

HS18

DISTRIBUTED SYSTEMS ADVANCED & BLOCKCHAIN

Ethereum Repetition

T. Bocek

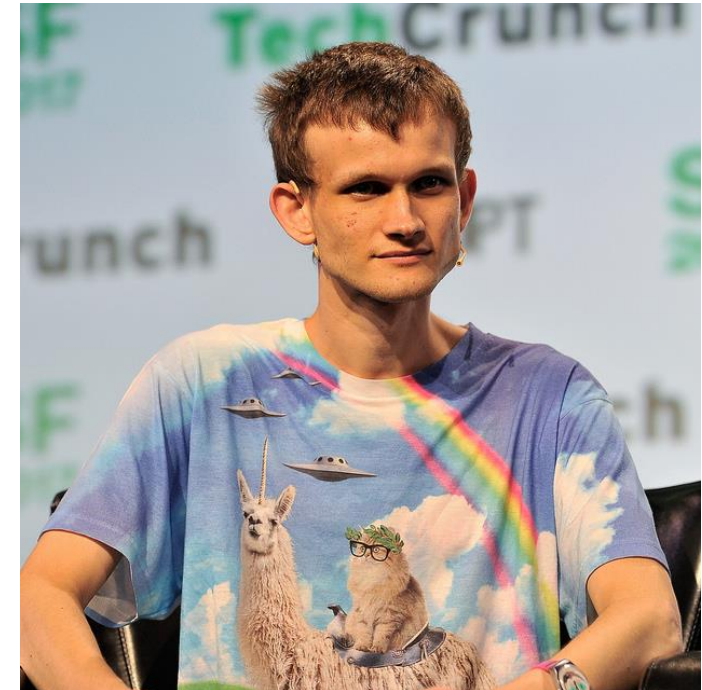
thomas.bocek@hsr.ch

■ “Issues” with Bitcoin

- Slow development, implementing new features difficult
 - [SegWit vs. BTU](#) (segregated witness vs. increasing block size voting)
- Bitcoin Script limited
 - Lightning network

■ Ethereum ([1 ETH ~230\\$](#))

- Generalized blockchain (loops, arithmetics, etc.)
- «Blockchain 2.0» with smart contracts
- [White paper](#) released in December 2013, release July 2015
- Ethereum foundation located in Zug (initiator known) - non-profit foundation
- Mining reward ~ block every ~14s – ~3 (2) ETH



Vitalik Buterin

Ethereum History

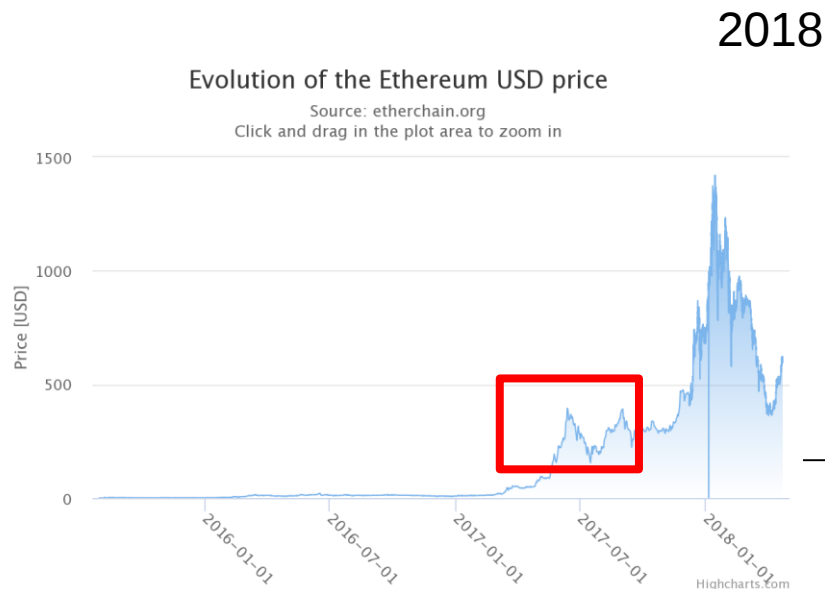
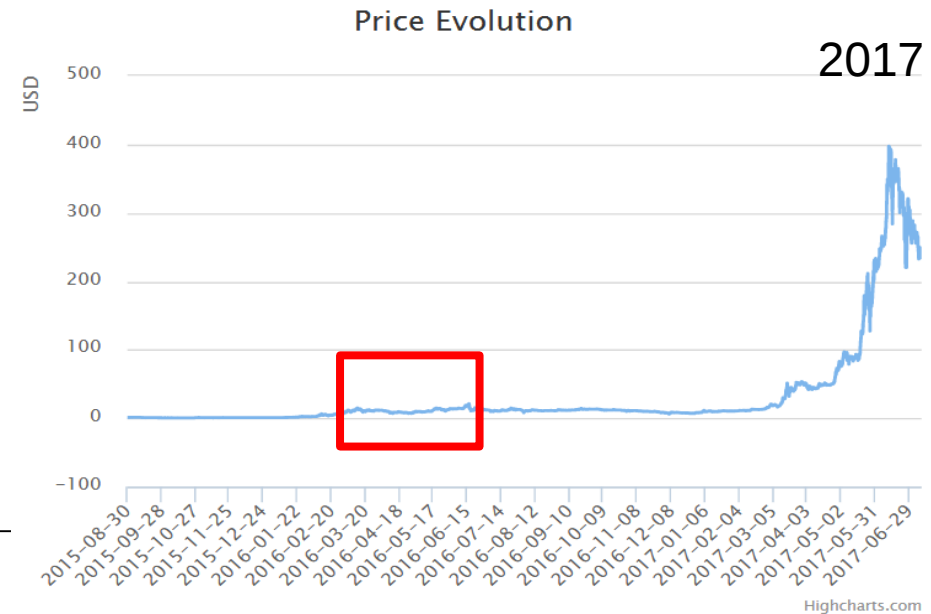
- **Olympic (past) – [released](#) 09.05.2015**
 - Last Ethereum Proof-of-Concept series
 - “Olympic will feature a total prize fund of up to 25,000 ether” (now 15.6m USD)
- **Frontier (past) - released 30.07.2015**
 - Main public network, “Beta”/use at your own risk
- **Homestead (past) - released 03.14.2016**
 - Public network considered “stable”, Integrate critical protocol changes
- **Metropolis ([Byzantium](#), now) - released 16.10.2017**
 - Initial supports for ZKP (private smart contracts), reducing mining reward to 3 ETH
- **Metropolis (Constantinople, future) (Testnet Ropsten, [14.10.2018](#))**
 - Foundations for proof-of-stake, ~~account abstraction~~ (define external accounts with smart contract)
- **Serenity (future)**
 - Scalability, proof-of-stake, Sharding, ZKP

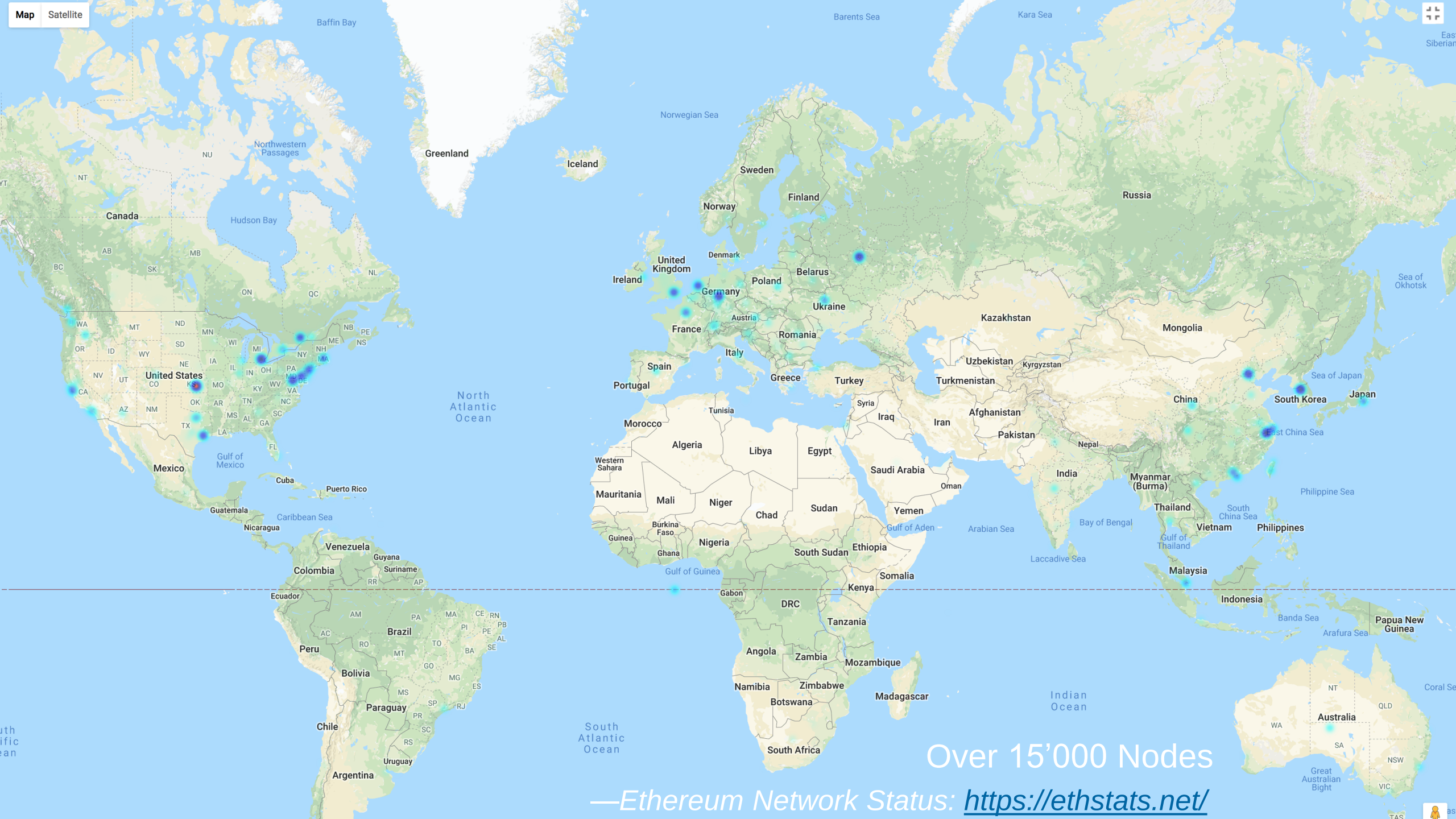


Ethereum Stats

■ Basic Stats

- 2nd (again) in [market cap](#) ~ 23b USD
- Transactions (highest ~15 TPS)
[470'000 per day](#)
- [Blocksize](#) ~25KB
- [Accounts](#) (46mio)

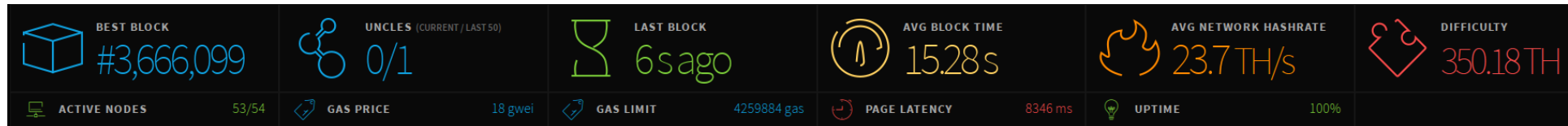




Over 15'000 Nodes

—Ethereum Network Status: <https://ethstats.net/>

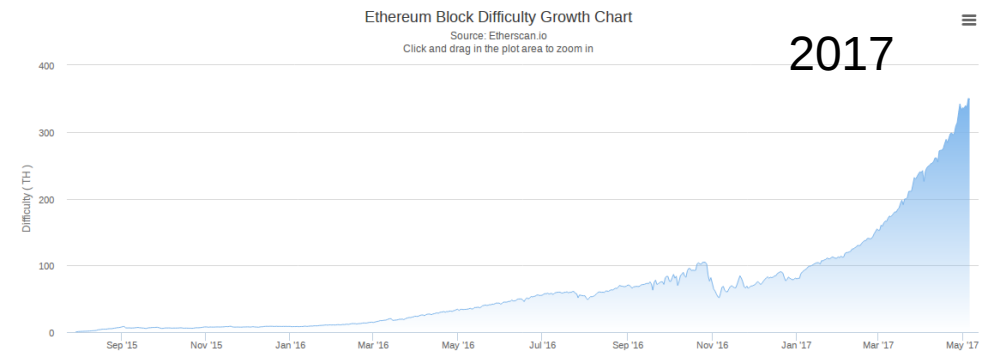
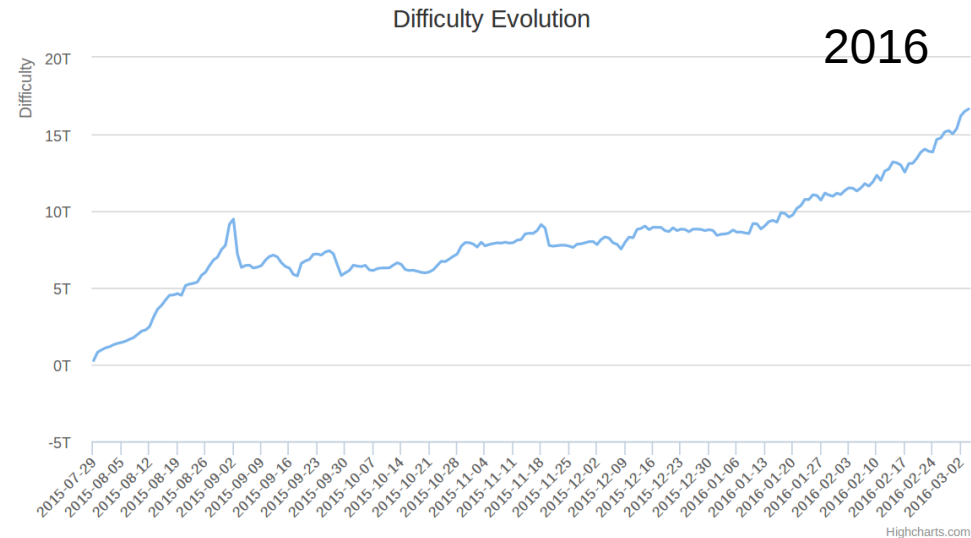
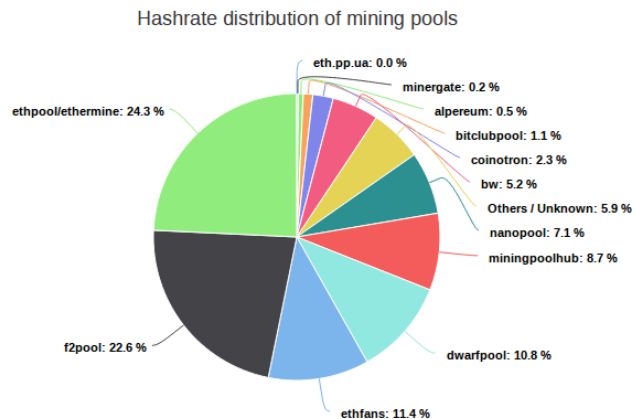
Ethereum Stats



■ 102mio ETH supply ([stats](#))

■ Increasing difficulty

- [Mining in pools](#)
- «ethpool» ~25%



Download: [CSV Data](#) (attribution required)

Blocktime and Gas

■ Block time: ~14-15s

■ Ice age

■ Contracts are turing complete

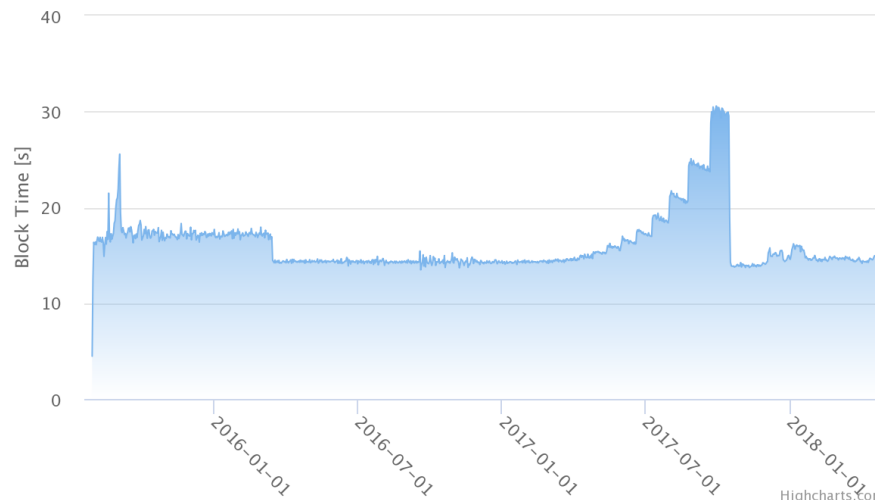
■ Every instruction needs to be paid for ([example](#))

■ Gas Price / Gas Limit by TX

■ If you run out of gas, state is reverted, ETH gone

Average block time of the Ethereum Network

Source: etherchain.org
Click and drag in the plot area to zoom in



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_{clear}	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.
$G_{codeposit}$	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 $\lceil \log_{256}(\text{exponent}) \rceil$ for the EXP operation.
G_{memory}	3	Paid for every additional word when expanding memory.
$G_{xcreate}$	32000	Paid by all contract-creating transactions after the Homestead transition.
$G_{xdatazero}$	4	Paid for every zero byte of data or code for a transaction.
$G_{xdatanonzero}$	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.

$W_{zero} = \{\text{STOP, RETURN}\}$

$W_{base} = \{\text{ADDRESS, ORIGIN, CALLER, CALLVALUE, CALLDATASIZE, CODESIZE, GASPRICE, COINBASE, TIMESTAMP, NUMBER, DIFFICULTY, GASLIMIT, POP, PC, MSIZE, GAS}\}$

$W_{verylow} = \{\text{ADD, SUB, NOT, LT, GT, SLT, SGT, EQ, ISZERO, AND, OR, XOR, BYTE, CALLDATALOAD, MLOAD, MSTORE, MSTORE8, PUSH*, DUP*, SWAP*}\}$

$W_{low} = \{\text{MUL, DIV, SDIV, MOD, SMOD, SIGNEXTEND}\}$

$W_{mid} = \{\text{ADDMOD, MULMOD, JUMP}\}$

$W_{high} = \{\text{JUMPI}\}$

$W_{extcode} = \{\text{EXTCODESIZE}\}$

Gas: Ethereum's Fuel

- Price that is paid for running a transaction or a contract
 - Should match the HW resources
- Similar to the use of Kilowatts (kW) for measuring electricity in your house
- Current Price: <https://ethgasstation.info>
Current Gas Price (02.10.18): 8.6 Gwei
- Every instruction needs to be paid for in advance
- If you run out of gas, state is reverted, ETH gone



- Computation 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
- For now, [proof of work](#) (PoW)
 - But difficult with ASIC (memory-hard), starts at 1GB RAM for full node and miner ([2GB RAM should be enough](#))

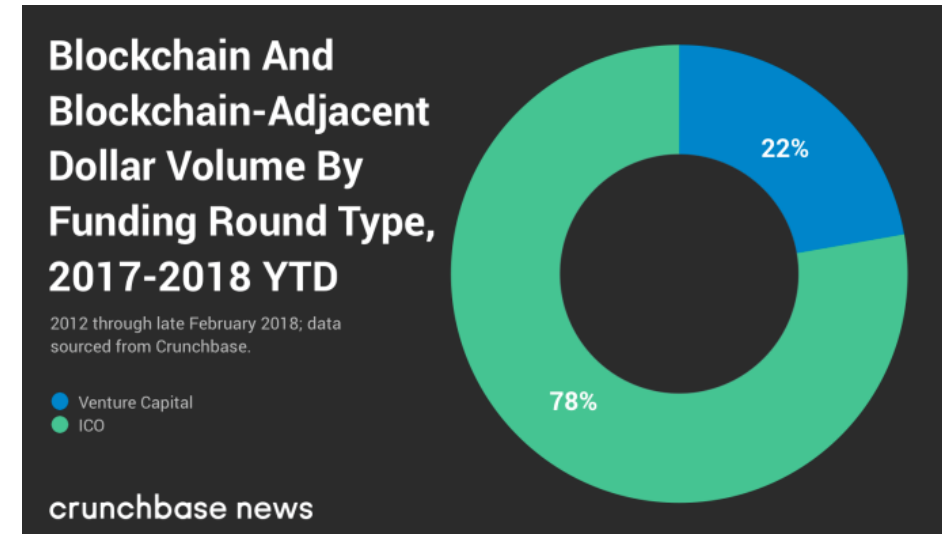
URL: b.socrative.com/student/

Room: HSR

What is an ICO

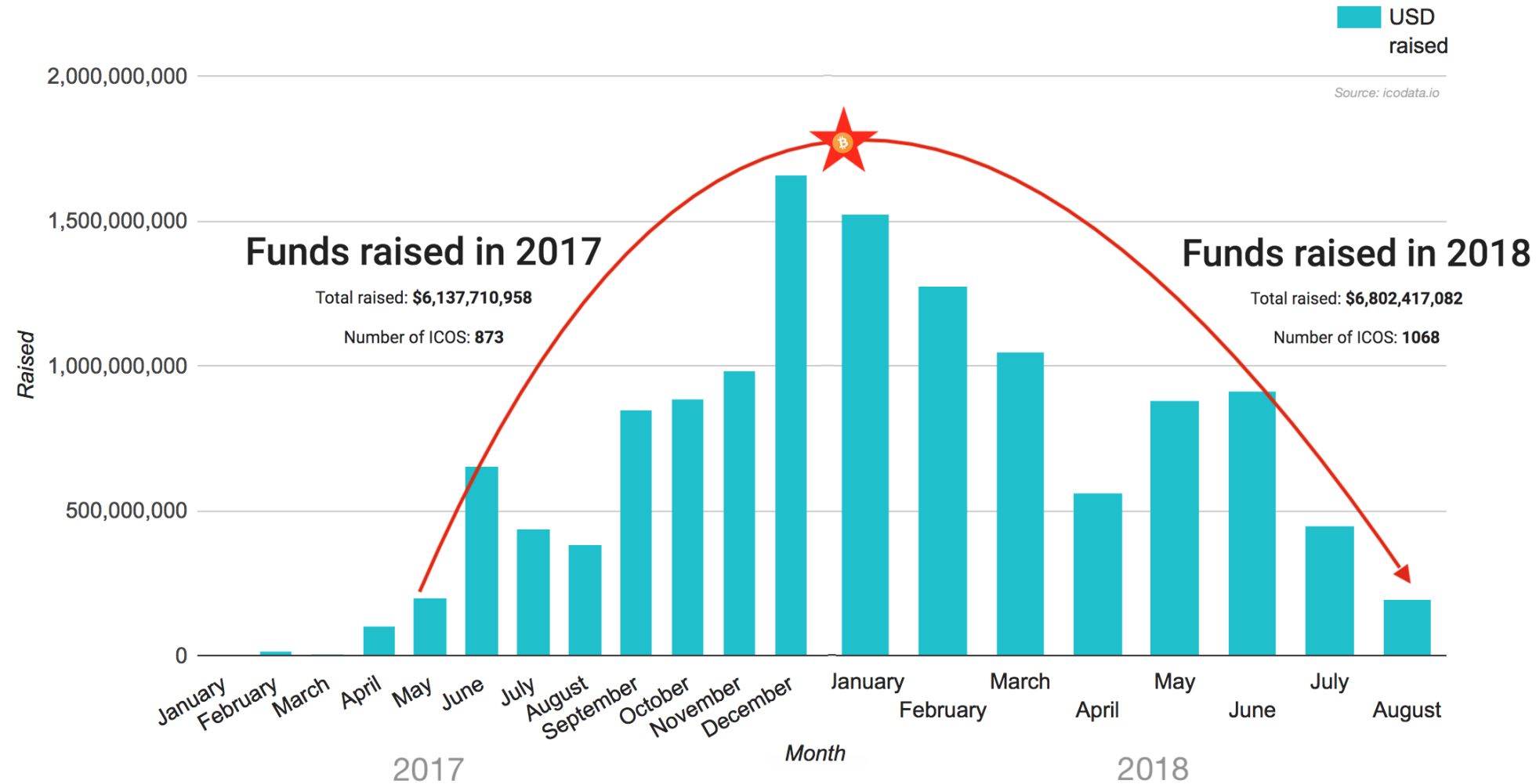
- An initial coin offering (ICO) is a means of crowdfunding
 - Tokensale - release of a new cryptocurrency
 - 1490 listed cryptocurrencies with a [marketcap](#), 4942 with [coinlib.io](#)
- ICOs vs IPOs
 - ICO little regulation, IPO are heavily regulated
 - ICO short in duration, IPO much longer
 - IPO are exclusive, ICO are open to anyone
- TechCrunch: Over 1000 Crypto Projects Are Considered 'Dead' Now

- ICOs delivered at least 3.5x more capital to blockchain startups than VC since 2017



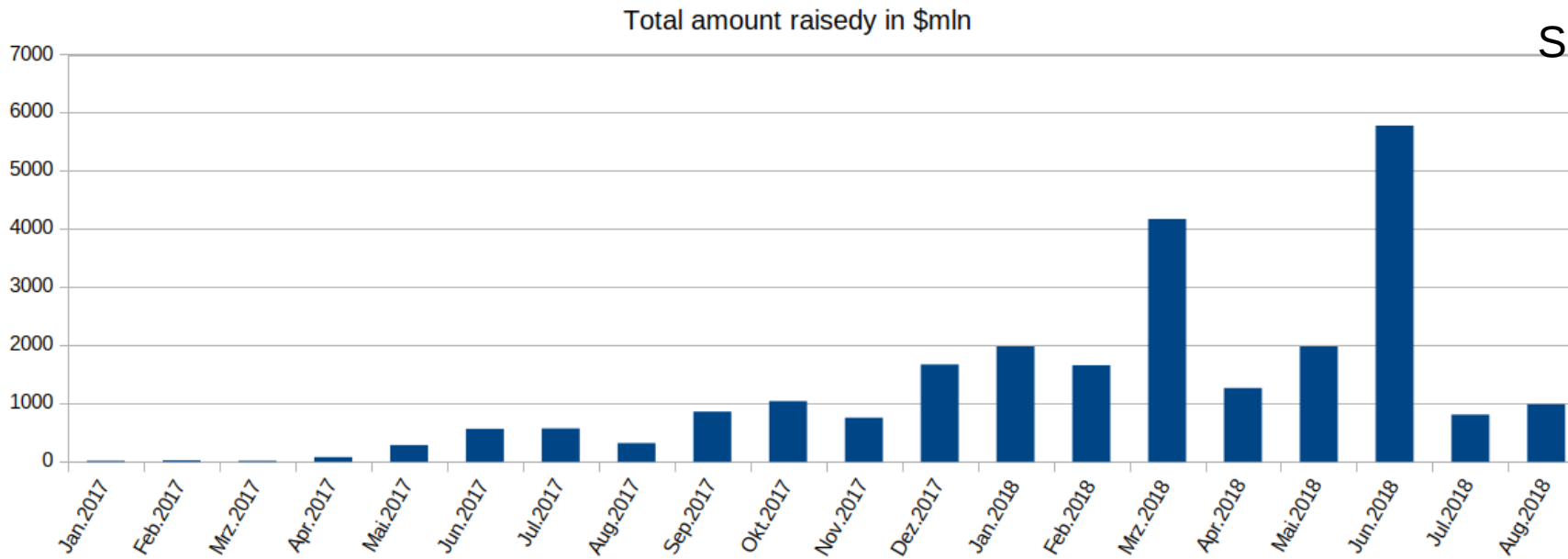
- Wall Street Journal: 20 percent of all ICOs are fraudulent
- SATIS Group Report: '78% of ICOs are Scams'

Total amount raised by all ICOs in total (\$)

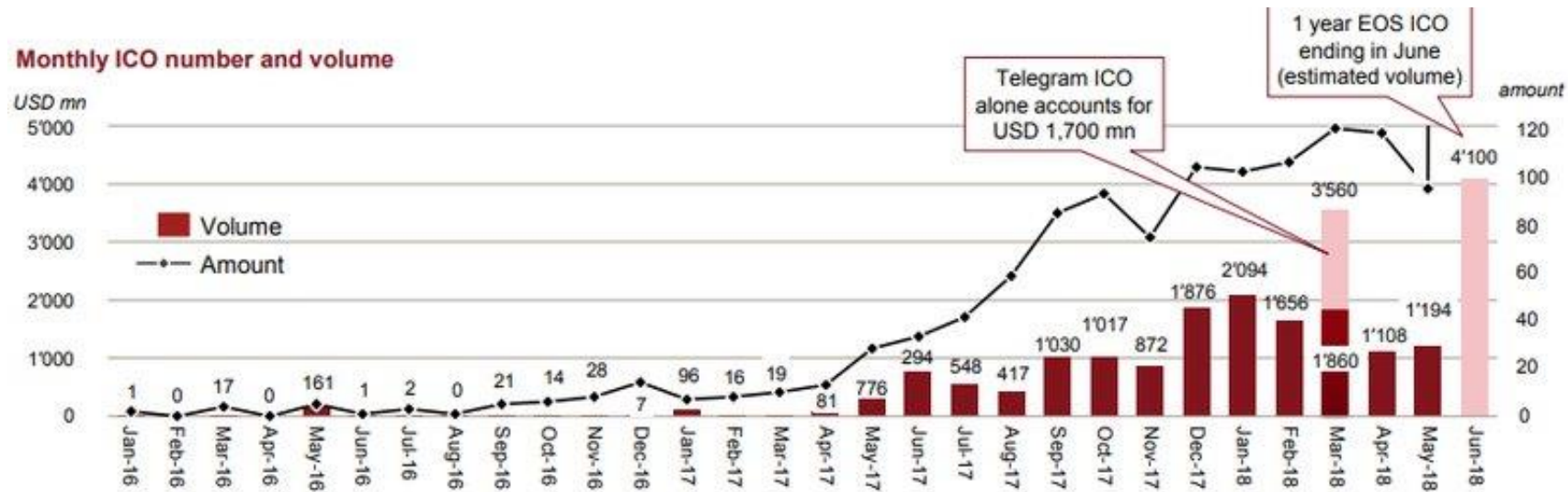


Source: icodata.io

Total amount raised by all ICOs in total (\$mIn)



Source: [Coinschedule](https://coinschedule.com/)



Source: PwC Report

ICO countries and categories

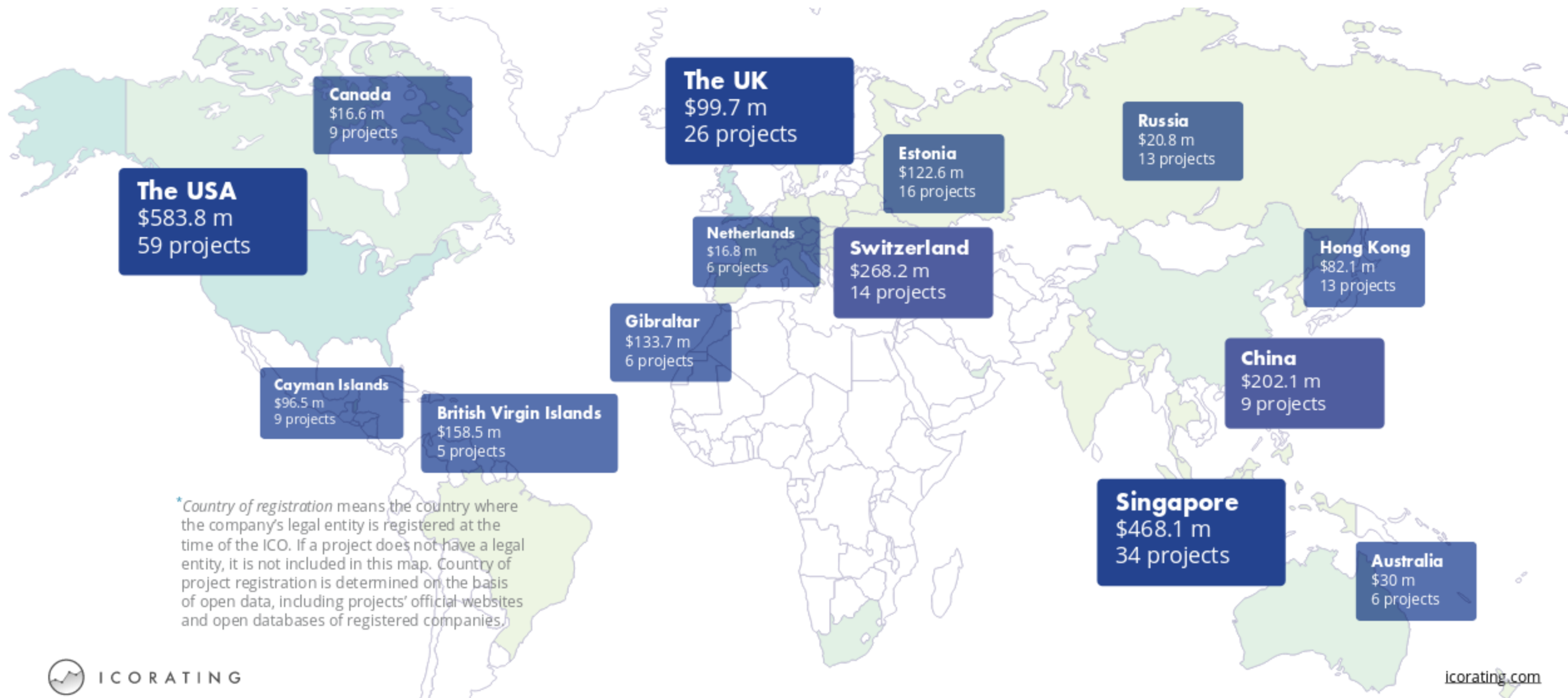
Number of projects

	Country	% of Projects	Total Raised
1	USA	16.3%	875m \$
2	UK	9.6%	173m \$
3	Singapore	7.5%	316m \$
4	Russia	7.2%	1003m \$
5	Switzerland	6.8%	540m \$
6	Estonia	4.1%	35m \$
7	Australia	3.2%	31m \$

Total Raised

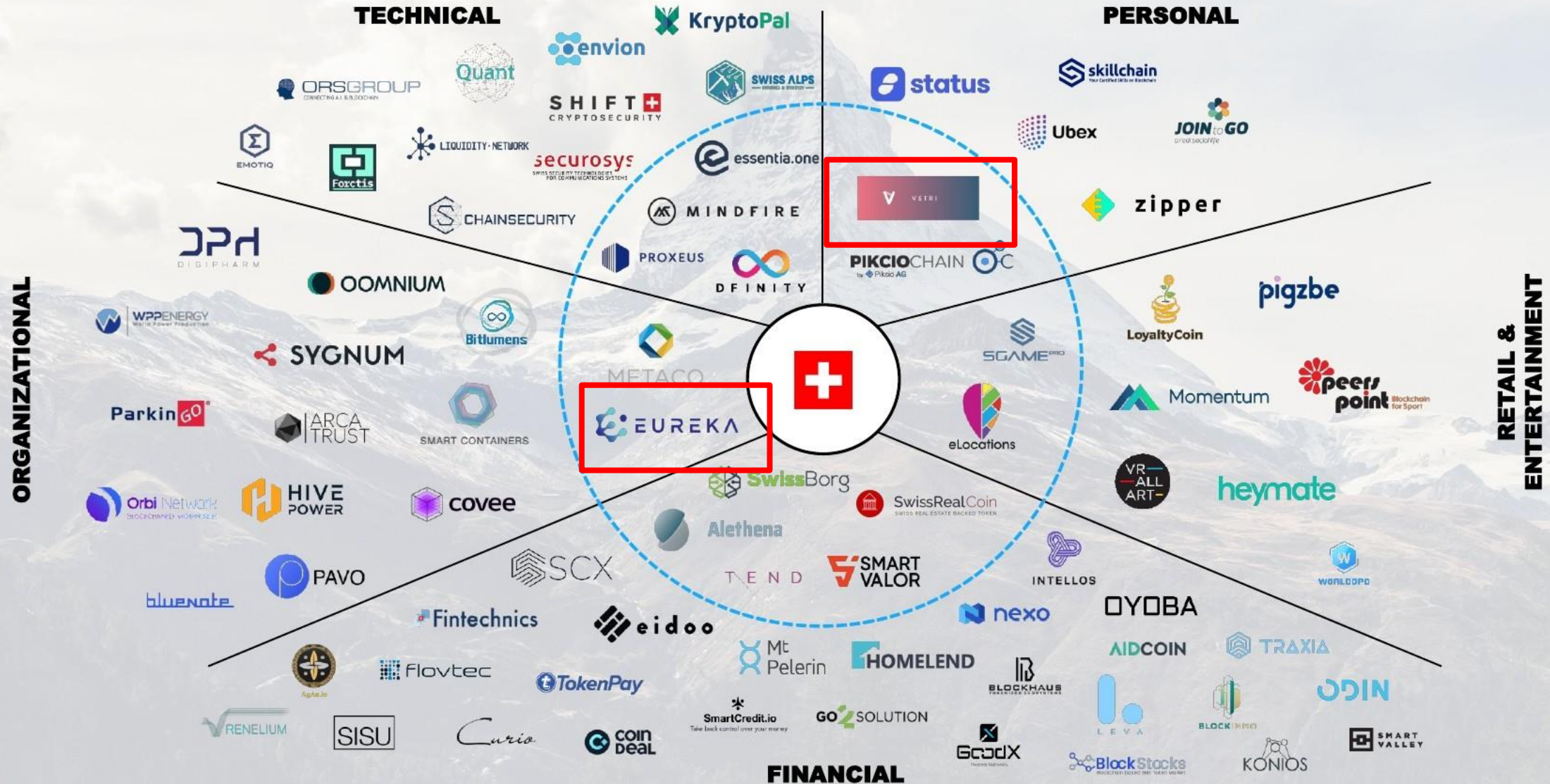
	Country	% of Projects	Total Raised
1	Russia	7.2%	1003m \$
2	USA	16.3%	875m \$
3	Switzerland	6.8%	540m \$
4	Singapore	7.5%	316m \$
5	UK	9.6%	173m \$
6	Estonia	4.1%	35m \$
7	Australia	3.2%	31m \$

ICO countries and categories



SWISS BLOCKCHAIN STARTUPS – NEWCOMERS 2018¹⁾

MARKET SCREENING OF 78 PROJECTS & SELECTION OF TOP 15 STARTUPS



URL: b.socrative.com/student/

Room: HSR

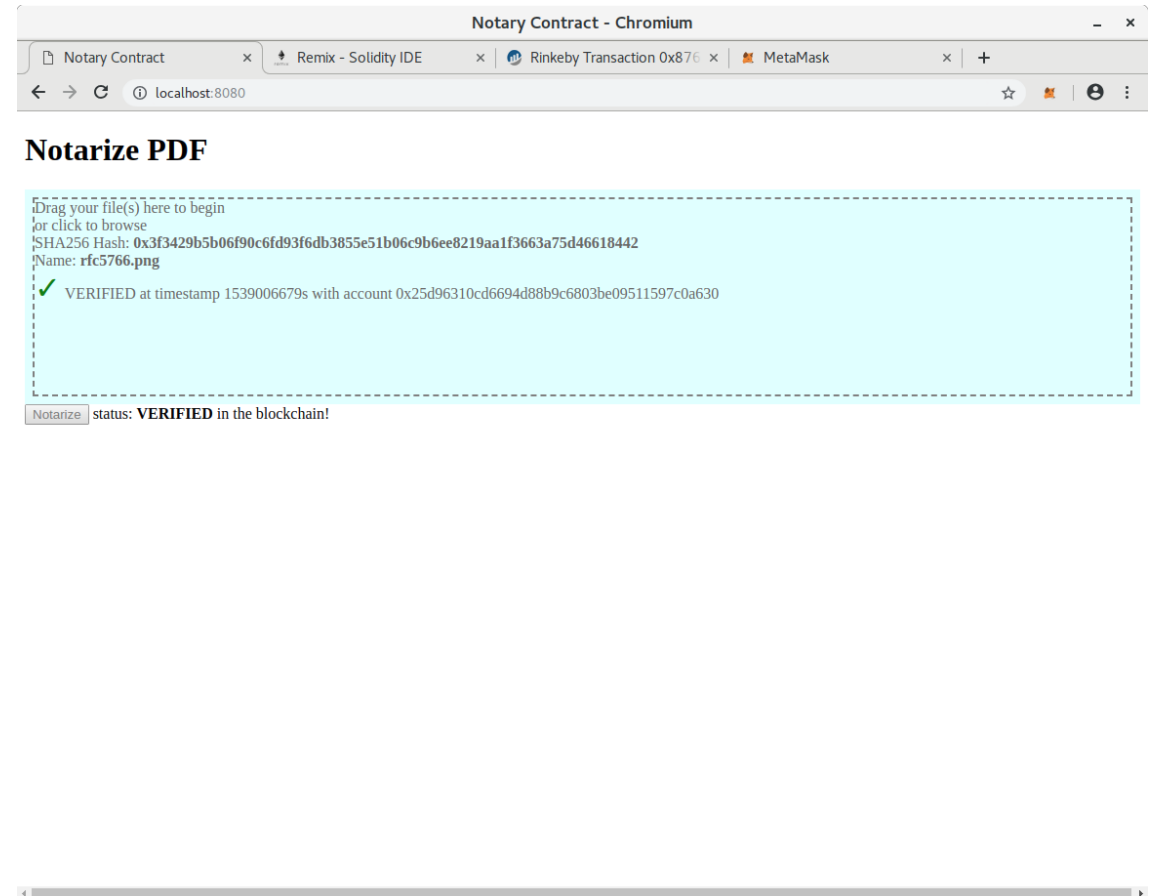
Java & JavaScript web3 examples

■ VSS recap

- Examples <https://github.com/tbocek/DSA-web3>
- Install MetaMask or your own client
- Run server locally
- Notarize

■ Testonator

- Truffle/Ganache, but with JUnit
 - Runs with latest Solidity
 - Web3 – generate wrapper for SC
 - Testonator – use SC directly
-
- Run web3 with rinkeby



Questions?

Prof. Dr. Thomas Bocek thomas.bocek@hsr.ch
Roman Blum roman.blum@hsr.ch