ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER

BYZANTIUM VERSION e0c3b5d - 2018-04-19

DR. GAVIN WOOD
FOUNDER, ETHEREUM & PARITY
GAVIN@PARITY.IO

ABSTRACT. The blockchain paradigm when coupled with cryptographically-secured transactions has demonstrated its utility through a number of projects, with Bitcoin being one of the most notable ones. Each such project can be seen as a simple application on a decentralised, but singleton, compute resource. We can call this paradigm a transactional singleton machine with shared-state.

Ethereum implements this paradigm in a generalised manner. Furthermore it provides a plurality of such resources, each with a distinct state and operating code but able to interact through a message-passing framework with others. We discuss its design, implementation issues, the opportunities it provides and the future hurdles we envisage.

1. Introduction

With ubiquitous internet connections in most places of the world, global information transmission has become incredibly cheap. Technology-rooted movements like Bitcoin have demonstrated through the power of the default, consensus mechanisms, and voluntary respect of the social contract, that it is possible to use the internet to make a decentralised value-transfer system that can be shared across the world and virtually free to use. This system can be said to be a very specialised version of a cryptographically secure, transaction-based state machine. Follow-up systems such as Namecoin adapted this original “currency application” of the technology into other applications albeit rather simplistic ones.

Ethereum is a project which attempts to build the generalised technology; technology on which all transaction-based state machine concepts may be built. Moreover it aims to provide to the end-developer a tightly integrated end-to-end system for building software on a hitherto unexplored compute paradigm in the mainstream: a trustful object messaging compute framework.

1.1. Driving Factors. There are many goals of this project; one key goal is to facilitate transactions between consenting individuals who would otherwise have no means to trust one another. This may be due to geographical separation, interfacing difficulty, or perhaps the incompatibility, incompetence, unwillingness, expense, uncertainty, inconvenience, or corruption of existing legal systems. By specifying a state-change system through a rich and unambiguous language, and furthermore architecting a system such that we can reasonably expect that an agreement will be thus enforced autonomously, we can provide a means to this end.

Deals in this proposed system would have several attributes not often found in the real world. The incorruptibility of judgement, often difficult to find, comes naturally from a disinterested algorithmic interpreter. Transparency, or being able to see exactly how a state or judgement came about through the transaction log and rules or instructional codes, never happens perfectly in human-based systems since natural language is necessarily vague, information is often lacking, and plain old prejudices are difficult to shake.

Overall, we wish to provide a system such that users can be guaranteed that no matter with which other individuals, systems or organisations they interact, they can do so with absolute confidence in the possible outcomes and how those outcomes might come about.

1.2. Previous Work. Buterin [2013a] first proposed the kernel of this work in late November, 2013. Though now evolved in many ways, the key functionality of a block-chain with a Turing-complete language and an effectively unlimited inter-transaction storage capability remains unchanged.

Dwork and Naor [1992] provided the first work into the usage of a cryptographic proof of computational expenditure (“proof-of-work”) as a means of transmitting a value signal over the Internet. The value signal was utilised here as a spam deterrence mechanism rather than any kind of currency, but critically demonstrated the potential for a basic data channel to carry a strong economic signal, allowing a receiver to make a physical assertion without having to rely upon trust. Back [2002] later produced a system in a similar vein.

The first example of utilising the proof-of-work as a strong economic signal to secure a currency was by Vishnumurthy et al. [2003]. In this instance, the token was used to keep peer-to-peer file trading in check, providing “consumers” with the ability to make micro-payments to “suppliers” for their services. The security model afforded by the proof-of-work was augmented with digital signatures and a ledger in order to ensure that the historical record couldn’t be corrupted and that malicious actors could not spoof payment or unjustly complain about service delivery. Five years later, Nakamoto [2008] introduced another such proof-of-work-secured value token, somewhat wider in scope. The fruits of this project, Bitcoin, became the first widely adopted global decentralised transaction ledger.

Other projects built on Bitcoin’s success; the alt-coins introduced numerous other currencies through alteration to the protocol. Some of the best known are Litecoin and Primecoin, discussed by Sprankel [2013]. Other projects sought to take the core value content mechanism of the protocol and repurpose it; Aron [2012] discusses, for example,
the Namecoin project which aims to provide a decentralised name-resolution system.

Other projects still aim to build upon the Bitcoin network itself, leveraging the large amount of value placed in the system and the vast amount of computation that goes into the consensus mechanism. The Mastercoin project, first proposed by Willett [2013], aims to build a richer protocol involving many additional high-level features on top of the Bitcoin protocol through utilisation of a number of auxiliary parts to the core protocol. The Coloured Coins project, proposed by Rosenfeld et al. [2012], takes a similar but more simplified strategy, embellishing the rules of a transaction in order to break the fungibility of Bitcoin’s base currency and allow the creation and tracking of tokens through a special “chroma-wallet”-protocol-aware piece of software. Additional work has been done in the area with discarding the decentralisation foundation; Ripple, discussed by Boutellier and Heinzen [2014], has sought to create a “federated” system for currency exchange, effectively creating a new financial clearing system. It has demonstrated that high efficiency gains can be made if the decentralisation premise is discarded. Early work on smart contracts has been done by Szabo [1997] and Miller [1997]. Around the 1990s it became clear that algorithmic enforcement of agreements could become a significant force in human cooperation. Though no specific system was proposed to implement such a system, it was proposed that the future of law would be heavily affected by such systems. In this light, Ethereum may be seen as a general implementation of such a crypto-law system.

For a list of terms used in this paper, refer to Appendix A.

2. The Blockchain Paradigm

Ethereum, taken as a whole, can be viewed as a transaction-based state machine: we begin with a genesis state and incrementally execute transactions to morph it into some final state. It is this final state which we accept as the canonical “version” of the world of Ethereum. The state can include such information as account balances, reputations, trust arrangements, data pertaining to information of the physical world; in short, anything that can currently be represented by a computer is admissible. Transactions thus represent a valid arc between two states; the ‘valid’ part is important—there exist far more invalid state changes than valid state changes. Invalid state changes might, e.g., be things such as reducing an account balance without an equal and opposite increase elsewhere. A valid state transition is one which comes about through a transaction. Formally:

\[ \sigma_{t+1} \equiv \Upsilon(\sigma_t, T) \]

where \( \Upsilon \) is the Ethereum state transition function. In Ethereum, \( \Upsilon \), together with \( \sigma \) are considerably more powerful than any existing comparable system; \( \Upsilon \) allows components to carry out arbitrary computation, while \( \sigma \) allows components to store arbitrary state between transactions.

Transactions are collated into blocks; blocks are chained together using a cryptographic hash as a means of referring. Blocks function as a journal, recording a series of transactions together with the previous block and an identifier for the final state (though do not store the final state itself—that would be far too big). They also punctuate the transaction series with incentives for nodes to mine. This incentivisation takes place as a state-transition function, adding value to a nominated account.

Mining is the process of dedicating effort (working) to bolster one series of transactions (a block) over any other potential competitor block. It is achieved thanks to a cryptographically secure proof. This scheme is known as a proof-of-work and is discussed in detail in section 11.5.

Formally, we expand to:

\[
\begin{align*}
\sigma_{t+1} & \equiv \Pi(\sigma_t, B) \\
B & \equiv (\ldots, (\Upsilon_0, T_1, \ldots)) \\
\Pi(\sigma, B) & \equiv \Omega(B, (\Upsilon(\sigma_0, T_1)\ldots))
\end{align*}
\]

Where \( \Pi \) is the block-finalisation state transition function (a function that rewards a nominated party); \( B \) is this block, which includes a series of transactions amongst some other components; and \( \Omega \) is the block-level state-transition function.

This is the basis of the blockchain paradigm, a model that forms the backbone of not only Ethereum, but all decentralised consensus-based transaction systems to date.

2.1. Value. In order to incentivise computation within the network, there needs to be an agreed method for transmitting value. To address this issue, Ethereum has an intrinsic currency, Ether, known also as ETH and sometimes referred to by the Old English ¹D. The smallest subdenomination of Ether, and thus the one in which all integer values of the currency are counted, is the Wei. One Ether is defined as being \( 10^{18} \) Wei. There exist other subdenominations of Ether:

<table>
<thead>
<tr>
<th>Multiplier</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>( 10^9 )</td>
<td>Wei</td>
</tr>
<tr>
<td>( 10^{12} )</td>
<td>Szabo</td>
</tr>
<tr>
<td>( 10^{15} )</td>
<td>Finney</td>
</tr>
<tr>
<td>( 10^{18} )</td>
<td>Ether</td>
</tr>
</tbody>
</table>

Throughout the present work, any reference to value, in the context of Ether, currency, a balance or a payment, should be assumed to be counted in Wei.

2.2. Which History? Since the system is decentralised and all parties have an opportunity to create a new block on some pre-existing block, the resultant structure is necessarily a tree of blocks. In order to form a consensus as to which path, from root (the genesis block) to leaf (the block containing the most recent transactions) through this tree structure, known as the blockchain, there must be an agreed-upon scheme. If there is ever a disagreement between nodes as to which root-to-leaf path down the block tree is the ‘best’ blockchain, then a fork occurs.

This would mean that past a given point in time (block), multiple states of the system may coexist: some nodes believing one block to contain the canonical transactions, other nodes believing some other block to be canonical, potentially containing radically different or incompatible transactions. This is to be avoided at all costs as the uncertainty that would ensue would likely kill all confidence in the entire system.

The scheme we use in order to generate consensus is a simplified version of the GHOST protocol introduced by Sompolinsky and Zohar [2013]. This process is described in detail in section 11.5.
Sometimes, a path follows a new protocol from a particular height. This document describes one version of the protocol. In order to follow back the history of a path, one must reference multiple versions of this document.

3. Conventions

We use a number of typographical conventions for the formal notation, some of which are quite particular to the present work:

- The two sets of highly structured, ‘top-level’, state values, are denoted with bold lowercase Greek letters. They fall into those of world-state, which are denoted $\sigma$ (or a variant thereupon) and those of machine-state, $\mu$.

- Functions operating on highly structured values are denoted with an upper-case Greek letter, e.g. $\mathcal{T}$, the Ethereum state transition function.

- For most functions, an uppercase letter is used, e.g. $C$, the general cost function. These may be subscripted to denote specialised variants, e.g. $C^\text{store}$, the cost function for the store operation. For specialised and possibly externally defined functions, we may format as typewriter text, e.g. the Keccak-256 hash function (as per the winning entry to the SHA-3 contest by Bertoni et al. [2017], rather than later releases), is denoted $\text{KEC}$ (and generally referred to as plain Keccak). Also $\text{KEC512}$ is referring to the Keccak 512 hash function.

- Tuples are typically denoted with an upper-case letter, e.g. $T$, is used to denote an Ethereum transaction. This symbol may, if accordingly defined, be subscripted to refer to an individual component, e.g. $T_a$; denotes the nonce of said transaction. The form of the subscript is used to denote its type; e.g. uppercase subscripts refer to tuples with subscriptable components.

- Scalars and fixed-size byte sequences (or, synonymously, arrays) are denoted with a normal lower-case letter, e.g. $n$ is used in the document to denote a transaction nonce $n$.

- Those with a particularly special meaning may be Greek, e.g. $\delta$, the number of items required on the stack for a given operation.

- Arbitrary-length sequences are typically denoted as a bold lower-case letter, e.g. $a$ is used to denote the byte sequence given as the output data of a message call. For particularly important values, a bold uppercase letter may be used.

- Throughout, we assume scalars are positive integers and thus belong to the set $\mathbb{N}$. The set of all byte sequences is $\mathbb{B}$, formally defined in Appendix B. If such a set of sequences is restricted to those of a particular length, it is denoted with a subscript, thus the set of all byte sequences of length 32 is named $\mathbb{B}_{32}$ and the set of all positive integers smaller than $2^{256}$ is named $\mathbb{N}_{256}$. This is formally defined in section 3.3.

- Square brackets are used to index into and reference individual components or subsequences of sequences, e.g. $\mu[0]$ denotes the first item on the machine’s stack. For subsequences, ellipses are used to specify the intended range, to include elements at both limits, e.g. $\mu_{[0..31]}$ denotes the first 32 items of the machine’s memory.

- In the case of the global state $\sigma$, which is a sequence of accounts, themselves tuples, the square brackets are used to reference an individual account.

- When considering variants of existing values, we follow the rule that within a given scope for definition, if we assume that the unmodified ‘input’ value be denoted by the placeholder $\Box$ then the modified and utilisable value is denoted as $\Box'$, and intermediate values would be $\Box^\ast$, $\Box^{\ast\ast}$.

When considering the use of existing functions, given a function $f$, the function $f'\delta$ denotes a similar, element-wise version of the function mapping instead between sequences. It is formally defined in section 4.3.

- We define a number of useful functions throughout. One of the more common is $\ell$, which evaluates to the last item in the given sequence:

$$\ell(x) \equiv x[|x| - 1]$$

4. Blocks, State and Transactions

Having introduced the basic concepts behind Ethereum, we will discuss the meaning of a transaction, a block and the state in more detail.

4.1. World State. The world state (state), is a mapping between addresses (160-bit identifiers) and account states (a data structure serialised as RLP, see Appendix B). Though not stored on the blockchain, it is assumed that the implementation will maintain this mapping in a modified Merkle Patricia tree (trie, see Appendix D). The trie requires a simple database backend that maintains a mapping of bytearrays to bytearrays; we name this underlying database the state database. This has a number of benefits; firstly the root node of this structure is graphically dependent on all internal data and as such its hash can be used as a secure identity for the entire system state.

- Secondly, being an immutable data structure, it allows any previous state (whose root hash is known) to be recalled by simply altering the root hash accordingly. Since we store all such root hashes in the blockchain, we are able to trivially revert to old states.

- The account state, $\sigma[a]$, comprises the following four fields:

  - nonce: A scalar value equal to the number of transactions sent from this address or, in the case of accounts with associated code, the number of contract-creations made by this account. For account of address $a$ in state $\sigma$, this would be formally denoted $\sigma[a]_\text{nonce}$.

  - balance: A scalar value equal to the number of Wei owned by this address. Formally denoted $\sigma[a]_\text{balance}$.

  - storageRoot: A 256-bit hash of the root node of a Merkle Patricia tree that encodes the storage contents of the account (a mapping between 256-bit integer values), encoded into the trie as a mapping from the Keccak 256-bit hash of the 256-bit integer keys to the RLP-encoded 256-bit integer values. The hash is formally denoted $\sigma[a]_\text{storageRoot}$.

  - codeHash: The hash of the EVM code of this account—this is the code that gets executed should this address receive a message call; it is immutable and thus, unlike all other fields, cannot be changed after construction. All such code fragments are contained in the state database under their corresponding hashes for later retrieval. This hash is...
formally denoted \( \sigma[a]_i \), and thus the code may be denoted as \( b \), given that \( RLP[b] = \sigma[a]_i \).

Since we typically wish to refer not to the trie’s root hash but to the underlying set of key/value pairs stored within, we define a convenient equivalence:

\[
\text{trie}(L_i(\sigma[a]_i)) \equiv \sigma[a]_a
\]

The collapse function for the set of key/value pairs in the trie, \( L_i \), is defined as the element-wise transformation of the base function \( L_i \), given as:

\[
L_i((k, v)) \equiv (\text{kec}(k), \text{rlp}(v))
\]

where:

\[
k \in \mathbb{B}_{32} \quad \& \quad v \in \mathbb{N}
\]

It shall be understood that \( \sigma[a]_b \) is not a ‘physical’ member of the account and does not contribute to its later serialisation.

If the codeHash field is the Keccak-256 hash of the empty string, i.e. \( \sigma[a]_n = \text{kec}() \), then the node represents a simple account, sometimes referred to as a “non-contract” account.

Thus we may define a world-state collapse function \( L_S \):

\[
L_S(\sigma) \equiv \{ p(a) : \sigma[a] \neq \emptyset \}
\]

where

\[
p(a) \equiv (\text{kec}(a), \text{rlp}((\sigma[a]_a, \sigma[a]_0, \sigma[a]_a, \sigma[a]_c)))
\]

This function, \( L_S \), is used alongside the trie function to provide a short identity (hash) of the world state. We assume:

\[
\forall a : \sigma[a] = \emptyset \quad \lor \quad (a \in \mathbb{B}_{20} \land v(\sigma[a]))
\]

where \( v \) is the account validity function:

\[
v(x) \equiv x_a \in \mathbb{N}_{256} \land x_n \in \mathbb{N}_{256} \land x_v \in \mathbb{B}_{32} \land x_s \in \mathbb{B}_{32}
\]

An account is empty when it has no code, zero nonce and zero balance:

\[
\text{empty}(\sigma, a) \equiv \sigma[a] = \text{kec}() \land \sigma[a]_n = 0 \land \sigma[a]_b = 0
\]

Even callable precompiled contracts can have an empty account state. This is because their account states do not usually contain the code describing its behavior.

An account is dead when its account state is non-existent or empty:

\[
\text{dead}(\sigma, a) \equiv \sigma[a] = \emptyset \lor \text{empty}(\sigma, a)
\]

4.2. The Transaction. A transaction (formally, \( T \)) is a single cryptographically-signed instruction constructed by an actor externally to the scope of Ethereum. While it is assumed that the ultimate external actor will be human in nature, software tools will be used in its construction and dissemination\(^1\); there are two types of transactions: those which result in message calls and those which result in \( T \)-creation. Both types specify a number of common fields:

- **nonce**: A scalar value equal to the number of transactions sent by the sender; formally \( T_n \).

- **gasPrice**: A scalar value equal to the number of Wei to be paid per unit of gas for all computation costs incurred as a result of the execution of this transaction; formally \( T_i \).

- **gasLimit**: A scalar value equal to the maximum amount of gas that should be used in executing this transaction. This is paid up-front, before any computation is done and may not be increased later; formally \( T_i \).

- **to**: The 160-bit address of the message call’s recipient or, for a contract creation transaction, \( \emptyset \), used here to denote the only member of \( B_0 \); formally \( T_t \).

- **value**: A scalar value equal to the number of Wei to be transferred to the message call’s recipient or, in the case of contract creation, as an endowment to the newly created account; formally \( T_v \).

\(^1\)Notably, such ‘tools’ could ultimately become so causally removed from their human-based initiation—or humans may become so causally-neutral—that there could be a point at which they rightly be considered autonomous agents. e.g. contracts may offer bounties to humans for being sent transactions to initiate their execution.
the RLP empty byte sequence and thus the member of \( B_0 \):

\[
T_k \in \begin{cases} \mathbb{B}_{20} & \text{if } T_k \neq \emptyset \\ \mathbb{B}_0 & \text{otherwise} \end{cases}
\]

4.3. The Block. The block in Ethereum is the collection of relevant pieces of information (known as the block header), \( H \), together with information corresponding to the comprised transactions, \( T \), and a set of other block headers \( U \) that are known to have a parent equal to the present block’s parent’s parent (such blocks are known as uncles\(^2\)). The block header contains several pieces of information:

- **parentHash**: The Keccak 256-bit hash of the parent block’s header, in its entirety; formally \( H_p \).
- **ommersHash**: The Keccak 256-bit hash of the uncles list portion of this block; formally \( H_u \).
- **beneficiary**: The 160-bit address to which all fees collected from the successful mining of this block be transferred; formally \( H_c \).
- **stateRoot**: The Keccak 256-bit hash of the root node of the state trie, after all transactions are executed and finalisations applied; formally \( H_r \).
- **transactionsRoot**: The Keccak 256-bit hash of the root node of the trie structure populated with each transaction in the transactions list portion of this block; formally \( H_t \).
- **receiptsRoot**: 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 this block; formally \( H_r \).
- **logsBloom**: 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; formally \( H_b \).
- **difficulty**: A scalar value corresponding to the difficulty level of this block. This can be calculated from the previous block’s difficulty level and the timestamp; formally \( H_d \).
- **number**: A scalar value equal to the number of ancestor blocks. The genesis block has a number of zero; formally \( H_d \).
- **gasLimit**: A scalar value equal to the current limit of gas expenditure per block; formally \( H_l \).
- **gasUsed**: A scalar value equal to the total gas used in transactions in this block; formally \( H_g \).
- **timestamp**: A scalar value equal to the reasonable output of Unix’s time() at this block’s inception; formally \( H_t \).
- **extraData**: An arbitrary array containing data relevant to this block. This must be 32 bytes or fewer; formally \( H_e \).
- **mixHash**: A 256-bit hash which, combined with the nonce, proves that a sufficient amount of computation has been carried out on this block; formally \( H_m \).

\( \text{nonce} \): A 64-bit value which, combined with the mix-hash, proves that a sufficient amount of computation has been carried out on this block; formally \( H_m \).

The other two components in the block are simply a list of outer block headers (of the same format as above), \( B_U \) and a series of the transactions, \( B_T \). Formally, we can refer to a block \( B \):

\[
B \equiv (B_H, B_T, B_U)
\]

4.3.1. Transaction Receipt. In order to encode information about a transaction concerning which it may be useful to form a zero-knowledge proof, or index and search, we encode a receipt of each transaction containing certain information from concerning its execution. Each receipt, denoted \( B_R[i] \), for the \( i \)th transaction, is placed in an index-keyed trie and the root recorded in the header as \( H_r \).

The transaction receipt, \( R \), is a tuple of four items comprising the cumulative gas used in the block containing the transaction receipt as of immediately after the transaction has happened, \( R_a \), the set of logs created through execution of the transaction, \( R_l \), and the Bloom filter composed from information in those logs, \( R_b \), and the status code of the transaction, \( R_s \):

\[
R \equiv (R_a, R_b, R_l, R_s)
\]

The function \( L_R \) trivially prepares a transaction receipt for being transformed into an RLP-serialised byte array:

\[
L_R(R) \equiv (0 \in \mathbb{B}_{256}, R_a, R_b, R_l)
\]

where \( 0 \in \mathbb{B}_{256} \) replaces the pre-transaction state root that existed in previous versions of the protocol.

We assert that the status code \( R_s \) is an integer.

\[
R_s \in \mathbb{N}
\]

We assert \( R_a \), the cumulative gas used is a positive integer and that the logs Bloom, \( R_b \), is a hash of size 2048 bits (256 bytes):

\[
R_a \in \mathbb{N} \quad \land \quad R_b \in \mathbb{B}_{256}
\]

The sequence \( R_l \) is a series of log entries, \( (O_0, O_1, \ldots) \). A log entry, \( O \), is a tuple of the logger’s address, \( O_d \), a series of 32-byte log topics, \( O_t \) and some number of bytes of data, \( O_d \):

\[
O \equiv (O_d, (O_t, O_{10}, \ldots), O_d)
\]

\[
O_d \in \mathbb{B}_{20} \quad \land \quad \forall t \in O_t : t \in \mathbb{B}_{32} \quad \land \quad O_d \in \mathbb{B}
\]

We define the Bloom filter function, \( M \), to reduce a log entry into a single 256-byte hash:

\[
M(O) \equiv \sum_{t \in (O_t) \cup O_d} (M_3 \times 2048(t))
\]

where \( M_3 \times 2048 \) is a specialised Bloom filter that sets three bits out of 2048, given an arbitrary byte sequence. It does this through taking the low-order 11 bits of each of the first three pairs of bytes in a Keccak-256 hash of the

\(^2\)ommers is a gender-neutral term to mean “sibling of parent”; see https://nonbinary.miraheze.org/wiki/Gender_neutral_language#Aunt.

\(^3\)Uncle: \( 20 \) \( \times \) \( 2048 \) = \( 2^{2048} \), and the low-order 11 bits is the modulo 2048 of the operand, which in this case is “each of the first three pairs of bytes in a Keccak-256 hash of the sequence.”
byte sequence. Formally:
\[ M_{3:2048}(x : x \in B) \equiv y : y \in B_{256} \text{ where:} \]
\[ y = (0,0,\ldots,0) \text{ except:} \]
\[ \forall i \in \{0,2,4\} : B_{0}(x,i)(y) = 1 \]
\[ m(x,i) \equiv \text{KEC}(x[i,i+1]) \text{ mod } 2048 \]
where \( B \) is the bit reference function such that \( B_{j}(x) \) equals the bit of index \( j \) (indexed from 0) in the byte array \( x \).

4.3.2. Holistic Validity. We can assert a block’s validity if and only if it satisfies several conditions: it must be internally consistent with the ommer and transaction block hashes and the given transactions \( B_{T} \) (as specified in section 11), when executed in order on the base state \( \sigma \).

4.3.3. Serialisation. The function \( L_{B} \) and \( L_{H} \) are the preparation functions for a block and block header respectively. Much like the transaction receipt preparation function \( L_{T} \), we assert the types and order of the structure for the when the RLP transformation is required:
\[ L_{H}(H) \equiv (H_{p},H_{o},H_{c},H_{i},H_{e},H_{b},H_{t},H_{m},H_{a},H_{i},H_{t},H_{i},H_{e},H_{b},H_{s},H_{m},H_{a}) \]
\[ L_{B}(B) \equiv (L_{H}(B_{H}),L_{T}(B_{T}),L_{B}(B_{B})) \]
With \( L_{T} \) and \( L_{H} \) being element-wise sequence transformations, thus:
\[ f((x_{0},x_{1},\ldots)) \equiv (f(x_{0}),f(x_{1}),\ldots) \text{ for any function } f \]
The component types are defined thus:
\[ H_{p} \in B_{32} \land H_{o} \in B_{32} \land H_{c} \in B_{32} \land H_{e} \in B_{32} \land H_{b} \in B_{256} \land H_{i} \in N \land H_{t} \in N \land H_{m} \in B_{32} \land H_{a} \in B_{8} \]
\[ \text{where } B_{n} = \{ B : B \in B \land ||B|| = n \} \]

4.3.4. Block Header Validity. We define \( P(B_{H}) \) to be the parent block of \( B \), formally:
\[ P(H) \equiv B' : \text{KEC}(\text{RLP}(B'_{H})) = H_{s} \]
The block number is the parent’s block number incremented by one:
\[ H_{i} \equiv P(H)H_{i} + 1 \]
The canonical difficulty of a block of header \( H \) is defined as \( D(H) \):
\[ D(H) \equiv \begin{cases} D_{0} & \text{if } H_{i} = 0 \\ \max(D_{0},P(H)H_{i} + x) & \text{otherwise} \end{cases} \]
where:
\[ D_{0} \equiv 131072 \]
\( H_s \) is the timestamp (in Unix’s time()) of block \( H \) and must fulfill the relation:

\[
H_s \geq P(H) H_t s
\]

This mechanism enforces a homeostasis in terms of the time between blocks; a smaller period between the last two blocks results in an increase in the difficulty level and thus additional computation required, lengthening the likely next period. Conversely, if the period is too large, the difficulty, and expected time to the next block, is reduced.

The nonce, \( H_m \), must satisfy the relations:

\[
n \leq \frac{2^{256}}{H_d} \land m = H_m
\]

with \((n, m) = \text{PoW}(H_{fr}, H_{in}, d)\).

Where \( H_{fr} \) is the new block’s header \( H \), but without the nonce and mix-hash components, \( d \) being the current DAG, a large data set needed to compute the mix-hash, and \( \text{PoW} \) is the proof-of-work function (see section 11.5): this evaluates to an array with the first item being the mix-hash, to prove that a correct DAG has been used, and the second item being a pseudo-random number cryptographically dependent on \( H \) and \( d \). Given an approximately uniform distribution in the range \([0, 2^{64}]\), the expected time to find a solution is proportional to the difficulty, \( H_d \).

This is the foundation of the security of the blockchain and is the fundamental reason why a malicious node cannot propagate newly created blocks that would otherwise overwrite (“rewrite”) history. Because the nonce must satisfy this requirement, and because its satisfaction depends on the contents of the block and in turn its composed transactions, creating new, valid, blocks is difficult and, over time, requires approximately the total compute power of the trustworthy portion of the mining peers.

Thus we are able to define the block header validity function \( V(H) \):

\[
V(H) \equiv n \leq \frac{2^{256}}{H_d} \land m = H_m \land H_d = D(H) \land H_s \leq H_t \land H_t < P(H) H_t s + \frac{P(H) H_t s}{1024} \land H_t > P(H) H_t s + \frac{P(H) H_t s}{1024} \land H_t \geq 5000 \land H_s \geq P(H) H_t s \land H_t = P(H) H_t s + 1 \land \|H_d\| \leq 32
\]

where \((n, m) = \text{PoW}(H_{fr}, H_{in}, d)\).

Noting additionally that \textit{extraData} must be at most 32 bytes.

5. Gas and Payment

In order to avoid issues of network abuse and to sidestep the inevitable questions stemming from Turing completeness, all programmable computation in Ethereum is subject to fees. The fee schedule is specified in units of gas (see Appendix G for the fees associated with various computation). Thus any given fragment of programmable computation (this includes creating contracts, making message calls, utilising and accessing account storage and executing operations on the virtual machine) has a universally agreed cost in terms of gas.

Every transaction has a specific amount of gas associated with it: \textit{gasLimit}. This is the amount of gas which is implicitly purchased from the sender’s account balance. The purchase happens at the according \textit{gasPrice}, also specified in the transaction. The transaction is considered invalid if the account balance cannot support such a purchase. It is named \textit{gasLimit} since any unused gas at the end of the transaction is refunded (at the same rate of purchase) to the sender’s account. Gas does not exist outside of the execution of a transaction. Thus for accounts with trusted code associated, a relatively high gas limit may be set and left alone.

In general, Ether used to purchase gas that is not refunded is delivered to the \textit{beneficiary} address, the address of an account typically under the control of the miner. Transactors are free to specify any \textit{gasPrice} that they wish, however miners are free to ignore transactions as they choose. A higher gas price on a transaction will therefore cost the sender more in terms of Ether and deliver a greater value to the miner and thus will more likely be selected for inclusion by more miners. Miners, in general, will choose to advertise the minimum gas price for which they will execute transactions and transactors will be free to canvas these prices in determining what gas price to offer. Since there will be a (weighted) distribution of minimum acceptable gas prices, transactors will necessarily have a trade-off to make between lowering the gas price and maximising the chance that their transaction will be mined in a timely manner.

6. Transaction Execution

The execution of a transaction is the most complex part of the Ethereum protocol: it defines the state transition function \( \text{Υ} \): It is assumed that any transactions executed first pass the initial tests of intrinsic validity. These include:

1. The transaction is well-formed RLP, with no additional trailing bytes;
2. the transaction signature is valid;
3. the transaction nonce is valid (equivalent to the sender account’s current nonce);
4. the gas limit is no smaller than the intrinsic gas, \( g_0 \), used by the transaction; and
5. the sender account balance contains at least the cost, \( v_0 \), required in up-front payment.

Formally, we consider the function \( \text{Υ} \) with \( T \) being a transaction and \( \sigma \) the state:

\[
\sigma' = \text{Υ}(\sigma, T)
\]

Thus \( \sigma' \) is the post-transactional state. We also define \( \text{Υ}^{\text{in}} \) to evaluate to the amount of gas used in the execution of a transaction, \( \text{Υ}^{\text{out}} \) to evaluate to the transaction’s accrued log items and \( \text{Υ}^{\text{state}} \) to evaluate to the status code resulting from the transaction. These will be formally defined later.

6.1. Substate. Throughout transaction execution, we accrue certain information that is acted upon immediately following the transaction. We call this \textit{transaction substate}, and represent it as \( A \), which is a tuple:

\[
A \equiv (A_s, A_1, A_2, A_e)
\]
The tuple contents include \( A_s \), the self-destruct set: a set of accounts that will be discarded following the transaction’s completion. \( A_s \) is the log series: this is a series of archived and indexable ‘checkpoints’ in VM code execution that allow for contract-calls to be easily tracked by onlookers external to the Ethereum world (such as decentralised application front-ends). \( A_s \) is the set of touched accounts, of which the empty ones are deleted at the end of a transaction. Finally there is \( A_t \), the refund balance, increased through using the \( SSTORE \) instruction in order to reset contract storage to zero from some non-zero value. Though not immediately refunded, it is allowed to partially offset the total execution costs.

We define the empty substate \( A^0 \) to have no self-destructs, no logs, no touched accounts and a zero refund balance:

\[
A^0 \equiv (\varnothing, (), \varnothing, 0)
\]

6.2. Execution. We define intrinsic gas \( g_0 \), the amount of gas this transaction requires to be paid prior to execution, as follows:

\[
g_0 \equiv \sum_{i \in T_d} \left\{ \begin{array}{ll} G_{\text{txdatazero}} & \text{if } i = 0 \\ G_{\text{txdata nonzero}} & \text{otherwise} \end{array} \right. + G_{\text{txcreate}} \text{ if } T_i = \varnothing \text{ otherwise}
\]

where \( T_i, T_d \) means the series of bytes of the transaction’s associated data and initialisation EVM-code, depending on whether the transaction is for contract-creation or message-call. \( G_{\text{txcreate}} \) is added if the transaction is contract-creating, but not if a result of EVM-code. \( G \) is fully defined in Appendix G.

The up-front cost \( v_0 \) is calculated as:

\[
v_0 \equiv T_q T_d \beta + T_q \beta
\]

The validity is determined as:

\[
S(T) \neq \varnothing \land \sigma[S(T)] \neq \varnothing \land T_0 = \sigma[S(T)]_0 \land g_0 \leq T_0 \land v_0 \leq \sigma[S(T)]_1 \land T_0 \leq B_{R} - (\beta B_R)\beta
\]

Note the final condition: the sum of the transaction’s gas limit, \( T_0 \), and the gas utilised in this block prior, given by \( \beta B_R \), must be no greater than the block’s gasLimit, \( B_R \).

The execution of a valid transaction begins with an irrevocable change made to the state: the nonce of the account of the sender, \( S(T) \), is incremented by one and the balance is reduced by part of the up-front cost, \( T_0 T_p \). The gas available for the proceeding computation, \( g \), is defined as \( T_0 - g_0 \). The computation, whether contract creation or a message call, results in an eventual state (which may legally be equivalent to the current state), the change to which is deterministic and never invalid: there can be no invalid transactions from this point.

We define the checkpoint state \( \sigma_0 \):

\[
\sigma_0 \equiv \sigma \text{ except:}
\]

\[
\sigma_0[S(T)]_0 \equiv \sigma[S(T)]_0 - T_0 T_p
\]

\[
\sigma_0[S(T)]_1 \equiv \sigma[S(T)]_1 + 1
\]

Evaluating \( \sigma_p \) from \( \sigma_0 \) depends on the transaction type; either contract creation or message call; we define the tuple of post-execution provisional state \( \sigma_p \), remaining gas \( g' \), substate \( A \) and status code \( z \):

\[
(\sigma_p, g', A, z) \equiv \left\{ \begin{array}{ll} (\Lambda_4(\sigma_0, S(T), T_0, g, T_p, T_v, T_0, 0, \top) & \text{if } T_i = \varnothing \\ \Theta_3(\sigma_0, S(T), T_v, T_0, 0, \top) & \text{otherwise} \end{array} \right.
\]

where \( g \) is the amount of gas remaining after deducting the basic amount required to pay for the existence of the transaction:

\[
g \equiv T_0 - g_0
\]

and \( T_0 \) is the original transactor, which can differ from the sender in the case of a message call or contract creation not directly triggered by a transaction but coming from the execution of EVM-code.

We note use \( \Theta_3 \) and \( \Lambda_4 \) to denote the fact that only the first four components of the functions’ values are taken; the final represents the message-call’s output value (a byte array) and is unused in the context of transaction evaluation.

After the message call or contract creation is processed, the refund counter has to be incremented for the account that were self-destructed throughout its invocation.

Then the state is finalised by determining the amount to be refunded, \( g^* \) from the remaining gas, \( g' \), plus some allowance from the refund counter, to the sender at the original rate.

\[
g^* \equiv g' + \min \left\{ \left[ \frac{T_0 - g'}{2} \right] A' \right\}
\]

The total refundable amount is the legitimately remaining gas \( g^* \), added to \( A' \); with the latter component being capped up to a maximum of half (rounded down) of the total amount used \( T_0 - g^* \). Therefore, \( g^* \) is the total gas that remains after the transaction has been executed.

The Ether for the gas is given to the miner, whose address is specified as the beneficiary of the present block \( B \). We define the pre-final state \( \sigma^* \) in terms of the provisional state \( \sigma_p \):

\[
\sigma^* \equiv \sigma_p \text{ except}
\]

\[
\sigma^*[S(T)]_0 \equiv \sigma_p[S(T)]_0 + g'T_p
\]

\[
\sigma^*[m]_0 \equiv \sigma_p[m]_0 + (T_0 - g^*)T_p
\]

\[
m \equiv B_R
\]

The final state, \( \sigma^* \), is reached after deleting all accounts that either appear in the self-destruct list or are touched and empty:

\[
\forall i \in A_s : \sigma^*[i] = \varnothing
\]

And finally, we specify \( \Upsilon^* \), the total gas used in this transaction \( T^1 \), the logs created by this transaction and
Υ, the status code of this transaction:

\[(73) \quad \Upsilon^0(\sigma, T) \equiv T_k - g^* \]

\[(74) \quad \Upsilon^1(\sigma, T) \equiv |A| \]

\[(75) \quad \Upsilon^2(\sigma, T) \equiv z \]

These are used to help define the transaction receipt and are also used later for state and nonce validation.

7. Contract Creation

There are a number of intrinsic parameters used when creating an account: sender \((s)\), original transactor \((o)\), available gas \((g)\), gas price \((p)\), endowment \((v)\), together with an arbitrary length byte array, \(i\), the initialisation EVM code, the present depth of the message-call/contract-creation stack \((e)\) and finally the permission to make modifications to the state \((w)\).

We define the creation function formally as the function \(\Lambda\), which evaluates from these values, together with the state \(\sigma\) to the tuple containing the new state, remaining gas, accrued transaction substate and an error message \((\sigma', g', A, o)\), as in section 60.

\[(76) \quad (\sigma', g', A, o) \equiv \Lambda(\sigma, s, o, g, p, v, i, e, w) \]

The address of the new account is defined as being the rightmost 160 bits of the Keccak hash of the RLP encoding of the structure containing only the sender and the account nonce. Thus we define the resultant address for the new account \(a\):

\[(77) \quad a \equiv B_{96.256}(\text{KEC}(\text{RLP}(\{s, \sigma[s]|a - 1\}))) \]

where \(\text{KEC}\) is the Keccak 256-bit hash function, \(\text{RLP}\) is the RLP encoding function, \(B_{96.256}(X)\) evaluates to a binary value containing the bits of indices in the range \([a, b]\) of the binary data \(X\), and \(\sigma[x]\) is the address state of \(x\), or \(\emptyset\) if none exists. Note we use one fewer than the sender’s nonce value; we assert that we have incremented the sender account’s nonce prior to this call, and so the value used is the sender’s nonce at the beginning of the responsible transaction or VM operation.

The account’s nonce is initially defined as one, the balance as the value passed, the storage as empty and the code hash as the Keccak 256-bit hash of the empty string; the sender’s balance is also reduced by the value passed. Thus the mutated state becomes \(\sigma^*:\)

\[(78) \quad \sigma^* \equiv \sigma\] except:

\[(79) \quad \sigma^*[a] = \begin{cases} 1, v + v', \text{TRIE}(\emptyset), \text{KEC}(\{\}) & \text{if } s[a] \neq \emptyset \land v = 0 \\ \emptyset & \text{otherwise} \end{cases} \]

\[(80) \quad \sigma^*[s] = \begin{cases} \emptyset & \text{if } \sigma[s] = \emptyset \land v = 0 \\ a^* & \text{otherwise} \end{cases} \]

\[(81) \quad a^* \equiv (\sigma[s]|a, \sigma[s]|b - v, \sigma[s], \sigma[s]|c) \]

where \(v'\) is the account’s pre-existing value, in the event it was previously in existence:

\[(82) \quad v' \equiv \begin{cases} 0 & \text{if } \sigma[a] = \emptyset \\ \sigma[a], \text{otherwise} \end{cases} \]

Finally, the account is initialised through the execution of the initialising EVM code \(i\) according to the execution model (see section 3). Code execution can effect several events that are not internal to the execution state: the account’s storage can be altered, further accounts can be created and further message calls can be made. As such, the code execution function \(\Xi\) evaluates to a tuple of the resultant state \(\sigma^*\), available gas remaining \(g^*\), the accrued substate \(A\) and the body code of the account \(o\).

\[(83) \quad (\sigma^*, g^*, A, o) \equiv \Xi(\sigma^*, g, I, \{s, a\}) \]

where \(I\) contains the parameters of the execution environment: that is:

\[(84) \quad I_s \equiv a \]

\[(85) \quad I_o \equiv o \]

\[(86) \quad I_p \equiv p \]

\[(87) \quad I_a \equiv () \]

\[(88) \quad I_s \equiv s \]

\[(89) \quad I_v \equiv v \]

\[(90) \quad I_i \equiv i \]

\[(91) \quad I_e \equiv e \]

\[(92) \quad I_w \equiv w \]

\(I_a\) evaluates to the empty tuple as there is no input data to this call. \(I_H\) has no special treatment and is determined from the blockchain.

Code execution depletes gas, and gas may not go below zero, thus execution may exit before the code has come to a natural halting state. In this (and several other) exceptional cases we say an out-of-gas (OOG) exception has occurred: The evaluated state is defined as being the empty set, \(\emptyset\), and the entire create operation should have no effect on the state, effectively leaving it as it was immediately prior to attempting the creation.

If the initialization code completes successfully, a final contract-creation cost is paid, the code-deposit cost, \(c\), proportional to the size of the created contract’s code:

\[(93) \quad c \equiv \text{G codedeposit} \times |o| \]

If there is not enough gas remaining to pay this, i.e. \(g^* < c\), then we also declare an out-of-gas exception.

The gas remaining will be zero in any such exceptional condition, i.e. if the creation was conducted as the reception of a transaction, then this doesn’t affect payment of the intrinsic cost of contract creation; it is paid regardless. However, the value of the transaction is not transferred to the aborted contract’s address when we are out-of-gas.

If such an exception does not occur, then the remaining gas is refunded to the originator and the now-altered state is allowed to persist. Thus formally, we may specify the resultant state, gas, substate and status code as \((\sigma', g', A, z)\) where:
when executing transactions, however message calls can be
initiated due to VM-code execution and in this case this
substate, message calls also have an extra component—the
depth of the message-call/contract-creation stack (c),
and gas price (g) usually the same as recipient), available gas (g),
value (v) and gas price (p) together with an arbitrary length byte
array, d, the input data of the call and finally the present
depth of the message-call/contract-creation stack (c).

Aside from evaluating to a new state and transaction
substate, message calls also have an extra component—the
output data denoted by the byte array o. This is ignored
when executing transactions, however message calls can be
initiated due to VM-code execution and in this case this
information is used.

(98) \((\sigma', g', A, z, o) \equiv \Theta(\sigma, s, o, r, c, g, p, v, \bar{v}, d, e, w)\)

Note that we need to differentiate between the value that is
to be transferred, v, from the value apparent in the
execution context, \(\bar{v}\), for the DELEGATECALL instruction.

We define \(\sigma_1\), the first transitional state as the original
state but with the value transferred from sender to
recipient:

(99) \(\sigma_1[r], s \equiv \sigma[r], s + v \land \sigma_1[s], o \equiv \sigma[s], o - v\)

unless \(s = r\).

Throughout the present work, it is assumed that if \(\sigma_1[r]\)
was originally undefined, it will be created as an account
with no code or state and zero balance and nonce. Thus
the previous equation should be taken to mean:

(100) \(\sigma_1 \equiv \sigma_1'\) except:

(101) \(\sigma_1[s] \equiv \begin{cases} o & \text{if } \sigma_1'[s] = o \land v = 0 \\ a_1 & \text{otherwise} \end{cases}\)

(102) \(a_1 \equiv (\sigma_1'[s], o, \sigma_1'[s], o - v, \sigma_1'[s], o, \sigma_1'[s], o)\)

(103) and \(\sigma_1' \equiv \sigma\) except:

(104) \(\sigma_1'[r] \equiv (0, v, \text{TRIE}(o), \text{KEC}(p)) \) \text{if } \sigma[r] = o \land v \neq 0

(105) \(\sigma_1'[r] \equiv o \) \text{if } \sigma[r] = o \land v = 0

The account’s associated code (identified as the fragment
whose Keccak hash is \(\sigma[c]\)) is executed according to
the execution model (see section 9). Just as with contract
creation, if the execution halts in an exceptional fashion
(i.e. due to an exhausted gas supply, stack underflow,
invalid jump destination or invalid instruction), then no gas
is refunded to the caller and the state is reverted to the
point immediately prior to balance transfer (i.e. \(\sigma\)).

8. Message Call

In the case of executing a message call, several parameters are required: sender (s), transaction originator (o), recipient (r), the account whose code is to be executed (c, generally the same as recipient), available gas (g), value (v) and gas price (p) together with an arbitrary length byte array, d, the input data of the call and finally the present
depth of the message-call/contract-creation stack (c).

Aside from evaluating to a new state and transaction
substate, message calls also have an extra component—the
output data denoted by the byte array o. This is ignored
when executing transactions, however message calls can be
initiated due to VM-code execution and in this case this
information is used.

(106) \(\sigma' \equiv \begin{cases} \sigma & \text{if } \sigma'' = \emptyset \\ \sigma'' & \text{otherwise} \end{cases}\)

(107) \(g' \equiv \begin{cases} 0 & \text{if } \sigma'' = \emptyset \land \text{else} \\ o = \emptyset & \text{otherwise} \end{cases}\)

(108) \((\sigma'', g'', A, o) \equiv 0\)

(109) \(I_a \equiv r\)

(110) \(I_o \equiv o\)

(111) \(I_p \equiv p\)

(112) \(I_d \equiv d\)

(113) \(I_s \equiv s\)

(114) \(I_v \equiv \bar{v}\)

(115) \(I_e \equiv e\)

(116) \(I_w \equiv w\)

(117) \(t \equiv \{s, r\}\)

(118) where
The execution model specifies the function Ξ, which can evaluate the execution environment that the execution agent must provide; these are contained in the tuple \( I \):

- \( I_a \), 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.
- \( I_d \), the byte array that is the input data to this execution; if the execution agent is a transaction, this would be the transaction data.
- \( I_v \), 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.
- \( I_b \), 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 CREATEEs being executed at present).
- \( I_w \), the permission to make modifications to the state.

The execution model defines the function \( \Xi \), which can compute the resultant state \( \sigma' \), the remaining gas \( g' \), the transaction processor or, recursively, the spawning execution environment which will deal with it separately.

9.2. Fees Overview. Fees (denominated in gas) are charged under three distinct circumstances, all three as prerequisite to the execution of an operation. The first and most common is the fee intrinsic to the computation of the operation (see Appendix \( G \)). Secondly, gas may be deducted in order to form the payment for a subordinate message call or contract creation; this forms part of the payment for CREATE, CALL and CALLCODE. Finally, gas may be paid due to an increase in the usage of the memory.

Over an account’s execution, the total fee for memory-usage payable is proportional to smallest multiple of 32 bytes that are required such that all memory indices (whether for read or write) are included in the range. This is paid for on a just-in-time basis; as such, referencing an area of memory at least 32 bytes greater than any previously indexed memory will certainly result in an additional memory usage fee. Due to this fee it is highly unlikely addresses will ever go above 32-bit bounds. That said, implementations must be able to manage this eventually.

Storage fees have a slightly nuanced behaviour—to incentivise minimisation of the use of storage (which corresponds directly to a larger state database on all nodes), the execution fee for an operation that clears an entry in the storage is not only waived, a qualified refund is given; in fact, this refund is effectively paid up-front since the initial usage of a storage location costs substantially more than normal usage.

See Appendix \( H \) for a rigorous definition of the EVM gas cost.

9.3. Execution Environment. In addition to the system state \( \sigma \), and the remaining gas for computation \( g \), there are several pieces of important information used in the execution environment that the execution agent must provide; these are contained in the tuple \( I \):

- \( I_a \), 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.
- \( I_d \), the byte array that is the input data to this execution; if the execution agent is a transaction, this would be the transaction data.
- \( I_v \), 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.
- \( I_b \), 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 CREATEEs being executed at present).
- \( I_w \), the permission to make modifications to the state.

The execution model defines the function \( \Xi \), which can compute the resultant state \( \sigma' \), the remaining gas \( g' \), the
accrued substate \( A \) and the resultant output, \( o \), given these definitions. For the present context, we will define it as:

\[
(\sigma', g', A, o) \equiv \Xi(\sigma, g, I)
\]

where we will remember that \( A \), the accrued substate is defined as the tuple of the suicides set \( s \), the log series \( l \), the touched accounts \( t \) and the refunds \( r \):

\[
A \equiv (s, l, t, r)
\]

9.4. Execution Overview. We must now define the \( \Xi \) function. In most practical implementations this will be modelled as an iterative progression of the pair comprising the full system state, \( \sigma \) and the machine state, \( \mu \). Formally, we define it recursively with a function \( X \). This uses an iterator function \( O \) (which defines the result of a single cycle of the state machine) together with functions \( Z \) which determines if the present state is an exceptional halting state of the machine and \( H \), specifying the output data of the instruction if and only if the present state is a normal halting state of the machine.

The empty sequence, denoted (\( \varepsilon \)), is not equal to the empty set, denoted \( \varnothing \); this is important when interpreting the output of \( H \), which evaluates to \( \varnothing \) when execution is to continue but a series (potentially empty) when execution should halt.

\[
\Xi(\sigma, g, I, T) \equiv (\sigma', \mu', A, o)
\]

\[
(\sigma', \mu, A, ..., o) \equiv X((\sigma, \mu, A^0, I))
\]

\[
\mu_{pc} \equiv g
\]

\[
\mu_0 \equiv 0
\]

\[
\mu_1 \equiv 0
\]

\[
\mu_2 \equiv (0, 0, ...)
\]

\[
\mu_3 \equiv (\varnothing, A, I)
\]

\[
X((\sigma, \mu, A, I)) \equiv \begin{cases} 
(\varnothing, A, I, \varnothing) & \text{if } Z(\sigma, \mu, I) \\
(\sigma', \mu', A^0, I, \varnothing) & \text{if } w = \text{REVERT} \\
O(\sigma, \mu, A, I) \cdot o & \text{if } o \neq \varnothing \\
X(O(\sigma, \mu, A, I)) & \text{otherwise}
\end{cases}
\]

where

\[
o \equiv H(\mu, I)
\]

\[
(a, b, c, d) \cdot e \equiv (a, b, c, d, e)
\]

\[
\mu' \equiv \mu \text{ except:}
\]

\[
\mu'_{g} \equiv \mu_{g} - C(\sigma, \mu, I)
\]

Note that, when we evaluate \( \Xi \), we drop the fourth element \( I' \) and extract the remaining gas \( \mu'_{g} \) from the resultant machine state \( \mu' \).

\( X \) is thus cycled (recursively here, but implementations are generally expected to use a simple iterative loop) until either \( Z \) becomes true indicating that the present state is exceptional and that the machine must be halted and any changes discarded or until \( H \) becomes a series (rather than the empty set) indicating that the machine has reached a controlled halt.

9.4.1. Machine State. The machine state \( \mu \) is defined as the tuple \((g, pc, m, i, s)\) which are the gas available, the program counter \( pc \in \mathbb{N}_{256} \), the memory contents, the active number of words in memory (counting continuously from position 0), and the stack contents. The memory contents \( \mu_{m} \) are a series of zeroes of size \( 2^{256} \).

For the case of reading, the instruction mnemonics, written in small-caps (e.g. ADD), should be interpreted as their numeric equivalents; the full table of instructions and their specifics is given in Appendix \( \mathbb{H} \).

For the purposes of defining \( Z, H \) and \( O \), we define \( w \) as the current operation to be executed:

\[
w \equiv \begin{cases} 
I_{b}[\mu_{pc}] & \text{if } \mu_{pc} \leq ||I_{b}|| \\
\text{STOP} & \text{otherwise}
\end{cases}
\]

We also assume the fixed amounts of \( \delta \) and \( \alpha \), specifying the stack items removed and added, both subscriptable on the instruction and an instruction cost function \( C \) evaluating to the full cost, in gas, of executing the given instruction.

9.4.2. Exceptional Halting. The exceptional halting function \( Z \) is defined as:

\[
Z(\sigma, \mu, I) \equiv \mu_{g} < C(\sigma, \mu, I) \quad \forall
\]

\[\mu_{w} \equiv \varnothing \quad \forall \]

\[||\mu_{w}|| < \delta_{w} \quad \forall \]

\[w = \text{JUMP} \quad \land \quad \mu_{w}[0] \notin D(I_{b}) \quad \forall \]

\[w = \text{JUMP} \quad \land \quad \mu_{w}[1] \neq 0 \quad \land \]

\[\mu_{w}[0] \notin D(I_{b}) \quad \forall \]

\[w = \text{RETURN} \quad \land \]

\[\mu_{w}[1] + \mu_{w}[2] > ||\mu_{w}|| \quad \forall \]

\[||\mu_{w}|| - \delta_{w} + \alpha_{w} > 1024 \quad \lor \quad (\neg \mu_{w} \land W(w, \mu)) \]

where

\[
W(w, \mu) \equiv w \in \{\text{CREATE, SSTORE, SELFDESTRUCT}\} \quad \lor \quad \text{LOGO} \leq w \land w \leq \text{LOG4} \quad \lor \quad w \in \{\text{CALL, CALLCODE}\} \land \mu_{w}[2] \neq 0
\]

This states that the execution is in an exceptional halting state if there is insufficient gas, if the instruction is invalid (and therefore its \( \delta \) subscript is undefined), if there are insufficient stack items, if a JUMP/JUMPI destination is invalid, the new stack size would be larger than 1024 or state modification is attempted during a static call. The astute reader will realise that this implies that no instruction can, through its execution, cause an exceptional halt.

9.4.3. Jump Destination Validity. We previously used \( D \) as the function to determine the set of valid jump destinations given the code that is being run. We define this as any position in the code occupied by a JUMPDEST instruction.

All such positions must be on valid instruction boundaries, rather than sitting in the data portion of PUSH operations and must appear within the explicitly defined portion of the code (rather than in the implicitly defined \( \text{STOP} \) operations that trail it).

Formally:

\[
D(c) \equiv D_{J}(c, 0)
\]
where:

\[
D_J(c, i) \equiv \begin{cases} 
\emptyset & \text{if } i \geq |c| \\
\{i\} \cup D_J(c, N(i, c[i])) & \text{if } c[i] = \text{JUMPDEST} \\
D_J(c, N(i, c[i])) & \text{otherwise}
\end{cases}
\]

where \( N \) is the next valid instruction position in the code, skipping the data of a PUSH instruction, if any:

\[
N(i, w) \equiv \begin{cases} 
i + w - \text{PUSH1} + 2 & \text{if } w \in \{\text{PUSH1, PUSH32}\} \\
i + 1 & \text{otherwise}
\end{cases}
\]

9.4.4. Normal Halting. The normal halting function \( H \) is defined:

\[
H(\mu, l) \equiv \begin{cases} 
H_{\text{RETURN}}(\mu) & \text{if } w \in \{\text{RETURN, REVERT}\} \\
() & \text{if } w \in \{\text{STOP, SELFDESTRUCT}\} \\
\emptyset & \text{otherwise}
\end{cases}
\]

The data-returning halt operations, \text{RETURN} and \text{REVERT}, have a special function \( H_{\text{RETURN}} \). Note also the difference between the empty sequence and the empty set as discussed here.

9.5. The Execution Cycle. Stack items are added or removed from the left-most, lower-indexed portion of the series; all other items remain unchanged:

\[
O((\sigma, \mu, A, l)) \equiv (\sigma', \mu', A', l)
\]

\[
\Delta \equiv \alpha_w - \delta_w
\]

\[
\|\mu_w\| \equiv \|\mu_w\| + \Delta
\]

\[
\forall x \in [\alpha_w, \|\mu_w\|): \mu_w[x] \equiv \mu_w[x - \Delta]
\]

The gas is reduced by the instruction’s gas cost and for most instructions, the program counter increments on each cycle, for the three exceptions, we assume a function \( J \), subscripted by one of two instructions, which evaluates to the according value:

\[
\mu'_g \equiv \mu_g - C(\sigma, \mu, l)
\]

\[
\mu'_pc \equiv \begin{cases} 
\text{JUMP}(\mu) & \text{if } w = \text{JUMP} \\
\text{JUMP}(\mu) & \text{if } w = \text{JUMP} \\
N(\mu_{pc}, w) & \text{otherwise}
\end{cases}
\]

In general, we assume the memory, self-destruct set and system state don’t change:

\[
\mu'_m \equiv \mu_m
\]

\[
\mu'_i \equiv \mu_i
\]

\[
A' \equiv A
\]

\[
\sigma' \equiv \sigma
\]

However, instructions do typically alter one or several components of these values. Altered components listed by instruction are noted in Appendix H, alongside values for \( \alpha \) and \( \delta \) and a formal description of the gas requirements.

10. Blocktree to Blockchain

The canonical blockchain is a path from root to leaf through the entire block tree. In order to have consensus over which path it is, conceptually we identify the path that has had the most computation done upon it, or, the heaviest path. Clearly one factor that helps determine the heaviest path is the block number of the leaf, equivalent to the number of blocks, not counting the unmined genesis block in the path. The longer the path, the greater the total mining effort that must have been done in order to arrive at the leaf. This is akin to existing schemes, such as that employed in Bitcoin-derived protocols.

Since a block header includes the difficulty, the header alone is enough to validate the computation done. Any block contributes toward the total computation or total difficulty of a chain.

Thus we define the total difficulty of block \( B \) recursively as:

\[
B_i \equiv B'_i + B_d
\]

\[
B' \equiv P(B_H)
\]

As such given a block \( B, B_i \) is its total difficulty, \( B' \) is its parent block and \( B_d \) is its difficulty.

11. Block Finalisation

The process of finalising a block involves four stages:

1. Validate (or, if mining, determine) ommer(s);
2. validate (or, if mining, determine) transactions;
3. apply rewards;
4. verify (or, if mining, compute a valid) state and block nonce.

11.1. Ommer Validation. The validation of an ommer header means nothing more than verifying that each ommer header is both a valid header and satisfies the relation of \( N \)-th generation ommer to the present block where \( N \leq 6 \). The maximum of ommer headers is two. Formally:

\[
\| B_U \| \leq 2 \bigwedge_{U \in B_k} \left( V(U) \land k(U, P(B_H)U, 6) \right)
\]

where \( k \) denotes the “is-kin” property:

\[
k(U, H, n) \equiv \begin{cases} 
\text{false} & \text{if } n = 0 \\
\lor k(U, P(H)U, n - 1) & \text{otherwise}
\end{cases}
\]

and \( s \) denotes the “is-sibling” property:

\[
s(U, H) \equiv \begin{cases} 
(P(H) = P(U) \land H \neq U \land U \notin B(H)U) & \text{otherwise}
\end{cases}
\]

where \( B(H) \) is the block of the corresponding header \( H \).

11.2. Transaction Validation. The given \( \text{gasUsed} \) must correspond faithfully to the transactions listed: \( B_{\text{gas}} \), the total gas used in the block, must be equal to the accumulated gas used according to the final transaction:

\[
B_{\text{gas}} = \langle \text{R} \rangle
\]
11.3. Reward Application. The application of rewards to a block involves raising the balance of the accounts of the beneficiary address of the block and each ommer by a certain amount. We raise the block’s beneficiary account by $R_{\text{block}}$; for each ommer, we raise the block’s beneficiary by an additional $\frac{1}{32}$ of the block reward and the beneficiary of the ommer gets rewarded depending on the block number. Formally we define the function $\Omega$:

$$\Omega(B, \sigma) \equiv \sigma' : \sigma' = \sigma$$

except:

$$\sigma'[U_c] = \begin{cases} \emptyset & \text{if } \sigma[U_c] = \emptyset \land R = 0 \\ \sigma'[U_c] & \text{otherwise} \end{cases}$$

11.4. State & Nonce Validation. We may now define the function, $\Gamma$; that maps a block $B$ to its initiation state:

$$\Gamma(B) \equiv \begin{cases} \sigma_{\text{root}} \equiv \sigma & \text{if } P(B_H) = \emptyset \\ \sigma_{\text{Trie}} \equiv \text{Trie}(L_S(\sigma)) = P(B_H)_{\text{Trie}} & \text{otherwise} \end{cases}$$

Here, $\text{Trie}(L_S(\sigma))$ means the hash of the root node of a trie of state $\sigma$; it is assumed that implementations will store this in the state database, which is trivial and efficient since the trie is by nature an immutable data structure. And finally we define $\Phi$, the block transition function, which maps an incomplete block $B$ to a complete block $B'$:

$$\Phi(B) \equiv B' : B' = B^*$$

except:

$$B'_n = n : x \leq 2^{256}$$

$$B'_m = m \text{ with } (x, m) = \text{PoW}(B'_n, n, d)$$

$$B' = B \text{ except: } B'_m \equiv B_{\text{block}}$$

With $d$ being a dataset as specified in appendix J.

As specified at the beginning of the present work, $\Pi$ is the state-transition function, which is defined in terms of $\Omega$; the block finalisation function and $\Upsilon$, the transaction-evaluation function, both now well-defined.

As previously detailed, $R[n]_a$, $R[n]_i$, and $R[n]_u$ are the $n$th corresponding status code, logs and cumulative gas used after each transaction ($R[n]_u$, the fourth component in the tuple, has already been defined in terms of the logs). We also define the $n$th state $\sigma[n]$, which is defined simply as the state resulting from applying the corresponding transaction to the state resulting from the previous transaction (or the block’s initial state in the case of the first such transaction):

$$\sigma'[n] = \begin{cases} \Omega(B) & \text{if } n < 0 \\ \Upsilon(\sigma[n-1], B_T[n]) & \text{otherwise} \end{cases}$$

In the case of $R[n]_u$, we take a similar approach defining each item as the gas used in evaluating the corresponding transaction summed with the previous item (or zero, if it is the first), giving us a running total:

$$R[n]_u = \begin{cases} 0 & \text{if } n < 0 \\ R[n-1]_u + R[n]_u & \text{otherwise} \end{cases}$$

For $R[n]_i$, we utilise the $\Upsilon$; function that we conveniently defined in the transaction execution function.

$$R[n]_i = \Upsilon(\sigma[n-1], B_T[n])$$

Finally, we define $\Pi$ as the new state given the block reward function $\Omega$ applied to the final transaction’s resultant state, $\Upsilon(\sigma[n])$:

$$\Pi(\sigma, B) \equiv \Pi(B, \sigma(B))$$

Thus the complete block-transition mechanism is defined, except for $\text{PoW}$, the proof-of-work function.

11.5. Mining Proof-of-Work. The mining proof-of-work (PoW) exists as a cryptographically secure nonce that proves beyond reasonable doubt that a particular amount of computation has been expended in the determination of some token value $n$. It is utilised to enforce the blockchain security by giving meaning and credence to the notion of difficulty (and, by extension, total difficulty). However, since mining new blocks comes with an attached reward, the proof-of-work not only functions to the notion of difficulty (and, by extension, total difficulty). However, since mining new blocks comes with an attached reward, the proof-of-work not only functions as a method of securing confidence that the blockchain will remain canonical into the future, but also as a wealth distribution mechanism.

For both reasons, there are two important goals of the proof-of-work function; firstly, it should be as accessible as possible to as many people as possible. The requirement of, or reward from, specialised and uncommon hardware should be minimised. This makes the distribution model as open as possible, and, ideally, makes the act of mining a simple swap from electricity to Ether at roughly the same rate for anyone around the world.

Secondly, it should not be possible to make super-linear profits, and especially not so with a high initial barrier. Such a mechanism allows a well-funded adversary to gain a troublesome amount of the network’s total mining power and as such gives them a super-linear reward (thus skewing distribution in their favour) as well as reducing the network security.

One plague of the Bitcoin world is ASICs. These are specialised pieces of compute hardware that exist only to do a single task (Smith, [1997]). In Bitcoin’s case the task is the SHA256 hash function (Courtois et al., [2014]). While ASICs exist for a proof-of-work function, both goals are placed in jeopardy. Because of this, a proof-of-work function that is ASIC-resistant (i.e. difficult or economically inefficient to implement in specialised compute hardware) has been identified as the proverbial silver bullet.
Two directions exist for ASIC resistance; firstly make it sequential memory-hard, i.e. engineer the function such that the determination of the nonce requires a lot of memory and bandwidth such that the memory cannot be used in parallel to discover multiple nonces simultaneously. The second is to make the type of computation it would need to do general-purpose; the meaning of “specialised hardware” for a general-purpose task set is, naturally, general purpose hardware and as such commodity desktop computers are likely to be pretty close to “specialised hardware” for the task. For Ethereum 1.0 we have chosen the first path.

More formally, the proof-of-work function takes the form of PoW:

\[ m = H_m \land n \leq 2^{256} \text{ with } (m, n) = \text{PoW}(H_B, H_n, d) \]

Where \( H_B \) is the new block’s header but without the nonce and mix-hash components; \( H_n \) is the nonce of the header; \( d \) is a large data set needed to compute the mixHash and \( H_d \) is the new block’s difficulty value (i.e. the block difficulty from section 10). PoW is the proof-of-work function which evaluates to an array with the first item being the mixHash and the second item being a pseudo-random number cryptographically dependent on \( H \) and \( d \). The underlying algorithm is called Ethash and is described below.

11.5.1. Ethash. Ethash is the PoW algorithm for Ethereum 1.0. It is the latest version of Dagger-Hashimoto, introduced by Buterin [2013b] and Dryja [2014], although it can no longer appropriately be called that since many of the original features of both algorithms were drastically changed with R&D from February 2015 until May 4 2015 (Jentzsch [2015]). The general route that the algorithm takes is as follows:

There exists a seed which can be computed for each block by scanning through the block headers up until that point. From the seed, one can compute a pseudorandom cache, \( J_{cacheinit} \), bytes in initial size. Light clients store the cache. From the cache, we can generate a dataset, \( J_{datastore} \), bytes in initial size, with the property that each item in the dataset depends on only a small number of items from the cache. Full clients and miners store the dataset. The dataset grows linearly with time.

Mining involves grabbing random slices of the dataset and hashing them together. Verification can be done with low memory by using the cache to regenerate the specific pieces of the dataset that you need, so you only need to store the cache. The large dataset is updated once every \( 10,000 \) blocks, so the vast majority of a miner’s effort will be reading the dataset, not making changes to it. The mentioned parameters as well as the algorithm is explained in detail in appendix J.

12. Implementing Contracts

There are several patterns of contracts engineering that allow particular useful behaviours; two of these that we will briefly discuss are data feeds and random numbers.

12.1. Data Feeds. A data feed contract is one which provides a single service: it gives access to information from the external world within Ethereum. The accuracy and timeliness of this information is not guaranteed and it is the task of a secondary contract author—the contract that utilises the data feed—to determine how much trust can be placed in any single data feed.

The general pattern involves a single contract within Ethereum which, when given a message call, replies with some timely information concerning an external phenomenon. An example might be the local temperature of New York City. This would be implemented as a contract that returned that value of some known point in storage. Of course this point in storage must be maintained with the correct such temperature, and thus the second part of the pattern would be for an external server to run an Ethereum node, and immediately on discovery of a new block, creates a new valid transaction, sent to the contract, updating said value in storage. The contract’s code would accept such updates only from the identity contained on said server.

12.2. Random Numbers. Providing random numbers within a deterministic system is, naturally, an impossible task. However, we can approximate with pseudo-random numbers by utilising data which is generally unknowable at the time of transacting. Such data might include the block’s hash, the block’s timestamp and the block’s beneficiary address. In order to make it hard for malicious miners to control those values, one should use the \( \text{BLOCKHASH} \) operation in order to use hashes of the previous 256 blocks as pseudo-random numbers. For a series of such numbers, a trivial solution would be to add some constant amount and hashing the result.

13. Future Directions

The state database won’t be forced to maintain all past state trie structures into the future. It should maintain an age for each node and eventually discard nodes that are neither recent enough nor checkpoints. Checkpoints, or a set of nodes in the database that allow a particular block’s state trie to be traversed, could be used to place a maximum limit on the amount of computation needed in order to retrieve any state throughout the blockchain.

Blockchain consolidation could be used in order to reduce the amount of blocks a client would need to download to act as a full, mining node. A compressed archive of the trie structure at given points in time (perhaps one in every 10,000th block) could be maintained by the peer network, effectively recasting the genesis block. This would reduce the amount to be downloaded to a single archive plus a hard maximum limit of blocks.

Finally, blockchain compression could perhaps be conducted: nodes in state trie that haven’t sent/received a transaction in some constant amount of blocks could be thrown out, reducing both Ether-leakage and the growth of the state database.

13.1. Scalability. Scalability remains an eternal concern. With a generalised state transition function, it becomes difficult to partition and parallelise transactions to apply the divide-and-conquer strategy. Unaddressed, the dynamic value-range of the system remains essentially fixed and as the average transaction value increases, the less valuable of them become ignored, being economically pointless to include in the main ledger. However, several strategies exist that may potentially be exploited to provide a considerably more scalable protocol.

Some form of hierarchical structure, achieved by either consolidating smaller lighter-weight chains into the main
block or building the main block through the incremental combination and adhesion (through proof-of-work) of smaller transaction sets may allow parallelisation of transaction combination and block-building. Parallelism could also come from a prioritised set of parallel blockchains, consolidating each block and with duplicate or invalid transactions thrown out accordingly.

Finally, verifiable computation, if made generally available and efficient enough, may provide a route to allow the proof-of-work to be the verification of final state.

14. Conclusion

We have introduced, discussed and formally defined the protocol of Ethereum. Through this protocol the reader may implement a node on the Ethereum network and join others in a decentralised secure social operating system. Contracts may be authored in order to algorithmically specify and autonomously enforce rules of interaction.

15. Acknowledgements

Many thanks to Aaron Buchanan for authoring the Homestead revisions. Christoph Jentzsch for authoring the Ethash algorithm and Yoichi Hirai for doing most of the EIP-150 changes. Important maintenance, useful corrections and suggestions were provided by a number of others from the Ethereum DEV organisation and Ethereum community at large including Gustav Simonsson, Paweł Bylica, Jutta Steiner, Nick Savers, Viktor Trón, Marko Simovic, Giacomo Tassarri and, of course, Vitalik Buterin.

16. Availability

The source of this paper is maintained at https://github.com/ethereum/yellowpaper/. An auto-generated PDF is located at https://ethereum.github.io/yellowpaper/paper.pdf.

References


Afri Schoedon and Vitalik Buterin. EIP-649: Metropolis difficulty bomb delay and block reward reduction,
Appendix A. Terminology

**External Actor:** A person or other entity able to interface to an Ethereum node, but external to the world of Ethereum. It can interact with Ethereum through depositing signed Transactions and inspecting the blockchain and associated state. Has one (or more) intrinsic Accounts.

**Address:** A 160-bit code used for identifying Accounts.

**Account:** Accounts have an intrinsic balance and transaction count maintained as part of the Ethereum state. They also have some (possibly empty) EVM Code and a (possibly empty) Storage State associated with them. Though homogenous, it makes sense to distinguish between two practical types of account: those with empty associated EVM Code (thus the account balance is controlled, if at all, by some external entity) and those with non-empty associated EVM Code (thus the account represents an Autonomous Object). Each Account has a single Address that identifies it.

**Transaction:** A piece of data, signed by an External Actor. It represents either a Message or a new Autonomous Object. Transactions are recorded into each block of the blockchain.

**Autonomous Object:** A notional object existent only within the hypothetical state of Ethereum. Has an intrinsic address and thus an associated account; the account will have non-empty associated EVM Code. Incorporated only as the Storage State of that account.

**Storage State:** The information particular to a given Account that is maintained between the times that the Account’s associated EVM Code runs.

**Message:** Data (as a set of bytes) and Value (specified as Ether) that is passed between two Accounts, either through the deterministic operation of an Autonomous Object or the cryptographically secure signature of the Transaction.

**Message Call:** The act of passing a message from one Account to another. If the destination account is associated with non-empty EVM Code, then the VM will be started with the state of said Object and the Message acted upon. If the message sender is an Autonomous Object, then the Call passes any data returned from the VM operation.

**Gas:** The fundamental network cost unit. Paid for exclusively by Ether (as of PoC-4), which is converted freely to and from Gas as required. Gas does not exist outside of the internal Ethereum computation engine; its price is set by the Transaction and miners are free to ignore Transactions whose Gas price is too low.

**Contract:** Informal term used to mean both a piece of EVM Code that may be associated with an Account or an Autonomous Object.

**Object:** Synonym for Autonomous Object.

**App:** An end-user-visible application hosted in the Ethereum Browser.

**Ethereum Browser:** (aka Ethereum Reference Client) A cross-platform GUI of an interface similar to a simplified browser (a la Chrome) that is able to host sandboxed applications whose backend is purely on the Ethereum protocol.

**Ethereum Virtual Machine:** (aka EVM) The virtual machine that forms the key part of the execution model for an Account’s associated EVM Code.

**Ethereum Runtime Environment:** (aka ERE) The environment which is provided to an Autonomous Object executing in the EVM. Includes the EVM but also the structure of the world state on which the EVM relies for certain I/O instructions including CALL & CREATE.

**EVM Code:** The bytecode that the EVM can natively execute. Used to formally specify the meaning and ramifications of a message to an Account.

**EVM Assembly:** The human-readable form of EVM-code.

**LLL:** The Lisp-like Low-level Language, a human-writable language used for authoring simple contracts and general low-level language toolkit for trans-compiling to.

Appendix B. Recursive Length Prefix

This is a serialisation method for encoding arbitrarily structured binary data (byte arrays).
We define the set of possible structures $\mathbb{T}$:

$$\mathbb{T} \equiv \mathbb{L} \cup \mathbb{B}$$

$$\mathbb{L} \equiv \{ t : t = (t[0], t[1], ...) \land \forall n < |t| t[n] \in \mathbb{T} \}$$

$$\mathbb{B} \equiv \{ b : b = (b[0], b[1], ...) \land \forall n < |b| b[n] \in \mathbb{O} \}$$

Where $\mathbb{O}$ is the set of bytes. Thus $\mathbb{B}$ is the set of all sequences of bytes (otherwise known as byte-arrays, and a leaf if imagined as a tree), $\mathbb{L}$ is the set of all tree-like (sub-)structures that are not a single leaf (a branch node if imagined as a tree) and $\mathbb{T}$ is the set of all byte-arrays and such structural sequences.

We define the RLP function as $\text{RLP}$ through two sub-functions, the first handling the instance when the value is a byte array, the second when it is a sequence of further values:

$$\text{RLP}(x) \equiv \begin{cases} R_b(x) & \text{if } x \in \mathbb{B} \\ R_l(x) & \text{otherwise} \end{cases}$$

If the value to be serialised is a byte-array, the RLP serialisation takes one of three forms:

- If the byte-array contains solely a single byte and that single byte is less than 128, then the input is exactly equal to the output.
- If the byte-array contains fewer than 56 bytes, then the output is equal to the input prefixed by the byte equal to the length of the byte array plus 128.
- Otherwise, the output is equal to the input prefixed by the minimal-length byte-array which when interpreted as a big-endian integer is equal to the length of the input byte array, which is itself prefixed by the number of bytes required to faithfully encode this length value plus 183.

Formally, we define $R_b$:

$$R_b(x) \equiv \begin{cases} x & \text{if } |x| = 1 \land x[0] < 128 \\ (128 + |x|) \cdot x & \text{else if } |x| < 56 \\ (183 + \text{BE}(|x|)) \cdot \text{BE}(|x|) \cdot x & \text{otherwise} \end{cases}$$

$$\text{BE}(x) \equiv (b_0, b_1, ...) \land b_0 \neq 0 \land x = \sum_{n=0}^{n<|b|} b_n \cdot 256^{b|-1-n}$$

Thus $\text{BE}$ is the function that expands a positive integer value to a big-endian byte array of minimal length and the dot operator performs sequence concatenation.

If instead, the value to be serialised is a sequence of other items then the RLP serialisation takes one of two forms:

- If the concatenated serialisations of each contained item is less than 56 bytes in length, then the output is equal to that concatenation prefixed by the byte equal to the length of this byte array plus 192.
- Otherwise, the output is equal to the concatenated serialisations prefixed by the minimal-length byte-array which when interpreted as a big-endian integer is equal to the length of the concatenated serialisations byte array, which is itself prefixed by the number of bytes required to faithfully encode this length value plus 247.

Thus we finish by formally defining $R_l$:

$$R_l(x) \equiv \begin{cases} (192 + |s(x)|) \cdot s(x) & \text{if } |s(x)| < 56 \\ (217 + \text{BE}(|s(x)|)) \cdot \text{BE}(|s(x)|) \cdot s(x) & \text{otherwise} \end{cases}$$

$$s(x) \equiv \text{RLP}(x[0]) \cdot \text{RLP}(x[1])...$$

If RLP is used to encode a scalar, defined only as a positive integer ($N$ or any $x$ for $\mathbb{N}_x$), it must be specified as the shortest byte array such that the big-endian interpretation of it is equal. Thus the RLP of some positive integer $i$ is defined as:

$$\text{RLP}(i : i \in \mathbb{N}) \equiv \text{RLP}(\text{BE}(i))$$

When interpreting RLP data, if an expected fragment is decoded as a scalar and leading zeroes are found in the byte sequence, clients are required to consider it non-canonical and treat it in the same manner as otherwise invalid RLP data, dismissing it completely.

There is no specific canonical encoding format for signed or floating-point values.

### Appendix C. Hex-Prefix Encoding

Hex-prefix encoding is an efficient method of encoding an arbitrary number of nibbles as a byte array. It is able to store an additional flag which, when used in the context of the trie (the only context in which it is used), disambiguates between node types.

It is defined as the function $\text{HP}$ which maps from a sequence of nibbles (represented by the set $\mathbb{Y}$) together with a boolean value to a sequence of bytes (represented by the set $\mathbb{B}$):
The key is accumulated through the traversal, acquiring a single nibble from each branch node (just as with a radix tree). Thus we define in terms of $c$

Unlike a radix tree, in the case of multiple keys sharing the same prefix or in the case of a single key having a unique

When considering such a sequence, we use the common numeric subscript notation to refer to a tuple’s key or value, thus:

Any series of bytes may also trivially be viewed as a series of nibbles, given an endian-specific notation; here we assume

We define the function $\text{TRIE}$, which evaluates to the root of the trie that represents this set when encoded in this structure:

We also assume a function $n$, the trie’s node cap function. When composing a node, we use RLP to encode the structure. As a means of reducing storage complexity, for nodes whose composed RLP is fewer than 32 bytes, we store the RLP directly; for those larger we assert prescience of the byte array whose Keccak hash evaluates to our reference. Thus we define in terms of $c$, the node composition function:

In a manner similar to a radix tree, when the trie is traversed from root to leaf, one may build a single key-value pair. The key is accumulated through the traversal, acquiring a single nibble from each branch node (just as with a radix tree). Unlike a radix tree, in the case of multiple keys sharing the same prefix or in the case of a single key having a unique suffix, two optimising nodes are provided. Thus while traversing, one may potentially acquire multiple nibbles from each of the other two node types, extension and leaf. There are three kinds of nodes in the trie:

Leaf: A two-item structure whose first item corresponds to the nibbles in the key not already accounted for by the accumulation of keys and branches traversed from the root. The hex-prefix encoding method is used and the second parameter to the function is required to be $true$.

Extension: A two-item structure whose first item corresponds to a series of nibbles of size greater than one that are shared by at least two distinct keys past the accumulation of the keys of nibbles and the keys of branches as traversed from the root. The hex-prefix encoding method is used and the second parameter to the function is required to be $false$.

Branch: A 17-item structure whose first sixteen items correspond to each of the sixteen possible nibble values for the keys at this point in their traversal. The 17th item is used in the case of this being a terminator node and thus a key being ended at this point in its traversal.
A branch is then only used when necessary; no branch nodes may exist that contain only a single non-zero entry. We may formally define this structure with the structural composition function \( c \):

\[
(194)\quad c(\mathcal{J}, i) = \begin{cases} 
\operatorname{RLP}(\mathcal{H}(\mathcal{I}[i . (||I_0|| - 1)], \text{true}, I_1)) & \text{if } ||\mathcal{J}|| = 1 \text{ where } \exists I : I \in \mathcal{J} \\
\operatorname{RLP}(\mathcal{H}(\mathcal{I}[i . (j - 1)], \text{false}, n(\mathcal{J}, j))) & \text{if } i \neq j \text{ where } j = \arg \max_x : \exists I : ||I|| = x : \forall I \in \mathcal{J} \text{ where } I_0[0..(x - 1)] = 1 \\
\operatorname{RLP}(u(0), u(1), \ldots, u(15), v) & \text{otherwise where } u(j) = n(\{ I : I \in \mathcal{J} \wedge I_0[i] = j, i + 1 \}) \\
v = \begin{cases} 
I_1 & \text{if } \exists I : I \in \mathcal{J} \wedge ||I_0|| = i \\
() & \text{otherwise}
\end{cases}
\end{cases}
\]

D.1. Trie Database. Thus no explicit assumptions are made concerning what data is stored and what is not, since that is an implementation-specific consideration; we simply define the identity function mapping the key-value set \( \mathcal{J} \) to a 32-byte hash and assert that only a single such hash exists for any \( \mathcal{J} \), which though not strictly true is accurate within acceptable precision given the Keccak hash’s collision resistance. In reality, a sensible implementation will not fully recompute the trie root hash for each set.

A reasonable implementation will maintain a database of nodes determined from the computation of various tries or, more formally, it will memoise the function \( c \). This strategy uses the nature of the trie to both easily recall the contents of any previous key-value set and to store multiple such sets in a very efficient manner. Due to the dependency relationship, Merkle-proofs may be constructed with an \( O(\log N) \) space requirement that can demonstrate a particular leaf must exist within a trie of a given root hash.

Appendix E. Precompiled Contracts

For each precompiled contract, we make use of a template function, \( \Xi_{\text{PRE}} \), which implements the out-of-gas checking.

\[
(195)\quad \Xi_{\text{PRE}}(\sigma, g, I, T) = \begin{cases} 
(\emptyset, 0, A^0, ()) & \text{if } g < g_r \\
(\sigma, g - g_r, A^0, o) & \text{otherwise}
\end{cases}
\]

The precompiled contracts each use these definitions and provide specifications for the \( o \) (the output data) and \( g_r \), the gas requirements.

We define \( \Xi_{\text{ECREC}} \) as a precompiled contract for the elliptic curve digital signature algorithm (ECDSA) public key recovery function (ECDSARECOVER). See Appendix F for the definition of the function ECDSARECOVER. We also define \( d \) to be the input data, well-defined for an infinite length by appending zeroes as required. In the case of an invalid signature (ECDSARECOVER(\( h, v, r, s \) = \( \emptyset \)), we return no output.

\[
(196)\quad \Xi_{\text{ECREC}} \equiv \Xi_{\text{PRE}} \text{ where:}
\]

\[
(197)\quad g_r = 3000
\]

\[
(198)\quad |o| = \begin{cases} 
0 & \text{if } \text{ECDSARECOVER}(h, v, r, s) = \emptyset \\
32 & \text{otherwise}
\end{cases}
\]

\[
(199)\quad \text{if } |o| = 32:
\]

\[
(200)\quad o[0..11] = 0
\]

\[
(201)\quad o[12..31] = \text{KEC}(\text{ECDSARECOVER}(h, v, r, s))[12..31] \text{ where:}
\]

\[
(202)\quad d[0..(||I_0|| - 1)] = I_d \\
(203)\quad d[||I_d|| - 1] = (0, 0, \ldots)
\]

\[
(204)\quad h = d[0..31]
\]

\[
(205)\quad v = d[32..63]
\]

\[
(206)\quad r = d[64..95]
\]

\[
(207)\quad s = d[96..127]
\]

We define \( \Xi_{\text{SHA256}} \) and \( \Xi_{\text{RIPEMD}} \) as precompiled contracts implementing the SHA2-256 and RIPEMD-160 hash functions respectively. Their gas usage is dependent on the input data size, a factor rounded up to the nearest number of words.
For the purposes here, we assume we have well-defined standard cryptographic functions for RIPEMD-160 and SHA2-256 of the form:

\begin{align}
\Xi_{SHA256} & \equiv \Xi_{pre} \quad \text{where:} \\
\xi & = 60 + 12 \left\lfloor \frac{|I\alpha|}{32} \right\rfloor \\
\Xi_{RIPEMD} & \equiv \Xi_{pre} \quad \text{where:} \\
\xi & = 600 + 120 \left\lfloor \frac{|I\alpha|}{32} \right\rfloor \\
o[0.31] & = SHA256(I\alpha) \\
o[0.11] & = 0 \\
o[12.31] & = RIPEMD160(I\alpha)
\end{align}

E.1. zkSNARK Related Precompiled Contracts. We choose two numbers, both of which are prime.

\begin{align}
p & \equiv 2188824271839275222224640574525725708869631115729782366268903789464522620583 \\
r & \equiv 21888242718392752222246405745257257088548364400416034343698204186575808495617
\end{align}

Since \( p \) is a prime number, \( \{0, 1, \ldots, p - 1\} \) forms a field with addition and multiplication modulo \( p \). We call this field \( F_p \).
We define a set $C_1$ with
\[(234)\]
\[C_1 \equiv \{(X, Y) \in F_p \times F_p \mid Y^2 = X^3 + 3\} \cup \{(0, 0)\}\]
We define a binary operation $+$ on $C_1$ for distinct elements $(X_1, Y_1), (X_2, Y_2)$ with
\[(235)\]
\[(X_1,Y_1) + (X_2,Y_2) \equiv \begin{cases} (X,Y) & \text{if } X_1 \neq X_2 \\ (0,0) & \text{otherwise} \end{cases}
\[
\lambda \equiv \frac{Y_2 - Y_1}{X_2 - X_1} \\
X \equiv \lambda^2 - X_1 - X_2 \\
Y \equiv \lambda(X_1 - X) - Y_1
\]
In the case where $(X_1, Y_1) = (X_2, Y_2)$, we define $+$ on $C_1$ with
\[(236)\]
\[(X_1,Y_1) + (X_2,Y_2) \equiv \begin{cases} (X,Y) & \text{if } Y_1 \neq 0 \\ (0,0) & \text{otherwise} \end{cases}
\[
\lambda \equiv \frac{3X_1^2}{2Y_1} \\
X \equiv \lambda^2 - 2X_1 \\
Y \equiv \lambda(X_1 - X) - Y_1
\]
$(C_1, +)$ is known to form a group. We define scalar multiplication $\cdot$ with
\[(237)\]
\[n \cdot P \equiv (0,0) + P + \cdots + P_n\]
for a natural number $n$ and a point $P$ in $C_1$.
We define $P_1$ to be a point $(1, 2)$ on $C_1$. Let $G_1$ be the subgroup of $(C_1, +)$ generated by $P_1$. $G_1$ is known to be a cyclic group of order $q$. For a point $P$ in $G_1$, we define $\log_{P_1}(P)$ to be the smallest natural number $n$ satisfying $n \cdot P_1 = P$. $\log_{P_1}(P)$ is at most $q - 1$.
Let $F_{p^2}$ be a field $F_p[i]/(i^2 + 1)$. We define a set $C_2$ with
\[(238)\]
\[C_2 \equiv \{(X, Y) \in F_{p^2} \times F_{p^2} \mid Y^2 = X^3 + 3(i + 9)^{-1} - 1\} \cup \{(0, 0)\}\]
We define a binary operation $+$ and scalar multiplication $\cdot$ with the same equations $(235)$, $(236)$ and $(237)$. $(C_2, +)$ is also known to form a group. We define $P_2$ in $C_2$ with
\[(239)\]
\[P_2 \equiv (11559732932986387107991004021392285783925812861821119253091740315145291805634 \times i + 108570469990230571359445706722328294813707565957851808699051999328565582781,\]
\[408236787586343368133220340314543556831685132759340120810574107621412093531 \times i + 8495653923123431417604973247489272438418190587263600148770280649306958101930)\]
We define $G_2$ to be the subgroup of $(C_2, +)$ generated by $P_2$. $G_2$ is known to be the only cyclic group of order $q$ on $C_2$. For a point $P$ in $G_2$, we define $\log_{P_2}(P)$ to be the smallest natural number $n$ satisfying $n \cdot P_2 = P$. With this definition, $\log_{P_2}(P)$ is at most $q - 1$.
Let $G_T$ be the multiplicative abelian group underlying $F_{p^2}$. It is known that a non-degenerate bilinear map $e : G_1 \times G_2 \to G_T$ exists. This bilinear map is a type three pairing. There are several such bilinear maps, it does not matter which is chosen to be $e$. Let $P_T = e(P_1, P_2)$, a be a set of $k$ points in $G_1$, and $b$ be a set of $k$ points in $G_2$. It follows from the definition of a pairing that the following are equivalent
\[(240)\]
\[\log_{P_1}(a_1) \times \log_{P_2}(b_1) + \cdots + \log_{P_1}(a_k) \times \log_{P_2}(b_k) \equiv 1 \mod q\]
\[(241)\]
\[\prod_{i=0}^{k} e(a_i, b_i) = P_T\]
Thus the pairing operation provides a method to verify $(240)$.
A 32 byte number $x \in P_{256}$ might and might not represent an element of $F_p$.
\[(242)\]
\[\delta_p(x) \equiv \begin{cases} x & \text{if } x < p \\ \emptyset & \text{otherwise} \end{cases}\]
A 64 byte data $x \in \mathbb{B}_{512}$ might and might not represent an element of $G_1$.

$$\delta_1(x) \equiv \begin{cases} \{g_i \text{ if } g_i \in G_1 \} & \text{otherwise} \\ \emptyset & \text{otherwise} \end{cases}$$

$$g_i \equiv \begin{cases} (x, y) \text{ if } x \neq \emptyset \land y \neq \emptyset \\ \emptyset \text{ otherwise} \end{cases}$$

$$x \equiv \delta_1(x_{[0..31]})$$

$$y \equiv \delta_1(x_{[32..63]})$$

A 128 byte data $x \in \mathbb{B}_{1024}$ might and might not represent an element of $G_2$.

$$\delta_2(x) \equiv \begin{cases} \{g_2 \text{ if } g_2 \in G_2 \} & \text{otherwise} \\ \emptyset & \text{otherwise} \end{cases}$$

$$g_2 \equiv \begin{cases} ((x_0 + y_0), (x_1 + y_1)) \text{ if } x_0 \neq \emptyset \land y_0 \neq \emptyset \land x_1 \neq \emptyset \land y_1 \neq \emptyset \\ \emptyset \text{ otherwise} \end{cases}$$

$$x_0 \equiv \delta_2(x_{[0..31]})$$

$$y_0 \equiv \delta_2(x_{[32..63]})$$

We define $\Xi_{SNARK}$ as a precompiled contract which checks if $\delta_1(x)$ holds, for intended use in zkSNARK verification.

$$\Xi_{SNARK} \equiv \Xi_{PRE} \text{ except:}$$

$$\Xi_{SNARK}(\sigma, g, I) \equiv (\emptyset, 0, A^0, (\emptyset)) \text{ if } F$$

$$F \equiv ((|I_a| \mod 192 \neq 0 \lor (\exists j. a_j = \emptyset \lor b_j = \emptyset))$$

$$k \equiv \frac{|I_a|}{192}$$

$$g_0 \equiv 60000k + 40000$$

$$\omega_{[0..31]} \equiv \begin{cases} 0x00000000000000000000000000000000000000000000000000000000000000001 \text{ if } v \land \neg F \\ 0x0000000000000000000000000000000000000000000000000000000000000000 \text{ if } \neg v \land \neg F \end{cases}$$

$$v \equiv (\log_{P_1}(a_1) \times \log_{P_2}(b_1) + \cdots + \log_{P_1}(a_k) \times \log_{P_2}(b_k)) \equiv 1 \mod q$$

$$a_1 \equiv \delta_1(I_a[0..63])$$

$$b_1 \equiv \delta_2(I_a[64..191])$$

$$\vdots$$

$$a_k \equiv \delta_1(I_a[|I_a| - 192]| |I_a| - 129])$$

$$b_k \equiv \delta_2(I_a[|I_a| - 128]| |I_a| - 1])$$

We define a precompiled contract for addition on $G_1$.

$$\Xi_{ADD} \equiv \Xi_{ADD} \text{ except:}$$

$$\Xi_{ADD}(\sigma, g, I) \equiv (\emptyset, 0, A^0, (\emptyset)) \text{ if } x = \emptyset \lor y = \emptyset$$

$$g_0 \equiv 500$$

$$\omega \equiv \delta_1^{-1}(x + y) \text{ where } + \text{ is the group operation in } G_1$$

$$x \equiv \delta_1(I_a[0..63])$$

$$y \equiv \delta_1(I_a[64..127])$$

$$I_a[x] \equiv \begin{cases} I_a[x] \text{ if } x < |I_a| \\ 0 \text{ otherwise} \end{cases}$$

We define a precompiled contract for scalar multiplication on $G_1$, where $I_a$ is defined in $270$.

$$\Xi_{SM} \equiv \Xi_{SM} \text{ except:}$$

$$\Xi_{SM}(\sigma, g, I) \equiv (\emptyset, 0, A^0, (\emptyset)) \text{ if } x = \emptyset$$

$$g_0 \equiv 40000$$

$$\omega \equiv \delta_1^{-1}(n \cdot x) \text{ where } \cdot \text{ is the scalar multiplication in } G_1$$

$$n \equiv I_a[0..31]$$

$$x \equiv \delta_1(I_a[32..95])$$
Appendix F. Signing Transactions

The method of signing transactions is similar to the ‘Electrum style signatures’ as defined by Arnaud et al. [2017], heading “Managing styles with Radium” in the bullet point list. This method utilises the SECP-256k1 curve as described by Courtois et al. [2014], and is implemented similarly to as described by Gura et al. [2004] on p. 9 of 15, para. 3.

It is assumed that the sender has a valid private key \( p_s \), which is a randomly selected positive integer (represented as a byte array of length 32 in big-endian form) in the range \([1, \text{secp256k1n} - 1]\).

We assume the existence of functions \textsc{Ecdsapubkey}, \textsc{Ecdsasign} and \textsc{Ecdsarecover}. These are formally defined in the literature, e.g. by Johnson et al. [2001].

\[
\begin{align*}
\textsc{Ecdsapubkey}(p_s & \in B_{32}) \equiv p_s \in B_{64} \\
\textsc{Ecdsasign}(e & \in B_{32}, p_s \in B_{32}) \equiv (v \in B_{1}, r \in B_{32}, s \in B_{32}) \\
\textsc{Ecdsarecover}(e & \in B_{32}, v \in B_{1}, r \in B_{32}, s \in B_{32}) \equiv p_s \in B_{64}
\end{align*}
\]

Where \( p_s \) is the public key, assumed to be a byte array of size 64 (formed from the concatenation of two positive integers each \(< 2^{256}\) ), \( p_s \) is the private key, a byte array of size 32 (or a single positive integer in the aforementioned range) and \( e \) is the hash of the transaction, \( h(T) \). It is assumed that \( v \) is either the ‘recovery identifier’ or ‘chain identifier doubled plus 35 or 36’. The recovery identifier is a 1 byte value specifying the parity and finiteness of the coordinates of the curve point for which \( r \) is the \( x \)-value; this value is in the range of [27, 30], however we declare the upper two possibilities, representing infinite values, invalid. The value 27 represents an even \( y \) value and 28 represents an odd \( y \) value. In the second case, where \( v \) is the chain identifier doubled plus 35 or 36, the values 35 and 36 assume the role of the ‘recovery identifier’ by specifying the parity of \( y \), with the value 35 representing an even value and 36 representing an odd value.

We declare that a signature is invalid unless all the following conditions are true:

\[
\begin{align*}
0 & < r < \text{secp256k1n} \\
0 & < s < \text{secp256k1n} \div 2 + 1 \\
\forall v & \in \{27, 28, \text{chain_id} \times 2 + 35, \text{chain_id} \times 2 + 36\}
\end{align*}
\]

where:

\[
\text{secp256k1n} = 1157920892373161954233709850088897907852837564479035034481539378775881345762871
\]

For a given private key, \( p_s \), the Ethereum address \( A(p_s) \) (a 160-bit value) to which it corresponds is defined as the right most 160-bits of the Keccak hash of the corresponding ECDSA public key:

\[
A(p_s) = B_{255}(\text{KEC}\{\textsc{Ecdsapubkey}(p_s)\})
\]

The message hash, \( h(T) \), to be signed is the Keccak hash of the transaction. Two different flavors of signing schemes are available. One operates without the latter three signature components, formally described as \( T_r \) and \( T_s \). The other operates on nine elements:

\[
L_s(T) = \begin{cases} 
(T_n, T_p, T_g, T_t, T_s, p) & \text{if } v \in \{27, 28\} \\
(T_n, T_p, T_g, T_t, T_s, p, \text{chain_id}, (), ()) & \text{otherwise}
\end{cases}
\]

where

\[
p = \begin{cases} 
T_t & \text{if } T_t = 0 \\
T_a & \text{otherwise}
\end{cases}
\]

\[
h(T) = \text{KEC}(L_s(T))
\]

The signed transaction \( G(T, p_s) \) is defined as:

\[
G(T, p_s) \equiv T \text{ except:} \\
(T_w, T_r, T_t) = \textsc{Ecdsasign}(h(T), p_s)
\]

\[
S(T) \equiv B_{255}(\text{KEC}\{\textsc{Ecdsarecover}(h(T), v_0, T_r, T_s)\})
\]

\[
v_0 = \begin{cases} 
T_w & \text{if } T_w \in \{27, 28\} \\
28 - (T_w \mod 2) & \text{otherwise}
\end{cases}
\]

The assertion that the sender of a signed transaction equals the address of the signer should be self-evident:

\[
\forall T : \forall p_s : S(G(T, p_s)) \equiv A(p_s)
\]
**Appendix G. Fee Schedule**

The fee schedule $G$ is a tuple of 31 scalar values corresponding to the relative costs, in gas, of a number of abstract operations that a transaction may effect.

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
<th>Description*</th>
</tr>
</thead>
<tbody>
<tr>
<td>$G_{\text{zero}}$</td>
<td>0</td>
<td>Nothing paid for operations of the set $W_{\text{zero}}$.</td>
</tr>
<tr>
<td>$G_{\text{base}}$</td>
<td>2</td>
<td>Amount of gas to pay for operations of the set $W_{\text{base}}$.</td>
</tr>
<tr>
<td>$G_{\text{verylow}}$</td>
<td>3</td>
<td>Amount of gas to pay for operations of the set $W_{\text{verylow}}$.</td>
</tr>
<tr>
<td>$G_{\text{low}}$</td>
<td>5</td>
<td>Amount of gas to pay for operations of the set $W_{\text{low}}$.</td>
</tr>
<tr>
<td>$G_{\text{mid}}$</td>
<td>8</td>
<td>Amount of gas to pay for operations of the set $W_{\text{mid}}$.</td>
</tr>
<tr>
<td>$G_{\text{high}}$</td>
<td>10</td>
<td>Amount of gas to pay for operations of the set $W_{\text{high}}$.</td>
</tr>
<tr>
<td>$G_{\text{extcode}}$</td>
<td>700</td>
<td>Amount of gas to pay for operations of the set $W_{\text{extcode}}$.</td>
</tr>
<tr>
<td>$G_{\text{balance}}$</td>
<td>400</td>
<td>Amount of gas to pay for a BALANCE operation.</td>
</tr>
<tr>
<td>$G_{\text{load}}$</td>
<td>200</td>
<td>Paid for a SLOAD operation.</td>
</tr>
<tr>
<td>$G_{\text{jumpdest}}$</td>
<td>20000</td>
<td>Paid for an SSTORE operation when the storage value is set to non-zero from zero.</td>
</tr>
<tr>
<td>$G_{\text{reset}}$</td>
<td>5000</td>
<td>Paid for an SSTORE operation when the storage value’s zeroness remains unchanged or is set to zero.</td>
</tr>
<tr>
<td>$R_{\text{reset}}$</td>
<td>15000</td>
<td>Refund given (added into refund counter) when the storage value is set to zero from non-zero.</td>
</tr>
<tr>
<td>$R_{\text{selfdestruct}}$</td>
<td>24000</td>
<td>Refund given (added into refund counter) for self-destructing an account.</td>
</tr>
<tr>
<td>$G_{\text{selfdestruct}}$</td>
<td>5000</td>
<td>Amount of gas to pay for a SELFDESTRUCT operation.</td>
</tr>
<tr>
<td>$G_{\text{create}}$</td>
<td>32000</td>
<td>Create paid for a CREATE operation.</td>
</tr>
<tr>
<td>$G_{\text{codedeposit}}$</td>
<td>200</td>
<td>Paid per byte for a CREATE operation to succeed in placing code into state.</td>
</tr>
<tr>
<td>$G_{\text{call}}$</td>
<td>700</td>
<td>Paid for a CALL operation.</td>
</tr>
<tr>
<td>$G_{\text{callvalue}}$</td>
<td>9000</td>
<td>Paid for a non-zero value transfer as part of the CALL operation.</td>
</tr>
<tr>
<td>$G_{\text{callstipend}}$</td>
<td>2300</td>
<td>A stipend for the called contract subtracted from $G_{\text{callvalue}}$ for a non-zero value transfer.</td>
</tr>
<tr>
<td>$G_{\text{newaccount}}$</td>
<td>25000</td>
<td>Paid for a CALL or SELFDESTRUCT operation which creates an account.</td>
</tr>
<tr>
<td>$G_{\text{exp}}$</td>
<td>10</td>
<td>Partial payment for an EXP operation.</td>
</tr>
<tr>
<td>$G_{\text{expbyte}}$</td>
<td>50</td>
<td>Partial payment when multiplied by $\lceil \log_{256}(\text{exponent}) \rceil$ for the EXP operation.</td>
</tr>
<tr>
<td>$G_{\text{memory}}$</td>
<td>3</td>
<td>Paid for every additional word when expanding memory.</td>
</tr>
<tr>
<td>$G_{\text{txcreate}}$</td>
<td>32000</td>
<td>Paid by all contract-creating transactions after the Homestead transition.</td>
</tr>
<tr>
<td>$G_{\text{txdatazero}}$</td>
<td>4</td>
<td>Paid for every zero byte of data or code for a transaction.</td>
</tr>
<tr>
<td>$G_{\text{txdatanonzero}}$</td>
<td>68</td>
<td>Paid for every non-zero byte of data or code for a transaction.</td>
</tr>
<tr>
<td>$G_{\text{transaction}}$</td>
<td>21000</td>
<td>Paid for every transaction.</td>
</tr>
<tr>
<td>$G_{\text{log}}$</td>
<td>375</td>
<td>Partial payment for a LOG operation.</td>
</tr>
<tr>
<td>$G_{\text{logdata}}$</td>
<td>8</td>
<td>Paid for each byte in a LOG operation’s data.</td>
</tr>
<tr>
<td>$G_{\text{logtopic}}$</td>
<td>375</td>
<td>Paid for each topic of a LOG operation.</td>
</tr>
<tr>
<td>$G_{\text{sha3}}$</td>
<td>30</td>
<td>Paid for each SHA3 operation.</td>
</tr>
<tr>
<td>$G_{\text{sha3word}}$</td>
<td>6</td>
<td>Paid for each word (rounded up) for input data to a SHA3 operation.</td>
</tr>
<tr>
<td>$G_{\text{copy}}$</td>
<td>3</td>
<td>Partial payment for *COPY operations, multiplied by words copied, rounded up.</td>
</tr>
<tr>
<td>$G_{\text{blockhash}}$</td>
<td>20</td>
<td>Payment for BLOCKHASH operation.</td>
</tr>
<tr>
<td>$G_{\text{quadratic}}$</td>
<td>100</td>
<td>The quadratic coefficient of the input sizes of the exponentiation-over-modulo precompiled contract.</td>
</tr>
</tbody>
</table>

**Appendix H. Virtual Machine Specification**

When interpreting 256-bit binary values as integers, the representation is big-endian.

When a 256-bit machine datum is converted to and from a 160-bit address or hash, the rightwards (low-order for BE) 20 bytes are used and the left most 12 are discarded or filled with zeroes, thus the integer values (when the bytes are interpreted as big-endian) are equivalent.

**H.1. Gas Cost.** The general gas cost function, $C$, is defined as:
\[ C(\sigma, \mu, I) \equiv C_{\text{mem}}(\mu') - C_{\text{mem}}(\mu) + C_{\text{store}}(\sigma, \mu) + C_{\text{selfdestruct}}(\sigma, \mu) \]

where:

\[ w \equiv \begin{cases} \lfloor I_b / \mu_{pc} \rfloor & \text{if } \mu_{pc} < \|I_b\| \\ \text{STOP} & \text{otherwise} \end{cases} \]

with \( C_{\text{call}}, C_{\text{selfdestruct}} \) and \( C_{\text{store}} \) as specified in the appropriate section below. We define the following subsets of instructions:

\[ W_{\text{base}} = \{ \text{STOP, RETURN, REVERT} \} \]

\[ W_{\text{base}} = \{ \text{ADDRESS, ORIGIN, CALLER, CALLVALUE, CALLDATASIZE, CODESIZE, GASPRICE, COINBASE, TIMESTAMP, NUMBER, DIFFICULTY, GASLIMIT, RETURNDATASIZE, POP, PC, MSIZE, GAS} \} \]

\[ W_{\text{everylow}} = \{ \text{ADD, SUB, NOT, LT, GT, SLT, SGT, EQ, ISZERO, AND, OR, XOR, BYTE, CALLDATACOPY, MLOAD, MSTORE, MSTORE8, PUSH*, DUP*, SWAP*} \} \]

\[ W_{\text{low}} = \{ \text{MUL, DIV, SDIV, MOD, SMOD, SIGNEXTEND} \} \]

\[ W_{\text{mid}} = \{ \text{ADDMOD, MULMOD, JUMP} \} \]

\[ W_{\text{high}} = \{ \text{JUMPI} \} \]

\[ W_{\text{extcode}} = \{ \text{EXTCODESIZE} \} \]

Note the memory cost component, given as the product of \( G_{\text{memory}} \) and the maximum of 0 & the ceiling of the number of words in size that the memory must be over the current number of words, \( \mu_{pc} \), in order that all accesses reference valid memory whether for read or write. Such accesses must be for non-zero number of bytes.

Referencing a zero length range (e.g. by attempting to pass it as the input range to a CALL) does not require memory to be extended to the beginning of the range. \( \mu' \) is defined as this new maximum number of words of active memory; special-cases are given where these two are not equal.

While defining the instruction set, we defined the memory-expansion for range function, \( M \), thus:
Another useful function is “all but one 64th” function $L$ defined as:

\[
L(n) \equiv n - \lfloor n/64 \rfloor
\]
## 0s: Stop and Arithmetic Operations

All arithmetic is modulo $2^{256}$ unless otherwise noted. The zero-th power of zero $0^0$ is defined to be one.

<table>
<thead>
<tr>
<th>Value</th>
<th>Mnemonic</th>
<th>δ</th>
<th>α</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x00</td>
<td>STOP</td>
<td>0</td>
<td>0</td>
<td>Halts execution.</td>
</tr>
<tr>
<td>0x01</td>
<td>ADD</td>
<td>2</td>
<td>1</td>
<td>Addition operation. $\mu_s'[0] \equiv \mu_s[0] + \mu_s[1]$</td>
</tr>
<tr>
<td>0x02</td>
<td>MUL</td>
<td>2</td>
<td>1</td>
<td>Multiplication operation. $\mu_s'[0] \equiv \mu_s[0] \times \mu_s[1]$</td>
</tr>
<tr>
<td>0x03</td>
<td>SUB</td>
<td>2</td>
<td>1</td>
<td>Subtraction operation. $\mu_s'[0] \equiv \mu_s[0] - \mu_s[1]$</td>
</tr>
<tr>
<td>0x04</td>
<td>DIV</td>
<td>2</td>
<td>1</td>
<td>Integer division operation. $\mu_s'[0] \equiv \begin{cases} 0 &amp; \text{if } \mu_s[1] = 0 \ \lfloor \mu_s[0] \div \mu_s[1] \rfloor &amp; \text{otherwise} \end{cases}$</td>
</tr>
<tr>
<td>0x05</td>
<td>SDIV</td>
<td>2</td>
<td>1</td>
<td>Signed integer division operation (truncated). $\mu_s'[0] \equiv \begin{cases} 0 &amp; \text{if } \mu_s[1] = 0 \ -2^{255} &amp; \text{if } \mu_s[0] = -2^{255} \land \mu_s[1] = -1 \ \text{sgn}(\mu_s[0]) \lfloor</td>
</tr>
<tr>
<td>0x06</td>
<td>MOD</td>
<td>2</td>
<td>1</td>
<td>Modulo remainder operation. $\mu_s'[0] \equiv \begin{cases} 0 &amp; \text{if } \mu_s[1] = 0 \ \mu_s[0] \mod \mu_s[1] &amp; \text{otherwise} \end{cases}$</td>
</tr>
<tr>
<td>0x07</td>
<td>SMOD</td>
<td>2</td>
<td>1</td>
<td>Signed modulo remainder operation. $\mu_s'[0] \equiv \begin{cases} 0 &amp; \text{if } \mu_s[1] = 0 \ \text{sgn}(\mu_s[0]) \lfloor</td>
</tr>
<tr>
<td>0x08</td>
<td>ADDMOD</td>
<td>3</td>
<td>1</td>
<td>Modulo addition operation. $\mu_s'[0] \equiv \begin{cases} 0 &amp; \text{if } \mu_s[2] = 0 \ (\mu_s[0] + \mu_s[1]) \mod \mu_s[2] &amp; \text{otherwise} \end{cases}$ \small All intermediate calculations of this operation are not subject to the $2^{256}$ modulo.</td>
</tr>
<tr>
<td>0x09</td>
<td>MULMOD</td>
<td>3</td>
<td>1</td>
<td>Modulo multiplication operation. $\mu_s'[0] \equiv \begin{cases} 0 &amp; \text{if } \mu_s[2] = 0 \ (\mu_s[0] \times \mu_s[1]) \mod \mu_s[2] &amp; \text{otherwise} \end{cases}$ \small All intermediate calculations of this operation are not subject to the $2^{256}$ modulo.</td>
</tr>
<tr>
<td>0x0a</td>
<td>EXP</td>
<td>2</td>
<td>1</td>
<td>Exponential operation. $\mu_s'[0] \equiv \mu_s[0]^\mu_s[1]$</td>
</tr>
<tr>
<td>0x0b</td>
<td>SIGNEXTEND</td>
<td>2</td>
<td>1</td>
<td>Extend length of two’s complement signed integer. $\forall i \in [0..255]: \mu_s'[i] \equiv \begin{cases} \mu_s[1] &amp; \text{if } i \leq t \text{ where } t = 256 - 8(\mu_s[0] + 1) \ \mu_s[1] &amp; \text{otherwise} \end{cases}$ $\mu_s[x]$ gives the $i$th bit (counting from zero) of $\mu_s[x]$</td>
</tr>
</tbody>
</table>
### 10s: Comparison & Bitwise Logic Operations

<table>
<thead>
<tr>
<th>Value</th>
<th>Mnemonic</th>
<th>δ</th>
<th>α</th>
<th>Description</th>
</tr>
</thead>
</table>
| 0x10  | LT       | 2 | 1 | Less-than comparison.  
|       |          |   |   | \( \mu_s'[0] \equiv \begin{cases} 1 & \text{if } \mu_s[0] < \mu_s[1] \\ 0 & \text{otherwise} \end{cases} \) |
| 0x11  | GT       | 2 | 1 | Greater-than comparison.  
|       |          |   |   | \( \mu_s'[0] \equiv \begin{cases} 1 & \text{if } \mu_s[0] > \mu_s[1] \\ 0 & \text{otherwise} \end{cases} \) |
| 0x12  | SLT      | 2 | 1 | Signed less-than comparison.  
|       |          |   |   | \( \mu_s'[0] \equiv \begin{cases} 1 & \text{if } \mu_s[0] < \mu_s[1] \\ 0 & \text{otherwise} \end{cases} \)  
|       |          |   |   | Where all values are treated as two’s complement signed 256-bit integers. |
| 0x13  | SGT      | 2 | 1 | Signed greater-than comparison.  
|       |          |   |   | \( \mu_s'[0] \equiv \begin{cases} 1 & \text{if } \mu_s[0] > \mu_s[1] \\ 0 & \text{otherwise} \end{cases} \)  
|       |          |   |   | Where all values are treated as two’s complement signed 256-bit integers. |
| 0x14  | EQ       | 2 | 1 | Equality comparison.  
|       |          |   |   | \( \mu_s'[0] \equiv \begin{cases} 1 & \text{if } \mu_s[0] = \mu_s[1] \\ 0 & \text{otherwise} \end{cases} \) |
| 0x15  | ISZERO   | 1 | 1 | Simple not operator.  
|       |          |   |   | \( \mu_s'[0] \equiv \begin{cases} 1 & \text{if } \mu_s[0] = 0 \\ 0 & \text{otherwise} \end{cases} \) |
| 0x16  | AND      | 2 | 1 | Bitwise AND operation.  
|       |          |   |   | \( \forall i \in [0..255] : \mu_s'[0]_i \equiv \mu_s[0]_i \land \mu_s[1]_i \) |
| 0x17  | OR       | 2 | 1 | Bitwise OR operation.  
|       |          |   |   | \( \forall i \in [0..255] : \mu_s'[0]_i \equiv \mu_s[0]_i \lor \mu_s[1]_i \) |
| 0x18  | XOR      | 2 | 1 | Bitwise XOR operation.  
|       |          |   |   | \( \forall i \in [0..255] : \mu_s'[0]_i \equiv \mu_s[0]_i \oplus \mu_s[1]_i \) |
| 0x19  | NOT      | 1 | 1 | Bitwise NOT operation.  
|       |          |   |   | \( \forall i \in [0..255] : \mu_s'[0]_i \equiv \begin{cases} 1 & \text{if } \mu_s[0]_i = 0 \\ 0 & \text{otherwise} \end{cases} \) |
| 0x1a  | BYTE     | 2 | 1 | Retrieve single byte from word.  
|       |          |   |   | \( \forall i \in [0..255] : \mu_s'[0]_i \equiv \begin{cases} \mu_s[1]_{i+8s} & \text{if } i < 8 \land \mu_s[0] < 32 \\ 0 & \text{otherwise} \end{cases} \)  
|       |          |   |   | For the Nth byte, we count from the left (i.e. N=0 would be the most significant in big endian). |

### 20s: SHA3

<table>
<thead>
<tr>
<th>Value</th>
<th>Mnemonic</th>
<th>δ</th>
<th>α</th>
<th>Description</th>
</tr>
</thead>
</table>
| 0x20  | SHA3     | 2 | 1 | Compute Keccak-256 hash.  
|       |          |   |   | \( \mu_s'[0] \equiv \text{Keccak}(\mu_m[0] \ldots (\mu_k[0] + \mu_k[1] - 1)) \)  
|       |          |   |   | \( \mu_i' \equiv M(\mu_i, \mu_s[0], \mu_s[1]) \) |
### 30s: Environmental Information

<table>
<thead>
<tr>
<th>Value</th>
<th>Mnemonic</th>
<th>δ</th>
<th>α</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x30</td>
<td>ADDRESS</td>
<td>0</td>
<td>1</td>
<td>Get address of currently executing account. ( \mu_s[0] \equiv I_s )</td>
</tr>
<tr>
<td>0x31</td>
<td>BALANCE</td>
<td>1</td>
<td>1</td>
<td>Get balance of the given account. ( \mu_s[0] \equiv \begin{cases} \sigma[\mu_s[0]], &amp; \text{if } \sigma[\mu_s[0]] \mod 2^{160} \neq \emptyset \ 0, &amp; \text{otherwise} \end{cases} )</td>
</tr>
<tr>
<td>0x32</td>
<td>ORIGIN</td>
<td>0</td>
<td>1</td>
<td>Get execution origination address. ( \mu_s[0] \equiv I_s ) This is the sender of original transaction; it is never an account with non-empty associated code.</td>
</tr>
<tr>
<td>0x33</td>
<td>CALLER</td>
<td>0</td>
<td>1</td>
<td>Get caller address. ( \mu_s[0] \equiv I_s ) This is the address of the account that is directly responsible for this execution.</td>
</tr>
<tr>
<td>0x34</td>
<td>CALLVALUE</td>
<td>0</td>
<td>1</td>
<td>Get deposited value by the instruction/transaction responsible for this execution. ( \mu_s[0] \equiv I_s )</td>
</tr>
<tr>
<td>0x35</td>
<td>CALLDATALOAD</td>
<td>1</td>
<td>1</td>
<td>Get input data of current environment. ( \mu_s[0] \equiv I_s { \mu_s[0] } \ldots { \mu_s[0] + 31 } ) with ( I_s[x] = 0 ) if ( x &gt;</td>
</tr>
<tr>
<td>0x36</td>
<td>CALLDATASIZE</td>
<td>0</td>
<td>1</td>
<td>Get size of input data in current environment. ( \mu_s[0] \equiv</td>
</tr>
<tr>
<td>0x37</td>
<td>CALLDATALOAD</td>
<td>3</td>
<td>0</td>
<td>Copy input data in current environment to memory. ( \forall i \in (0...\mu_s[2] - 1) \mu_m[\mu_s[0] + i] \equiv \begin{cases} I_s[\mu_s[1] + i] &amp; \text{if } \mu_s[1] + i &lt;</td>
</tr>
<tr>
<td>0x38</td>
<td>CODESIZE</td>
<td>0</td>
<td>1</td>
<td>Get size of code running in current environment. ( \mu_s[0] \equiv</td>
</tr>
<tr>
<td>0x39</td>
<td>CODECOPY</td>
<td>3</td>
<td>0</td>
<td>Copy code running in current environment to memory. ( \forall i \in (0...\mu_s[2] - 1) \mu_m[\mu_s[0] + i] \equiv \begin{cases} I_s[\mu_s[1] + i] &amp; \text{if } \mu_s[1] + i &lt;</td>
</tr>
<tr>
<td>0x3a</td>
<td>GASPRICE</td>
<td>0</td>
<td>1</td>
<td>Get price of gas in current environment. ( \mu_s[0] \equiv I_p ) This is gas price specified by the originating transaction.</td>
</tr>
<tr>
<td>0x3b</td>
<td>EXTCODESIZE</td>
<td>1</td>
<td>1</td>
<td>Get size of an account’s code. ( \mu_s[0] \equiv</td>
</tr>
<tr>
<td>0x3c</td>
<td>EXTCODECOPY</td>
<td>4</td>
<td>0</td>
<td>Copy an account’s code to memory. ( \forall i \in (0...\mu_s[3] - 1) \mu_m[\mu_s[1] + i] \equiv \begin{cases} c[\mu_s[2] + i] &amp; \text{if } \mu_s[2] + i &lt;</td>
</tr>
<tr>
<td>0x3d</td>
<td>RETURNDATASIZE</td>
<td>0</td>
<td>1</td>
<td>Get size of output data from the previous call from the current environment. ( \mu_s[0] \equiv</td>
</tr>
<tr>
<td>0x3e</td>
<td>RETURNDATALOAD</td>
<td>3</td>
<td>0</td>
<td>Copy output data from the previous call to memory. ( \forall i \in (0...\mu_s[2] - 1) \mu_m[\mu_s[0] + i] \equiv \begin{cases} \mu_s[1] [\mu_s[1] + i] &amp; \text{if } \mu_s[1] + i &lt;</td>
</tr>
</tbody>
</table>
### 40s: Block Information

<table>
<thead>
<tr>
<th>Value</th>
<th>Mnemonic</th>
<th>δ</th>
<th>α</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x40</td>
<td>BLOCKHASH</td>
<td>1</td>
<td>1</td>
<td>Get the hash of one of the 256 most recent complete blocks.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>( \mu_s[0] \equiv P(I_H, \mu_s[0], 0) )</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>where ( P ) is the hash of a block of a particular number, up to a maximum age. 0 is left on the stack if the looked for block number greater than</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>the current block number or more than 256 blocks behind the current block.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>( P(h, n, a) \equiv \begin{cases} 0 &amp; \text{if } n &gt; H_i \lor a = 256 \lor h = 0 \ h &amp; \text{if } n = H_i \ P(H_p, n, a + 1) &amp; \text{otherwise} \end{cases} )</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>and we assert the header ( H ) can be determined from its hash ( h ) unless as its hash is the parent ( h ) is zero.</td>
</tr>
<tr>
<td>0x41</td>
<td>COINBASE</td>
<td>0</td>
<td>1</td>
<td>Get the block’s beneficiary address.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>( \mu_s[0] \equiv I_{H_c} )</td>
</tr>
<tr>
<td>0x42</td>
<td>TIMESTAMP</td>
<td>0</td>
<td>1</td>
<td>Get the block’s timestamp.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>( \mu_s[0] \equiv I_{H_s} )</td>
</tr>
<tr>
<td>0x43</td>
<td>NUMBER</td>
<td>0</td>
<td>1</td>
<td>Get the block’s number.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>( \mu_s[0] \equiv I_{H_1} )</td>
</tr>
<tr>
<td>0x44</td>
<td>DIFFICULTY</td>
<td>0</td>
<td>1</td>
<td>Get the block’s difficulty.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>( \mu_s[0] \equiv I_{H_d} )</td>
</tr>
<tr>
<td>0x45</td>
<td>GASLIMIT</td>
<td>0</td>
<td>1</td>
<td>Get the block’s gas limit.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>( \mu_s[0] \equiv I_{H_1} )</td>
</tr>
</tbody>
</table>
### 50s: Stack, Memory, Storage and Flow Operations

<table>
<thead>
<tr>
<th>Value</th>
<th>Mnemonic</th>
<th>δ</th>
<th>α</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x50</td>
<td>POP</td>
<td>1</td>
<td>0</td>
<td>Remove item from stack.</td>
</tr>
</tbody>
</table>
| 0x51  | MLOAD    | 1 | 1 | Load word from memory.  
  \[
  \mu_s^0[0] \equiv \mu_s[0] \ldots (\mu_s[0] + 31)  
  \]
  \[
  \mu_i^1 \equiv \max(\mu_i, ([\mu_s[0] + 32] \div 32))  
  \]
  The addition in the calculation of \( \mu_i' \) is not subject to the \( 2^{256} \) modulo. |
| 0x52  | MSTORE   | 2 | 0 | Save word to memory.  
  \[
  \mu_s'[0] \equiv \mu_s[1]  
  \]
  \[
  \mu_i' \equiv \max(\mu_i, ([\mu_s[0] + 32] \div 32))  
  \]
  The addition in the calculation of \( \mu_i' \) is not subject to the \( 2^{256} \) modulo. |
| 0x53  | MSTORE8  | 2 | 0 | Save byte to memory.  
  \[
  \mu_s'[0] \equiv (\mu_s[1] \mod 256)  
  \]
  \[
  \mu_i' \equiv \max(\mu_i, ([\mu_s[0] + 1] \div 32))  
  \]
  The addition in the calculation of \( \mu_i' \) is not subject to the \( 2^{256} \) modulo. |
| 0x54  | SLOAD    | 1 | 1 | Load word from storage.  
  \[
  \sigma[I_a][\mu_s[0]]  
  \]
| 0x55  | SSTORE   | 2 | 0 | Save word to storage.  
  \[
  C_{\text{STORE}}(\sigma, \mu) \equiv \begin{cases}  
  G_{\text{set}} & \text{if } \mu_s[1] \neq 0 \land \sigma[I_a][\mu_s[0]] = 0 \\
  G_{\text{reset}} & \text{otherwise}  
  \end{cases}  
  \]
  \[
  A' = A + \begin{cases}  
  R_{\text{clear}} & \text{if } \mu_s[1] = 0 \land \sigma[I_a][\mu_s[0]] \neq 0 \\
  0 & \text{otherwise}  
  \end{cases}  
  \]
| 0x56  | JUMP     | 1 | 0 | Alter the program counter.  
  \[
  J_{\text{JUMP}}(\mu) \equiv \mu_s[0]  
  \]
  This has the effect of writing said value to \( \mu_{pc} \). See section 9. |
| 0x57  | JUMPI    | 2 | 0 | Conditionally alter the program counter.  
  \[
  J_{\text{JUMPI}}(\mu) \equiv \begin{cases}  
  \mu_s[0] & \text{if } \mu_s[1] \neq 0 \\
  \mu_{pc} + 1 & \text{otherwise}  
  \end{cases}  
  \]
  This has the effect of writing said value to \( \mu_{pc} \). See section 9. |
| 0x58  | PC       | 0 | 1 | Get the value of the program counter prior to the increment corresponding to this instruction.  
  \[
  \mu_s'[0] \equiv \mu_{pc}  
  \]
| 0x59  | MSIZE    | 0 | 1 | Get the size of active memory in bytes.  
  \[
  \mu_s'[0] \equiv 32\mu_s  
  \]
| 0x5a  | GAS      | 0 | 1 | Get the amount of available gas, including the corresponding reduction for the cost of this instruction.  
  \[
  \mu_s'[0] \equiv \mu_g  
  \]
| 0x5b  | JUMPDEST | 0 | 0 | Mark a valid destination for jumps.  
  This operation has no effect on machine state during execution. |
60s & 70s: Push Operations

<table>
<thead>
<tr>
<th>Value</th>
<th>Mnemonic</th>
<th>δ</th>
<th>α</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x60</td>
<td>PUSH1</td>
<td>0</td>
<td>1</td>
<td>Place 1 byte item on stack.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(\mu'<em>s[0] \equiv c(\mu</em>{pc} + 1))</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>where (c(x) \equiv \begin{cases} I_b[x] &amp; \text{if } x &lt; |I_b| \ 0 &amp; \text{otherwise} \end{cases})</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>The bytes are read in line from the program code's bytes array.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>The function (c) ensures the bytes default to zero if they extend past the limits.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>The byte is right-aligned (takes the lowest significant place in big endian).</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| 0x61  | PUSH2    | 0  | 1  | Place 2-byte item on stack. |
|       |          | \(\mu'_s[0] \equiv c((\mu_{pc} + 1) \ldots (\mu_{pc} + 2))\) |
|       |          | with \(c(x) \equiv c(x_0, \ldots, c(x_{x_{\|x\| - 1}}))\) with \(c\) as defined as above. |
|       |          | The bytes are right-aligned (takes the lowest significant place in big endian). |

| 0x7f  | PUSH32   | 0  | 1  | Place 32-byte (full word) item on stack. |
|       |          | \(\mu'_s[0] \equiv c((\mu_{pc} + 1) \ldots (\mu_{pc} + 32))\) |
|       |          | where \(c\) is defined as above. |
|       |          | The bytes are right-aligned (takes the lowest significant place in big endian). |

80s: Duplication Operations

<table>
<thead>
<tr>
<th>Value</th>
<th>Mnemonic</th>
<th>δ</th>
<th>α</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x80</td>
<td>DUP1</td>
<td>1</td>
<td>2</td>
<td>Duplicate 1st stack item.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(\mu'_s[0] \equiv \mu_s[0])</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| 0x81  | DUP2     | 2  | 3  | Duplicate 2nd stack item. |
|       |          | \(\mu'_s[0] \equiv \mu_s[1]\) |

| 0x8f  | DUP16    | 16 | 17 | Duplicate 16th stack item. |
|       |          | \(\mu'_s[0] \equiv \mu_s[15]\) |

90s: Exchange Operations

<table>
<thead>
<tr>
<th>Value</th>
<th>Mnemonic</th>
<th>δ</th>
<th>α</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x90</td>
<td>SWAP1</td>
<td>2</td>
<td>2</td>
<td>Exchange 1st and 2nd stack items.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(\mu'_s[0] \equiv \mu_s[1])</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(\mu'_s[1] \equiv \mu_s[0])</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| 0x91  | SWAP2    | 3  | 3  | Exchange 1st and 3rd stack items. |
|       |          | \(\mu'_s[0] \equiv \mu_s[2]\) |
|       |          | \(\mu'_s[2] \equiv \mu_s[0]\) |

| 0x9f  | SWAP16   | 17 | 17 | Exchange 1st and 17th stack items. |
|       |          | \(\mu'_s[0] \equiv \mu_s[16]\) |
|       |          | \(\mu'_s[16] \equiv \mu_s[0]\) |
a0s: Logging Operations

For all logging operations, the state change is to append an additional log entry on to the substate’s log series:

\[ \Delta A'_1 \equiv A_1 \cdot (l_a, t, \mu_0[0] \ldots (\mu_0[0] + \mu_0[1] - 1)) \]

and to update the memory consumption counter:

\[ \mu'_i \equiv M(\mu_i, \mu_s[0], \mu_s[1]) \]

The entry’s topic series, \( t \), differs accordingly:

<table>
<thead>
<tr>
<th>Value</th>
<th>Mnemonic</th>
<th>( \delta )</th>
<th>( \alpha )</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0xa0</td>
<td>LOG0</td>
<td>2</td>
<td>0</td>
<td>Append log record with no topics.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>( t \equiv () )</td>
</tr>
<tr>
<td>0xa1</td>
<td>LOG1</td>
<td>3</td>
<td>0</td>
<td>Append log record with one topic.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>( t \equiv (\mu_s[2]) )</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0xa4</td>
<td>LOG4</td>
<td>6</td>
<td>0</td>
<td>Append log record with four topics.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>( t \equiv (\mu_s[2], \mu_s[3], \mu_s[4], \mu_s[5]) )</td>
</tr>
</tbody>
</table>
Value | Mnemonic | δ | α | Description
--- | --- | --- | --- | ---
0xf0 | CREATE | 3 | 1 | Create a new account with associated code.

\[ i \equiv \mu_m[\mu_a[1] \ldots (\mu_a[1] + \mu_a[2] - 1)] \]

\[ (\sigma', \mu', A^+, o) \equiv \begin{cases} 
\{ \Theta(\sigma, I_n, I_o, L(\mu_a), I_p, \mu_a[0], i, I_o + 1, I_o) \} & \text{if } \mu_a[0] \leq \sigma[I_a]_b \\
(\sigma, \mu, \varnothing) & \text{otherwise}
\end{cases} \]

\[ \sigma' \equiv \sigma \begin{cases} \text{except } \sigma'[I_a]_b = \sigma[I_a]_b + 1 \\
\end{cases} \]

\[ A' \equiv A \cup A^+ \]

\[ n \equiv \min\{\{\mu_a[6], o\}\} \]

\[ \mu_m'[5] \ldots (\mu_a[5] + n - 1) = o[0 \ldots (n - 1)] \]

\[ \mu_a[0] = o \]

\[ \mu_a'[0] \equiv \mu_a[0] + g' \]

\[ A' \equiv A \cup A^+ \]

\[ t \equiv \mu_a[1] \mod 2^{160} \]

Note the change in the fourth parameter to the call \( \Theta \) from the 2nd stack value \( \mu_a[0] \) (as in CALL) to the present address \( I_a \). This means that the recipient is in fact the same account as at present, simply that the code is overwritten.

0xf1 | CALL | 7 | 1 | Message-call into an account.

\[ i \equiv \mu_m[\mu_a[3] \ldots (\mu_a[3] + \mu_a[4] - 1)] \]

\[ (\sigma', \mu', \mu_a', A^+, o) \equiv \begin{cases} 
\{ \Theta(\sigma, I_n, I_o, t, t, \text{CALLGAS}(\mu_a), \) & \text{if } \mu_a[2] \leq \sigma[I_a]_b \\
(\sigma, \mu, a, \varnothing, () & \text{otherwise}
\end{cases} \]

\[ n \equiv \min\{\{\mu_a[6] \ldots o\}\} \]

\[ \mu_a'[5] \ldots (\mu_a[5] + n - 1) = o[0 \ldots (n - 1)] \]

\[ \mu_a[0] = o \]

\[ \mu_a'[0] \equiv \mu_a[0] + g' \]

\[ A' \equiv A \cup A^+ \]

\[ t \equiv \mu_a[1] \mod 2^{160} \]

Thus the operand order is: value, input offset, input size.

0xf2 | CALLOCODE | 7 | 1 | Message-call into this account with an alternative account’s code.

Exactly equivalent to CALL except:

\[ (\sigma', \mu', A^+, o) \equiv \begin{cases} 
\{ \Theta(\sigma', I_n, I_o, t, t, \text{CALLGAS}(\mu_a), \} & \text{if } \mu_a[2] \leq \sigma[I_a]_b \\
(\sigma, \mu, \varnothing, () & \text{otherwise}
\end{cases} \]

Note the change in the fourth parameter to the call \( \Theta \) from the 2nd stack value \( \mu_a[0] \) (as in CALL) to the present address \( I_a \). This means that the recipient is in fact the same account as at present, simply that the code is overwritten.

0xf3 | RETURN | 2 | 0 | Halt execution returning output data.

\[ H_{\text{RETURN}}(\mu) \equiv \mu_m[\mu_a[0] \ldots (\mu_a[0] + \mu_a[1] - 1)] \]

This has the effect of halting the execution at this point with output defined.

See section 9.2.

\[ \mu_a' \equiv M(\mu_a(1), \mu_a[2]) \]

Thus the operand order is: value, input offset, input size.
0xf4 DELEGATECALL 6 1 Message-call into this account with an alternative account’s code, but
persisting the current values for sender and value.
Compared with CALL, DELEGATECALL takes one fewer arguments. The
omitted argument is μₐ[2]. As a result, μₐ[3], μₐ[4], μₐ[5] and μₐ[6] in the
definition of CALL should respectively be replaced with μₐ[2], μₐ[3], μₐ[4] and
μₐ[5]. Otherwise it is equivalent to CALL except:
\[
(σ', g', A', o) \equiv \begin{cases}
\Theta(σ, I_s, I_o, I_a, t) & \text{if } I_o \leq σ[I_s] \wedge I_o \leq 1024 \\
(I_o < 1024) & \text{otherwise}
\end{cases}
\]
Note the changes (in addition to that of the fourth parameter) to the second
and ninth parameters to the call Θ.
This means that the recipient is in fact the same account as at present, simply
that the code is overwritten and the context is almost entirely identical.

0xfa STATICCALL 6 1 Static message-call into an account.
Exactly equivalent to CALL except:
The argument μₐ[2] is replaced with 0.
The deeper argument μₐ[3], μₐ[4], μₐ[5] and μₐ[6] are respectively replaced with μₐ[2], μₐ[3], μₐ[4] and μₐ[5].
The last argument of Θ is ⊥.
For the gas calculation, we use the memory expansion function,
\[\mu' \equiv M(\mu, \mu[0], \mu[1])\]

0xfd REVERT 2 0 Halt execution reverting state changes but returning data and remaining gas.
The effect of this operation is described in (131).
For the gas calculation, we use the memory expansion function,
\[\mu' \equiv M(\mu, \mu[0], \mu[1])\]

0xff SELFDESTRUCT 1 0 Halt execution and register account for later deletion.
\[A'_s \equiv A_s \cup \{I_s\}\]
\[σ'[r] \equiv \begin{cases}
\emptyset & \text{if } σ[r] = \emptyset \land σ[I_s] = 0 \\
(σ[r]₀, σ[r]₁, σ[I_s], σ[r]₂, σ[r]₃) & \text{if } r ≠ I_s \\
(σ[r]₀, 0, σ[r]₂, σ[r]₃) & \text{otherwise}
\end{cases}\]
where \(r = μₐ[0] \mod 2^{160}\)
\[σ'[I_s] = 0\]
\[C_{SELFDESTRUCT}(σ, μ) \equiv G_{selfdestruct} + \begin{cases}
G_{newaccount} & \text{if } n \\
0 & \text{otherwise}
\end{cases}\]
\[n \equiv \text{DEAD}(σ, μ[0]) \mod 2^{160} \land σ[I_s] ≠ 0\]

APPENDIX I. GENESIS BLOCK

The genesis block is 15 items, and is specified thus:
\[(301) \quad (((0)_{256}, \text{KEC}(\text{RLP}(()))), (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0))\]

Where \(0_{256}\) refers to the parent hash, a 256-bit hash which is all zeroes; \(0_{160}\) refers to the beneficiary address, a 160-bit hash which is all zeroes; \(0_{2048}\) refers to the log blob, 2048-bit of all zeroes; \(2^{17}\) refers to the difficulty; the transaction trie root, receipt trie root, gas used, block number and extradata are both 0, being equivalent to the empty byte array. The sequences of both ommers and transactions are empty and represented by (). \text{KEC}((42)) refers to the Keccak hash of a byte array of length one whose first and only byte is of value 42, used for the nonce. \text{KEC}(\text{RLP}(())) value refers to the hash of the omer list in RLP, both empty lists.
The proof-of-concept series include a development premine, making the state root hash some value \textit{stateRoot}. Also \textit{time} will be set to the initial timestamp of the genesis block. The latest documentation should be consulted for those values.

APPENDIX J. ETHASH

J.1. Definitions. We employ the following definitions:
J.2. Size of dataset and cache. The size for Ethash's cache $c \in \mathcal{B}$ and dataset $d \in \mathcal{B}$ depend on the epoch, which in turn depends on the block number.

$$E_{\text{epoch}}(H_i) = \left\lfloor \frac{H_i}{J_{\text{epoch}}} \right\rfloor$$

The size of the dataset growth by $J_{\text{dataset growth}}$ bytes, and the size of the cache by $J_{\text{cache growth}}$ bytes, every epoch. In order to avoid regularity leading to cyclic behavior, the size must be a prime number. Therefore the size is reduced by a multiple of $J_{\text{mix bytes}}$, for the dataset, and $J_{\text{hash bytes}}$ for the cache. Let $d_{\text{size}} = ||d||$ be the size of the dataset. Which is calculated using

$$d_{\text{size}} = E_{\text{prime}}(J_{\text{dataset init}} + J_{\text{dataset growth}} \cdot E_{\text{epoch}} - J_{\text{mix bytes}}, J_{\text{mix bytes}})$$

The size of the cache, $c_{\text{size}}$, is calculated using

$$c_{\text{size}} = E_{\text{prime}}(J_{\text{cache init}} + J_{\text{cache growth}} \cdot E_{\text{epoch}} - J_{\text{hash bytes}}, J_{\text{hash bytes}})$$

$$E_{\text{prime}}(x, y) = \begin{cases} x & \text{if } x/y \in \mathbb{N} \\ E_{\text{prime}}(x - 2 \cdot y, y) & \text{otherwise} \end{cases}$$

J.3. Dataset generation. In order to generate the dataset we need the cache $c$, which is an array of bytes. It depends on the cache size $c_{\text{size}}$ and the seed hash $s \in \mathcal{B}_{32}$.

J.3.1. Seed hash. The seed hash is different for every epoch. For the first epoch it is the Keccak-256 hash of a series of 32 bytes of zeros. For every other epoch it is always the Keccak-256 hash of the previous seed hash:

$$s = C_{\text{seed hash}}(H_i)$$

$$C_{\text{seed hash}}(H_i) = \begin{cases} 0_{32} & \text{if } E_{\text{epoch}}(H_i) = 0 \\ \text{KEC}(C_{\text{seed hash}}(H_i - J_{\text{epoch}})) & \text{otherwise} \end{cases}$$

With $0_{32}$ being 32 bytes of zeros.

J.3.2. Cache. The cache production process involves using the seed hash to first sequentially filling up $c_{\text{size}}$ bytes of memory, then performing $J_{\text{cacherounds}}$ passes of the RandMemoHash algorithm created by [Lerner, 2014]. The initial cache $c'$, being an array of arrays of single bytes, will be constructed as follows.

We define the array $c_i$, consisting of 64 single bytes, as the $i$th element of the initial cache:

$$c_i = \begin{cases} \text{KEC12}(s) & \text{if } i = 0 \\ \text{KEC12}(c_{i-1}) & \text{otherwise} \end{cases}$$

Therefore $c'$ can be defined as

$$c'[i] = c_i \quad \forall \quad i < n$$

$$n = \left\lfloor \frac{c_{\text{size}}}{J_{\text{hash bytes}}} \right\rfloor$$

The cache is calculated by performing $J_{\text{cacherounds}}$ rounds of the RandMemoHash algorithm to the initial cache $c'$:

$$c = E_{\text{cacherounds}}(c', J_{\text{cacherounds}})$$

$$E_{\text{cacherounds}}(x, y) = \begin{cases} x & \text{if } y = 0 \\ E_{\text{RMH}}(x) & \text{if } y = 1 \\ E_{\text{cacherounds}}(E_{\text{RMH}}(x), y - 1) & \text{otherwise} \end{cases}$$

Where a single round modifies each subset of the cache as follows:

$$E_{\text{RMH}}(x) = (E_{\text{rmh}}(x, 0), E_{\text{rmh}}(x, 1), ..., E_{\text{rmh}}(x, n - 1))$$
(314) \( E_{\text{rmh}}(x, i) = \text{KEC512}(x'[i-1+n] \mod n | x'[i]0 | \mod n) \)

with \( x' = x \) except \( x'[j] = E_{\text{rmh}}(x, j) \) \( \forall \ j < i \)

### 3.3. Full dataset calculation.

Essentially, we combine data from \( J_{\text{parents}} \) pseudorandomly selected cache nodes, and hash that to compute the dataset. The entire dataset is then generated by a number of items, each \( J_{\text{hashbytes}} \) bytes in size:

(315) \( d[i] = E_{\text{datasetitem}}(c, i) \) \( \forall \ i < \frac{d_{\text{size}}}{J_{\text{hashbytes}}} \)

In order to calculate the single item we use an algorithm inspired by the FNV hash (Glenn Fowler [1991]) in some cases as a non-associative substitute for XOR.

(316) \( E_{\text{FNV}}(x, y) = (x \cdot (0x01000193 \oplus y)) \mod 2^{32} \)

The single item of the dataset can now be calculated as:

(317) \( E_{\text{datasetitem}}(c, i) = E_{\text{parents}}(c, i, -1, 0) \)

(318) \( E_{\text{parents}}(c, i, p, m) = \begin{cases} E_{\text{parents}}(c, i, p+1, E_{\text{mix}}(m, c, i, p+1)) & \text{if } p < J_{\text{parents}} - 2 \\ E_{\text{mix}}(m, c, i, p+1) & \text{otherwise} \end{cases} \)

(319) \( E_{\text{mix}}(m, c, i, p) = \begin{cases} \text{KEC512}(c[i] \mod c_{\text{size}} | i) \oplus i & \text{if } p < 0 \\ E_{\text{FNV}}(m[c], E_{\text{FNV}}(c+1, m)) \mod \left( J_{\text{hashbytes}} / J_{\text{wordbytes}} \right) \mod c_{\text{size}} & \text{otherwise} \end{cases} \)

### 3.4. Proof-of-work function.

Essentially, we maintain a “mix” \( J_{\text{mixbytes}} \) bytes wide, and repeatedly sequentially fetch \( J_{\text{mixbytes}} \) bytes from the full dataset and use the \( E_{\text{FNV}} \) function to combine it with the mix. \( J_{\text{mixbytes}} \) bytes of sequential access are used so that each round of the algorithm always fetches a full page from RAM, minimizing translation lookaside buffer misses which ASICs would theoretically be able to avoid.

If the output of this algorithm is below the desired target, then the nonce is valid. Note that the extra application of KECC at the end ensures that there exists an intermediate nonce which can be provided to prove that at least a small amount of work was done; this quick out PoW verification can be used for anti-DDoS purposes. It also serves to provide statistical assurance that the result is an unbiased, 256 bit number.

The PoW-function returns an array with the compressed mix as its first item and the Keccak-256 hash of the concatenation of the compressed mix with the seed hash as the second item:

(320) \( \text{PoW}(H_H, H_n, d) = \{m, (\text{KEC}(RLP(L_H(H_H))), H_n, d); \text{KEC}(s_0(\text{KEC}(RLP(L_H(H_H))), H_n) + m, (\text{KEC}(RLP(L_H(H_H))), H_n, d))\} \)

With \( H_H \) being the hash of the header without the nonce. The compressed mix \( m_c \) is obtained as follows:

(321) \( m_c(h, n, d) = E_{\text{compress}}(E_{\text{accesses}}(d, \sum_{i=0}^{n_{\text{mix}}} s_h(h, n), s_0(h, n), -1), -4) \)

The seed hash being:

(322) \( s_h(h, n) = \text{KEC512}(h + E_{\text{revert}}(n)) \)

\( E_{\text{revert}}(n) \) returns the reverted bytes sequence of the nonce \( n \):

(323) \( E_{\text{revert}}(n)[i] = n[[n] - i] \)

We note that the “+” operator between two byte sequences results in the concatenation of both sequences.

The dataset \( d \) is obtained as described in section 3.3.3.

The number of replicated sequences in the mix is:

(324) \( n_{\text{mix}} = \left\lfloor J_{\text{mixbytes}} / J_{\text{hashbytes}} \right\rfloor \)

In order to add random dataset nodes to the mix, the \( \text{Eaccesses} \) function is used:

(325) \( \text{Eaccesses}(d, m, s, i) = \begin{cases} \text{Emixdataset}(d, m, s, i) & \text{if } i = J_{\text{accesses}} - 2 \\ \text{Eaccesses}(\text{Emixdataset}(d, m, s, i), s, i + 1) & \text{otherwise} \end{cases} \)

(326) \( \text{Emixdataset}(d, m, s, i) = E_{\text{FNV}}(m, \text{Enewdata}(d, m, s, i)) \)

\( E_{\text{newdata}} \) returns an array with \( n_{\text{mix}} \) elements:

(327) \( E_{\text{newdata}}(d, m, s, i)[j] = d[E_{\text{FNV}}(i + s[0], m[j] \mod J_{\text{mixbytes}}) \mod \left( J_{\text{hashbytes}} / n_{\text{mix}} \right) \cdot n_{\text{mix}} + j] \) \( \forall \ j < n_{\text{mix}} \)

The mix is compressed as follows:

(328) \( E_{\text{compress}}(m, i) = \begin{cases} m & \text{if } i \geq n_{\text{mix}} - 8 \\ E_{\text{compress}}(E_{\text{FNV}}(E_{\text{FNV}}(m[i + 4], m[i + 5]), m[i + 6]), m[i + 7]), i + 8) & \text{otherwise} \end{cases} \)
Appendix K. Anomalies on the Main Network

K.1. Deletion of an Account Despite Out-of-gas. At block 2675119, in the transaction 0xcf416c536ec1a19ed1fb89e4ec7ff3cf73aa413b3aa9b77d60e4fd81a4296ba, an account at address 0x03 was called and an out-of-gas occurred during the call. Against the equation (195), this added 0x03 in the set of touched addresses, and this transaction turned $\sigma[0x03]$ into $\emptyset$.

Appendix L. List of mathematical symbols

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Latex Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\bigvee$</td>
<td>\texttt{\bigvee}</td>
<td>This is the least upper bound, supremum, or join of all elements operated on. Thus it is the greatest element of such elements (Davey and Priestley (2002)).</td>
</tr>
</tbody>
</table>