Multiparty Computing, Distributed Ledgers and Financial Services Theory and Practice

Department: Fudan International Summer Session 2024

Course Code	ECON130285		
Course Title	Overseas Lecturers' Short Courses 海外学者专题 (Note: Topic for 2024: Multiparty Computing, Distributed Ledgers and Financial Services Theory and Practice)		
Credit	2	**Credit Hours**	36+3 tutorial hours (one credit hour is 45 minutes)
Course Nature	□Specific General Education Courses □Core Courses ☑General Education Elective Courses □Basic Courses in General Discipline □Professional Compulsory Courses □Professional Elective Courses □Others		
Course Objectives	Acquire basic knowledge about how multiparty computation works, how to design infrastructure with MPC in mind and the future of financial services.		
Course Description	Multiparty computation is the process by which mutually distrustful agents come together to supply computing machinery to achieve a common goal. The classic example of MPC is the millionaires problem. Distributed ledger technology, is a relative common approach to building secure distributed infrastructure for various activities such as cryptocurrencies and smart contracts. There are a number of different approaches to implementing MPC solutions and each has pros and cons relative to the problem being addressed. This module looks at the role of the technology. The conceptual ideas about how it works and then provides some examples of different approaches within the realm of financial services. One of the core technologies we will talk about are zero knowledge proofs, why they are useful and how they can be used to increase the speed an efficiency of various MPC and DLT implementations. The module provides students with an underpinning of the core theories. An overview of some of the main results relating to how each of the technologies is implemented. Using case studies and existing research approaches we will explore the utility of these approaches and look at near future applications.		

Course Requirements: (Pre-reqs)

Prerequisites: None specifically, although the course contains some concepts from game theory and computer science as well as finance. The module does not require any prior knowledge of programming, finance or computer science, the objective is to build knowledge and the module is fully self-contained.

Teaching Methods:

Lectures and class discussions (this is not a programming module).

Instructor's Academic Background:

Professor Julian Williams, Chair in Finance, Professor of Finance and Head of Department Durham University

PhD in Finance

MSc in Finance

BSc in Chemistry

https://www.durham.ac.uk/business/our-people/julian-williams/

Has 40+ publications in finance and computer science. Holds awarded and licensed patents on MPC and blockchain technologies.

Course Schedule

- Where are we now with financial services.
- Basics of Blockchains
- Basics of Secure MPC
- Contracts and securities
- DAOs and virtual firms
- Building markets
- The Futures MEX protocol
- AI and SMPC
- Where will the future be?

The design of class discussion or exercise, practice, experience and so on:

Interactive lectures and discussion groups.

Flipped classroom discussion and feedback sessions

'Future gazing'.

Grading & Evaluation：

Final group presentation and oral feedback.

Final grade will be P/NP.

Teaching Materials & References (Including Author, Title, Publisher and Publishing time):

No book, but lots of interesting papers to read on the topics.

Lectures will be taken from the following research by the presenter and his co-authors and collaborators:

- Ngo, C. N., Massacci, F., Kerschbaum, F., & Williams, J. (2021). Practical Witness-Key-Agreement for Blockchain-based Dark Pools Financial Trading. In N. Borisov, & C. Diaz (Eds.), Financial Cryptography and Data Security 25th International Conference, FC 2021, Virtual Event, March 1–5, 2021, Revised Selected Papers, Part II (579-598). Springer Verlag. https://doi.org/10.1007/978-3-662-64331-0_30
- Massacci, F., Ngo, C., Venturi, D., & Williams, J. (in press). Non-Monotonic Security Protocols and Failures in Financial Intermediation.
- Massacci, F., Ngo, C., Nie, J., Venturi, D., & Williams, J. (2018). FuturesMEX: Secure Distributed Futures Market Exchange. In 2018 IEEE symposium on security and privacy SP 2018 (335-353). https://doi.org/10.1109/sp.2018.00028
- Massacci, F., Ngo, C., Nie, J., Venturi, D., & Williams, J. (2017). The seconomics (security-economics) vulnerabilities of Decentralized Autonomous Organizations. In F. Stajano, J. Anderson, B. Christianson, & V. Matyáš (Eds.), Security protocols XXV : 25th international workshop, Cambridge, UK, March 20-22, 2017 : revised selected papers (171-179). https://doi.org/10.1007/978-3-319-71075-4_19
- Elliott, Karen, Fabio Massacci, Chan-Nam Ngo, and Julian M. Williams. "Unruly Innovation: Distributed Ledgers, Blockchains and the Protection of Transactional Rents." *Blockchains and the Protection of Transactional Rents (December 22, 2016)*(2016).
- Method and apparatus for distributed, privacy-preserving and integrity-preserving exchange, inventory and order book
- https://www.taurushq.com/blog/mpc-smartcontract/
- Baum, Carsten, Bernardo David, and Tore Kasper Frederiksen. "P2DEX: privacy-preserving decentralized cryptocurrency exchange." In *International Conference on Applied Cryptography and Network Security*, pp. 163-194. Cham: Springer International Publishing, 2021.
- Cartlidge, John, Nigel P. Smart, and Younes Talibi Alaoui. "MPC joins the dark side." In *Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security*, pp. 148-159. 2019.
- Constantinides, Theodoros, and John Cartlidge. "Block auction: A general blockchain protocol for privacy-preserving and verifiable periodic double auctions." In *2021 IEEE International Conference on Blockchain (Blockchain)*, pp. 513-520. IEEE, 2021.
- Mazloom, Sahar, Benjamin Diamond, Antigoni Polychroniadou, and Tucker Balch. "An Efficient

Data-Independent Priority Queue and its Application to Dark Pools." *Proceedings on Privacy Enhancing Technologies* (2023).