How Tor-based Cryptocurrencies Solve The Anonymity Problems of Bitcoin

The Razor Cryptocurrency Development Team
http://razorco.in

Abstract. The past few months have seen a plethora of coins which claim to solve the problems of Bitcoin's pseudononymous transactions. Unfortunately, these efforts have failed miserably due to a lack of understanding of what the anonymity issues of Bitcoin truly are, as none of these alleged anonymous systems have addressed the fundamental problem of detaching the user from the transaction itself. Tor-based cryptocurrencies, such as Razor, solve this problem by creating an entire ecosystem which exists solely within a time-tested, secure, distributed, and anonymous network.

Keywords: Bitcoin, anonymity, Tor, Razor

I. Introduction

Satoshi Nakamoto, the author of Bitcoin, asserted that the network was "pseudononymous"[1], inferring that the responsibility of anonymity was placed upon the user. Anonymity is not achieved through obscuring the transactions on the blockchain, but divorcing any given transaction from a distinct individual. While certain attempts have been made at "group addressing" and "coin mixing," these methods only obscure the historical record of financial transactions between addresses and not the individual that owns the address. The primary flaw in this is that the IP address of the client of every single transaction is exposed when the transaction is sent to connected nodes.

II. Background

The transactions of any given address are irrelevant as far as individual identification purposes, so long as the veil of anonymity is not broken via a third party, such as a shipping address or an IP address from the originating transaction. Pennsylvania State University published a paper for peer review in 2013 which was able to match transactions to a specific originating IP at an alarming success rate of up to 99% accuracy [2]. Given all that is now in the public consciousness regarding government monitoring of internet traffic, it is naive to think that cryptocurrency traffic - even for such "anonymous" networks as DarkCoin - is not being monitored.

Tor is self-described on its homepage as a "free software and an open network that helps you defend against traffic analysis, a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security." [3] The decentralized nature of the Tor network lends well to the decentralized nature of cryptocurrencies and the marriage between them is quite easily achieved from a technical standpoint.

III. True Anonymity

While Bitcoin and other cryptocurrencies certainly provide for Tor-based networks, they are not wholly implemented in such a manner. As such there is logical reason to assume that any given transaction, no matter how it originated, cannot be traced back to the user via the network employed. Cryptocurrencies that adopt a Tor-based network permanently divorce all network traffic from being traced back to the originating IP, providing a level of security and anonymity that cannot be paralleled by any like cryptocurrency network that is not entirely Tor-based.

As every pool, wallet, exchange, and use case must eventually force transactions through the blockchain via the Tor network, every single point of heuristic analysis employed by the researchers at Pennsylvania State University fails completely. The research from PSU specifically states "transactions sent through proxy services such as Tor, I2P, or the tool provided in [given reference] would still be assigned to incorrect owners since we cannot establish direct connections to their true creators" [4]. In this manner cryptocurrencies such as Razor succeed where all other attempts at anonymity have failed due to a complete misunderstanding of what provides actual anonymity in any given cryptocurrency transaction.

References

1. Nakamoto, S. (2008) "Bitcoin: A peer-to-peer electronic cash system," Consulted,
1, p.2012.
2. Philip Koshy, P., Koshy D.,McDaniel P. (2013) "An Analysis of Anonymity in Bitcoin Using P2P Network Traffic" pg. 15 http://fc14.ifca.ai/papers/fc14_submission_71.pdf
3. The Tor Project (2014) https://www.torproject.org/
4. Koshy, pg. 15