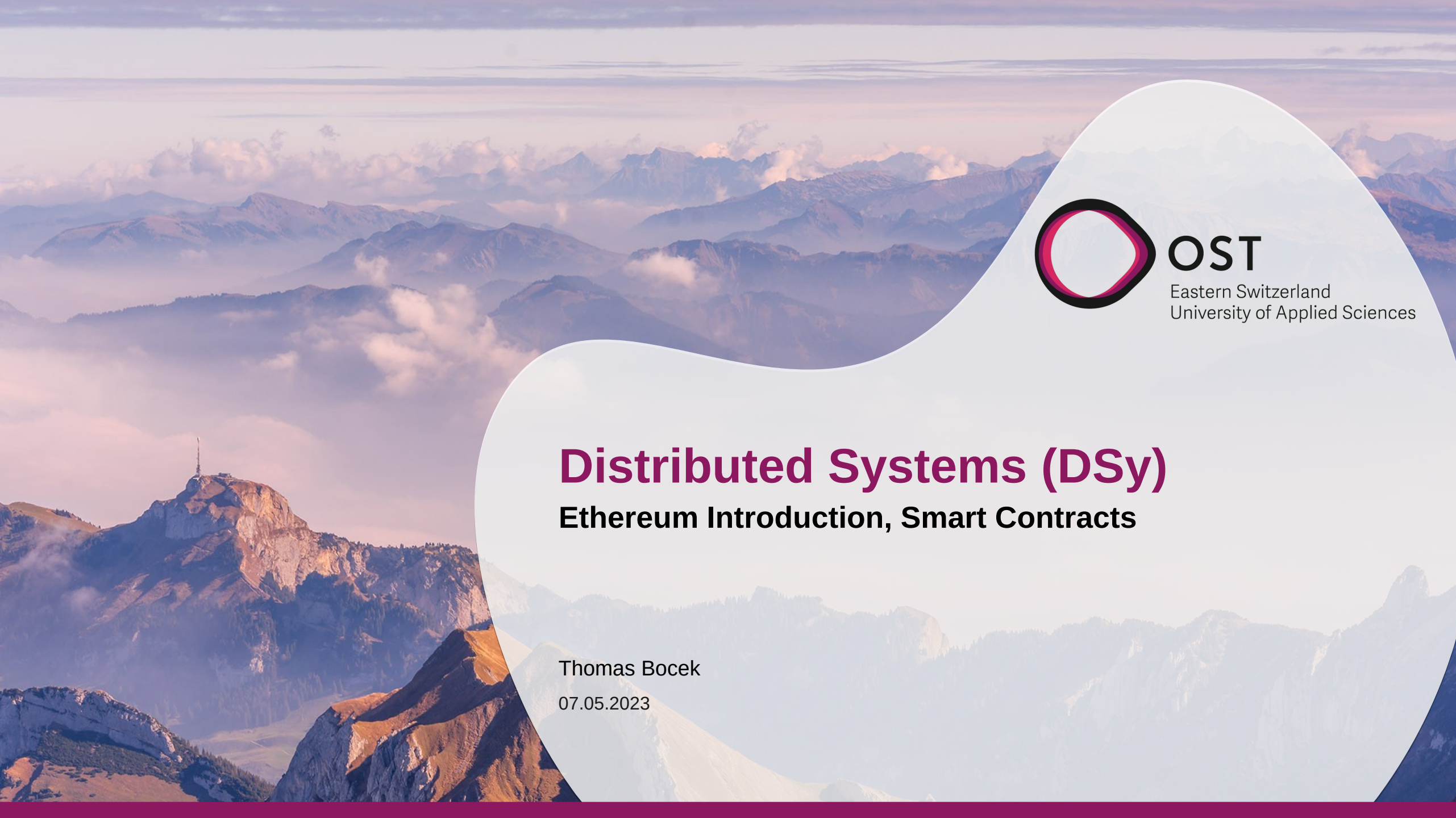


OST
Eastern Switzerland
University of Applied Sciences

Distributed Systems (DSy)

Ethereum Introduction, Smart Contracts

Thomas Bocek

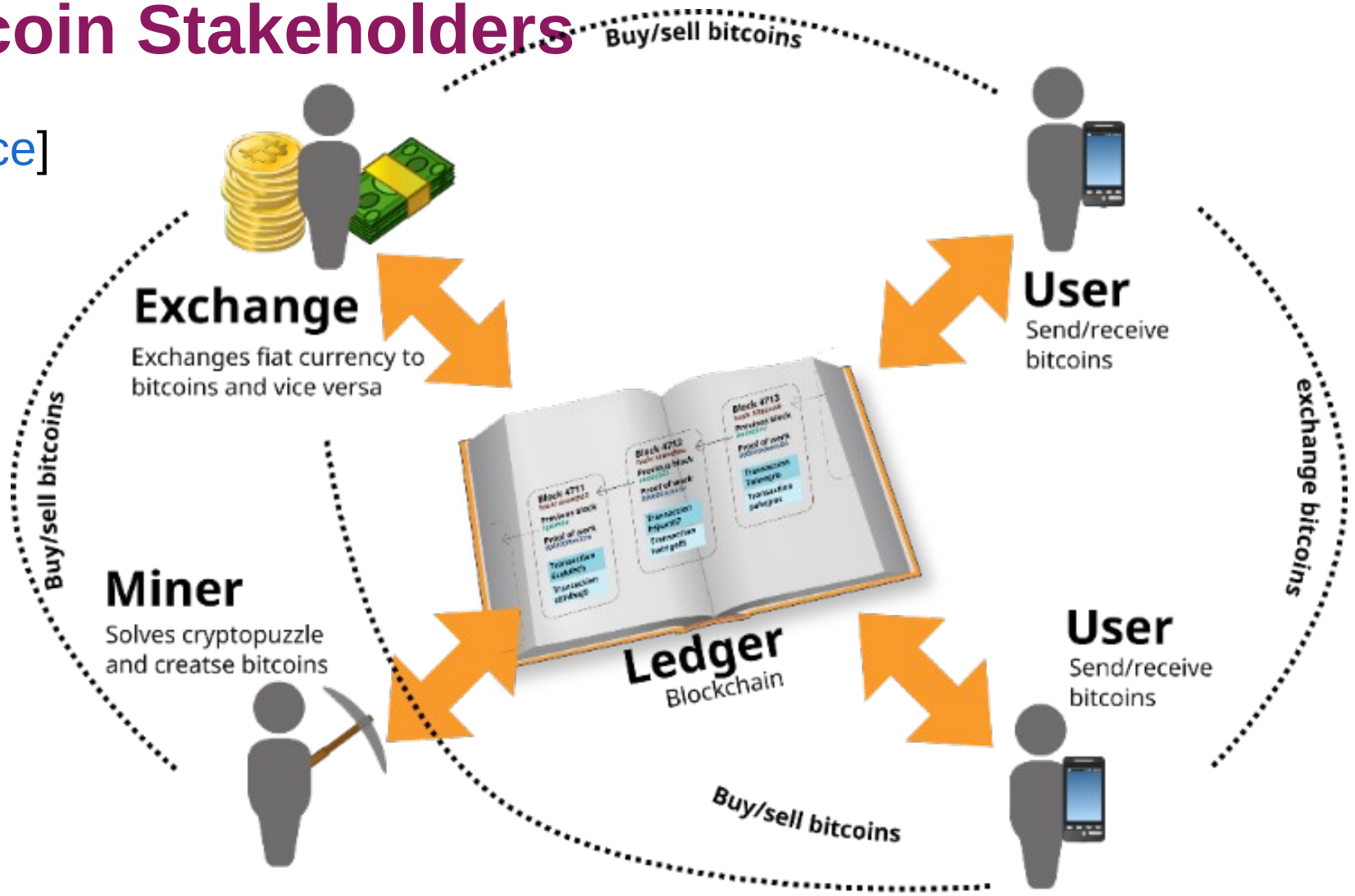
07.05.2023

Learning Goals

- Lecture 13
  - 51% Attacks
  - Ethereum basic concepts
    - Gas
    - Smart contracts
    - Account / UTXO
    - Web3

Summary: Bitcoin Stakeholders

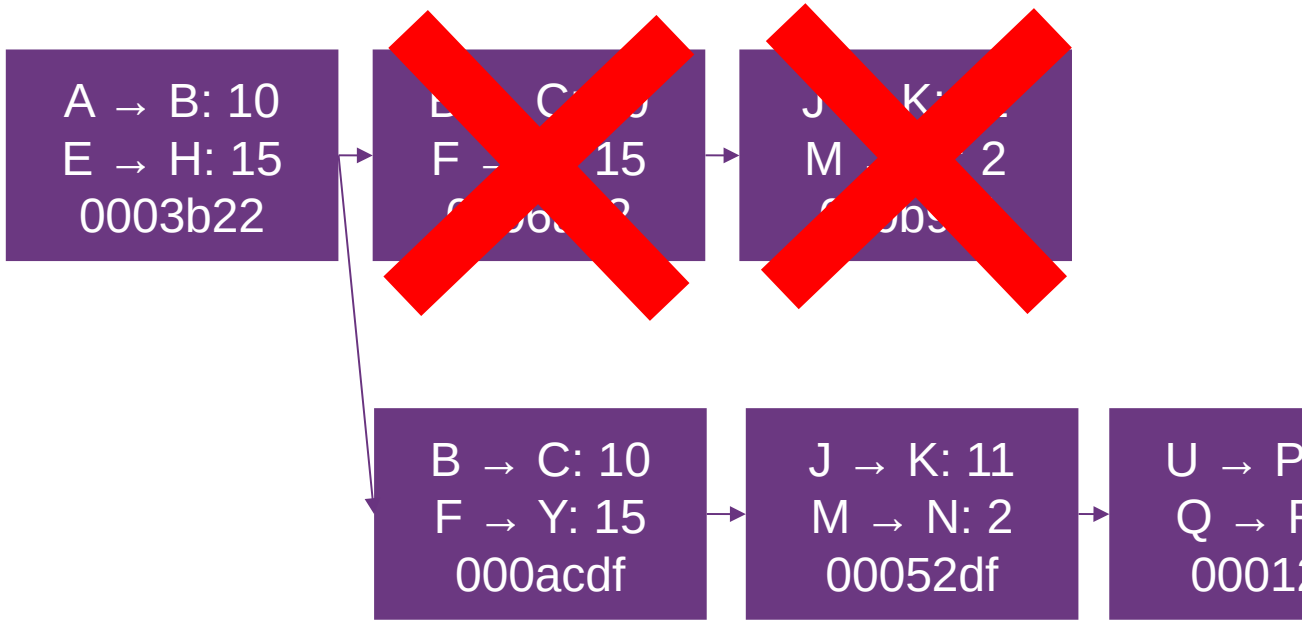
- Building blocks [source]



OST

51% Attack

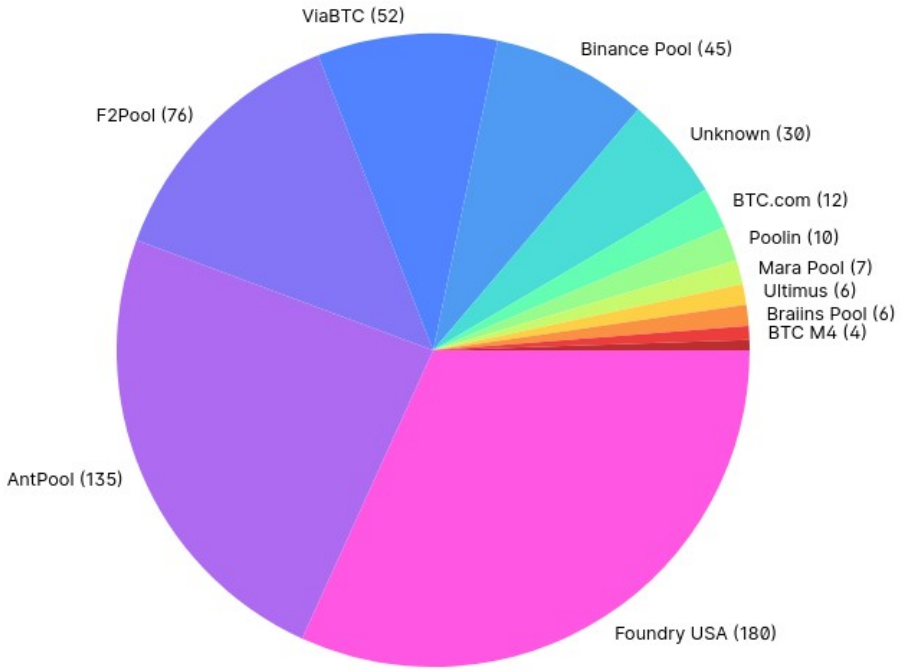
- “If a majority of CPU power is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing chains.”
  - https://bitcoin.org/bitcoin.pdf
- PoW: majority of hashing power, PoS: majority of coins
- How expensive is a 51% attack?
  - Buy an attack?
- Double spend, or rollback 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).”
- 23.04.2020: DeFi Platform Suffers 51% Attack From Its Top Miners — or Does It? [link]
  - “resulted in $6.7 million worth of the USD-pegged stablecoin pUSD”
- 08.11.2020: Grin network hit with 51% attack while GRIN token remains resilient [link]

OST

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 ~ 1900$)
  - 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 ~14s – ~7.7% (“always”, unlike Bitcoin)

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 70m 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

Ethereum protocol upgrades

Protocol layer	Code name	Release date	Block no. or Beacon Chain epoch
Execution[clarification needed]	Frontier	30 July 2015[26][5]	0
Execution	Ice Age	8 September 2015	200,000[citation needed]
Execution	Homestead	15 March 2016	1,150,000
Execution	DAO fork	20 July 2016	1,920,000
Execution	Tangerine Whistle	18 October 2016	2,463,000[citation needed]
Execution	Spurious Dragon	23 November 2016	2,675,000[citation needed]
Execution	Byzantium	16 October 2017	4,370,000
Execution	Constantinople	28 February 2019	7,280,000
Execution	St. Petersburg	28 February 2019	7,280,000
Execution	Istanbul	8 December 2019	9,069,000
Consensus[clarification needed]	Phase 0	1 December 2020	0 (epoch)
Execution	Muir Glacier	2 January 2020	9,200,000
Execution	Berlin	15 April 2021[27]	12,244,000
Execution	London	5 August 2021[28]	12,965,000
Consensus	Altair	27 October 2021	74,240 (epoch)
Execution	Arrow Glacier	8 December 2021	13,773,000
Execution	Gray Glacier	30 June 2022	15,050,000
Consensus	Bellatrix	6 September 2022	144,896 (epoch)
Execution	Paris	15 September 2022	15,537,394[29]
Execution	Shanghai	TBD	TBD
Consensus	Capella[30]	TBD	TBD

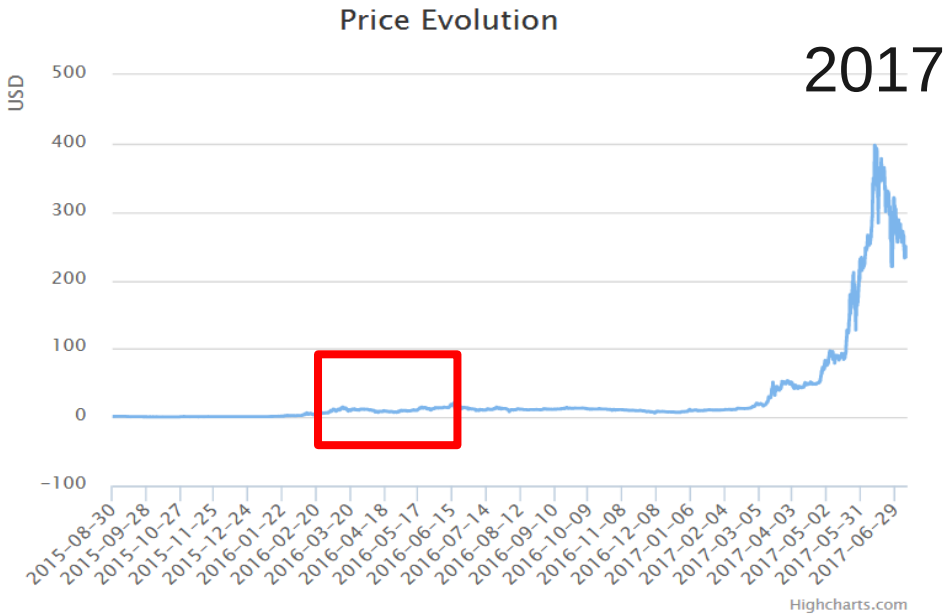
https://en.wikipedia.org/wiki/Ethereum

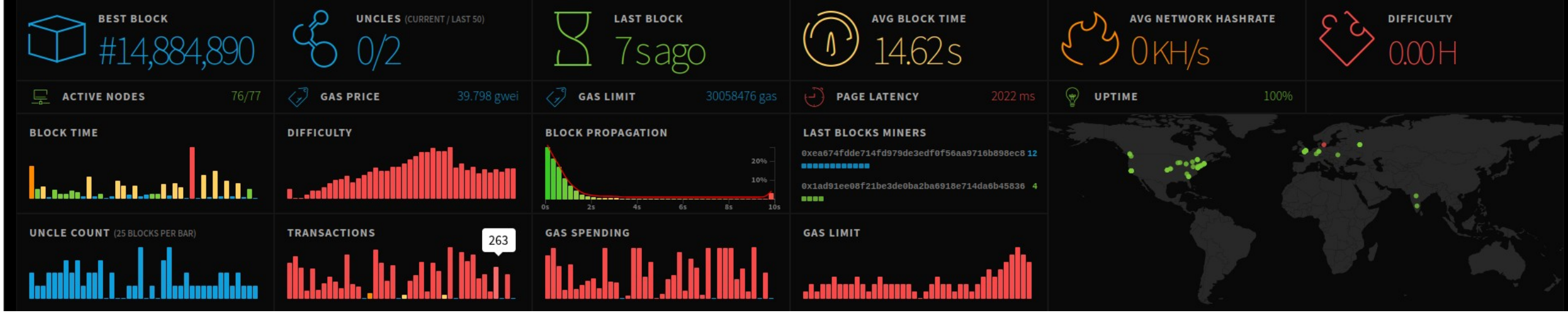
- “Ethereum 2.0” – aka Ethereum
  - Scalability, proof-of-stake, Sharding, ZKP

OST

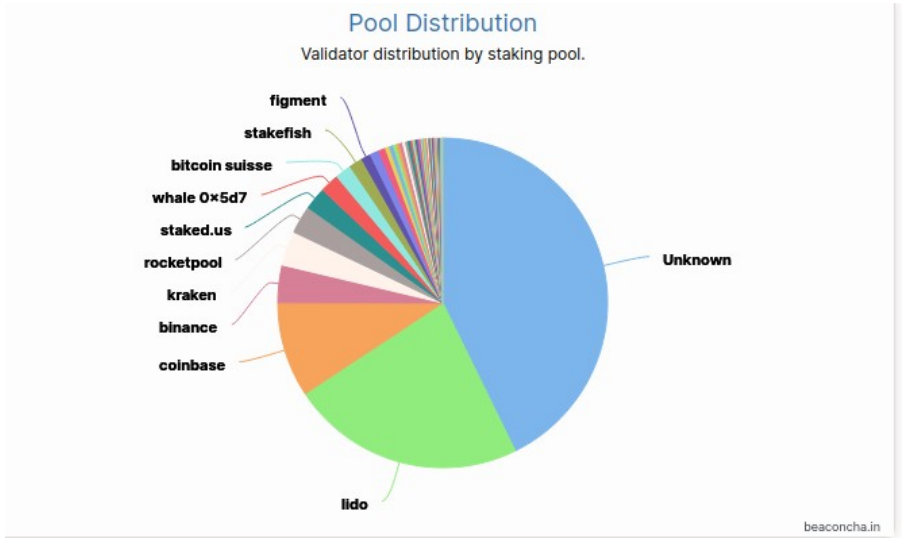
Ethereum Stats

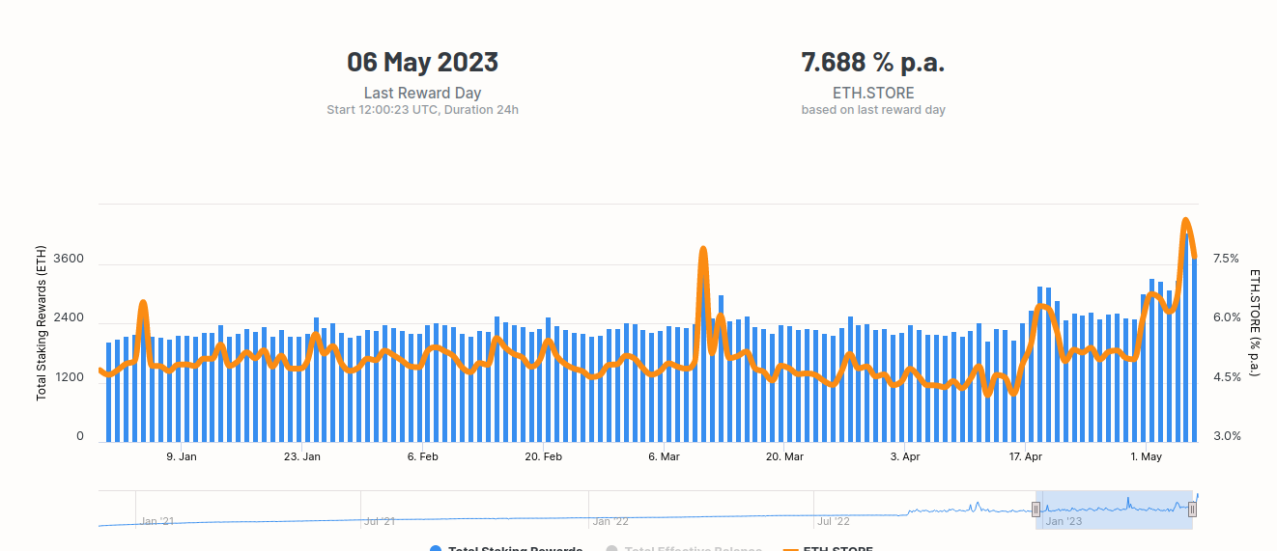
- Basic Stats
  - 2nd in market cap ~ 235b USD
  - Daily transactions (highest ~18.2 TPS, 22.4.2021)
    now ~1150k per day
  - Node count (~10k or 1k nodes?)
  - Blocksize ~125KB
  - Accounts (230mio)





- 115mio ETH supply (stats)
- PoW difficulty, now
  - Mining in pools





https://beaconcha.in/ethstore

OST

Blocktime and Gas

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

- Units:

1 ether =	
1000000000000000000	wei
1000000000000000	Kwei
1000000000000	Mwei
1000000000	Gwei
1000000	szabo
1000	finney
1	ether
0.001	Kether
0.000001	Mether
0.000000001	Gether
0.000000000001	Tether

OST

Blocktime and Gas

- Block time: ~12-13s
  - Ice age
- Smart Contracts are turing complete
  - Every instruction needs to be paid for (example)
- Gas price
  - If you run out of gas, state is reverted, ETH gone

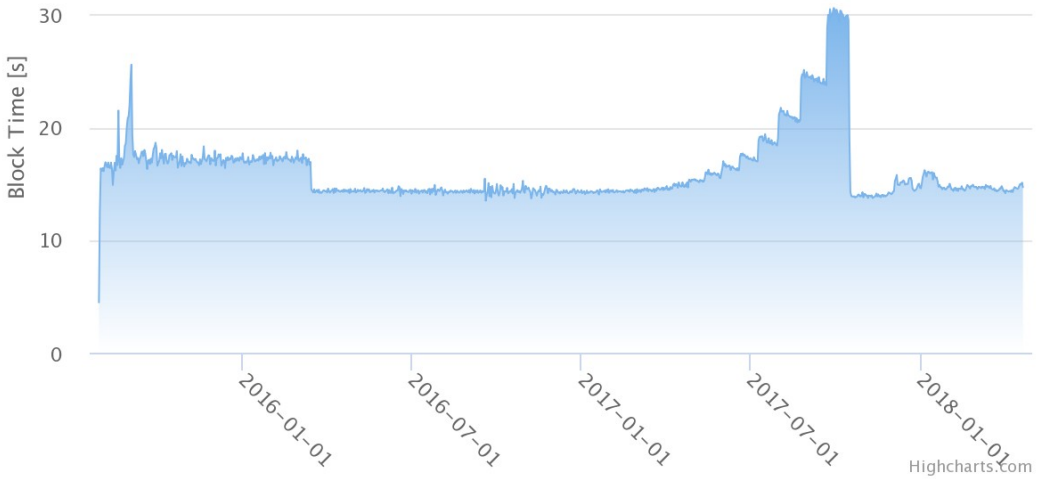
$W_{zero} = \{\text{STOP, RETURN}\}$
$W_{base} = \{\text{ADDRESS, ORIGIN, CALLER, CALLVALUE, CALLDATASIZE, CODESIZE, GASPRICE, COINBASE, TIMESTAMP, NUMBER, DIFFICULTY, GASLIMIT, POP, PC, MSIZE, GAS}\}$
$W_{verylow} = \{\text{ADD, SUB, NOT, LT, GT, SLT, SGT, EQ, ISZERO, AND, OR, XOR, BYTE, CALLDATALOAD,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

source

Appendix G. Fee Schedule

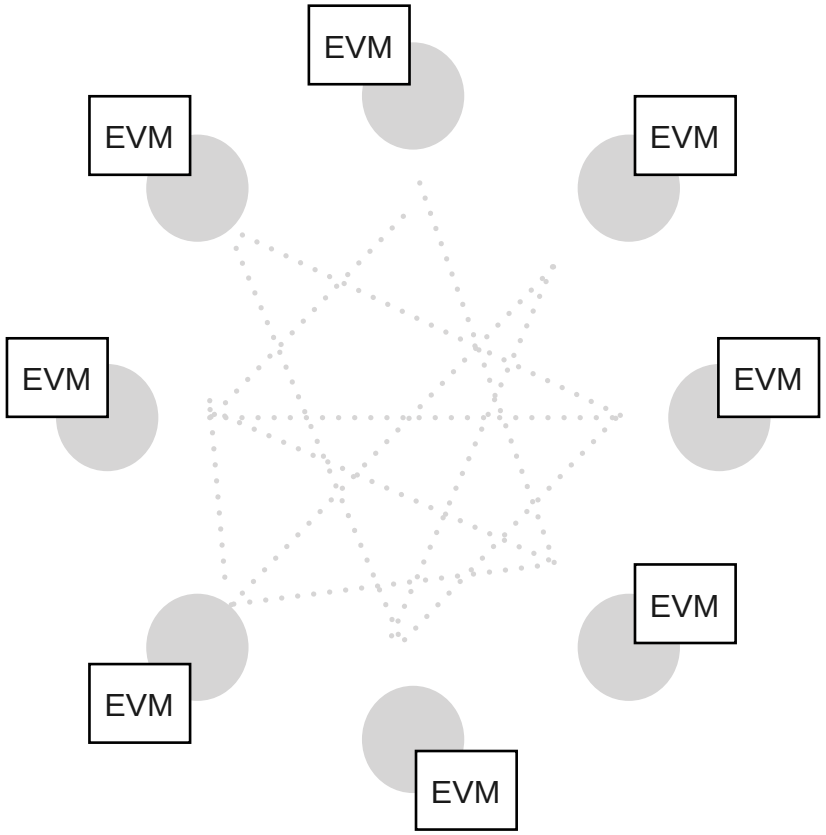
The fee schedule G is a tuple of 31 scalar values corresponding to the relative costs, in gas, of a number of abstract operations that a transaction may effect.

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.



Ethereum smart contract

- In the past, proof of work (PoW)
  - But was difficult with ASIC (memory-hard), starts at 1GB RAM for full node and miner (2GB RAM should be enough)
- 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



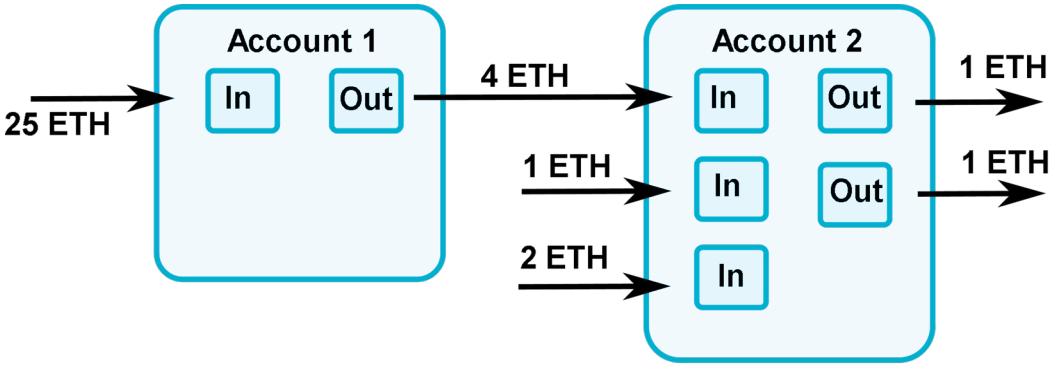
ethereum

OST

Account vs UTXO - Introduction

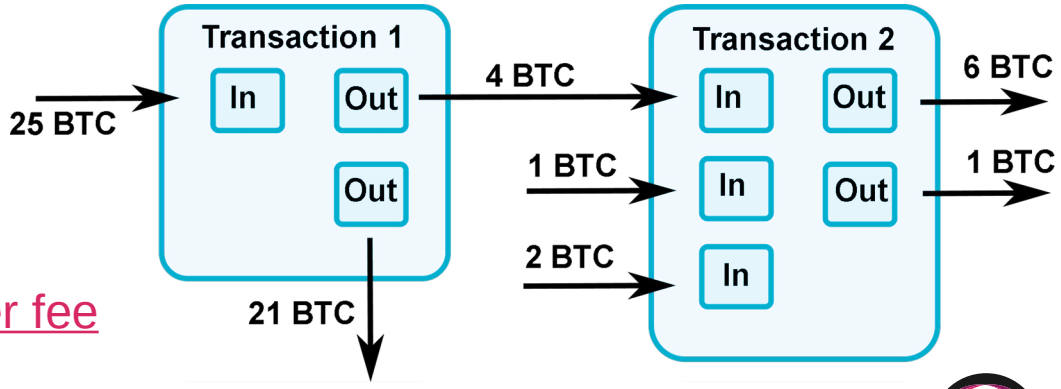
Account-based

- 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

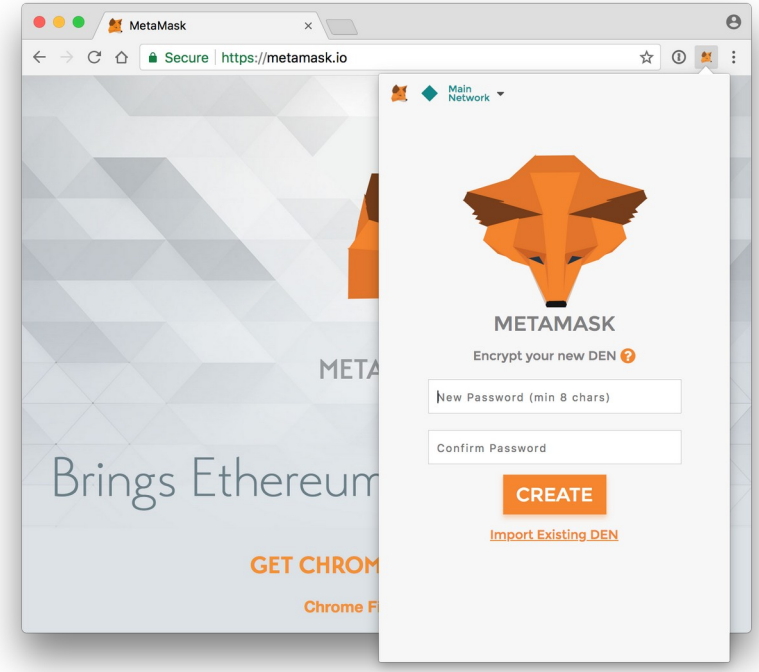
- Every referenced input must be valid and not yet spent
- Total value of the inputs must equal or exceed the total value of the outputs
  - You always spend all outputs
- Transaction must have a signature matching the owner of the input for every input
  - Script determines if input is valid



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
  - Uses infura
- Remix IDE: https://remix.ethereum.org
- Testnet: goerli
  - https://goerli.etherscan.io/ (blockchain explorer)



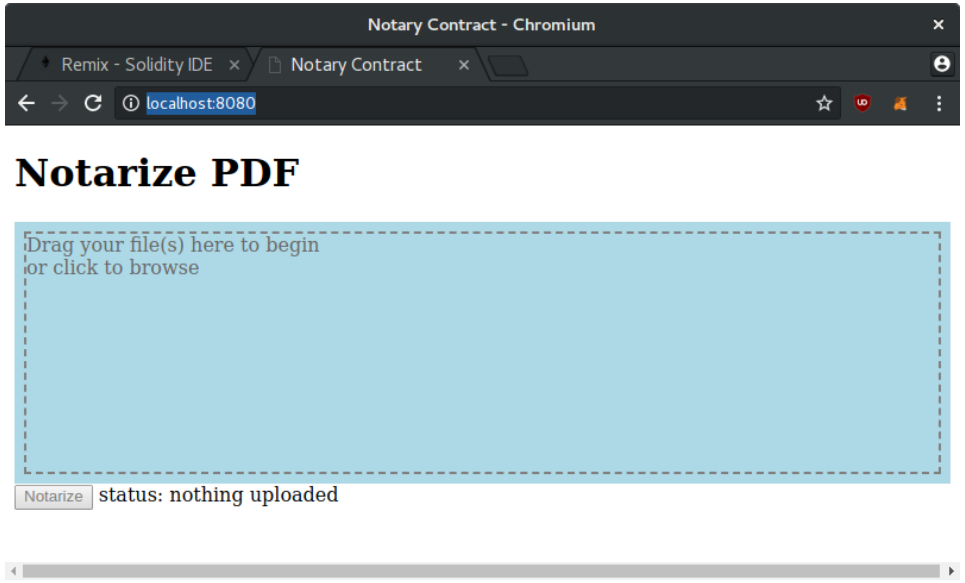

```
INFO [05-08|17:14:43] Commit new mining work                   number=891910 txs=0  uncles=0 elapsed=392.257µs
INFO [05-08|17:15:06] Imported new chain segment               blocks=1 txs=0  mgas=0.000 elapsed=17.225ms  mgasps=0.000   number=891910 hash=812c12…de3c2e
INFO [05-08|17:15:06] Commit new 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://goerli-faucet.pk910.de/)

OST

Example

- Installation
  - npm install
  - ./node_modules/.bin/webpack
  - ./node_modules/.bin/webpack serve
- Open Browser: http://localhost:8080/




```
draft@home: ~/git/VSS-web3js
File  Edit  View  Search  Terminal  Help
draft@home:~/git/VSS-web3js$ ./node_modules/.bin/webpack-dev-server
i ｢wds｣: Project is running at http://localhost:8080/
i ｢wds｣: webpack output is served from /
i ｢wdm｣: Hash: c4c7c0d3279286de6649
Version: webpack 4.7.0
Time: 1139ms
Built at: 2018-05-06 12:57:52
                         Asset       Size  Chunks             Chunk Names
main.c4c7c0d3279286de6649.js    947 KiB    main  [emitted]  main
                  index.html  395 bytes          [emitted]
Entrypoint main = main.c4c7c0d3279286de6649.js
[./node_modules/ansi-html/index.js] 4.16 KiB {main} [built]
[./node_modules/loglevel/lib/loglevel.js] 7.68 KiB {main} [built]
[./node_modules/strip-ansi/index.js] 161 bytes {main} [built]
[./node_modules/url/url.js] 22.8 KiB {main} [built]
[./node_modules/vue/dist/vue.esm.js] 286 KiB {main} [built]
[./node_modules/webpack-dev-server/client/index.js?http://localhost:8080] (webpack)-dev-server/c
lient?http://localhost:8080 7.75 KiB {main} [built]
[./node_modules/webpack-dev-server/client/overlay.js] (webpack)-dev-server/client/overlay.js 3.5
8 KiB {main} [built]
[./node_modules/webpack-dev-server/client/socket.js] (webpack)-dev-server/client/socket.js 1.05
KiB {main} [built]
[./node_modules/webpack/hot sync ^\.\/log$] (webpack)/hot sync nonrecursive ^\.\/log$ 170 bytes
{main} [built]
[./node_modules/webpack/hot/emitter.js] (webpack)/hot/emitter.js 77 bytes {main} [built]
[./node_modules/webpack/hot/log.js] (webpack)/hot/log.js 1010 bytes {main} [optional] [built]
[./src/App.vue] 908 bytes {main} [built]
[./src/App.vue?vue&type=template&id=7ba5bd90] 194 bytes {main} [built]
[0] multi (webpack)-dev-server/client?http://localhost:8080 ./src 40 bytes {main} [built]
[./src/index.js] 129 bytes {main} [built]
    + 63 hidden modules
Child html-webpack-plugin for "index.html":
     1 asset
    Entrypoint undefined = index.html
    [./node_modules/html-webpack-plugin/lib/loader.js!./index.html] 527 bytes {0} [built]
    [./node_modules/lodash/lodash.js] 527 KiB {0} [built]
    [./node_modules/webpack/buildin/global.js] (webpack)/buildin/global.js 489 bytes {0} [built]
    [./node_modules/webpack/buildin/module.js] (webpack)/buildin/module.js 497 bytes {0} [built]
i ｢wdm｣: Compiled successfully.
```


OST