Ethereum as IoT opportunity

Blockchain 360; Boston, MA; 2016-10-17

20 billion

By 2020

uniquely identifiable and addressable objects connected to the Internet

often embedded with transducers (sensors, actuators, controllers)

Problem statements

- infeasible for billions of devices to be controlled by a single organization
- bandwidth costs alone would be astronomical, so must seek how to remove intermediate communication steps
- already lots of embedded devices have unpatched security concerns
- need to figure out a way to manage devices when growth is exponentially increasing

Goals

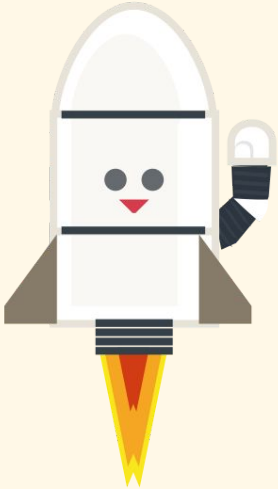
```
> unified data platform

> high interoperability

> low maintenance
```

Aren’t blockchains too slow for billions of devices?

Challenges

Ongoing research

- State-channels
  - Off-chain negotiation with on-chain settlement (reduce chattiness)
  - Direct peer communication → only publicize settlement info
- Proof-of-Stake
  - More efficient than Proof-of-Work
  - Decrease time between blocks (ideally under 3 seconds)
- Sharding
  - Increase transactions/second
  - Removes requirement “all nodes store all data”



How about privacy?

Blockchains are fully public

Privacy concerns

- hybrid approach might include storing an identifier in the blockchain, but keeping the actual data in encrypted format in another place (i.e. IPFS)
- secure multiparty computation and zero-knowledge proofs are some initial ways to deal with obscuring bits of information without moving data off-chain
- homomorphic encryption may become expansive & efficient enough to one day use

Impractical

For a large entities to maintain control over all devices

```
> Decentralization.value()

Resiliency
```

What about collecting and analyzing all that data?

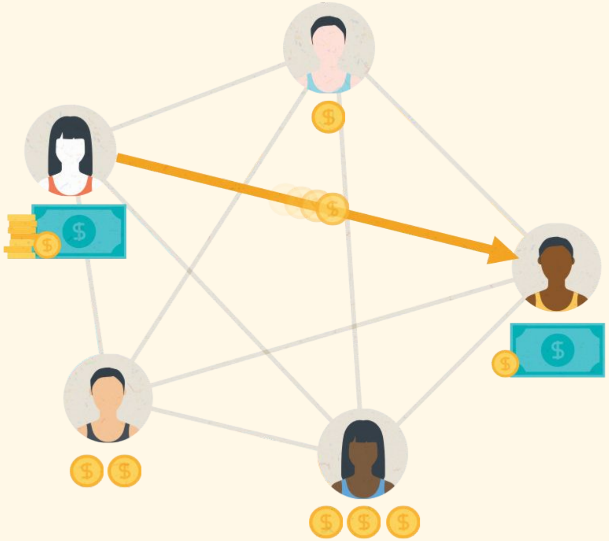
Smart homes & cities

- blockchains as a distributed ledger is trust-free, tamper-resistant, auditable system of operation
- confidence that data has not been altered in unexpected ways (assumes sensor is accurate)
- enables new possibilities, such as leasing of data
- agreements may require dual legal approach whereby self-executing smart contracts references standard legal documents and vice versa

IoT will birth M2M

M2M economy

- enabled by existence of cryptocurrencies, which are well-suited for micropayments
- devices can charge and pay for services
- extension of sharing economy: instead of renting a bedroom, the device can rent its extra capacity
- bootstrap into the network by sharing idle bandwidth & storage



Smart contracts

- self-enforcing digital contracts well-suited for semi-autonomous devices
- automated exchange of not only data, but also value will be a boon to the types of activity
- when achieved using a single interoperability standard, we gain the most benefit
- impossible to dictate the exact software to be installed on all these devices, but using a thin cloud substrate like EVM gives flexibility in implementation

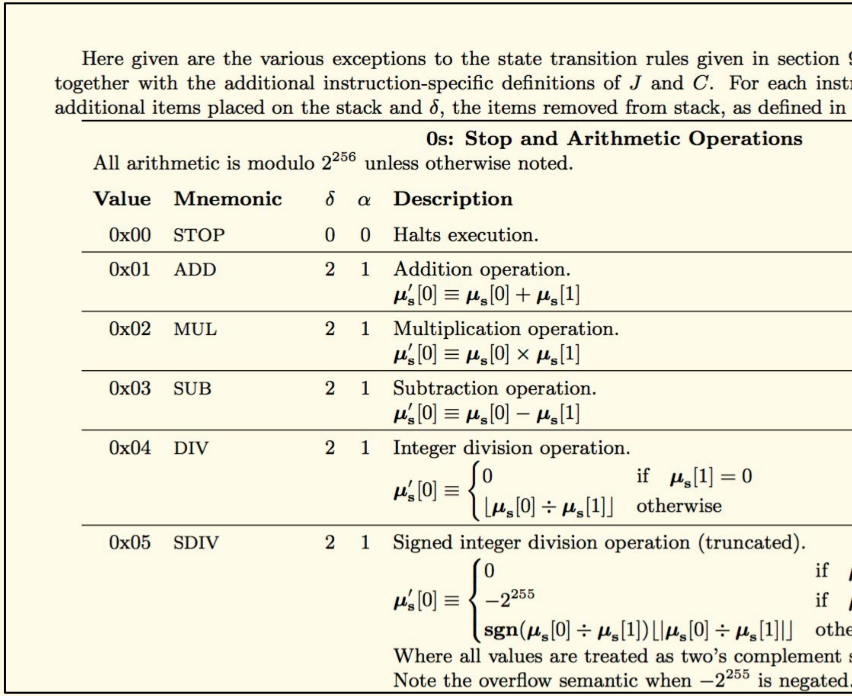
EVM

Stack-based virtual machine

Sandboxed accounts can store code, data, and value

Well-defined set of operations in "Yellow Paper"

Implemented in Python, CPP, Go, Java, JavaScript, Rust, Ruby, Haskell



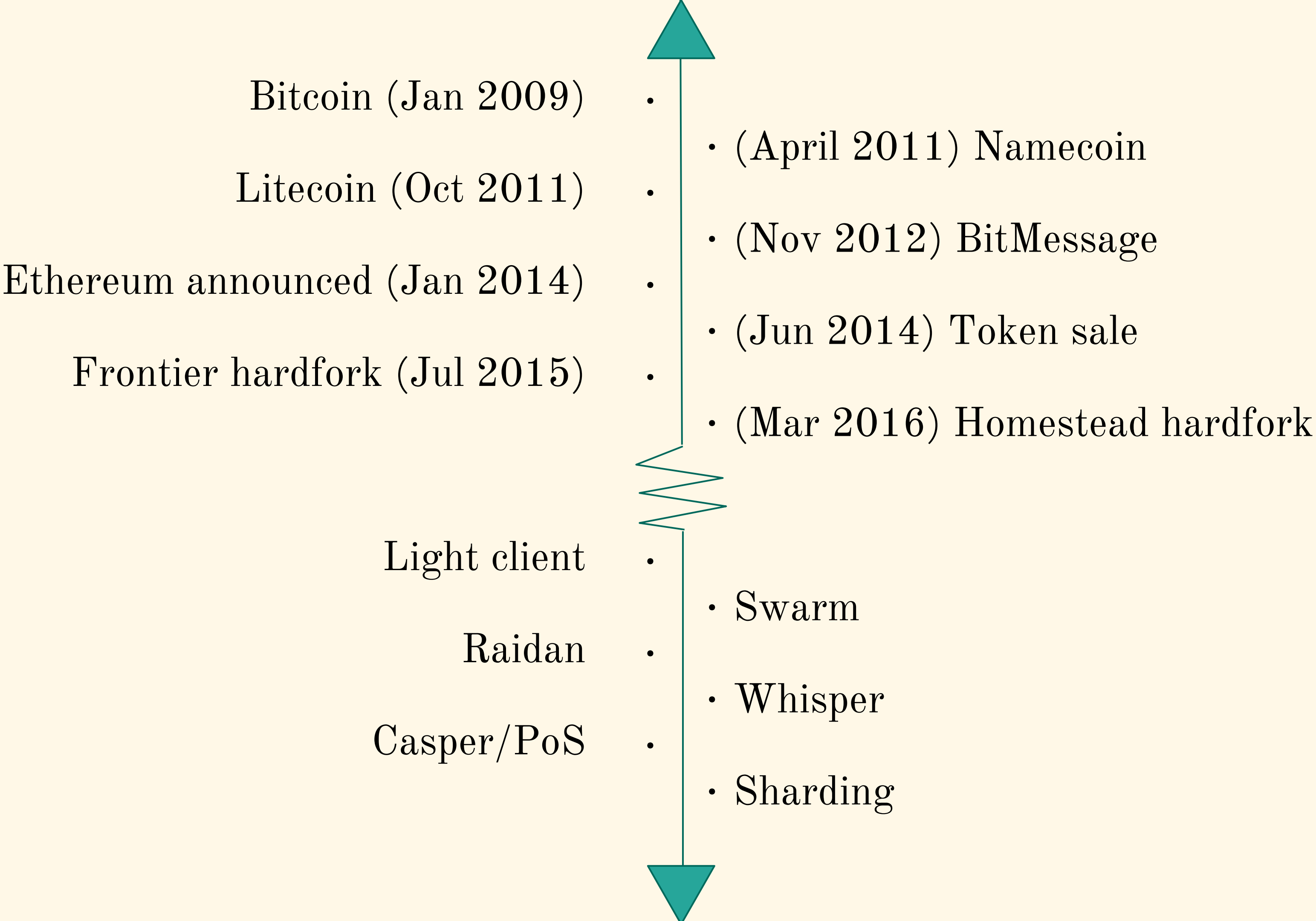
Here given are the various exceptions to the state transition rules given in section together with the additional instruction-specific definitions of J and C. For each instr additional items placed on the stack and δ, the items removed from stack, as defined in

0s: Stop and Arithmetic Operations

All arithmetic is modulo 2^{256} unless otherwise noted.

Value	**Mnemonic**	δ	α	**Description**
0x00	STOP	0	0	Halts execution.
0x01	ADD	2	1	Addition operation. $\boldsymbol{\mu}'_{\mathrm{s}}[0] \equiv \boldsymbol{\mu}_{\mathrm{s}}[0] + \boldsymbol{\mu}_{\mathrm{s}}[1]$
0x02	MUL	2	1	Multiplication operation. $\boldsymbol{\mu}'_{\mathrm{s}}[0] \equiv \boldsymbol{\mu}_{\mathrm{s}}[0] \times \boldsymbol{\mu}_{\mathrm{s}}[1]$
0x03	SUB	2	1	Subtraction operation. $\boldsymbol{\mu}'_{\mathrm{s}}[0] \equiv \boldsymbol{\mu}_{\mathrm{s}}[0] - \boldsymbol{\mu}_{\mathrm{s}}[1]$
0x04	DIV	2	1	Integer division operation. $\boldsymbol{\mu}'_{\mathrm{s}}[0] \equiv \begin{cases} 0 & \text{if} \quad \boldsymbol{\mu}_{\mathrm{s}}[1] = 0 \\ \lfloor \boldsymbol{\mu}_{\mathrm{s}}[0] \div \boldsymbol{\mu}_{\mathrm{s}}[1] \rfloor & \text{otherwise} \end{cases}$
0x05	SDIV	2	1	Signed integer division operation (truncated). $\boldsymbol{\mu}'_{\mathrm{s}}[0] \equiv \begin{cases} 0 & \text{if} \\ -2^{255} & \text{if} \\ \mathbf{sgn}(\boldsymbol{\mu}_{\mathrm{s}}[0] \div \boldsymbol{\mu}_{\mathrm{s}}[1]) \lfloor \lvert \boldsymbol{\mu}_{\mathrm{s}}[0] \div \boldsymbol{\mu}_{\mathrm{s}}[1] \rvert \rfloor & \text{othe} \end{cases}$ Where all values are treated as two's complement Note the overflow semantic when -2^{255} is negated.

Future plans



Bitcoin (Jan 2009)

(April 2011) Namecoin

Litecoin (Oct 2011)

(Nov 2012) BitMessage

Ethereum announced (Jan 2014)

(Jun 2014) Token sale

Frontier hardfork (Jul 2015)

(Mar 2016) Homestead hardfork

Light client

Swarm

Raidan

Whisper

Casper/PoS

Sharding

Philosophy

Philosophical concerns

- should look at IoT devices as extension of human capture-time, but not allow it to rule our needs
- could result in unpredictable, dystopian results
- must be cautious for hyper tokenization leading to digital feudalism
- future would look like a society whose actions are heavily incentivised by corporations against the desire & will of the individual humans

Taylor Gerring

Ethereum Foundation

taylor@ethereum.org
@TaylorGerring