ETHEREUM AND SMART CONTRACTS

Created: Sept 2022
Last Edited: Sept 2022

UofT: CSCD71F22
-David Liu, Founder of dApp Technology Inc.

TOPICS

1. Smart Contract Live Coding
2. Ethereum Internals
3. Blockchain Development

Smart Contract Live Coding

REMIX IDE

- A learning platform for developing, deploying and administering ETH Smart Contracts.

VIP PASS CONTRACT

Variables		
admin	address	Admin of the Contract
isMinter	mapping(minter: address => isMinter: bool)	Minter Permissions
balanceOf	mapping(holder: address => balance: uint)	The amount of VIP Passes
isApproved	mapping(account: address => mapping(approvedSpender: address => isApproved))	Permissions for transferring VIP Passes on another's behalf

Functions		
constructor	(admin: address)	Sets the admin
mint	(receiver: address, mintAmt: uint)	Mints new VIP Passes to an account
transfer	(sender: address, receiver: address, transferAmt: uint)	Transfer VIP Passes from the caller's account to another account
manageMinters	(minter: address, isMinter: bool)	Set Minter permission
approveSpender	(spender: address, _isApproved: bool)	Set the approval permission of transferring VIP Passes for caller's account

Events		
Transfer	(sender: address, receiver: address, amt: uint)	A VIP Pass transfer occurred

VIP PASS SALES CONTRACT

Variables		
sales	mapping(salesId: uint => sale: Sale)	All sales info
salesIdCounter	uint	An incremental counter for sales id
VipPass Contract	address	The VIP Pass Contract

Sale Struct		
price	uint	Price of one pass in Wei
supplyLeft	uint	Amount of passes unsold
seller	address	The account that made the sale

Functions		
constructor	(vipPassContract: address)	Sets the VIP Pass Contract
createSale	(supply: uint, price: uint)	Create a new VIP Pass sale
buyFromSale	(salesId: uint, buyAmt: uint)	Buy an amount of VIP Passes from a sale

Events		
SaleCreation	(supply: uint, price: uint, seller: address)	A new sale has been created
SaleTransacted	(saleQuantity: uint, saleId: uint, price: uint, supplyLeft: uint, seller: address)	A purchase has occurred

BLOCKCHAIN 1.0

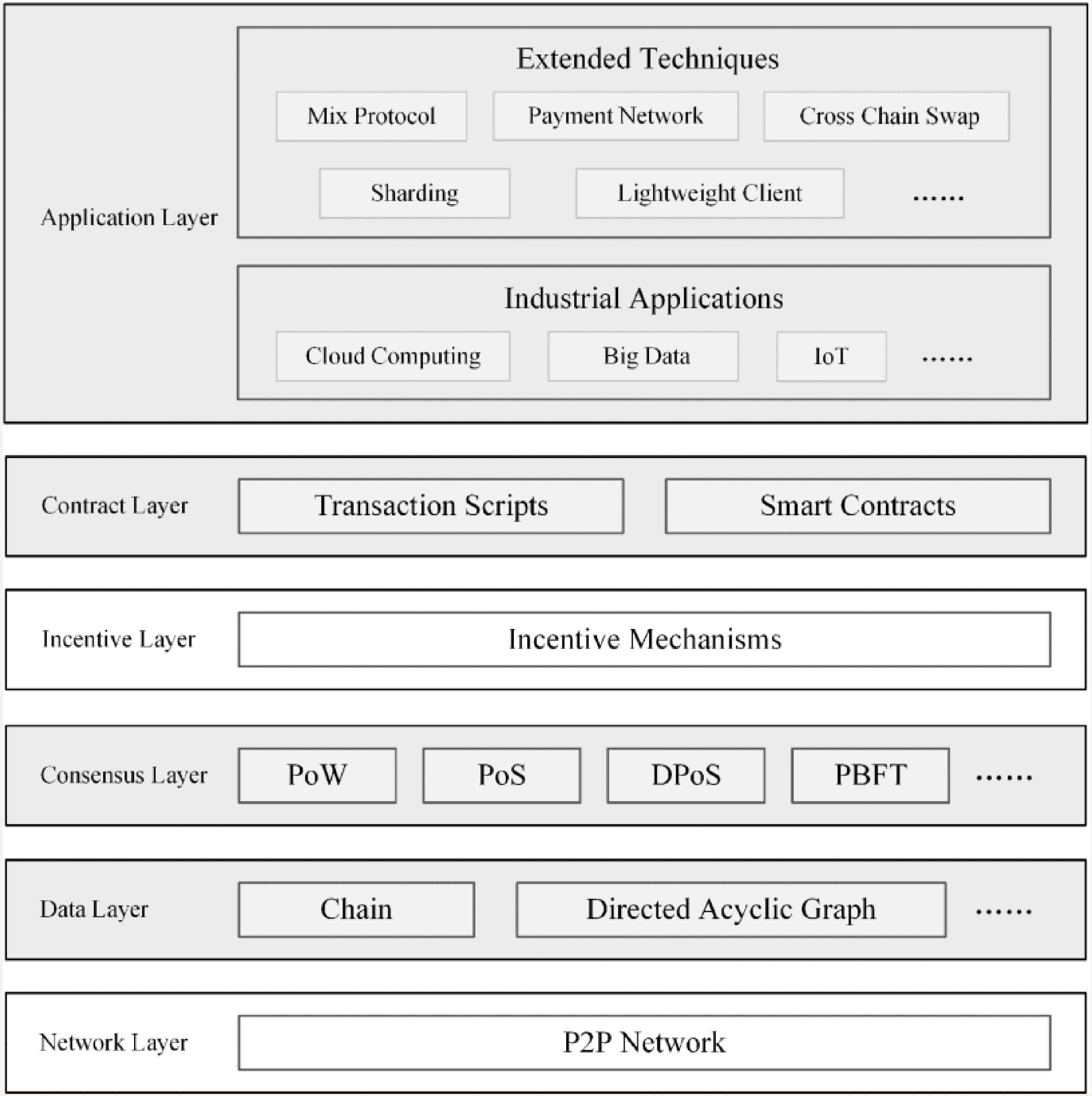
- First concept of decentralization
- Focus on cryptocurrency
- Emergence of cryptocurrency wallets, mining rigs, mining software and decentralized blockchain computer

- Notable projects:
- ECash (by DigiCash 1983)
- Bitcoin (by Cypherpunks 2009)

BLOCKCHAIN 2.0

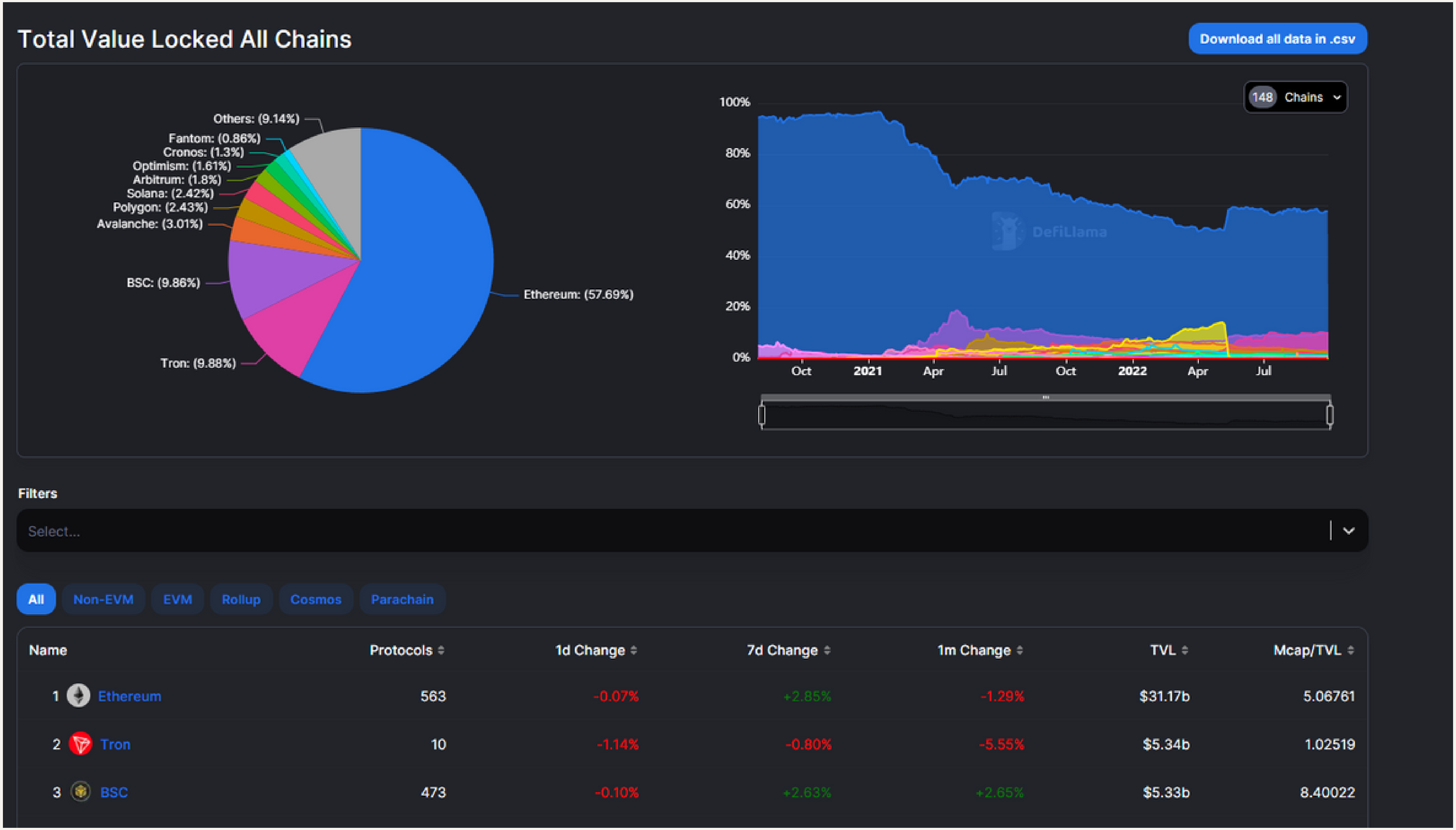
- Emergence of Decentralized Code (Smart Contract)
- Mass adoption of Decentralized Applications (dApps)

- Notable projects:
- Ethereum (Blockchain by Vitalik Buterin 2013)
- Uniswap (ETH dApp by Hayden Adams 2018)


Application Layer
Extended Techniques
Mix Protocol
Payment Network
Cross Chain Swap
Sharding
Lightweight Client
......
Industrial Applications
Cloud Computing
Big Data
IoT
......
Contract Layer
Transaction Scripts
Smart Contracts
Incentive Layer
Incentive Mechanisms
Consensus Layer
PoW
PoS
DPoS
PBFT
......
Data Layer
Chain
Directed Acyclic Graph
......
Network Layer
P2P Network

ETHEREUM

- First Decentralized Blockchain with Smart Contracts
- Programs run on the Ethereum Virtual Machine (EVM)
- Ether is the native token used to pay for transactions (Gas Fees)
- Largest adopted blockchain for dApps and largest community support
- Solidity is the most popular coding language



Total Value Locked All Chains

Download all data in .csv

Filters

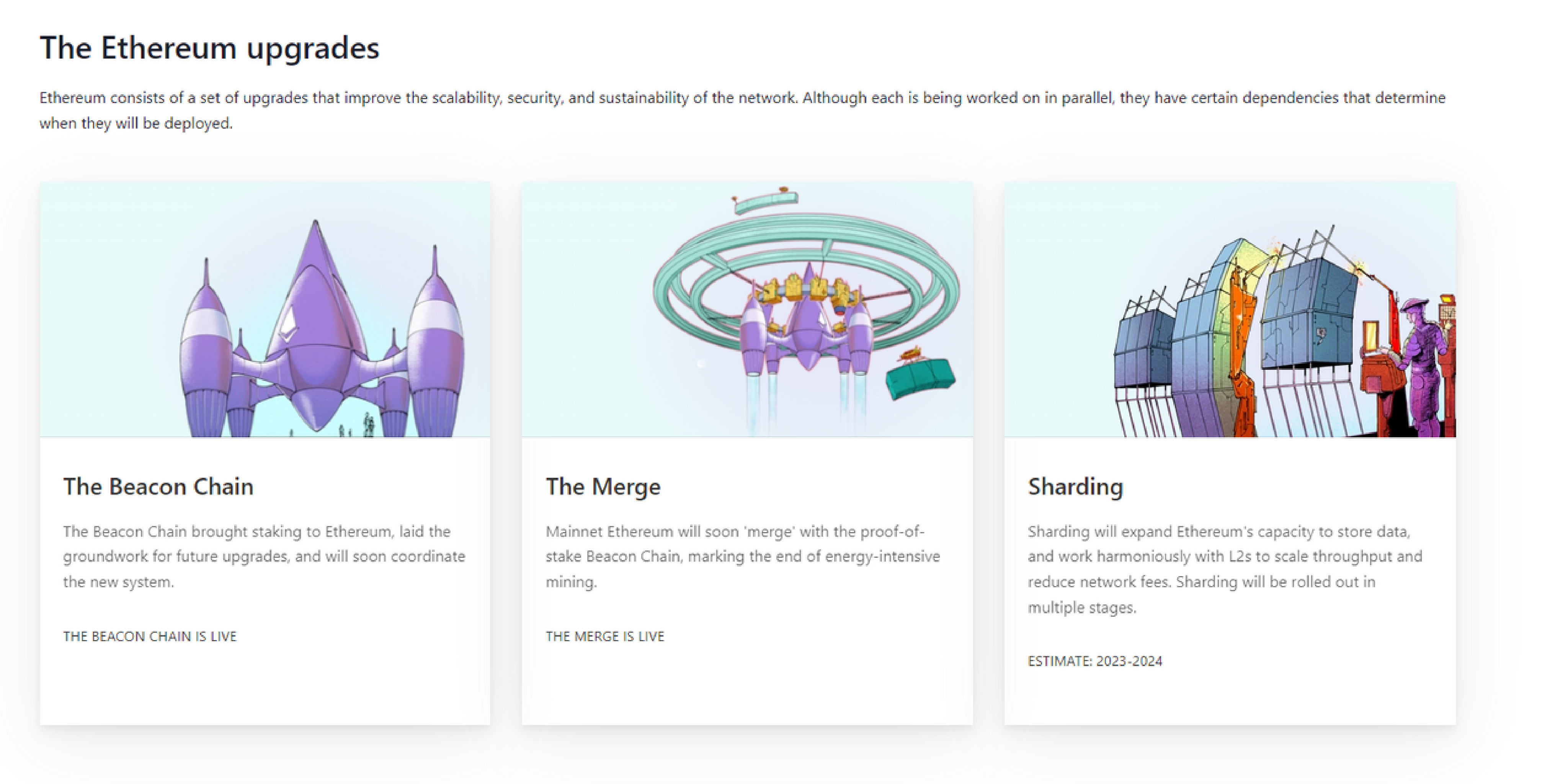
Select...

All | Non-EVM | EVM | Rollup | Cosmos | Parachain

Name	Protocols	1d Change	7d Change	1m Change	TVL	Mcap/TVL
1 Ethereum	563	-0.07%	+2.85%	-1.29%	$31.17b	5.06761
2 Tron	10	-1.14%	-0.80%	-5.55%	$5.34b	1.02519
3 BSC	473	-0.10%	+2.63%	+2.65%	$5.33b	8.40022

Sept 28, 2022
DeFi Llama

ETHEREUM ROADMAP (SEPT 2022)



The Ethereum upgrades

Ethereum consists of a set of upgrades that improve the scalability, security, and sustainability of the network. Although each is being worked on in parallel, they have certain dependencies that determine when they will be deployed.

The Beacon Chain

The Beacon Chain brought staking to Ethereum, laid the groundwork for future upgrades, and will soon coordinate the new system.

THE BEACON CHAIN IS LIVE

The Merge

Mainnet Ethereum will soon 'merge' with the proof-of-stake Beacon Chain, marking the end of energy-intensive mining.

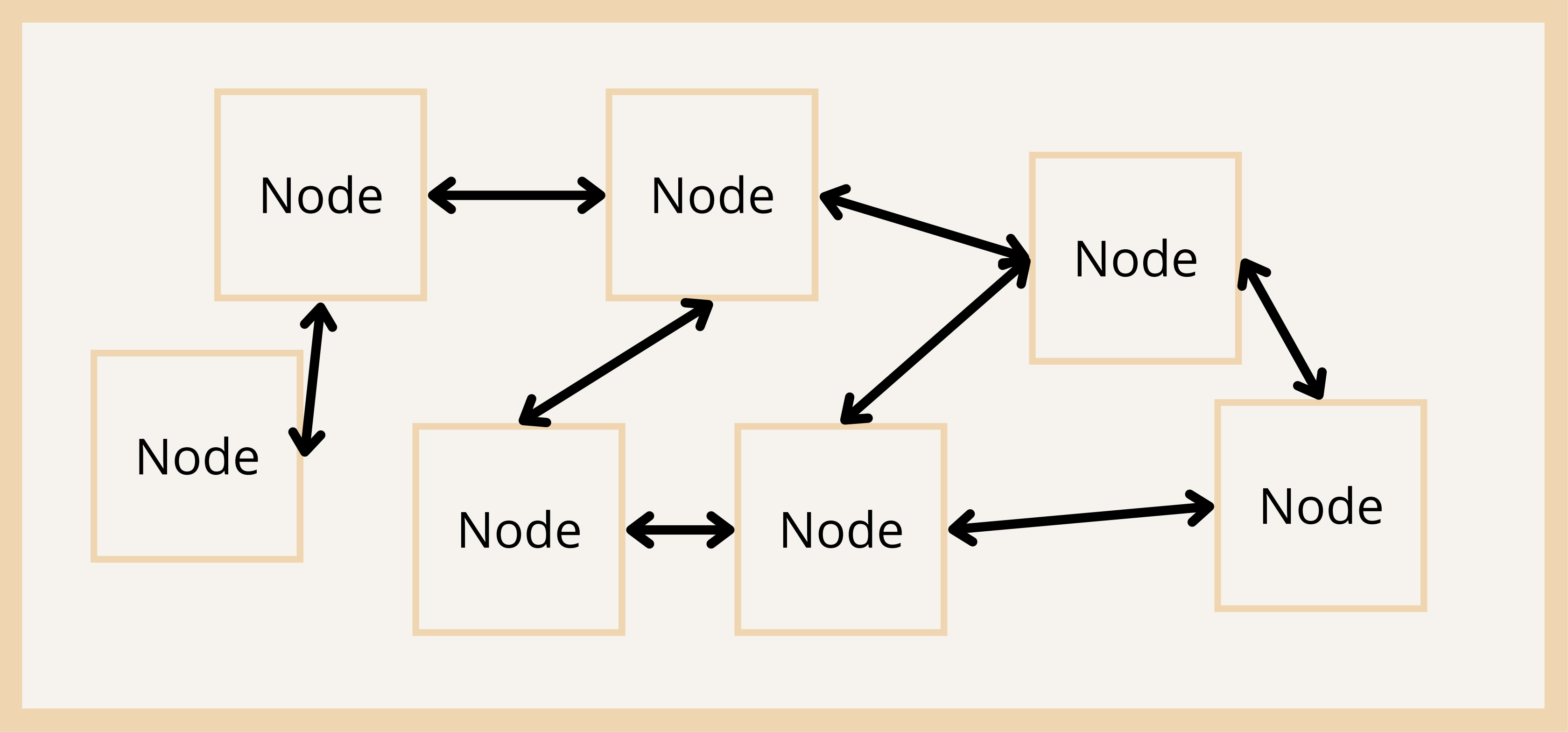
THE MERGE IS LIVE

Sharding

Sharding will expand Ethereum's capacity to store data, and work harmoniously with L2s to scale throughput and reduce network fees. Sharding will be rolled out in multiple stages.

ESTIMATE: 2023-2024

ETHEREUM NETWORK



- Each Node stores a portion of the blockchain and runs the EVM to execute code from Smart Contracts
- Ethereum Validators receives data from the nodes and adds new blocks to the blockchain

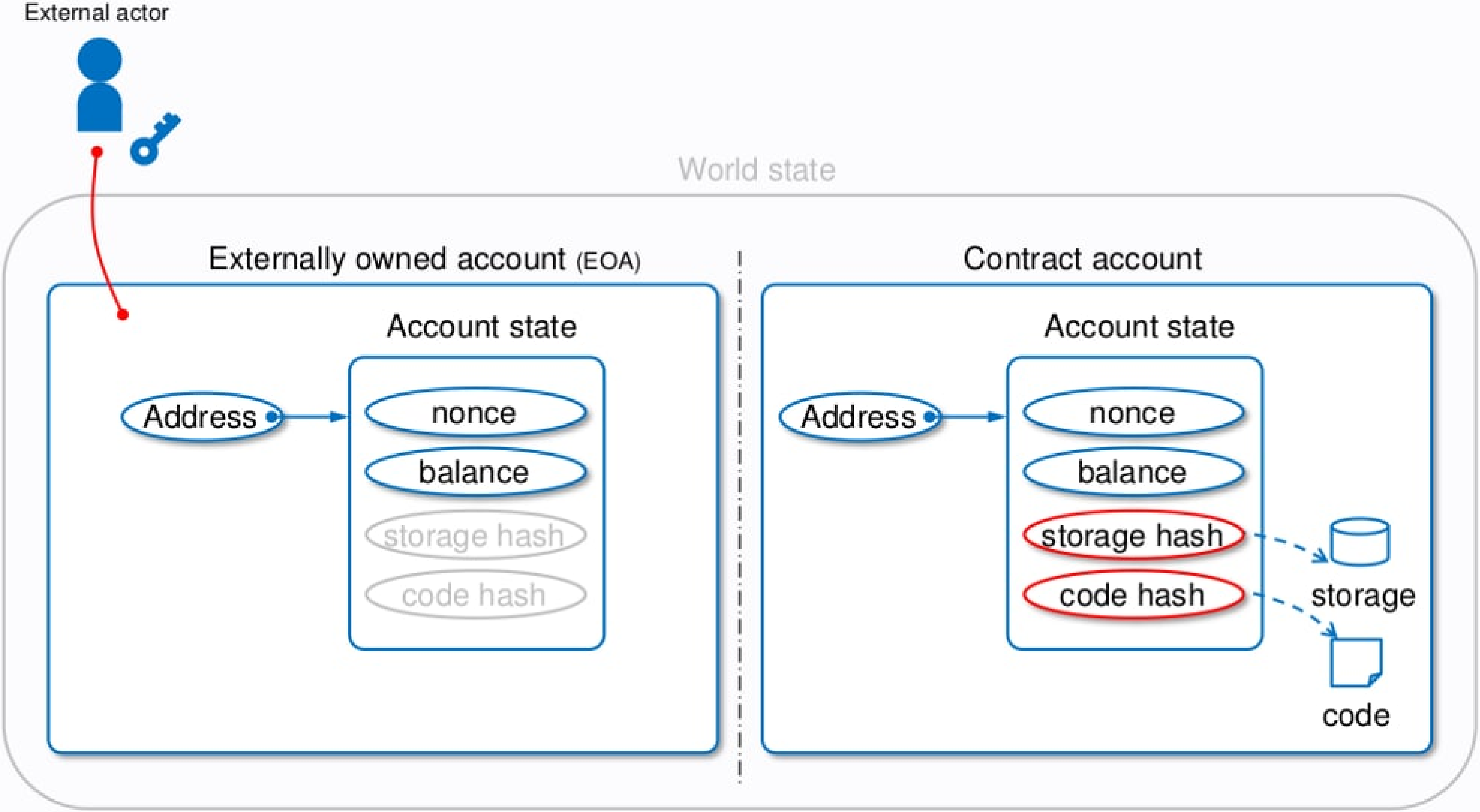
ETH ACCOUNTS

Externally Owned Accounts (EOA) and Smart Contracts on Ethereum are ETH Accounts, identified by their ETH address.

Example:
0x397507d0E34756A192dE72787A0309bD3E8C038d

Smart Contracts can hold cryptocurrencies just like EOAs.

Both EOA and Smart Contracts can interact with Smart Contracts.



EOA is controlled by a private key.
EOA cannot contain EVM code.

Contract contains EVM code.
Contract is controlled by EVM code.

EOA I

An EOA private key can be generated using the Elliptic Curve Digital Signature Algorithm (ECDSA). Generation can happen locally on any device.

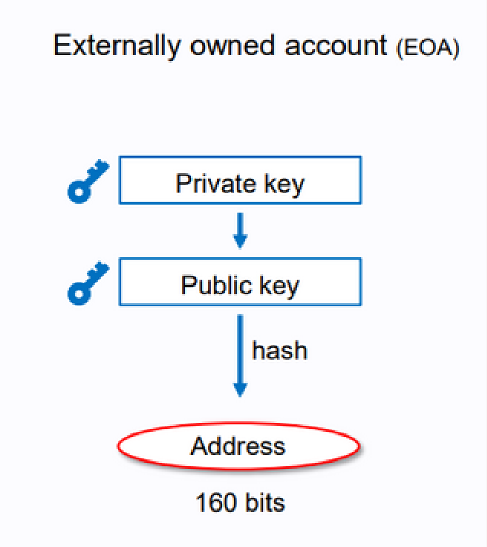
Private Key Example:

fffffffffffffffffffffffffffffffebaaedce6af48a03bbfd25e8cd036415f

A private key can derive a public key which can in turn derive a public ETH address.

ETH Address Example

0xb794f5ea0ba39494ce839613fffba74279579268



EOA II

A private key can also sign messages and transactions which output a signature.

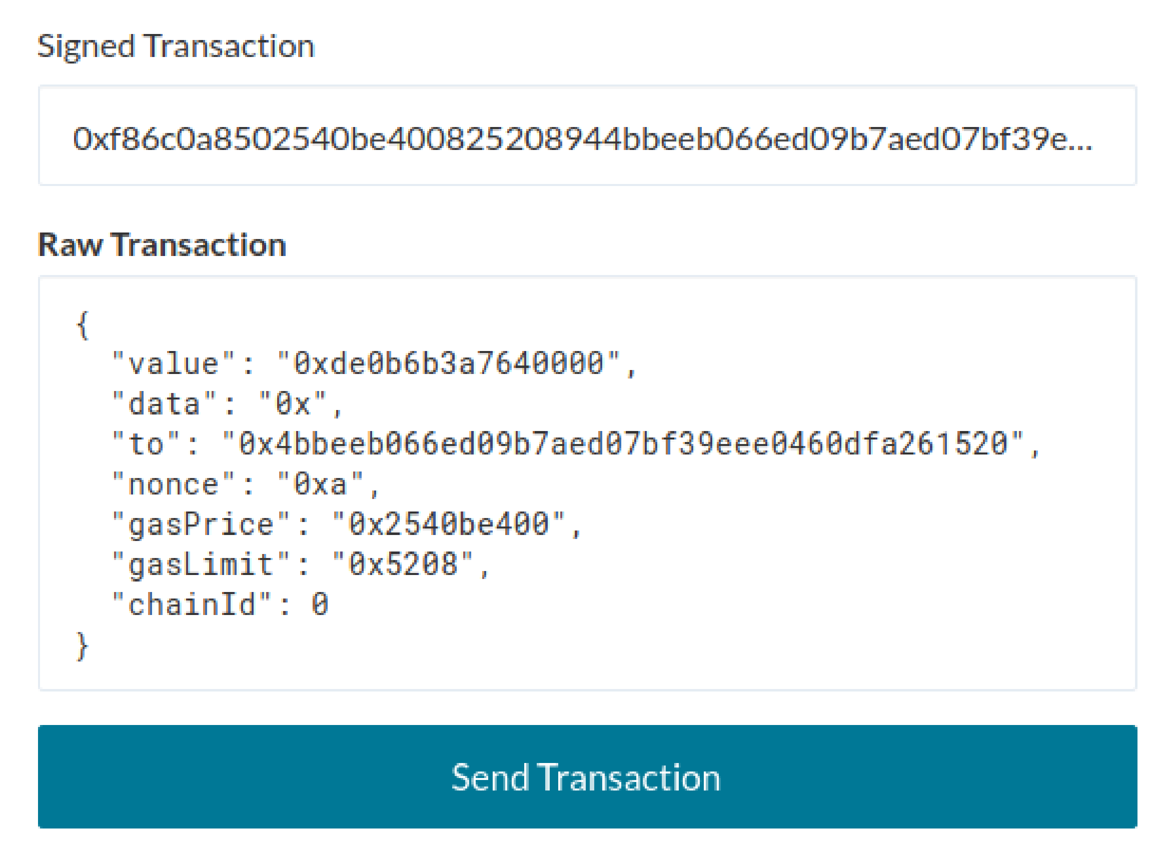
ETH Signed Message Example:

```
{
  "address": "0x76e01859d6cf4a8637350bdb81e3cef71e29b7c2",
  "msg": "Hello world!",
  "sig":
 "0x21fbf0696d5e0aa2ef41a2b4ffb623bcaf070461d61cf7251c74161f
82fec3a4370854bc0a34b3ab487c1bc021cd318c734c51ae29374f2be
b0e6f2dd49b4bf41c",
  "version": "2"
}
```

EOA III

A private key can also sign messages and transactions which output a signature.

ETH Signed Transaction Example:



Signed Transaction

0xf86c0a8502540be400825208944bbeeb066ed09b7aed07bf39e...

Raw Transaction

```
{
  "value": "0xde0b6b3a7640000",
  "data": "0x",
  "to": "0x4bbeeb066ed09b7aed07bf39eee0460dfa261520",
  "nonce": "0xa",
  "gasPrice": "0x2540be400",
  "gasLimit": "0x5208",
  "chainId": 0
}
```

HD WALLETS

A Hierarchal Deterministic (HD) Wallet is a type of Deterministic Wallet that utilizes a single root key to derive multiple private keys. The root key is usually in the form of a Mnemonic Word Sequence.
Mnemonic Phrase Example: indoor dish desk flag debris potato excuse depart ticket judge file exit

An implementation of HD Wallet is Metamask via its Keyring Module.

Resources Used:

https://coinsbench.com/about-evm-opcode-gas-ethereum-accounts-9f0896f09d04
https://ethereum.org/
https://hardhat.org/
https://docs.ethers.io/v5/
https://www.openzeppelin.com/
https://takenobu-hs.github.io/downloads/ethereum_evm_illustrated.pdf
https://www.skillsoft.com/