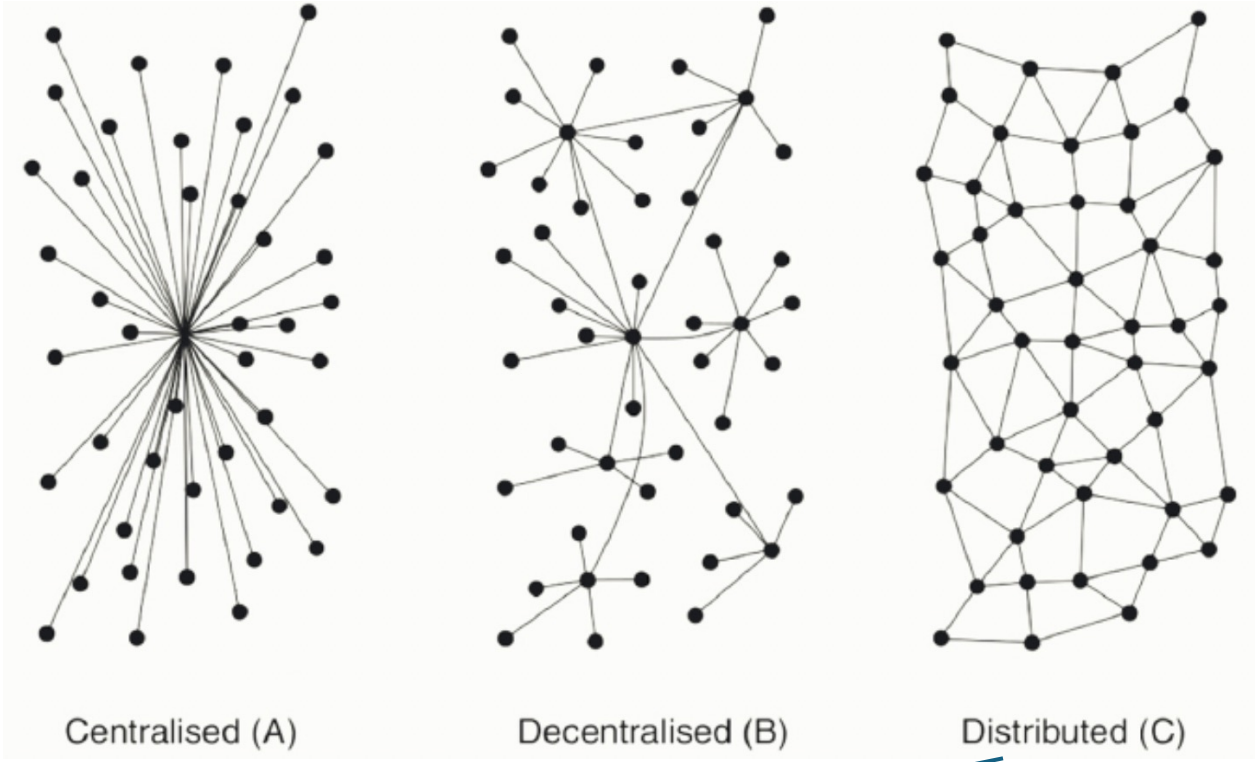
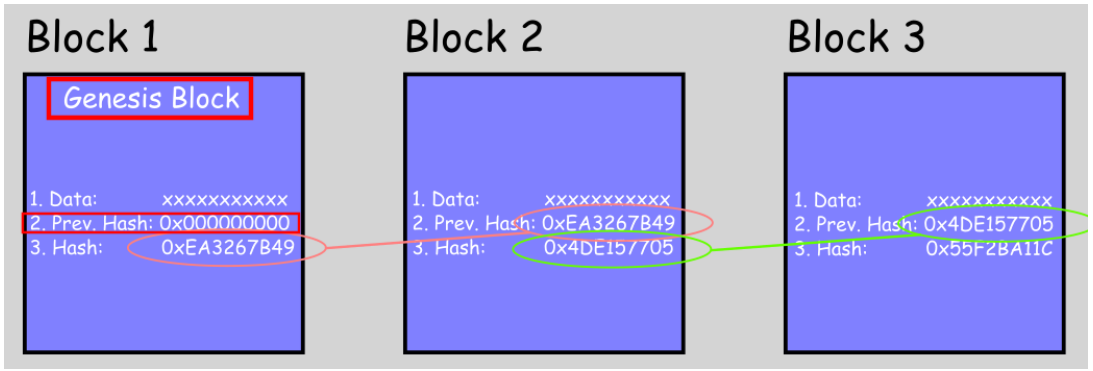
Bitcoin Weesen: Intro into Ethereum

Samuel Bisig, May 14th 2024

Distributed Ledger Technology (**DLT**)

- "**Block-chain**" (eg. Bitcoin) a subcategory (others: DAG, hashgraph)





→ chain (via hashing) of blocks (data, „txs", „state")

→ **no** single point of failure (higher resilience)
→ **no** (centralized) intermediaries ("peer-to-peer")
→ **trust abstraction**

Ethereum Facts (Web2 → Web3)

- 2014/15: peer-to-peer **permissionless** blockchain network
- first blockchain that included a **Turing-complete virtual machine** (**EVM**)
- "**decentralized permissionless operating system**, where **anyone** in the world with an **internet connection** can provide **financial and commercial services** to **anyone** else, through the use of **smart contracts deployed on-chain**"
- **Account** model (not UTXO* as Bitcoin)
  - regular "externally owned" **accounts** (**EOA**), controlled by **users**
  - contract accounts (**CA**) or "**smart contracts**", controlled by **code**

* Unspent transaction output

Ethereum as Open source (computation)

- **Similar** to Linux and Apache

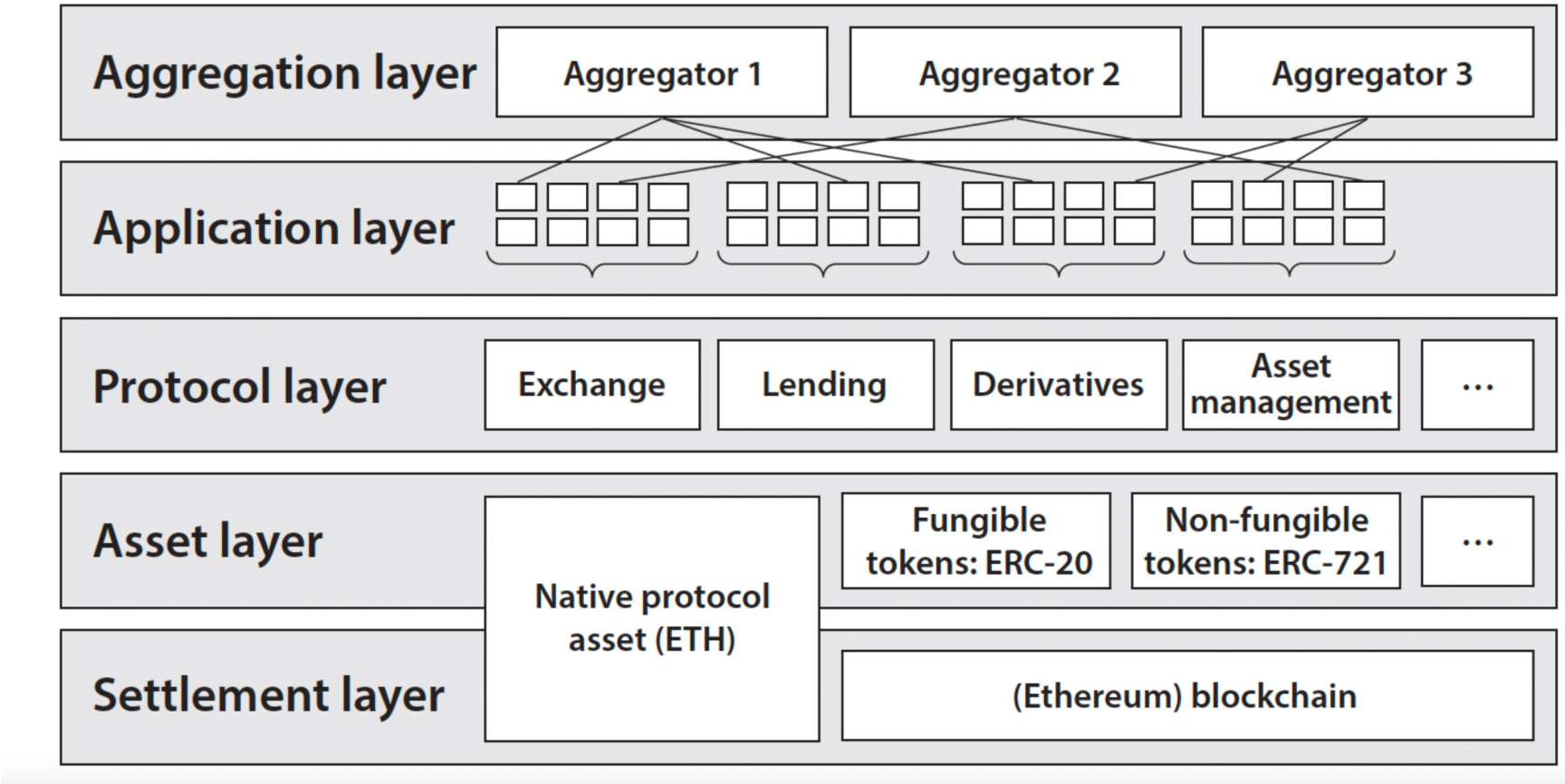
..**but** (like Bitcoin):

- **Native token** (value incentive) → **1 Ether** = 10^9 Gwei (Giga Wei) = **10^18 Wei**
  - **pay gas price** for on-chain computations/transactions
  - **pay** miners (PoW) / **stakers (PoS)** in order to keep **network security** high
  - **„programmable money“**
- Size addressable market (Linux: $16 billion; Ethereum: $260 billion)*

* 2022 data, https://www.fortunebusinessinsights.com/linux-operating-system-market-103037
→ Crypto assets market total $1.6 trillion (=$1600 billion)

Distributed Ledger Technology (**DLT**)

- **Ethereum** as a (Turing-complete) blockchain-based "**distributed computational platform**", enabling eg. "**Decentralized Finance**" (DeFi)



Schär, 2021: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3843844

Ethereum Bits & Pieces

“Execution vs Consensus*”

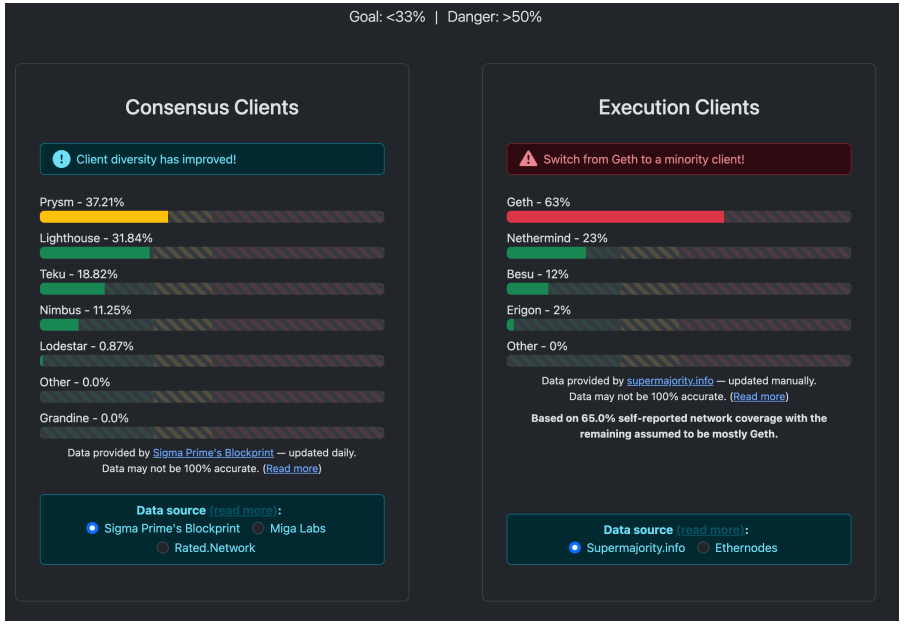
- **Protocol** (governing **rule set** for Execution/Consensus)
- **Clients** (software in compliance with specific **protocol** rules)
- **Nodes** (instance of a specific **client** implementation)
- **Application** (smart contracts deployed on **nodes**-maintained blockchain)
- Native **Ether** as **asset** (“programmable money”) and **gas**
- **Governance** Transparent, open process with “rough consensus”

*** execution:** listen/relay/exec **txs**, store current/past **db state; consensus**: **validity** and order

Client diversity (Execution)

- Enhances network resilience (bugs)
- Mitigates centralized governance concerns
- GitHub commits to client code from limited athors (affiliated with EF or ConsenSys, Gini coeff: >0.80)
- Execution:
  - Geth: Go
  - Nethermind: C#
  - Besu: Java
  - Erigon: Go
  - Reth: Rust

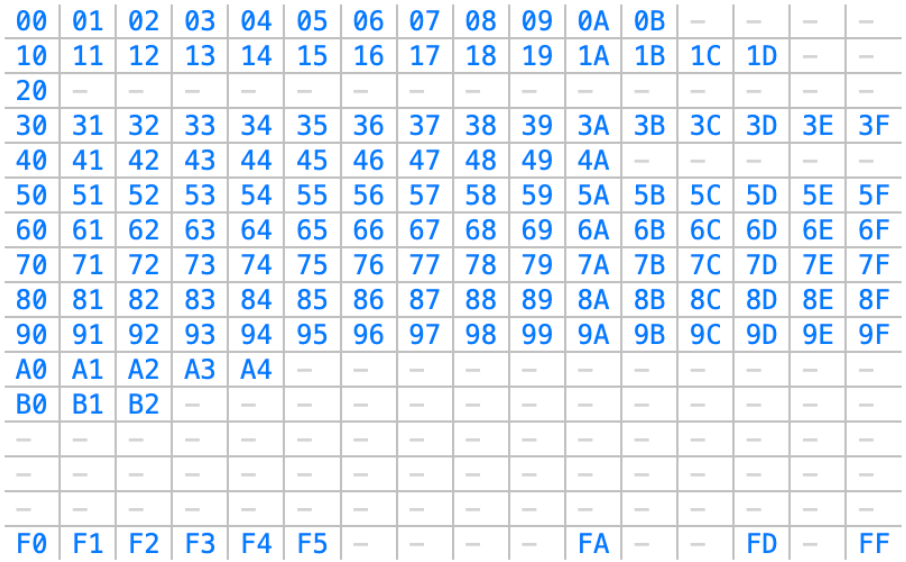
https://clientdiversity.org/



Op codes (Ethereum Virtual Machine*)

- **140 unique** Op codes, cf. https://www.ethervm.io/

Stack	Name	Gas	Initial Stack
00	STOP	0	
01	ADD	3	a, b
02	MUL	5	a, b
03	SUB	3	a, b
04	DIV	5	a, b
05	SDIV	5	a, b
06	MOD	5	a, b
07	SMOD	5	a, b
08	ADDMOD	8	a, b, N
09	MULMOD	8	a, b, N



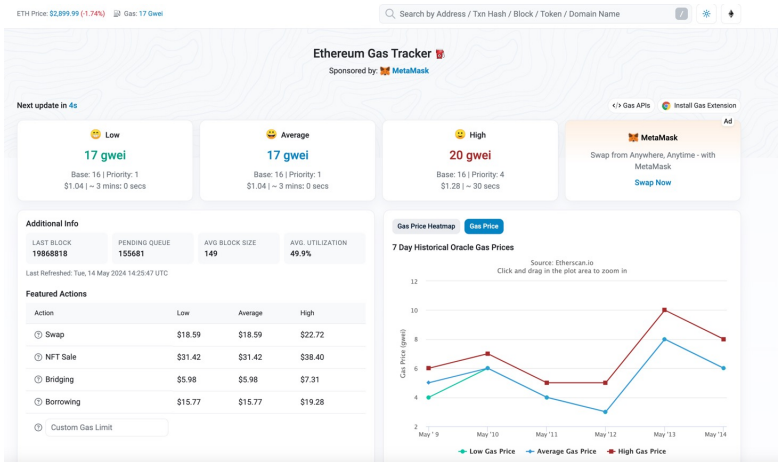
* Virtual execution environment, similar to eg. Java Virtual Machine

Gas and gas price

- **Problem**
  - prevent endless loops
  - Denial-of-Service (DoS) attacks
- **Idea**
  - each **computation** = associated **cost**
  - paid in ETH
  - Simple ERC-20 token transfer (21000 g.u.*)
- Implementation detail:
  - Dynamic adjustments of **gas price** between blocks
  - higher demand = higher gas price
  - Gas tracker: https://etherscan.io/gastracker

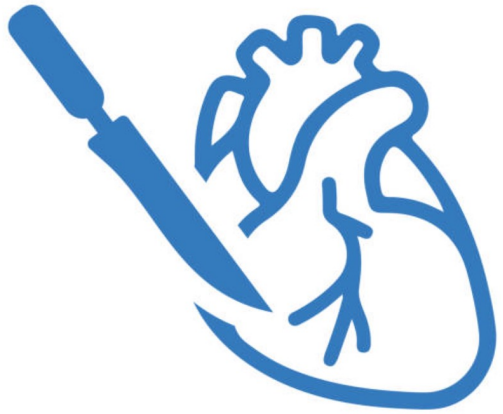
* Gas units

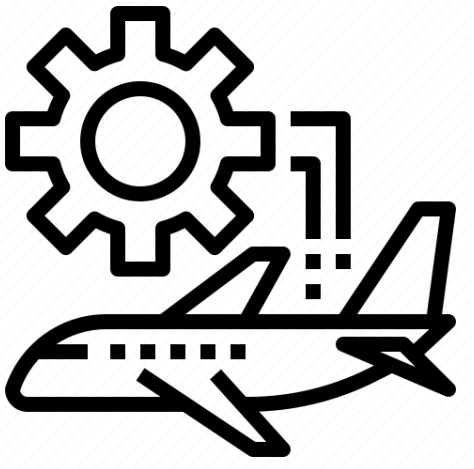
Opcode	Name	Description	Extra Info	Gas
0x00	STOP	Halts execution	-	0
0x01	ADD	Addition operation	-	3
0x02	MUL	Multiplication operation	-	5
0x03	SUB	Subtraction operation	-	3
0x04	DIV	Integer division operation	-	5
0x05	SDIV	Signed integer division operation (truncated)	-	5
0x06	MOD	Modulo remainder operation	-	5
0x07	SMOD	Signed modulo remainder operation	-	5
0x08	ADDMOD	Modulo addition operation	-	8
0x09	MULMOD	Modulo multiplication operation	-	8
0x0a	EXP	Exponential operation	-	10*
0x0b	SIGNEXTEND	Extend length of two's complement signed integer	-	5
0x0c - 0x0f	Unused	Unused	-	
0x10	LT	Less-than comparison	-	3
0x11	GT	Greater-than comparison	-	3
0x12	SLT	Signed less-than comparison	-	3
0x13	SGT	Signed greater-than comparison	-	3



PoW vs. PoS (Consensus)

- Highest security by using **proof-of-work (PoW)** as used in **Bitcoin**
  - Due to **laws of physics** (energy consumption for exhaustive computation)
- **Ethereum** (before Sept 2023): **PoW**
- **Ethereum** (after Sept 2023, "**The Merge**"): **PoS**
  - **Highly challenging upgrade** ("open heart surgery", "exchange engine while flying")

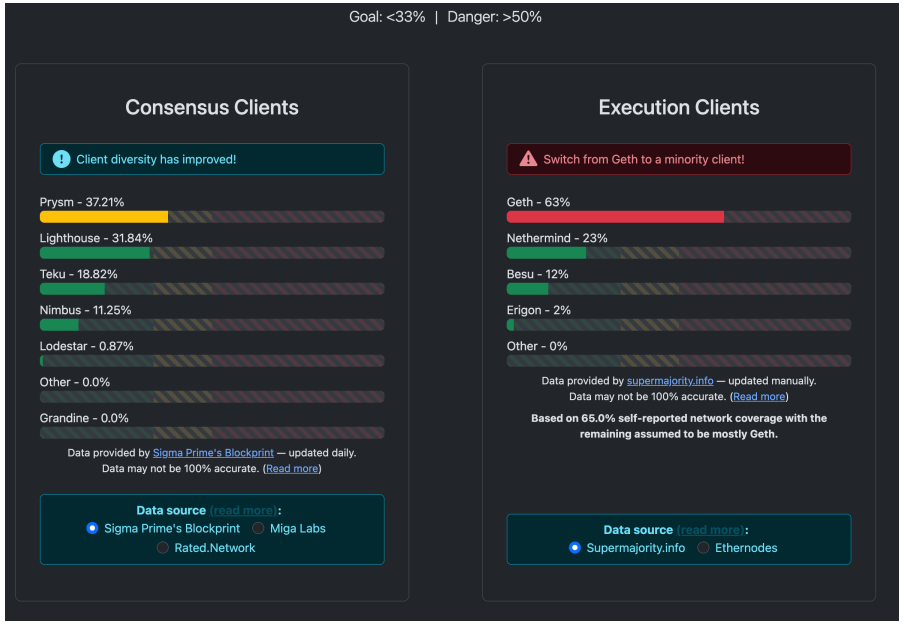




	Proof of Work (PoW)	**Proof of Stake (PoS)**
Scalability	Limited due to computational constraints.	Potentially more scalable.
Cost	High hardware and energy costs for mining.	Lower energy costs.
Decentralization	Concerns about centralization due to mining pool dominance.	Risks of centralization based on wealth distribution.
Forking Risk	Less susceptible due to resource requirements.	Slightly higher risk due to staking.

Client diversity (Consensus)

- *“Technically, clients cannot be forced to implement all finalized EIPs. They are often constrained in their resources to implement changes to the software. Not implementing the same changes as other clients could lead to consensus issues and **unintentional chain splits**. Consequently, the **client teams often work together with the community at large** to find which **finalized EIPs** should be implemented first.”*
- Consensus
  - Prysm: Go
  - Lighthouse: Rust
  - Teku: Java
  - Lodestar: TypeScript



https://clientdiversity.org/

Ethereum ecosystem main actors

- Peer-to-peer **nodes** (core infrastructure)
  - 2024: 7000 full nodes, 1 million validators (each staked 32 ETH) → 90 billion USD
- **Ethereum Foundation** (non-profit, registered in Zug CH) as "**steward**"
- **Application** (smart contract) developers
  - often controlled by **on-chain governance** and token supply via **DAO***
  - **Decentralized finance**: lending/borrowing, DEX, derivatives, asset management
  - **Digital identity**
  - **Gaming**

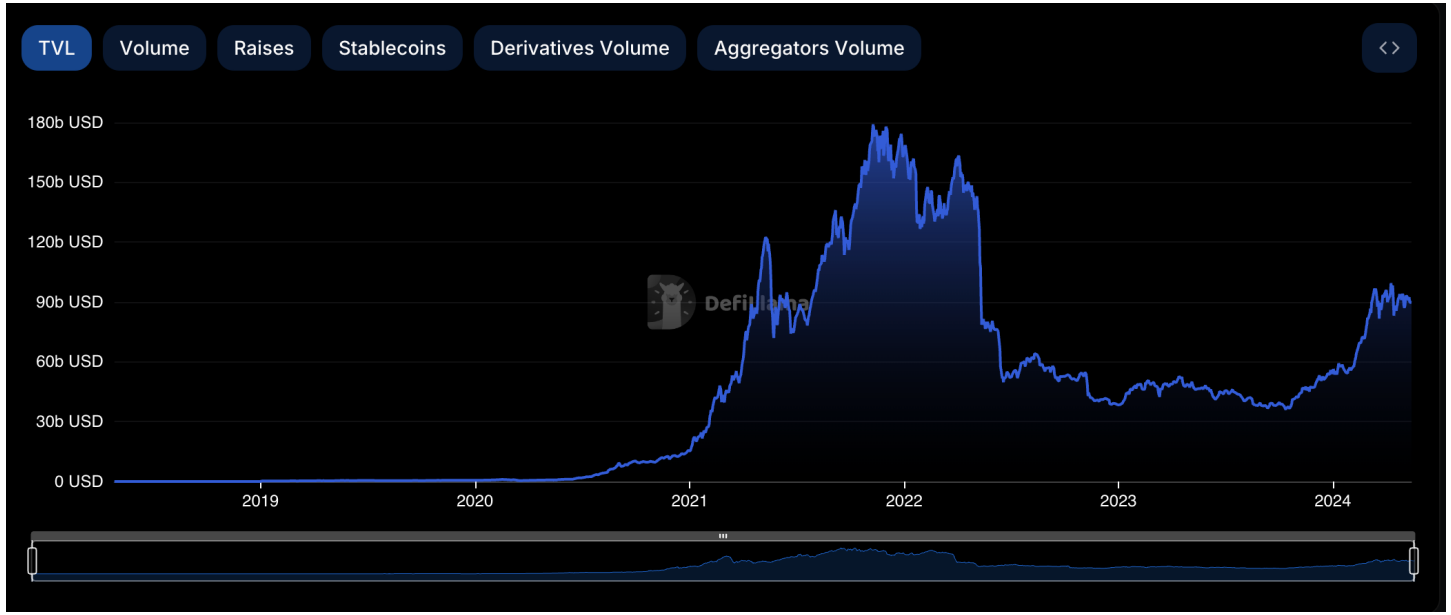
  2024: >35 million smart contracts deployed
- **End-users**
  - **"wallet" account/EOA (pseudonymous digital identity, private/public keys)**

  2024: 250 million unique addresses, 400k daily active

* Decentralized Autonomous Organization, **voting rights** via governance token

Decentralized Finance*

- **Lending/Borrowing**:
  - Lido (Liquid Staking)
  - Maker (DAI)
  - Aave



Source: defillama.com

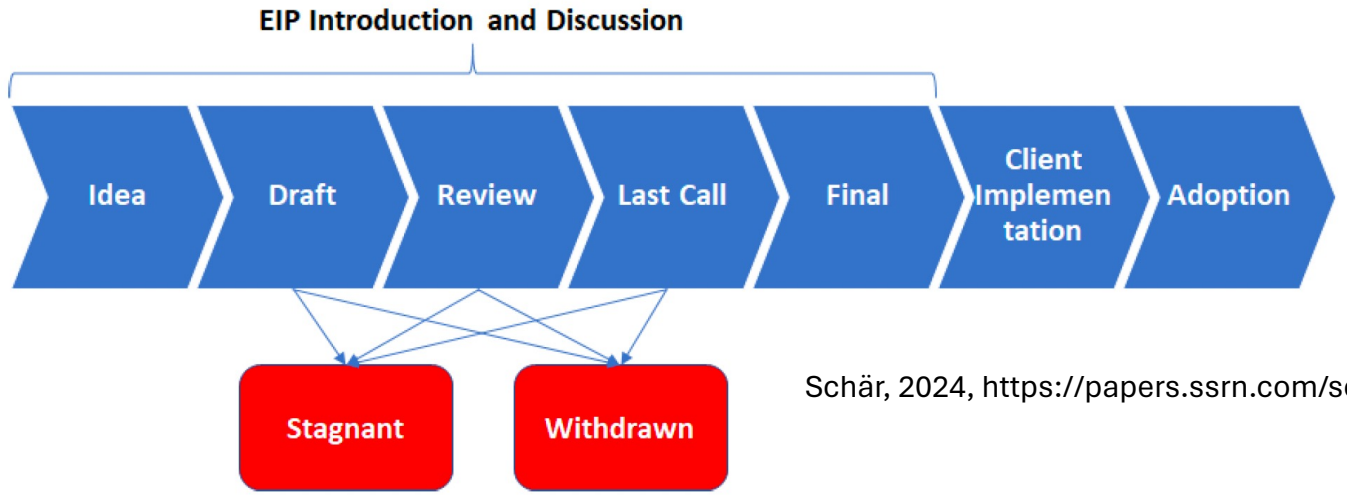
- **Exchange (DEX)**:
  - Uniswap
  - Curve
  - Balancer

- **Derivatives/Asset management**:
  - dYdX
  - Synthetix
  - Set protocol

* Stablecoins and CBDC are not considered fully decentralized/distributed

Ethereum Improvement Proposal (EIP)

- Inspired by BIP/PEP*
  - Concise description
  - Technical specification
- →”**rough consensus**” (among 1k contributors, active developers 8k): GitHub repo, forums, conferences, developer calls→**finalized**

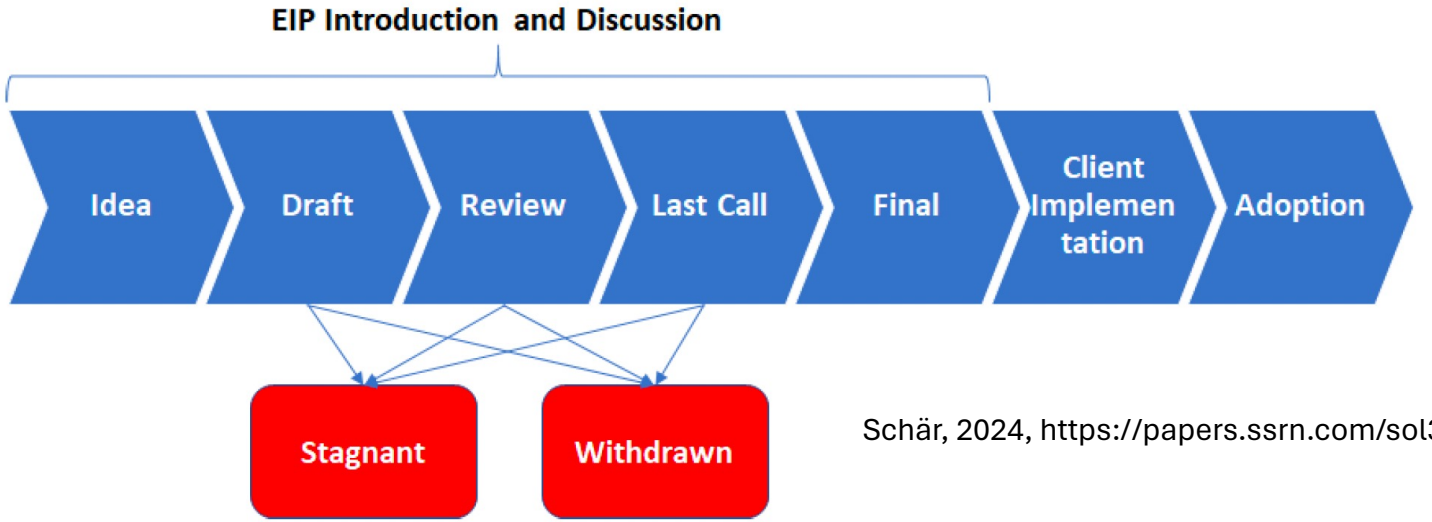


Schär, 2024, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4691000

* Bitcoin Improvement Proposal/Python Enhancement Proposal

EIP Examples: https://eips.ethereum.org/EIPS/eip-20, https://eips.ethereum.org/EIPS/eip-721, https://www.eip4844.com/ resp. https://github.com/ethereum/EIPs/blob/master/EIPS/eip-4844.md

Ethereum Improvement Proposal (EIP)

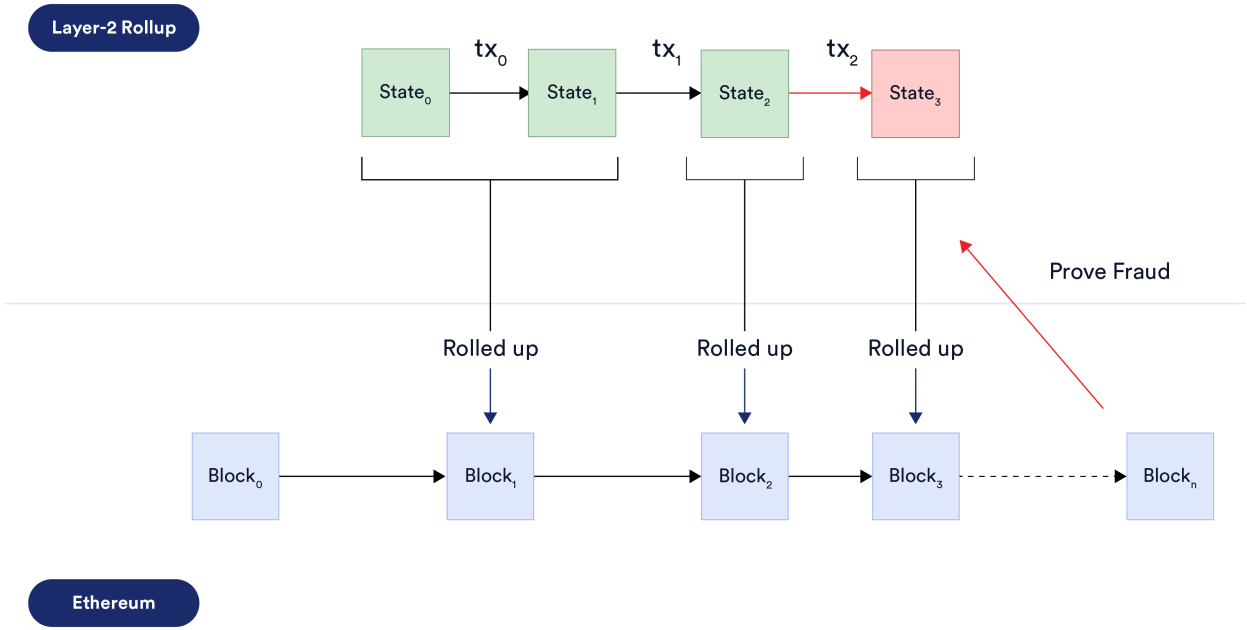


Schär, 2024, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4691000

- Client developers will integrate (bundle multiple EIPs)
- **Devnets** deployment and testing
- Orchestrated software upgrade (consensus/execution)
  - Last: Dencun, 13 March 2024, https://beaconcha.in/slot/**8626176**
  - Next: Pectra, Q4 2024 (to be finalized), https://eips.ethereum.org/EIPS/eip-7600

Layer-2 (scalability)

- Problem:
  - High costs
  - Low transaction throughput



Source: https://blog.chain.link/scaling-the-ethereum-ecosystem/

- Rollups (smart contracts on Layer-1)
  - "optimistic" (based on **fraud** proofs with report **time window**)

  vs.
  - "zero-knowledge" (based on **instant validity** proofs)

Highly secure, generic computation layer

- **Ethereum/EVM**:
  - Ethereum mainnet (Layer-1)
  - Polygon PoS (EVM-equivalent)
  - Optimism, Arbitrum, Polygon zkEVM, zkSync (Layer-2)

- **Bitcoin**:
  - BitVM (generic computation)
  - Lightning (Layer-2)

- → fruitful **technology feedback**
- → **interoperability** as key challenge!

Demo 1: wallet (self-custody) setup

- Metamask self-custody (hot wallet)

Alternatives:

- Self-custody (cold wallet), via eg. BitBox02, Nanoledger, Trezor
- Regulated Bank (hot/cold wallet)

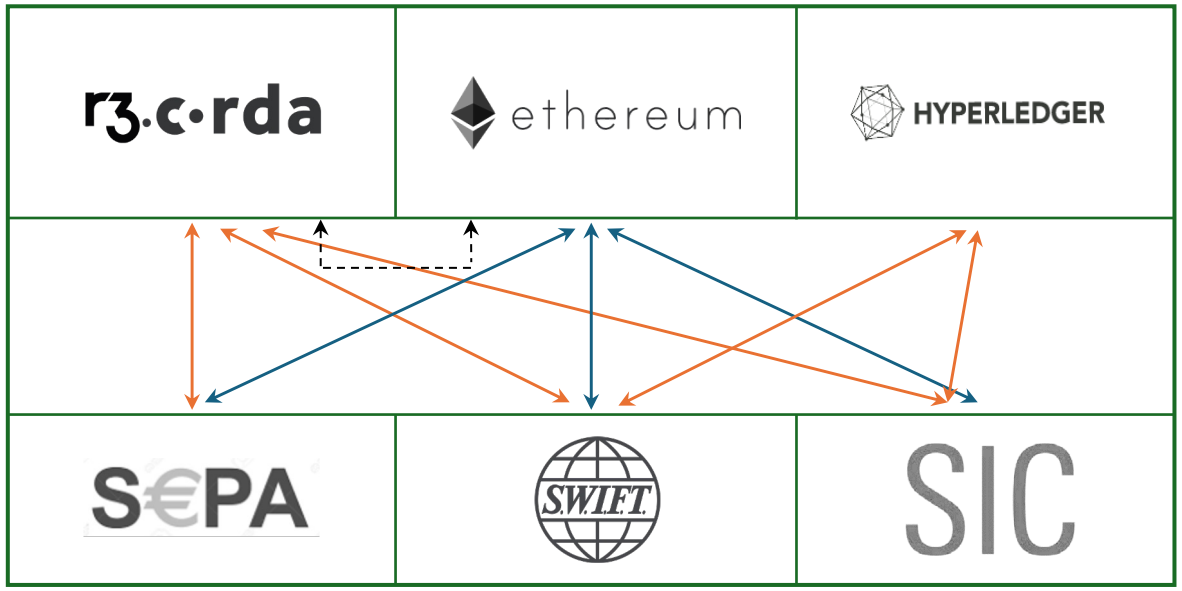
Demo 2: deployment of smart contract

using

- Remix (“IDE”, compiler, deployment, UI)
- Metamask (wallet)
- Etherscan (monitoring)

on Ethereum **Sepolia test** network

Case study: DLT2PAY



DLT2PAY

Sources: https://www.history.com/topics/landmarks/golden-gate-bridge, https://edition.cnn.com/travel/article/secrets-of-london-bridges/index.html, https://www.touropia.com/most-famous-bridges-in-the-world/

DLT2PAY: “pay on-chain in fiat”

- Central Bank Digital Currency (**CBDC**)
  - Not available (experimental state, unclear tech platform, policy implications)
- **Stablecoins** (eg. USDT, USD Coin, PYUSD, DAI, XCHF*, jCHF**, DCHF***, CCHF****)
  - Additional risks (regulatory risk, technology risk, inflationary pressure)
- **DLT/Payment links** (eg. **DLT2PAY**)
  - Seamless integration with existing IT/legal infrastructure
  - Fully leveraging Smart Contract innovation
  - Co-integrates CBDC and stablecoins

* Bitcoin Suisse
** Mt Pelerin (Jarvis Network)
*** Sygnum
**** Centi

Sources:
https://de.wikipedia.org/wiki/Mission_Control_Center#/media/Datei:Views_in_the_Main_Control_Room_(12052189474).jpg
https://www.nytimes.com/interactive/2023/04/16/science/spacex-starship-rocket-launch.html

CMTA/BX Swiss

PoC/Production (2022-24)

- **Renowned partners** (banks, digital assets infrastructure, law firms and exchanges) in Swiss market

- **First of its kind (worldwide)** project to innovate **on-chain trade of tokenized securities** and **off-chain fiat payments**

- **PoC** as **blueprint** for **further expansion** (other DLT networks, other exchanges, other jurisdictions, other payment systems, eg. T2/TARGET2)

- **Key innovations**: no prefunding, no CSD/CCP, public blockchain, near-instant/automated

→ Go-Live **PoC** Q4/2022, cf. https://cmta.ch/news-articles/trading-and-settlement-in-digital-securities

→ Go-Live **Production** Q3/2024, Goals: **time to finality (~15min)**

Demo 3: DvP wout counterparty risk

- **Delivery-vs-Payment** (DvP) of **tokenized securities** (shares, bonds) via licensed “DLT-Handelssystem” (FINMA) in **CHF fiat**