

DEVELOPING DAPPS IN ETHEREUM: THEORY AND PRACTICE

4TH SCIENTIFIC SCHOOL ON BLOCKCHAIN &
DISTRIBUTED LEDGER TECHNOLOGIES

CAGLIARI 12 15 SEPTEMBER 2023



ANDREA PINNA - ROBERTO TONELLI



ETHEREUM

BLOCKCHAIN 2.0

Ethereum



In 2015, Ethereum was released, the first blockchain for unstoppable applications conceived and conceived by Gavin Wood and Vitalik Buterin starting from 2013.

It is proposed to evolve the transactional mechanism into a state machine where account information becomes part of the state of a programmable virtual machine: the Ethereum Virtual Machine (EVM).

BLOCKCHAIN 2.0



BLOCKCHAIN 2.0



The state **transition function** is implemented with the algorithm for generating the next block.

Ethereum allows you to **run programs** on the EVM, known as smart contracts, which can be interacted with via blockchain transactions. The **block time is 12 seconds**.

It is an **open source** project and the protocol is constantly updated. The functioning of ethereum is analytically described in the yellow paper.

<https://ethereum.github.io/yellowpaper/paper.pdf>

ETHER

Ethereum's native currency (or token) is Ether and in September 2023 it can be exchanged for around 1600 dollars.

Like bitcoin, Ether is also divisible into smaller units.

The smallest unit of Ether is called **wei**.

1 ether = 10^{18} wei, (one ether is worth a trillion wei)

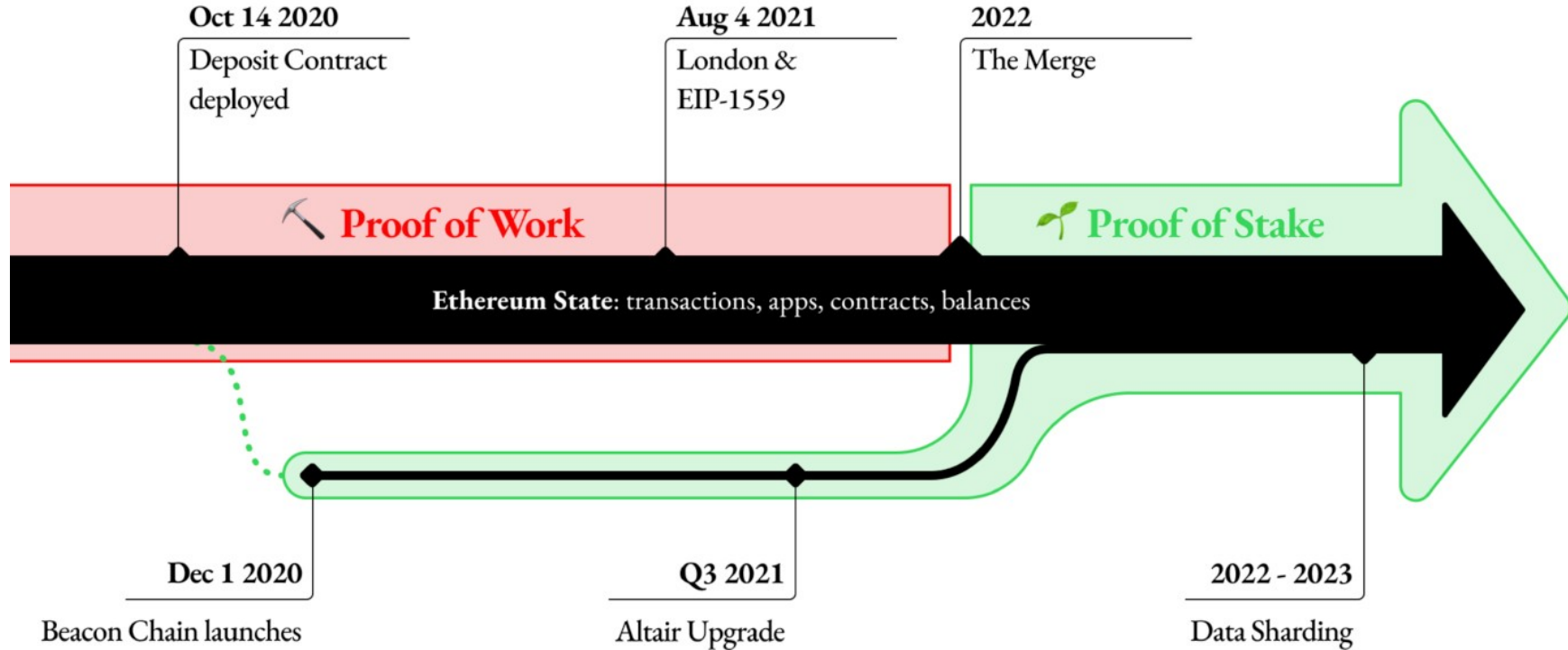
<https://coinmarketcap.com/currencies/ethereum/>

<https://bitinfocharts.com/ethereum/>

ETHEREUM UPGRADES

Ethereum's Upgrade Path

The Merge: when the existing PoW consensus is replaced by the Beacon Chain's PoS.
Graphic: @trent_vanepps, not "official," subject to change



PROOF OF STAKE

Ethereum has a block structure similar to bitcoin but instead of proof-of-work, it uses proof-of-stake (PoS) to create blocks.

In PoS the entire block generation process becomes low computational cost. The miners become “validators” and the block is said to be “finalized”.

Participants with more cryptocurrency blocked in the stack are more likely to be chosen as the “proposer” (those who generate the new block).

Explorer: <https://etherscan.io/>

ETH. 2.0 - VALIDATORS

A user who wants to become a validator must deposit 32 ETH in a “deposit” contract and launch three software: the execution client, the consensus client, and the validator.

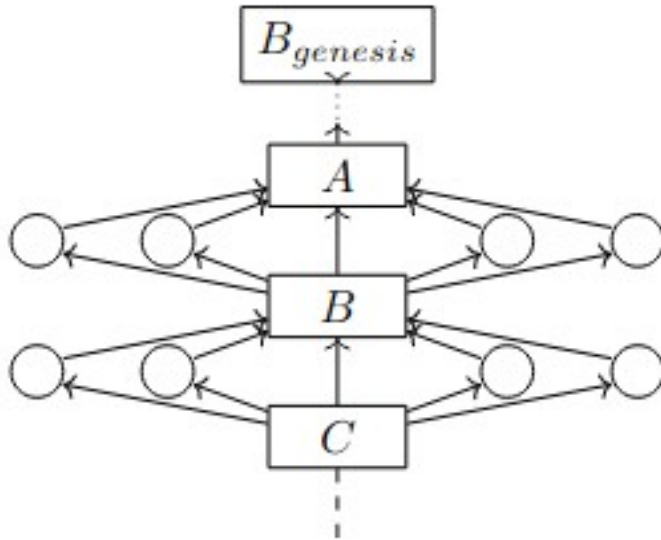
- The user queues in the validation queue.
- Once accepted, the validator begins receiving blocks and verifies the contents transaction by transaction.
- If the validator deems this block valid, it votes in favor and forwards it to the network.
- This operation is performed every 12 seconds (slot). An epoch is defined as a set of 32 slots. The first block of an epoch is called a checkpoint.
- At each slot, a validator is chosen on a random basis as the proposer of the new block. A subset (committee) of validators is also chosen for the vote.


Note: Validators must be synchronized!


Spiegazione estesa: <https://ethos.dev/beacon-chain>

ETH. 2.0 - VALIDATORS

The favorable votes are called “Attestations”.

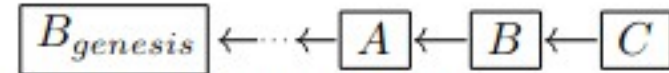


blocks: 

attestations: 



B depends on A



The chain of C or $\text{chain}(C)$

<https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/attestations/>

<https://arxiv.org/pdf/2003.03052.pdf>

ETH. 2.0 - FINALIZATION

How do we decide which block goes at the head of the chain?

Eth.2.0 uses two techniques.

1. Latest Message Driven Greedy Heaviest Observed Sub Tree (LMD-GHOST).

The block at the head of the chain is calculated based on the last vote made by each validator, and none of the votes made in the past.

2. Casper, the Friendly Finality Gadget (**Casper FFG**)

Variant of **PBFT** responsible for finalizing blocks and therefore deciding whether or not the block can be part of the chain. Casper doesn't finalize every slot, but it **finalizes every epoch** (6.4 minutes).

Paper: <https://arxiv.org/pdf/2003.03052.pdf>

<https://blockdaemon.com/documentation/guides/the-ultimate-guide-to-ethereum-2-0/>

ETHEREUM 2.0

These block computation techniques are not as onerous as PoW. For this reason, the rewards to validators **are lower**.

- We have seen that based on the value locked (maximum 32 ETH), validators will have a reward when they vote or propose blocks. This is the reward of the “Consensus Layer”.
- The reward for the “execution layer” is no longer awarded.

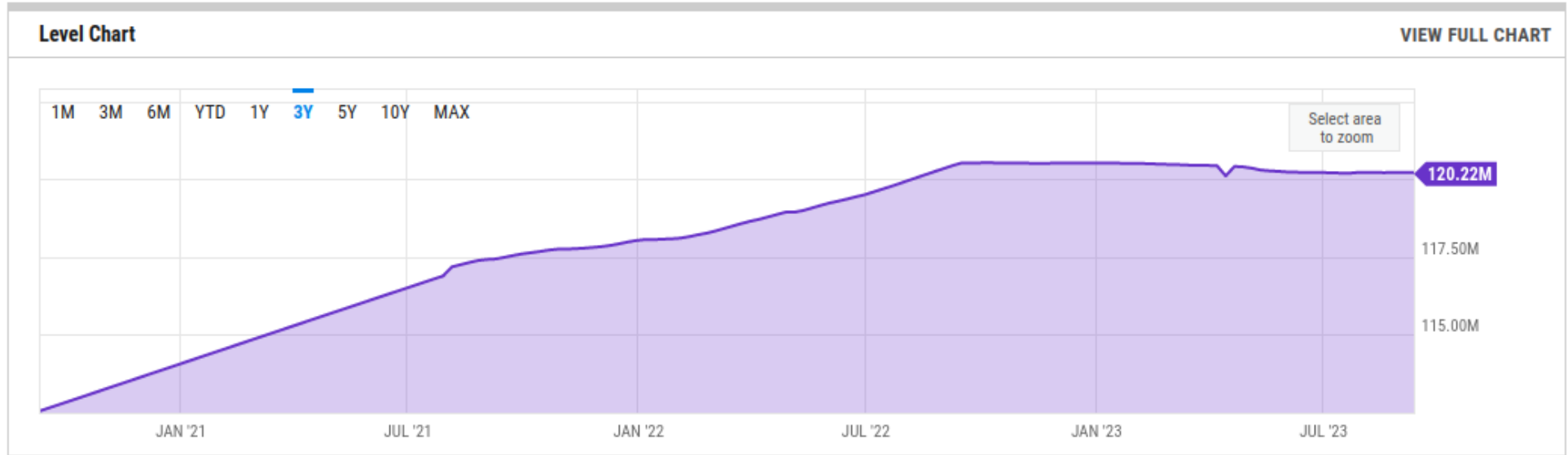
Note: Rewards currently go to separate accounts and have been made usable with the Shanghai Update (April 2023)

ETHEREUM 2.0

After the Shanghai update, stakers can withdraw all blocked funds, or only the excess portion of the 32 ETH.

- There is a limit to the number of ETH that can return to circulation.
- Initially maximum 6 validators within 6.4 minutes, then decreasing.
- This allows ETH to maintain a certain stability in value.

ETHEREUM BURNING



https://ycharts.com/indicators/ethereum_supply

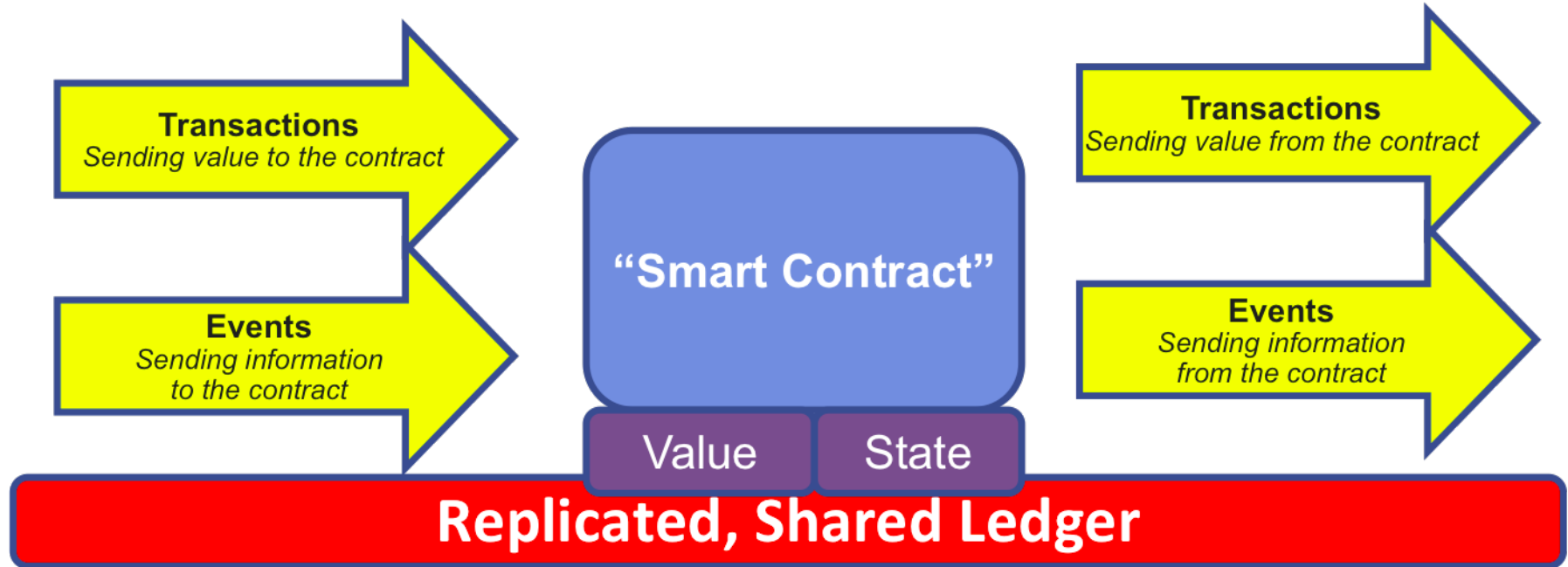
SMART CONTRACT

Ethereum allows you to insert arbitrarily complex computer programs into the blockchain and execute them with the EVM. The EVM is said to be “**Turing complete**”. These programs are called Smart Contracts.

Smart contracts were conceived by **Nick Szabo in 1990**. The idea is to exploit information technologies to allow agreements to be reached between people who do not trust each other.

The Ethereum **white paper** describes them as elements of the blockchain.

SMART CONTRACT



SMART CONTRACT

In the context of blockchains, a smart contract is a **program**, written in a specific programming language which, after being **compiled**, is **transmitted** and **recorded** on a blockchain via a special transaction called deploy.

From that moment the smart contract **starts executing** and is assigned an address with which to interact.

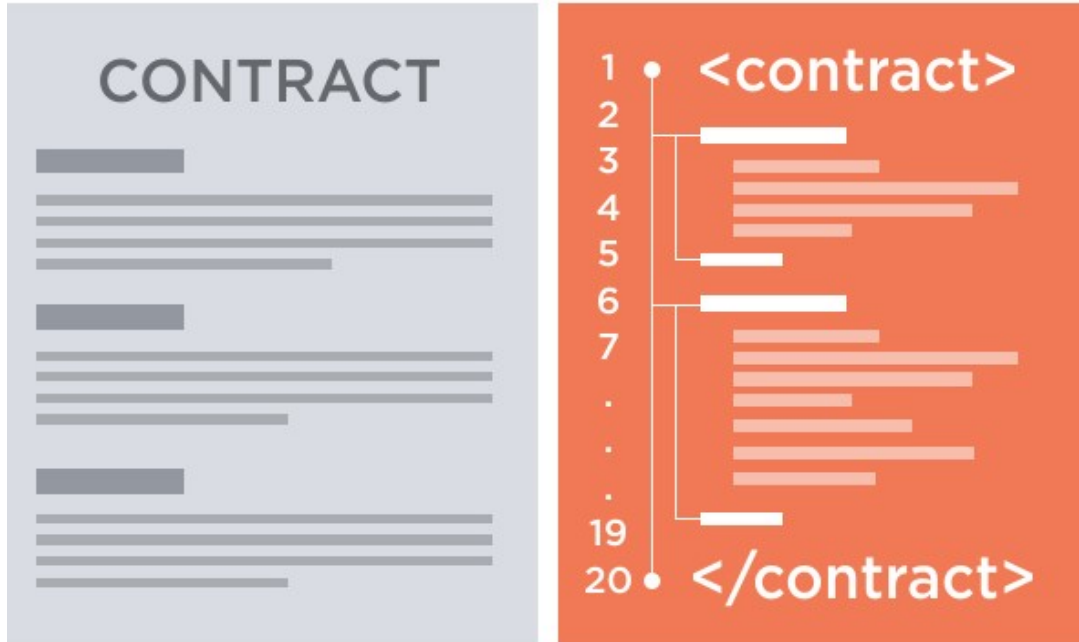
SMART CONTRACT

Transactions that perform functions are called “**messages**”. The messages are composed of the identification code of the function to be executed and the arguments to be passed.

The operations envisaged by the smart contract will be performed by all nodes in the network. These are subject to a tax calculated based on the computational cost (expressed in gas)

The code of a running smart contract cannot be altered.

WHAT IS A SMART CONTRACT?



Computer program operating within the blockchain that **automates** a procedure, according to an agreement between multiple parties.

Smart contract

SMART CONTRACT ELEMENTS



Address



Balance



Code



State

0x16E0022b17B...

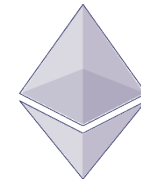
0 Ether

```
contract Counter {  
    uint counter;
```

```
    function Counter() public {  
        counter = 0;
```

```
    }  
    function count() public {  
        counter = counter + 1;
```

```
    }  
}
```



ethereum



SOLIDITY

ETHEREUM

Messages to smart contracts can be forwarded to any node connected to the network that exposes remote request services (for example via RPC or websocket). This way users can avoid installing node on their machine. A list of RPC nodes can be found here: <https://chainlist.org/>

The Ethereum blockchain contains many smart contracts and many more blocks than the bitcoin blockchain. This is why it is a very large data (over 12TB).

There are programs called bridges that connect to a network node and allow you to conveniently manage your accounts (such as wallets) and send and receive transactions. These programs can be extensions of web browsers (e.g. Metamask).

ETHEREUM

To be an Ethereum user you have several options: **use a node**, or use a **wallet/bridge** on your computer, or communicate with a node via remote procedures.

At this point you can interact with the blockchain to:

- Send monetary (ethers) transactions
- Create and deploy a new smart contract
- Use the features of a smart contract

ETHEREUM

Example: we want to query the Sepolia blockchain via the node reachable from the public URL `https://rpc.sepolia.org/` to know the balance of the address:

`0x4B20bC8490Cc69f5bb6fB280c5FDD2a88dB0Cee4`

```
curl --header "content-Type: application/json" -X POST --data '{"jsonrpc":"2.0","method":"eth_getBalance","params":["0x4B20bC8490Cc69f5bb6fB280c5FDD2a88dB0Cee4","latest"],"id":0}' https://rpc.sepolia.org/
```

<https://ethereum.github.io/execution-apis/api-documentation/>
<https://ethereum.org/en/developers/docs/apis/json-rpc/>

FEE AND GAS

The use of blockchain technology involves the transaction validation algorithm in all nodes of the network. On Ethereum, nodes must also process **all interactions with and between smart contracts**. This means that all nodes will consume resources and energy to carry out calculations that can be arbitrarily complex (that is, until sharding is fully used). regime).

To **discourage** the execution of excessively onerous calculations, a mechanism has been designed that allows the execution of the functionality of the blockchain and smart contracts upon payment of a "tax" called **transaction fee**, calculated on the basis of the complexity of the calculation. The cost of the operation is measured in **units of "Gas"**. For example, a write operation on the blockchain is more expensive (requires more gas) than a calculation operation.

FEE E GAS

The amount of gas needed to complete a certain operation is decided by Ethereum specifications.

https://github.com/ethereum/go-ethereum/blob/master/params/protocol_params.go

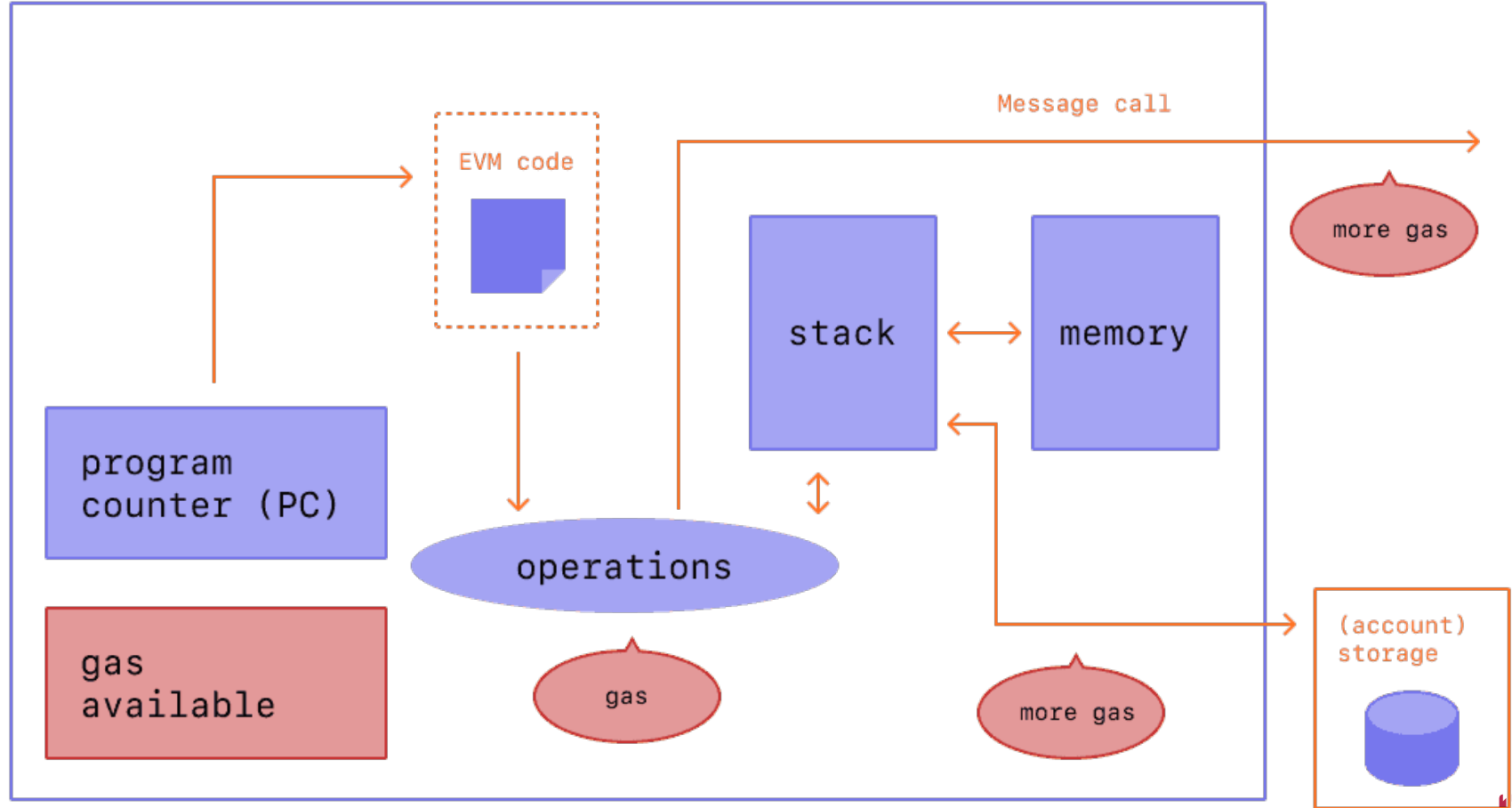
Write operations on blockchain have a much higher cost than data operations. **Reading only operations are free.**

The gas price is established by the algorithm while **the tip** is established by the user.

I can decide whether **to save and wait longer**, or pay more tips and **get a certain priority**.

<https://www.youtube.com/watch?v=AJvzNICwcwc&feature=youtu.be>

GAS IN THE EVM



EVM MEMORY TYPES

The EVM distinguishes different types of memory.

- **memory**: volatile memory of the EVM, used only for the execution of the SC
- **storage**: memory within the blockchain, very expensive: around 22K (allocation) gas for 32 bytes. Costs are defined by the EIP-2200.
- **calldata**: the (read-only) data passed by the transaction, which includes the parameters passed in the function call, if any.
- **stack**: the stack where instructions and registers reside
- **logs**: the space where events are recorded

MEMORY

The data area called **memory** is reserved by the EVM for each message call.

This area is linear and can be addressed at the byte level, but is read 256 bits at a time (1 word)

It can be written for single bytes, or for 256-bit words

When new memory is needed for reading or writing, the memory is "expanded" in steps of 256 bits

Each expansion costs gas, depending on the memory used by making the call (EIP-2200).

$$C_{mem}(a) \equiv G_{memory} \cdot a + \left\lfloor \frac{a^2}{512} \right\rfloor$$

Where **Gmemory** is **3** and **a** is the number of words of 256 bit

Soruce: Yellow Paper.

MEMORY

N	Formula	bytes32[N]
1	3	578
10	30	632
100	319	1193
1000	4953	8544
10000	225312	256079
100000	19831250	20133775

This table shows the estimated value with the formula (N = number of words) and the potential cost of the call.. With the gasprice at 77gwei and Ether at \$2000, storing 3MB in memroy would cost around \$3000

STORAGE

Each account and smart contracts has a **persistent** data area in the blockchain called storage. All the variables that make up the data structure of a smart contract (its state) are stored in storage.

The storage is composed of key-value pairs and maps 256-bit words to 256-bit words. However, it is not possible to enumerate storage from within a SC

Each word of storage is **always** initialized to zero.

STORAGE

Storage is expensive to read, and even more expensive to initialize and modify, so its use should be kept to a minimum: derivative calculations, and other non-permanent data should not be recorded in storage.

The gas cost is established by the EVM as described in the yellow paper. The growth of the writing cost is proportional to the number of words to be recorded.

G_{sset}	20000	Paid for an SSTORE operation when the storage value is set to non-zero from zero.
G_{sreset}	2900	Paid for an SSTORE operation when the storage value's zeroness remains unchanged or is set to zero.

Note: A smart contract can only directly read and write its own storage

STORAGE

N	Execution cost scrittura su Bytes32[100000]	Execution cost sovascrittura
1	22779	2879
10	223650	24650
100	2232360	242360
1000	22319460	2419460
10000	223190460	24190460
100000	2231900460	241900460

This table shows only the **Execution cost** (to which is added 21000 fixed + the gas for the function code and parameters) as calculated by Remix.

We see that the cost of writing **grows proportionally with N**.

The cost of writing is approximately 22000 gas units (**gset** 20000 + access costs) per word. The cost of overwriting is 2400 per word.

In dollars, the cost of **writing 1MB** on the mainnet is in the order of **\$100,000**.

GAS COST TABLE

Mnemonic	Gas Used	Notes
STOP	0	Halts execution.
ADD	3	Addition operation
MUL	5	Multiplication operation.
LT	3	Less-than comparison.
ADDRESS	2	Get address of currently executing account.
BALANCE	400	Get balance of the given account.
CALLER	2	Get caller address.
EXTCODESIZE	700	Get size of an account's code.
BLOCKHASH	20	Get the hash of one of the 256 most recent complete blocks.
MLOAD	3	Load word from memory.
MSTORE	3	Save word to memory
MSTORE8	3	Save byte to memory.
SLOAD	200	Load word from storage
JUMP	8	Alter the program counter
JUMPI	10	Conditionally alter the program counter.

FEE AND GAS

The price of gas is expressed in Gwei (giga wei).

The base price varies rapidly.

Some sites offer a recommendation on priority fees.

Recommended priority fee in Gwei

2

FAST < 2m

\$0.07 / Transfer

Gas Price (legacy): 53

1

STANDARD < 5m

\$0.03 / Transfer

Gas Price (legacy): 14.3

0

SAFE LOW < 30m

\$0.00 / Transfer

Gas Price (legacy): 14.3

Base Fee: 20 (\$0.67 / Transfer)

<https://ethgasstation.info/>
<https://etherbase.org/gas/>

PRIORITY FEE

We said that with Ethereum upgrades, users are allowed to acquire priorities regardless of gas, using Priority fees (tips).

Priority fees make it possible to discourage the harmful practice of validators who create empty blocks.

Example of empty block... <https://etherscan.io/block/14755267>

<https://ethereum.org/en/developers/docs/gas/>

GAS LIMIT

Users can set a gas limit for the single transaction.

This is to avoid unpleasant surprises due to possible errors in creating a transaction and executing the code.

The utility of the gas limit in transactions is especially useful when sending transactions to smart contracts or when uploading smart contracts to the blockchain.

----- ETHEREUM TESTNET

Testnets were created to allow developers to create decentralized applications before deploying them on the main blockchain.

In test networks it is possible to obtain “dummy” ethers that can be used for contract deploy and to pay costs related to gas consumption.

ATTENTION: the accounts (and private keys) used on the testnet are also valid on the main-net. Therefore, it **is not recommended to disclose** the private key to the public, even for addresses that are only used on different testnets.

ETHEREUM TESTNET

Recent history of testnets



BLOCKCHAIN 2.0 AND DAPP

The birth of Ethereum and Smart Contracts has led to:

- the development of new forms of **decentralized activities and organisations**.
- the creation of new forms of money (called **tokens**)
- the **ICO** boom around 2018.
- the **NFT** boom that has occurred in recent years.

In general, with **blockchain 2.0** it is possible to **create decentralized applications**.

Note: There are currently many blockchains that allow you to create NFTs,

DAPP

A decentralized application (dApp) is a software system that contains both “traditional” components and blockchain-based components.

Blockchain and smart contracts are entrusted with the role of management, data verification and execution of the functions that are to be made **available (and traceable), safe and incorruptible**.

dApps rely on off-chain systems for all the functions that do not require the features of the blockchain. For example: the user interface, logging of complex data, processing of large amounts of data, etc.

DAPP

Ethereum is referred to as an enabler of **web 3.0**.

Web3.0 implements and provides web3 libraries for several programming languages. These libraries allow the creation of websites and applications connected to the blockchain.

Among the most popular programming languages for programming dApps are: **javascript, python and Java**

Python: <https://web3py.readthedocs.io/en/stable/>

Javascript: <https://web3js.org/#/> and <https://docs.ethers.org/v6/>

Java: <https://www.web3labs.com/web3j-sdk>

TOKEN



TOKEN AND UTILITY TOKEN

Tokens can be created and issued even without going through an ICO. Two types of tokens can be distinguished

Coins: tokens created to become new cryptocurrencies (which however are not always divisible into small parts).

Utility token: without a purely financial purpose but with a specific **practical utility** (participating in DAO, purchasing services or products).

This distinction is useful in some countries for tax reporting and therefore for calculating taxes.

Example: fan tokens <https://www.socios.com/>

TOKEN ERC-20

An ERC-20 based token is a program within the blockchain that allows for the creation of a new currency and allows for

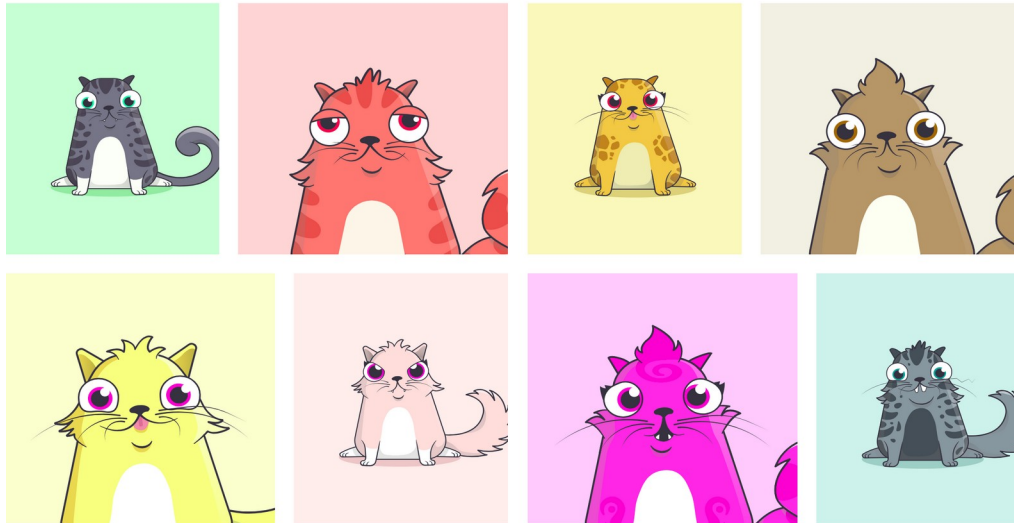
- Get tokens (associated with my address)
- Give tokens and transfer them to another address
- Check how many tokens I have
- Allow another address to manage my tokens.

<https://eips.ethereum.org/EIPS/eip-20>

NFT

An NFT is a “**Non Fungible Token**” created with a smart contract. Two tokens of the same NFT are different from each other and therefore not fungible (substitutable).

Famous example: Cryptokitties. Each kitty has a different code and value.



<https://www.cryptokitties.co/>

NFT

NFTs have developed thanks to the possibility of creating smart contracts.

On Ethereum, NFTs are based on the **ERC-721 standard**.

An ERC-721 smart contract extends the functions of the ERC-20 standard because it allows you to **assign unique characteristics** to each individual token.

For this reason these tokens are **called non-fungible** (they are not coins but "**objects**" distinguishable from each other).

<http://erc721.org/>

NFT

Through an NFT token it is possible to provide a certificate of ownership and uniqueness that is impossible to falsify and can be associated with a real or virtual object. There are numerous applications:

- Graphic arts (NFT art)

- GIFs

- Videos of sporting events

- Collections (real or virtual)

- Virtual avatars and video game skins

- Designer sneakers (designer shoes)

- Web domain names

- Music

NFTs have become very popular in recent years.

<https://opensea.io/>











NFT

Each NFT token is different from another. It is possible to sell different tokens at different prices.

<https://www.blockchain.com/nfts>

Top NFTs

These are the top NFTs that have been sold in the last 24 hours.

 <p>Bored Ape Yacht Club #7947</p> <p>Price: 150 ETH Value: \$306,729.00 Floor Price: 95 ETH Last Sale: 2022-05-22 22:46</p> <p>Creator Owner Collection</p>	 <p>Bored Ape Yacht Club #6339</p> <p>Price: 129 ETH Value: \$263,786.94 Floor Price: 95 ETH Last Sale: 2022-05-22 17:52</p> <p>Creator Owner Collection</p>	 <p>Wrapped Ether Rock #92</p> <p>Price: 100 WETH Value: \$204,486.00 Floor Price: 140 ETH Last Sale: 2022-05-22 17:24</p> <p>Creator Owner Collection</p>	 <p>Bored Ape Yacht Club #3731</p> <p>Price: 98 WETH Value: \$200,396.28 Floor Price: 95 ETH Last Sale: 2022-05-22 15:28</p> <p>Creator Owner Collection</p>	 <p>Bored Ape Yacht Club #3989</p> <p>Price: 95 ETH Value: \$194,261.70 Floor Price: 95 ETH Last Sale: 2022-05-23 02:59</p> <p>Creator Owner Collection</p>
 <p>Bored Ape Yacht Club #1685</p> <p>Price: 92.8 ETH Value: \$189,763.01 Floor Price: 95 ETH Last Sale: 2022-05-23 02:26</p> <p>Creator Owner Collection</p>	 <p>Bored Ape Yacht Club #1971</p> <p>Price: 87.49 WETH Value: \$178,904.80 Floor Price: 95 ETH Last Sale: 2022-05-22 18:32</p> <p>Creator Owner Collection</p>	 <p>Nouns #103</p> <p>Price: 85 ETH Value: \$173,813.10 Floor Price: 80 ETH Last Sale: 2022-05-23 06:37</p> <p>Creator Owner Collection</p>	 <p>Ringers by Dmitri Cherniak #13000714</p> <p>Price: 62 WETH Value: \$126,781.32 Floor Price: 42.09 ETH Last Sale: 2022-05-22 21:25</p> <p>Creator Owner Collection</p>	 <p>BEANZ Official #19597</p> <p>Price: 52 ETH Value: \$106,332.72 Floor Price: 1.389 ETH Last Sale: 2022-05-23 02:32</p> <p>Creator Owner Collection</p>

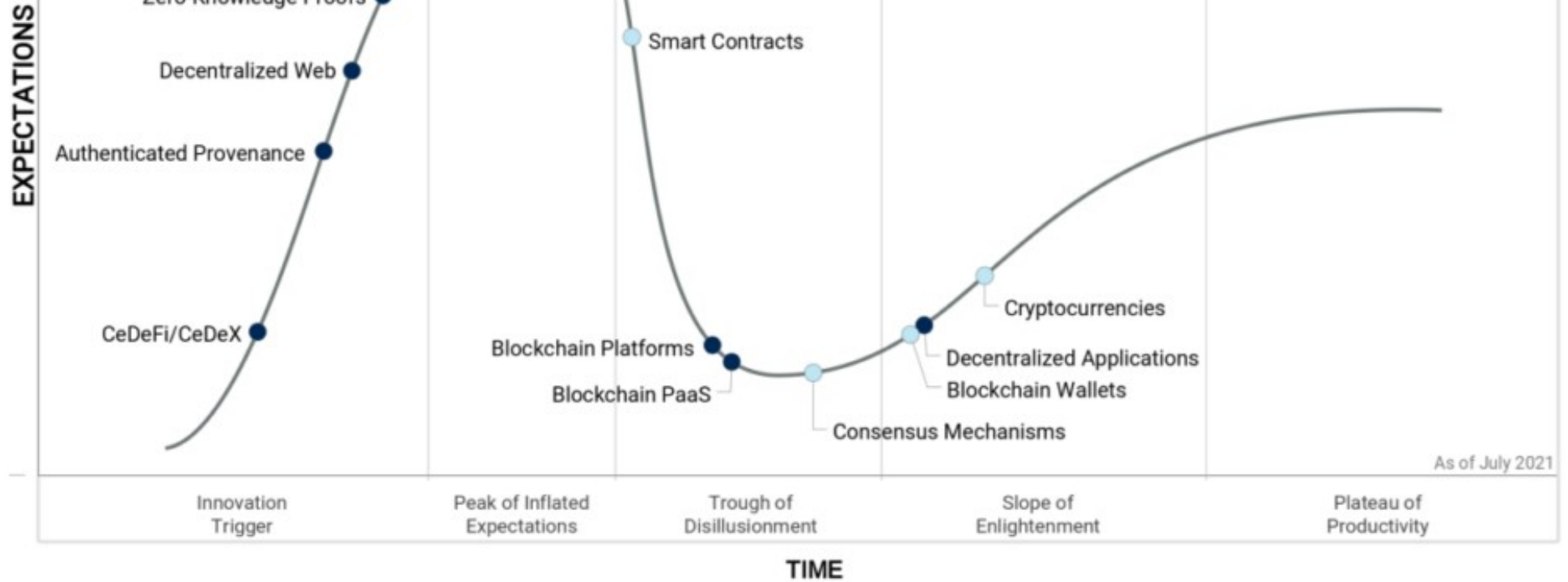
APPLICATIONS

Other fields of application include:

-
- Healthcare systems (anti-counterfeiting of drugs, data privacy, etc.)
- Public administrations (land registry data, communications between PAs, voting, etc.)
- Management of employment contracts
- Copyright management,
- Metaverse and Online Games
- Management of tourist destinations
- Identity management
- Notarization of data

Hype Cycle for Blockchain, 2021

EXPECTATIONS



As of July 2021

TIME

Plateau will be reached: ○ < 2 yrs. ● 2-5 yrs. ● 5-10 yrs. ▲ >10 yrs. ✗ Obsolete before plateau

2023 Gartner Emerging Technologies and Trends Impact Radar

