4 Proofs of Construction

- what does safety mean? - putting money into joint control. can I get some of it back if cooperation breaks down.

- paper aims to put in place a framework for reasoning about the correctness of state channel constructions - reasoning about what I hold off-chain and what if means to me

- how to extract value - states —¿ outcomes —¿ money - reducing channel diagrams –¿ value

- outcome diagrams - fundamental rule of state channels - if two states are worth the same, I will transition between them - the "simple rule of state channels" - we ignore other factors - value - funded ? - offloaded

- safe - this is the guarantee that if a participant stops at any point other participants don't lose out

- allows rewriting - [diagram] example: closing off-chain

- two questions (finalization + redistribution) - what can I definitely finalize? - what can I definitely redistribute to myself?

- protocol design: how can I move between states in single moves that keep the value the same - .. when we don't allow atomic changes across channels

- presenting a construction / protocol - in particular when presenting a protocol we must demonstrate a series single state updates, demonstrate that the value is preserved - in particular the way we do this: - demostrate a construction funds a channel - demonstrate we can build it from another state - give a series of waypoint states - universally finalizable outcomes - of a special type of channel - consensus channels, running a particilar protocol - use the specifics of this channel to say we can move between them in a safe manner

4.1 Finalizable outcomes

- definition: statement - definition: channel state - definition: adjudicator state - definition: system state

- the rules of strategies

subsection consensus game [diagram] - pictorial representation of consensus game

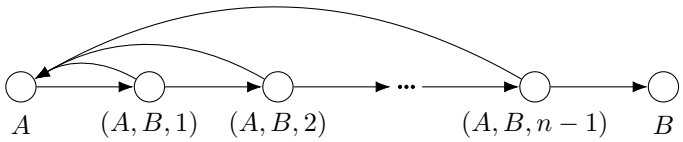

Figure 1: *Cool, huh?*