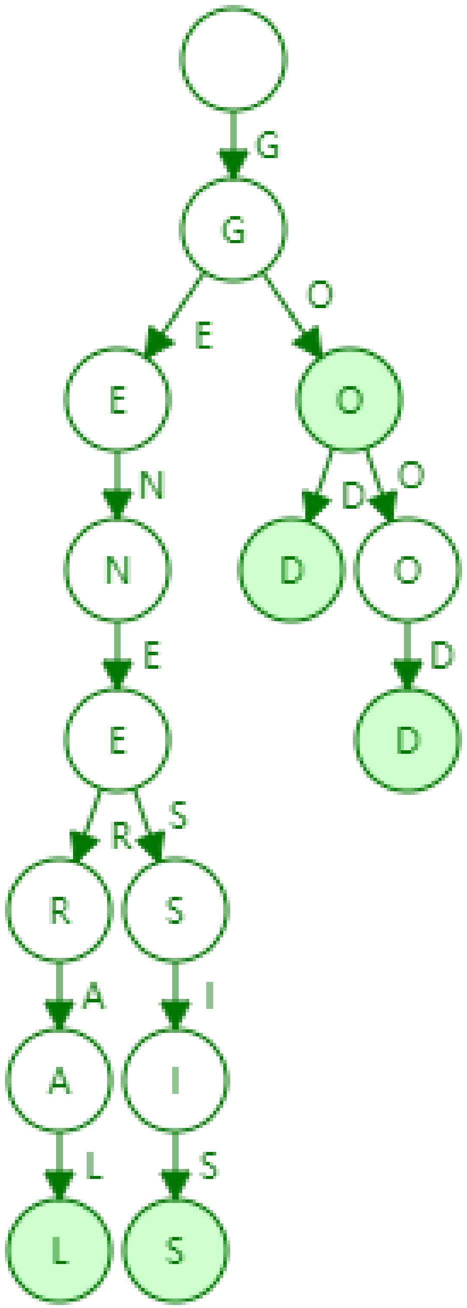
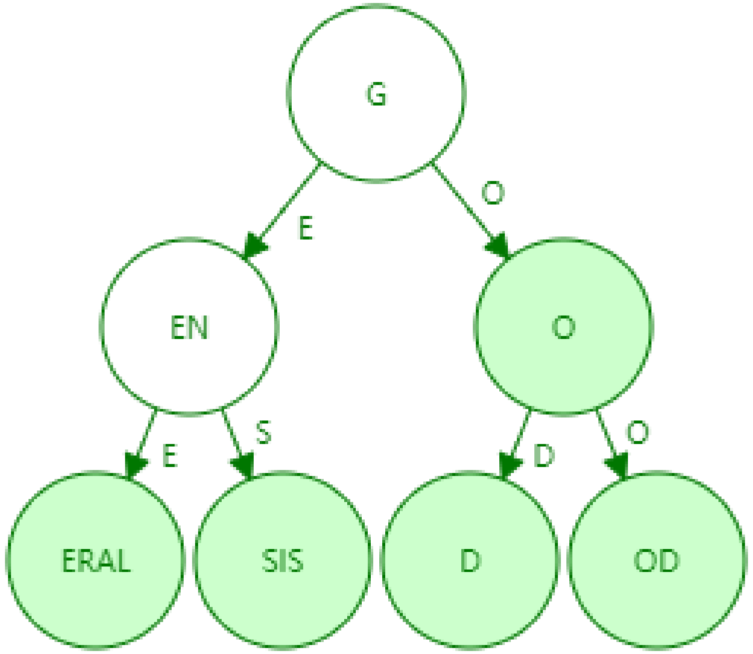
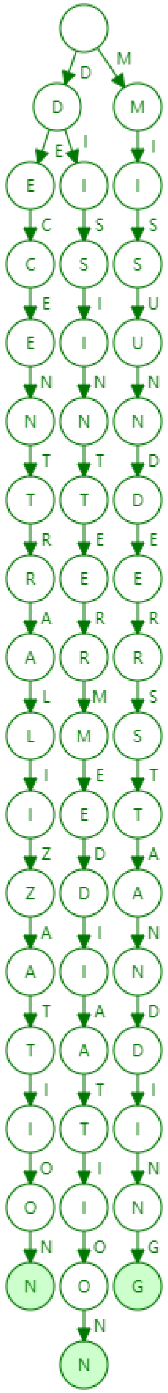


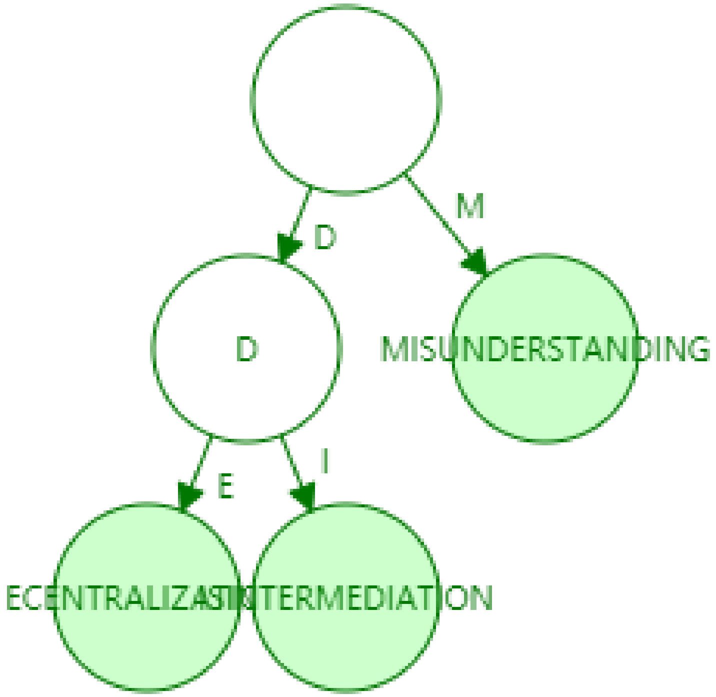
General
Genesis
Go
God
Good



General
Genesis
Go
God
Good



Misunderstanding
Decentralization
Disintermediation



Misunderstanding
Decentralization
Disintermediation

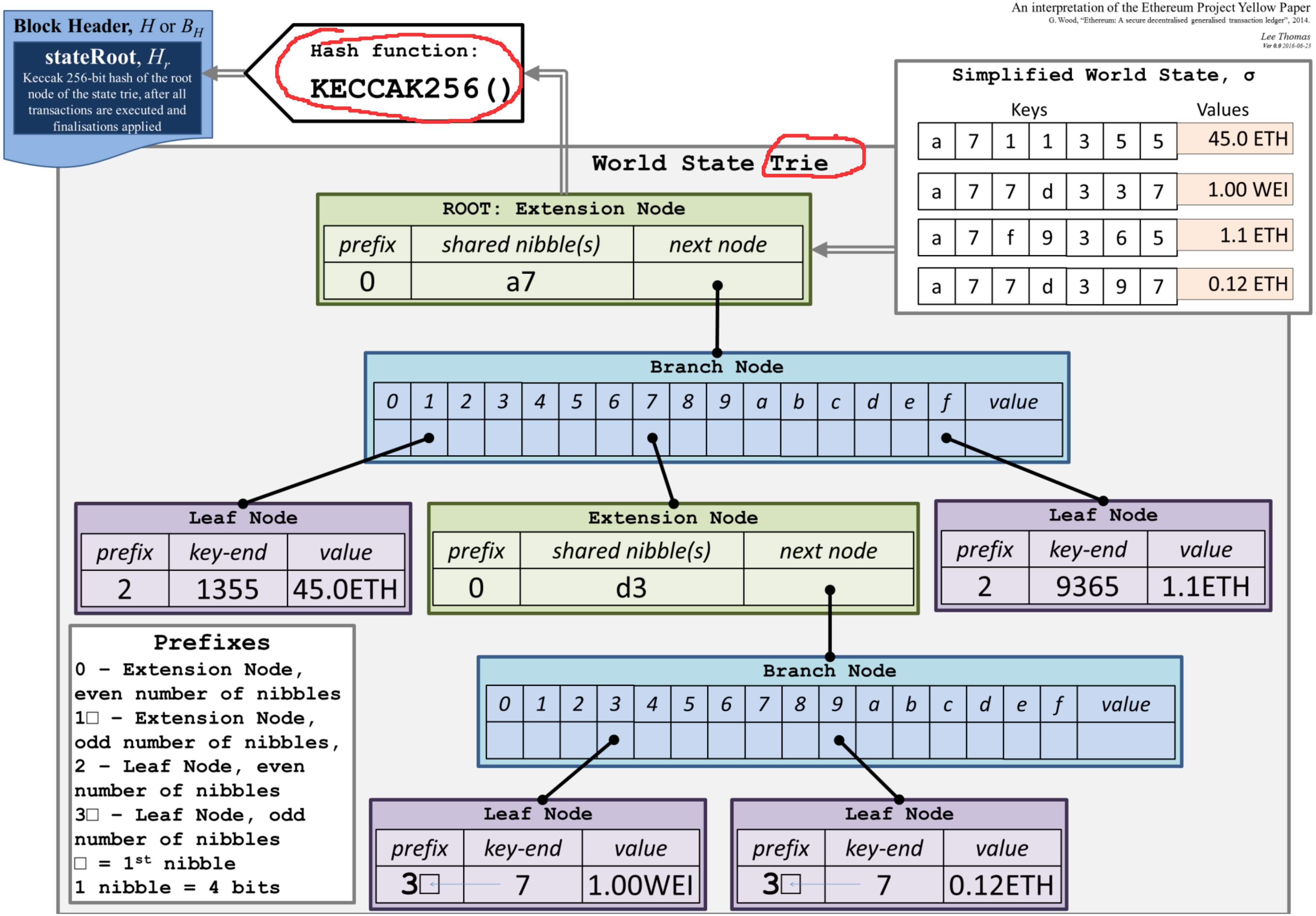
Ethereum Modified Merkle-Paricia-Trie System

An interpretation of the Ethereum Project Yellow Paper

G. Wood, "Ethereum: A secure decentralised generalised transaction ledger", 2014.

Lee Thomas

Ver 0.0 2016-06-23



Block Header, H or B_H

stateRoot, H_r

Keccak 256-bit hash of the root node of the state trie, after all transactions are executed and finalisations applied

Hash function:

KECCAK256()

World State Trie

Simplified World State, σ

Keys							Values
a	7	1	1	3	5	5	45.0 ETH
a	7	7	d	3	3	7	1.00 WEI
a	7	f	9	3	6	5	1.1 ETH
a	7	7	d	3	9	7	0.12 ETH

ROOT: Extension Node

prefix	shared nibble(s)	next node
0	a7	●

Branch Node

0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f	value
	●						●								●	

Leaf Node

prefix	key-end	value
2	1355	45.0ETH

Extension Node

prefix	shared nibble(s)	next node
0	d3	●

Leaf Node

prefix	key-end	value
2	9365	1.1ETH

Branch Node

0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f	value
			●						●							

Leaf Node

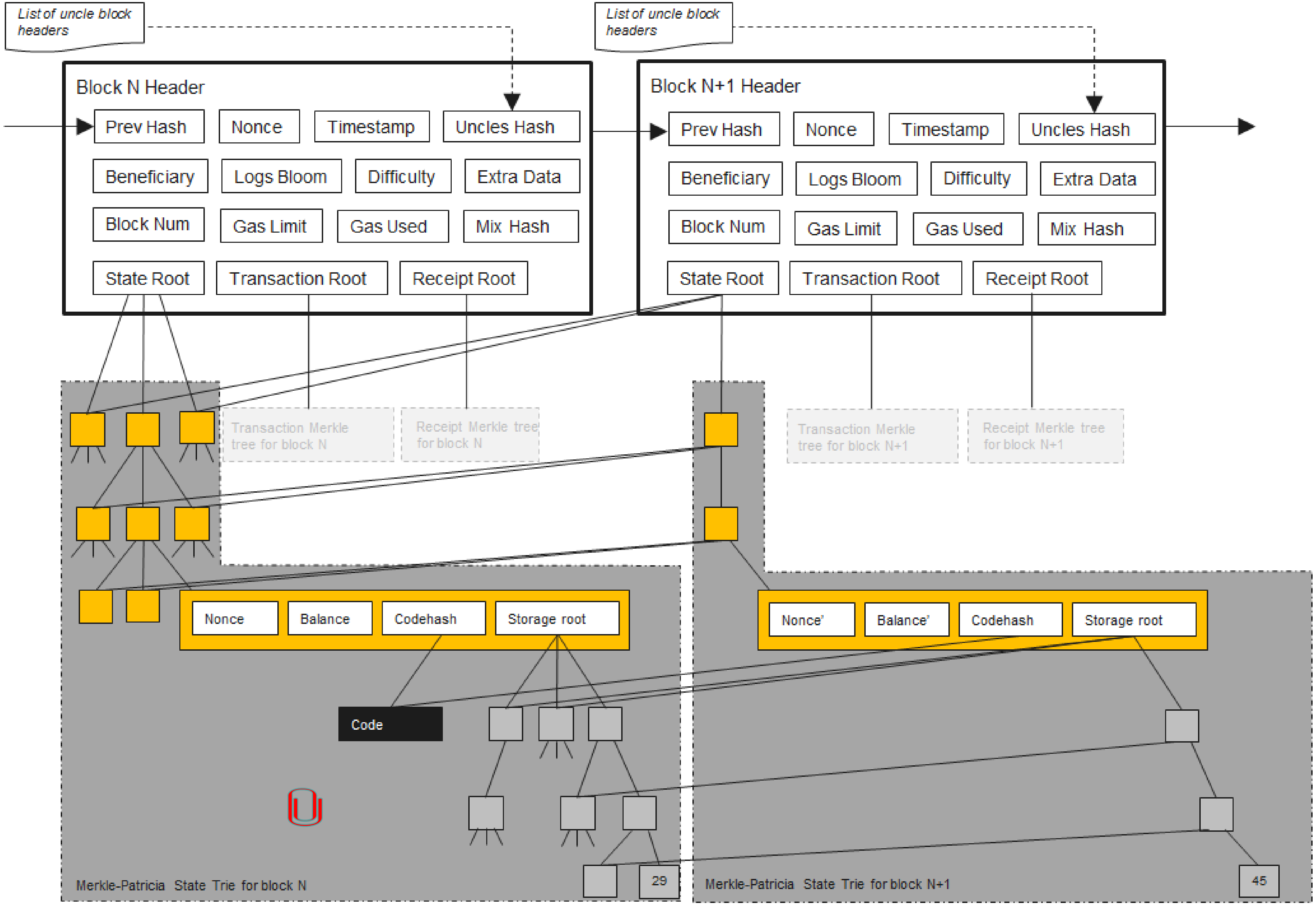
prefix	key-end	value
3□	7	1.00WEI

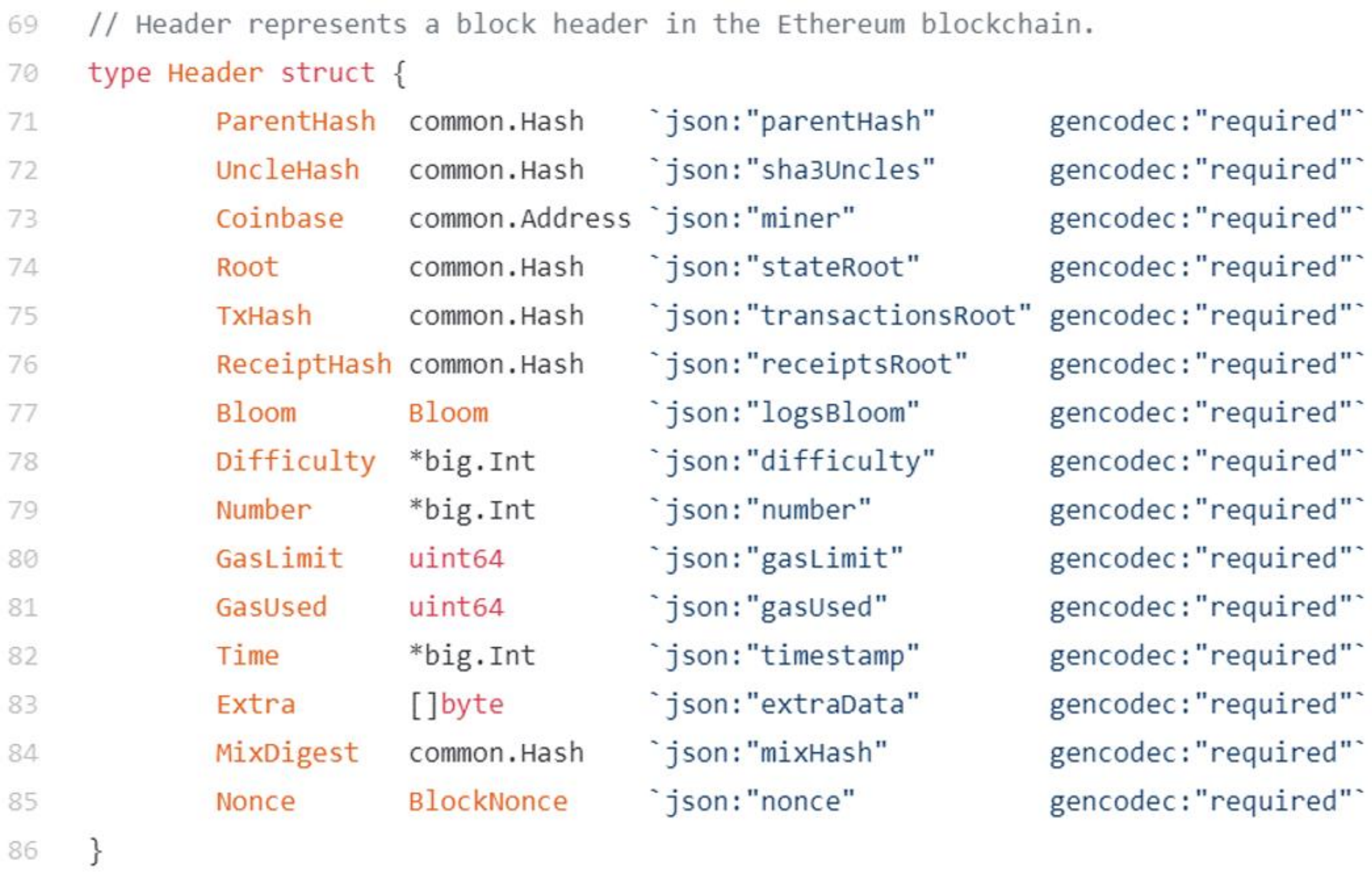
Leaf Node

prefix	key-end	value
3□	7	0.12ETH

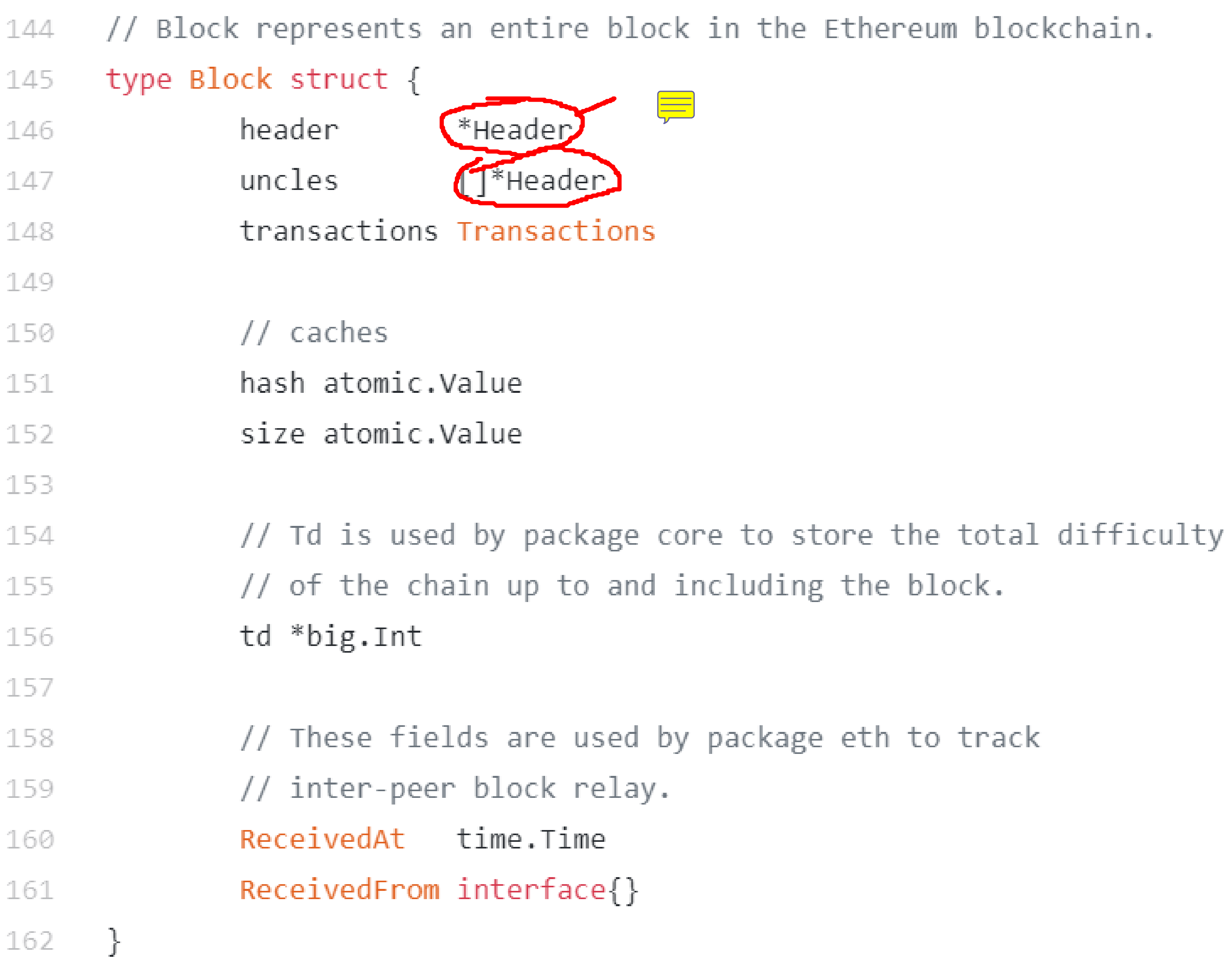
Prefixes

0 – Extension Node, even number of nibbles
1□ – Extension Node, odd number of nibbles,
2 – Leaf Node, even number of nibbles
3□ – Leaf Node, odd number of nibbles
□ = 1st nibble
1 nibble = 4 bits


List of uncle block headers
List of uncle block headers
Block N Header
Prev Hash
Nonce
Timestamp
Uncles Hash
Beneficiary
Logs Bloom
Difficulty
Extra Data
Block Num
Gas Limit
Gas Used
Mix Hash
State Root
Transaction Root
Receipt Root
Block N+1 Header
Prev Hash
Nonce
Timestamp
Uncles Hash
Beneficiary
Logs Bloom
Difficulty
Extra Data
Block Num
Gas Limit
Gas Used
Mix Hash
State Root
Transaction Root
Receipt Root
Transaction Merkle tree for block N
Receipt Merkle tree for block N
Transaction Merkle tree for block N+1
Receipt Merkle tree for block N+1
Nonce
Balance
Codehash
Storage root
Nonce'
Balance'
Codehash
Storage root
Code
29
45
Merkle-Patricia State Trie for block N
Merkle-Patricia State Trie for block N+1



```go
// Header represents a block header in the Ethereum blockchain.
type Header struct {
	ParentHash  common.Hash    `json:"parentHash"       gencodec:"required"`
	UncleHash   common.Hash    `json:"sha3Uncles"       gencodec:"required"`
	Coinbase    common.Address `json:"miner"            gencodec:"required"`
	Root        common.Hash    `json:"stateRoot"        gencodec:"required"`
	TxHash      common.Hash    `json:"transactionsRoot" gencodec:"required"`
	ReceiptHash common.Hash    `json:"receiptsRoot"     gencodec:"required"`
	Bloom       Bloom          `json:"logsBloom"        gencodec:"required"`
	Difficulty  *big.Int       `json:"difficulty"       gencodec:"required"`
	Number      *big.Int       `json:"number"           gencodec:"required"`
	GasLimit    uint64         `json:"gasLimit"         gencodec:"required"`
	GasUsed     uint64         `json:"gasUsed"          gencodec:"required"`
	Time        *big.Int       `json:"timestamp"        gencodec:"required"`
	Extra       []byte         `json:"extraData"        gencodec:"required"`
	MixDigest   common.Hash    `json:"mixHash"          gencodec:"required"`
	Nonce       BlockNonce     `json:"nonce"            gencodec:"required"`
}
```

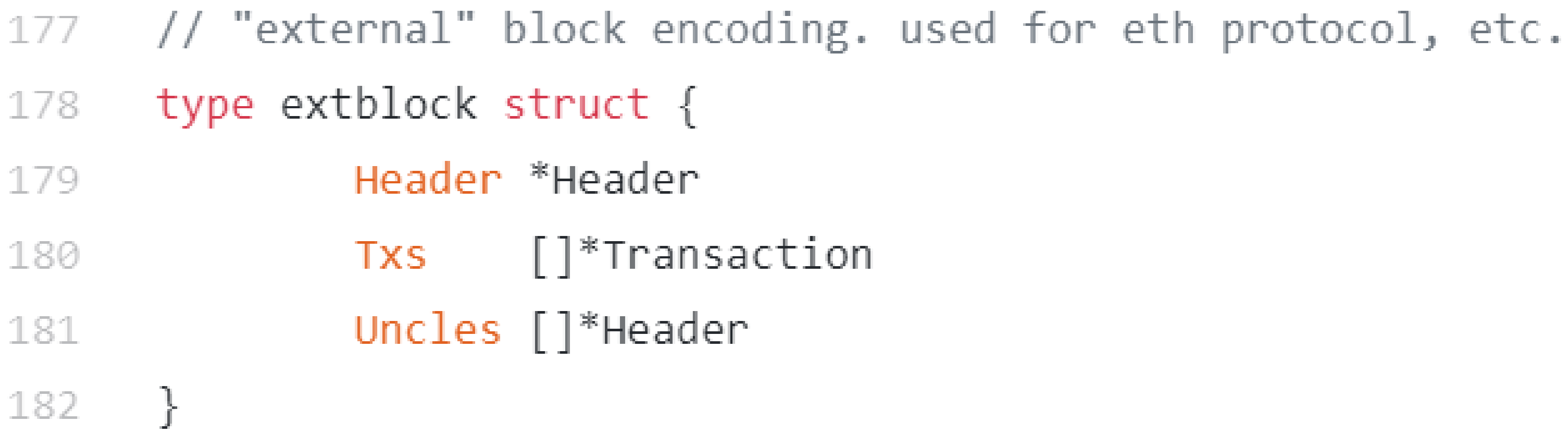


```
// Block represents an entire block in the Ethereum blockchain.
type Block struct {
        header       *Header
        uncles       []*Header
        transactions Transactions

        // caches
        hash atomic.Value
        size atomic.Value

        // Td is used by package core to store the total difficulty
        // of the chain up to and including the block.
        td *big.Int

        // These fields are used by package eth to track
        // inter-peer block relay.
        ReceivedAt   time.Time
        ReceivedFrom interface{}
}
```



```go
// "external" block encoding. used for eth protocol, etc.
type extblock struct {
	Header *Header
	Txs    []*Transaction
	Uncles []*Header
}
```