Dandelion: Redesigning the Bitcoin Network for Anonymity

Shaileshh Bojja Venkatakrishnan
University of Illinois at Urbana-Champaign
bjjvnkt2@illinois.edu

Giulia Fanti
University of Illinois at Urbana-Champaign
fanti@illinois.edu

Pramod Viswanath
University of Illinois at Urbana-Champaign
pramodv@illinois.edu

ACM Reference format:
Shaileshh Bojja Venkatakrishnan, Giulia Fanti, and Pramod Viswanath. 2017. Dandelion: Redesigning the Bitcoin Network for Anonymity. In *Proceedings of SIGMETRICS '17, June 5–9, 2017, Urbana-Champaign, IL, USA*, , 1 pages.
DOI: http://dx.doi.org/10.1145/3078505.3078528

Cryptocurrencies are digital currencies that provide cryptographic verification of transactions. In recent years, they have transitioned from an academic research topic to a multi-billion dollar industry [2]. Bitcoin is the best-known example of a cryptocurrency [3].

Cryptocurrencies exhibit two key properties: egalitarianism and transparency. In this context, *egalitarianism* means that no single party wields disproportionate power over the network's operation. This diffusion of power is achieved by asking other network nodes (e.g., other Bitcoin users) to validate transactions, instead of the traditional method of using a centralized authority for this purpose. Moreover, all transactions and communications are managed over a fully-distributed, peer-to-peer (P2P) network. Cryptocurrencies are *transparent* in the sense that all transactions are verified and recorded with cryptographic integrity guarantees; this prevents fraudulent activity like double-spending of money. Transparency is achieved through a combination of clever cryptographic protocols and the publication of transactions in a ledger known as a *blockchain*. This blockchain serves as a public record of every financial transaction in the network.

A property that Bitcoin does *not* provide is anonymity. Each user is identified in the network by a public, cryptographic key. If one were to link such a key to its owner's human identity, the owner's financial history could be partially learned from the public blockchain. In practice, it is possible to link public keys to identities through a number of channels, including the networking protocols on which Bitcoin is built [1]. This is a massive privacy violation, and can be dangerous for deanonymized users.

The objective of this paper is to redesign the Bitcoin networking stack from *first principles* to *prevent network-facilitated deanonymization* of users. Critically, this redesign must not reduce the network's reliability or performance. Although the networking stack is only one avenue for deanonymization attacks, it is an avenue that is powerful, poorly-understood, and often-ignored.

We seek a network management policy that exhibits two properties: (a) strong anonymity against an adversarial group of colluding nodes (which are a fraction p of the total network size), and (b) low broadcasting latency. The anonymity guarantees we provide are network-wide, uniformly protecting all users against a full-network deanonymization. Critically, these networking protocols should be *lightweight* and provide *statistical anonymity guarantees against computationally-unbounded adversaries.* Part of the novelty of our work is that the Bitcoin P2P networking stack has not been modeled in any detailed way (much less analyzed theoretically), to the best of our knowledge. In addition to modeling this complex, real-world networking system, our contributions are threefold:

(1) Fundamental anonymity bounds. The act of user deanonymization can be thought of as classifying transactions to source nodes. Hence we use precision and recall as natural performance metrics. Given a networking protocol, the adversary has a region of feasible (recall, precision) operating points, which are achieved by varying the source classification algorithm. We give fundamental bounds on the best precision and recall achieved by the adversary for any networking protocol.

(2) Optimal algorithm. We propose a simple networking protocol called Dandelion, whose achievable precision-recall region is nearly optimal, in the sense that it is contained in the achievable region of (nearly) every other possible networking protocol. Dandelion consists of two phases. In the first phase, each transaction is propagated on a random line; that is, each relay passes the message to exactly one (random) node for a random number of hops. In the second phase, the message is broadcast as fast as possible using diffusion. Dandelion has two key features: (a) in the first phase, all transactions from all sources should propagate over the *same* line, and (b) the adversary should not be able to learn the structure of the line beyond the adversarial nodes' immediate neighbors.

(3) Practical considerations. We outline the practical challenges associated with implementing Dandelion. In particular, constructing the graph for Dandelion in a distributed fashion, and enforcing the assumption that the adversary cannot learn the graph, are nontrivial. We therefore propose simple heuristics for addressing these challenges. A preprint of our full-paper can be found at [4].

REFERENCES

[1] Alex Biryukov, Dmitry Khovratovich, and Ivan Pustogarov. 2014. Deanonymisation of clients in Bitcoin P2P network. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 15–29.
[2] CoinMarketCap. 2016. Cryptocurrency Market Capitalizations. (2016).
[3] Satoshi Nakamoto. 2008. Bitcoin: A peer-to-peer electronic cash system. (2008).
[4] Shaileshh Bojja Venkatakrishnan, Giulia Fanti, and Pramod Viswanath. 2017. Dandelion: Redesigning the Bitcoin Network for Anonymity. *arXiv preprint arXiv:1701.04439* (2017).

SIGMETRICS '17, June 5–9, 2017, Urbana-Champaign, IL, USA
© 2017 Copyright held by the owner/author(s). ACM ISBN 978-1-4503-5032-7/17/06.
DOI: http://dx.doi.org/10.1145/3078505.3078528