

Virtual Channels and Rebalancing in State Channel Networks

Arya Stark

Introduction

This research note was written because there are some unsolved problems in designing state channel networks that are not well-known or being worked on. Precisely defining these problems requires formally modelling of state channel networks, and the problems presented are only present if the formal models include agents' preferences over network topology (payment capacity), blockchain fees, and capital costs.

Relevant Prerequisite Literature

This section goes through relevant existing literature. Note that even if you know all this, many definitions will be used in later sections.

Ball-and-bead model of PCN

I first saw this nice model from Peter Rizun on Twitter. TBW.

Rebalancing

We say that two channel networks are value-equivalent if the set of agents is the same and each agent owns the same. A channel network is rebalanced when it transitions into a value-equivalent state. This transition can include on-chain transactions or not. Here are examples.

In the ball-and-bead model, an on-chain rebalance is represented by "hopping wires".

Are off-chain rebalances sufficient? In general, no. In fact we can import the existing literature on flow networks to state this quite precisely.

TBW: define a a, b -flow, apply max-flow-min-cut theorem, etc.

Note some assumptions implicitly made when applying this theorem: the max flow might require very global knowledge to compute.

Fun exercise! A self-payment is a special type of off-chain rebalance. Show that any rebalance can be expressed as a series of self-payments.

Subchannels

Also known as channel factories, although this is not such a good name.

Virtual Channels

TBW

State Channel Networks

Multipath

Ejecting Virtual Channels

Plasma

Claim: a super-optimized channel network will be less useful than a very suboptimal one that supports funding via plasma!

Informal Formal Model

Ejection Test Cases

Asymmetric

This is a plausible test case because it is minimal in the number of transactions. Even after account abstraction, it is minimal in the number of ERCECOVERS.

Symmetric

Plausible because of capacity

Symmetric Unidirectional

Asymmetric Unidirectional

Long-Chain Large-Radius

Long-Chain Short-Radius

Multipath

Long-Chain Multipath

Thanos Star

Minimal in number of transactions

Self-Lock-In