Enabling Privacy in IOU Settlement Networks

Pedro Moreno-Sanchez¹, Tim Ruffing², Aniket Kate¹
¹ Purdue University, ²Saarland University

Ripple
- I Owe You (IOU) settlement network
- Inter-currency transactions
- Geographically-independent low fees and fast transactions
- Verifiability is enforced through a publicly available log

Strong Privacy Solution: PrivPay [2]

Compatible Solution: Mixing Several Transactions

Privacy Issues: Inter-log Linkability

Step 1: Key Agreement

Step 2: Announcement

Step 3: Recover A', B', C' from power sums [3]

Evaluation

Accountable Anonymous Broadcast [3]

Constant number of rounds independently of the number of participants in the mixing

Security and Privacy Properties

- Nobody can steal coins (Verifiability)
- Disruptive participants can be accurately identified (Accountability)
- Sender and receiver address cannot be linked together (Unlinkability)

References