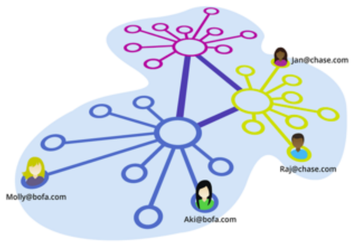
Linking Wallets and Deanonymizing Payments in the Ripple Network

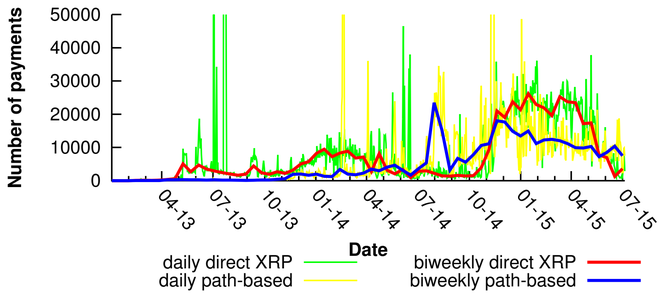
Pedro Moreno-Sanchez[1], Muhammad Bilal Zafar[2], Aniket Kate[1]

[1]Purdue University; [2]MPI-SWS

1. The Ripple Network

The Ripple network is being adopted by banks, cross-border payment services, Bitcoin merchants and many others as their backbone network.





- More than 169,000 users
- $2M daily payments volume
- $470M network value

Verifiability is enforced through a public transaction ledger.

Huge Privacy Issues!

2. Linking Wallets: Interaction with gateways H1

Deposit operation:
- A user sends BTC to a gateway
- The gateway issues BTC IOU to the user

Withdrawal operation:
- A user sends BTC IOU to a gateway
- The gateway sends BTC to the user

Bitcoin Transaction	
Input	**Output**
$Alice_1$: 30 BTC	$Gateway_1$: 20 BTC
	$Alice_2$: 10 BTC

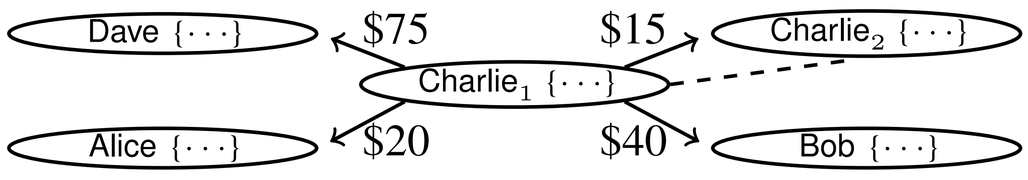
Ripple Transaction	
Field	**Value**
Sender	$Gateway_2$
Receiver	$Alice_3$
Amount	20 BTC IOU

Ripple Transaction	
Field	**Value**
Sender	$Alice_4$
Receiver	$Gateway_3$
Amount	10 BTC IOU

Bitcoin Transaction	
Input	**Output**
$Gateway_4$: 15 BTC	$Alice_5$: 10 BTC
	$Gateway_5$: 5 BTC

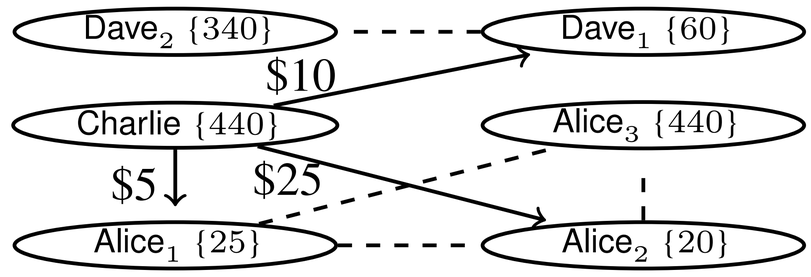
3. Linking Wallets: Hot and Cold Wallets H2

Using the connectivity in the Ripple network, we have defined two novel heuristics to link Ripple wallets controlled by the same user. [1]



Ripple Ledger					
Sender	**Receiver**	**Amount**	**Sender**	**Receiver**	**Amount**
$Charlie_1$	$Charlie_2$	$80	$Charlie_2$	Bob	$50
$Charlie_2$	Alice	$10	$Charlie_2$	Dave	$75
$Charlie_1$	$Charlie_2$	$70	Bob	Alice	$10

H3



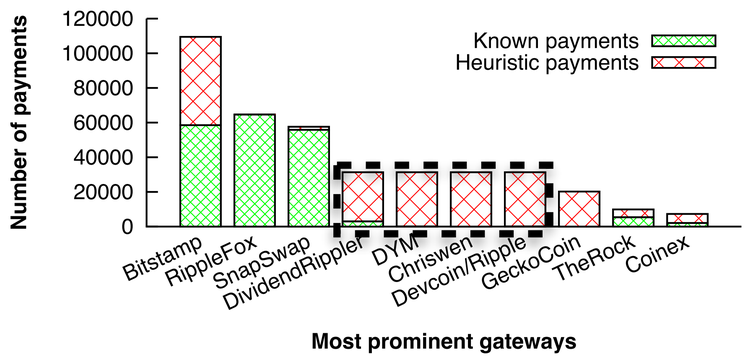
Ripple Ledger					
Sender	**Receiver**	**Amount**	**Sender**	**Receiver**	**Amount**
$Alice_1$	$Alice_3$	60 XRP	$Alice_2$	$Alice_3$	200 XRP
$Alice_2$	$Alice_3$	130 XRP	$Dave_1$	$Dave_2$	240 XRP
$Dave_1$	$Dave_2$	100 XRP	$Alice_1$	$Alice_3$	50 XRP

4. Deanonymizing Ripple Users

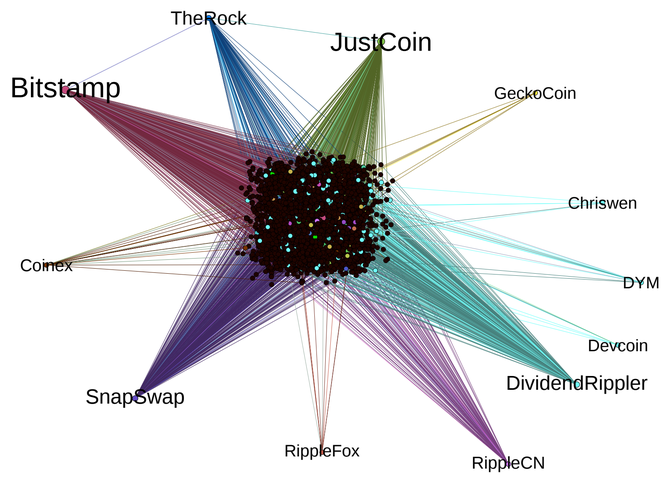
Grouping heuristics:
- 14% total Ripple payments
- More than $360K billion payments volume

Heuristic	Ripple		Bitcoin	Altcoins
	Wallets	Payments	Wallets	Wallets
H1	425	64,808	3,113	1,130
H2	323	339,442	-	-
H3	2,483	690,878	-	-
Grouped	3,166	946,078	3,113	1,130

Reconstructing gateways business:
- Deanonymized almost 50% payments previously unknown for Bitstamp
- DividendRippler, Dym, Chriswen and Devcoin gateways have the same owner



Deanonymizing our clustered graph:
- 78% total payments in the cluster
- More than $177 million payments volume



5. Discussion and Future Work

- Detected 68% of the wallets published by the 109 studied gateways
- Results confirmed by Ripple Labs and 2 contacted gateways
- Our work shows a privacy problem in the design of payment networks
- Privacy-preserving payments are necessary [2, 3, 4]
- Further deanonymization possible using a Ripple server:
  - Linking wallets in payments sent from the same IP address

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.

[2] Pedro Moreno-Sanchez, Aniket Kate, Matteo Maffei, Kim Pecina. *Privacy Preserving Payments in Credit Networks.* NDSS 2015.

[3] Tim Ruffing, Pedro Moreno-Sanchez, Aniket Kate. *CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin.* ESORICS 2014.

[4] Aniket Kate, Matteo Maffei, Giulio Malavolta, Pedro Moreno-Sanchez. *ZeroPay: A Decentralized Architecture for Enforcing Privacy in Credit Networks.* Under submission.