Towards Enhanced Network Privacy for Blockchains

David Mödinger, Henning Kopp, Frank Kargl and Franz J. Hauck
Institute of Distributed Systems, Ulm University
Email: {david.moedinger, henning.kopp, frank.kargl, franz.hauck}@uni-ulm.de

***Abstract*—Privacy aspects of blockchains have gained attention as the log of transactions can be view by any interested party. Privacy mechanisms applied to the ledger can be undermined by attackers on the network level, resulting in deanonymization of the transaction senders. We discuss current approaches to this problem, e.g. Dandelion, sketch our own approach to provide even stronger privacy mechanisms and discuss the challenges and open questions for further research in this area.**

I. Introduction

Public blockchains provide a persistent append-only log of so called transactions. These transactions are created by local devices of users. They can include financial transactions or more general payloads, depending on the blockchain. From a privacy perspective, transactions can leak sensible information such as purchasing behavior and credit balances [1]. To provide privacy for their users, many blockchain implementations include privacy enhancing technologies, such as ring signatures or zero knowledge proofs [2]–[6].

These technologies focus on the blockchain level, i.e., they consider read access to the immutable log but do not consider privacy leaks through other possible channels like the network. Previous work [7] has shown that transactions can be attributed to a sender via the activity of a user in the network, by observing many nodes.

In this paper we examine current approaches to solve this problem of anonymous transaction dissemination. We take a look at approaches designed specifically for blockchains, as well as more general solutions. Lastly, we discuss open questions and known challenges towards improved privacy for users of blockchain systems.

II. Approaches

In this section, we list some current approaches to realize an anonymous broadcast mechanism. Figure 1 provides an illustration of the current problem, i.e. few available privacy options for blockchains on the network layer (visualized as a red ring marked with 4. in the figure). Our approach (2.) is envisioned to fill the gap between inefficient cryptographic mechanisms (1.) and efficient mechanisms which assume a somewhat weak attacker (3.).

A major anonymous cryptographic broadcast mechanism is Chaum's dining cryptographer network [8], which spawned many protocol variants and is still applied in modern state-of-the-art systems such as Dissent [9]. While cryptographic systems like this provide strong privacy guarantees, they lack performance. Dining cryptographer networks operate by having all participants compute the bit-wise xor of random

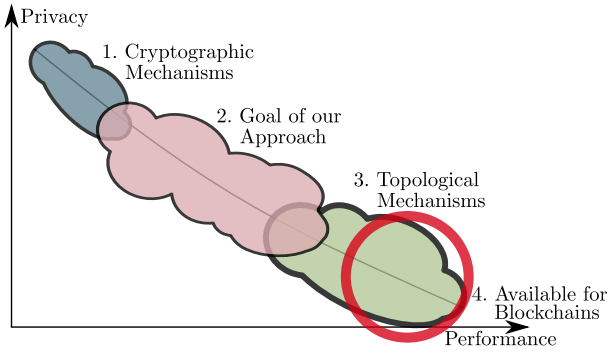

Fig. 1. Simplified illustration of the privacy-performance landscape.

message slices. If exactly one participant shares a message per round, the message can be reconstructed by all participants. Otherwise collisions can occur which must be handled appropriately. The real sender is indistinguishable among all honest participants within the group, which is the maximum guarantee that can theoretically be achieved.

On the end of the efficient protocols in the privacy-efficiency landscape, topological methods provide lightweight solutions to improved privacy. These protocols approach the problem of easy deanonymization of users through methods cheap enough that close to everyone can mount them through bot networks. However, they fail for very strong attackers that control large parts of a network.

Dandelion [10] approaches this problem through an anonymity phase, sending the message along a line graph, before applying a regular flood and prune broadcast for the actual dissemination. Dandelion was designed specifically for blockchains and provides easy adaptability for current networks that only apply regular broadcasts. Dandelion provides fast dissemination times, but its guarantees for privacy are fairly low.

Other topological mechanisms, such as adaptive diffusion [11] are not adapted specifically for blockchain applications and thus provide new challenges, as the messages transmitted by the protocol may not reach all participants. Adaptive diffusion determines a virtual source, marked by a transferable token. Throughout the protocol, the changing virtual source appears to be the originator of the message if the attacker assumes a flood and prune broadcast. If the attacker assumes the adaptive diffusion protocol is used, the probability of a node to be the origin of the message is

inversely proportional to the number of nodes that already received the broadcast.

III. Our Approach

For new blockchain applications we propose a new protocol. Our protocol consists of the following three phases.

1) Spread message within a dining cryptographer (DC) network of size k [12].
2) Determine the first virtual source within the DC-network and continue with Adaptive Diffusion for d rounds.
3) Perform a flood and prune broadcast until every participant in the network is reached.

To switch from Phase 1 to 2, the participant with the smallest xor-distance between their hashed identity and the message hash initiates Phase 2. This procedure results in a pseudo-random deterministic choice for the transition without relying on secret information while sharing the performance overhead.

For the transition to Phase 3, the last virtual source initiates a flood and prune broadcast with a command message. The round counter to determine being last is known for the current virtual source, so the information in use is neither private nor related to the origin.

As none of these transitions use any private information through the phase they transition from, they can not introduce additional information leaks. Further formalization of this working hypothesis is required for future work.

The advantage of our approach is the resistance to stronger attackers than those of Dandelion. Further, parameters k and the length of the forwarding line in Phase 2 can be chosen as a tradeoff between privacy and performance demands.

IV. Open Questions

Considering the proposed approach, there are still many challenges left for privacy researchers in the blockchain space.

- **Suitable attacker model**: Robustness of protocols depends on the choice of the attacker model. The complex structure of financial incentives of blockchains might make different attacker models more suitable for modelling. The efficiency of the protocol is heavily dependent on the chosen mechanisms to detect and avert robustness, so a suitable model might change evaluations and model selections should be discussed.
- **Choice of parameters**: For real world adoption and evaluation of privacy systems suitable parameters need to be selected. The choice of secure parameters is a problem for architects and should be addressed by research evaluations.
- **Privacy evolution** for protocols of current systems: Privacy is a desired trait not only for future blockchain applications but also for already deployed networks. Privacy evolution, the change of protocols towards more privacy while having non conforming nodes in the network, remains a huge challenge for existing systems.
- **Generalization** from transactions: Currently, approaches focus on transactions as they contain the most sensitive information. However, many blockchains come with application specific protocols, e.g., file transmission for storage systems [4], and block dissemination. While block transmissions might use privacy mechanisms, they have differing requirements from transactions, such as low latency.
- **Practical requirements**: Users are in general not going to adopt solutions to problems that inhibit their work flow or reduce their payoff or value from a system. High-latency privacy systems might not be adequate for many blockchain applications. However, the acceptable latencies for blockchain transactions are unclear and make evaluation of privacy mechanisms hard to evaluate for practical adoption.

These challenges need to be addressed for truly private blockchain systems. Solutions to these problems have interconnections with many other aspects of blockchains, so changes to the privacy aspects influence other design criteria, as well as changes to other parts of a blockchain application might break privacy or devastate efficiency of the protocol.

Acknowledgment

This work was partially funded by the Baden-Württemberg Stiftung.

References

[1] D. Ron and A. Shamir, "Quantitative analysis of the full bitcoin transaction graph," in *Financial Cryptography and Data Security*. Springer, 2013, pp. 6–24.

[2] N. van Saberhagen, "Cryptonote v 2.0," 2013, https://cryptonote.org/whitepaper.pdf.

[3] S. Noether and S. Noether, "Monero is not that mysterious," Tech. Rep., 2014, https://lab.getmonero.org/pubs/MRL-0003.pdf.

[4] H. Kopp, D. Mödinger, F. J. Hauck, F. Kargl, and C. Bösch, "Design of a privacy-preserving decentralized file storage with financial incentives," in *Proc. of IEEE Sec. & Priv. on the Blockch. (S&B) (aff. with EUROCRYPT 2017)*. IEEE, 2017.

[5] I. Miers, C. Garman, M. Green, and A. D. Rubin, "Zerocoin: Anonymous distributed e-cash from bitcoin," in *Proc. of the IEEE Symp. on Sec. and Priv. (SP)*. IEEE, 2013, pp. 397–411.

[6] E. Ben Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza, "Zerocash: Decentralized anonymous payments from bitcoin," in *IEEE Symp. on Sec. and Priv. (SP)*. IEEE, 2014, pp. 459–474.

[7] A. Biryukov, D. Khovratovich, and I. Pustogarov, "Deanonymisation of clients in bitcoin p2p network," in *Proc. of the ACM SIGSAC Conf. on Comp. and Comm. Sec. (CCS)*. New York, NY, USA: ACM, 2014, pp. 15–29.

[8] D. Chaum, "The dining cryptographers problem: Unconditional sender and recipient untraceability," *Journal of Cryptology*, vol. 1, no. 1, pp. 65–75, Jan 1988.

[9] D. I. Wolinsky, H. Corrigan-Gibbs, B. Ford, and A. Johnson, "Dissent in numbers: Making strong anonymity scale." in *Proc. of the 10th Symp. on Oper. Sys. Des. and Impl. (OSDI)*, 2012, pp. 179–182.

[10] S. Bojja Venkatakrishnan, G. Fanti, and P. Viswanath, "Dandelion: Redesigning the bitcoin network for anonymity," *Proc. of the ACM Measurement and Analysis of Comp. Sys. (POMACS)*, vol. 1, no. 1, pp. 22:1–22:34, Jun. 2017.

[11] G. Fanti, P. Kairouz, S. Oh, and P. Viswanath, "Spy vs. spy: Rumor source obfuscation," *SIGMETRICS Perform. Eval. Rev.*, vol. 43, no. 1, pp. 271–284, Jun. 2015.

[12] L. von Ahn, A. Bortz, and N. J. Hopper, "K-anonymous message transmission," in *Proc. of the 10th ACM Conf. on Comp. and Comm. Sec. (CCS)*. New York, NY, USA: ACM, 2003, pp. 122–130.