Enabling Asynchronous State Channels with uSHARDING

Collaboration Proposal

Eleftherios Kokoris-Kogias
EPFL

1 Extended Abstract

Off-chain protocols (or so called Layer 2) are a promising solution to the scalability and privacy challenged of blockchain systems. One prominent approach are state-channels, whose core idea is that the state changes between two parties in consensus need not be transparently published. Instead on-chain computation (acting as a trusted third party) is only required when the parties are in dispute.

Current proposals however have two major shortcomings, first they require a synchronous network to preserve the fairness of the channel signaling to an adversary the exact amount of time he needs to control the network in order to attack clients. Second they forfeit auditability of the state-changes in the channel in order to provide some notion of privacy, which makes channels unsuitable for any kind of regulated process.

In this work we propose the use of committees selected by the channel participants in order to provide secure channels even in the presence of full asynchrony. The core idea is that committees witness the totally ordered state-changes of the channel's state and step in when a dispute among the parties exist. In order realistically support committees we propose an incentive mechanism to defend against DoS attacks and the creation of a witness market supported by an accountable reputation system to provide deterrents to bribing. We call our approach uSHARDING as we borrow the idea of a threshold secure committee from the on-chain sharding approached, however we note that in our approach the committee selection is driven by the channel participants and need not be globally agreed.

After introducing the uSHARDING, we can further leverage the committees to provide audibility of channels. We construct the channel's state update to form a temporary internal blockchain which the committee stores. In order to preserve privacy the state updates are encrypted and only then presented to the committee, however the encryption key is secret-shared towards the committee and can be reconstructed if a regulator request such. In order to provide accountability for the regulator we require that he posts his decryption request on-chain and only then will the committee provide him with the decryption key and the requested encrypted state changes.

References