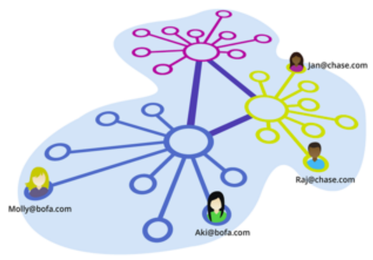
CERIAS
The Center for Education and Research in Information Assurance and Security

Enabling Privacy in IOU Settlement Networks

Pedro Moreno-Sanchez[1], Tim Ruffing[2], Aniket Kate[1]
[1] Purdue University, [2] Saarland 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

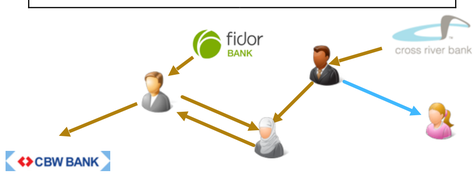


fidor BANK · cross river bank · CBW BANK · CommonwealthBank · Microsoft · earthport

Privacy Issues: Inter-log Linkability

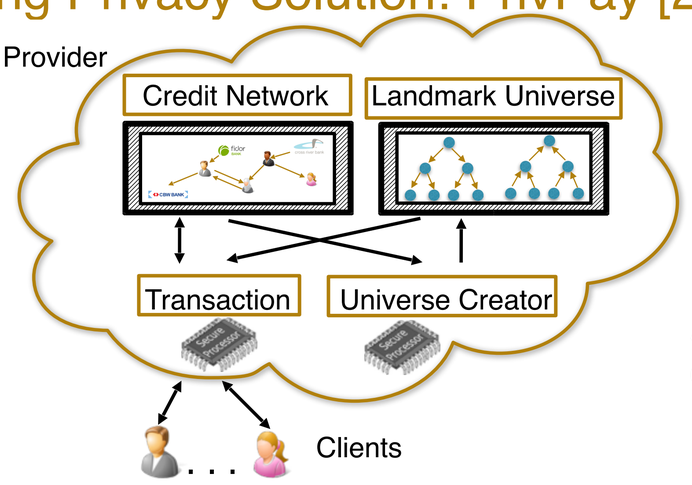
Input	Output
Alice: 6 BTC	Bob: 6 BTC
Alice	

Sender	Bob
Receiver	Alice
Value	1 BTC IOU
Path	Bob —> Alice
Bob	



This is only the tip of the iceberg! More privacy issues in Ripple [1]

Strong Privacy Solution: PrivPay [2]

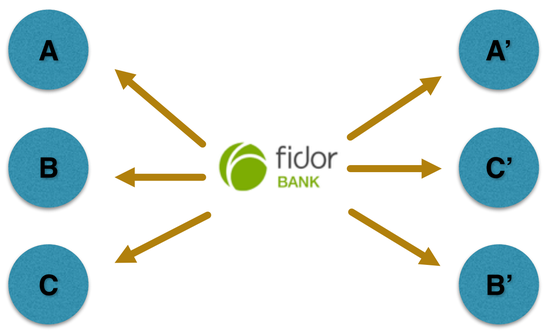


- Sender privacy
- Receiver privacy
- Value privacy

Architecture is not fully compatible with current Ripple network

Compatible Solution: Mixing Several Transactions

Idea: Perform several transactions simultaneously enables privacy-preserving transactions

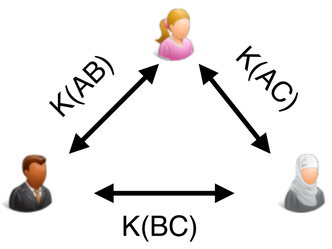


Ripple only allows single sender/receiver per transaction

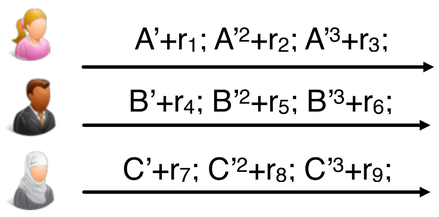
Who are the receivers?
Who pays first?

Accountable Anonymous Broadcast [3]

Step 1: Key Agreement



Step 2: Announcement



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

$A' + B' + C' = s_1$ | $a_2 = -s_1$

$A'^2 + B'^2 + C'^2 = s_2$ | $a_2 * s_1 + 2 * a_1 = -s_2$

$A'^3 + B'^3 + C'^3 = s_3$ | $a_2 * s_2 + a_1 * s_1 + 3\, a_0 = -s_3$

$f(x) = x^3 + a_2 x^2 + a_1 x + a_0$

With roots A', B', C'

PathShuffle: Private transactions in Ripple

A/B/C

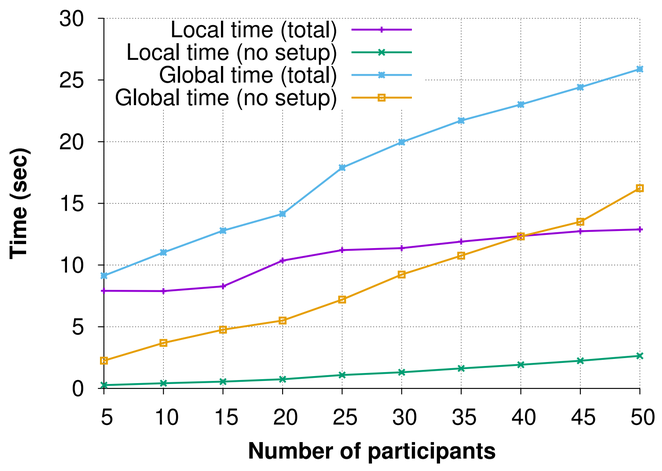
Shared Wallet:
- Alice, Bob and Carol must agree to perform a transaction

100% Compatible with Ripple. Tested in real network!

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**)

Evaluation



Local: Users in a LAN
Global: Users in Internet
Setup: Connect to each other

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

References

[1] Pedro Moreno-Sanchez, Muhammad Bilal-Zafar, Aniket Kate. *I Owe You Ripples: Linking Wallets and Deanonymizing Payments in the Ripple Network.* Under submission at PETS 2016.
[2] Pedro Moreno-Sanchez, Aniket Kate, Matteo Maffei, Kim Pecina. *Privacy Preserving Payments in Credit Networks.* Published at NDSS'15.
[3] Pedro Moreno-Sanchez,Tim Ruffing, Aniket Kate. *Enabling Anonymous Payments with Round Efficient Protocol for Traffic Analysis Resistant Anonymous Communication.* Work in progress.
[4] Tim Ruffing, Pedro Moreno-Sanchez, Aniket Kate. *CoinShuffle: a Practical Decentralized Coin Mixing for Bitcoin.* Published at ESORICS'14.

CERIAS · PURDUE UNIVERSITY