OST
Eastern Switzerland
University of Applied Sciences

Blockchain (BlCh)

Ethereum

Thomas Bocek

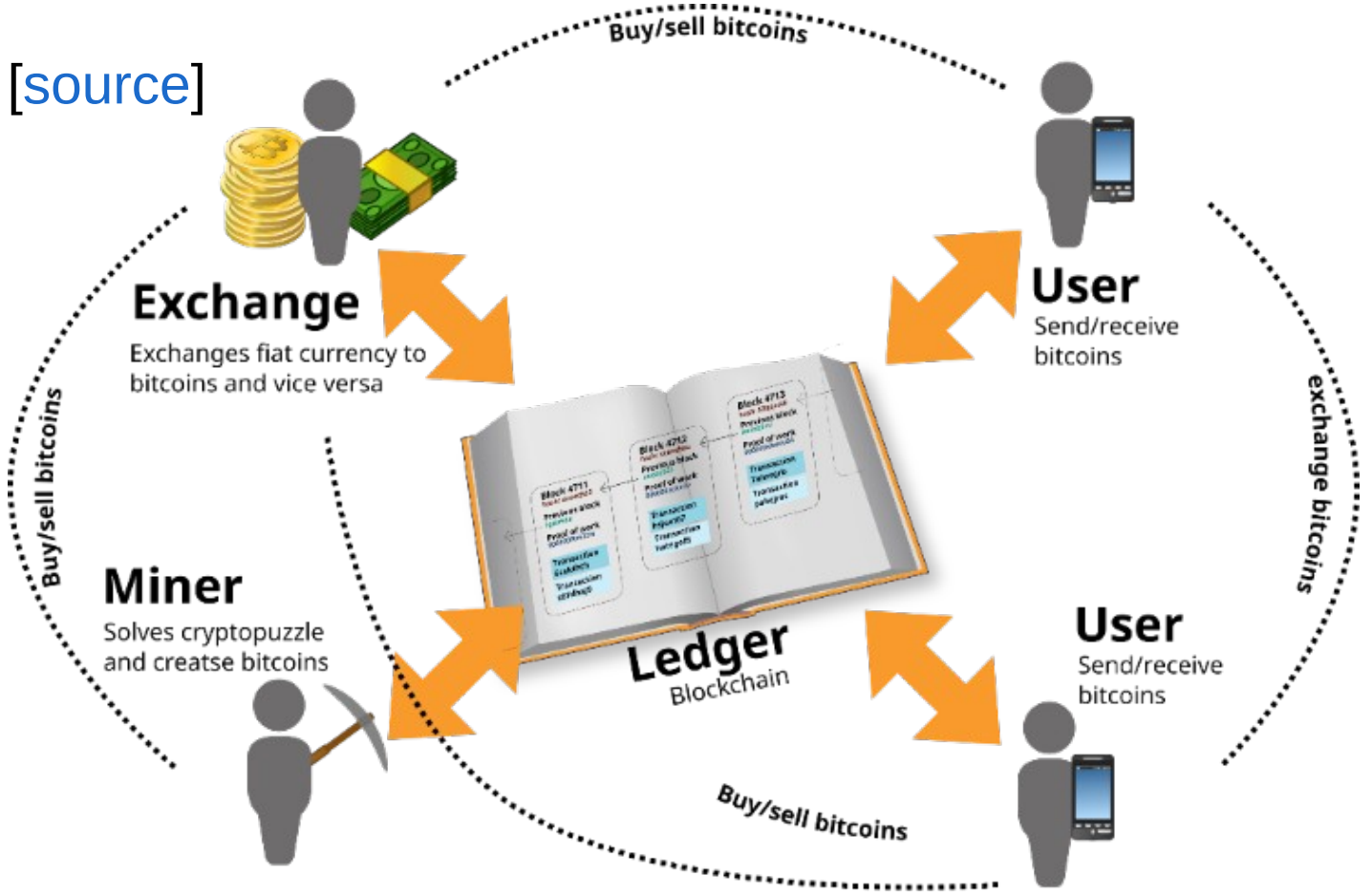
25.09.2025

Learning Goals

- Lecture 3
  - Ethereum basic concepts
    - Gas
    - Smart contracts
    - Account / UTXO
    - Web3
    - Architecture
  - 51% Attacks

Summary: Bitcoin Stakeholders

- Building blocks [source]



Bitcoin / Ethereum

- Bitcoin vs. Ethereum
  - Implementing new features slow
    - Many Bitcoin hardforks (segregated witness vs. increasing block size voting) Cash vs. SV
  - Bitcoin Script limited
    - Lightning network
  - Pros and Cons – no silver bullet
- Ethereum (1 ETH ~ 2900$)
  - Generalized blockchain (loops, arithmetics, etc.)
  - White paper released in December 2013
  - Protocols designed from scratch (not like Litecoin, Peercoin)
- Ethereum foundation located in Zug (initiator known) - non-profit foundation
- Mining reward ~ block every ~12s – ~3%

Vitalik Buterin

OST

Ethereum History

- Olympic (past) – released 09.05.2015
  - Last Ethereum Proof-of-Concept series
  - “Olympic will feature a total prize fund of up to 25,000 ether” (now 100m USD)
- Frontier (past) - released 30.07.2015
  - Main public network, “Beta”/use at your own risk
- Homestead (past) - released 14.03.2016
  - Public network considered “stable”, integrate critical protocol changes
- Fusaka – 03.12.2025

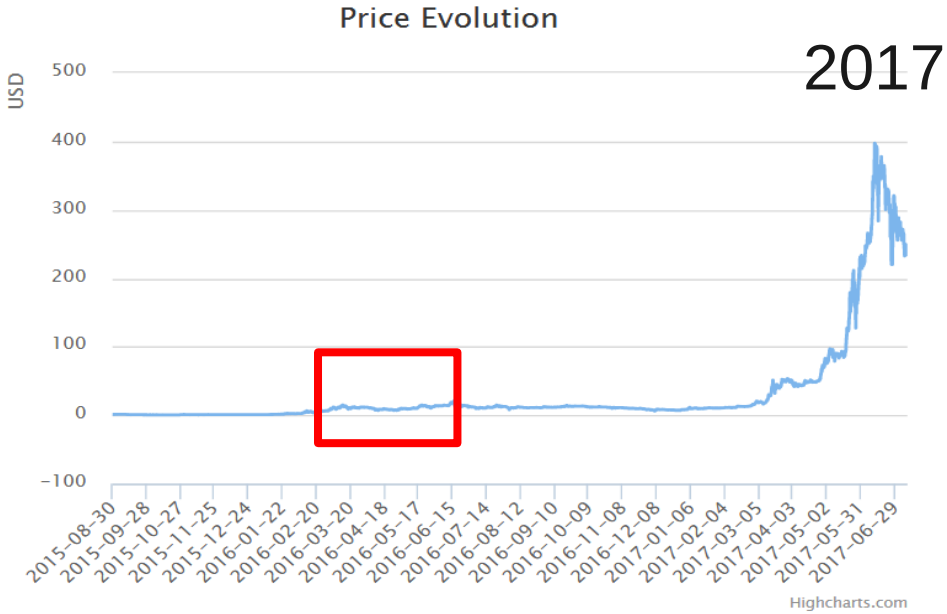
Name	Release Date	Description
Prague-Electra ("Pectra")	May 7, 2025	The Prague-Electra ("Pectra") upgrade included several improvements to the Ethereum protocol aimed at enhancing the experience for all users, layer 2 networks, stakers and node operators.
Cancun-Deneb ("Dencun")	Mar 13, 2024	Introduced EIP-4844 (Proto-Danksharding) for reducing layer 2 rollup costs, among other enhancements.
Shanghai-Capella ("Shapella")	Apr 12, 2023	Enabled staking withdrawals from the consensus layer to the execution layer.
Paris (The Merge)	Sep 15, 2022	Transitioned Ethereum from proof-of-work to proof-of-stake, significantly reducing energy consumption of the network.
Bellatrix	Sep 6, 2022	Prepared the network for The Merge by updating fork choice rules and bringing validator penalties to full enforcement.
Gray Glacier	Jun 29, 2022	Delayed the difficulty bomb to ease the transition to proof-of-stake.
Arrow Glacier	Dec 8, 2021	Similar to Gray Glacier, it delayed the difficulty bomb to ease the transition to proof-of-stake.
Altair	Oct 27, 2021	Enhanced support for light clients, increased validator penalties, and introduced sync committees.
London	Aug 5, 2021	Implemented EIP-1559, altering the transaction fee model to improve predictability and reduce fee volatility.
Berlin	Apr 15, 2021	Improved gas costs for certain EVM actions and added support for multiple transaction types.
Muir Glacier	Jan 2, 2020	Delayed the Ethereum difficulty bomb, intending to decrease block times until the next planned upgrade.
Istanbul	Dec 8, 2019	Implemented various EIPs to enhance denial-of-service attack resilience, and gas cost efficiencies for certain EVM operations.
Constantinople	Feb 28, 2019	Introduced several cost-adjustments for on-chain operations to improve network performance and interoperability with Zcash.
Byzantium	Oct 16, 2017	Part of the Metropolis update, it included privacy improvements and added new opcodes for contract developers.
Spurious Dragon	Nov 22, 2016	Enhanced network security and refined the blockchain following the DAO attack by introducing state clearing.
Tangerine Whistle	Oct 18, 2016	Addressed the denial-of-service attack vectors and adjusted the gas pricing for various opcodes.
Homestead	Mar 14, 2016	Officially moved Ethereum from beta to a more stable stage with improvements to transaction processing.
Frontier	Jul 30, 2015	The initial release of Ethereum, setting the foundation of the blockchain with the capability of executing smart contracts.

https://ethereum.org/history/

OST

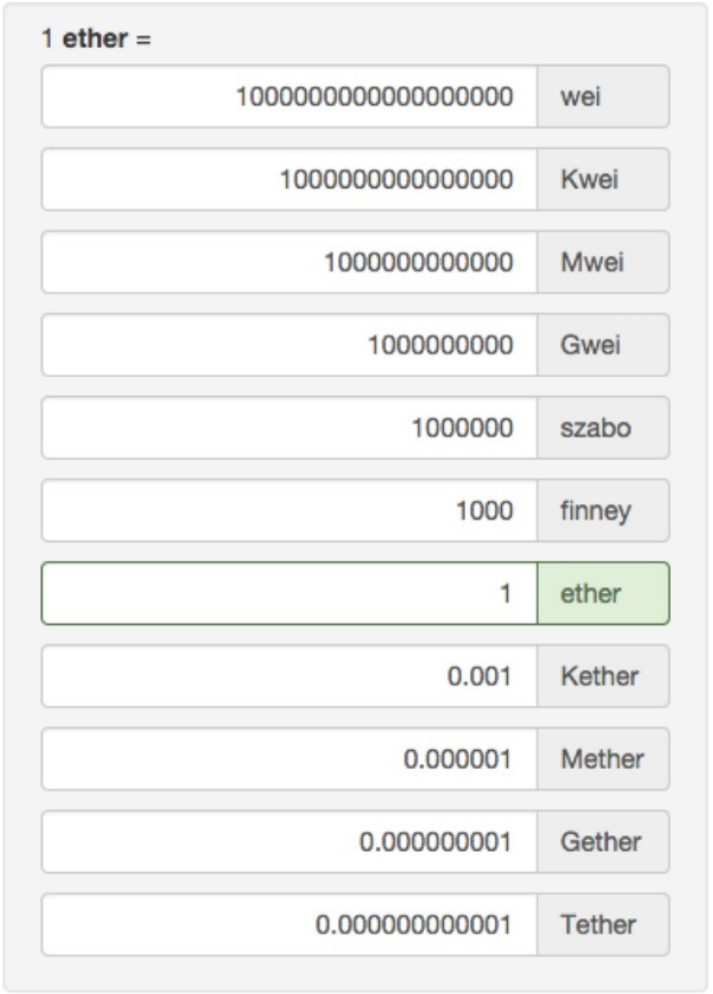
Ethereum Stats

- Basic Stats
  - 2nd in market cap ~ 480b USD
  - Daily transactions
    now ~1500k per day (17tx/s avg)
  - Node count (~10k)
  - Blocksize ~90-270KB
  - Accounts (340mio)
  - Mining – 35m ETH staked, Top 12 (2023)



What is Gas? (1)

- Past: Gas Price set by Miner
- Now: algorithmic base fee + priority fee
  - Gas price ~36+2 gwei
- Miner decides which transaction at which gas price to include
  - Market for transactions
- Gas price with low priority fee, longer waiting time until TX will be included
- Units:



OST

What is Gas? (2)

- Block time: ~12-13s

- Smart Contracts are turing complete
  - Every instruction needs to be paid for (example)
- Malicious / faulty contracts
  - If you run out of gas, state is reverted, ETH gone

$W_{zero} = \{\text{STOP, RETURN}\}$
$W_{base} = \{\text{ADDRESS, ORIGIN, CALLER, CALLVALUE, CALLDATASIZE, CODESIZE, GASPRICE, COINBASE, TIMESTAMP, NUMBER, DIFFICULTY, GASLIMIT, POP, PC, MSIZE, GAS}\}$
$W_{verylow} = \{\text{ADD, SUB, NOT, LT, GT, SLT, SGT, EQ, ISZERO, AND, OR, XOR, BYTE, CALLDATALOAD, MLOAD, MSTORE, MSTORE8, PUSH*, DUP*, SWAP*}\}$
$W_{low} = \{\text{MUL, DIV, SDIV, MOD, SMOD, SIGNEXTEND}\}$
$W_{mid} = \{\text{ADDMOD, MULMOD, JUMP}\}$
$W_{high} = \{\text{JUMPI}\}$
$W_{extcode} = \{\text{EXTCODESIZE}\}$

source

Appendix G. Fee Schedule

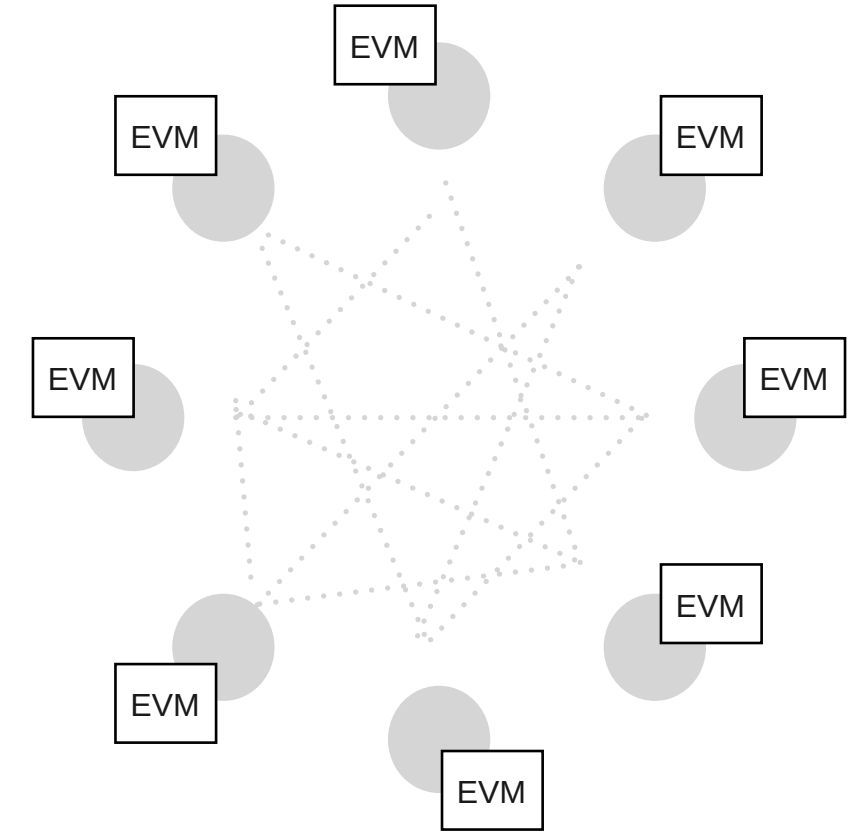
The fee schedule G is a tuple of 31 scalar values corresponding to the relative costs, in gas, of a number of abstract operations that a transaction may effect.

Name	Value	Description*
G_{zero}	0	Nothing paid for operations of the set W_{zero}.
G_{base}	2	Amount of gas to pay for operations of the set W_{base}.
$G_{verylow}$	3	Amount of gas to pay for operations of the set $W_{verylow}$.
G_{low}	5	Amount of gas to pay for operations of the set W_{low}.
G_{mid}	8	Amount of gas to pay for operations of the set W_{mid}.
G_{high}	10	Amount of gas to pay for operations of the set W_{high}.
$G_{extcode}$	700	Amount of gas to pay for operations of the set $W_{extcode}$.
$G_{balance}$	400	Amount of gas to pay for a BALANCE operation.
G_{sload}	200	Paid for a SLOAD operation.
$G_{jumpdest}$	1	Paid for a JUMPDEST operation.
G_{sset}	20000	Paid for an SSTORE operation when the storage value is set to non-zero from zero.
G_{sreset}	5000	Paid for an SSTORE operation when the storage value's zeroness remains unchanged or is set to zero.
R_{sclear}	15000	Refund given (added into refund counter) when the storage value is set to zero from non-zero.
$R_{suicide}$	24000	Refund given (added into refund counter) for suiciding an account.
$G_{suicide}$	5000	Amount of gas to pay for a SUICIDE operation.
G_{create}	32000	Paid for a CREATE operation.
$G_{codedeposit}$	200	Paid per byte for a CREATE operation to succeed in placing code into state.
G_{call}	700	Paid for a CALL operation.
$G_{callvalue}$	9000	Paid for a non-zero value transfer as part of the CALL operation.
$G_{callstipend}$	2300	A stipend for the called contract subtracted from $G_{callvalue}$ for a non-zero value transfer.
$G_{newaccount}$	25000	Paid for a CALL or SUICIDE operation which creates an account.
G_{exp}	10	Partial payment for an EXP operation.
$G_{expbyte}$	10	Partial payment when multiplied by $\lceil \log_{256}(exponent) \rceil$ for the EXP operation.
G_{memory}	3	Paid for every additional word when expanding memory.
$G_{txcreate}$	32000	Paid by all contract-creating transactions after the *Homestead transition*.
$G_{txdatazero}$	4	Paid for every zero byte of data or code for a transaction.
$G_{txdatanonzero}$	68	Paid for every non-zero byte of data or code for a transaction.
$G_{transaction}$	21000	Paid for every transaction.
G_{log}	375	Partial payment for a LOG operation.
$G_{logdata}$	8	Paid for each byte in a LOG operation's data.
$G_{logtopic}$	375	Paid for each topic of a LOG operation.
G_{sha3}	30	Paid for each SHA3 operation.
$G_{sha3word}$	6	Paid for each word (rounded up) for input data to a SHA3 operation.
G_{copy}	3	Partial payment for *COPY operations, multiplied by words copied, rounded up.
$G_{blockhash}$	20	Payment for BLOCKHASH operation.

OST

Ethereum smart contract

- Computation and storage on EVM is "very expensive“: every contract is run on every full Ethereum node
  - Result on every node is the same
  - Global computer, always running, always correct
- Account-based
  - 2 types: externally controlled, contract
    - Both can have and send ether
    - External accounts: controlled by private keys
  - Contract accounts never executed on their own
    - Contract accounts: controlled by code
    - All action fired from externally controlled accounts



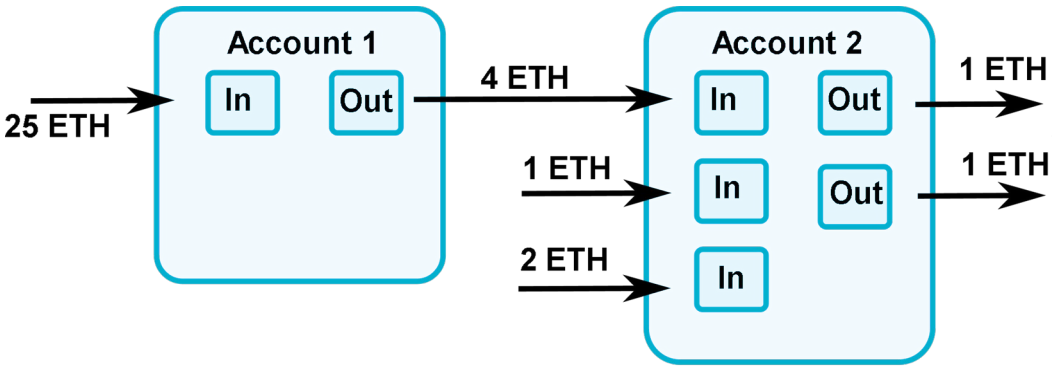
ethereum

OST

Account vs UTXO - Introduction

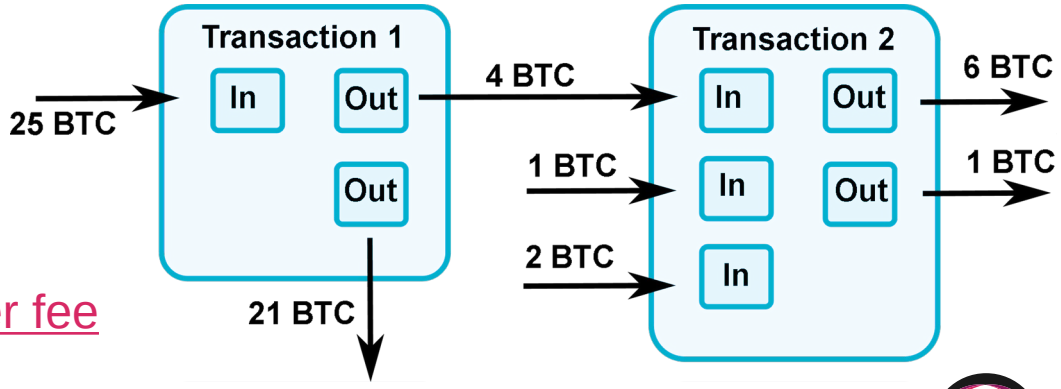
Account-based

- Global state stores a list of accounts with balances and code
- Transaction is valid if the sending account has enough balance
  - Balance on sender is deducted, new balance
- If the receiving account has code, the code runs, and state may be changed
  - Signature must match sending account



UTXO-based

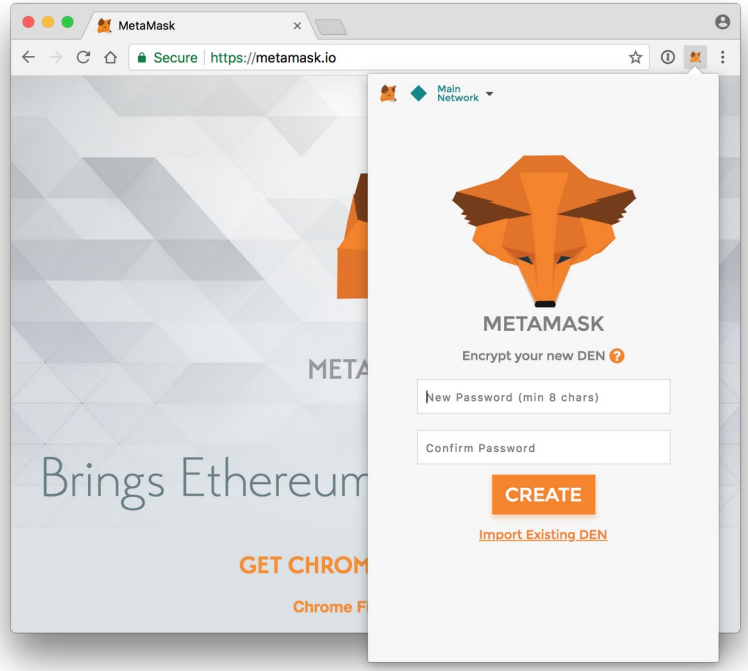
- Every referenced input must be valid and not yet spent
- Total value of the inputs must equal or exceed the total value of the outputs
  - You always spend all outputs
- Transaction must have a signature matching the owner of the input for every input
  - Script determines if input is valid



OST

MetaMask

- MetaMask
  - Web3 browser plugin to make Ethereum transactions in browsers
  - Manage your key pairs and sign blockchain transactions
  - MetaMask injects javascript library - ethers.js / viem
  - Uses infura
- Remix IDE: https://remix.ethereum.org
- Testnet: sepolia
  - https://sepolia.etherscan.io/ (blockchain explorer)



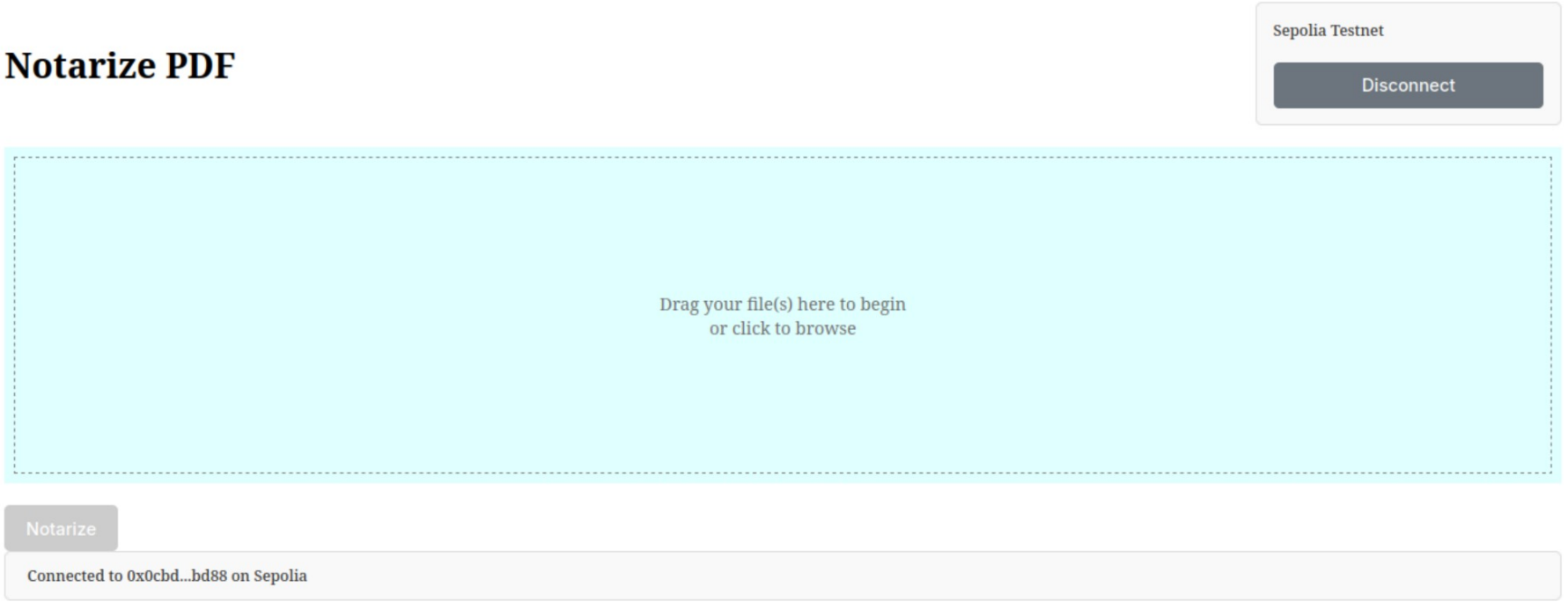

```
INFO [05-08|17:14:43] Commit new mining work                   number=891910 txs=0  uncles=0 elapsed=392.257µs
INFO [05-08|17:15:06] Imported new chain segment               blocks=1 txs=0  mgas=0.000 elapsed=17.225ms  mgasps=0.000   number=891910 hash=812c12…de3c2e
INFO [05-08|17:15:06] Commit new mining work                   number=891911 txs=2  uncles=0 elapsed=6.039ms
INFO [05-08|17:15:16] Successfully sealed new block            number=891911 hash=9efde0…7642c5
INFO [05-08|17:15:16] 🔨 mined potential block                  number=891911 hash=9efde0…7642c5
INFO [05-08|17:15:16] Commit new mining work                   number=891912 txs=0  uncles=0 elapsed=507.117µs
INFO [05-08|17:15:23] Imported new chain segment               blocks=1 txs=0  mgas=0.000 elapsed=6.596ms  mgasps=0.000   number=891912 hash=c80dc0…5fbfde
```

- No mining (use faucet https://sepolia-faucet.pk910.de/)

OST

Example

- Installation of notary-example
  - docker compose up --build
  - pnpm install && pnpm run dev
- Open Browser: http://localhost:3000

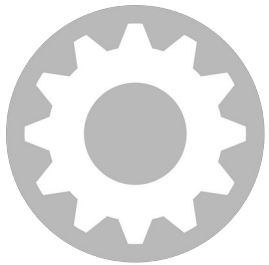


OST

Architecture Overview

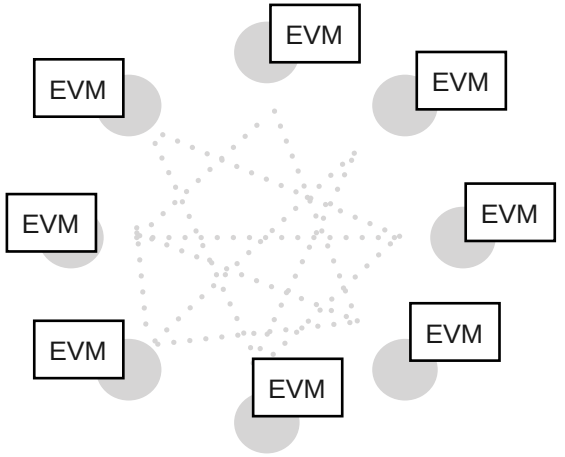
```
pragma solidity
^0.7.1;

contract Notary {
    …
}
```

METAMASK



Compiler

Remix IDE



ethereum

EVM

Local Ethereum Node

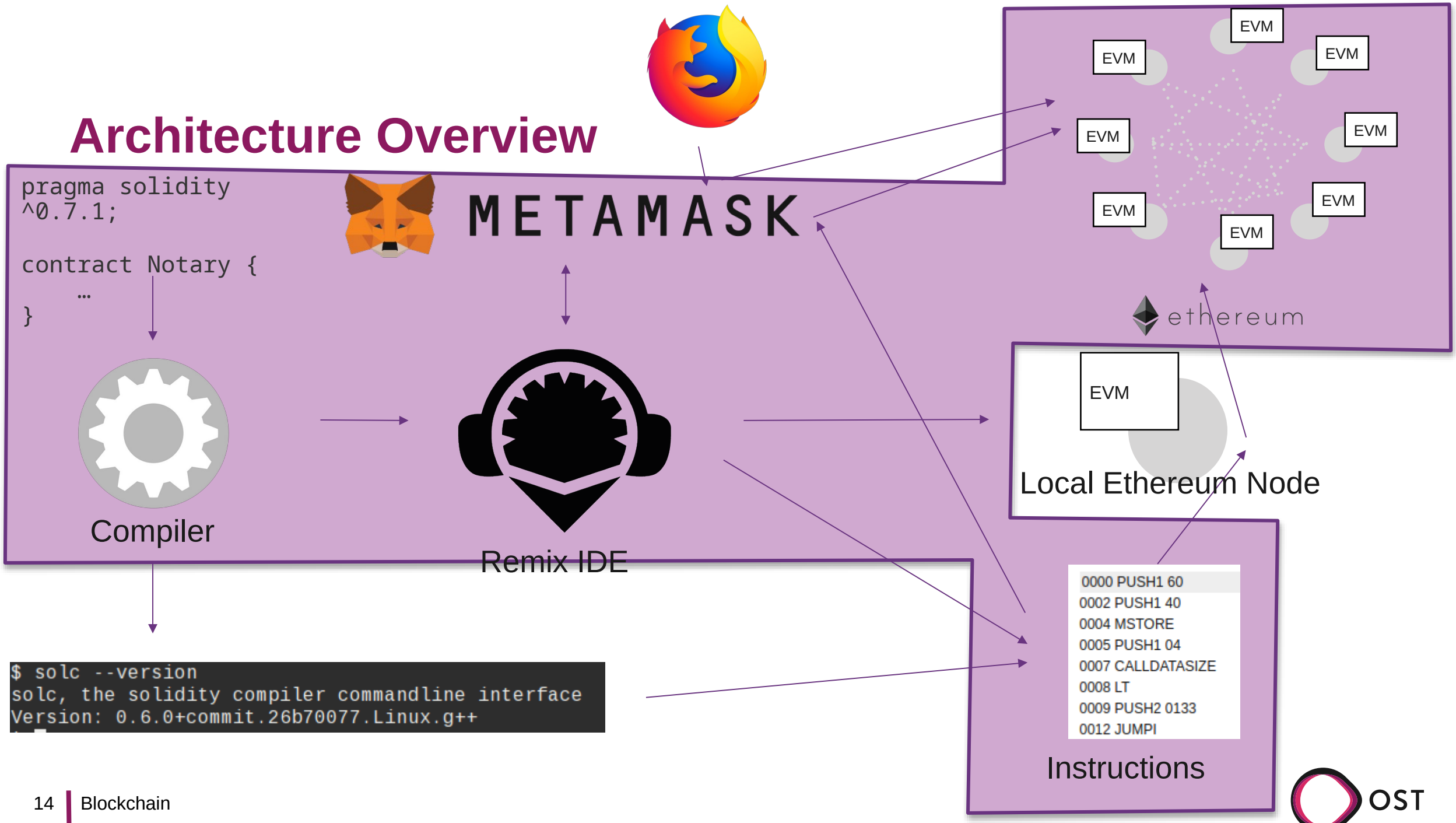
```
$ solc --version
solc, the solidity compiler commandline interface
Version: 0.6.0+commit.26b70077.Linux.g++
```

```
0000 PUSH1 60
0002 PUSH1 40
0004 MSTORE
0005 PUSH1 04
0007 CALLDATASIZE
0008 LT
0009 PUSH2 0133
0012 JUMPI
```

Instructions

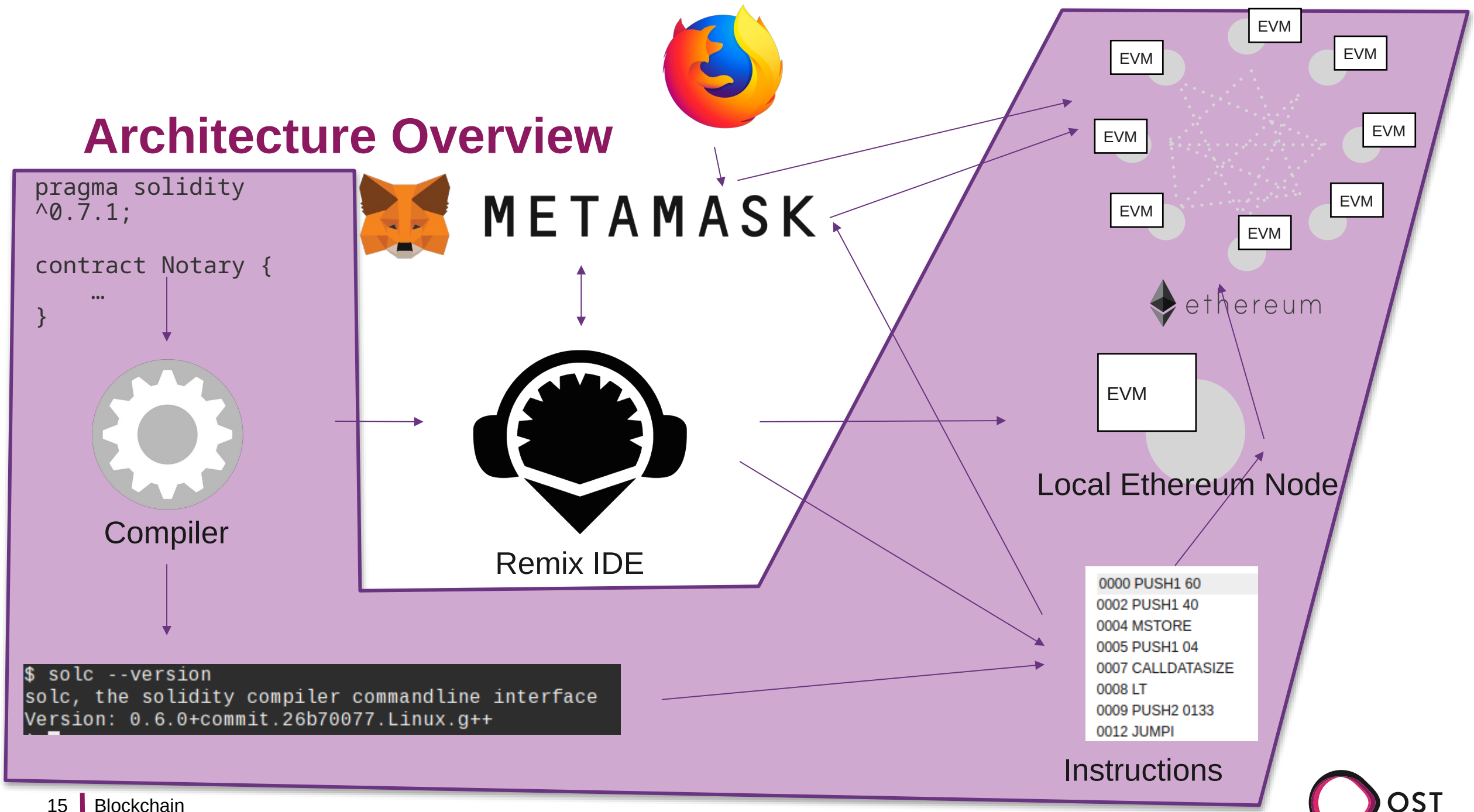
OST

Architecture Overview



OST

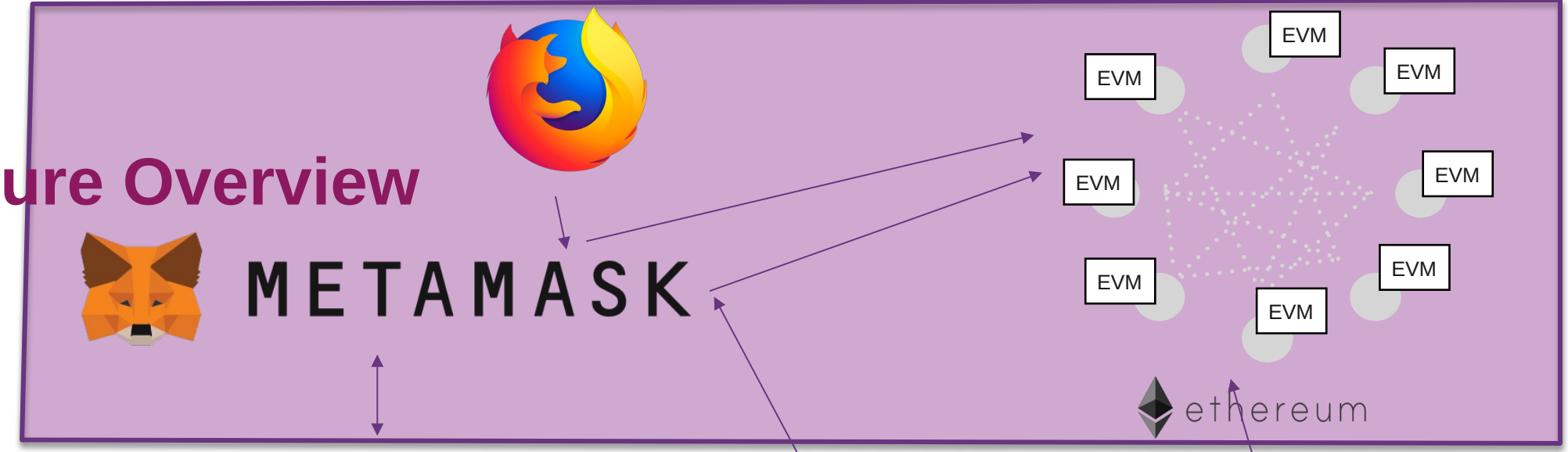
Architecture Overview



OST

Architecture Overview

```
pragma solidity
^0.7.1;

contract Notary {
    …
}
```



Compiler

Remix IDE

EVM

Local Ethereum Node

```
$ solc --version
solc, the solidity compiler commandline interface
Version: 0.6.0+commit.26b70077.Linux.g++
```

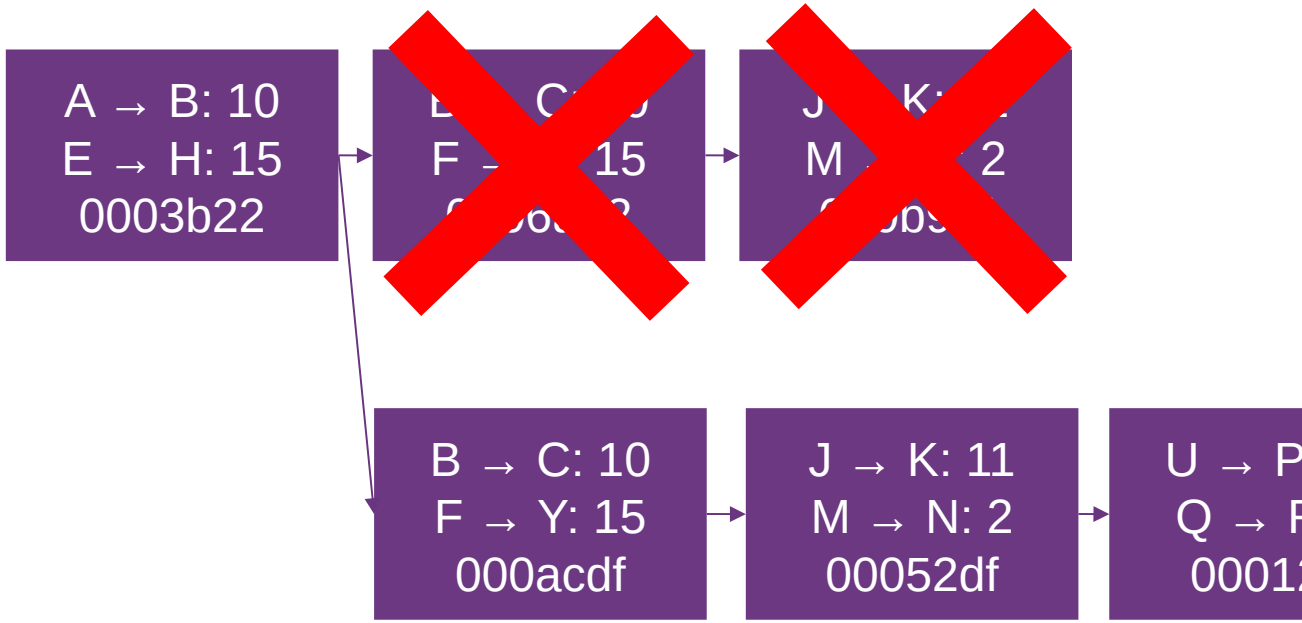
```
0000 PUSH1 60
0002 PUSH1 40
0004 MSTORE
0005 PUSH1 04
0007 CALLDATASIZE
0008 LT
0009 PUSH2 0133
0012 JUMPI
```

Instructions

OST

51% Attack

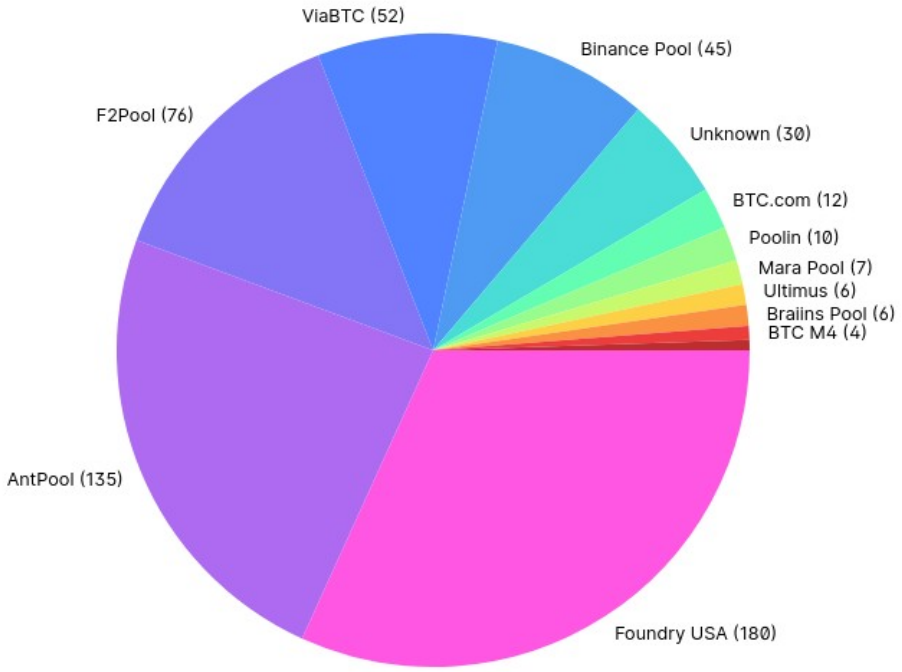
- “If a majority of CPU power is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing chains.”
  - https://bitcoin.org/bitcoin.pdf
- PoW: majority of hashing power, PoS: majority of coins
- How expensive is a 51% attack?
  - Buy an attack?
- Double spend, or rollback transactions
  - X is an exchange
  - Mine secretly, Y is your address
  - X arrived – payout (1 block conf.)
  - You mine faster, broadcast secret chain
  - Tx F→X: 15 never happened, goes to Y



51% Attack

- Control over 50% of the scarce resources
  - Pools: cooperative puzzle solving
  - Solo: competitive puzzle solving

http://blockchain.info/pools



- 07.08.2021: Bitcoin SV rocked by three 51% attacks in as many months [link]
- 30.08.2020: Ethereum Classic suffers another 51% attack [link]
  - “The total value of the double spends that we have observed thus far is 219,500 ETC (~$1.1M).”
- 08.11.2020: Grin network hit with 51% attack while GRIN token remains resilient [link]
- 17.08.2025: Kraken pauses Monero deposits following 51% attack [link]

OST