree in computer science from Ocean University of China in 2018. Since July 2019, she has been a visiting scholar at Center on Frontiers of Computing Studies, Peking University. Her research interests include blockchain and algorithmic game theory.

12pm-1pm Lunch break

1pm-1:25pm Zhanghao Yao, Suzhou University of Science and Technology

**Equilibrium analysis of block withholding attack: an evolutionary game perspective**

**Abstract:** With the advancement of blockchain technology, blockchain-based digital cryptocurrencies, like Bitcoin, have received broad interest. Due to the permissionless environment, the blockchain is vulnerable to different kinds of attacks, such as the block withholding (BWH) attack. BWH attack is one common selfish mining attack, by which the attacking pool infiltrates the attacked pool, and the infiltrating miners withhold all the blocks newly discovered in the attacked pool. Therefore, the attacking pool benefit by withholding blocks, damaging the revenue-sharing rights of honest pools. In this paper, we introduce the additional rewards to the miners who successfully mine blocks, and propose an evolutionary game model for BWH attack among pools to study the strategy selection of pools. By constructing the replicator dynamic equations, the evolutionary stable strategies of pools are explored based on different levels of additional rewards. Our results provide enlightening significance to mitigate the negative influence from BWH attacks in practice.

**Bio:** Zhanghao Yao, a postgraduate student of the Business School, Suzhou University of Science and Technology. His research interests include blockchain and game theory.

1:30pm-1:55pm Hongyin Chen, Peking University

**FileInsurer: A Scalable and Reliable Protocol for Decentralized File Storage in Blockchain**

**Abstract:** With the development of blockchain applications, the requirements for file storage in blockchain are increasing rapidly. Many protocols, including Filecoin, Arweave, and Sia, have been proposed to provide scalable decentralized file storage for blockchain applications. However, the reliability is not well promised by existing protocols. Inspired by the idea of insurance, we innovatively propose a decentralized file storage protocol in blockchain, named as FileInsurer, to achieve both scalability and reliability. While ensuring scalability by distributed storage, FileInsurer guarantees reliability by enhancing robustness and fully compensating for the file loss. Specifically, under mild conditions, we prove that no more than 0.1\% value of all files should be compensated even if half of the storage collapses. Therefore, only a relatively small deposit needs to be pledged by storage providers to cover the potential file loss. Because of lower burdens of deposit, storage providers have more incentives to participate in the storage network. FileInsurer can run in the top layer of the InterPlanetary File System (IPFS), and thus it can be directly applied in Web 3.0, Non-Fungible Tokens, and Metaverse.

**Bio:** Hongyin Chen received the B.S. degree at School of EECS, Peking University in 2020. He is currently pursuing the doctor’s degree at Center on Frontiers of Computing Studies, Peking University. His current research interests include Blockchain and Mechanism Design.

2pm-2:25pm Stefanos Leonardos, King's College London

**EIP-1559: Chaos and Efficiency in Ethereum's Transaction Fee Market**

**Abstract:** Ethereum Improvement Proposal (EIP) 1559 is a recently implemented upgrade that transformed Ethereum's transaction fee market. EIP-1559 uses an algorithmic update rule with a constant learning rate to estimate and broadcast a base fee that users need to pay to have their transactions included in the blockchain. The base fee reflects prevailing network conditions and aims to efficiently stabilize block occupancies at a target block size.

In this talk, we will try to understand the dynamics of the resulting transaction fee market using a diverse toolbox. We will stress test the system and study its behavior under a wide range of adversarial conditions that can emerge in practice. We will then compare our theoretical findings with empirical data and proceed to analyze alternative update rules that overcome undesirable properties of the current model. In the most important and surprising takeaway of our talk, we will show that these systems can be provable efficient despite being formally chaotic.

**Bio:** Stefanos Leonardos recently joined King's College London as a Lecturer in Machine Learning at the Department of Informatics. Before coming to London, Stefanos spent 4 exciting years as a Research Fellow at Singapore University of Technology and Design working in game theory, game dynamics, multi-agent systems and their applications in artificial intelligence, machine learning and blockchain economies. Stefanos holds a PhD and a MSc in Game Theory and Operations Research from University of Athens and a Diploma in Mathematics from Technical University Darmstadt.

2:30pm-2:55pm Vassilis Zikas, Purdue University

**A Rational Protocol Treatment of 51% Attacks**

**Abstract:** Game-theoretic analyses of cryptocurrencies and---more generally---blockchain-based decentralized ledgers offer insight on their economic robustness and behavior when even their underpinning cryptographic assumptions fail. In this work we utilize the recently proposed blockchain adaptation of the rational protocol design (RPD) framework [EUROCRYPT'18] to analyze 51% double-spending attacks against Nakamoto-style proof-of-work based cryptocurrencies. We first observe a property of the originally proposed utility class that yields an unnatural conclusion against such attacks, and show how to devise a utility that avoids this pitfall and makes predictions that match the observable behavior---i.e., that renders attacking a dominant strategy in settings where an attack was indeed observed in reality. We then propose a generic remedy to the underlying protocol parameters that provably deter adversaries controlling a majority of the system's resources from attacks on blockchain consistency, including the 51% double-spending attack. This can be used as guidance to patch systems that have suffered such attacks, e.g., Ethereum Classic and Bitcoin Cash, and serves as a demonstration of the power of game-theoretic analyses.

This is joint work with Christian Badertscher and Yun Lu.

**Bio:** Vassilis Zikas is an Associate Professor at the Computer Science Department at Purdue University, and director of the Purdue Blockchain Lab. Prior to his current position, he was an Associate Professor (Sr. Lecturer) in Security and Privacy and the Vice Director of the Blockchain Technology Lab at the University of Edinburgh; a Research Fellow and Area Leader of multi-party computation for IOHK---a leading research-and-development company in the area of blockchain technologies and distributed ledger; an Assistant Professor at Rensselaer Polytechnic Institute (RPI), Troy, NY; a Fellow of the Simons Institute for the Theory of Computing at UC Berkeley; a Senior Researcher at ETH Zurich, and a postdoctoral researcher at UCLA and at the University of Maryland.