Polkadot Runtime Specification Glossary

Web3 Foundation

February 2020

Basics

Symbol	Description	Defined
b	a sequence of bytes of length n	$b := (b_0, b_1, ..., b_{n-1})$ such that $0 \leq b_i \leq 255$
$\mathbb{B}_n$	the set of all byte arrays of length n	$\mathbb{B} := \bigcup_{i=0}^{\infty} \mathbb{B}_i$
I	little-endian representation of a non-negative integer	$I = (B_n...B_0)_{256}$
B	byte array	$B = (b_0, b_1, ..., b_n)$ such that $b_1 := B_i$
C	a blockchain is a directed path graph. Each node of the graph is called Block and indicated by B	
$P(B)$	the parent of block B	$B_{n+1} := P(B_n)$
$\mathcal{N}$	the set of the nodes of the Polkadot state trie	
N	an individual node in the trie	$N \in \mathcal{N}$
$\mathcal{N}_b$	a branch node which has one child or more (max 16)	$\mathcal{N}_b := \{N \in \mathcal{N} \mid N is a branch node\}$
$\mathcal{N}_l$	a leaf node is a childless node	$\mathcal{N}_l := \{N \in \mathcal{N} \mid N is a leaf node\}$
pk_N	TODO	
pk_N^{Agr}	TODO	
$HeadN$	the node header of node N	
v_N	the node value which is stored by the node $N \in \mathcal{N}$	$v_N := Head_N \parallel Enc_{HE}(pk_N) \parallel SV_N$

Block Format

Symbol	Description	Defined
H_p	the 32-byte Blake2b hash of the header of the parent of the block	

SCALE Codec

Symbol	Description	Defined
A	Byte array	$A := b_1, b_2, ...b_n$
T	Tuple where A_i 's are values of different types	$T := (A_1, ..., A_n)$
S	Sequence where Ai 's are values of the same type (and the decoder is unable to infer value of n from the context)	$S := A_1, ..., A_n$
τ	Varying data type (TODO)	$T = \{T_1, ..., T_n\}$
$Enc_{SC}(A)$	SCALE encoding of byte array A such that $n < 2^{256}$	$Enc_{SC}(A) := Enc_{SC}^{Len}(\parallel A \parallel) \parallel A$
$Enc_{SC}(T)$	SCALE encoding of tuple T	$Enc_{SC}(T) := Enc_{SC}(A_1) \parallel Enc_{SC}(A_2) \parallel ... \parallel Enc_{SC}(A_n)$
$Enc_{SC}(S)$	SCALE encoding of sequence S	$Enc_{SC}(S) := Enc_{SC}^{Len}(\parallel S \parallel) Enc_{SC}(A_1) \mid Enc_{SC}(A_2) \mid ... \mid Enc_{SC}(A_n)$

GRANDPA

Symbol	Description	Defined
v	GRANDPA Voter	
k_v^{pr}	ED25519 private key of v	
v_{id}	ED25519 public key of v	
$\mathbb{V}$	set of all GRANDPA voters	
$\mathbb{V}_B$	set of all GRANDPA voters for a given block	
$\mathbb{V}_{id}$	is an incremental counter tracking membership, which changes in V	
GS	GRANDPA state	$GS := \{\mathbb{V}, id_{\mathbb{V}}, r\}$
$V(B)$	GRANDPA vote	$V(B) := (H_h(B), H - I(B))$
$V_v^{r,pv}$	pre-vote	
$V_v^{r,pc}$	pre-commit	
r	Voting round number	
V_id	Incremental counter tracking membership	
$V_v^{r,stage}(B)$	equivocatory vote	
$\mathcal{E}^{r,stage}$	set of all equivocators voters in sub-round "stage" of round r	
$\mathcal{E}_{obs(v)}^{r,stage}$	set of all equivocators voters in sub-round "stage" of round r observed by voter v	
$VD_{obs(v)(B)}^{r,stage}$	the set of observed direct votes for block B in round r	
$V_{obs(v)}^{r,stage}$	the set of total votes observed by voter v in sub-round "stage" of round r	
$V_{obs(v)}^{r,stage}(B)$	set of all observed votes by v in the sub-round stage of round r for block B	$V_{obs(v)}^{r,stage}(B) := \bigcup_{v \in \mathbb{V}, B \geq B'} VD_{obs(v)}^{r,stage}(B')$

Symbol	Description	Defined
$M_v^{r,stage}$	A broadcasted message by the voter v casting his vote to the network	$M_v^{r,stage} :=$ $Enc_{SC}(r, id_{\mathbb{V}}, Enc_{SC}(stage, V_v^{r,stage}, Sig_{ED25519}(Enc_{SC}(stage, V_v^{r,stage}, r, V_{id}), v_{id})))$
$J^r(B)$	The justification for block B in round r	The justification is a vector of pairs of the type $(V(B'), (Sign_{vi}^{r,pc}(B'), v_{id}))$ in which either $B' \geq B$ or $V_{vi}^{r,pc}(B')$ is an equivocatory vote
$Sign_{vi}^{r,pc}(B')$	The signature of voter v , broadcasted during the pre-commit sub-round of round r	
$M_v^{r,Fin}(B)$	The finalizing message broadcasted by voter v to the network indicating that voter v has finalized bock B in round r	$M_v^{r,Fin}(B) := Enc_{SC}(r, V(B), J^r(B))$

Cryptographic keys

Symbol	Description	Defined
Account key (sk^a, pk^a)	A keypair of type of either SR25519, ED25519, secp256k1	

Hex encoding

Symbol	Description	Defined
Account key (sk^a, pk^a)	A keypair of type of either SR25519, ED25519, secp256k1	