GRANDPA

Introduction

GRANDPA, which stands for "G host-basedR ecursiveAN cestorD erivingP refixA greement ," is the consensus algorithms used by Avail. GRANDPA works in conjunction with another consensus GRANDPA in and of itself is a block finalization algorithm, and as such needs to be paired with block-authoring mechanisms likeAura(opens in a new tab) or BABE (Avail uses BABE) to ensure a properly functioning blockchain.

Finality in GRANDPA's context means that once a block is added to the blockchain, it is irreversible and cannot be reverted. This is in contrast to probabilistic finality found in some other consensus mechanisms.

To observe a straightforward illustration of GRANDPA in action, inspecting Avail node log files reveals both the importation of blocks and the subsequent finalization of these blocks. In the below logs extract, the first block to undergo finalization is 127972, followed by 127973 and 127974. As emphasized earlier, this signifies that the information contained in blocks from 127974 and those preceding it has achieved finality, rendering them immutable and irreversible.

Idle (18 peers), best: #127974 (0x181d…06a9), finalized #127972 (0x21ce…50eb), ⬇ 339.5kiB/s ⬆ 368.3kiB/s ✣ Imported #127975 (0x334f…38b7)   Idle (18 peers), best: #127975 (0x334f…38b7), finalized #127973 (0x9513…0b53), ⬇ 298.8kiB/s ⬆ 380.2kiB/s ✣ Imported #127976 (0x4f1d…c015)   Idle (18 peers), best: #127976 (0x6a21…1904), finalized #127974 (0x181d…06a9), ⬇ 224.2kiB/s ⬆ 374.0kiB/s

GRANDPA Functions

Here's an overview of how GRANDPA functions within Avail, up and above finality.

GHOST Protocol : GRANDPA utilizes the GHOST (Greedy Heaviest Observed Sub-Tree) protocol, a concept borrowed from Ethereum's blockchain protocol. The GHOST protocol helps in selecting the most secure and agreed-upon chain by considering not only the main chain but also the "uncles" or competing blocks.

Recursive Ancestor Derivation : GRANDPA employs a recursive ancestor derivation mechanism to efficiently determine the finality of blocks. This process involves determining a common ancestor among a set of competing blocks in the network. This common ancestor is then used to finalize the blocks.

Byzantine Fault Tolerance : GRANDPA is Byzantine Fault Tolerant, meaning it can maintain its correctness and security even when some nodes in the network behave maliciously or fail. This is crucial for ensuring the robustness of the consensus algorithm in the face of potential attacks.

Finality Gadget : GRANDPA is often referred to as a "finality gadget" because it specifically focuses on providing finality to the blocks produced by the BABE consensus algorithm on the Avail chain. While BABE is responsible for proposing and producing blocks, GRANDPA finalizes these blocks, ensuring that they are permanently added to the blockchain.

GRANDPA Finalisation Steps

GRANDPA sequence of events to bring about the finalization of new blocks:

- A node assigned as the "primary" disseminates the highest block it deems potentially final from the preceding round.
- Following a network delay, each validator broadcasts a "pre-vote" for the highest block it believes should be finalized. Assuming the supermajority of validators are honest,
- this block should extend the chain initially broadcast by the primary. This newly proposed chain might consist of several blocks more than the last chain that was officially finalized.
- Each validator calculates the highest block that can be deemed finalized based on the collection of pre-votes. If the set of pre-votes extends the last officially finalized chain,
- each validator proceeds to cast a "pre-commit" in favor of that particular chain.
- Subsequently, each validator awaits the reception of adequate pre-commits to formulate a commit message, officially endorsing the newly finalized chain.

BABE NPoS