NOKIA Bell Labs

IoT Security Challenges & Opportunities

Erez Waisbard

Haifa 3rd Security Research Seminar

December 2016

NOKIA Bell Labs

A Tale of IoT

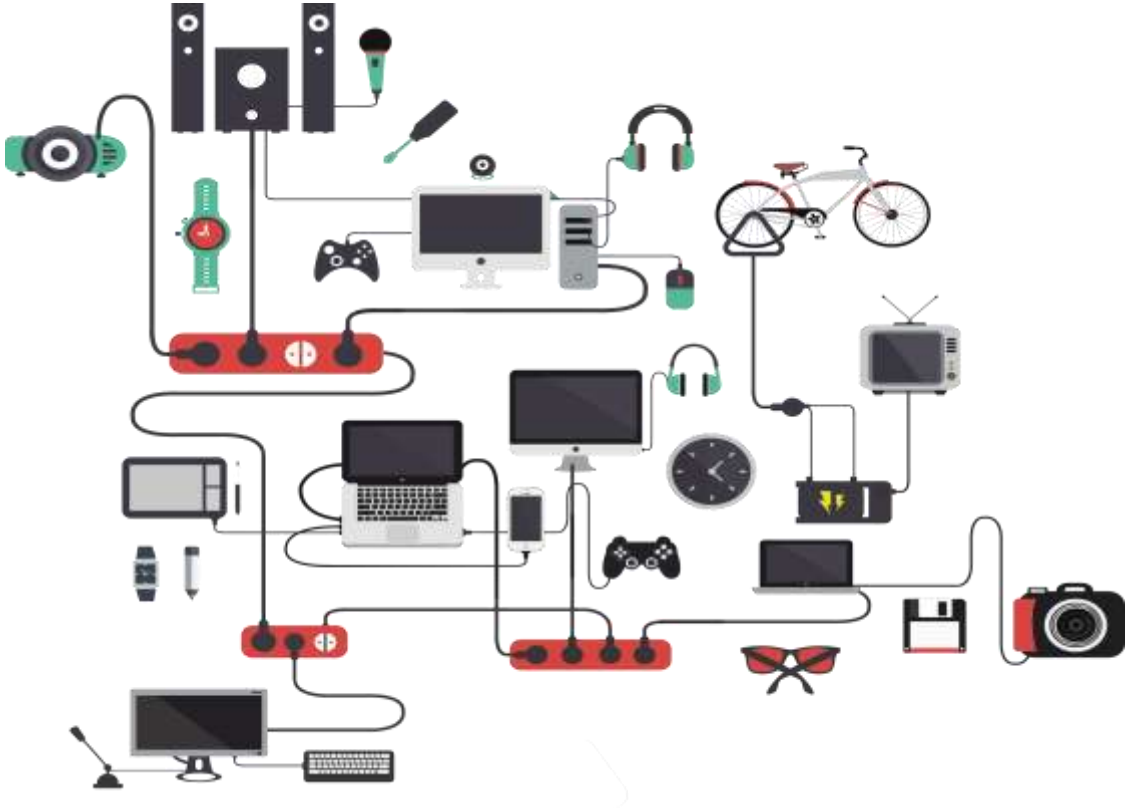
A Tale of IoT
Smart Refrigerator

No Milk

Interconnecting different devices from different vendors

NOKIA Bell Labs

A Tale of IoT
Ideal world



Secure Intercommunication

A Tale of IoT
The real world

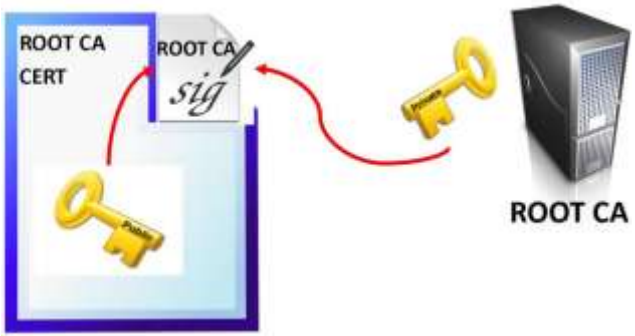
Tower of Babel

No Intercommunication

NOKIA Bell Labs

The Security Model

Security Model
The Internet model

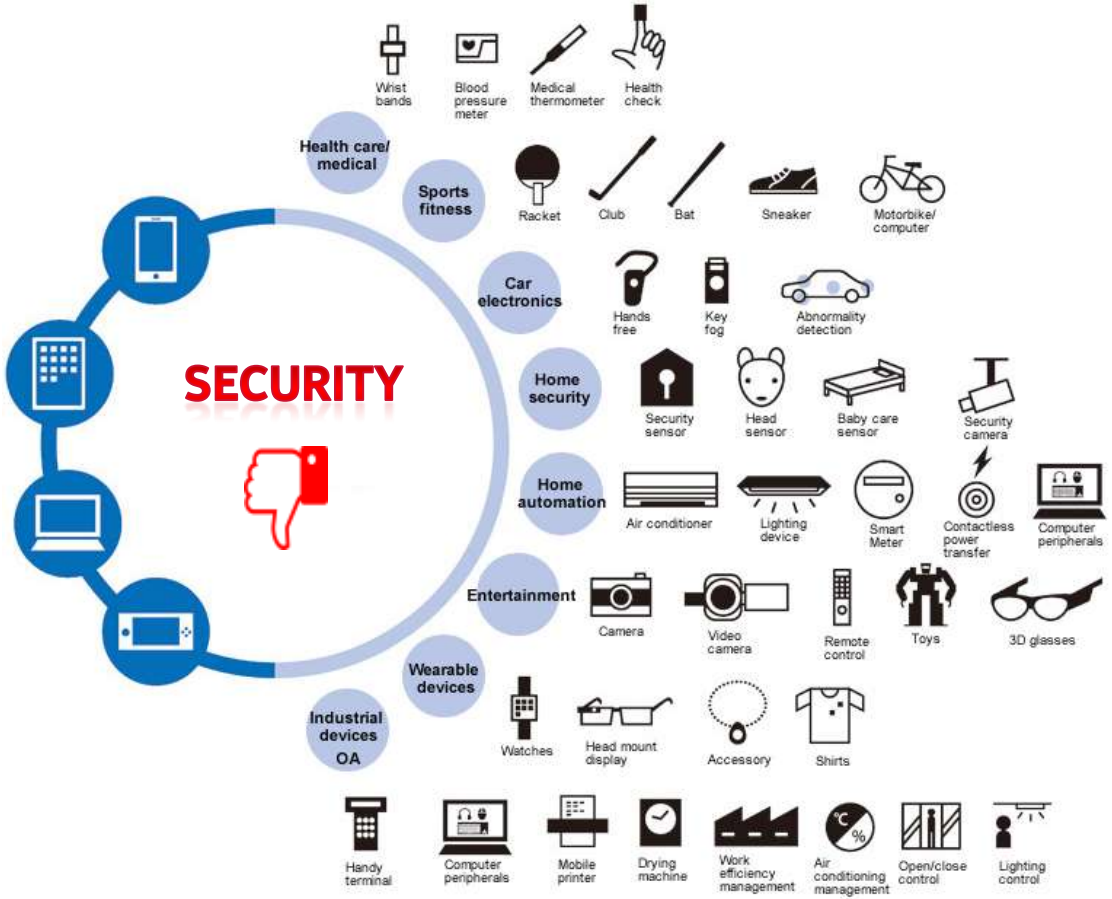


© Leo Blanchette * www.ClipartOf.com/17596

Trust relies on Root CA and public key cryptography

Security Model
IoT devices security

- NO SECURE STORAGE
- NO PROCESSING POWER FOR PKI
- NO SECURITY PATCHES



IoT Devices are not secure

NOKIA Bell Labs

Security Model
IoT devices security

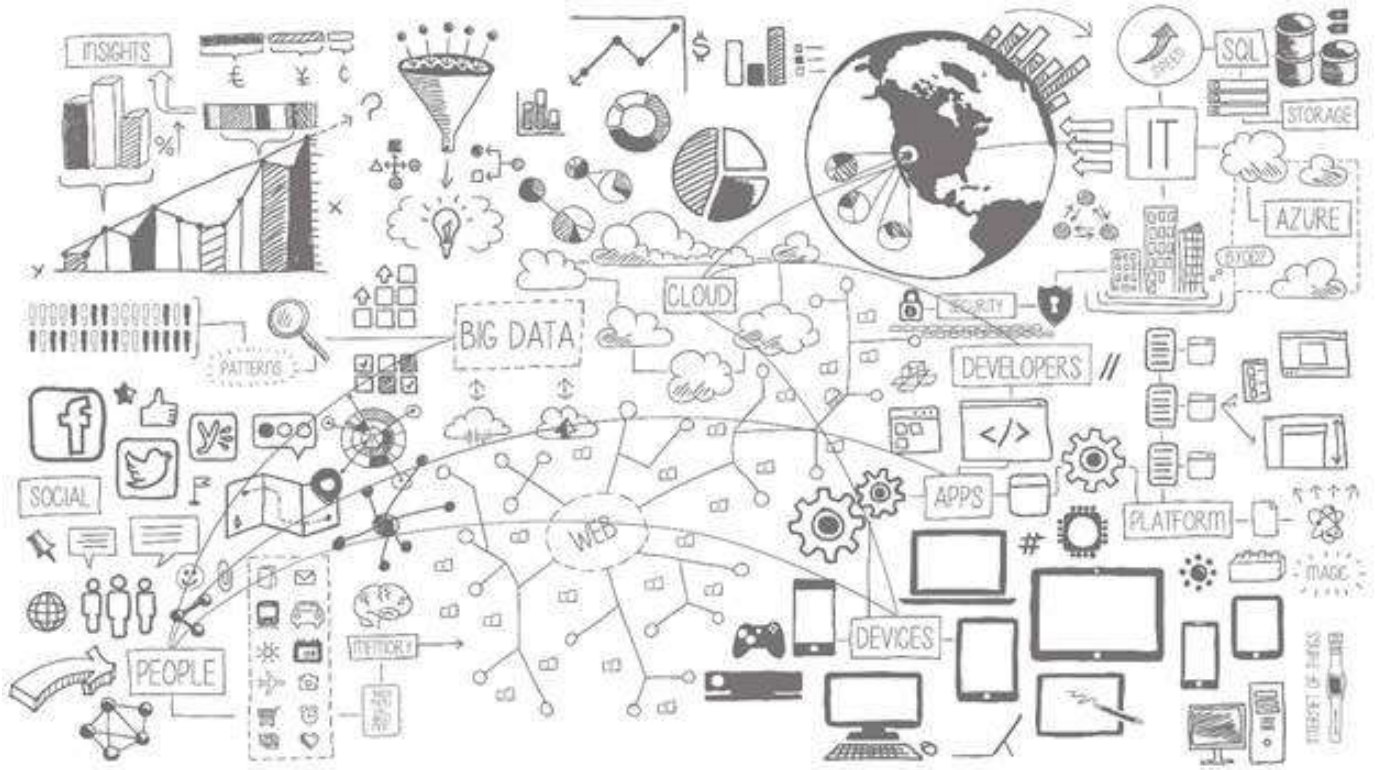
We’re at a crisis point now with regard to the security of embedded systems, where computing is embedded into the hardware itself — as with the Internet of Things.

Bruce Schneier, Jan, 2014

IoT Devices are not secure

Security Model
The IoT model

- No central Trusted Authority
- Multiple vendors
- Multiple service providers
- Multiple Protocols
- Low power unprotected devices



PKI is not suited for IoT

NOKIA Bell Labs

NOKIA Bell Labs

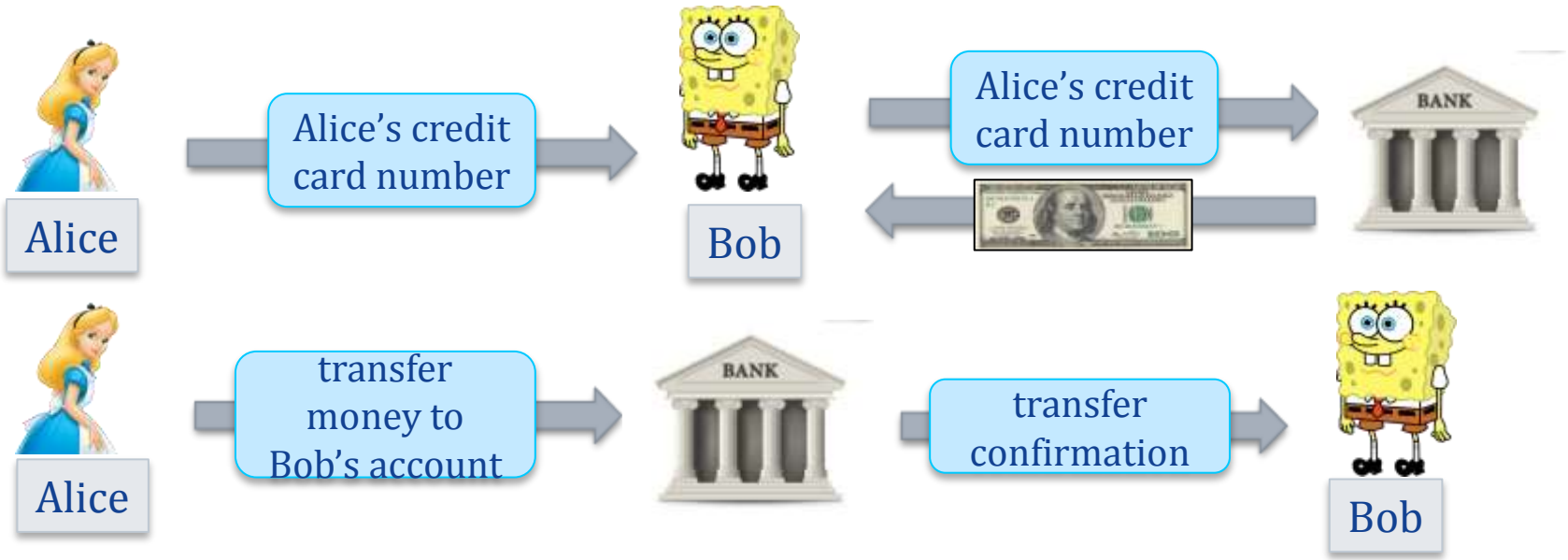
The Blockchain Technology

Bitcoin [October 2008]

Popularity

Ransomeware & Darknet

Digital Payment before Bitcoin (using banks)



Relies on a central trusted entity

No digital cash

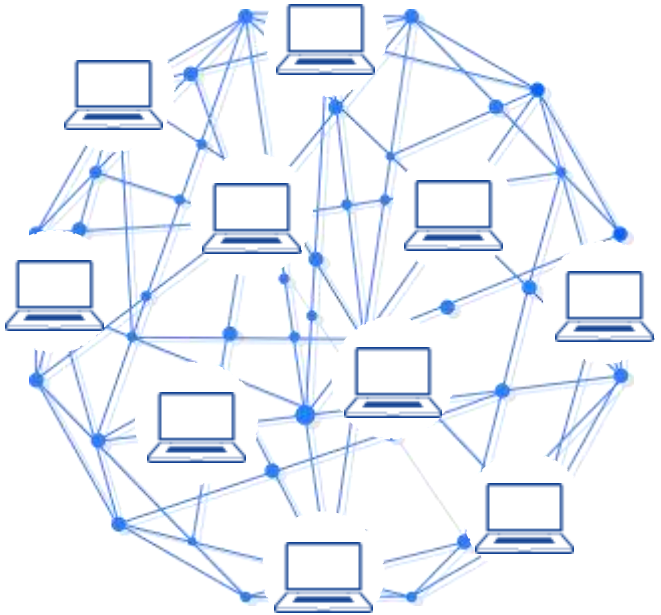
Replacing the bank with a bulletin board

- PUBLIC (TRUSTED) BULLETIN-BOARD
- EACH TRANSACTION IS RECORDED

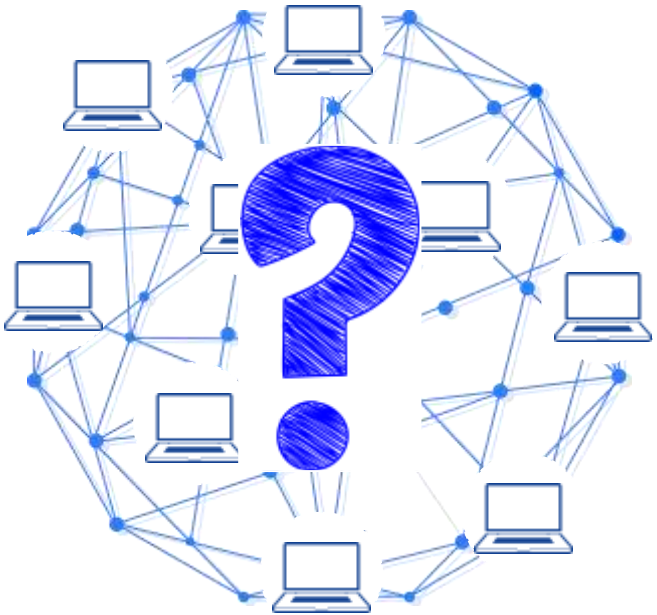
User $\mathbf{P_1}$ transfers a coin #16fa35afc6831 to user $\mathbf{P_2}$

Distributed Bulletin-Board

- BROADCASTING TRANSACTIONS
- DECISION BASED ON HONEST CONSENSUS



Blockchain Technology
Problem Definition

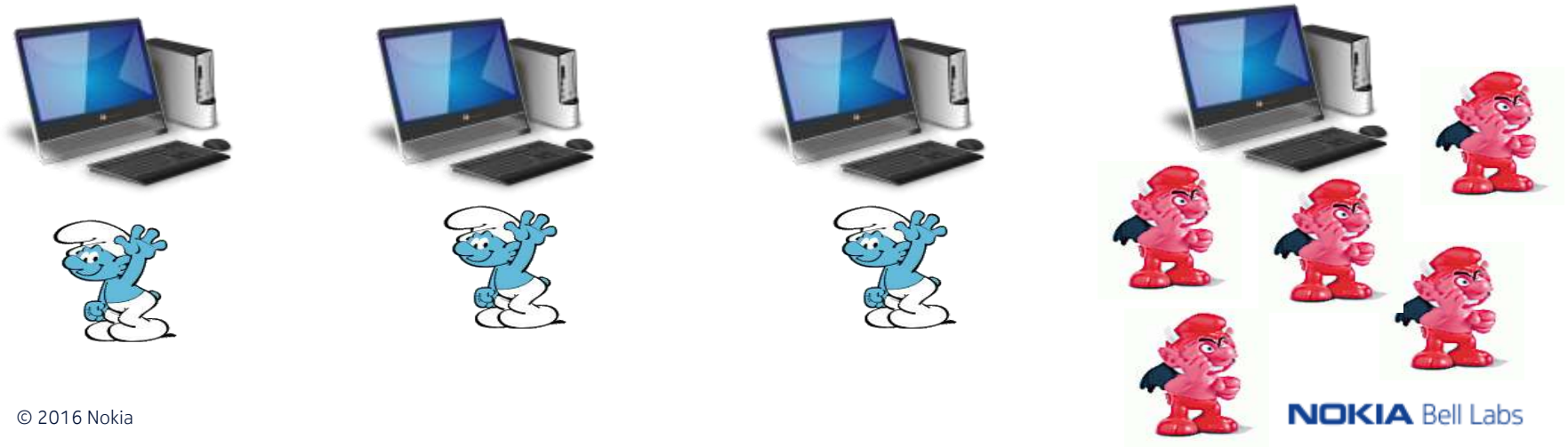


MAIN ISSUES

1. NO NOTION OF GLOBAL TIME
2. PEERS MIGHT CRASH
3. PEERS MIGHT TURN MALICIOUS
4. VOTING DOES NOT WORK

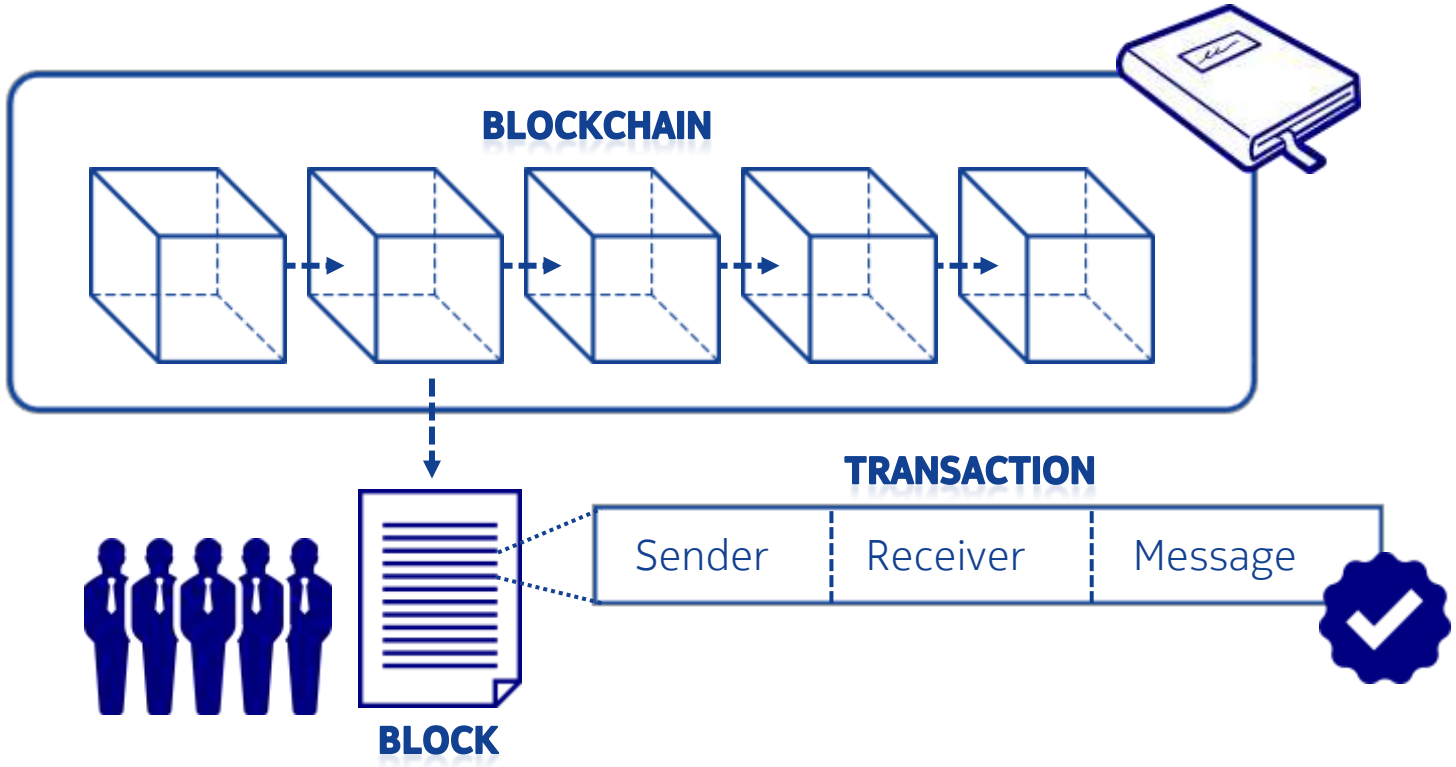
The Bitcoin solution

Majority of computing power instead of majority of parties

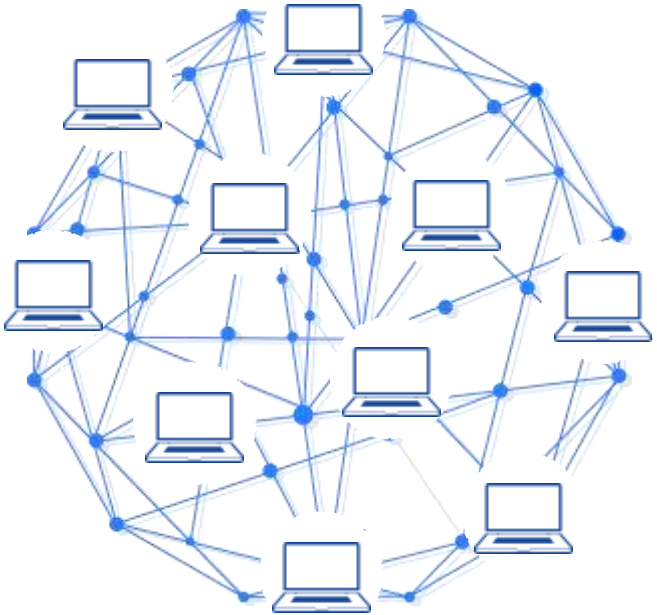


NOKIA Bell Labs

What is a blockchain?



Blockchain Technology
Open Challenges



PRIVACY

- TRANSACTIONS LINKED TO REAL IDENTITIES
- ONE GLOBAL CHAIN

SECURITY

- DENIAL OF SERVICE (TRANSACTION FLOOD)
- ECLIPSE ATTACK

SCALABILITY

- BROADCAST BASED
- PROOF OF WORK BASED

Blockchain Applications (beyond BitCoin)

Anti-Counterfeit

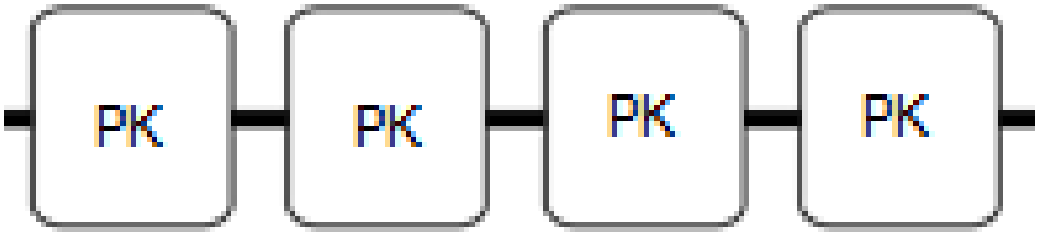
- Each product is labeled with a block verified tag.
- Verified supply chain
- Consumer activation and validation

Notary

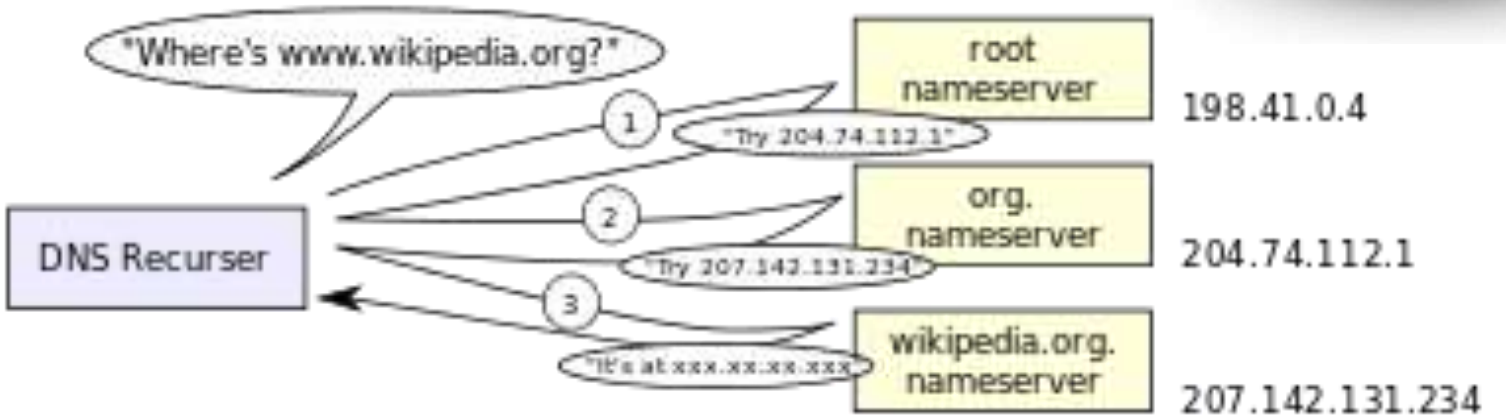
- Proofs of:
  - Ownership
  - Integrity

- Privacy preserved using cryptographic hash functions

Distributed CA



Secure DNS

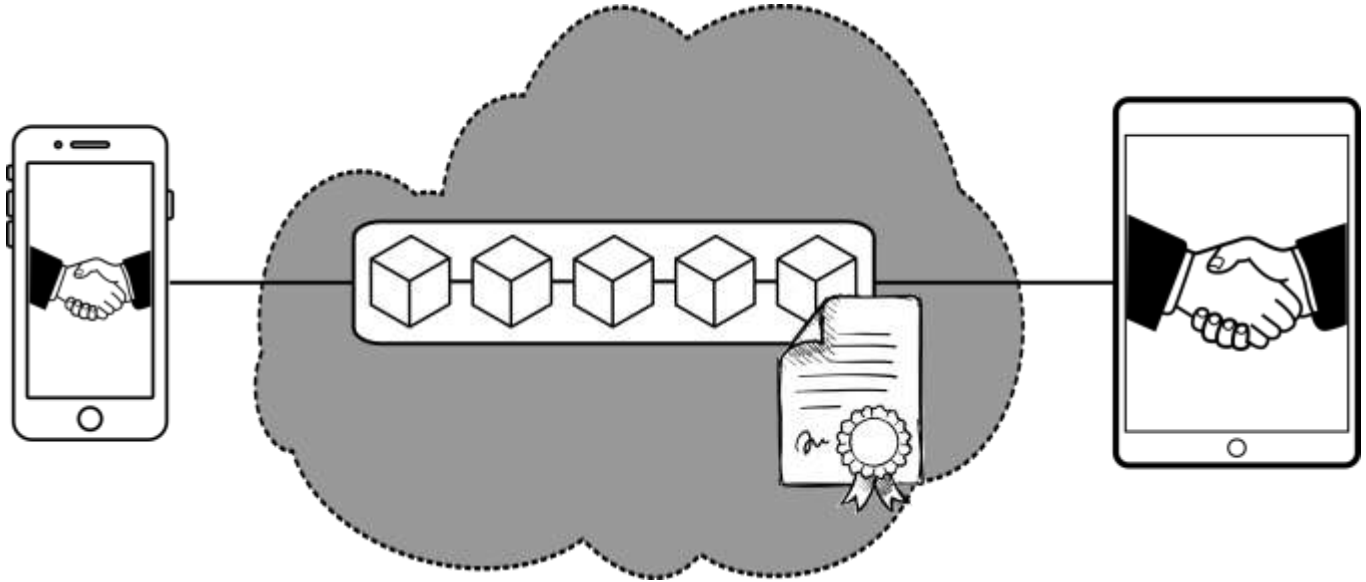


Distributed web hosting

NOKIA Bell Labs

Research Tracks
Bell-Labs

Research Track : Trust in IoT



NOKIA