Listening to Whispers of Ripple: Linking Wallets and Deanonymizing Transactions in the Ripple Network

Introduction: The paper discuss an overview of Ripple network, analyze visible logs and characterize privacy issue. The paper discuss heuristic to link ripple wallets using general interaction with online currency exchanges. The paper discuss heuristic verification, novelty of heuristic linking across cryptocurrencies, privacy impact because of deanonymizing Ripple and Bitcoin wallets. Ripple has features such as it is third largest cryptocurrency after Bitcoin and Ethereum, it is fast and efficient for same and cross-currency payments, It has IOU(I owe you) transaction network. Until paper was written, it has 170k user wallet, network value of $790 million and daily transaction volume of over $1 million.

Ripple IOU Network: The Ripple network is a weighted, directed graph G = (V,E). The set V of vertices represents the wallets in the network. The set E of weighted edges represents the IOU credit links between wallets

Ripple Transactions Ripple allows two kinds of transactions. The direct XRP payments allow the exchange of XRP between two wallets. The edge weights in the Ripple network represent IOUs for three different types of currencies, namely, fiat currencies (e.g., USD), cryptocurrencies (e.g., bitcoins) and user defined currencies. Path-based settlement transactions make use of the credit lines available in the Ripple network

Linking of Ripple wallets to Bitcoin Wallets Users pay certain amount of BTC to gateway and gateway issues corresponding IOU. The use of the publicly available information regarding deposit and withdrawal transactions at the gateways to link together Ripple and Bitcoin wallets that belong to the same user. Wallets published by DividendRippler were identified with their links. It also has privacy impact to all the wallets linked to a business that can be deanonymized.

Linking of Ripple wallets to Cold Wallets Ripple defines the hot-cold wallet security mechanism to issue IOUs of any currency. The cold wallet is publicly linked to a certain user.However, actual issuing of the IOUs in a credit link extended to the cold wallet is performed by the hot wallet. The hot wallet is therefore considered to be online as it is used for daily settlement transactions. Thus, the cold wallet is considered offline.

Deanonymizing Ripple user The group of heuristics results, thereby increasing the linking among Ripple and cryptocurrencies wallets: if a wallet in a cluster gets deanonymized, the complete cluster can be deanonymized, independently of the system where the deanonymized wallet belongs. The concrete instances of deanonymization of such clusters identifying transactions associated to Ripple gateways were made.

Conclusions: The heuristics allows to cluster wallets belonging to the same user,not only from the Ripple network but also from several (publicly verifiable) blockchain-based cryptocurrency systems such as Bitcoin. The clustering has enabled the deanonymization of more than 78% of the clustered transactions. The analysis characterizes the privacy challenges faced by the emerging transaction networks.

Future Works: The heuristics show a privacy problem directly in the design and the use pattern of credit networks such as Ripple. The heuristics described in this work augur promising results when the Ripple network activity takes off, their effectiveness will improve when the Ripple network expands and become more structured