

Name	Description
<b>High level constructs</b>	
$\sigma_t$	World-state at time $t$ .
$T$	An Ethereum transaction
$T_0, T_1, \dots$	Individual transactions within a block
$B$	A block: $B \equiv (\dots, (T_0, T_1, \dots))$
$\Upsilon$	The Ethereum state transition function: $\sigma_{t+1} \equiv \Upsilon(\sigma_t, T)$
$\Omega$	The block-finalisation state transition function (pays out the mining reward).
$\Pi$	The block-level state-transition function: $\Pi(\sigma, B) \equiv \Omega(B, \Upsilon(\Upsilon(\sigma, T_0), T_1) \dots)$
$\mu$	Machine-state tuple, $(g, pc, \mathbf{m}, i, \mathbf{s})$ , which are gas, program counter, memory, memory size, stack.
<b>World state</b>	
$\sigma[a]_n$	The nonce of account $a$ .
$\sigma[a]_b$	The balance of account $a$ .
$\sigma[a]_s$	A 256-bit hash of the root node of a Merkle Patricia tree that encodes the storage contents of account $a$ . Note that $\text{TRIE}(L_I^*(\sigma[a]_s)) \equiv \sigma[a]_s$
$\sigma[a]_c$	The hash of the EVM code of account $a$ .
<b>Machine state</b>	
$\mu_g$	The gas available.
$\mu_{pc}$	The program counter.
$\mu_{\mathbf{m}}$	The memory contents.
$\mu_i$	The number of memory words allocated.
$\mu_{\mathbf{s}}$	The stack.
$\mu_{\mathbf{s}}[n]$	Item at stack depth $n$ .
<b>Substate</b>	
$A$	A Transaction substate during execution: $\equiv (A_{\mathbf{s}}, A_{\mathbf{l}}, A_r)$ .
$A_{\mathbf{s}}$	The self-destruct set.
$A_{\mathbf{l}}$	The log series.
$A_r$	The gas refund balance. Can partially offset execution costs.
$A^0$	The empty substate: $A^0 \equiv (\emptyset, (), 0)$ .
<b>Execution environment</b>	
$I_a$	The address of the account which owns the code that is executing.
$I_o$	The sender address of the transaction that originated this execution.
$I_p$	The price of gas in the transaction that originated this execution.
$I_{\mathbf{d}}$	The byte array that is the input data to this execution; if the execution agent is a transaction, this would be the transaction data.
$I_s$	The address of the account which caused the code to be executing; if the execution agent is a transaction, this would be the transaction sender.
$I_v$	The value, in Wei, passed to this account as part of the same procedure as execution; if the execution agent is a transaction, this would be the transaction value.
$I_{\mathbf{b}}$	The byte array that is the machine code to be executed.
$I_H$	The block header of the present block.
$I_e$	The depth of the present message-call or contract-creation (i.e. the number of CALLs or CREATEs being executed at present).
<b>Blocks</b>	
$B$	A block: $B \equiv (B_H, B_{\mathbf{T}}, B_{\mathbf{U}})$ .
$B_H$	The block's header.
$B_{\mathbf{T}}$	The block's transactions.
$B_{\mathbf{U}}$	Headers of ommer/uncle blocks of this block.
$B_{\mathbf{R}}$	Transaction receipts.

Name	Description
Block header	
$H_p$	<b>parentHash</b> The Keccak 256-bit hash of the parent block's header, in its entirety.
$H_o$	<b>ommersHash</b> The Keccak 256-bit hash of the ommers list portion of this block.
$H_c$	<b>beneficiary</b> The 160-bit address to which all fees collected from the successful mining of this block be transferred.
$H_r$	<b>stateRoot</b> The Keccak 256-bit hash of the root node of the state trie, after all transactions are executed and finalisations applied.
$H_t$	<b>transactionsRoot</b> The Keccak 256-bit hash of the root node of the trie structure populated with each transaction in the transactions list portion of the block.
$H_e$	<b>receiptsRoot</b> The Keccak 256-bit hash of the root node of the trie structure populated with the receipts of each transaction in the transactions list portion of the block.
$H_b$	<b>logsBloom</b> The Bloom filter composed from indexable information (logger address and log topics) contained in each log entry from the receipt of each transaction in the transactions list.
$H_d$	<b>difficulty</b> A scalar value corresponding to the difficulty level of this block.
$H_i$	<b>number</b> A scalar value equal to the number of ancestor blocks. The genesis block has a number of zero.
$H_l$	<b>gasLimit</b> A scalar value equal to the current limit of gas expenditure per block.
$H_g$	<b>gasUsed</b> A scalar value equal to the total gas used in transactions in this block.
$H_s$	<b>timestamp</b> A scalar value equal to the reasonable output of Unix's time() at this block's inception.
$H_x$	<b>extraData</b> An arbitrary byte array containing data relevant to this block. This must be 32 bytes or fewer.
$H_m$	<b>mixHash</b> A 256-bit hash which proves combined with the nonce that a sufficient amount of computation has been carried out on this block.
$H_n$	<b>nonce</b> A 64-bit hash which proves combined with the mix-hash that a sufficient amount of computation has been carried out on this block.
$V(H)$	The block header validity function.

### Transactions

$T_n$	Transaction nonce.
$T_p$	Gas price for the transaction.
$T_g$	The maximum gas for a transaction.
$T_t$	The "to" address for the transaction.
$T_v$	The value to be transferred by the transaction.
$T_w, T_r, T_s$	The $v, r, s$ values of the transaction signature.
$T_i$	EVM-code for account initialisation (i.e. contract deployment).
$T_d$	Input data of a message call.
$S(T)$	The sender address of a transaction.

### Transaction Receipt

$R$	A transaction receipt: $R \equiv (R_\sigma, R_u, R_b, R_l)$
$R_\sigma$	The post-transaction state.
$R_u$	The cumulative gas used so far in the block.
$R_b$	The bloom filter composed from the information in the transaction logs.
$R_l$	The log entries created by the transaction, $(O_0, O_1, \dots)$ .
$O$	A log entry: $O \equiv (O_a, (O_{t0}, O_{t1}, \dots), O_d)$ .
$O_a$	The logger's address.
$O_t$	A 32-byte log topic.
$O_d$	The log data for this entry.

### Misc functions

$\ell(\mathbf{x})$	The last item in sequence $\mathbf{x}$ : $\ell(\mathbf{x}) \equiv \mathbf{x}[\ \mathbf{x}\  - 1]$
$M(s, f, l)$	Memory expansion function. $s$ is the current top of memory; $f$ is the start of writing; $l$ is the number of bytes to be written.
$L(n)$	The "all but one 64th" function: $L(n) \equiv n - \lfloor n/64 \rfloor$ .
$L_I((k, v))$	Representation of key-value pairs in the trie: $L_I((k, v)) \equiv (\text{KEC}(k), \text{RLP}(v))$

Name	Description
$S(T)$	Sender function—recovers the sender address from the transaction: $S(T) \equiv \mathcal{B}_{96..255}(\text{KEC}(\text{ECDSARECOVER}(h(T), T_w, T_r, T_s)))$ .
<b>Conventions</b>	
$\square$	A placeholder in the following; the ‘input’ value.
$\square'$	A modified and utilisable value.
$\square^*, \square^{**}$	Intermediate values.
$f^*$	An element-wise version of a function $f$ that maps between sequences.
<b>Todo</b>	
$\mathbf{b}$	The code associated with an account. $\text{KEC}(\mathbf{b}) = \sigma[a]_c$ .
$L_R$	Eqn 19
$L_S$	Eqn 19
$L_T$	Eqn 13
$V(H)$	Block header validity Eqn 48.
$\Xi$	Code execution function.
<i>etc.</i>	