Graduate School Event

Thesis Defense: On Secure Chain Selection Rules from Physical Resources in a Permissionless Setting

Mirza Baig (Pietrzak Group)
Pietrzak Group

Host: Julia Reisenbauer

Blockchains enable distributed consensus in permissionless settings, where participants are unknown, dynamically changing, and do not trust each other. While Bitcoin, based on Proof-of-Work (PoW), was the first protocol in this model, significant research has focused on permissionless protocols using alternative physical resources, specifically Proof-of-Space (PoSpace) and Verifiable Delay Functions (VDFs). This thesis investigates the theoretical limits and design space of longest-chain protocols in the fully permissionless and dynamically available settings using these three resources. First, we address the feasibility of blockchains relying solely on storage as a resource. We prove a fundamental impossibility result: there exists no secure longest-chain protocol based exclusively on Proof-of-Space in the fully permissionless or dynamically available settings. Further, we quantify the adversarial capabilities required to execute a double-spend attack. Our result formally justifies the necessity of coupling PoSpace with time-dependent primitives (such as VDFs) or to move to less permissive settings (quasi-permissionless or permissioned) to ensure security.Second, we generalize Nakamoto-like heaviest chain consensus to protocols utilizing combinations of multiple physical resources. We analyze chain selection rules governed by a weight function Γ(S, V,W), which assigns weight to blocks based on recorded Space (S), VDF speed (V), and Work (W). We provide a complete classification of secure weight functions, proving that a weight function is secure against private double-spend attacks if and only if it is homogeneous in the timed resources (V,W) and sub-homogeneous in S. This framework unifies existing protocols like Bitcoin and Chia under a single theoretical model and provides a powerful tool for designing new longest-chain blockchains from a mix of physical resources.

Tuesday, March 17, 2026 10:00am - 11:00am
Moonstone Bldg / Ground floor / Seminar Room C (I24.EG.030c) and Zoom

This invitation is valid as a ticket for the ISTA Shuttle from and to Heiligenstadt Station. Please find a schedule of the ISTA Shuttle on our webpage: https://ista.ac.at/en/campus/how-to-get-here/ The ISTA Shuttle bus is marked ISTA Shuttle (#142) and has the Institute Logo printed on the side.