Blockchains and IoT: a reality check

Pekka Nikander, Aalto University

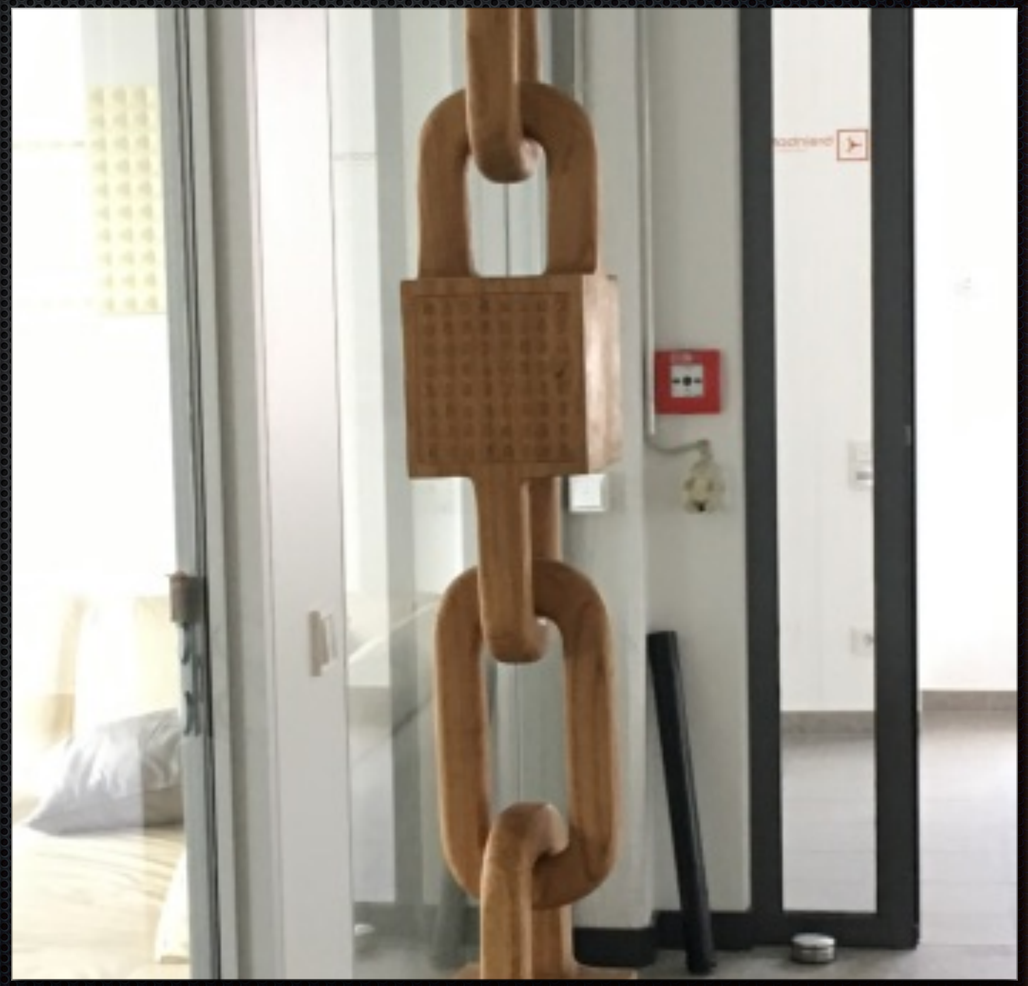
IoT Week 2018, Bilbao

Outline

- Introduction
- Constraint device characteristics
- Distributed Ledgers reality
- Toughest stuff in practice
- Conclusions

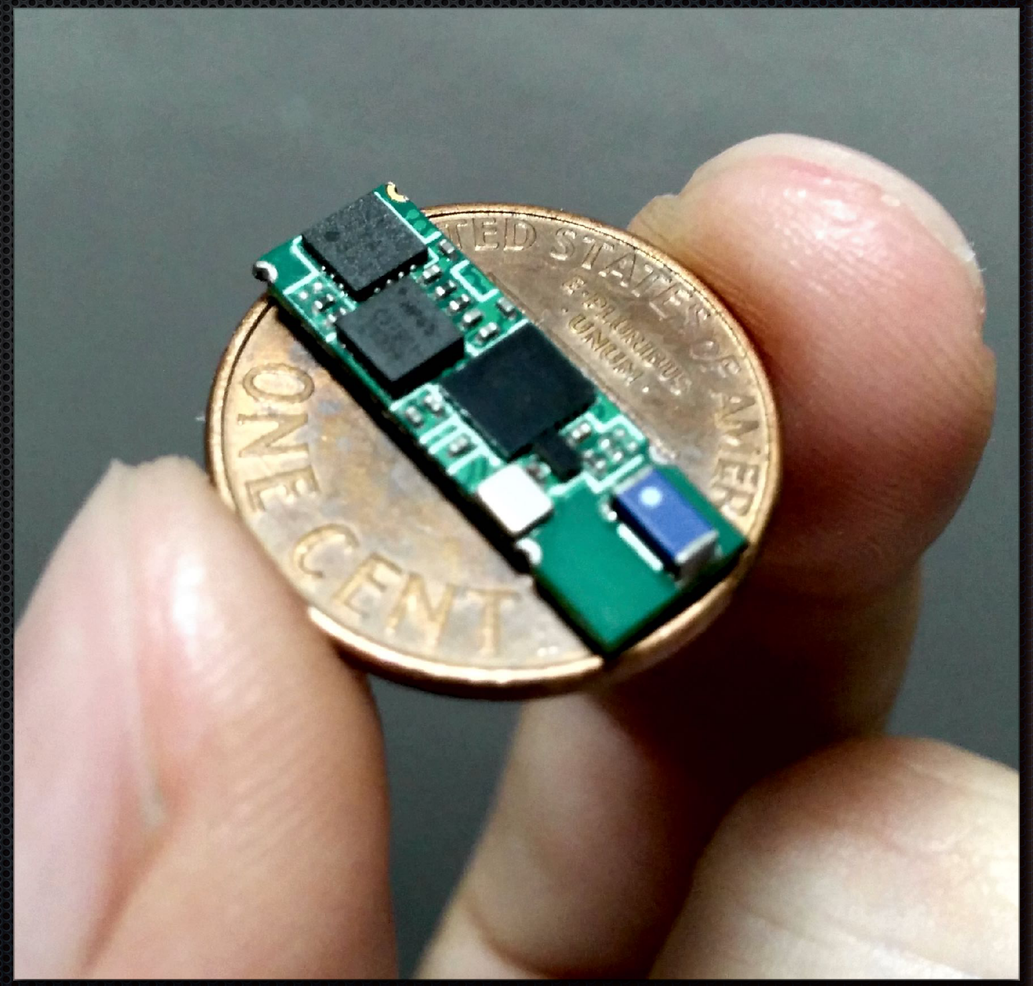
Introduction

- Blockchains are touted as the panacea for IoT security
- But blockchains are bulky
- Do they really fit with IoT?



Constrained devices

- Tiny things
  - 4 kb SRAM, 32 kb Flash
  - But often a 32 bit CPU
- Small devices
  - 256 kb to 2 Mb of RAM
  - Few megabytes of Flash



Distributed ledgers reality

- A full node is **bulky**
  - even for IOTA…
- Full node needed to *trust*
  - Trust involves checking

Ethereum system requirements

- Ethereum *archival* node:
  stores all of Ethereum history
  - 1.1 Tb of striped SSD
    (2 x 1 Tb fast SSD)
  - Server class fast PC
  - Finland's fastest available Internet connectivity
- Sync from zero: **2 weeks**

Ethereum system requirements

- Ethereum *full* node:
  able to verify new transactions
  (and mine, with a GPU)
  - 10 Gb of storage
  - Minimum 4 Gb memory
- Sync from zero: **about 2 hours**

Ethereum reality

- **Time** to secure a transaction:
  - about 2 minutes
- **Cost** to secure a transaction:
  - average today ~ $1*
  - very volatile: $ 0.40 – 4.15

* For an average sized transaction. Mere fund transfer some $ 0.20 as of today.

IOTA reality

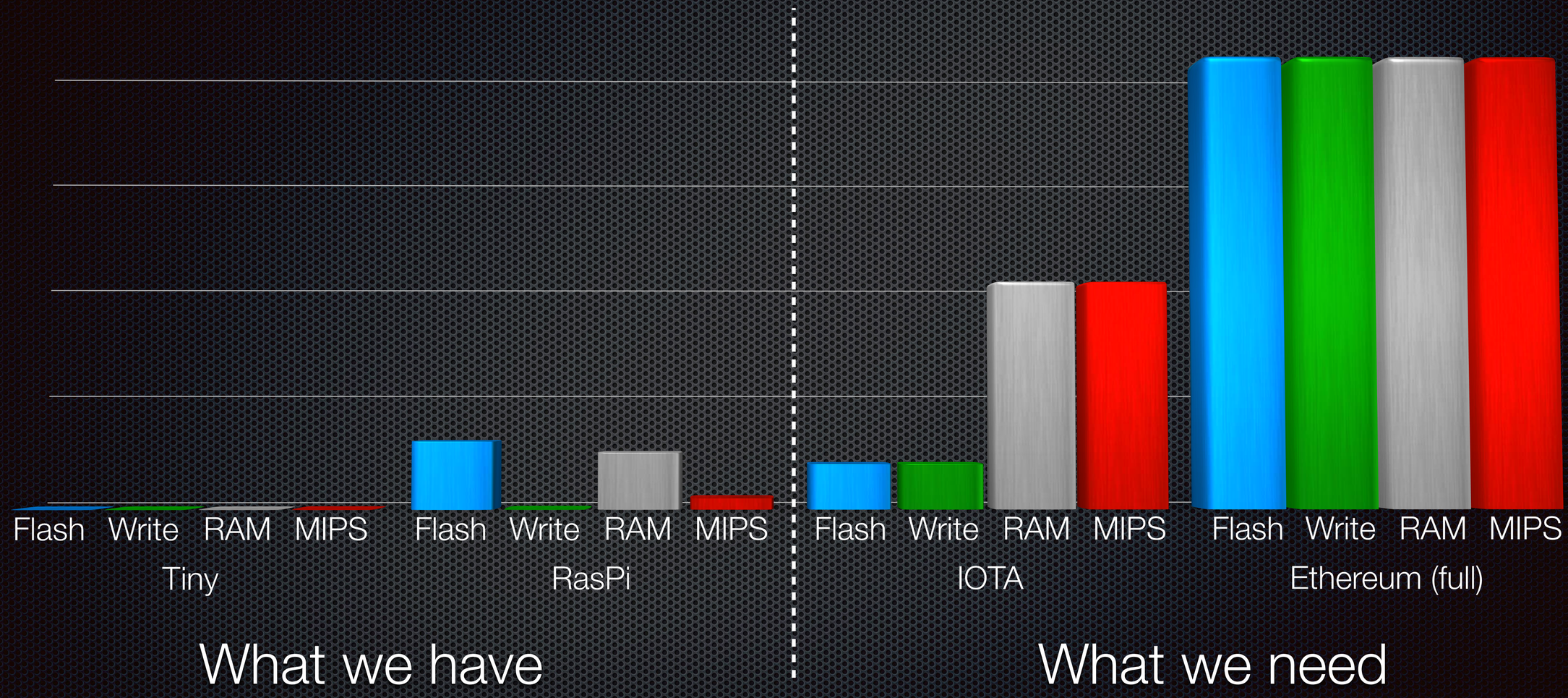
- IOTA full node
  - 20+ GB of Storage
  - 4+ GB of RAM
  - Server class PC

Reality check

	Tiny thing	RasPi 3+	IOTA full node	Ethereum full node	Ethereum archive
CPU MIPS	40	2500	50 000 ?	100 000	100 000
RAM	4 kb	1 Gb	4 Gb	8 Gb	16 Gb
Storage	32 kb	32 Gb	20 Gb	20 Gb	1100 Gb
Read speed	600 Mbps	2 Gbps	> 100 Mbps ?	~ 1 Gbps	~ 1 Gbps
Write speed	< 100 kbps	~ 1 Mbps	> 100 Mbps ?	~1 Gbps	~ 1 Gbps
Node cost	< $5	< $40	> $200 ?	> $500	> $2000

Some numbers are **educated guesses**. IOTA numbers largely unknown.

Reality check (in relative terms, Ethereum = 1)



What we have

What we need

Note: **No mining** involved here, merely keeping up to date

Toughest aspects

- **Cost**: Cannot afford a full DLT node (> $200) everywhere
  - Even if can afford storage space, not the storage I/O speed
- **Latency**: Often < 2 seconds vs. minutes or hours in DLT
- **Intermittent connectivity**: IoT must work even if Internet is down
  - Sometimes possible to tolerate reduced functionality for a while

Verdict

- DLTs don’t help *individual* IoT systems: you need *trusted* nodes anyway
- DLTs may be *useful* for *inter-connecting* IoT systems
  - Cf. e.g. the EU H2020 project SOFIE, http://sofie-iot.eu
- DLTs are ***not* a panacea** for IoT security problems
  - Among other things, public DLTs are **very expensive** to use
  - E.g. cost of computing in Ethereum ≈ 1 000 000 × computing in cloud