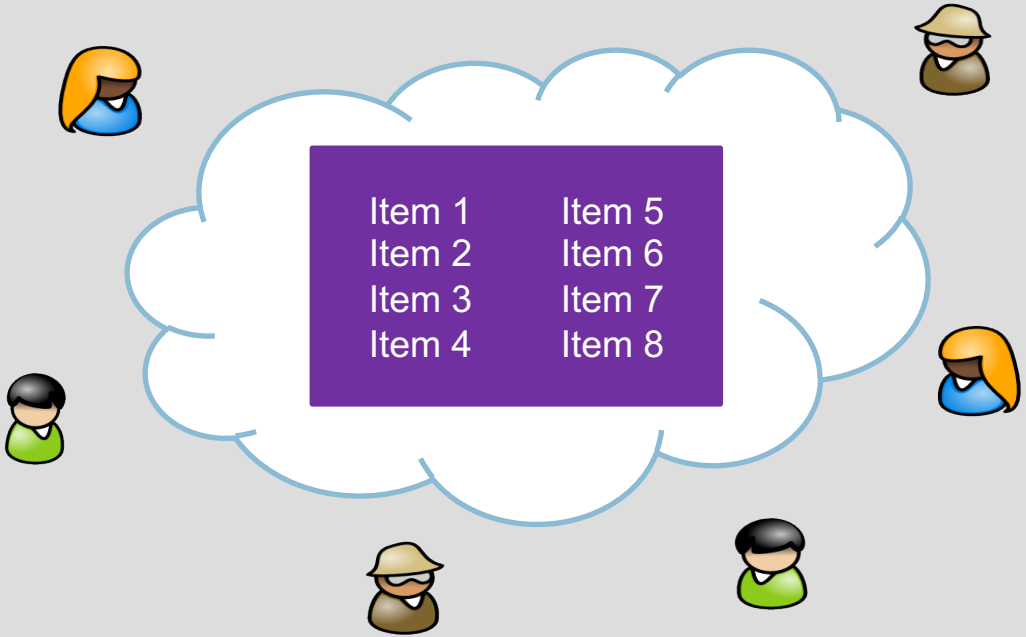
Cryptography in Crypto

Jan Camenisch
Head of Research

@janCamenisch jan.camenisch.org jan@dfinity.org

A *distributed* bulletin board



No trust in a single party, but in a majority, so less trust needed

Distributed Bulletin Board

Problem: Items are sent as input to (most) parties, but are received possibly in different order! Thus, parties need to agree on inputs and their order. How?

Millennial solution:

- Select a leader (lottery – interesting crypto problem!)
- Leader makes proposal
- Parties sign proposal if they agree with leader
- Full agreement if >1/2 (or >2/3) signatures
- If no agreement start over (no proposal or insufficient sigs)

Not quite solved:

- Might have to start over quite a few times, so not really practical
- Who are the parties who participate?
- Running a distributed protocol often very costly

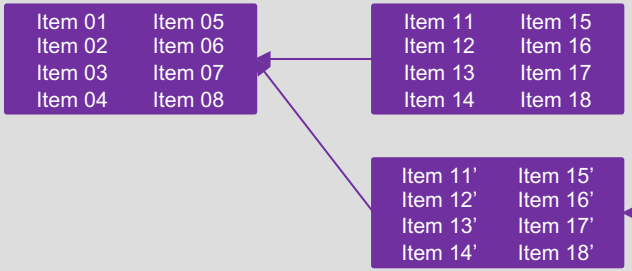
Blockchain solves this

1. Public lottery – determine who can participate
    1. Need to limit amounts of times single individual can participate
    2. Anyone with sufficient computational power is allowed to participate
    3. Find pre-image of hash-function for output with last x bits = 0

2. Combine lottery with authentication of proposal by winner – select leader:

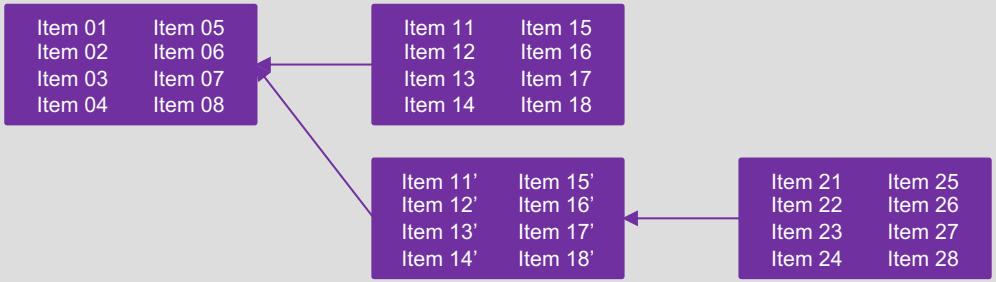
    Hash(item1, … , item8, random) = 0x****000000

3. Eventual agreement, i.e., allow temporary disagreement (forks)



- Two leaders made a proposal each
- Leader was malicious and made two proposals
- Rely on agreement being found at some point

Blockchain continued



Interesting crypto problems:

1. Prove the security of this construction (see literature for more)
    - what does it achieve?
    - under what assumptions?
    - under what adversarial models?

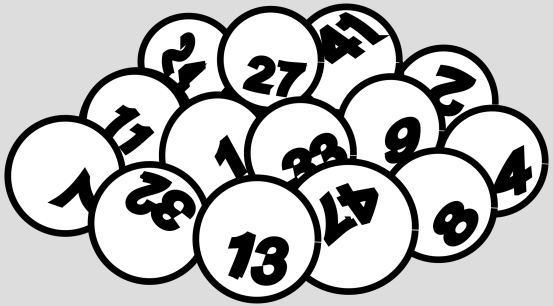
2. Huge drawback: uses way to much computational power, can we do better?

More Interesting Crypto Problems

How do we do a lottery?

Use a (pseudo) random function to select leader (i.e., list of ranked leaders):

a. Global random function (random beacon)
   - requires multi-party computation
   - leader is known to all, potentially vulnerable to adaptive attacks
   - only top ranked leaders need to act

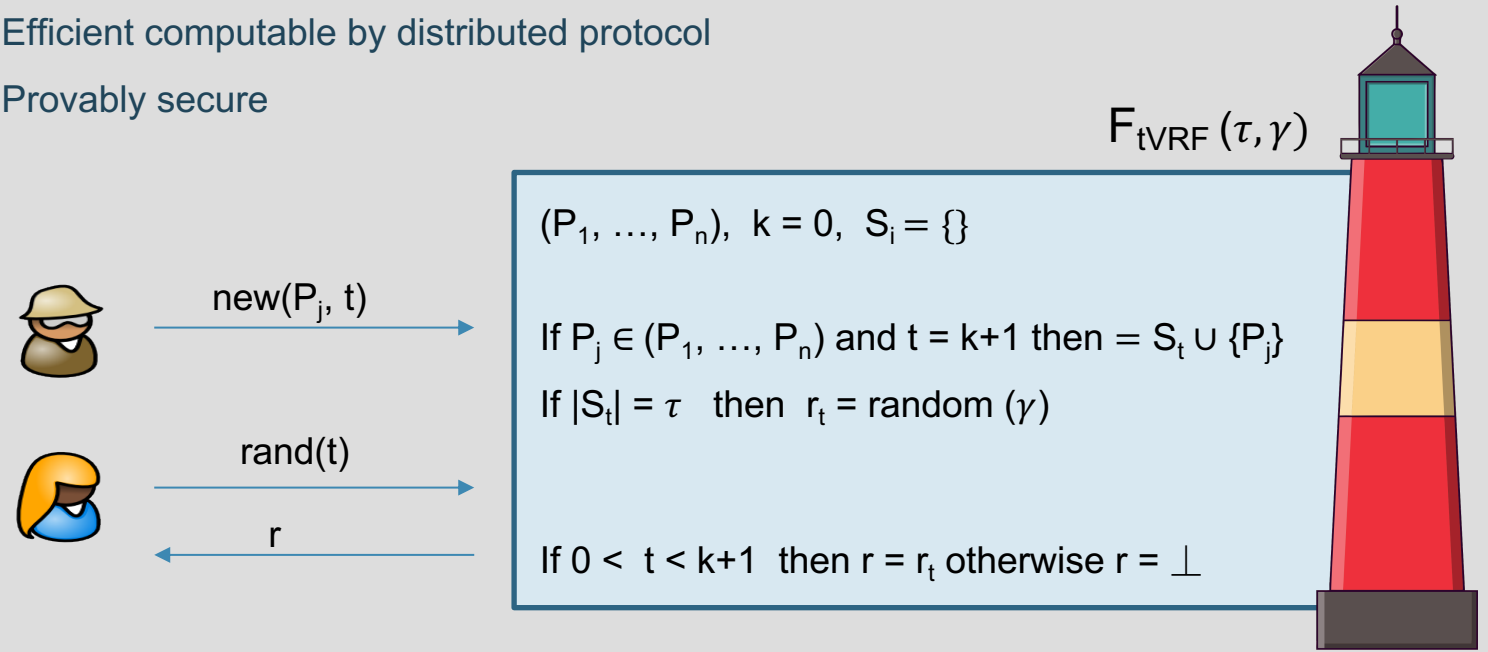


b. Local random function
   - parties need be able to prove they executed function correctly: VRF
   - leader only known, if all parties have announced their results
   - protects better against adaptive attacks

Global random function (random beacon)

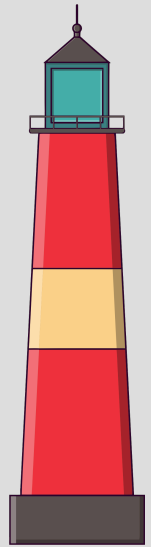
Requirements: threshold verifiable (pseudo)random function

- Regularly provide fresh pseudo random (as soon as >1/2 or >2/3 decide new period has started)
- Efficient computable by distributed protocol
- Provably secure



[Cachin, Kursawe, Shoup ’00,
Hanke, Movahedi, Williams ‘18]

Realization of random beacon



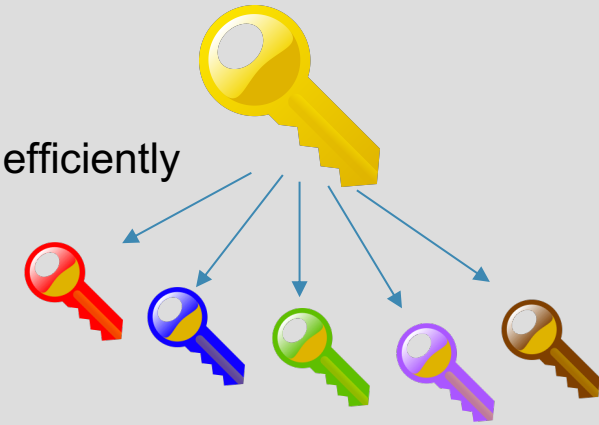
Idea: use *non-interactive & unique* threshold signature scheme

- $r_t = Hash(sig_x(time))$ is random in the random oracle model
- Signature scheme such that
  - with shared secret key $x \rightarrow x1, \ldots, xn$
  - Non-interactively reconstruct $sig_x(t)$ from $sig_{xi}(t)$
- Known candidates are RSA and BLS together with Shamir’s Secret Sharing

BLS : Secret key: random $x \in \mathbb{Z}_q$, Public key: $y = g^x$,

Signature: $sig_x(time) = Hash(time)^x = \Pi(Hash(time)^{xi})^{\lambda i}$

Distributed Key Generation for BLS



- Recall $y = g^x$
- Generate public key and secret key shares distributedly and efficiently
- Notice: Shamir's secret sharing is linear:
  - Let $p1()$ and $p2()$ share $s1$ and $s2$, respectively
  - Then $p() = p1()+ p2()$ shares $s = s1 + s2$
- Thus, we can implement DKG by
  - Set of dealers each sharing random value & use NIZK that they did this correctly
  - Agree on dealers with correct NIZK (using bulletin board ☺)
  - Locally sum up shares received from correct dealers
  - Works if at least one dealer is honest (although PK/SK could be biased)

Is this a secure construction?

Yes, secure, but actually non-trivial to prove!

Lots of building blocks are composed in the construction:

- Distributed generation of shares
- Proof of correct sharing via NIZKs
- Threshold version of a signature scheme
- Hash of signature to get randomness

Each property and building block needs to be properly defined

Need to show that they play together in a secure fashion!

- If overall scheme is not secure then one of the building blocks is not.

Provable Security – Why bother?

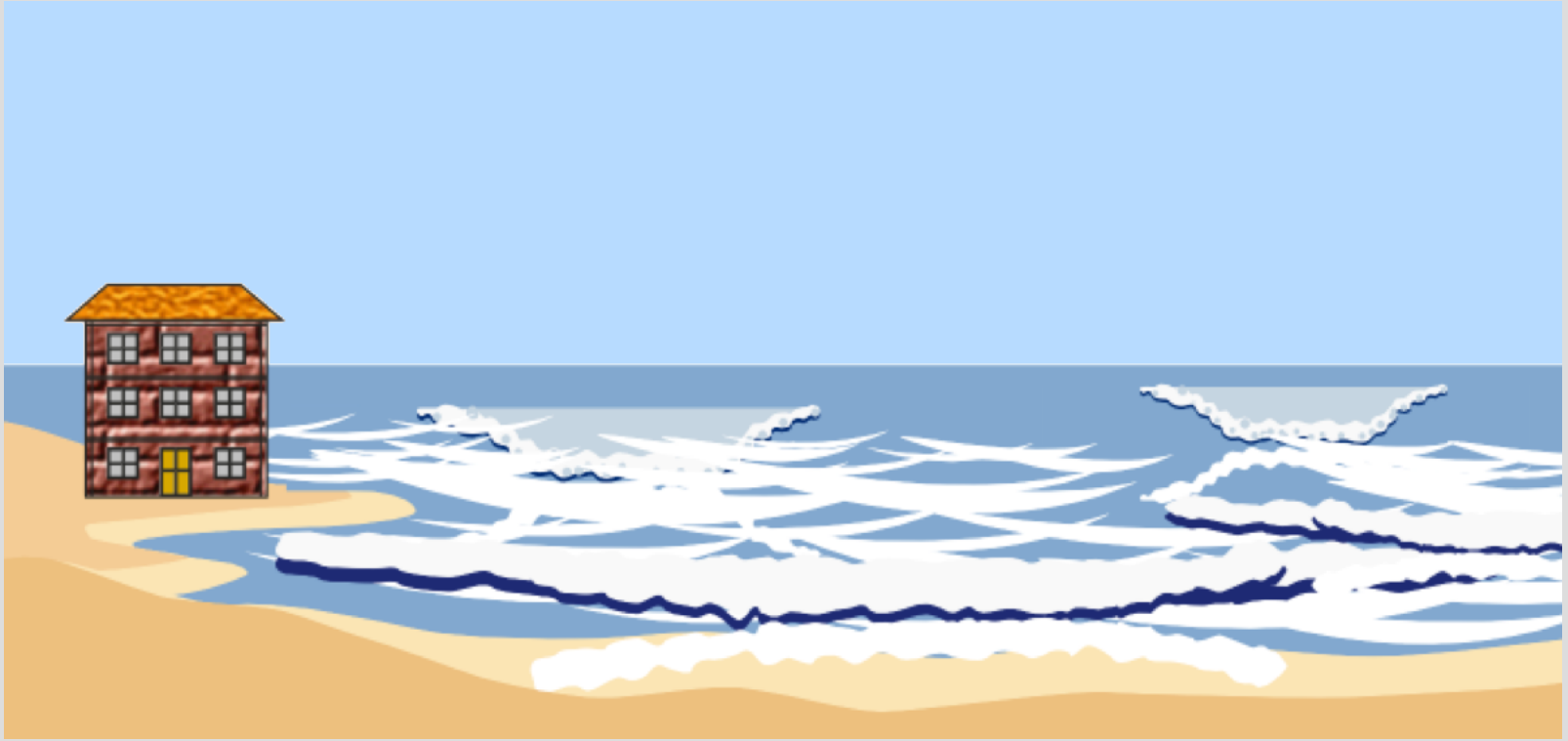
Cryptographic protocols w/out proper security analysis *do* get broken

- Bleichenbacher PKCS #1
- ISO Direct Anonymous Attestation, recent 5G attacks, …. no end here...
- Blockchains are an attractive target
  - Crypto was lost due to bad crypto, e.g., Zerocoin (370’000 coins out of thin air)
  - Bad protocol design in some cases (BitGrail $170M lost, etc)
  - Indy/Sovrin BLS multi-sigs: rolled out with rogue-key vulnerability enabling forgeries
- Many more (unknowingly) broken protocols out there,
  - Often not analysed b/c it does not payoff

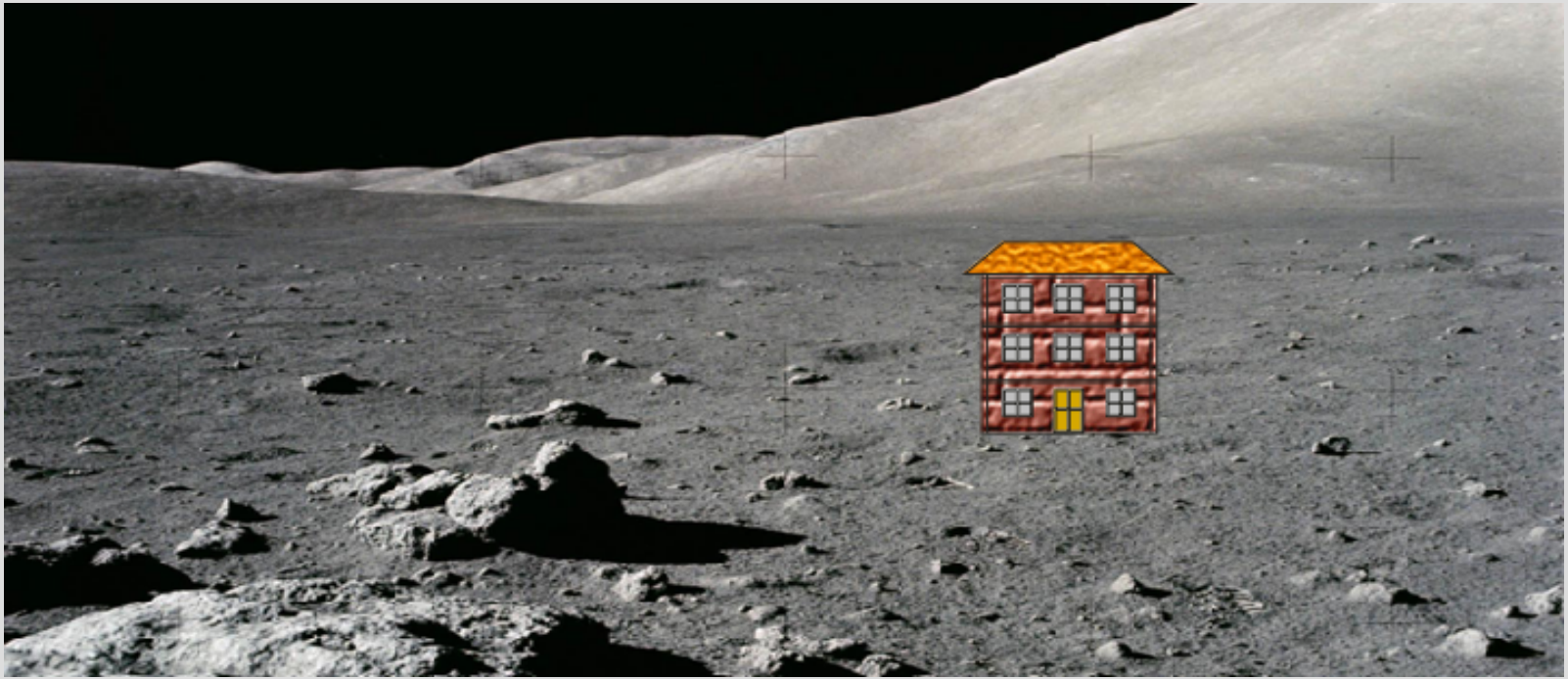
Why is security so hard?


Our world is turning into
cyberspace

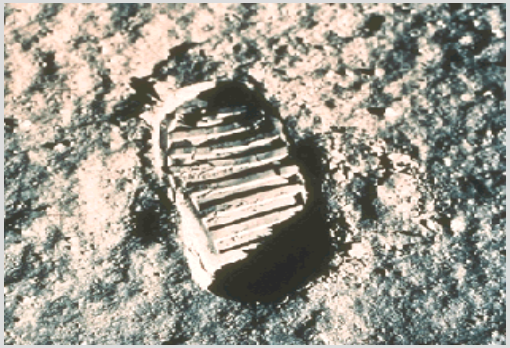
Still, we build apps thinking this



… 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

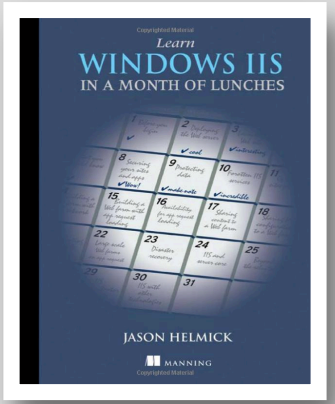
- Humans forget most things too quickly
- Paper collects dust in drawers

But that's how we design and build applications!

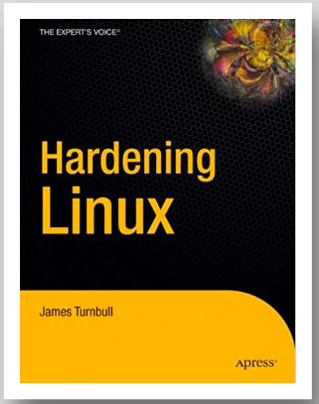
A cyberspace full of enemies

Today’s IT stack is too complex to make secure

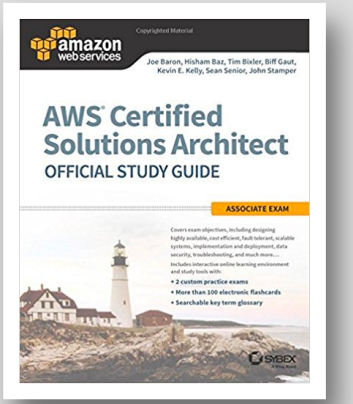
An insecure component, a misconfiguration, a bad line of code, and… hackers can get in!



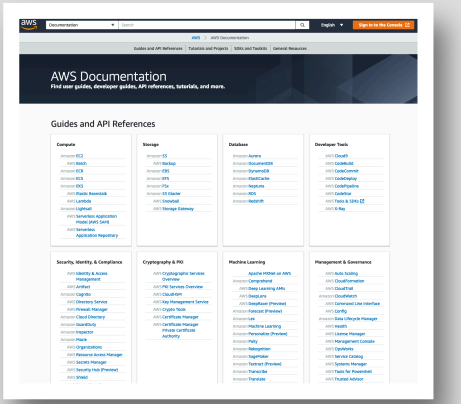
372
PAGES



584
PAGES



437
PAGES



Over 100K
PAGES

Don’t believe in data hungry aliens?

Marriott
350 million (2018)

EQUIFAX
143 million (2017)

AdultFriendFinder
412 million (2016)

Anthem.
78 million (2015)

ebay
145 million (2014)

JPMorgan Chase & Co.
76 million (2014)

THE HOME DEPOT
56 million (2014)

YAHOO!
3 billion (2013)

TARGET
110 million (2013)

United States Office of Personnel Management
22 million (2012)

PlayStation
77 million (2011)

RSA
40 million (2011)

Crypto means cryptography….

Secure asset transfer system

Crypto means cryptography…

Secure asset transfer

Crypto means cryptography…

Secure smart contract

Secure asset transfer

Crypto means cryptography…

DFINITY

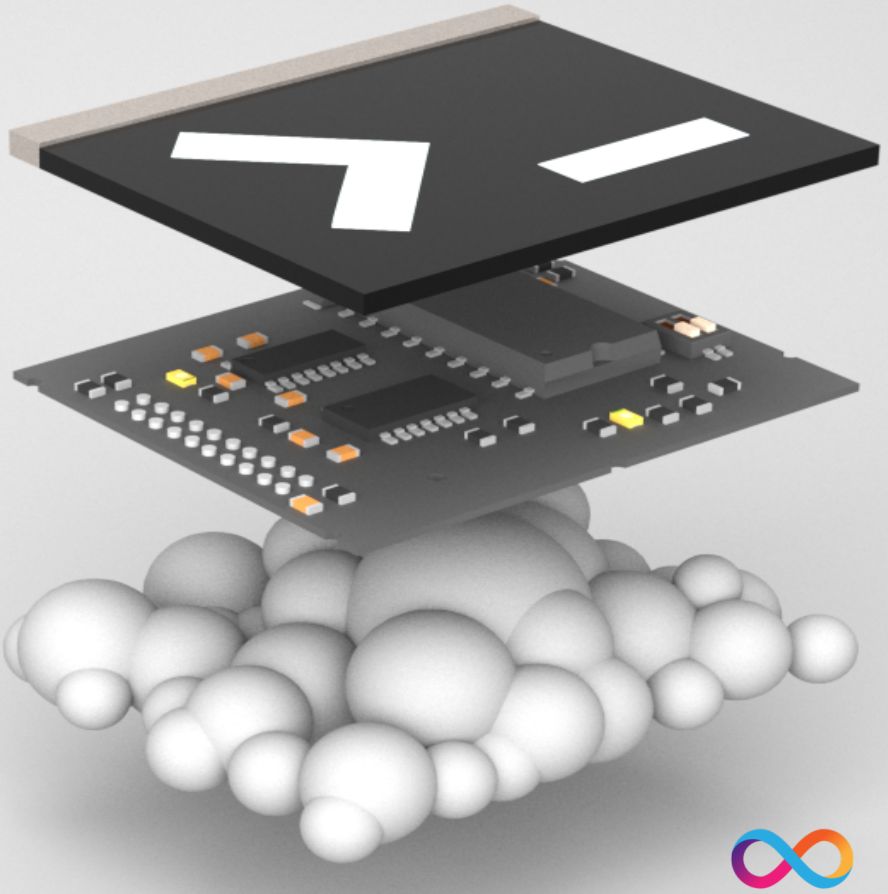
Secure Internet computer

ethereum

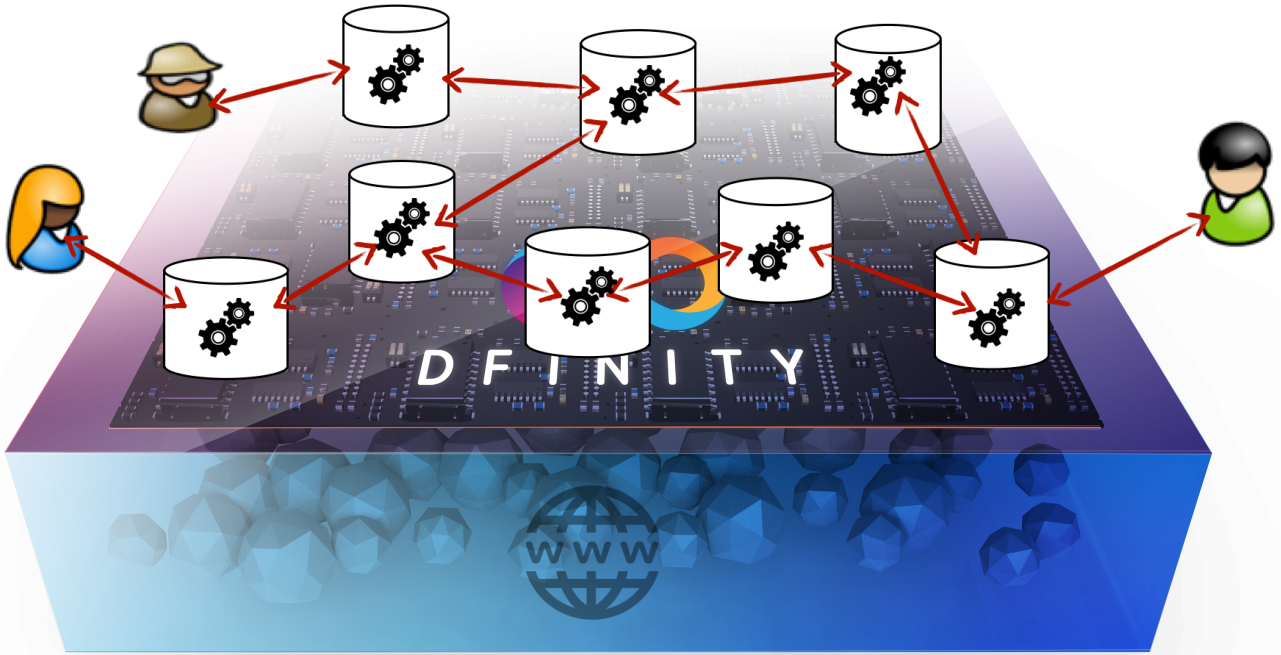
Secure smart contract

bitcoin

Secure asset transfer



The ICP protocol will create a thick Internet & a serverless cloud



The Internet will become a distributed OS that also hosts and runs software and services

New “open internet services” will eliminate platform risk

Open internet services, and shared pan-industry business protocols, will become part of the Internet itself

Conclusions

Cyberspace is not earth as we know it

Crypto protocols can make it secure!

Provable security matters - and very hard!

Tons of research needed

DFINITY

Let’s do some rocket science!

@janCamenisch jan.camenisch.org jan@dfinity.org