SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

Interhead Hydra: Two Heads are Better than One

Maxim Jourenko * Mario Larangeira † Keisuke Tanaka ‡

Keywords: blockchain, channels, Layer-2, cryptographic protocols

Abstract

Distributed ledger are maintained through consensus protocols executed by mutually distrustful parties. However, these consensus protocols have inherent limitations thus resulting in scalability issues of the ledger. Layer-2 protocols operate on *channels* and allow parties to interact with another without going through the consensus protocol albeit relying on its security as fall-back. Prominent Layer-2 protocols are payment channels for Bitcoin that allow two parties to exchange coins and State Channels for Ethereum that allow two parties to execute a state machine. Channels can be concatenated into networks using techniques such as Hashed Timelocked Contracts to execute payments or virtual state channels as introduced by Dziembowski et al. [3, 4] to execute state machines. These constructions allow interaction between two parties across a channel network, i.e. the two endpoints of a path of channels. This is realized by utilizing *intermediaries*, which are the parties on the channel path which are in-between both endpoints, who have to pay collateral to ensure security of the constructions. Dziembowski et al. [2] introduced multi-party state channels based on a virtual channel construction and more recently Hydra *heads* [1] is a channel construction that allows multiple parties the execution of Constraint Emitting Machines (CEM). While existing protocols such as HTLCs can be extended s.t. two parties can interact with another across multi-party channels, there are no dedicated constructions that utilize multi-party channels and similarly allow more than two parties to interact across a network of such channels. This presentation presents our ongoing work to address this gap by extending Hydra and introducing the Interhead construction that allows for the iterative creation of virtual Hydra heads. Our construction is the first that (1) supports and utilizes multi-party channels and (2) allows for collateral to be paid by multiple intermediaries which allows to share this burden and thus improves practicality.

References

[1] Manuel MT Chakravarty, Sandro Coretti, Matthias Fitzi, Peter Gazi, Philipp Kant, Aggelos Kiayias, and Alexander Russell. Hydra: Fast isomorphic state channels. In *International Conference on Financial Cryptography and Data Security*. Springer, 2021.

[2] Stefan Dziembowski, Lisa Eckey, Sebastian Faust, Julia Hesse, and Kristina Hostáková. Multi-party virtual state channels. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 625–656. Springer, 2019.

[3] Stefan Dziembowski, Lisa Eckey, Sebastian Faust, and Daniel Malinowski. Perun: Virtual payment hubs over cryptocurrencies. In *Perun: Virtual Payment Hubs over Cryptocurrencies*. IEEE, 2017.

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

* The University of Tokyo, 7 Chome-3-1 Hongo, Bunkyo City, Tokyo 113-8654

† Tokyo Institute of Technology, 2 Chome-12-1 Ookayama, Meguro City, Tokyo 152-8550
IOHK, IOG Singapore Pte Ltd 4 Battery Road, #25-01 Bank of China Building, Singapore (049908)

‡ Tokyo Institute of Technology, 2 Chome-12-1 Ookayama, Meguro City, Tokyo 152-8550