Privacy in Bitcoin Literature Survey

There are many studies evaluating the privacy guarantees of Bitcoins. Most studies start from a known starting point; users announce ownership of a public-keys or addresses. Users may identify public-keys associated with them for many reasons. Services, such as Bitcoin exchanges, have public-key associated with their real-world identity in order to facilitate business. Other users may identify public-keys related to them in order ask for donations. From these known identities, Reid and Harrigan use flow analysis of Bitcoins to show that transactions to and from these identities are not lost among all the other transactions. They studied how stolen Bitcoins are moved as proof of concept to show how law enforcement may follow stolen Bitcoins until it arrives at one of the few exchanges or washers that would allow the thief to de-associate the stolen Bitcoins with his identity. Unfortunately, the stolen Bitcoins were never used with any public store or service. Other studies attempt to cluster public-keys and study Bitcoin flows in order to identify generic users. The two main heuristics to cluster public-keys with users are multi-input transactions and shadow or change accounts. Multi-input transactions occur when the user uses multiple public-keys in one transaction. Bitcoins does not currently support multiple users in one transaction therefore all the public-keys used for one transaction must belong to one user. Shadow accounts are new accounts created for the user to collect change from a transaction. In 2011, users rarely issue transactions to two different users. Flow analysis compromises the privacy of a considerable fraction of users (roughtly 35% in paper by Androulaki, Karame, et al.). Flow analysis is more complete when targeting multiple vendors in the same geographical area such as a university campus. Zerocoin creates a decentralized pool of coins in an attempt to foil flow analysis. If the coin a user spends is not the same coin that the user puts into the pool, then flow analysis will not work. Zerocoin uses a system of commitments and zero-knowledge proofs in order to desynchronize coins that are deposited and coins that are removed. This system does not protect the user against attacks of anonymity that target other identifiable information such as IP address.

IP addresses can be leaked from the TCP/IP layer. Due to the need to propagate block chain information and transaction waiting to be verified, many announcements are made over the Bitcoins peer-to-peer network. By opening a connection to every node on the public cloud at once and monitor messages, over time, the first node that announces a transaction is the node that produced it. This gives you the IP address originating that transaction. As Dan Kaminsky notes, although users can hide their outbound identity through proxy services like Tor, many user's still listen on TCP/8333 and will allow inbound connections. Inbound connections will bypass the Tor network and reveal the user's IP address when making transactions.

References

1. Fergal Reid and Martin Harrigan. 2013. An Analysis of Anonymity in the Bitcoin System. *Security and Privacy in Social Networks*. Springer, New York, NY, USA, 197-223.
2. Elli Androulaki, Ghassan O. Karame, Marc Roeschlin, Tobias Scherer, and Srdjan Capkun. 2013. Evaluating User Privacy in Bitcoin. *Financial Cryptography and Data Security*. Springer, Berlin, Heidelberg, 34-51.
3. Sarah Meiklejohn, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoy, Geoffrey M. Voelker, and Stefan Savage. 2013. A fistful of bitcoins: characterizing payments among men with no names. In Proceedings of the 2013 conference on Internet measurement conference(IMC '13). ACM, New York, NY, USA, 127-140.
4. Dorit Ron and Adi Shamir. 2013. Quantitative Analysis of the Full Bitcoin Transaction Graph. *Financial Cryptography and Data Security*. Springer, Berlin, Heidelberg, 6-24.
5. Ian Miers, Christina Garman, Matthew Green, and Aviel D. Rubin. 2013. Zerocoin: Anonymous Distributed E-Cash from Bitcoin. In Proceedings of the 2013 IEEE Symposium on Security and Privacy (SP '13). IEEE Computer Society, Washington, DC, USA, 397-411.
6. Dan Kaminsky. 2011. Black Ops of TCP/IP 2011. *Black Hat USA 2011.* <http://www.slideshare.net/dakami/black-ops-of-tcpip-2011-black-hat-usa-2011>