

Polkadot Runtime Environment

Protocol Specification

February 8, 2019

1 Conventions and Definitions

Definition 1. *Runtime* is the state transition function of the decentralized ledger protocol.

Definition 2. A **path graph** or a **path** of n nodes, formally referred to as P_n , is a tree with two nodes of vertex degree 1 and the other $n-2$ nodes of vertex degree 2. Therefore, P_n can be represented by sequences of (v_1, \dots, v_n) where $e_i = (v_i, v_{i+1})$ for $1 \leq i \leq n-1$ is the edge which connect v_i and v_{i+1} .

Definition 3. **radix r tree** is a variant of a trie in which:

- Every node has at most r children where $r = 2^x$ for some x ;
- Each node that is the only child of a parent, which does not represent a valid key is merged with its parent.

As a result, in a radix tree, any path whose interior vertices all have only one child and does not represent a valid key in the data set, is compressed into a single edge. This improves space efficiency when the key space is sparse.

Definition 4. By a **sequences of bytes** or a **byte array**, b , of length n , we refer to

$$b := (b_0, b_1, \dots, b_{n-1}) \text{ such that } 0 \leq b_i \leq 255$$

We define \mathbb{B}_n to be the **set of all byte arrays of length n** . Furthermore, we define:

$$\mathbb{B} := \bigcup_{i=0}^{\infty} \mathbb{B}_i$$

Notation 5. We represent the concatenation of byte arrays $a := (a_0, \dots, a_n)$ and $b := (b_0, \dots, b_m)$ by:

$$a || b := (a_0, \dots, a_n, b_0, \dots, b_m)$$

Definition 6. For a given byte b the **bitwise representation** of b is defined as

$$b := b^7 \dots b^0$$

where

$$b = 2^0 b^0 + 2^1 b^1 + \dots + 2^7 b^7$$

Definition 7. By **little-endian** representation of non-negative integer I represented as

$$I = (B_n \dots B_0)_{256}$$

In two base 256, is a byte array $B = (b_0, b_1, \dots, b_n)$ such that

$$b_i := B_i$$

Definition 8. By **UINT32** we refer to a non-negative integer stored in a byte array of length 4 using little-endian encoding format.

Definition 9. A **blockchain** C is a directed path graph. Each node of the graph is called **Block** and indicated by B . The unique sink of C is called **Genesis Block** and the source is called the **Head** of C . For any vertex (B_1, B_2) where $B_1 \rightarrow B_2$ we say B_2 is the **parent** of B_1 and we indicated by

$$B_2 := P(B_1)$$

2 Block

In Polkadot RE, a block is made of two main parts, namely the *block header* and the *list of extrinsics*. The *Extrinsics* represent the generalization of the concept of *transaction*, containing any set of data that is external to the system, and which the underlying chain wishes to validate and keep track of.

2.1 Block Header

The block header is designed to be minimalistic in order to boost the efficiency of the light clients. It is defined formally as follows:

Definition 10. The **header of block B** , $\text{Head}(B)$ is a 5-tuple containing the following elements:

- **parent_hash:** is the 32-byte Blake2s hash of the header of the parent of the block indicated henceforth by H_p .
- **number:** formally indicated as H_i is an integer, which represents the index of the current block in the chain. It is equal to the number of the ancestor blocks. The genesis block has number 0.
- **state_root:** formally indicated as H_r is the root of the Merkle trie, whose leaves implement the storage for the system.
- **extrinsics_root:** is the field which is reserved for the runtime to validate the integrity of the extrinsics which compose the block body. For example, it can hold the root hash of the Merkle trie which stores an ordered list of the extrinsics being validated in this block. This element is formally referred to as H_e .
- **digest:** this field is used to store any chain-specific auxiliary data, which could help the light clients interact with the block without the need of accessing the full storage. Polkadot RE does not impose any limitation or specification for this field. Essentially, it can be a byte array of any length. This field is indicated as H_d

Definition 11. The **Block Header Hash of Block B** , $H_h(b)$, is the hash of the header of block B encoded by simple codec:

$$H_h(b) := \text{Blake2s}(\text{Enc}_{\text{SC}}(\text{Head}(B)))$$

2.2 Justified Block Header

The Justified Block Header is provided by the consensus engine and presented to the Polkadot RE, for the block to be appended to the blockchain. It contains the following parts:

- **block_header** the complete block header as defined in Section 2.1 and denoted by $\text{Head}(B)$.

- **justification:** as defined by the consensus specification indicated by $\text{Just}(B)$ [\[link this to its definition from consensus\]](#).
- **authority Ids:** This is the list of the Ids of authorities, which have voted for the block to be stored and is formally referred to as $A(B)$. An authority Id is 32bit.

2.3 Extrinsics

Each block also contains a list of extrinsics. Polkadot RE does not specify or limit the internal of each extrinsics beside the fact that each extrinsics is a byte array encoded using SCALE codec [34].

The `extrinsics_root` is set by the runtime and its value is opaque to Polkadot RE.

The extrinsics in a block are ordered using by pairing each extrinsics by a UINT32 integer sequential number starting at 0 which is encoded using SCALE codeca.

3 Interactions with the Runtime

Runtime is the code which implement the logic of the chain. This code is decoupled from the Polkadot RE in order to make the runtime easily upgradable without the need to upgrade the Polkadot RE. In this section we describe the details upon which the Polkadot RE is interacting with the Runtime.

3.1 Loading the Runtime code

Polkadot RE expects to receive the code for the runtime of the chain as a compiled WebAssembly (Wasm) Blob. The current runtime is stored in the state database under the key represented as a byte array:

$$b = 3A,63,6F,64,65$$

which is the byte array of ASCII representation of string “:code” (see Section 9). For any call to the runtime, Polkadot RE makes sure that it has most updated runtime as calls to runtime have potentially the ability to change the runtime code.

The initial runtime code of the chain is embedded as an extrinsics into the chain initialization JSON file and is submitted to Polkadot RE (see Section 8).

Subsequent calls to the runtime have the ability to call the storage API (see Section 3.4) to insert a new Wasm blob into runtime storage slot to upgrade the runtime.

3.2 Code Executor

Polkadot RE provide a Wasm Virtual Machine (VM) to run the runtime. The Wasm VM exposes the Polkadot RE API to the Runtime. And execute call to the Runtime entries stored in the Wasm module. This part of the runtime environment is referred to as the *Executor*.

In this section we specify the general setup for an Executor call into the runtime. In Section 3.3 we specifies the parameter and the return value of each runtime entry separately.

3.2.1 ABI Encoding between Runtime and the Runtime Environment

All data exchanged between Polkadot RE and the runtime is encoded using SCALE codec described in Section 7.1.

3.2.2 Access to Runtime API

When Polkadot RE calls a runtime entry it should make sure runtime has access to the all Polkadot Runtime API functions described in Appendix 3.4. This can be done for example by loading another Wasm module alongside the runtime which imports these functions from Polkadot RE as host functions.

3.2.3 Sending argument to Runtime

In each invocation of a Runtime entry the arguments which are supposed to be sent to the entry needs to be encoded using SCALE coded into a byte array B . The executor then needs to retrieve the memory buffer of the runtime Wasm module and extend it to fit the size of the byte array and copy the byte array value in the correct offset of the extended buffer. Finally when the Wasm method corresponding to the entry is called, two UINT32 integer are sent to the method as arguments. The first is the offset of the byte array B in the extended shared memory buffer and the second is the size of B .

3.2.4 Return value from a Runtime entry

The value which is returned from the invocation is two consecutive UINT32 integers in which the first is the pointer to the offset of the result returned by the entry encoded in SCALE codec in the memory buffer. The second is the size of the blob.

3.3 Entries into Runtime

Polkadot RE assumes that at least the following functions are implemented in the Runtime Wasm blob and has been exported as shown in Snippet 1:

```
(export "version" (func $version))
(export "authorities" (func $authorities))
(export "execute_block" (func $execute_block))
(export "validate_transaction" (func $validate_transaction))
(export "initialise_block" (func $initialise_block))
```

Snippet 1. Snippet to export entries into the Wasm runtime module

The following sections describe the standard based on which Polkadot RE communicates with each runtime entry.

3.3.1 version

This entry receives no argument, it returns the version data encoded in ABI format described in Section 3.2.1 containing the following data:

Name	Type	Description
<code>spec_name</code>	String	runtime identifier
<code>impl_name</code>	String	the name of the implementation (e.g. C++)
<code>authoring_version</code>	UINT32	the version of the authorship interface
<code>spec_version</code>	UINT32	the version of the runtime specification
<code>impl_version</code>	UINT32	the version of the runtime implementation
<code>apis</code>	ApisVec	List of supported AP

Table 1. Detail of the version data type returns from runtime `version` function

3.3.2 authorities

This entry is to report the set of authorities at a given block. It receives `block_id` as an argument, it returns an array of `authority_id`'s.

3.3.3 execute_block

This entry is responsible to execute all extrinsics in the block and reporting back the changes into the state storage. It receives the block header and the block body as its arguments and it returns a triplet:

Name	Type	Description
<code>results</code>	Boolean	Indicating if the execution was su
<code>storage_changes</code>	[[?]]	Contains all changes to the state storage
<code>change_updat</code>	[[?]]	

Table 2. Detail of the data `execute_block` returns after execution

3.3.4 validate_transaction

[Explain function]

3.4 Runtime API

Runtime API is a set of functions, which Polkadot RE exposes to Runtime to access external functions which are needed for various reasons, such as Storage content access and manipulation, memory allocation and also for efficiency reason. In each subsequent subsection for each category of those functions are specified.

3.4.1 Storage

- `ext_child_storage_root`
- `ext_clear_child_storage`
- `ext_clear_prefix`
- `ext_clear_storage`
- `ext_exists_child_storage`
- `ext_get_allocated_child_storage`
- `ext_get_allocated_storage`
- `ext_get_child_storage_into`
- `ext_get_storage_into`
- `ext_kill_child_storage`
- `ext_set_child_storage`
- `ext_set_storage`

Sets the value of a specific key in the state storage.

Arguments:

- `key`: 32bit pointer pointing the buffer containing the key.

- `key_len`: UINT32 integer specifying the key length.
- `value`: 32bit pointer pointing the buffer containing the value to be stored under the key.
- `value_len`: UINT32 integer specifying the length of the value buffer.
- `ext_storage_changes_root`
- `ext_storage_root`
- `ext_exists_storage`

3.4.2 Memory

- `ext_malloc`
Allocates memory of size `size` in heap and returns a 32bit pointer to the allocated memory.
Arguments:
 - `size`: UINT32 integer indicating the size of the buffer to be allocated.
- `ext_free`
Deallocates a previously allocated memory.
Arguments:
 - `addr`: 32bit pointer pointing to the allocated memory.

3.4.3 Input/Output

- `ext_print_hex`
- `ext_print_num`
- `ext_print_utf8`

3.4.4 Cryptographic auxiliary functions

- `ext_blake2_256`
- `ext_blake2_256_enumerated_trie_root`
- `ext_ed25519_verify`
- `ext_twox_128`
- `ext_twox_256`

3.4.5 Sandboxing

- `ext_sandbox_instance_tear_down`
- `ext_sandbox_instantiate`
- `ext_sandbox_invoke`
- `ext_sandbox_memory_get`
- `ext_sandbox_memory_new`
- `ext_sandbox_memory_set`

- `ext_sandbox_memory_tearardown`

3.4.6 Misc

- `ext_chain_id`

4 Network Interactions

4.1 Extrinsics Submission

Extrinsic submission is done by sending an extrinsic network message. The structure of this message is specified in Definition 12.

Upon receiving an extrinsics message, Polkadot RE decodes the transaction and calls `validate_transaction` runtime function defined in Section 3.3.4, to check the validity of the extrinsic. If `validate_transaction` considers the submitted extrinsics as a valid one, Polkadot RE, makes the extrinsics available for the consensus engine for inclusion in future blocks.

4.2 Network Messages

Definition 12. *Extrinsic submission network message:* *[Extrinsic submission network message definition]*

4.3 Block Submission and Validation

Block validation is the process, by which the client asserts that a block is fit to be added to the blockchain. This means that the block is consistent with the world state and transitions from the state of the system to a new valid state.

Blocks can be handed to the Polkadot RE both from the network stack and from consensus engine.

Both the runtime and the Polkadot RE need to work together to assure block validity. This can be accomplished by Polkadot RE invoking `execute_block` entry into the runtime as a part of the validation process.

Polkadot RE implements the following procedure to assure the validity of the block:

Algorithm 1. `IMPORT-AND-VALIDATE-BLOCK(B , $\text{Just}(B)$)`

- 1: `VERIFY-BLOCK-JUSTIFICATION(B , $\text{Just}(B)$)`
 - 2: **if** B **is** Finalized **and** $P(B)$ **is not** Finalized
 - 3: `MARK-AS-FINAL($P(B)$)`
 - 4: Verify $H_{P(B)} \in \text{Blockchain}$
 - 5: `State-Changes = Runtime(B)`
 - 6: `UPDATE-WORLD-STATE(State-Changes)`
-

For the definition of finality and finalized block see Section 6.3.

5 State Storage and the Storage Trie

For storing the state of the system, Polkadot RE implements a hash table storage where the keys are used to access each data entry state. There is no limitation neither on the size of the key nor the size of the data stored under them, besides the fact that they are byte arrays.

5.1 Accessing The System Storage

Polkadot RE implements various functions to facilitate access to the system storage for the runtime. Section 3.4 lists all of those functions. Here we define the essential ones which are also used by the Polkadot RE.

Definition 13. *The **StateRead** and **StateWrite** functions provide basic access to the State Storage:*

$$v = \text{StateRead}(k)$$

$$\text{StateWrite}(k, v)$$

where v and k are byte arrays.

To authenticate the state of the system, the stored data needs to be re-arranged and hashed in a *radix 16 tree* also known as *base-16 modified Merkle Patricia Tree*, which hereafter we will refer to as the **Trie**, in order to compute the hash of the whole state storage consistently and efficiently at any given time.

As well, a modification has been made in the storing of the nodes' hash in the Merkle Tree structure to save space on entries storing small entries.

Because the Trie is used to compute the *state root*, H_r , (see Definition 10), which is used to authenticate the validity of the state database, Polkadot RE follows a rigorous encoding algorithm to compute the values stored in the trie nodes to ensure that the computed Merkle hash, H_r , matches across clients.

5.2 The General Tree Structure

As the trie is a radix 16 tree, in this sense, each key value identifies a unique node in the tree. However, a node in a tree might or might not be associated with a key in the storage.

To identify the node corresponding to a key value, k , first we need to encode k in a uniform way:

Definition 14. *For the purpose of labeling the branches of the Trie, the key k is encoded to k_{enc} using **KeyEncode** functions:*

$$k_{\text{enc}} := (k_{\text{enc}_1}, \dots, k_{\text{enc}_{2n}}) := \text{KeyEncode}(k) \quad (1)$$

such that:

$$\text{KeyEncode}(k): \begin{cases} \mathbb{B} & \rightarrow \text{Nibbles}_4 \\ k := (b_1, \dots, b_n) & \mapsto (b_1^1, b_1^2, b_2^1, b_2^2, \dots, b_n^1, b_n^2) \\ & := (k_{\text{enc}_1}, \dots, k_{\text{enc}_{2n}}) \end{cases}$$

where Nibble_4 is the set of all nibbles of 4-bit arrays and b_i^1 and b_i^2 are 4-bit nibbles, which are the little endian representations of b_i :

$$(b_i^1, b_i^2) := (b_i \bmod 16, b_i / 16)$$

, where \bmod is the remainder and $/$ is the integer division operators.

By looking at k_{enc} as a sequence of nibbles, one can walk the radix tree to reach the node identifying the storage value of k .

5.3 The Merkle proof

To prove the consistency of the state storage across the network and its modifications efficiently, the Merkle hash of the storage trie needs to be computed rigorously.

The Merkle hash of the trie is computed recursively. As such, hash value of each node depends on the hash value of all its children and also on its value. Therefore, it suffices to define how to compute the hash value of a typical node as a function of the hash value of its children and its own value.

Definition 15. Suppose node N of storage state trie has key value k_N , and parent key value of $k_{P(N)}$, such that:

$$\text{KeyEncode}(k_N) = (k_{\text{enc}_1}, \dots, k_{\text{enc}_{i-1}}, k_{\text{enc}_i}, \dots, k_{\text{enc}_{2n}})$$

and

$$\text{KeyEncode}(k_{P(N)}) = (k_{\text{enc}_1}, \dots, k_{\text{enc}_{i-1}})$$

We define

$$\text{pk}_N := (k_{\text{enc}_i}, \dots, k_{\text{enc}_{2n}})$$

to be the **the partial key** of N .

Definition 16. For a trie node N , **Node Prefix** function is a value specifying the node type as follows:

$$\text{NodePrefix}(N) := \begin{cases} 1 & N \text{ is a leaf node} \\ 254 & N \text{ is a branch node without value} \\ 255 & N \text{ is a branch node with value} \end{cases}$$

Definition 17. For a given node N , with partial key of pk_N and Value v , the **encoded representation** of N , formally referred to as $\text{Enc}_{\text{Node}}(N)$ is determined as follows, in case which:

- N is a leaf node:

$$\text{Enc}_{\text{Node}}(N) := \text{Enc}_{\text{len}}(N) \parallel \text{HPE}(\text{pk}_N) \parallel \text{Enc}_{\text{SC}}(v)$$

- N is a branch node:

$$\begin{aligned} \text{Enc}_{\text{Node}}(N) := & \\ & \text{NodePrefix}(N) \parallel \text{ChildrenBitmap}(N) \parallel \text{HPE}_{\text{PC}}(v) \parallel \text{Enc}_{\text{SC}}(\text{Enc}_{\text{Node}}) \parallel \\ & \text{Enc}_{\text{SC}}(N_{C_1}) \dots \text{Enc}_{\text{SC}}(N_{C_n}) \end{aligned}$$

Where $N_{C_1} \dots N_{C_n}$ with $n \leq 16$ are the children nodes of N .

Definition 18. For a given node N , the **Merkle value** of N , denoted by $H(N)$ is defined as follows:

$$\begin{aligned} H: \mathbb{B} &\rightarrow \bigcup_{i=0}^{32} \mathbb{B}_i \\ H(N): &\begin{cases} \text{Enc}_{\text{Node}}(N) & \|\text{Enc}_{\text{Node}}(N)\| < 32 \\ \text{Hash}(\text{Enc}_{\text{Node}}(N)) & \|\text{Enc}_{\text{Node}}(N)\| \geq 32 \end{cases} \end{aligned}$$

6 Consensus Engine

Consensus in Polkadot RE is achieved during the execution of two different procedures. The first procedure is block production and the second is finality. Polkadot RE must run these procedures, if and only if it is running on a validator node.

6.1 Block Tree

In the course of formation of a (distributed) blockchain, it is possible that the chain forks into multiple sub chains in various block positions. We refer to this structure as a *block tree*:

Definition 19. *The **Block Tree** of a blockchain is the union of all different versions of the blockchain observed by all the nodes in the system such as every such block is a node in the graph and B_1 is connected to B_2 if B_1 is a parent of B_2 .*

Because every block in the blockchain contains a reference to its parent, it is easy to see that the block tree is actually a tree.

A block tree naturally imposes a partial order relationships on the blocks as follows:

Definition 20. *We say B is **descendant of B'** , formally noted as $B > B'$ if B is a descendent of B' in the block tree.*

6.2 Block Production

6.3 Finality

Polkadot RE uses GRANDPA Finality protocol [?] to finalize blocks. Finality is obtained by consecutive rounds of voting by validator nodes. Validators execute GRANDPA finality process in parallel to Block Production as an independent service. In this section, we describe the different functions that GRANDPA service is supposed to perform to successfully participate in the block finalization process.

6.3.1 Preliminaries

Definition 21. *A **GRANDPA Voter**, v , is represented by a key pair $(k_v^{\text{pr}}, v_{\text{id}})$ where k_v^{pr} represents its private key which is a ED25519 private key, is a node running GRANDPA protocol, and broadcasts votes to finalize blocks in a Polkadot RE - based chain. The **set of all GRANDPA voters** is indicated by \mathbb{V} . For a given block B , we have*

$$\mathbb{V}_B = \text{authorities}(B)$$

where **authorities** is the entry into runtime described in Section 3.3.2.

Definition 22. ***GRANDPA state**, GS , is defined as*

$$\text{GS} := \{\mathbb{V}, \text{id}_{\mathbb{V}}, r\}$$

where:

\mathbb{V} : is the set of voters.

$\text{id}_{\mathbb{V}}$: is an incremental counter tracking membership, which changes in V .

r : is the voting round number.

Now we need to define how Polkadot RE counts the number of votes for block B . First a vote is defined as:

Definition 23. A **GRANDPA vote** or simply a vote for block B is an ordered pair defined as

$$V(B) := (H_h(B), H_i(B))$$

where $H_h(B)$ and $H_i(B)$ are block hash and block number defined in Definitions 10 and 11 respectively.

Definition 24. Voters engage in a maximum two sub-rounds of voting for each round r . The first sub-round is called **pre-vote** and the second sub-round is called **pre-commit**.

By $V_v^{r, \text{pv}}$ and $V_v^{r, \text{pc}}$ we refer to the vote casted by voter v in round r (for block B) during the pre-vote and the pre-commit sub-round respectively.

The GRANDPA protocol dictates how an honest voter should vote in each sub-round, which is described in Algorithm 3. After defining what constitutes a vote in GRANDPA, we define how GRANDPA counts votes.

Definition 25. Voter v **equivocates** if they broadcast two or more valid votes to blocks not residing on the same branch of the block tree during one voting sub-round. In such a situation, we say that v is an **equivocator** and any vote $V_v^{r, \text{stage}}(B)$ casted by v in that round is an **equivacatory vote** and

$$\mathcal{E}^{r, \text{stage}}$$

represents the set of all equivocators voters in sub-round “stage” of round r . When we want to refer to the number of equivocators whose equivocation has been observed by voter v we refer to it by:

$$\mathcal{E}_{\text{obs}(v)}^{r, \text{stage}}$$

Definition 26. A vote $V_v^{r, \text{stage}} = V(B)$ is **invalid** if

- $H(B)$ does not correspond to a valid block;
- B is not an (eventual) descendent of a previously finalized block;
- $M_v^{r, \text{stage}}$ does not bear a valid signature;
- id_V does not match the current V ;
- If $V_v^{r, \text{stage}}$ is an equivacatory vote.

Definition 27. For validator v , the set of observed direct votes for Block B in round r , formally denoted by $\text{VD}_{\text{obs}(v)}^{r, \text{stage}}(B)$ is equal to the union of:

- set of valid votes $V_{v_i}^{r, \text{stage}}$ casted in round r and received by v such that $V_{v_i}^{r, \text{stage}} = V(B)$.

Definition 28. We refer to the set of total votes observed by voter v in sub-round “stage” of round r by $V_{\text{obs}(v)}^{r, \text{stage}}$.

The set of all observed votes by v in the sub-round stage of round r for block B , $V_{\text{obs}(v)}^{r, \text{stage}}(B)$ is equal to all of the observed direct votes casted for block B and all of the B ’s descendents defined formally as:

$$V_{\text{obs}(v)}^{r, \text{stage}}(B) := \bigcup_{v_i \in V, B \geq B'} \text{VD}_{\text{obs}(v)}^{r, \text{stage}}(B')$$

The **total number of observed votes for Block B in round r** is defined to be the size of that set plus the total number of equivocators voters:

$$\#V_{\text{obs}(v)}^{r,\text{stage}}(B) = |V_{\text{obs}(v)}^{r,\text{stage}}(B)| + |\mathcal{E}_{\text{obs}(v)}^{r,\text{stage}}|$$

Definition 29. The current **pre-voted** block $B_v^{r,\text{pv}}$ is the block with

$$H_n(B_v^{r,\text{pv}}) = \text{Max}(H_n(B) \mid \forall B: \#V_{\text{obs}(v)}^{r,\text{pv}}(B) \geq 2/3|\mathbb{V}|)$$

Note that for genesis block Genesis we always have $\#V_{\text{obs}(v)}^{r,\text{pv}}(B) = |\mathbb{V}|$.

Finally we define when a voter v see a round as completable, that is when they are confident that $B_v^{r,\text{pv}}$ is an upper bound for what is going to be finalised in this round.

Definition 30. We say that round r is **completable** if $|V_{\text{obs}(v)}^{r,\text{pc}}| + \mathcal{E}_{\text{obs}(v)}^{r,\text{pc}} > \frac{2}{3}|\mathbb{V}|$ and for all $B' > B_v^{r,\text{pv}}$:

$$|V_{\text{obs}(v)}^{r,\text{pc}}| - \mathcal{E}_{\text{obs}(v)}^{r,\text{pc}} - |V_{\text{obs}(v)}^{r,\text{pc}}(B')| > \frac{2}{3}|\mathbb{V}|$$

Note that in practice we only need to check the inequality for those $B' > B_v^{r,\text{pv}}$ where $|V_{\text{obs}(v)}^{r,\text{pc}}(B')| > 0$.

6.3.2 Voting Messages Specification

Voting is done by means of broadcasting voting messages to the network. Validators inform their peers about the block finalized in round r by broadcasting a finalization message (see Algorithm 3 for more details). These messages are specified in this section.

Definition 31. A vote casted by voter v should be broadcasted as a **message** $M_v^{r,\text{stage}}$ to the network by voter v with the following structure:

$$M_v^{r,\text{stage}} := \text{EncSC}(r, \text{id}_{\mathbb{V}}, \text{EncSC}(\text{stage}, V_v^{r,\text{stage}}, \text{Sig}_{\text{ED25519}}(\text{EncSC}(\text{stage}, V_v^{r,\text{stage}}, r, V_{\text{id}}), v_{\text{id}}))$$

Where:

r :	round number	64 bit integer
V_{id} :	incremental change tracker counter	64 bit integer
v_{id} :	Ed25519 public key of v	4 byte array
stage:	0 if it is the pre-vote sub-round 1 if it the pre-commit sub-round	1 byte

Definition 32. The **justification for block B in round r** of GRANDPA protocol defined $J^r(B)$ is a vector of pairs of the type:

$$(V(B'), (\text{Sign}_{v_i}^{r,\text{pc}}(B'), v_{\text{id}}))$$

in which either

$$B' > B$$

or $V_{v_i}^{r,\text{pc}}(B')$ is an equivocatory vote.

In all cases $\text{Sign}_{v_i}^{r,\text{pc}}(B')$ is the signature of voter v_i broadcasted during the pre-commit sub-round of round r .

Definition 33. GRANDPA *finalizing message for block B in round r* represented as $M_v^{r, \text{Fin}}(B)$ is a message broadcasted by voter v to the network indicating that voter v has finalized block B in round r . It has the following structure:

$$M_v^{r, \text{Fin}}(B) := \text{Enc}_{\text{SC}}(r, V(B), J^r(B))$$

in which $J^r(B)$ is the justification defined in Definition 32.

6.3.3 Initiating the GRANDPA State

A validator needs to initiate its state and sync it with other validators, to be able to participate coherently in the voting process. In particular, considering that voting is happening in different rounds and each round of voting is assigned a unique sequential round number r_v , it needs to determine and set its round counter r in accordance with the current voting round r_n , which is currently undergoing in the network.

As instructed in Algorithm 2, whenever the membership of GRANDPA voters changes, r is set to 0 and V_{id} needs to be incremented.

Algorithm 2. JOIN-LEAVE-GRANDPA-VOTERS (\mathcal{V})

- 1: $r \leftarrow 0$
 - 2: $\mathcal{V}_{\text{id}} \leftarrow \text{ReadState}(\text{'AUTHORITY_SET_KEY'})$
 - 3: $\mathcal{V}_{\text{id}} \leftarrow \mathcal{V}_{\text{id}} + 1$
 - 4: EXECUTE-ONE-GRANDPA-ROUND(r)
-

Each voter should run Algorithm 2 to verify that a round is completable.

6.3.4 Voting Process in Round r

For each round r , an honest voter v must participate in the voting process by following Algorithm 3.

Algorithm 3. PLAY-GRANDPA-ROUND(r)

- 1: $t_{r,v} \leftarrow \text{Time}$
 - 2: $\text{primary} \leftarrow \text{DERIVE-PRIMARY}$
 - 3: **if** $v = \text{primary}$
 - 4: BROADCAST($M_v^{r-1, \text{Fin}}(\text{BEST-FINAL-CANDIDATE}(r-1))$)
 - 5: RECEIVE-MESSAGES(**until** $\text{Time} \geq t_{r,v} + 2 \times T$ **or** r **is completable**)
 - 6: $L \leftarrow \text{BEST-FINAL-CANDIDATE}(r-1)$
 - 7: **if** RECEIVED($M_{v_{\text{primary}}}^{r, \text{PV}}(B)$) **and** $B_v^{r, \text{PV}} \geq B > L$
 - 8: $N \leftarrow B$
 - 9: **else**
 - 10: $N \leftarrow B': H_n(B') = \max \{H_n(B'): B' > L\}$
 - 11: BROADCAST($M_v^{r, \text{PV}}(N)$)
 - 12: RECEIVE-MESSAGES(**until** $B_v^{r, \text{PV}} \geq L$ **and** ($\text{Time} \geq t_{r,v} + 4 \times T$ **or** r **is completable**))
 - 13: BROADCAST($M_v^{r, \text{PC}}(B_v^{r, \text{PV}})$)
 - 14: PLAY-GRANDPA-ROUND($r + 1$)
-

Algorithm 4. BEST-FINAL-CANDIDATE(r)

```

1:  $\mathcal{C} \leftarrow \{B' \mid B' \leq B_v^{r,\text{PV}}: |V_v^{r,\text{PC}}| - \#V_v^{r,\text{PC}}(B') \leq 1/3|\mathbb{V}|\}$ 
2: if  $\mathcal{C} = \phi$ 
3:   return  $\phi$ 
4: else
5:   return  $E \in \mathcal{C}: H_n(E) = \max \{H_n(B'): B' \in \mathcal{C}\}$ 

```

Algorithm 5. ATTEMPT-TO-FINALIZE-ROUND(r)

```

1:  $L \leftarrow \text{LAST-FINALIZED-BLOCK}$ 
2:  $E \leftarrow \text{BEST-FINAL-CANDIDATE}(r)$ 
3: if  $E \geq L$  and  $V_{\text{obs}(v)}^{r-1,\text{PC}}(E) > 2/3|\mathcal{V}|$ 
4:    $\text{LAST-FINALIZED-BLOCK} \leftarrow B^{r,\text{PC}}$ 
5:   if  $M_v^{r,\text{Fin}}(E) \notin \text{RECEIVED-MESSAGES}$ 
6:      $\text{BROADCAST}(M_v^{r,\text{Fin}}(E))$ 
7:   return
8: schedule-call ATTEMPT-TO-FINALIZE-ROUND( $r$ ) when RECEIVE-MESSAGES

```

7 Auxiliary Encodings

7.1 SCALE Codec

Polkadot RE uses *Simple Concatenated Aggregate Little-Endian* (*SCALE*) codec to encode byte arrays that provide canonical encoding and to produce consistent hash values across their implementation, including the Merkle hash proof for the State Storage.

Definition 34. The *SCALE* codec for *Byte array* A such that

$$A := b_1 b_2 \dots b_n$$

such that $n < 2^{536}$ is a byte array referred to $\text{Enc}_{\text{SC}}(A)$ and defined as follows:

$$\text{Enc}_{\text{SC}}(A) := \begin{cases} l_1 b_1 b_2 \dots b_n & 0 \leq n < 2^6 \\ i_1 i_2 b_1 \dots b_n & 2^6 \leq n < 2^{14} \\ j_1 j_2 j_3 b_1 \dots b_n & 2^{14} \leq n < 2^{30} \\ k_1 k_2 \dots k_m b_1 \dots b_n & 2^{14} \leq n \end{cases}$$

in which:

$l_1^1 l_1^0 = 00$
$i_1^1 i_1^0 = 01$
$j_1^1 j_1^0 = 10$
$k_1^1 k_1^0 = 11$

and n is stored in $\text{Enc}_{\text{SC}}(A)$ in little-endian format in base-2 as follows:

$$n = \begin{cases} l_1^7 \dots l_1^3 l_1^2 & n < 2^6 \\ i_2^7 \dots i_2^0 i_1^7 \dots i_1^2 & 2^6 \leq n < 2^{14} \\ j_4^7 \dots j_4^0 j_3^7 \dots j_1^7 \dots j_1^2 & 2^{14} \leq n < 2^{30} \\ k_2 + k_3 2^8 + k_4 2^{2 \cdot 8} + \dots + k_m 2^{(m-2)8} & 2^{30} \leq n \end{cases}$$

where:

$$m = l_1^7 \dots l_1^3 l_1^2 + 4$$

Definition 35. The **SCALE** codec for **Tuple** T such that:

$$T := (A_1, \dots, A_n)$$

Where A_i 's are values of different types, is defined as:

$$\text{Enc}_{\text{SC}}(T) := \text{Enc}_{\text{SC}}(A_1) | \text{Enc}_{\text{SC}}(A_2) | \dots | \text{Enc}_{\text{SC}}(A_n)$$

7.2 Hex Encoding

Practically, it is more convenient and efficient to store and process data which is stored in a byte array. On the other hand, radix-16 tree keys are broken in 4-bits nibbles. Accordingly, we need a method to encode sequences of 4-bits nibbles into byte arrays canonically:

Definition 36. Suppose that $\text{PK} = (k_1, \dots, k_n)$ is a sequence of nibbles, then

$$\text{Enc}_{\text{HE}}(\text{PK}) :=$$

$$\begin{cases} \text{Nibbles}_4 & \rightarrow \mathbb{B} \\ \text{PK} = (k_1, \dots, k_n) & \mapsto \begin{cases} (0, k_1 + 16 k_2, \dots, k_{2i-1} + 16 k_{2i}) & n = 2i \\ (k_1, k_2 + 16 k_3, \dots, k_{2i} + 16 k_{2i+1}) & n = 2i + 1 \end{cases} \end{cases}$$

7.3 Partial Key Encoding

Definition 37. Let N be a node in the storage state trie with Partial Key PK_N . We define the **Partial key length encoding** function, formally referred to as $\text{Enc}_{\text{len}}(N)$ as follows:

$$\begin{aligned} & \text{Enc}_{\text{len}}(N) & & := \\ & \text{NodePrefix}(N) & & + \\ & \begin{cases} (\|\text{PK}_N\|) & \text{NisleafNode} \quad \& \quad \|\text{PK}_N\| < 127 \\ (127) \|(\text{LE}(\|\text{PK}_N\| - 127))\| & \text{NisleafNode} \quad \& \quad \|\text{PK}_N\| \geq 127 \end{cases} \end{aligned}$$

where NodePrefix function is defined in Definition 16.

8 Genesis Block Specification

9 Predefined Storage keys

10 Runtime upgrade