DFINITY

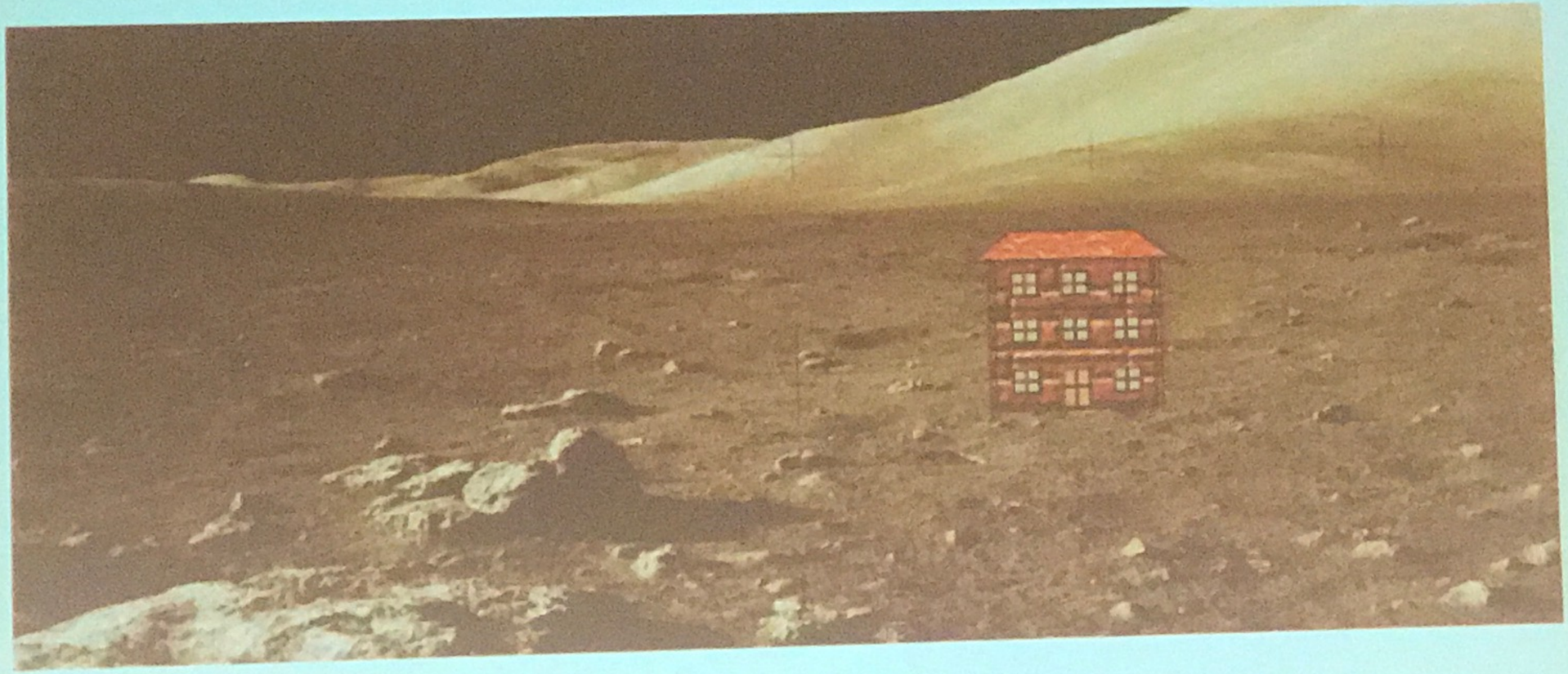
The Pros and Cons of Blockchain for Privacy

Dr. Jan Camenisch
Head of Cryptography & Privacy

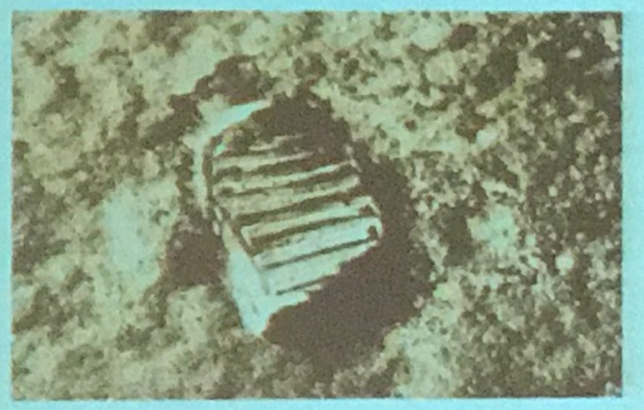
ifip

ifip

... but end up doing this



Computers never forget



- Data is stored by default
- Data mining gets ever better
- Apps built to use & generate (too much) data
- New (ways of) businesses using personal data

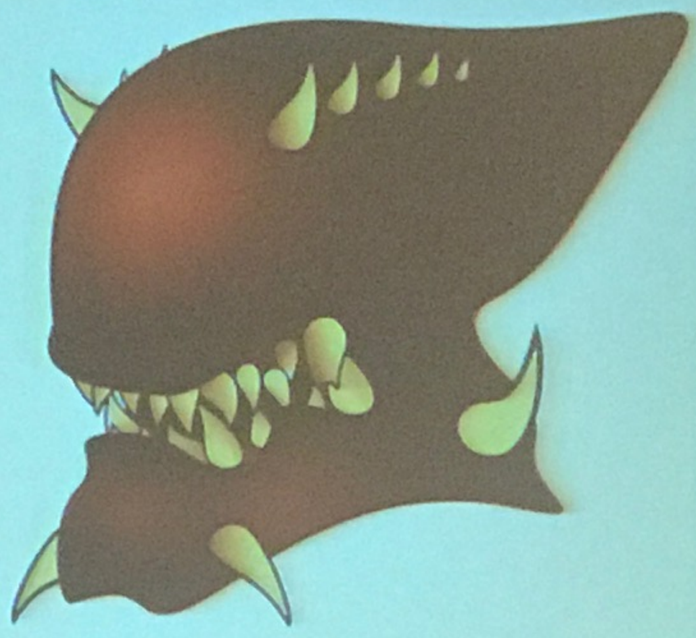
- Humans forget most things too quickly
- Paper collects dust in drawers

But that's how we design and build applications!

Don’t believe in (data-hungry) aliens?

Data is easily available

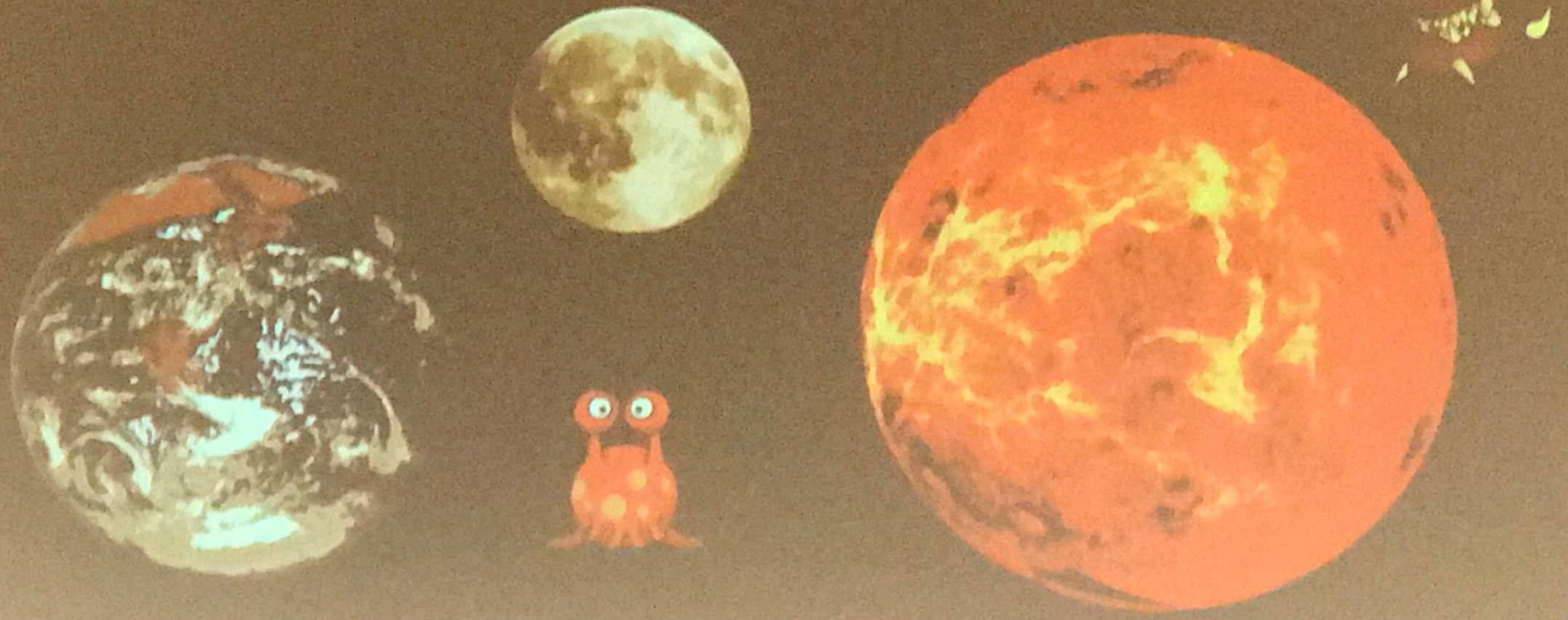
- cf *Massive* scale mass surveillance
- Collecting data and meta data
- Not by breaking encryption



Damage done

- Millions of hacked passwords (100'000 followers $115 - 2013)
- Stolen identity ($150 - 2005, $15 - 2009, $5 - 2013, $1 - 2016)
- $15'000'000'000 cost of identity theft worldwide (2015)

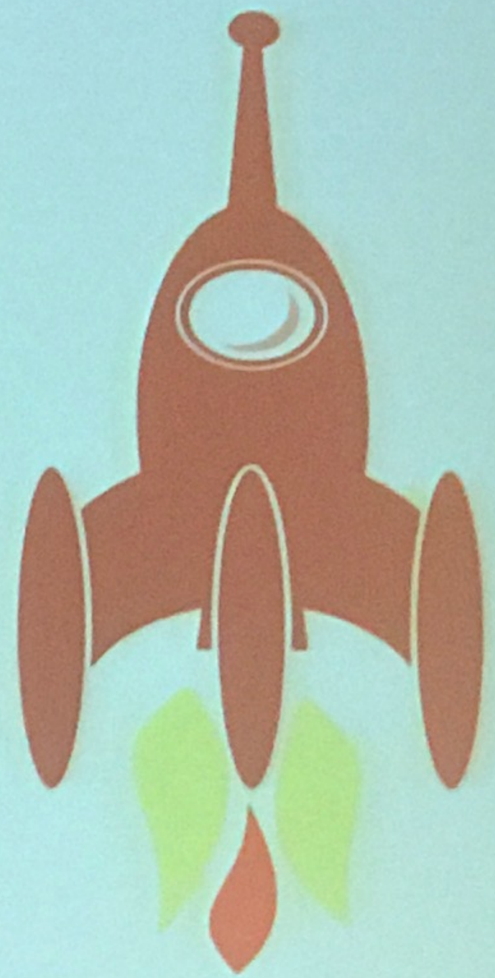
So, we will deploy in very nasty environments



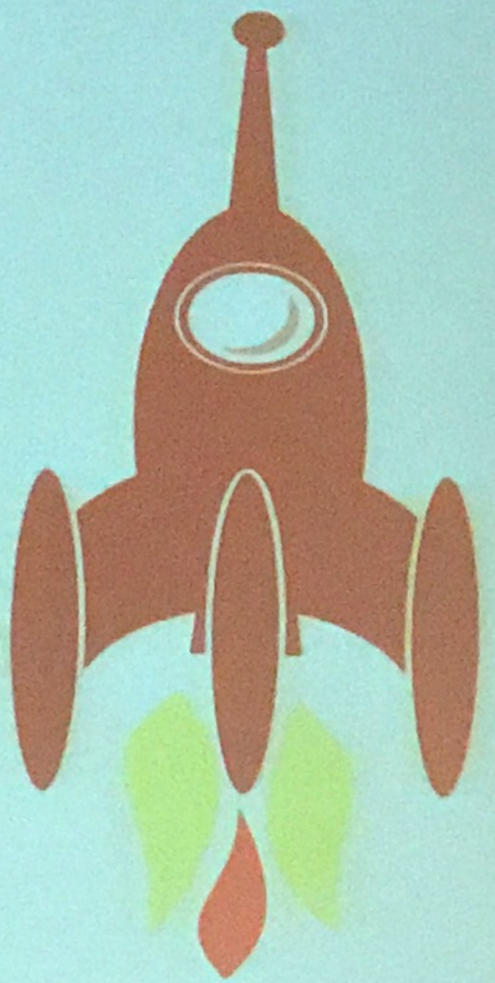
Security & Privacy is not a lost cause

We need paradigm shift:

build things for use on venus
rather than the sandy beach!



Security & Privacy is not a lost cause

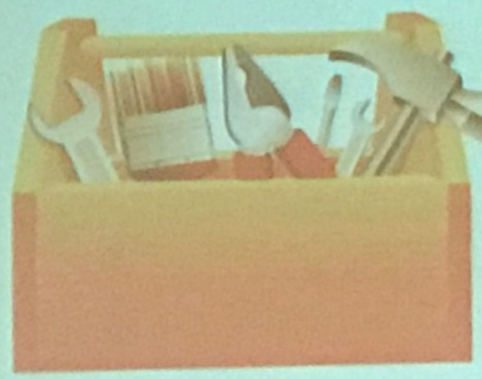


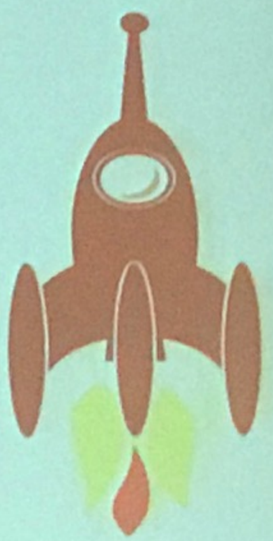
That means:

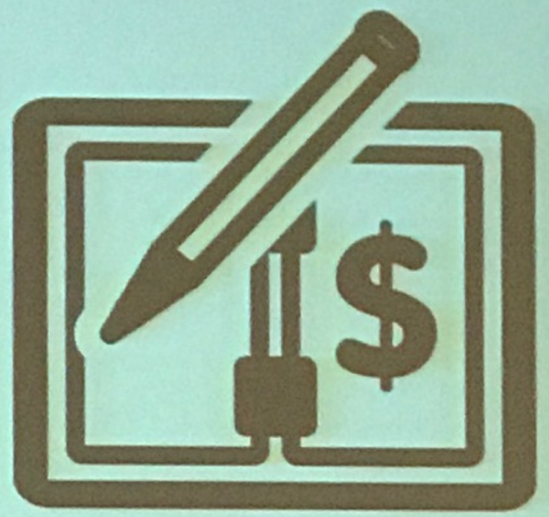
- Use only minimal data necessary
- Encrypt every bit – and keep it like that
- Attach usage policies to each bit

Good news:

Cryptography allows for that!



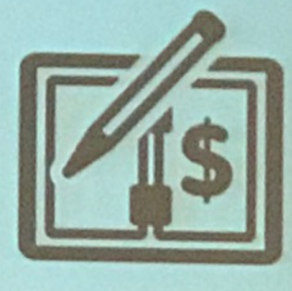


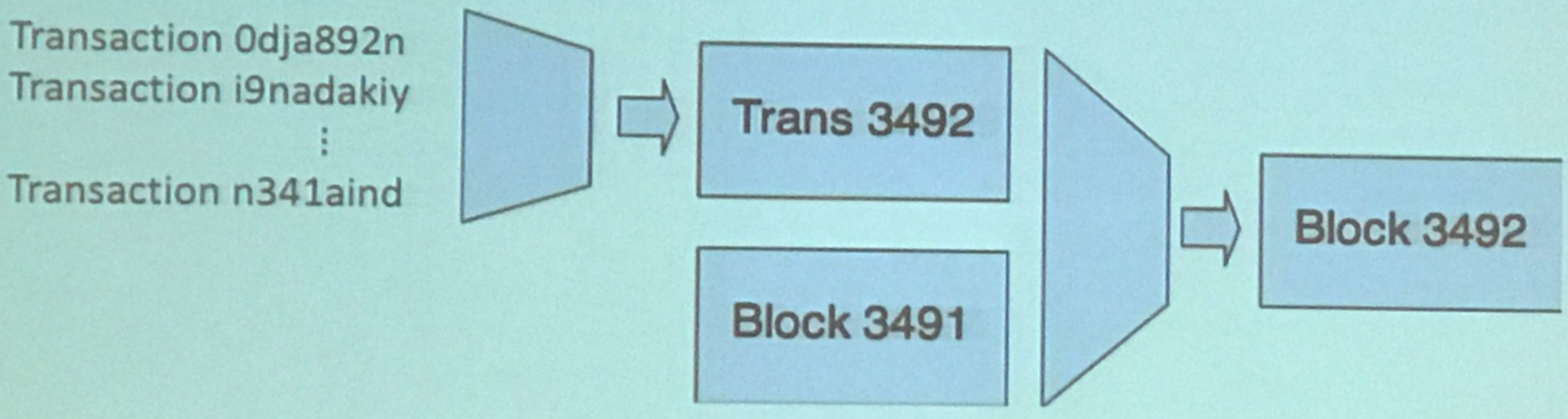


Bad news:

Everyone wants to publish all data on a blockchain!

A chain of blocks

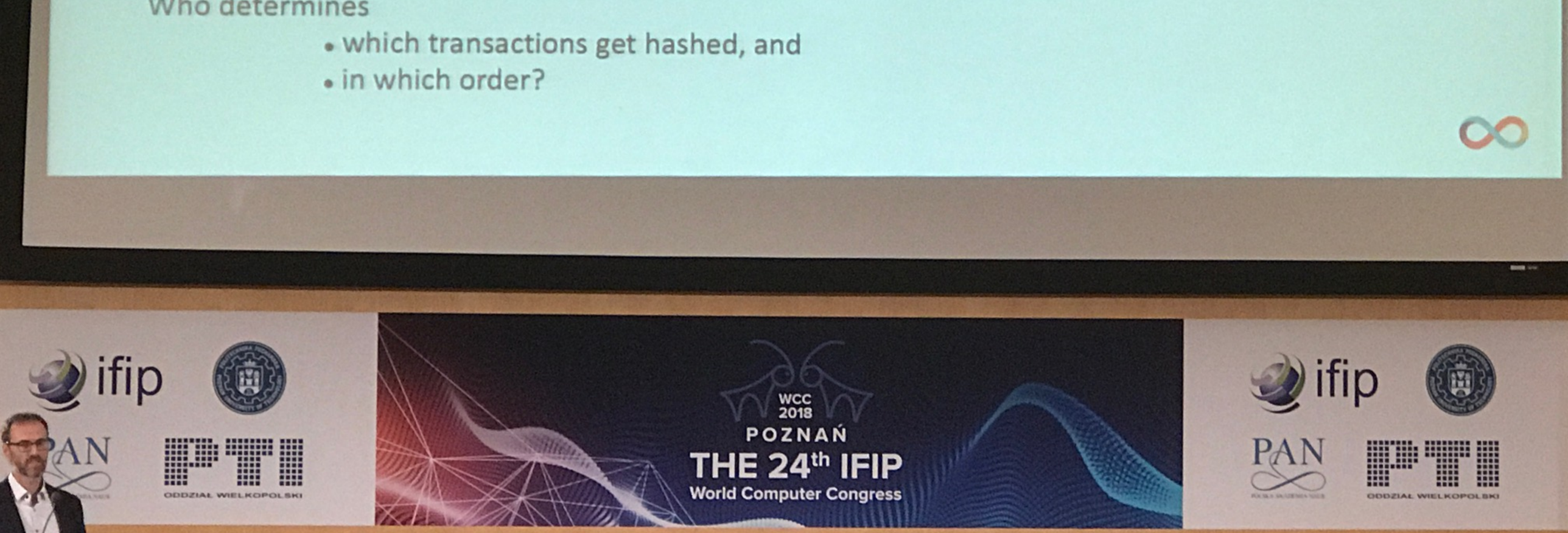




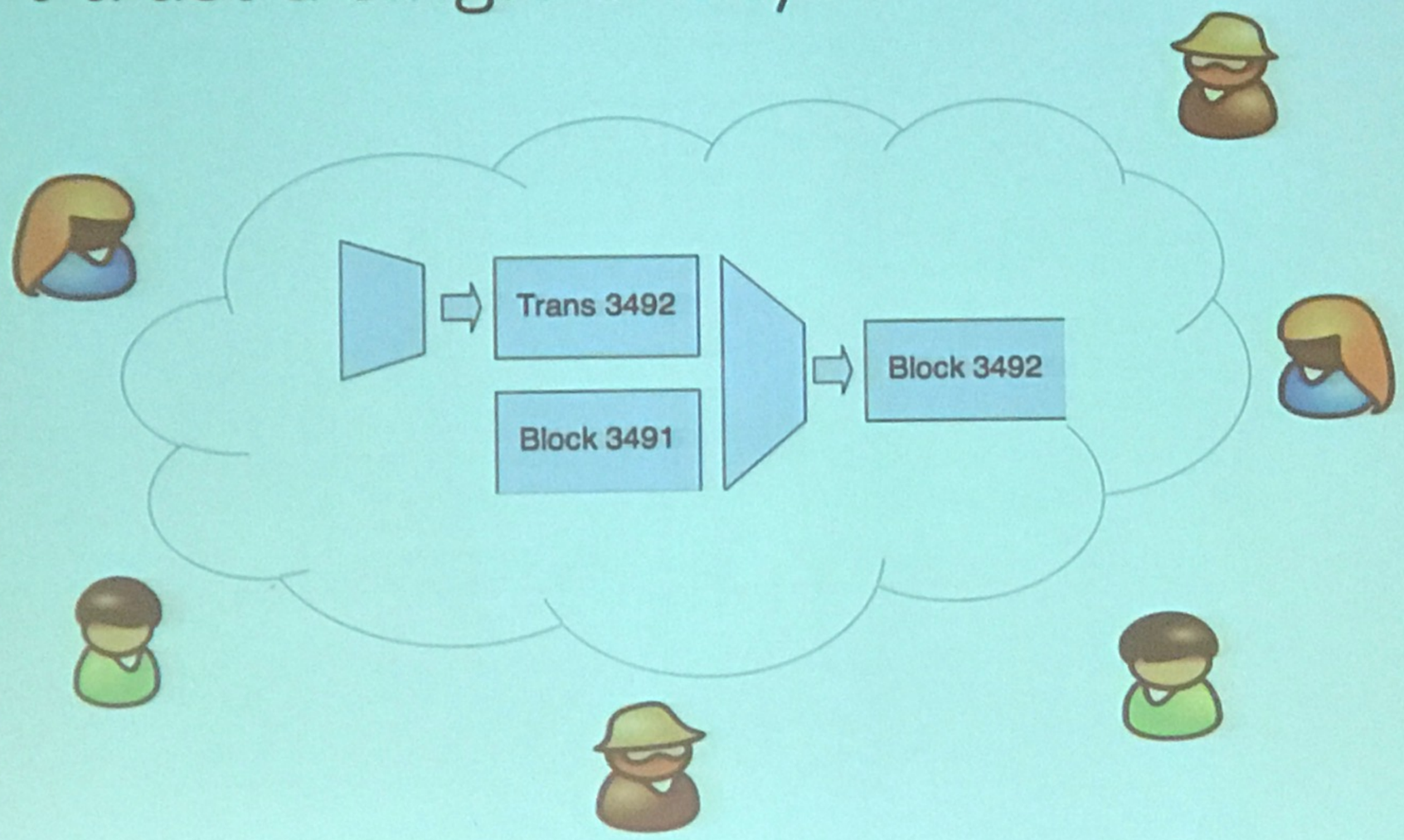
... just an iterated hash computation on transactions

Who determines

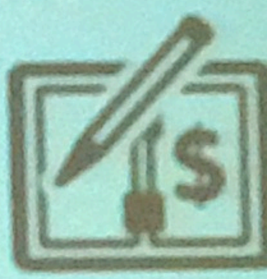
- which transactions get hashed, and
- in which order?



Can’t trust a single entity!



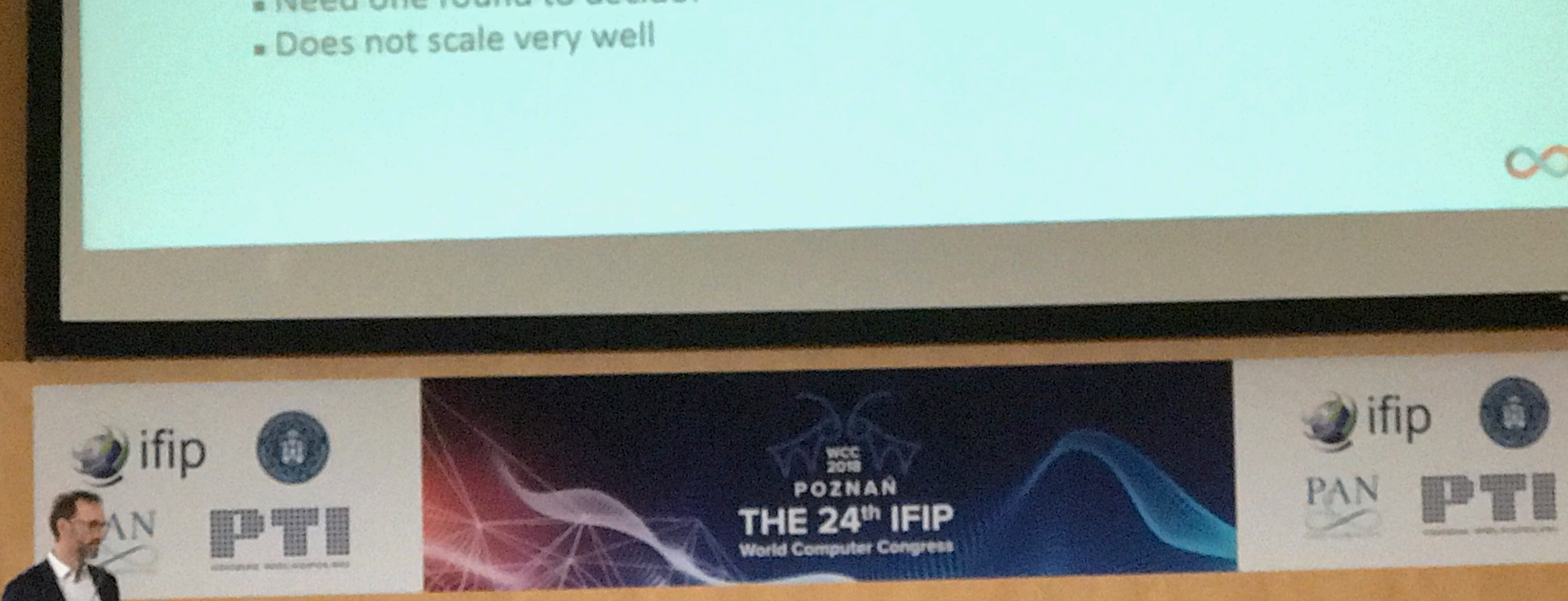
Different Blockchains, Depending on Who Decides



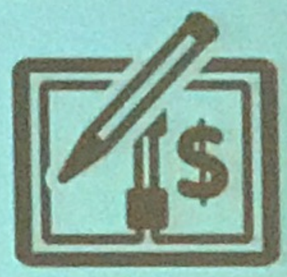
But *who* is the community, who has how *many* votes?

Classic Consensus Protocols (Byzantine Agreement)
Called *Permissioned* Blockchain

- Majority of chain-maintaining parties decide
- Works if majority (1/2 or 2/3, depending) is honest
- Need one round to decide!
- Does not scale very well



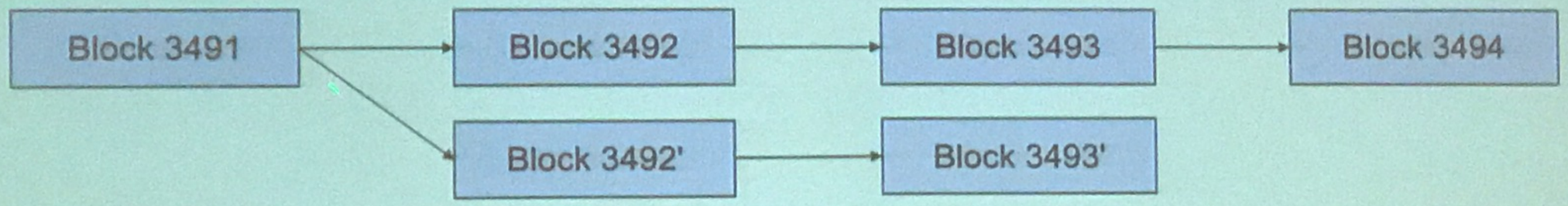
Different Blockchains, Depending on Who Decides



Proof of Work (Classic Bitcoin)

- Whoever finds r s.t. Hash(Block i, Tx i+1, r) = ***...****000...000 = Block i+1
- Need to test many r's; number of 0's defined by time it takes for someone to find r
- Decision is taken by whoever solves "hash-problem" first
- Needs many rounds to agree on final decision

Chain forks



Fork happens because

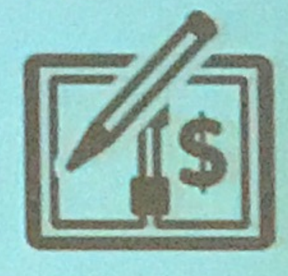
- Find different r at (almost) the same time (with possibly different transactions)
- People mine different blocks because they do not agree on transactions
- Adversary creates fork for its benefit

Conflict resolution: e.g., longest chain considered valid

- eventually chain can no longer be changed (too many hashes)
- thus one has to wait for some time to be sure a transaction has been recorded

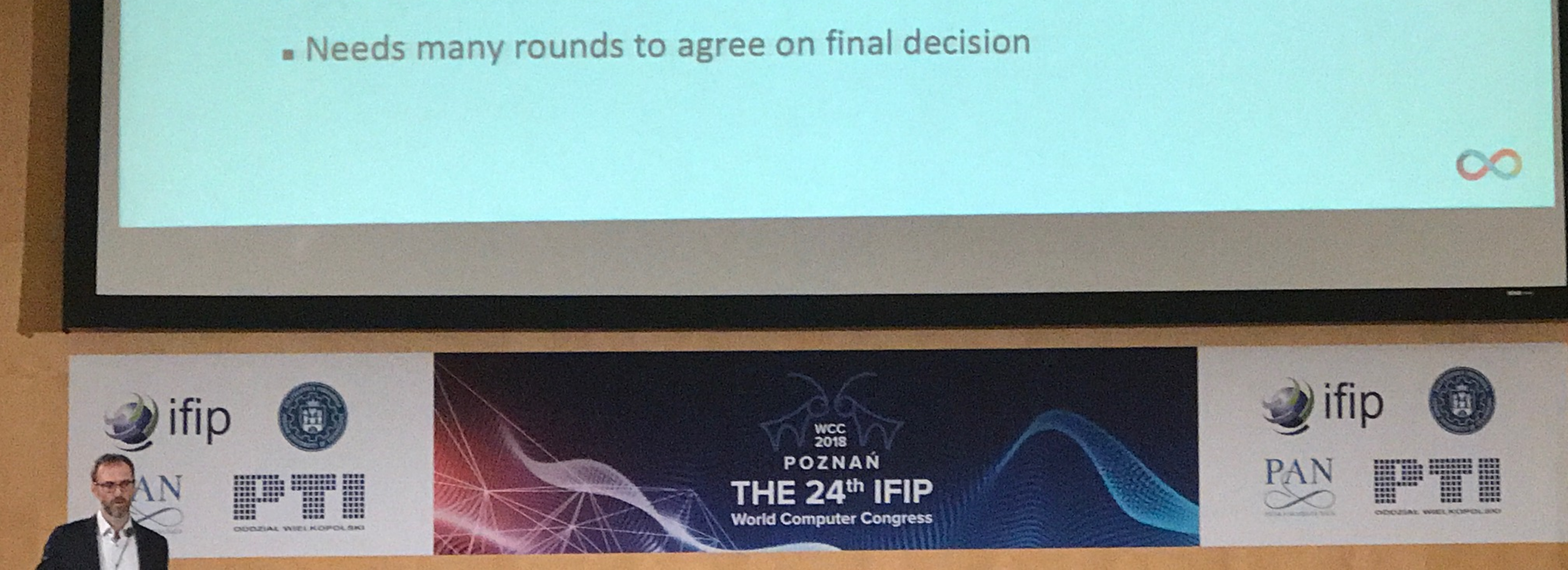
The one with the most computing power/cheapest energy source wins

Different Blockchains, Depending on Who Decides

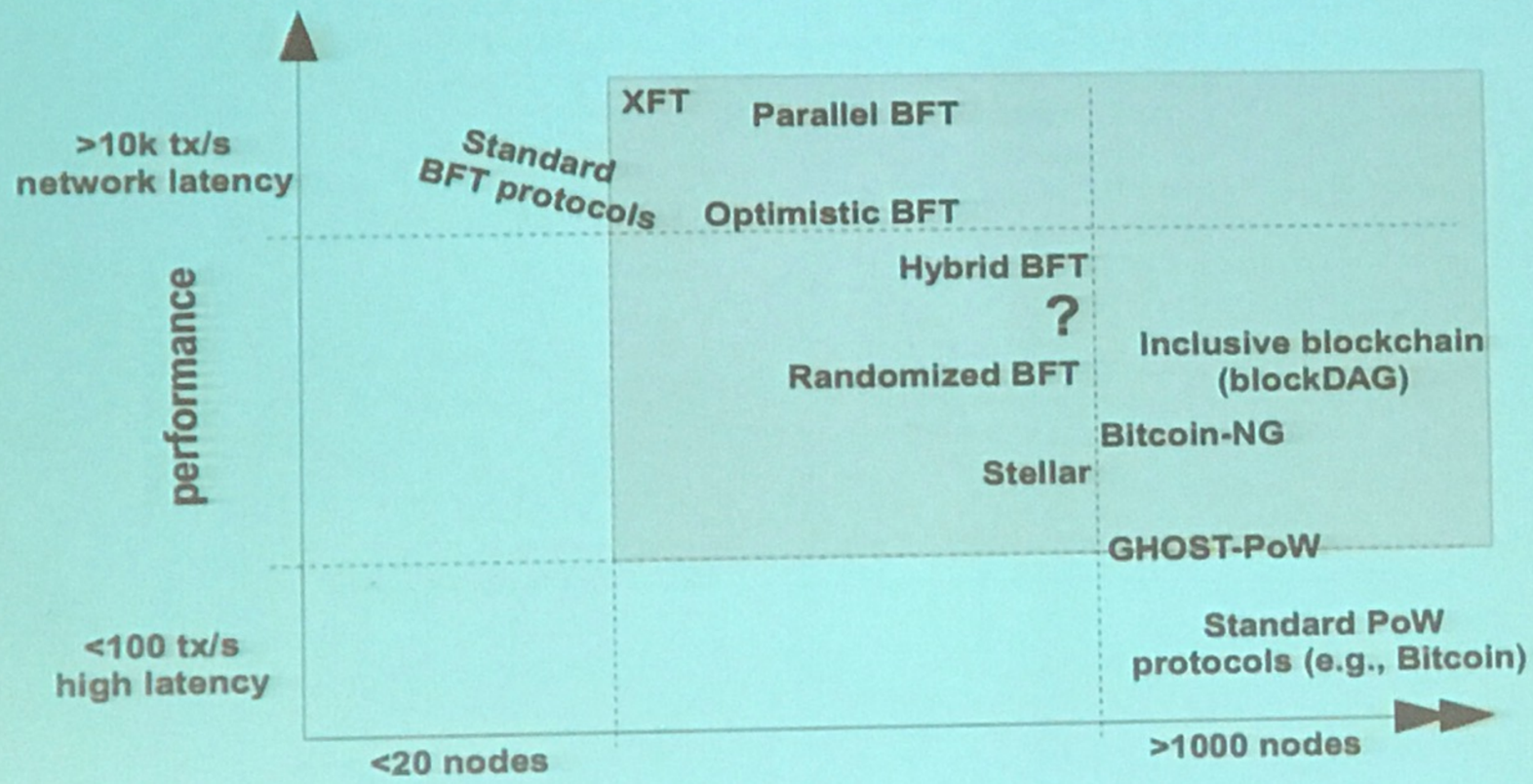


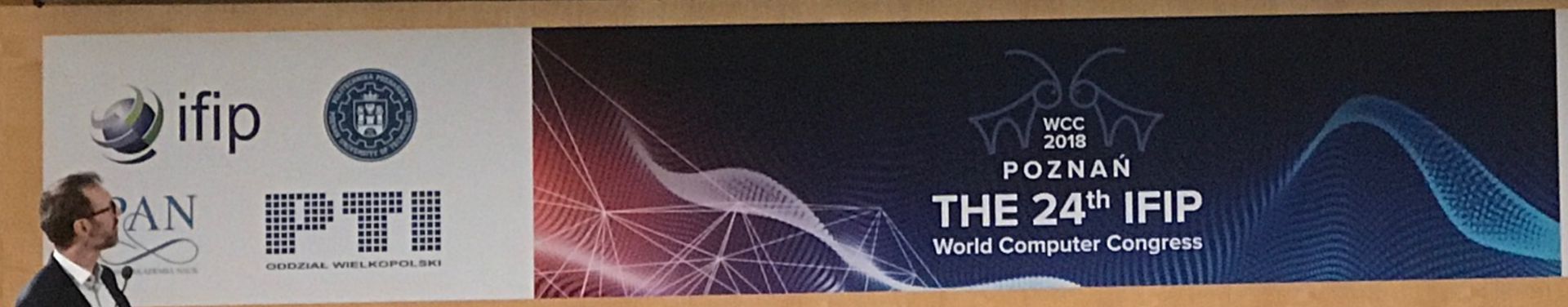
Proof of Stake (to Avoid Energy Waste)

- Designate leader for Block i+1 according to stake (e.g., number of coins, etc)
- Leader decides and makes Block, new leader gets designated
- Select leader in a pseudorandom way, to get an honest one once in a while
- Needs many rounds to agree on final decision

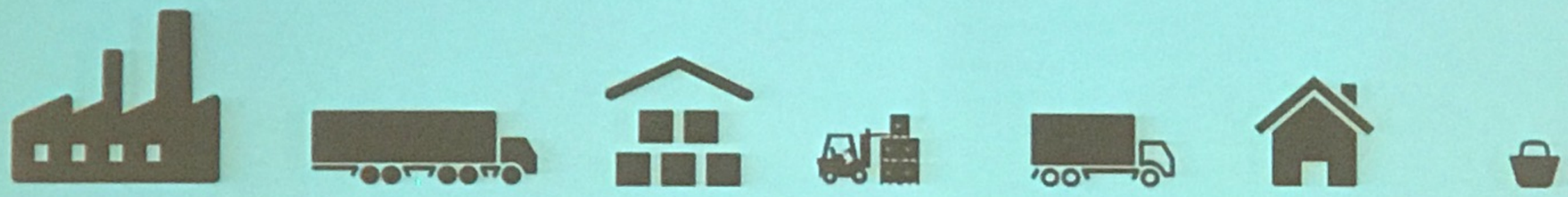


Comparison


>10k tx/s
network latency
<100 tx/s
high latency
performance
Standard
BFT protocols
XFT
Parallel BFT
Optimistic BFT
Hybrid BFT
?
Randomized BFT
Stellar
Inclusive blockchain
(blockDAG)
Bitcoin-NG
GHOST-PoW
Standard PoW
protocols (e.g., Bitcoin)
<20 nodes
>1000 nodes
node scalability


ifip
PAN
PTI
ODDZIAŁ WIELKOPOLSKI
WCC
2018
POZNAŃ
THE 24th IFIP
World Computer Congress
ifip
PAN
PTI
ODDZIAŁ WIELKOPOLSKI

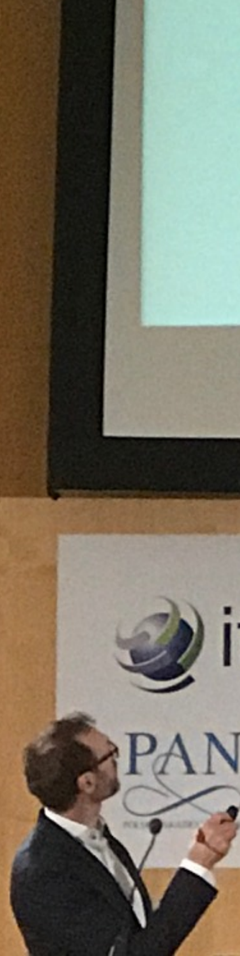
Use cases – supply chain



Everyone can check where product came from and how is was delivered

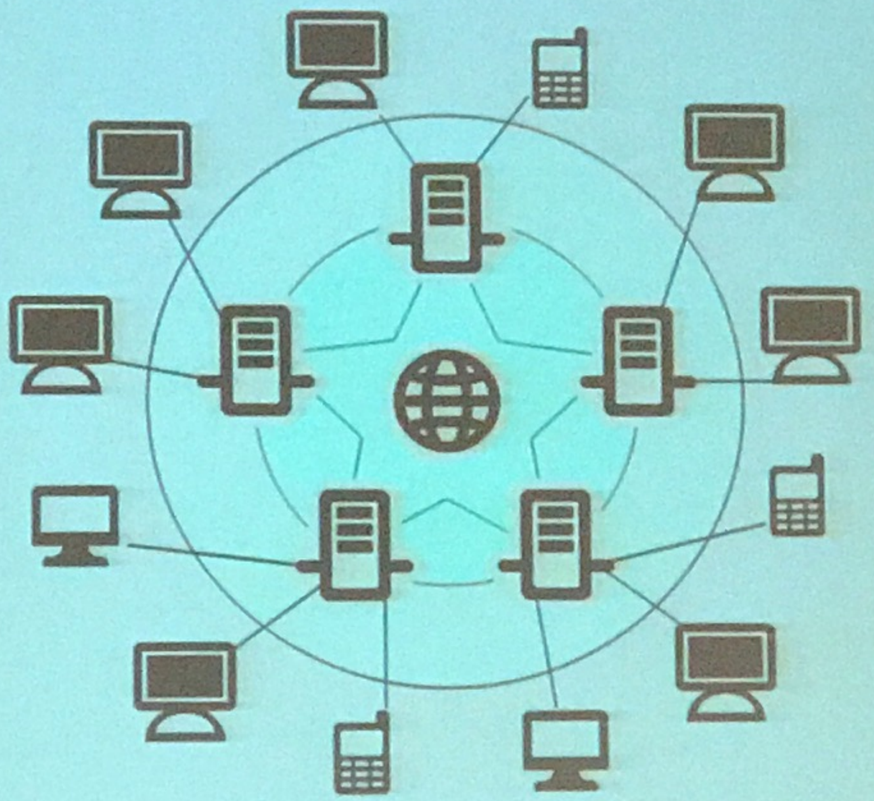
Medical tests, medicine (cooling), car parts, …

Chain maintained by set of parties who do not have a 1-1 relation



Use cases – joint registries

DNS
Revocation/Certificate transparency
Property registries
International Money transfers
Books with accountability



Commonality:

- Set of parties that do not trust each other
- have not one-to-one relation

Smart Contracts

- Transactions can be accompanied by piece of code
- Code is executed on the global state of ledger
- Examples
  - Transfer of money only if some conditions is met
  - Exchange of assets, e.g., rental of flat for a week in exchange of bitcoins
  - Insurance, e.g., flight delays
- Many security issues (increases as system becomes more complex)
  - Buggy code (see press for examples)
  - Contracts and data publicly known

Smart Contracts

- Transactions can be accompanied by piece of code
- Code is executed on the global state of ledger
- Examples
  - Transfer of money only if some conditions is met
  - Exchange of assets, e.g., rental of flat for a week in exchange of bitcoins
  - Insurance, e.g., flight delays
- Many security issues (increases as system becomes more complex)
  - Buggy code (see press for examples)
  - Contracts and data publicly known

Are blockchains bad news?

Cons

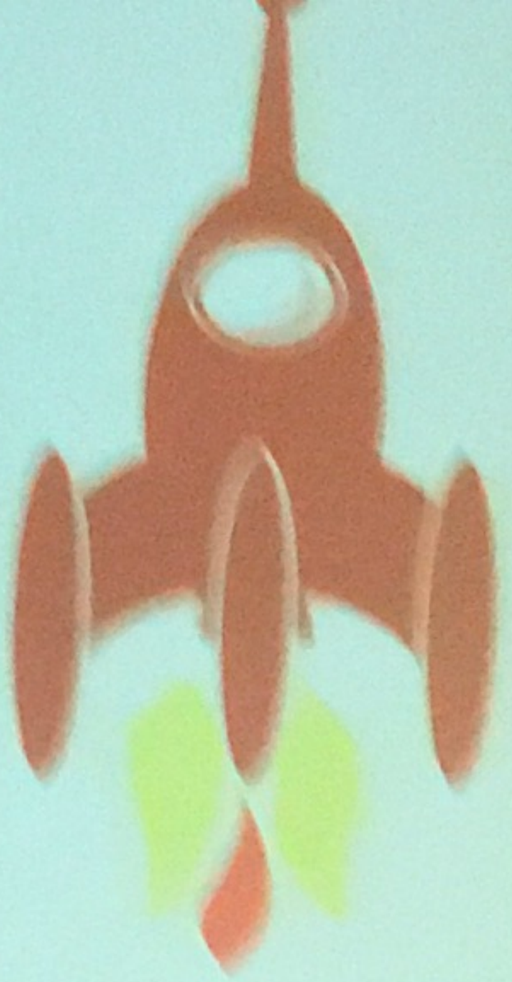
- Data on blockchain public or available to large audience!
  - Bitcoin is not anonymous…
- Even if data is encrypted or hashed
  - Metadata leaks information as well (sometime even more valuable)
  - Crypto system or hash function could be broken in the future
  - Quantum computers break all popular *public key* encryption schemes

Pros

- Data being public has great potential for transparency
- Solve PKI for encryption and privacy preserving authentication
- Everyone talks about crypto (but some mean crypto currency)

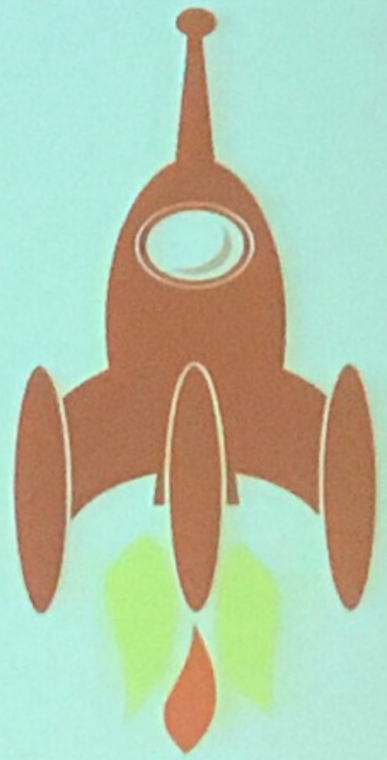
We need paradigm shift:

build things for use on the moon
rather than the sandy beach!



e-Identities done right

Conclusions



Blockchain = Distributing trust over the Internet

- Blockchain enables new trust models
- Distributed computing + cryptography + economics
- Enables building common infrastructure (also for privacy)
- We are only at the beginning

Need for Privacy more prominent than ever

- Putting all data on Blockchain is a bad idea!
- Much of the needed technology to secure apps exists
- … need to use them & build apps for “space”
- … and make apps usable & secure for end users