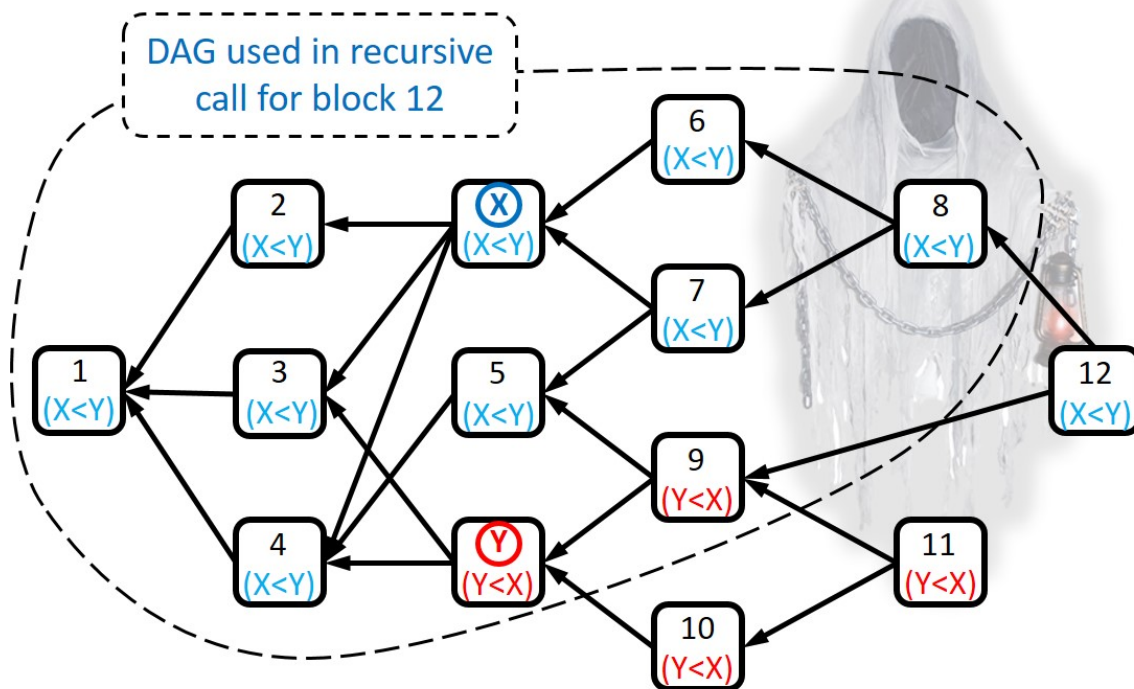


Relational Social-Choice Properties for Secure and Scalable Consensus in the Blockchain

Praxis der Forschung

Michael Kirsten



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?

Research Task

- Formalize consensus procedures using **off-chain-transactions**
- Goal: Formal model of provenly secure off-chain consensus procedure