Institute of Theoretical Informatics (ITI)
Application-oriented Formal Verification
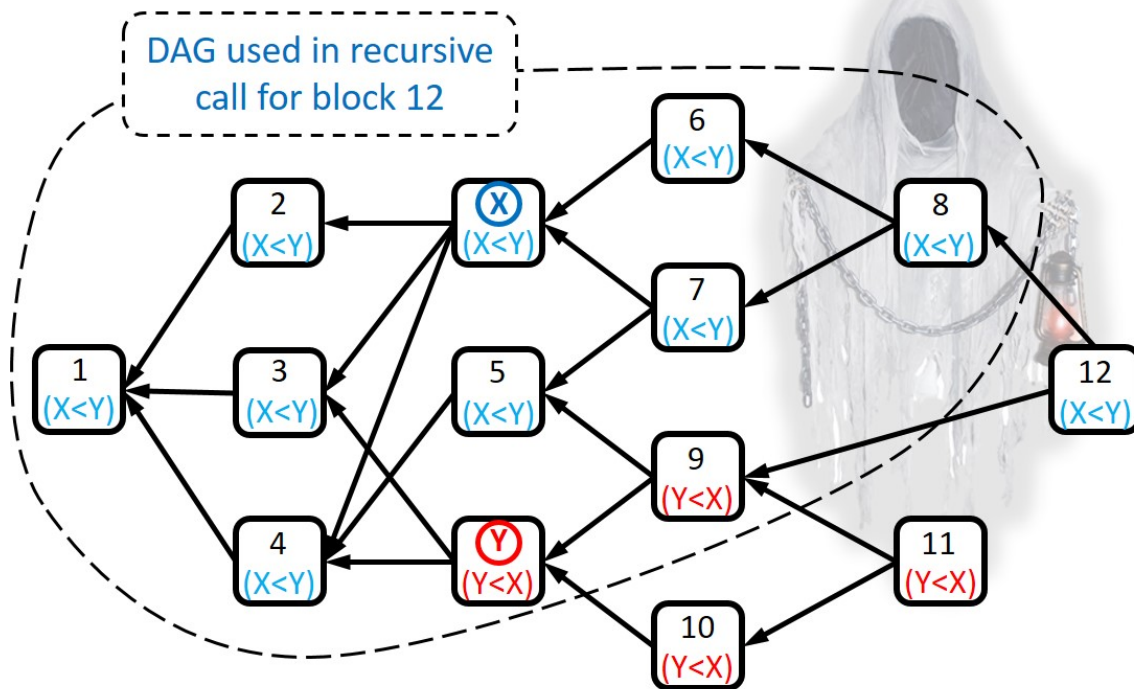Prof. Dr. Bernhard Beckert
https://formal.iti.kit.edu

Relational Social-Choice Properties for Secure and Scalable Consensus in the Blockchain

Masterarbeit – Forschungspraktikum

Background

- Blockchains allow secure transactions between non-trusting parties

- Finding consensus in such situations is hard and scales badly

- More recent protocols based on DAGs allow **off-chain-transactions**

- Critical: How to deal with parallel computations?

Objective

- Formalize consensus procedures based on voting mechanism in DAGs

- Goal: Formal model of provenly secure off-chain consensus procedure

Contact

Michael Kirsten   kirsten@kit.edu, Room 228 (Bldg. 50.34)