Report on "Perun: Virtual Payment Hubs over Cryptocurrencies"

Joakim Brorsson

May 2021

1 Introduction

Digital currencies are, among other things, expected to provide a technical means to enable microtransactions. In particular, digital currency transactions is expected to be fast and cheap. In the last decade, cryptocurrencies has been the by far most popular form of digital currencies in both research and rate of adoption. For example, the largest one by value, Bitcoin, is by now a household name.

A cryptocurrency revolves around a global ledger, called the *blockchain*, which records the current owners of coins by logging the transfer of them. This ledger is maintained by a decentralized consensus algorithm which allows anyone to participate in the process of determining the global state of the ledger. A transaction of a coin can only be guaranteed to be recognized by another party if it is recorded on the global ledger. Such a transaction is called *on-chain*. When using a blockchain, it is essential to only recognize on-chain transactions as valid in order to guard against any malicious party attempting to spend the same coin twice in a *double spending* attack.

Simultaneously, the consensus algorithms of the largest crytocurrencies have a low transaction troughput (Bitcoin: ∼7tx/s, Ethereum: ∼30tx/s), resulting in expensive transaction fees (about ∼20 USD for Bitcoin and Ethereum). Further they have long confirmation times (Bitcoin: ∼10-60min, Ethereum: ∼15-750s), making transactions slow.

1.1 Payment Channels

In order to facilitate microtransactions for cruyptocurrencies, we thus need new solutions. One of the most prominent ones is the concept of *payment channels*, which, allow *off-chain* transactions, not bound by the inefficiencies of decentralized consensus.

A payment channel is constructed by 2 parties contributing funds for the channel in an on-chain deposit, called the funding transaction. The parties can then maintain a local off-chain balance between them. At any time, any party can opt to close the channel and pay out the current balance using the on-chain

deposit. Locking the channel funding up on-chain maintains security against double spending attacks.

Due to the fact that payment channels requires on-chain transactions for both opening and closing channels, they are not suitable on their own for ad-hoc microtransactions, i.e. when payments are not regular between the same parties. This problem is addressed by *payment networks*, where multiple payment channels can be linked together to facilitate transactions through untrusted intermediaries. Thus, as long a there is a route in a network of payment channels, intermediaries on the route can facilitate the transaction, for a fee.

2 Virtual Payment Channels

The "Perun" paper [Dzi+19b] introduces the concept of *virtual* payment channels. If "regular" payment channels are seen as a layer on top of a blockchain, virtual payment channels can be seen as a layer on top of "regular" payment channels.

Assume that there exists 2 "regular" payment channels, one from Alice to Ingrid, and one from Ingrid to Bob. The innovation of virtual payment consists of being able to borrow from the deposits of existing "regular" channels to act as a deposit when establishing a new, virtual, channel between Alice and Bob. This enables allocation of payment channels without on-chain transactions. Further, the intermediary Ingrid only needs to be involved during channel establishment and closing. This contrasts to other proposals for paying via intermediaries, e.g. Lightning [PD16] where any intermediary needs to be involved in every transaction.

3 Discussion

Virtual payment channels constitute a new exciting building block for an alternative way to build payment networks, where the role of intermediaries is less involved. This is done in follow up work [DFH18]. Follow up work also leverages virtual payment channels to construct state channels, which is an extension to handle smart contracts on off-chain channels, and making the channels multi-party [Dzi+19a].

However, for a paper whose main goals is to lower fees, I miss a more detailed discussion on the financial incentives for collecting theses fees. The intermediate is expected to allow (parts of) its deposit to be used as deposit for transactions between other parties. While the virtual channel is open, the intermediary is thus prevented from using this part of the deposit to transact with Alice or Bob. Since the role if the intermediary is not completely removed, the complete removal of payments to intermediaries warrants further discussion than what is provided in the paper.

References

[PD16] Joseph Poon and Thaddeus Dryja. *The bitcoin lightning network: Scalable off-chain instant payments*. 2016.

[DFH18] Stefan Dziembowski, Sebastian Faust, and Kristina Hostáková. "General state channel networks". In: *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*. 2018, pp. 949–966.

[Dzi+19a] Stefan Dziembowski et al. "Multi-party virtual state channels". In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer. 2019, pp. 625–656.

[Dzi+19b] Stefan Dziembowski et al. "Perun: Virtual payment hubs over cryptocurrencies". In: *2019 IEEE Symposium on Security and Privacy (SP)*. IEEE. 2019, pp. 106–123.