GRANDPA
Finality Gadget

GRANDPA Introduction

GRANDPA is a finality gadget, that is a protocol that can be used to provide provable finality for a blockchain. It works in addition to a block production mechanism and a chain selection rule, that on their own would only provide eventual consensus.

- We have a set of n validators of whom at least n-f = 2f+1 are honest. Blocks are continually produced and are related to each other as a tree. The goal of a consensus protocol is to select blockchain, that is a branch of this tree, that all honest validators agree on.

- A block is final when all consensus participants agree that it is in their view of the consensus chain forever after.

  ↳ A protocol like Bitcoin has only probabilistic finality: any block might be reverted but we can bound the probability that it happened.

  ↳ Protocols that use Byzantine agreement, like Tendermint or Algorand, can have provable finality, where not only are blocks never reverted but we can provide a proof that a block is final under honesty assumptions.

  ↳ A finality gadget, like Casper FFG or GRANDPA, works with a block production mechanism and chain selection rule that has probabilistic finality and provides provable finality for blocks that it agrees on.

- GRANDPA attempts to finalise the prefix of the chain that 2/3 of voters agree on according to their best chain rule, whether that is one or thousands blocks.

- GRANDPA can work with many block production mechanisms and best chain rules. For example, the rule could be to build blocks on the longest chain including the latest block and the block production could be by miners using proof of work. If we do this, then we will probably agree on a longer chain that the last finalised block soon. At this point GRANDPA should finalise that.

The design of GRANDPA aims at separating the finality gadget and block production as cleanly as possible and obtain formal guarantees for the finality gadget.

Formal guarantees

Safety

All blocks finalised by any validator lie on a single chain.

Validity

For any finalised block B, it must hold that that at some prior time, an honest validator queried the chain selection rule for the best chain including an ancestor of B and then the response was a chain including B.

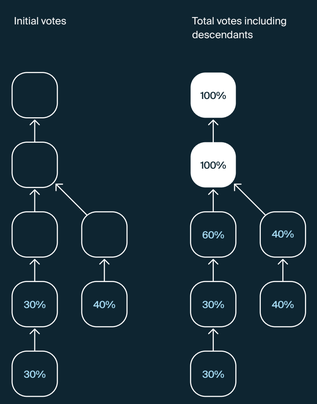
Liveness

For any finalised block B, it must hold that that at some prior time, an honest validator queried the chain selection rule for the best chain including an ancestor of B and then the response was a chain including B.

The finality gadget keeps finalising blocks unless the chain rule fails to agree on a child of the last finalised block or no such child is ever produced. That is, the following scenario is impossible:
↳ the finality gadget has finalised a block B but it never finalises any child of B and
↳ there is a child C of B, such that after some time, any validator sees that the best chain including B, also includes C.

The 2/3-GHOST function

We interpret a vote as for not just one block, but the chain with that block as head. The 2/3 GHOST function g(), applies to a set of votes and returns the head of the longest prefix of the chain that is a prefix of over 2/3 of these chains, that is the latest block such that over 2/3 of votes are for it or one of its descendents.



Description of GRANDPA protocol:

A validator starts round r > 1 when we have an estimate E of the last finalised block from the last round, r-1. Concretely E is the first block on the chain of g(prevotes seen in last round) that has that for every possible child C, either n-f prevotes or n-f precommits are not for C or its descendents. We update this estimate on receipt of new votes from the previous round.

1. Primary gossips their estimate E of the last possible block that could be finalised in round r-1.

2. After time t+2T, any node casts its prevote for the best chain containing the primaries estimate, if we received it and it is safe and valid, or else its own estimate. The primary's block is safe if it is a descendent of our estimate and valid if it is an ancestor of g(pre).

3. After time t+4T and after g(prevotes seen this round) is a descendent of or equal to our estimate E, gossip a precommit for g(prevotes seen this round)

We consider g(precommits seen from any one round) and all its ancestors final.

Key for protocol description:

- **g()** 2/3-GHOST function, see diagram
- **n** number of validators
- **f** maximum number of Byzantine validators, n=3f+1
- **E** current estimate of finalised block from previous round
- **T** upper bound on gossip time.
- **t** subjective start time of current round

Time

0*t* — 2*t* — 4*t*

Primary Broadcast

The primary sends their estimate of the latest block finalised in the last round.

Prevote phase

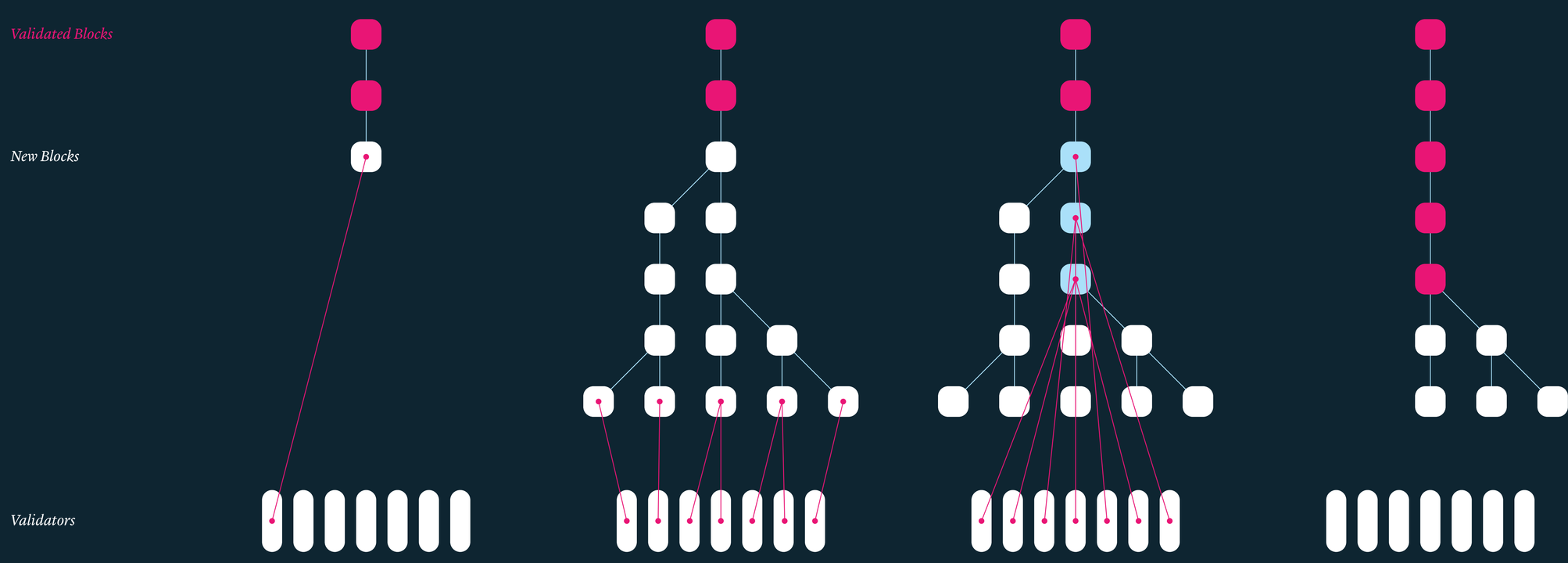
Each validator votes on the best chain containing either the primary's estimate or their own estimate.

Precommit phase

Each validator votes on the ⅔ GHOST of the prevotes they saw.

Finalisation

The ⅔ GHOST of the precommits is final.



GRANDPA advantages

Separating the block production from finality makes for a flexible consensus protocol, giving advantages such as:

- Block time can be completely independent of GRANDPA round time and in turn finality time. With many participants, finality time may need to be much longer, and we would finalise many blocks per round. Conversely block times may need to be longer than we could finalise blocks with only a few validators before the next block is produced.

- Changing consensus is easy. It is possible to switch GRANDPA on and off, or change the underlying block production mechanism relatively easily.
- We can selectively delay finality of blocks, without affecting block production. Essentially this allows producing blocks faster than we are able to fully verify their correctness.

This is crucial for GRANDPA's application to Polkadot, which needs additional criteria for finalizing a block, related to the correctness of sub-chains. If we need to wait for these, then we can still produce and execute blocks at the same rate and then hopefully finalise many at once.

GRANDPA in Practice

- GRANDPA is the finality gadget used for the Polkadot system (https://polkadot.network)
- Used in Polkadot's "canary network" Kusama (https://kusama.network)
- GRANDPA has been used with two block production protocols, Aura and BABE, and more are planned.
- It has been tested on testnets with up to 100 voters where it still was able to finalise blocks in under 2s.

web3 foundation · Polkadot. · KUSAMA