Can A Blockchain Keep A Secret?

Anders Konring

March 2021

Summary

In the paper *Can A Blockchain Keep A Secret?*, Benhamouda et al. investigate a public blockchain's ability to; store a piece of data, keep it secret and only use it under specific conditions.
One immediate application of such a scheme is signatures where the secret key ”lives” inside the blockchain and is used for signing statements on behalf of the blockchain. In particular, a blockchain can sign its own blocks (checkpointing) and let newly arrived nodes of the network validate the state of the blockchain by verifying only a small signature.

The paper considers a setting with a mobile adversary ([OY91]) which gives rise to a Proactive Secret Sharing (PSS) scheme[1]. This is the scheme that will let the blockchain ”keep” its secret safe. But it is prohibitively expensive to re-share the secret across thousands or even millions of nodes. Therefore the set of nodes that are holding the secret at any given time is capped to a certain threshold (i.e. committees).

The main challenge of the paper is that in order to keep communication complexity in a feasible range the size of committees needs to be $n \ll N$ where N is the total number of nodes in the network *but* a mobile adversary with a standard corruption budget (e.g. $N/4$) will have no problem corrupting all members of the small committee as soon as she knows who they are.

The main contribution of the paper is a way to overcome the above challenge by letting the adversary stay oblivious to the identity of the members in committee holding the secret. Only when the members have already shared the secret will the adversary become aware of their identity but at that point it is too late for the adversary to gain any knowledge about the secret. The members of the committee have already deleted their state and old shares before handing over the re-randomized shares to the next committee.

The paper seeks to construct at secret sharing scheme with the above properties and a natural technique to employ is that of ”player replaceability” which ensures the committee members are anonymous until after they have performed their actions. The construction suggested in the paper relies on an array of underlying primitives such as Verifiable Random Functions (VRFs), Anonymous Public Key Encryption (PKE) and the paper examines the security of these primitives in depth.

[1] https://en.wikipedia.org/wiki/Proactive_secret_sharing

Importance

The technique of ”player replaceability” was (re-)introduced in the paper describing the Algorand blockchain protocol ([Gil+17]). A lot of research is focused on combining the trust and resilience of blockchain systems with new applications in multiparty computation and, indeed, it is intriguing to think of a blockchain keeping a secret or maybe even computing on the secret before using it for some specific purpose. All while being secure against a mobile adversary.

Improvements

The construction suffers from the fact that it only allows for less than $N/4$ corrupted parties in order to stay secure. This threshold is much lower than what we normally expect from blockchain systems and thus it is interesting to research new ways to obtain the similar properties while, at the same time, allow for a higher corruption threshold.

References

[Gil+17] Yossi Gilad et al. “Algorand: Scaling byzantine agreements for cryptocurrencies”. In: *Proceedings of the 26th Symposium on Operating Systems Principles.* 2017, pp. 51–68.

[OY91] Rafail Ostrovsky and Moti Yung. “How to withstand mobile virus attacks”. In: *Proceedings of the tenth annual ACM symposium on Principles of distributed computing.* 1991, pp. 51–59.