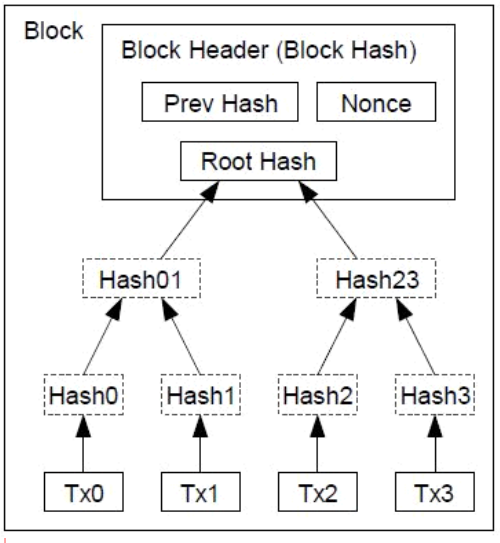
Gruodžio 3 d.: A. Michalkovič paskaita Post-Kvantinė kriptografija.
Gruodžio 10 d.: Stendinių pranešimų gynimas.
Gruodžio 17 d.: Stendinių pranešimų gynimas.
https://docs.google.com/document/d/1IPzwEVVmvnObQoJPRP9GDUiHccEGWgMw/edit?usp=sharing&ouid=111502255533491874828&rtpof=true&sd=true

https://docs.google.com/document/d/1Bp8NW2e4AbIsZ5UuBqa8BxkK6py01rjV/edit?usp=sharing&ouid=111502255533491874828&rtpof=true&sd=true

Merkle Tree



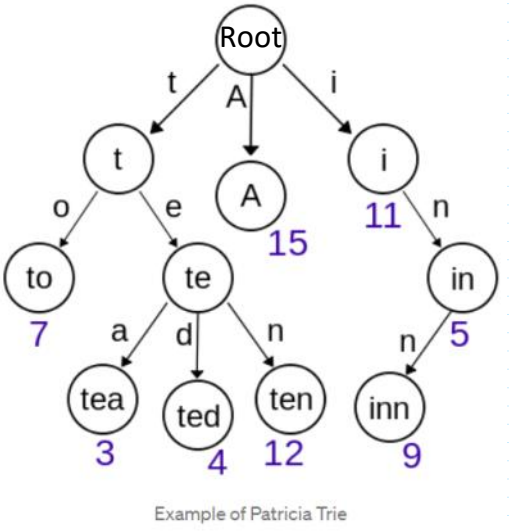
L0: 2^0=1

L1: 2^1=2

L2: 2^2=4

L10: 2^{10}=1024

Merkle Patricia Trie: Trie-Retrieve



Example of Patricia Trie

tricia-trie-how-ethereum-saves-a-state-e6d7555078dd

https://medium.com/codechain/modified-merkle-pa

Ethereum Yellow Paper Walkthrough (2/7) (lucassaldanha.com)

Merkle Tree and Ethereum Objects - Ethereum Yellow Paper Walkthrough (2/7)

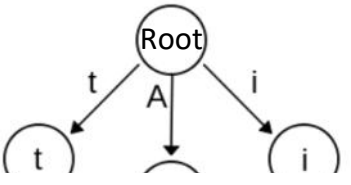


Lucas Saldanha
11 Dec 2018 • 11 min read
This is another post in our series exploring the Ethereum Yellow Paper. In this post, we will learn more about the main objects in Ethereum and their role. We'll also briefly discuss how Merkle trees are used in Ethereum.
(DISCLAIMER: this post is based on the Byzantium version of the Yellow Paper, version e94ebda from 5th June 2018)

https://medium.com/codechain/modified-merkle-patricia-trie-how-ethereum-saves-a-state-e6d7555078dd

Modified Merkle Patricia Trie (a.k.a MPT) as the method to save Ethereum state.
Basically, MPT is a combination of Patricia trie and Merkle tree, with few additional optimizations that fit the characteristics of Ethereum. Thus, an understanding of the Patricia trie and Merkle tree should precede the understanding

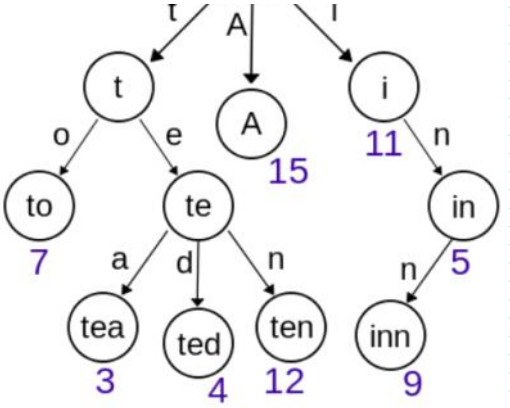
Trie <-- Retrieve



tree, with few additional optimizations that fit the characteristics of Ethereum. Thus, an understanding of the Patricia trie and Merkle tree should precede the understanding of MPT.

Patricia Trie

Patricia trie is a data structure which is also called Prefix tree, radix tree or trie. Trie uses a key as a path so the nodes that share the same prefix can also share the same path. This structure is fastest at finding common prefixes, simple to implement, and requires small memory. Thereby, it is commonly used for implementing routing tables, systems that are used in low specification machines like the router.

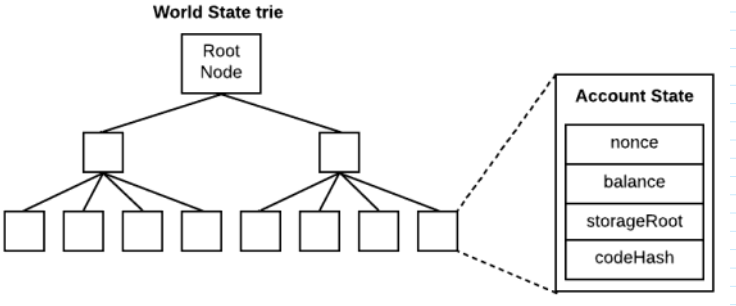


Example of Patricia Trie

World State

The **world state is a mapping between addresses (accounts) and account states**. The world state is not stored on the blockchain but the Yellow Paper states it is expected implementations store this data in a trie (also referred as the state database or state trie).The world state can be seen as the global state that is constantly updated by transaction executions. If you remember the discussion in the first post of the series about the Ethereum network being like a decentralized computer, the world state is considered this computer's hard drive.

All the information about Ethereum accounts live in the world state and is stored in the world state trie. If you want to know the balance of an account, or the current state of a smart contract, you query the world state trie to retrieve the account state of that account. We'll describe how this data is stored shortly.



World state trie and Account storage

EVM - Ethereum Vrtual Mashine

Account State

In Ethereum, there are two types of accounts: **External Owned Accounts** (**EOA**) and **Contract Accounts**. An EOA account is the account that you and I would have, that we can use to send Ether to one another and deploy smart contracts. A contract account is the account that is created when a smart contract is deployed. Every smart contract has its own Ethereum account.

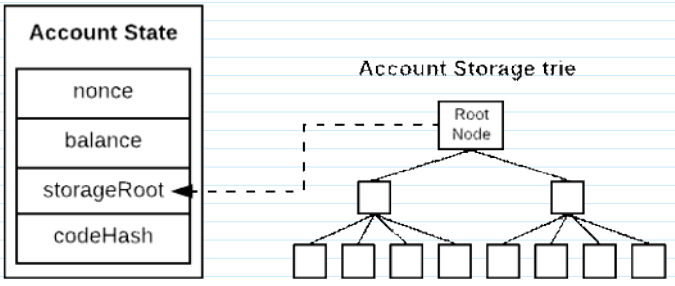
The account state contains information about an Ethereum account. For example, it stores how much Ether an account has and the number of transactions sent by the account. Each account has an account state. Let's take a look into each one of the fields in the account state:

- **nonce**
- Number of transactions sent from this address (if this is an External Owned Account - EOA) or the number of contract-creations made by this account (don't worry about what *contract-creations* means for now).
- **balance**
- Total Ether (in Wei) owned by this account.

1 Eth = 10^{18} Wei

- **storageRoot**
- Hash of the root node of the account storage trie (we'll see what the account storage is in a moment).
- **codeHash**
- For **contract accounts**, hash of the **EVM** code of this account. For EOAs, this will be empty.

One important details about the account state is that **all fields (except the codeHash) are mutable**. For example, when one account sends some Ether to another, the nonce will be incremented and the balance will be updated to reflect the new balance.
One of the consequences of the codeHash being immutable is that if you deploy a contract with a bug, you can't update the same contract. You need to deploy a new contract (the buggy version will be available forever). This is why it is important to use Truffle to develop and test your smart contracts and follow the best practices when working with Solidity.
The **Account Storage trie is where the data associated with an account is stored**. ~~This is only relevant for Contract Accounts, as for EOAs the storageRoot is empty and the codeHash is the hash of an empty string~~. All smart contract data is persisted in the account storage trie as a mapping between 32-bytes integers. We won't discuss in details how the contract data is persisted in the account state trie. If you really want to learn about the internals, I suggest reading this post. The hash of an account storage root node is persisted in the storageRoot field in the account state of the respective account.



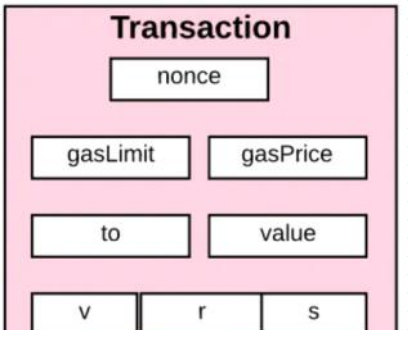
Account state and Account Storage trie

Transaction

T**ransactions are what makes the state change from the current state to the next state**. In Ethereum, we have three types of transactions:

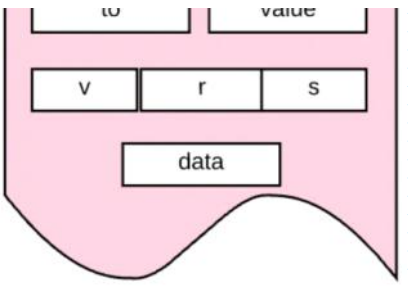
1. Transactions that **transfer value** between two **EOAs** (e.g, change the sender and receiver account balances)
2. Transactions that **send a message call** to a contract (e.g, set a value in the smart contract by sending a message call that executes a setter method)
3. Transactions that **deploy a contract** (therefore, create an account, the contract account)

(technically, types 1 and 2 are the same... transactions that send message



3. Transactions that **deploy a contract** (therefore, create an account, the contract account)

(technically, types 1 and 2 are the same... transactions that send message calls that affect an account state, either EOA or contract accounts. But is it easier to think about them as three different types)



These are the fields of a transaction:

- **nonce**
- Number of transactions sent by the account that created the transaction.
- **gasPrice**
- Value (in Wei) that will be paid per unit of gas for the computation costs of executing this transaction (in the case of PoW - Proof of Work).
- **gasLimit**
- Maximum amount of gas to be used while executing this transaction.
- **to**
- If this transaction is transfering Ether, address of the **EOA** account that will receive a value transfer.
- If this transaction is sending a message to a contract (e.g, calling a method in the smart contract), this is address of the contract.
- If this transactions is creating a contract, this value is always empty.
- **value**
- If this transaction is transfering Ether, amount in Wei that will be transferred to the recipient account.
- If this transaction is sending a message to a contract, amount of Wei payable by the smart contract receiving the message.
- If this transaction is creating a contract, this is the amount of Wei that will be added to the balance of the created contract.
- **v, r, s**
- Values used in the cryptographic signature of the transaction used to determine the sender of the transaction.
- **data** (only for value transfer and sending a message call to a smart contract)
- Input data of the message call (e.g, imagine you are trying to execute a setter method in your smart contract, the data field would contain the identifier of the setter method and the value that should be passed as parameter).
- **init** (only for contract creation)
- The **EVM**-code utilized for initialization of the contract.

Don't try to grasp all of this at once... Some fields like the *data* field or the *init* field require you to have a deeper understanding of the internals of Ethereum to really understand what they mean and how to use them. This is not the time to deeply understand any of these fields.

Not surprisingly, all transactions in a block are stored in a trie. And the root hash of this trie is stored in the... block header! Let's take a look into the anatomy of an Ethereum block.

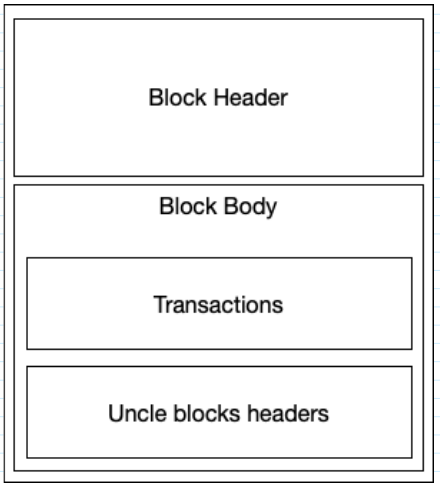
Block

The block header is divided in two parts, the **block header** and the **block body**.

The block header is the blockchain part of Ethereum. This is the structure that contains the hash of its predecessor block (also known as parent block), building a cryptographically guaranteed chain.

The block body contains a **list of transactions** that have been included in

this block and a **list of uncle (ommer) blocks headers** (if you want to know more about uncle blocks I recommend this post).



A high level diagram of the Ethereum block

Fields in the block header:

- **parentHash**
- Hash of the block header from the previous block. Each block contains a hash of the previous block, all the way to the first block in the chain. This is how all the data is protected against modifications (any modification in a previous block would change the hash of all blocks after the modified block).
- **ommersHash**
- Hash of the uncle blocks headers part of the block body.
- **beneficiary**
- Ethereum account that will get fees for mining this block.
- **stateRoot**
- Hash of the root node of the world state trie (after all transactions are executed).
- **transactionsRoot**
- Hash of the root node of the transactions trie. This trie contains all transactions in the block body.
- **receiptsRoot**
- Every time a transactions is executed, Ethereum generates a transaction receipt that contains information about the transaction execution. This field is the hash of the root node of the transactions receipt trie.
- **logsBloom**
- Bloom filter that can be used to find out if logs were generated on transactions in this block (if you want more details check this Stack Overflow answer). This avoids storing of logs in the block (saving a lot of space).
- **difficulty**
- In the case of PoW paradigm. Difficulty level of this block. This is a measure of how hard it was to mine this block (I'm not diving into the details of how this is calculated in this post).
- **number**
- Number of ancestor blocks. This represents the height of the chain (how

many blocks are in the chain). The genesis block has number zero.

- **gasLimit**
- Each transaction consumes gas. The gas limit specifies the maximum gas that can be used by the transactions included in the block. It is a way to limit the number of transactions in a block.
- **gasUsed**
- Sum of the gas cost of each transaction in the block.
- **timestamp**
- Unix timestamp when the block was created. Note that due to the decentralized nature of Ethereum, we can't trust in this value (specially when implementing smart contracts that have time related business logic).
- **extraData**
- Arbitrary byte array that can contain anything. When a miner is creating the block, it can choose to add anything in this field.
- **mixHash**
- Hash used to verify that a block has been mined properly (if you want to really understand this, read about the Ethash proof-of-work function).
- **nonce**
- Same as the mixHash, this value is used to verify that a block has been mined properly.

1 Eth = 10^{18} Wei

Conclusion

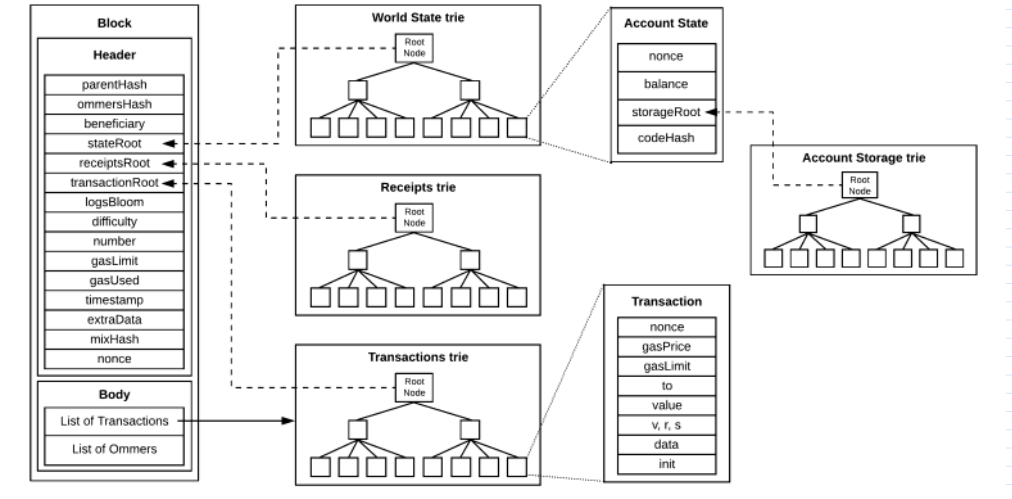
Basically, Ethereum has 4 types of tries:

1. **The world state trie contains the mapping between addresses and account states**. The hash of the root node of the world state trie is included in a block (in the **stateRoot** field) to represent the current state when that block was created. We only have one world state trie.
2. **The account storage trie contains the data associated to a smart contract**. The hash of the root node of the Account storage trie is included in the sccount state (in the **storageRoot** field). We have one Account storage trie for each account.
3. **The transaction trie contains all the transactions included in a block**. The hash of the root node of the Transaction trie is included in the block header (in the **transactionsRoot** field). We have one transaction trie per block.
4. **The transaction receipt trie contains all the transaction receipts for the transactions included in a block**. The hash of the root node of the transaction receipts trie is included in also included in the block header (in the **receiptsRoot** field); We have one transaction receipts trie per block.

And the objects that we discussed today are:

1. **World state**: the hard drive of the distributed computer that is Ethereum. It is a mapping between addresses and account states.
2. **Account state**: stores the state of each one of Ethereum's accounts. It also contains the storageRoot of the account state trie, that contains the storage data for the account.
3. **Transaction**: represents a state transition in the system. It can be a funds transfer, a message call or a contract deployment.
4. **Block**: contains the link to the previous block (parentHash) and contains a group of transactions that, when executed, will yield the new state of the system. It also contains the **stateRoot**, the **transactionRoot** and the **receiptsRoot**, the hash of the root nodes of the world state trie, the transaction trie and the transaction receipts trie, respectively.

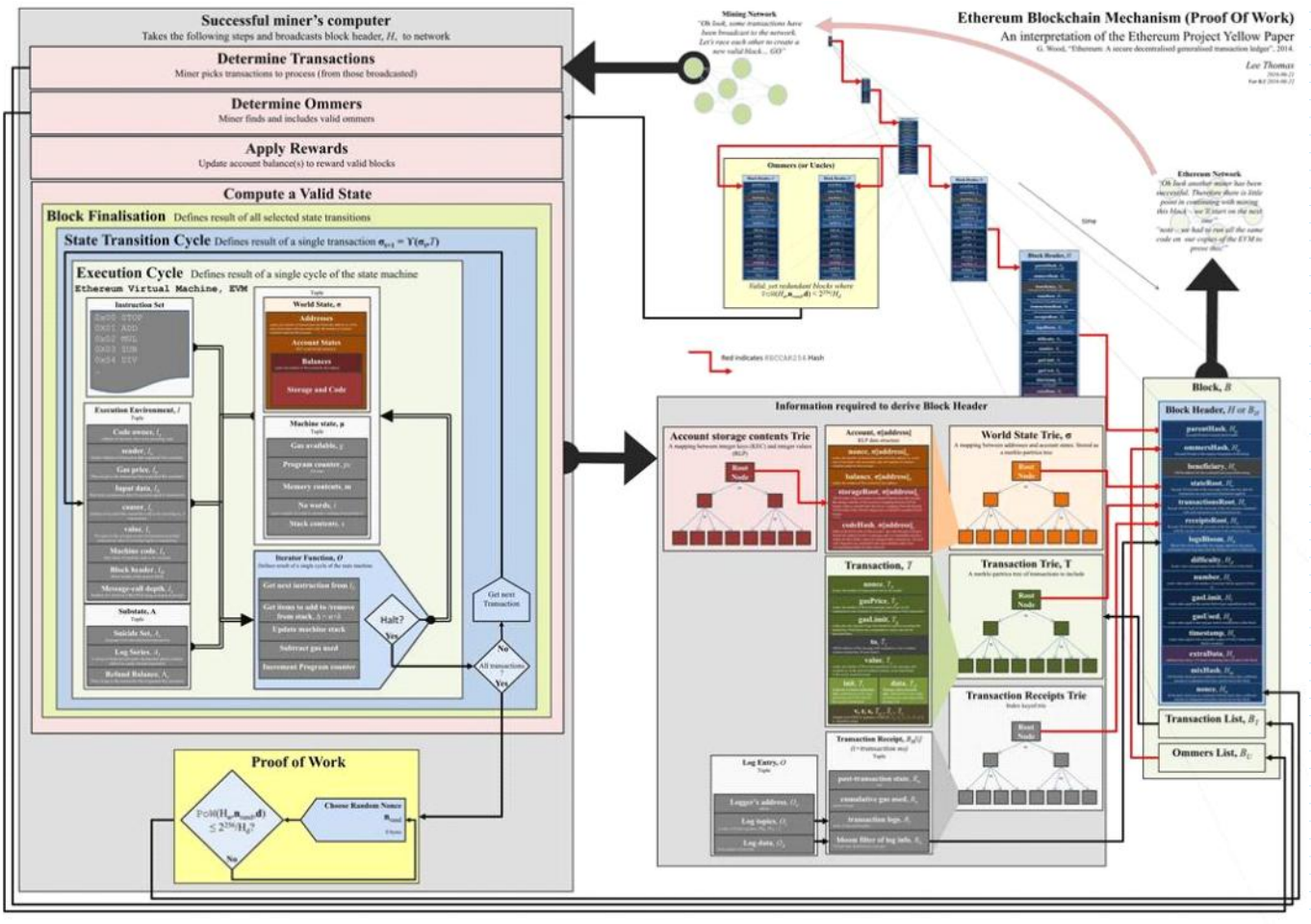
I tried to capture all the information contained in this post in this diagram:



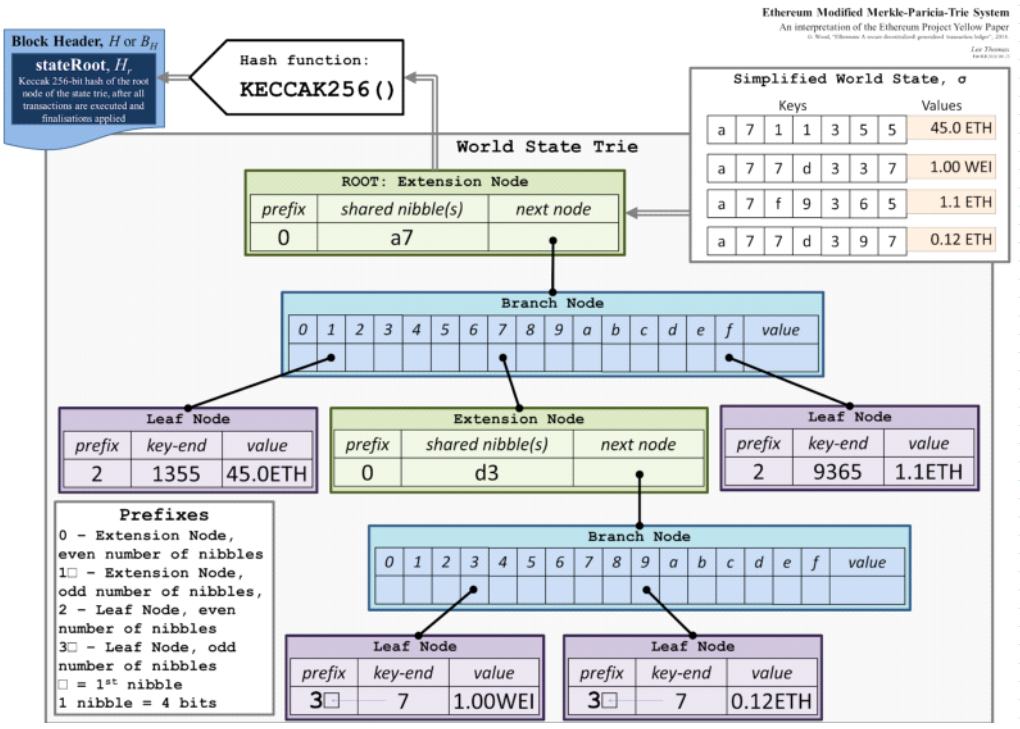
Block, transaction, account state objects and Ethereum tries

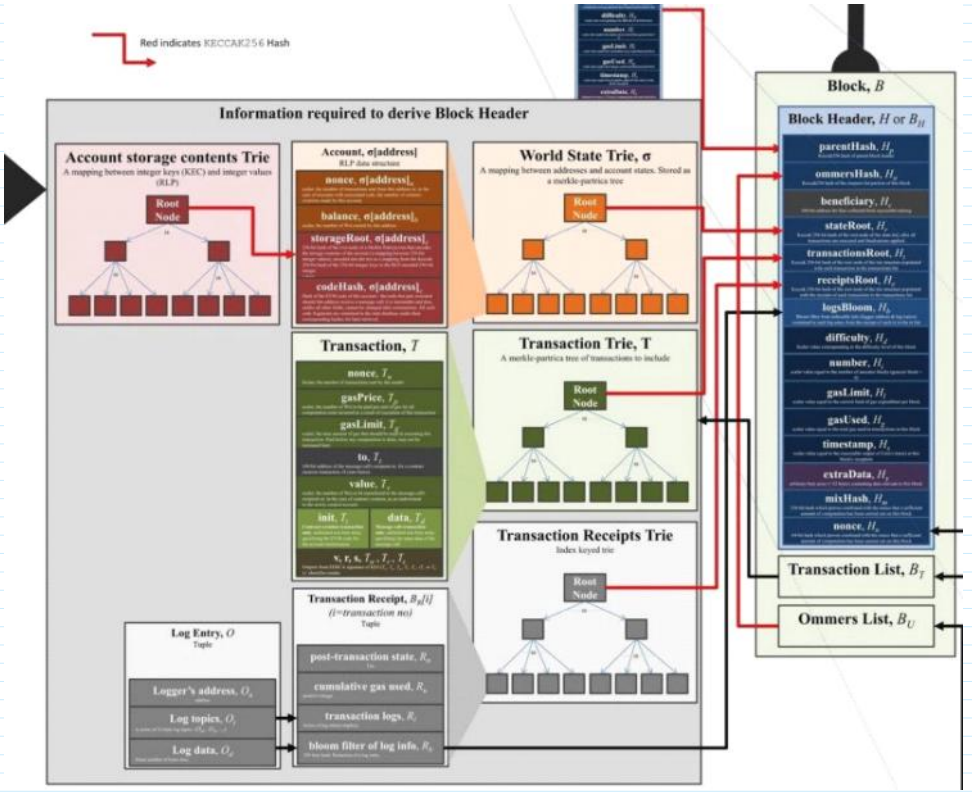
Working with Ethereum protocol is interesting. Every day, I have the opportunity to learn something new (and also relearn things that I thought

that I already knew). If you spot anything in this post that isn't quite clear (or even something that is clearly wrong), please comment and I'll try to address it as soon as possible. After all, we don't want to propagate misconceptions about the protocol.



Ethereum State Trie Architecture Explained | by eiki | Medium





References

- Merkle Trees
- Merkle Proofs
- How data is stored in Ethereum?
- Diving into Ethereum's world state
- How does Ethereum work anyway?

- A (Practical) Walkthrough of Smart Contract Storage
- Inside an Ethereum transaction
- Life Cycle of an Ethereum Transaction
- Ethereum Design Rationale
- Look at Ethereum white paper.