Do you Hear the Whispers of Ripple?

Study and Solutions for Privacy in *IOweYou* Credit Networks (Extended Abstract)

Pedro Moreno-Sanchez
Purdue University

Aniket Kate
Purdue University

I. Introduction

A distributed *IOweYou* (IOU) credit network Ripple [1] has gained prominence in the payment settlement space over the last few years. Its pseudonymous nature, ability to perform cross-currency transactions across the globe in a matter of seconds, and potential to monetize everything regardless of jurisdiction at a small consistent fee improves significantly upon drawbacks in the current banking system [8]. As a result, today several financial institutions leverage Ripple to perform their daily transactions [2], and it handles a daily transaction volume of $4M and caters to over 200 thousand user wallets.

Although originated from the same movement that started cryptocurrencies (e.g., Bitcoin), credit networks such as Ripple are conceptually different. Despite its unquestionable utility, Bitcoin (as any other currency) is inherently limited to transactions where both transacting users agree on a common (crypto-) currency. Credit networks, instead, smoothly enable cross-currency transactions in any user specified currency (including Bitcoin) as long as two users share a credit path with enough IOU credit on it.

II. Deanonymizing Ripple Transactions

Ripple is at its core, a replicated, *public* database (called the *Ripple ledger*) that tracks wallets and credit links extended between wallets along with their IOU balances. The Ripple network opted for demonstrating consistency of transactions through transparency: anyone can inspect the Ripple ledger and extract a complete historical record of the activity on Ripple. Ripple identities are pseudonyms; thus, while not explicitly tied to real-world individuals or organizations, all transactions are completely transparent up to pseudonyms.

In this direction, the Ripple community has started to consider the privacy issues in Ripple [4]. Banks do not wish to have all their transactions published on an open network [6]. There are proposals in the Ripple community to provide privacy [3], [5]; however, these ideas are immature at the best. The current situation of the Ripple network regarding privacy leads to the question: does the public nature of the Ripple ledger lead to any serious privacy issue? Can we measure this?

A. Our contribution

We have performed the first thorough study of the Ripple network aiming at improving the understanding of the traceability of Ripple flows and using it to explore the privacy breaches inherent to the public nature of the Ripple ledger. [12] Our goal is to cluster different Ripple wallets belonging to the same user. This allows then to recognize previously unlinked transactions performed by the known Ripple users and enables further deanonymization of businesses performed over Ripple.

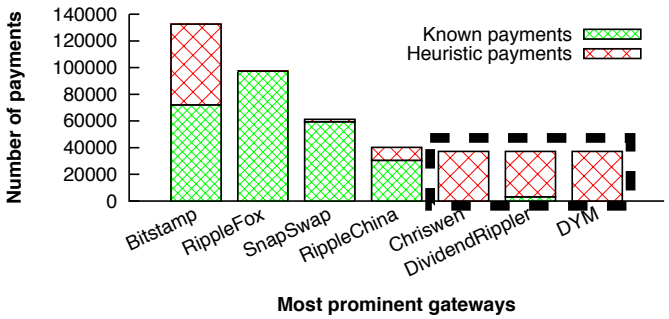

Fig. 1: Comparison of the number of transactions associated to publicly known major wallets from gateways (i.e., Known payments) and transactions performed with wallets clustered by our heuristics to those gateways (i.e., Heuristic payments). Dashed line groups gateways sharing an owner.

In this talk, we will first describe one of our novel heuristics to link wallets based on the patterns observed in the Ripple network as the result of two wallet owners settling a Bitcoin exchange over their Ripple credit link. This heuristic facilitates the linking of Bitcoin and Ripple wallets owned by the two involved users, therefore allowing for the first time to perform clustering of wallets across two different payment networks. In fact, it is not restricted to Bitcoin, and enables the clustering of Ripple wallets with other cryptocurrencies wallets (i.e., altcoins), thereby enlarging the set of clustered wallets.

Second, we will discuss the analysis of our findings. In particular, to analyze the efficacy of our heuristics, we crawl the Ripple network (as of December 2015) obtaining a total of *174,738 wallets*, *115,996 credit links*, and *17,645,343 transactions* using them. We deploy our heuristics over this dataset, resulting in the clustering of *959 Ripple wallets*, *3,113 Bitcoin wallets* and *1,130 Altcoin wallets*, which are involved in *934,484 transactions* in total. The set of clustered wallets has allowed us to reconstruct the complete set of transactions of the most widely deployed gateways[1], and showed that is indeed bigger than the set of transactions associated to their publicly announced Ripple wallets, as shown in Fig. 1.

Finally, we will also discuss the privacy implications of setting a Ripple validator server on the Ripple network. These servers collects transactions from the Ripple users and can significantly increase the deanonymization rate from the observed

[1] A gateway is a highly connected Ripple wallet that exchanges IOU in Ripple for the equivalent value in the outside world.

network identifiers (e.g., IP address) of the contacting users. The recent selection of commercial players such as Microsoft as a validator server [7] can lead to large scale privacy leaks undermining the privacy of the Ripple users.

III. Privacy Preserving Ripple Transactions

In the view of the current state of affairs regarding privacy in credit networks such as Ripple, there is an inherent need to enable anonymous transactions in the current Ripple network. Although a formally secure privacy protocol has already been proposed in this direction [10], it is not compatible with the currently deployed Ripple network.

A. Our Contribution

We find motivations in the proposals to improve privacy in Bitcoin and other cryptocurrencies, those based on coin mixing [9], [13]: they are typically just built on top of the existing Bitcoin system and thus can be seamlessly deployed in practice. The idea of coin mixing is that a group of users send each other bitcoins in such a manner that the relation between the owner of the coins and her account remains hidden.

Although interesting, the coin mixing concept cannot be trivially applied to credit networks. While in Bitcoin, direct payments from sender to receiver are performed, in a credit network the credit must be settled through a *credit path* with enough liquidity from sender to receiver. Therefore, in order to overcome this challenge we introduce the concept of path mixing, a novel key tool to address the critical concern of financial privacy within existing credit networks. In particular, we have designed PathShuffle, the first protocol for anonymous transactions in credit networks in a fully compatible manner with the Ripple network. In the second half of this talk, we will present the contributions of this ongoing work [11].

We will overview the two building blocks required in PathShuffle. First, the DiceMix [11] peer-to-peer mixing protocol allows a group of users to anonymously to broadcast their messages. In particular, we leverage DiceMix to anonymously broadcast a set of Ripple wallets set as the receiver wallets for the anonymous transactions created in the PathShuffle protocol.

Second, our novel PathJoin protocol allows to seamlessly perform atomic transactions in the Ripple network. PathJoin features a novel combination of the Ripple network functionality and a distributed threshold signature scheme to ensure that a group of users atomically transfer credit from a set of input wallets to a set of output wallets, thereby solving a standard fairness problem that arises in this scenario.

Finally, we will describe the details of PathShuffle, a protocol that can be seamlessly implemented in the current Ripple network and enables for the first time anonymous transactions in the current Ripple network. An example is depicted in Fig. 2. In this example, DiceMix is first used to anonymously broadcast receiver wallets $\{\mathsf{A}^*_{out}, \ldots, \mathsf{E}^*_{out}\}$. Then, PathJoin enables an atomic transaction to transfer 10 IOU from the input wallets $\{\mathsf{A}^*_{in}, \ldots, \mathsf{E}^*_{in}\}$ to the output wallets.

Our key observation in this work is that a set of credit paths that share a common Ripple wallet can be mixed such that the output wallet of a honest user cannot be linked to the specific honest user. Interestingly, in the current Ripple network, common wallets among credit paths are prevalent in the form of Ripple gateways. Moreover, PathShuffle ensures that the credit balance of a user is not reduced and thus users do not incur on credit loss while using PathShuffle. Additionally, PathShuffle is compatible with the currently deployed Ripple network as demonstrated by a proof-of-concept implementation that performs a path mixing transaction between five users in the currently deployed Ripple network.

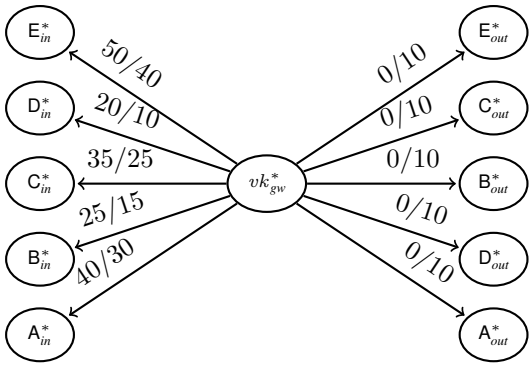

Fig. 2: An example for path mixing to mix 10 IOU among five users. Nodes denote wallets in the credit network. An arrow $a \to b$ denotes that a owes credit to b. The weight x/y on the arrow denotes the amount of credit before the mixing (x) and after the mixing (y).

This work has been done in collaboration with our colleagues Tim Ruffing and Muhammad Bilal Zafar, and we thank them for their efforts.

References

[1] Ripple Webpage. https://ripple.com/.

[2] Several Global Banks Join Ripple's Growing Network. https://ripple.com/insights/several-global-banks-join-ripples-growing-network/.

[3] Ripple privacy. Ripple Forum, Nov 2012. https://forum.ripple.com/viewtopic.php?f=1&t=4.

[4] Ripple Privacy - details on proxy payments or alternative? Ripple Forum, Nov 2014. https://forum.ripple.com/viewtopic.php?f=1&t=8304&p=57936.

[5] Using multi-signature transactions to provide privacy. Ripple Forum, Oct 2014. https://forum.ripple.com/viewtopic.php?f=2&t=8215.

[6] Implementing the Interledger Protocol in Ripple. Ripple blog, Oct 2015. https://ripple.com/insights/implementing-the-interledger-protocol/.

[7] Microsoft Explores Adding Ripple Tech to Blockchain Toolkit. CoinDesk Blog, Dec 2015. http://www.coindesk.com/microsoft-hints-future-ripple-blockchain-toolkit/.

[8] Santander: Distributed Ledger Tech Could Save Banks $20 Billion a Year. Ripple Blog, Jun 2015. https://ripple.com/blog/santander-distributed-ledger-tech-could-save-banks-20-billion-a-year/.

[9] Heilman, E., Alshenibr, L., Baldimtsi, F., Scafuro, A., and Goldberg, S. TumbleBit: An Untrusted Bitcoin-Compatible Anonymous Payment Hub, 2016. http://eprint.iacr.org/2016/575.

[10] Moreno-Sanchez, P., Kate, A., Maffei, M., and Pecina, K. Privacy Preserving Payments in Credit Networks: Enabling trust with privacy in online marketplaces. In *NDSS '15*.

[11] Moreno-Sanchez, P., Ruffing, T., and Kate, A. PathShuffle: Mixing Credit Paths for Anonymous Transactions in Ripple. http://crypsys.cs.purdue.edu/projects/internetOfValue/PathShuffle/.

[12] Moreno-Sanchez, P., Zafar, M. B., and Kate, A. Listening to Whispers of Ripple: Linking Wallets and Deanonymizing Transactions in the Ripple Network. *PETS '16 2016*, 4 (July 2016), 436–453.

[13] Ruffing, T., Moreno-Sanchez, P., and Kate, A. *CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin.* ESORICS '14.