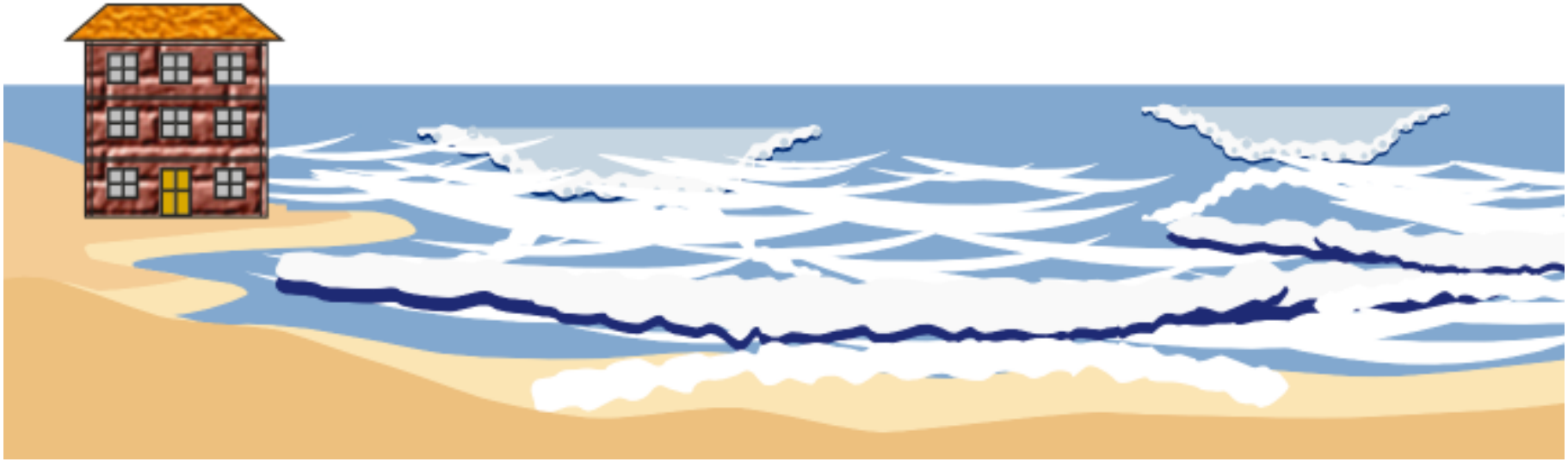
Cryptography for Privacy

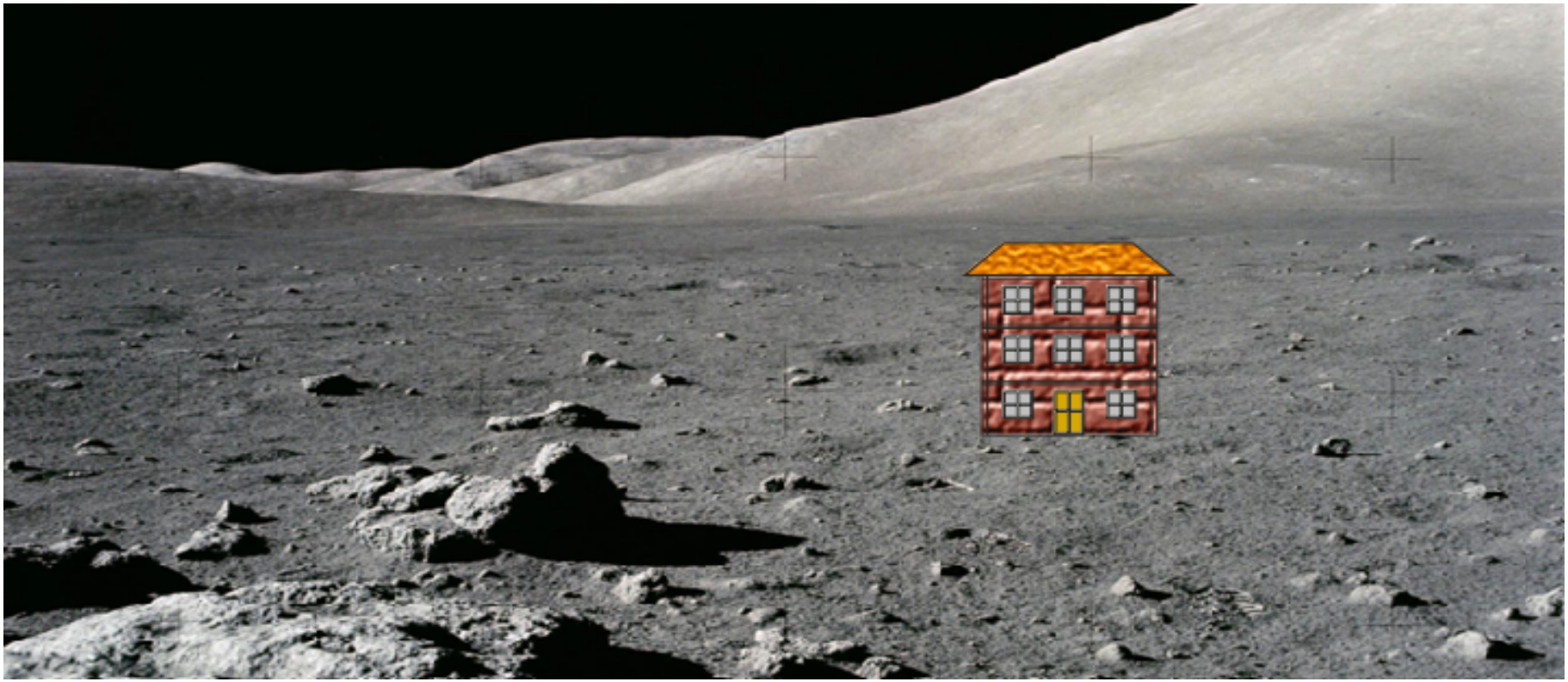
Dr. Jan Camenisch
Head of Research


Our world is turning into cyberspace

That’s what we plan

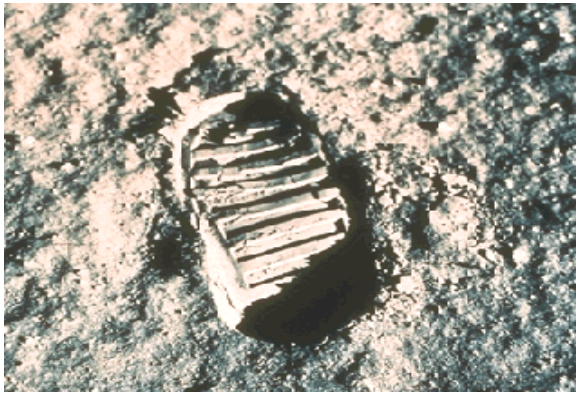


… and that what we end up doing




Houston, we have
a problem!

Computers never forget



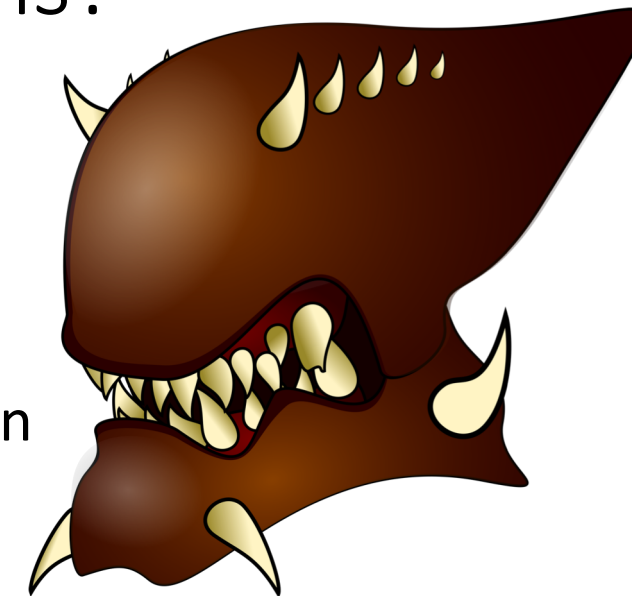
- Data is stored by default
- Data mining gets ever better
- Apps built to use & generate (too much) data
- New (ways of) businesses using personal data

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

But that's how we design and build applications!


Cyberspace, full of enemies

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



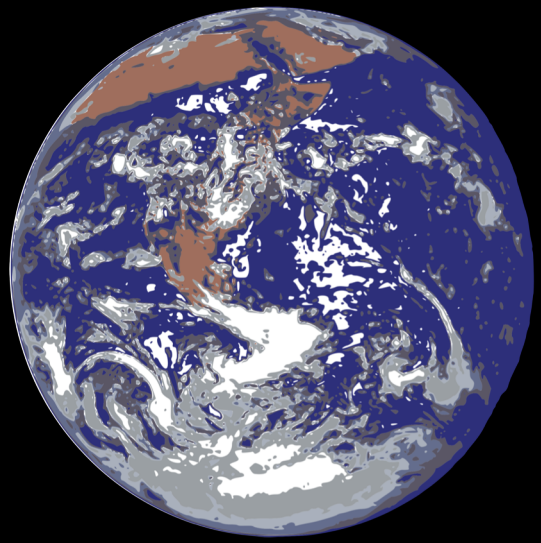
Data is easily available

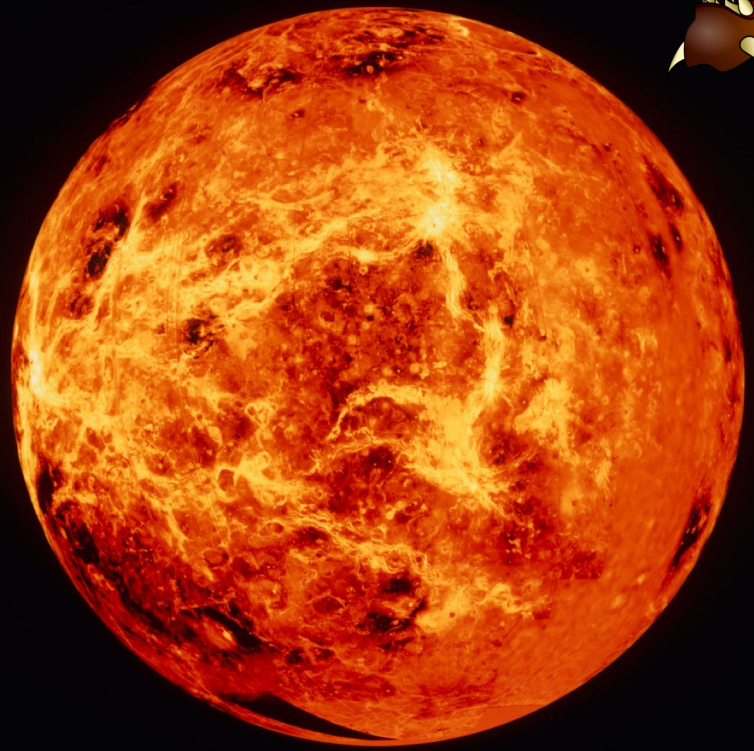
- cf *Massive* scale mass surveillance
- Every one is collecting data and meta data
- Getting data does not require breaking encryption

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

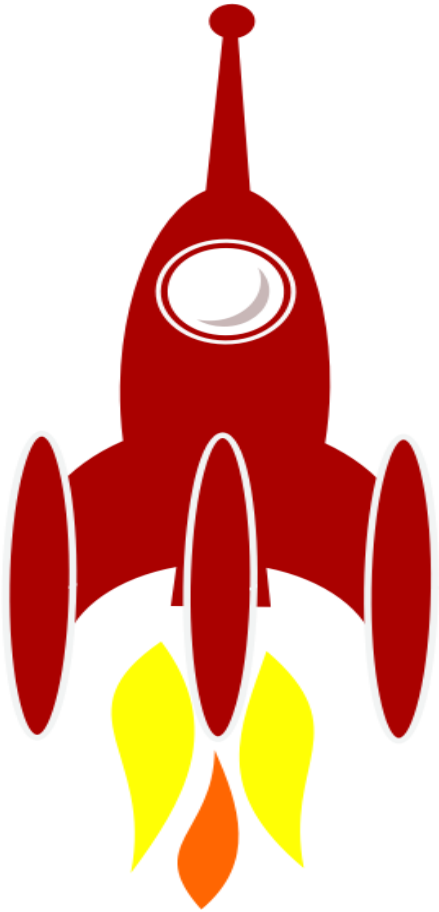




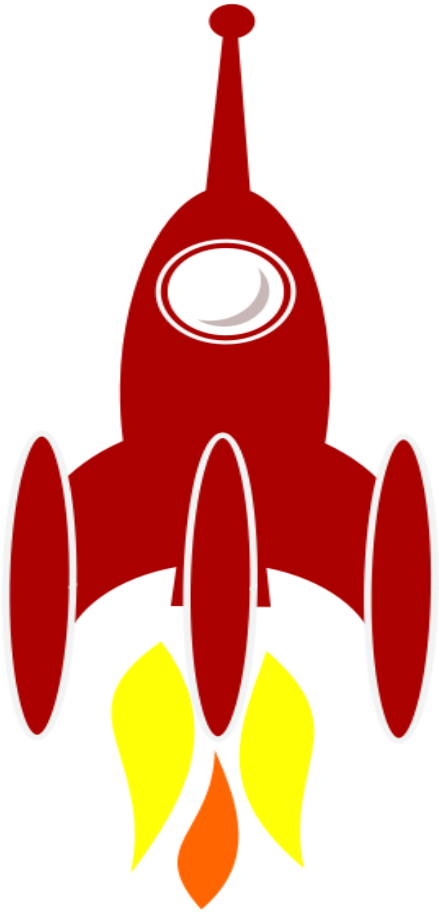
Security & Privacy is not a lost cause!

We need paradigm shift:

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



Security & Privacy is not a lost cause!

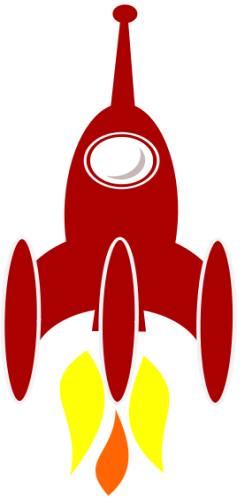


That means:

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

Good news:

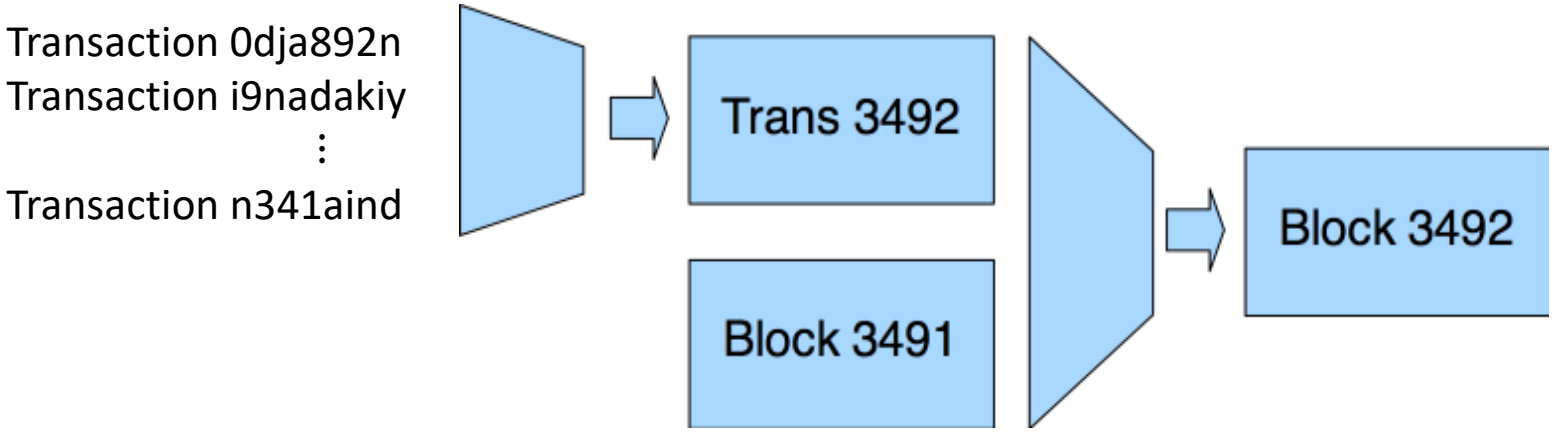
Cryptography allows for that!



Bad news:

Everyone wants to put all data on a blockchain!

A chain of blocks

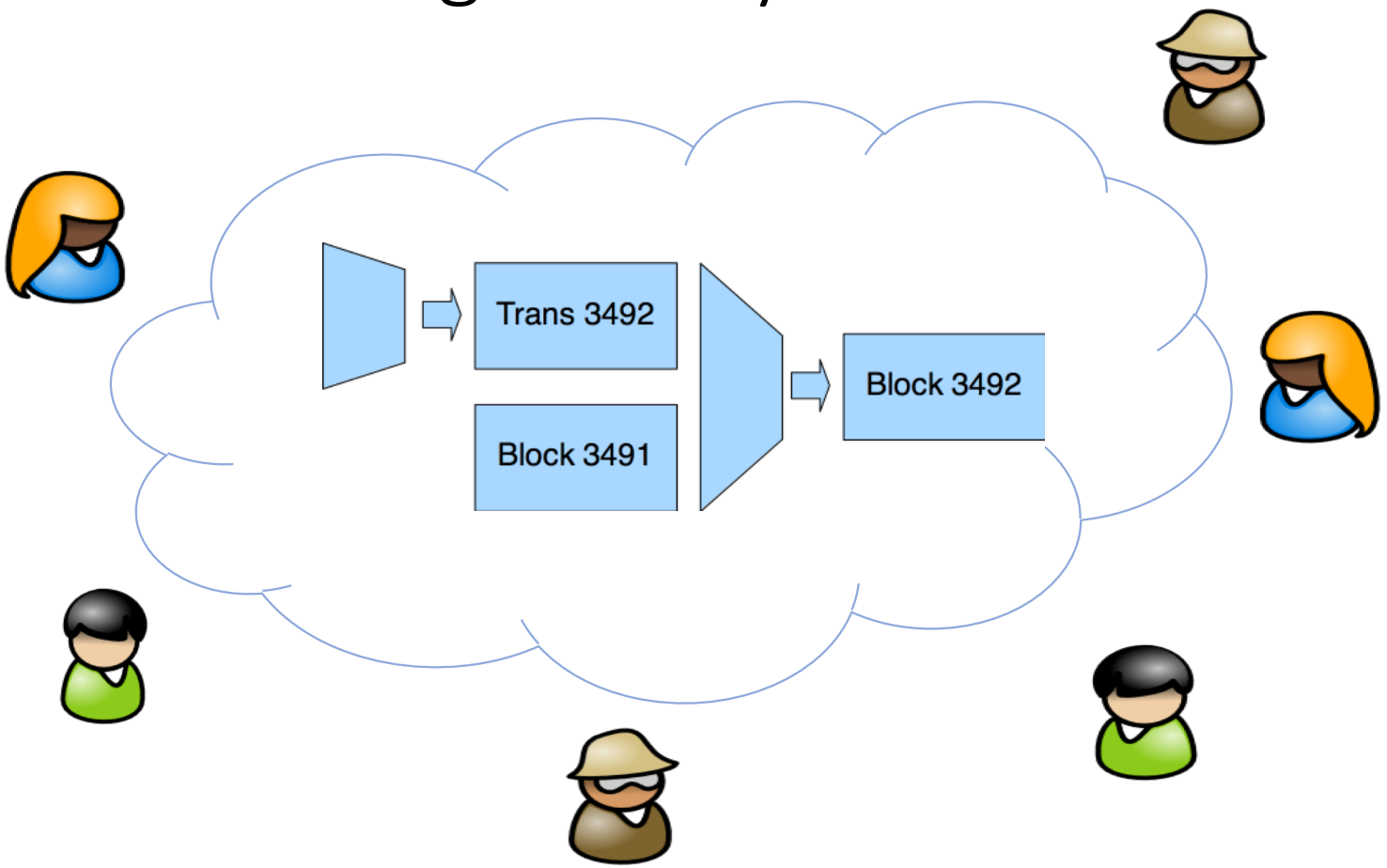


… just an iterated hash computation on transactions
… realizes a write only bulletin board with order

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

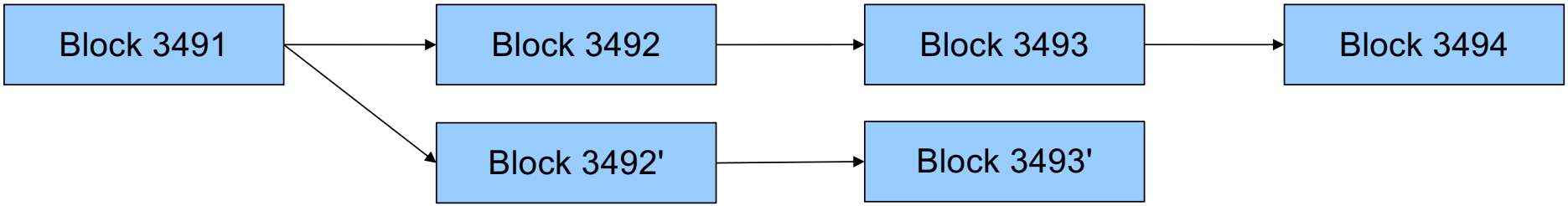
- Majority of chain-maintaining parties decide
- Works if majority (1/2 or 2/3, depending) is honest
- Need one round to decide!
- Does not scale very well

Different Blockchains, Depending on Who Decides

Proof of Work (Classic Bitcoin)

- Whoever finds r st Hash(Block i, Tx i+1, r) = **...**00...00 = Block i+1
- Need to test many r's; # of 0's defined by time it takes to find r
- Decision is taken by whoever solves "hash-problem" first
- Needs many rounds to agree on final "decision"

Chain forks



Forks 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

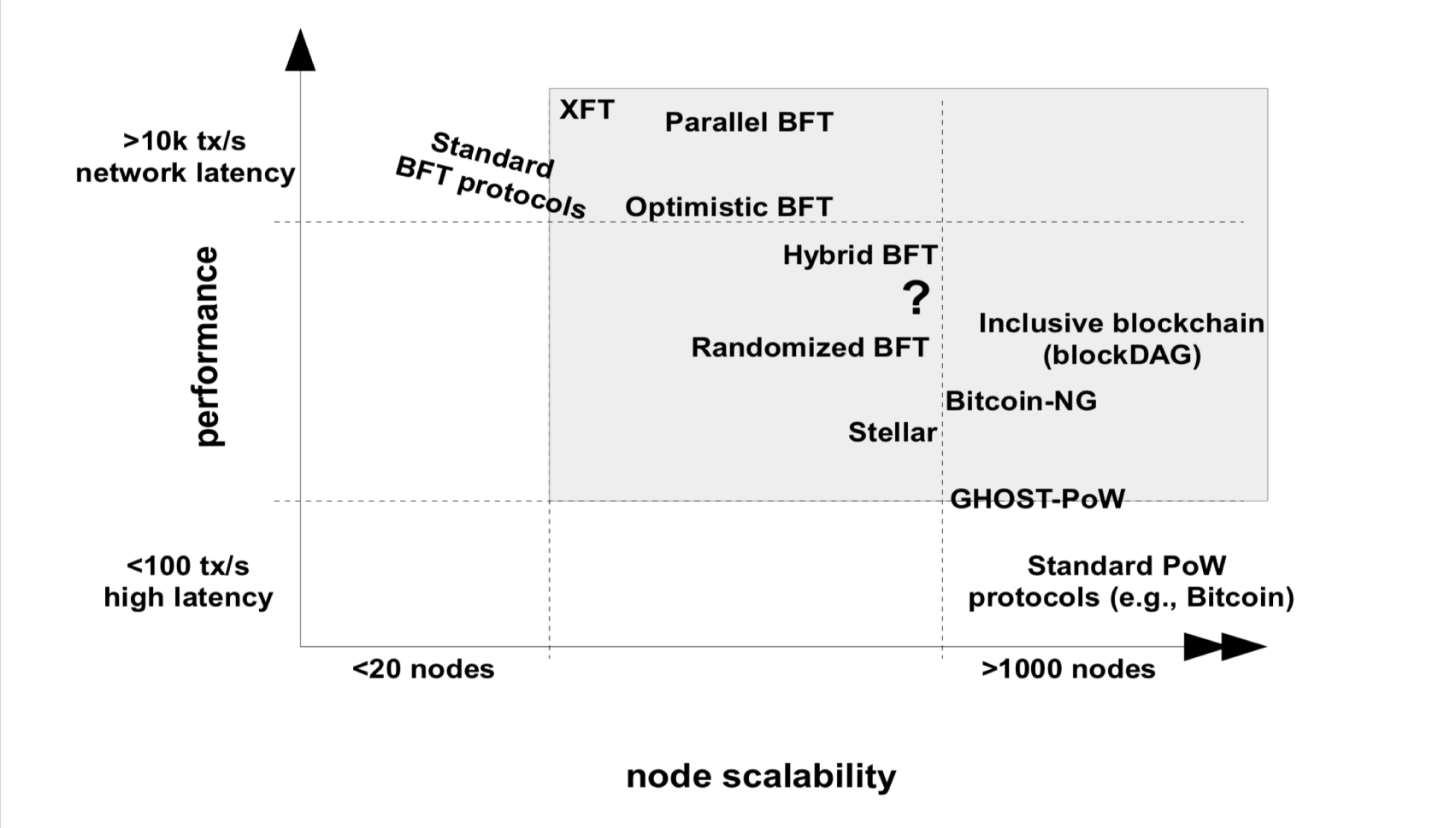
The one with the most computing power/cheapest energy source wins

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
- Can have forks if there is a misbehaving leader
- Needs many rounds to agree on final decision

Comparison


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

Use cases – joint registries

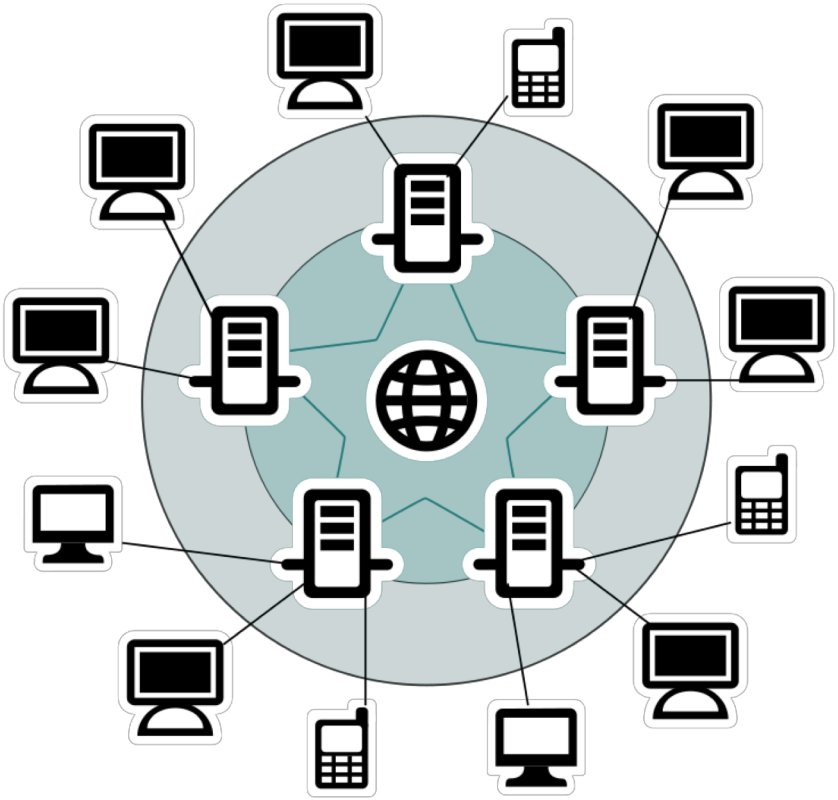
DNS

Revocation/Certificate transparency

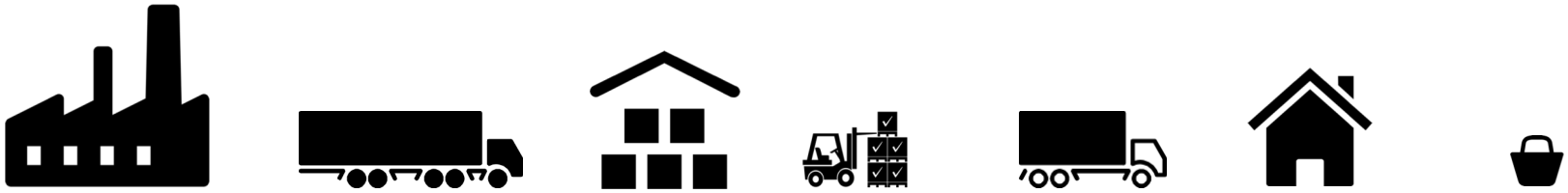
Property registries

International Money transfers

Books with accountability



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

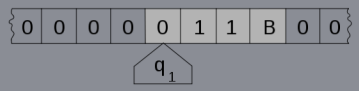
Commonality:

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

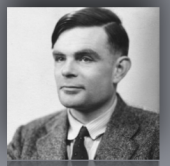
Smart Contracts

- 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

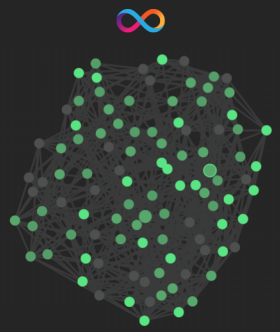
Internet Computer - DFINITY



A computer described **mathematically**…



A computer created by a **physical machine**



A computer created by a **network of computers**

Are blockchains bad news?

Cons

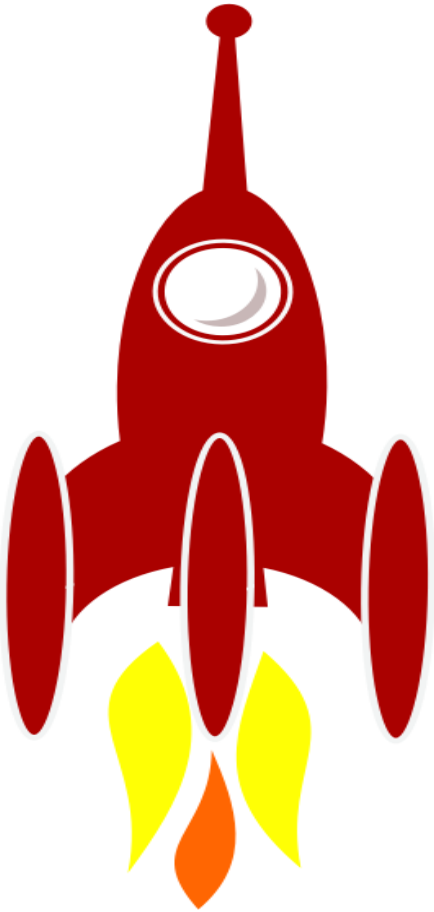
- Data on blockchain public or available to large audience!
  - Bitcoin is not anonymous…
- Even if data is encrypted or hashed
  - Metadata leaks information as well (sometime even more valuable)
  - Crypto system or hash function could be broken in the future
  - Quantum computers break all popular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



Cryptography to the aid!

Mix Networks

Oblivious Transfer

Searchable Encryption

Onion Routing

Confirmer signatures

Group signatures

OT with Access Control

Anonymous Credentials

Blind signatures

Priced OT

Pseudonym Systems

Secret Handshakes

e-voting

Private information retrieval

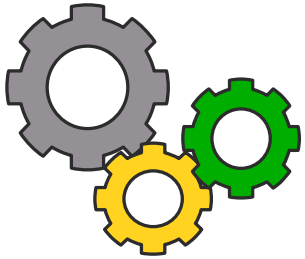
Homomorphic Encryption

Different Cryptographic Approaches

1. Dedicated tailored cryptographic protocol

- Handcrafted from cryptographic primitives
- Tailored Security definitions and proofs
- + fits well
- - hard to do, lots of work, needs to be done for each problem

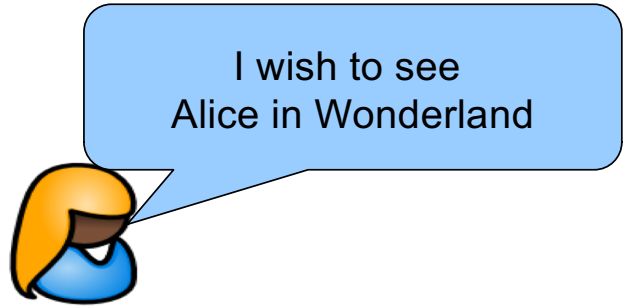
2. Generic approach with multiparty computation (MPC)



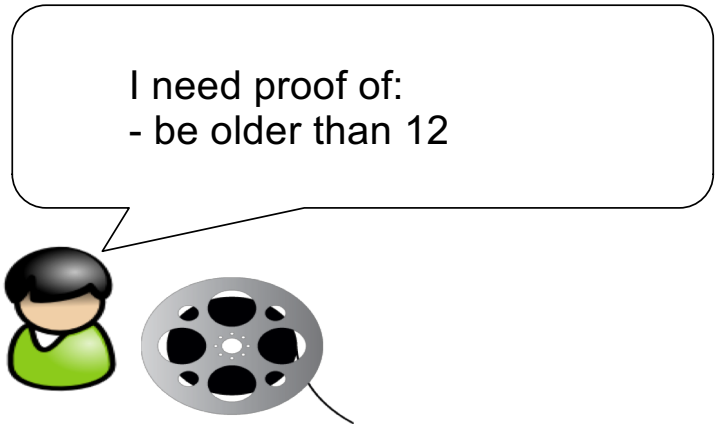
- Use one of the generic MPC “engines”
- Define required function as program
- “compile” program into multiparty
- + Security follows from MPC engine
- - requires all parties to run protocol (however, not all parties are equal)


e-Identities done right

Alice wants to watch a movie at Mplex

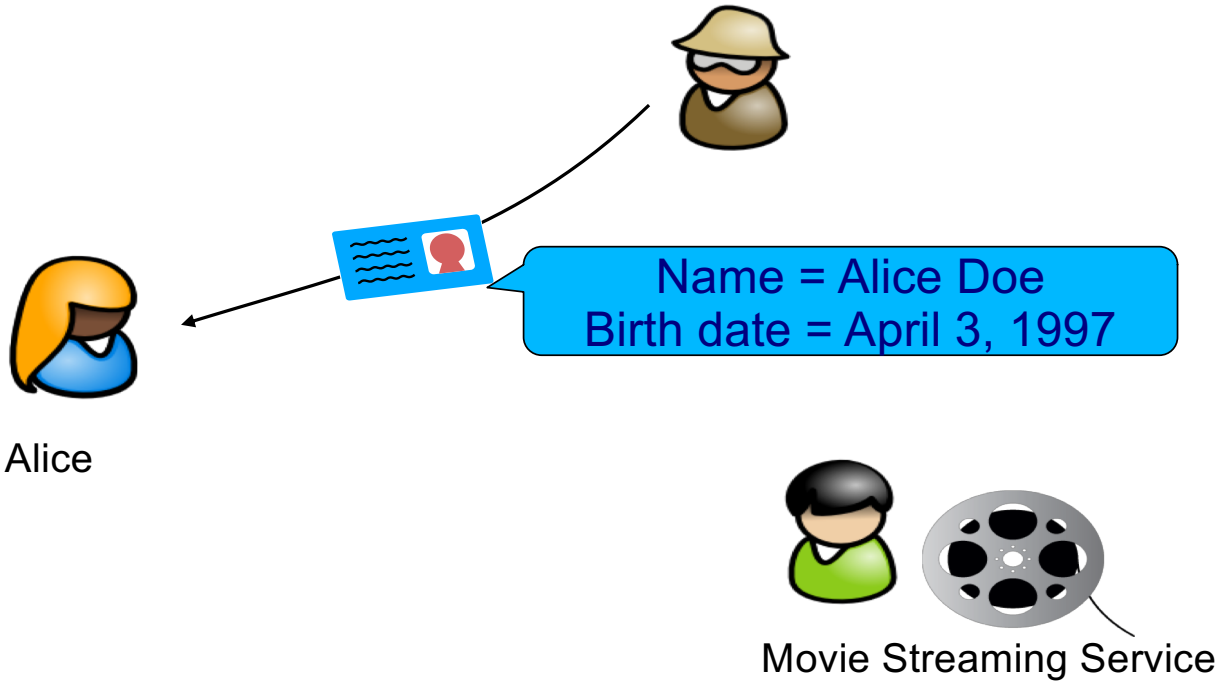


Alice

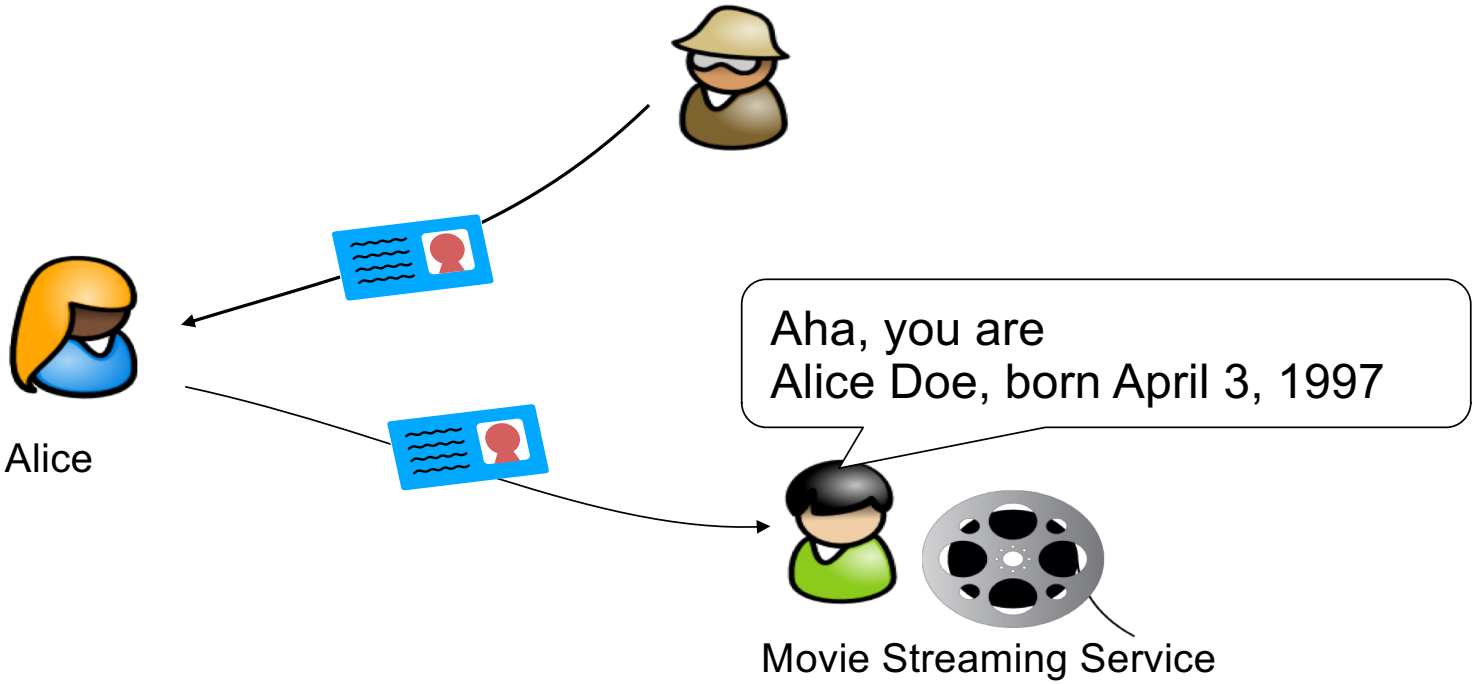


Movie Streaming Service

Alice wants to watch a movie at Mplex



Alice wants to watch a movie at Mplex

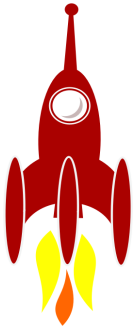


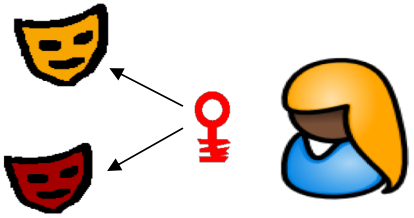
Too much information is revealed!

Privacy-protecting authentication with Anonymous Credentials

Like PKI, but better:

- One secret Identity (secret key)
- Many Public Pseudonyms (public keys)

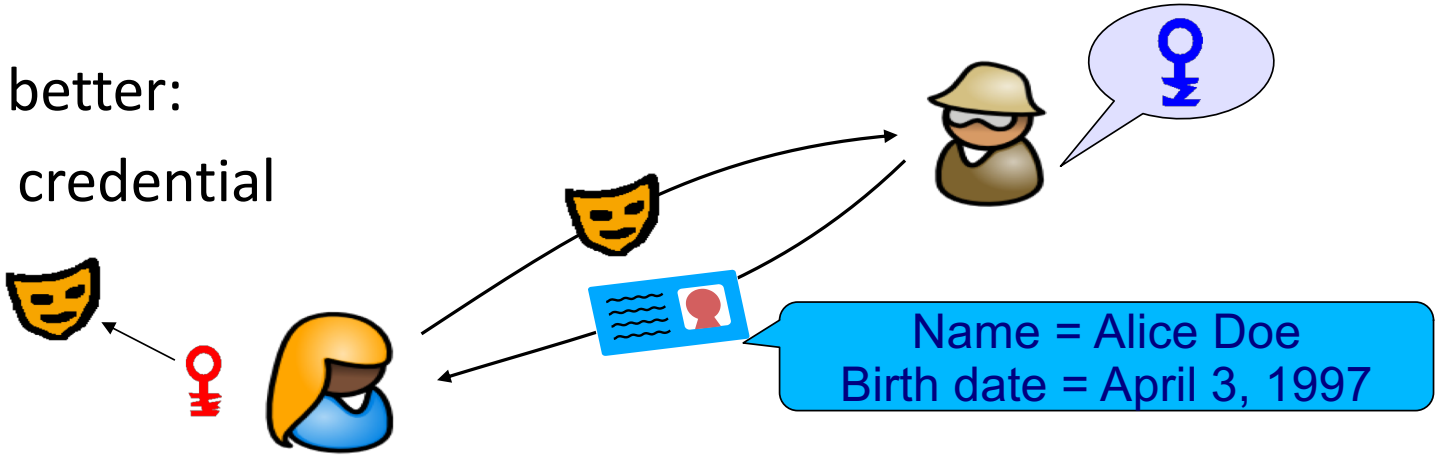


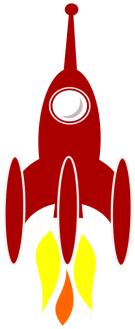


Privacy-protecting authentication with Anonymous Credentials

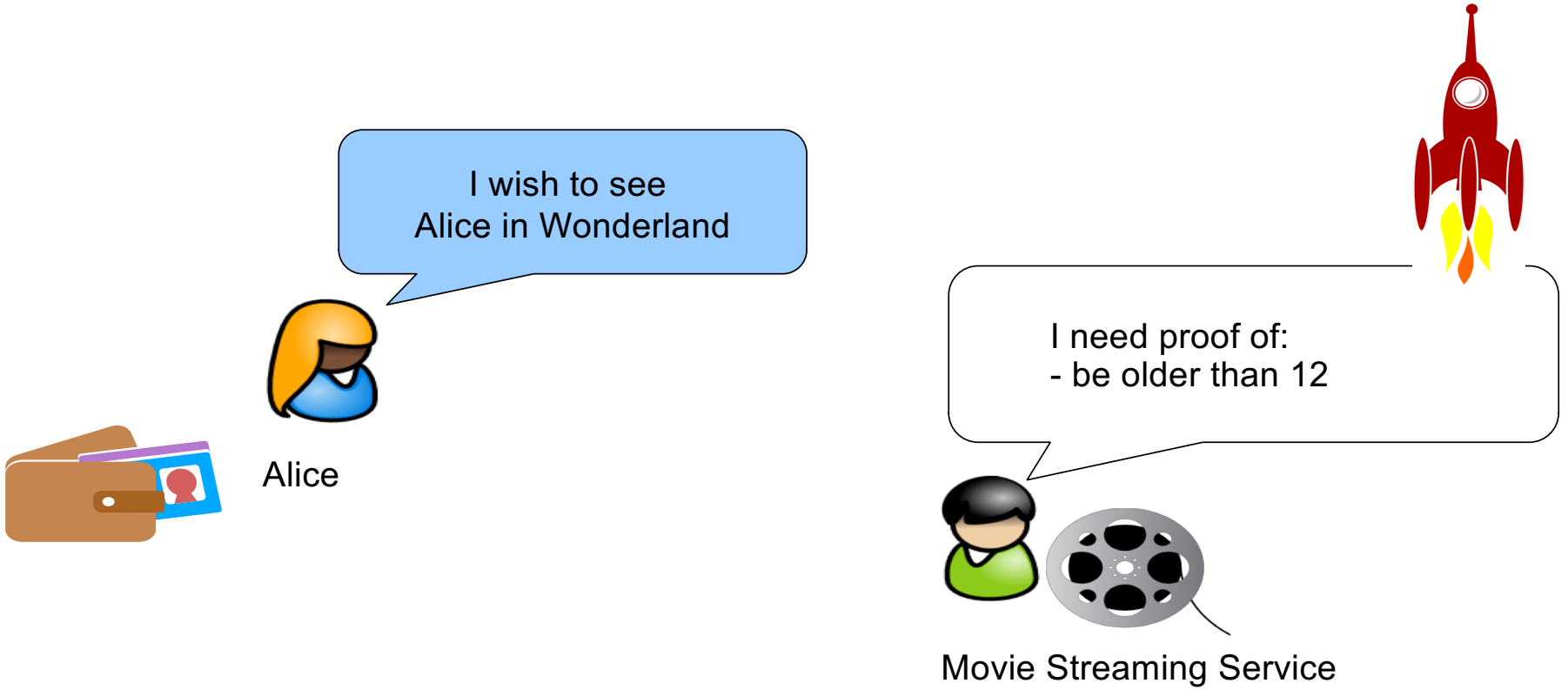
Like PKI, but better:

- Issuing a credential





Privacy-protecting authentication with Anonymous Credentials



Privacy-protecting authentication with Anonymous Credentials

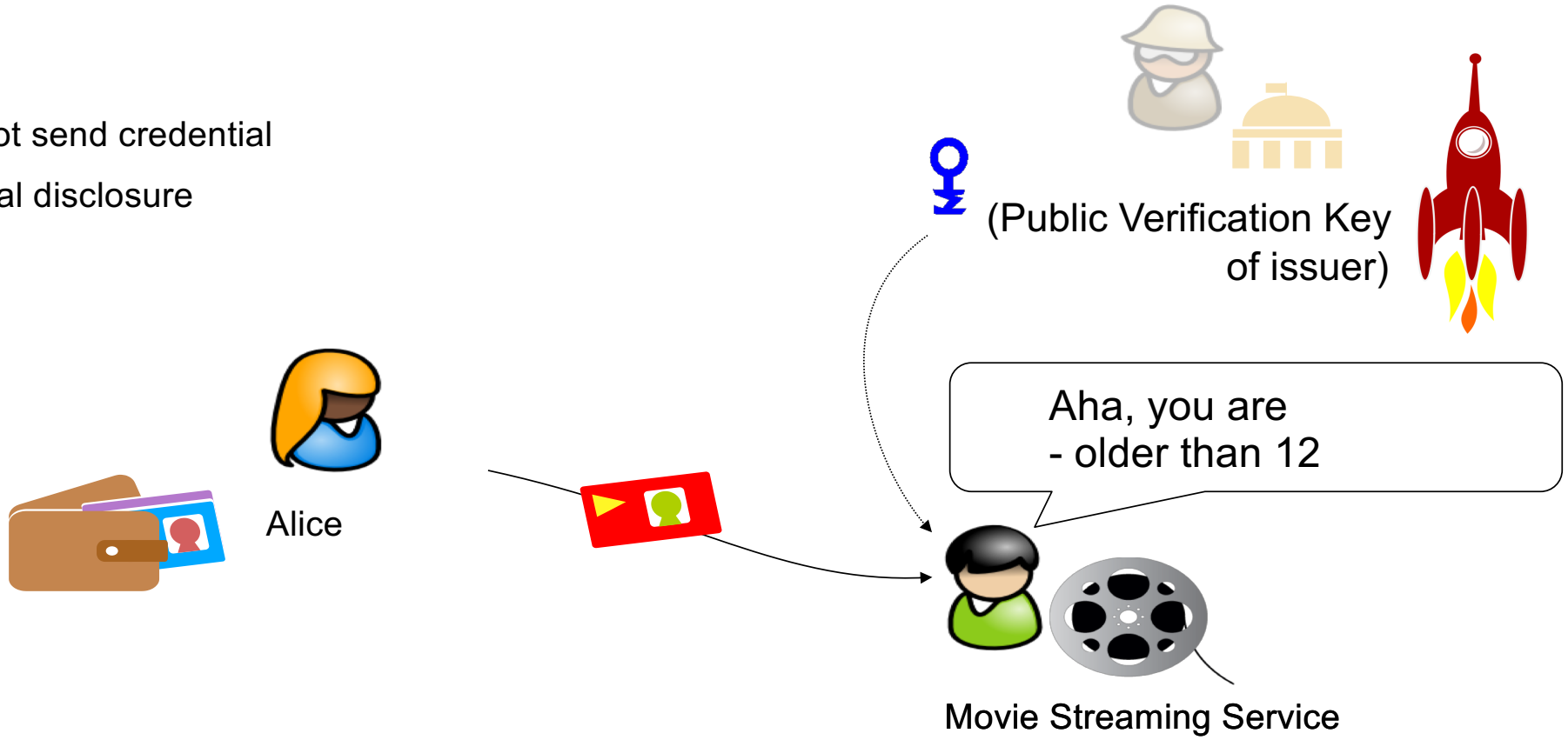
Like PKI

- but does not send credential
- only minimal disclosure

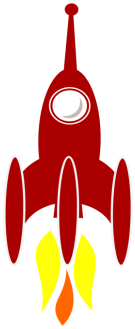
Privacy-protecting authentication with Anonymous Credentials

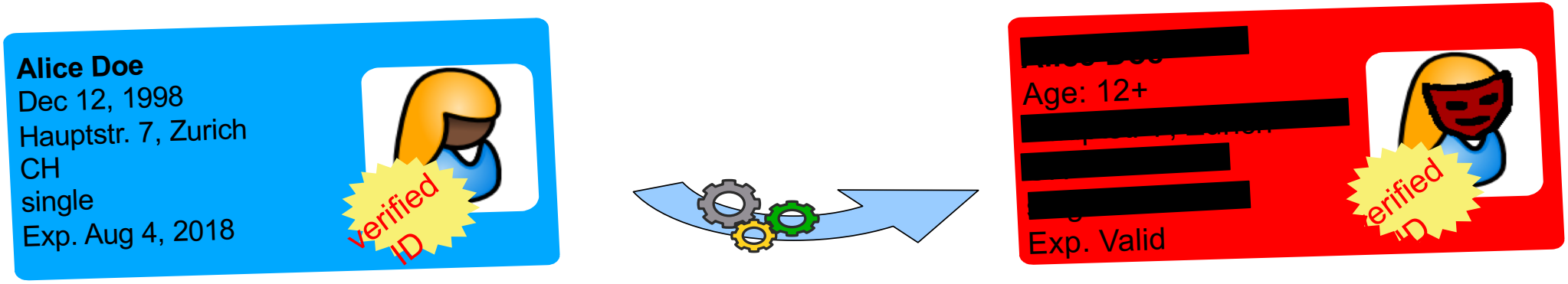
Like PKI

- but does not send credential
- only minimal disclosure

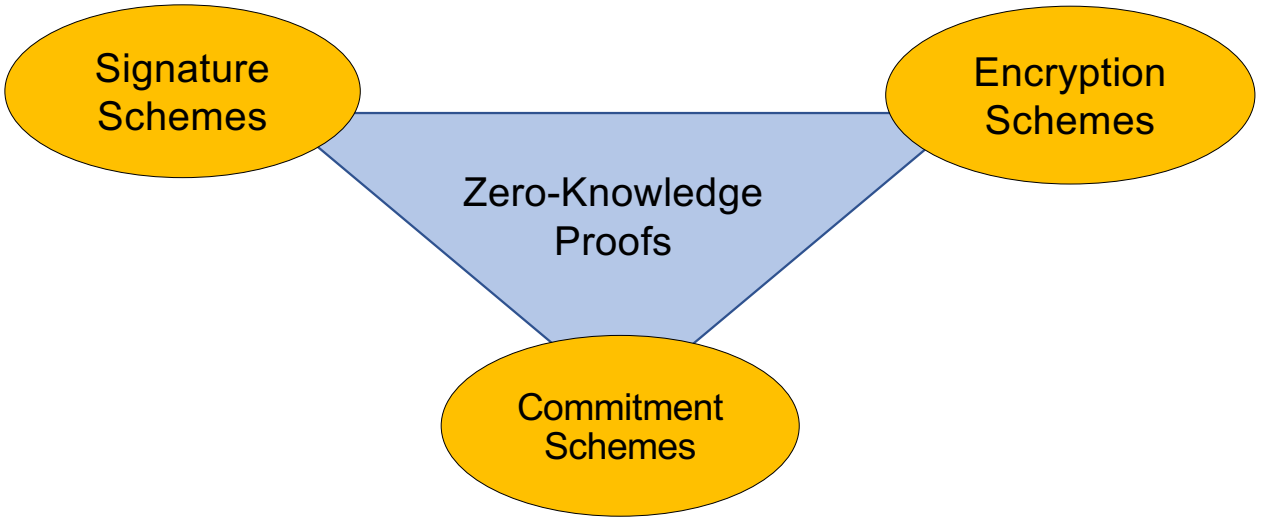


Proving Identity Claims: Minimal Disclosure with ZKP





Crypto toolbox

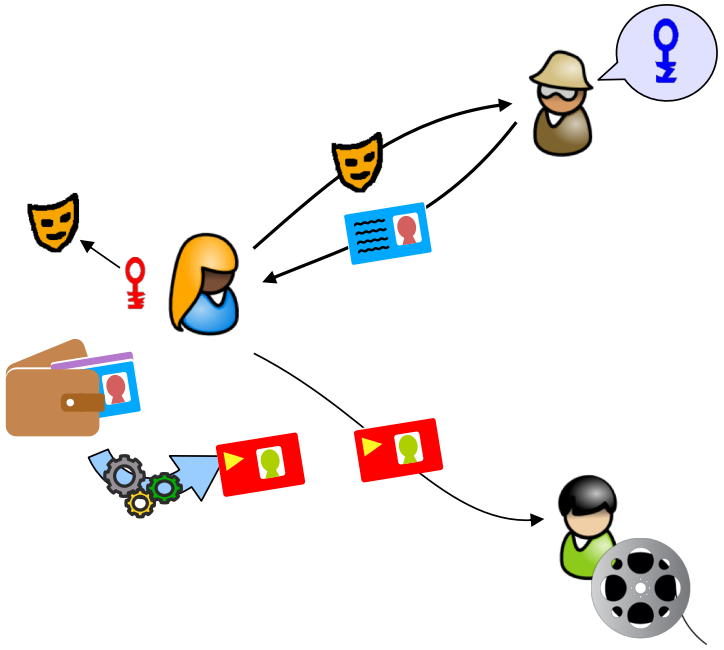


..... challenge is to do all this efficiently!

Why do we not have this today?

No ecosystem – PKI and standards:

- Public keys, revocation information
- Formats of credentials
- Formats of request



Here's where Blockchain comes in

- Hyperledger Indy / Sovrin

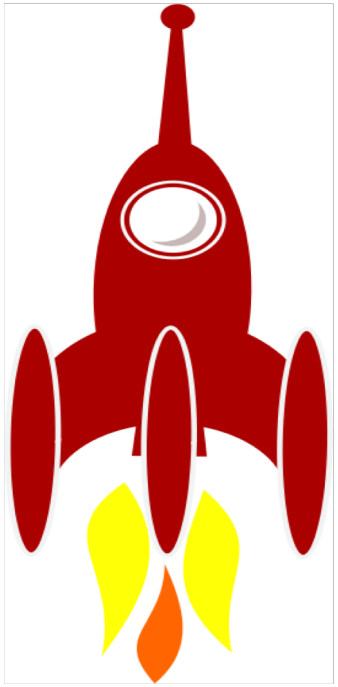
Conclusions

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
- Still lots of research needed nevertheless



Let’s do some rocket science!

@JanCamenisch jan@dfinity.org