Zero-Link Soduko: Real vs. Perceived Anonymity

Author: N/A

June 17, 2019

Abstract

Bitcoin purports to offer users censorship-resistant financial access through a permission-less peer-to-peer distributed public network. However, a payment system that is public, may be subject to censorship if observers are able to link real world or online identities with particular coins and transactions. Thus, a truly censorship-resistant financial system must guarantee a method to ensure coins remain fungible. Recently, the Zero-link protocol [1] has been proposed as a solution to this problem, by allowing users to engage in equal-output Chaumian CoinJoins of fixed denominations. Wasabi Wallet [2], an open-source desktop client, is the first widely used implementation of Zero-Link. Wasabi Wallet combines network level privacy with an in-wallet CoinJoin feature and strong coin control. We analyzed over 5,000 CoinJoins over a one year period via Wasabi, using four attack vector heuristics to reduce the anonymity sets of participants. This analysis allowed us (1) to answer the question: What is a more accurate upper-bound for anonymity achieved through the Wasabi wallet as compared to current perceived anonymity metrics? and (2) to propose a few minor protocol and implementation changes to mitigate untended anonymity reduction.

Introduction

Bitcoin is a peer-to-peer protocol that claims to allow any two individuals to engage in economic activity without censorship from governments or financial institutions [3]. However, what was once perceived as sufficient privacy (sometimes described as anonymity) is now widely considered insufficient, with a plethora of forensics and data analytic papers demonstrating linkability of coins through transaction heuristics [4] [5]. Furthermore, it has become clear that for a financial network to remain censorship free, merchants and payment providers must not be able to discriminate one coin from another, based on its history. In order to guarantee the fungible property of Bitcoin (i.e., the property of one coin being indistinguishable and thus interchangeable from the other) a handful of techniques have emerged, from off-chain payments which leverage onion-routing, to on-chain methods like centralized mixers, CoinJoin, PayJoin, Stone Wall, etc. On-chain solutions in nearly all instances leverage what is referred to as obfuscation tactics for achieving user privacy, where a user will try

to hide the history of the coin among other participants in the network, impeding passive observers from easily linking a coin received from a coin sent. Since obfuscation relies on hiding in a crowd of participants, a heuristic for evaluating the degree of privacy achieved is calculated by determining the size of the crowd in which the user is hiding. However, if participants in an obfuscation system are de-anonymized through on-chain behaviour, whether on purpose (in the form of a malicious Sybil attack) or by accident (in the form of poor understanding of protocol limitations) this has a negative impact on the privacy of other participants leveraging the crowd. This paper examines a set of over 5000 transactions constructed by an open-source desktop client implementing Chaumian CoinJoins, over one year from August 2018 to August 2019. We begin by formalizing the concept of the anonymity set, and proceed by introducing four attack vectors that use exclusively on-chain evidence to de-anonymize participants in Wasabi CoinJoins. We proceed to analyze the effectiveness of each of these attacks insofar as they reduce the anonymity set of other participants. We try to draw conclusions about the size of the gap between real and perceived anonymity sets of Wasabi CoinJoins. We then propose a few minor protocol and implementation changes that could mitigate unintended anonymity set reduction. Finally, we will discuss the trade-offs in these alterations and consider their potential implications on anonymity.

This paper is a work-in-progress.

References

[1] Ficsor, Adam. *ZeroLink: The Bitcoin Fungibility Framework* https://github.com/nopara73/ZeroLink

[2] ZKSnacks Ltd. *Wasabi Wallet* https://wasabiwallet.io/

[3] Nakamoto, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System* https://bitcoin.org/bitcoin.pdf

[4] Androulaki E., Karame G.O., Roeschlin M., Scherer T., Capkun S. (2013) *Evaluating User Privacy in Bitcoin* Sadeghi AR. (eds) Financial Cryptography and Data Security. FC 2013. Lecture Notes in Computer Science, vol 7859. Springer, Berlin, Heidelberg

[5] Sean Foley, Jonathan R Karlsen, Tālis J Putniņš (2019) *Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed through Cryptocurrencies?* The Review of Financial Studies, Volume 32, Issue 5, May 2019, Pages 1798–1853, https://doi.org/10.1093/rfs/hhz015