Security via Fraud Proof

As AltLayer provisioned rollups are optimistic in nature, they are secured by the underlying chain via fraud proofs. AltLayer uses a bisection protocol to narrow down the point of contention to a single VM instruction. Once the specific instruction on which there is a contention has been identified, the system proceeds to re-execute that specific instruction with the corresponding state. This section presents the on-chain dispute resolution using bisection. Bisection in itself is an interactive off-chain protocol between a proposer claiming that a set of transaction and the ensuing state changes are valid and a challenger claiming otherwise. The end result of the bisection protocol is a transaction and an instruction in that transaction that the challenger claims to have been incorrectly executed. The protocol works as follows: 1. 1. 2. Challenger chooses to dispute one or more of the properties of the pack being finalized, e.g., wrong state transition hash, wrong transaction root hash; 3. 2. 4. For each of the properties being disputed, the jury is being notified of the point of contention between the proposer and the challenger using a bisection method; 5. 3. 6. Challenger disputes any Merkle root hash asserted by the proposer; 7. 4. 8. Proposer produces the two hashes used to generate the Merkle root hash, each corresponding to half of the state transitions; 9. 5. 10. Challenger chooses one of the two sides to dispute, resulting in the proposer producing the two hashes used to generate the disputed hash This goes on until the dispute is on the hash of the Merkle tree leaf node; 11. 6. 12. Note that this leaf node is the contention between the challenger and the proposer. AltLayer's In-House Rollup Stack in Depth -Previous Decentralized Sequencer Set Next- Rollup Types Flash Layer Rollups