We would like to introduce Perun – a protocol system for building virtual payment and state channel networks.

Perun is currently described in two academic research papers. A short description of these research papers and links to the pre-print versions are given below.

1. Perun: Virtual Payment Hubs over Cryptographic Currencies (http://eprint.iacr.org/2017/635)

Introduces the concept of channel virtualization as an alternative for routing payments via intermediaries using the hash-locked based transactions. The main advantage of channel virtualization is that once the virtual channel is established, payments can be carried out without interaction with the intermediary. This reduces fees and latency, while at the same time improving availability.

1. Foundations of state channel networks (https://eprint.iacr.org/2018/320).

Develops formal protocol specification for building state channel networks that have two main features: (i) our protocols allow to run arbitrary smart contracts off-chain, and (ii) we can support channel networks of any complexity (i.e., any number of intermediaries can be involved). Our state channel network supports full concurrency and use channel virtualization to minimize the need for interaction with intermediaries.

All our protocols are given in pseudocode and are proven secure in the universal composability framework commonly used in cryptography for analyzing the security of protocols. We would be happy to further work together closely with the Ethereum research community and improve our models and constructions. For us it would be helpful to receive further feedback on our approach – in particular whether the Ethereum community views formal security models (such as our UC modeling) for off-chain protocols as an important criteria for massive deployment of these technologies.

Best regards,

The Perun research team