Blockchains for Trusted IoT

Didier Donsez, Vivien Quéma
Univ. Grenoble Alpes
LIG

Outline

- Blockchain : a short state-of-the art
- Blockchain : IoT use cases
- Our work on Blockchains

Blockchain: a short state-of-the-art

What is a Blockchain?

- Append-only Distributed Database...
  - Irrevocable
  - Trustless (or not)

- ... in which transactions (or anything else) can be stored

- Main metrics
  - Throughput
  - Latency
  - Cost

- This is also called “Distributed Ledger Technology” (DLT)

Some Blockchains...

- Bitcoin 
- Ethereum 
- Hyperledger 

Blockchain use cases

Financial

- Trade Finance
- Cross currency payments
- Mortgages

Public Sector

- Asset Registration
- Citizen Identity
- Medical records
- Medicine supply chain

Retail

- Supply chain
- Loyalty programs
- Information sharing (supplier – retailer)

Insurance

- Claims processing
- Risk provenance
- Asset usage history
- Claims file

Manufacturing

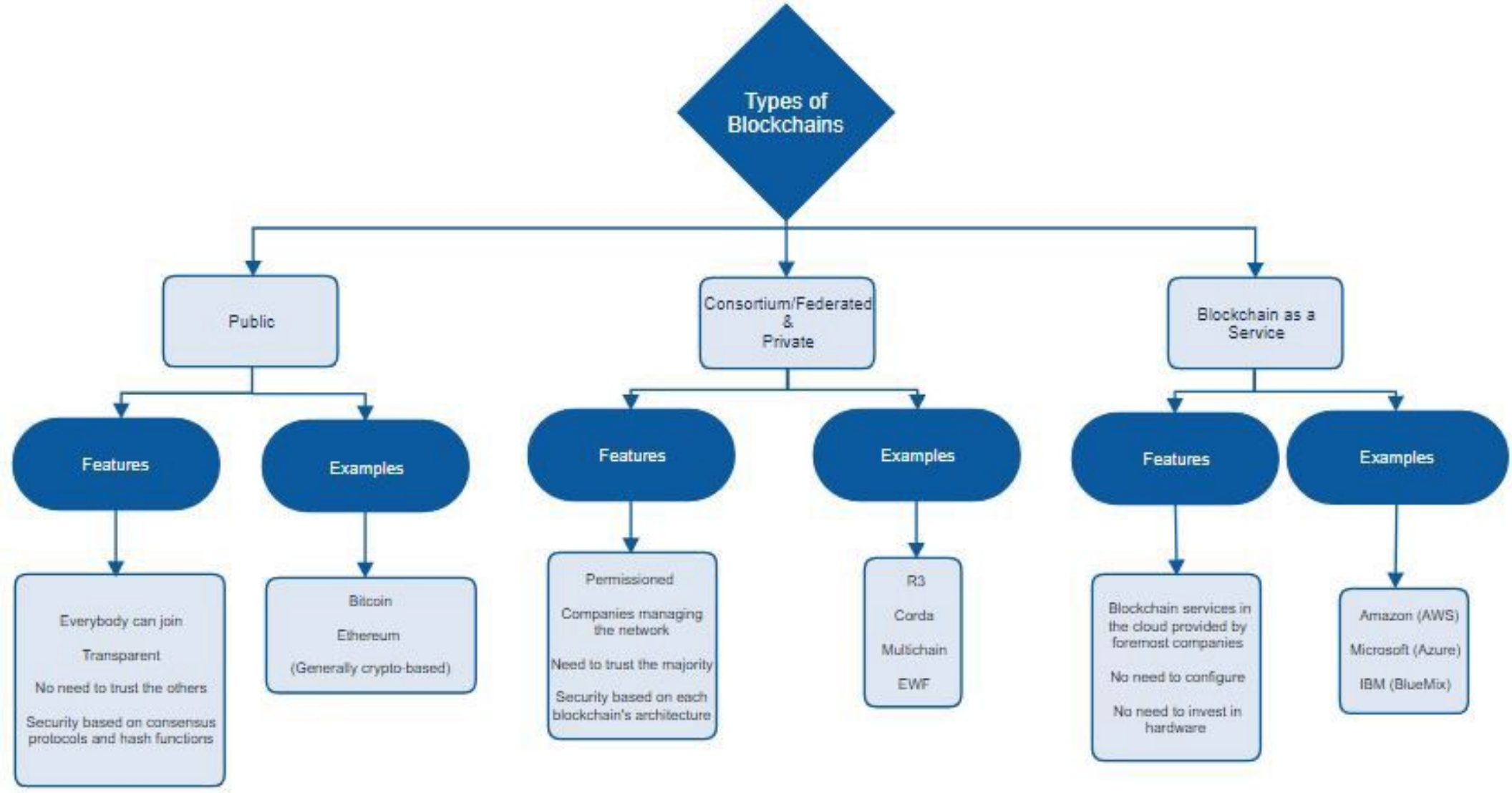
- Supply chain
- Product parts
- Maintenance tracking

https://www-05.ibm.com/hr/watson-see-summit/assets/files/IBM_RD_perspective-_innovation_is_what_makes_the_difference_-_Dr_Marko_Vukolic_IBM_Research.pdf

The many faces of Blockchains (1/2)

- Public blockchain
- Consortium/Federated blockchain
- Private blockchain
- Blockchain-as-a-Service

The many faces of Blockchains (2/2)



credit : M.A. Lopez

5 factors to choose the right Blockchain

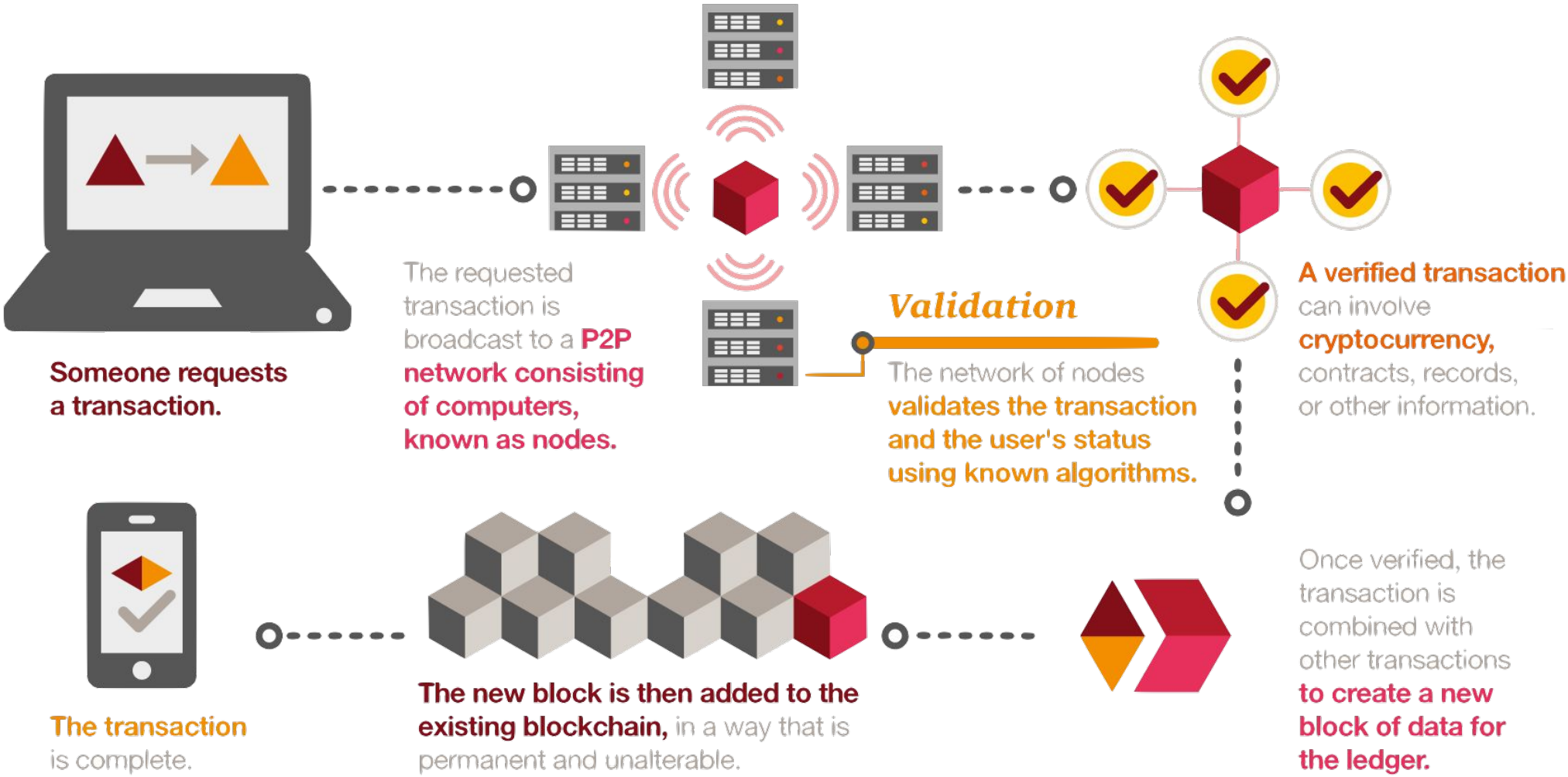
Five Factors in Determining a Good Business Case With DLTs

Source: Aite Group

Throughput	Latency	Node scalability	Security	Cost
Volume of transactions the DLT is able to process (tps) • Bitcoin protocol has an extremely low throughput of 7 tps • Many DLTs have made significant progress on throughput, ranging from 500 tps to 5,000 tps	How long the DLT takes to confirm and commit each transaction • Bitcoin protocol takes 10 minutes on average to validate transactions • Private DLTs running on a consensus algorithm without mining can provide subsecond latency levels	How many nodes the DLT supports without compromising performance • Bitcoin protocol is the most scalable DLT in number of validation nodes •Private DLTs provide sufficient client-node scalability but with limited validation-node scalability	How resilient the DLT system is to various security threats •The security aspects are fundamentally impacted by the consensus algorithms -Client onboarding -Digital signatures -Network attacks -Data privacy -Governance control -Legal enforcement	How much it costs to build and run a DLT system •Running cost: Cost per confirmed transactions (CPCT) •Building cost: capital investment in hardware and equipment, software development and licensing, and IT staffing

https://www.aitegroup.com/report/building-business-cases-distributed-ledger-technology-things-know

How does a Blockchain work?

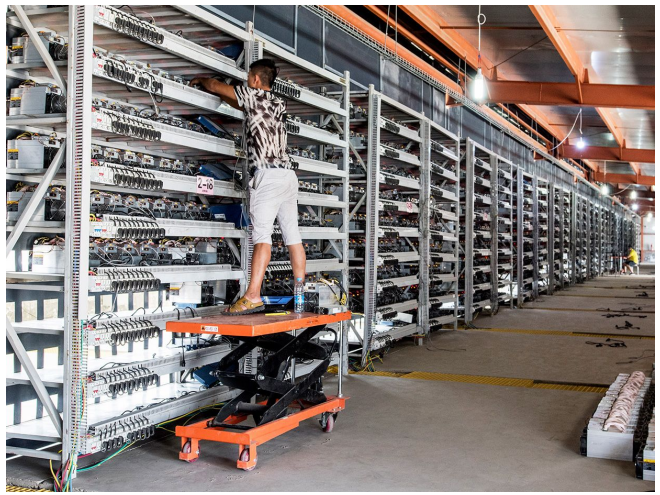


© PWC/ how Blockchain works

How does a Blockchain work?

Permissionless validation (Proof of Work)

- Everyone (Miner) can participate to the validation
  - Slow (and huge amont of electricity)
  - Scalability



Bitmain. credit Stephen Chow

Permissioned validation (Byzantine consensus)

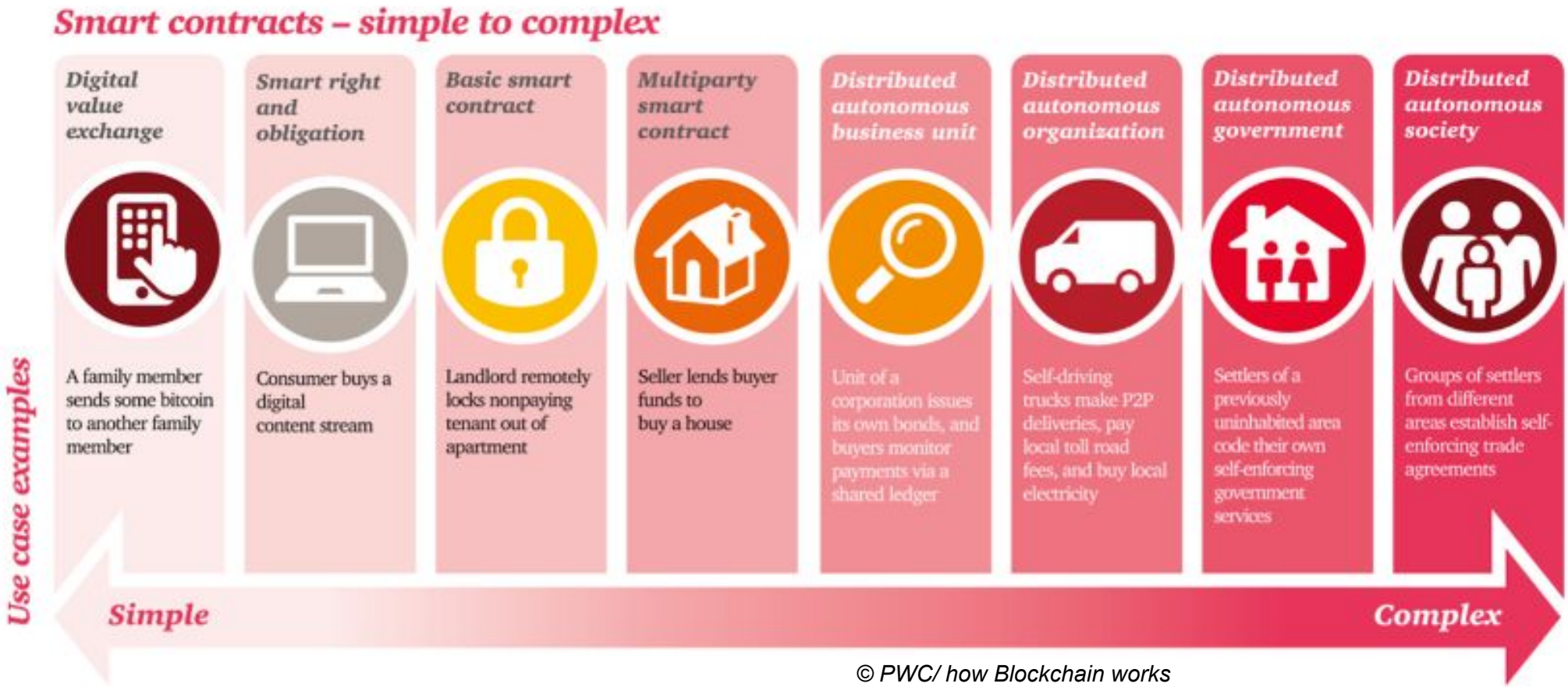
- Only authenticated and permissioned validators participate to the validation
  - Fast
  - Limited scalability

A word on Smart Contracts

- Program (Turing Complete) executing the terms of a contract between 2 or more participants
  - *Same as a Stored Procedure in SQL Databases.*
  - Basic contract : exchange X assets A (owned by Alice) for Y assets B (owned by Bob).
  - Assets: money (ether), token, kW, km, man-hour, weather forecast, licence key, property title ...

- Smart Contract Execution
  - Replicated State Machine
    - on several computing nodes
  - New state recorded in the Distributed Ledger.

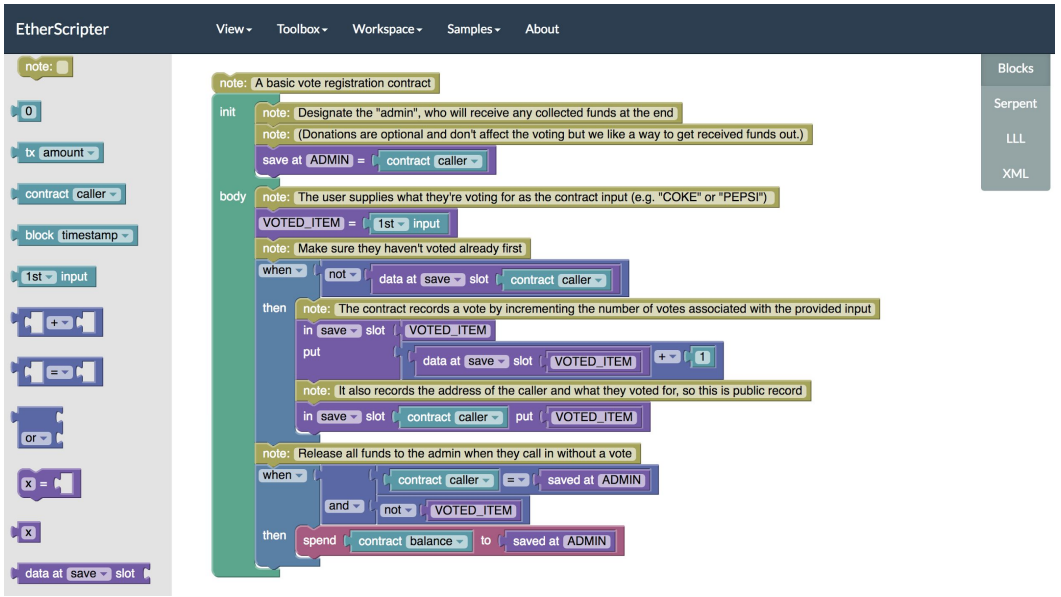
Smart Contracts : simple to complex



© PWC/ how Blockchain works

Smart Contracts platforms

- Ethereum Smart Contracts
  - Ethereum Virtual Machine (EVM)
  - Serpent (Python), Solidity (Node) ...
  - EtherScripter



Example : Vote registry with EtherScripter

- Hyperledger Chaincodes
  - Go, Java

Blockchain: IoT use cases

IoT reference architecture

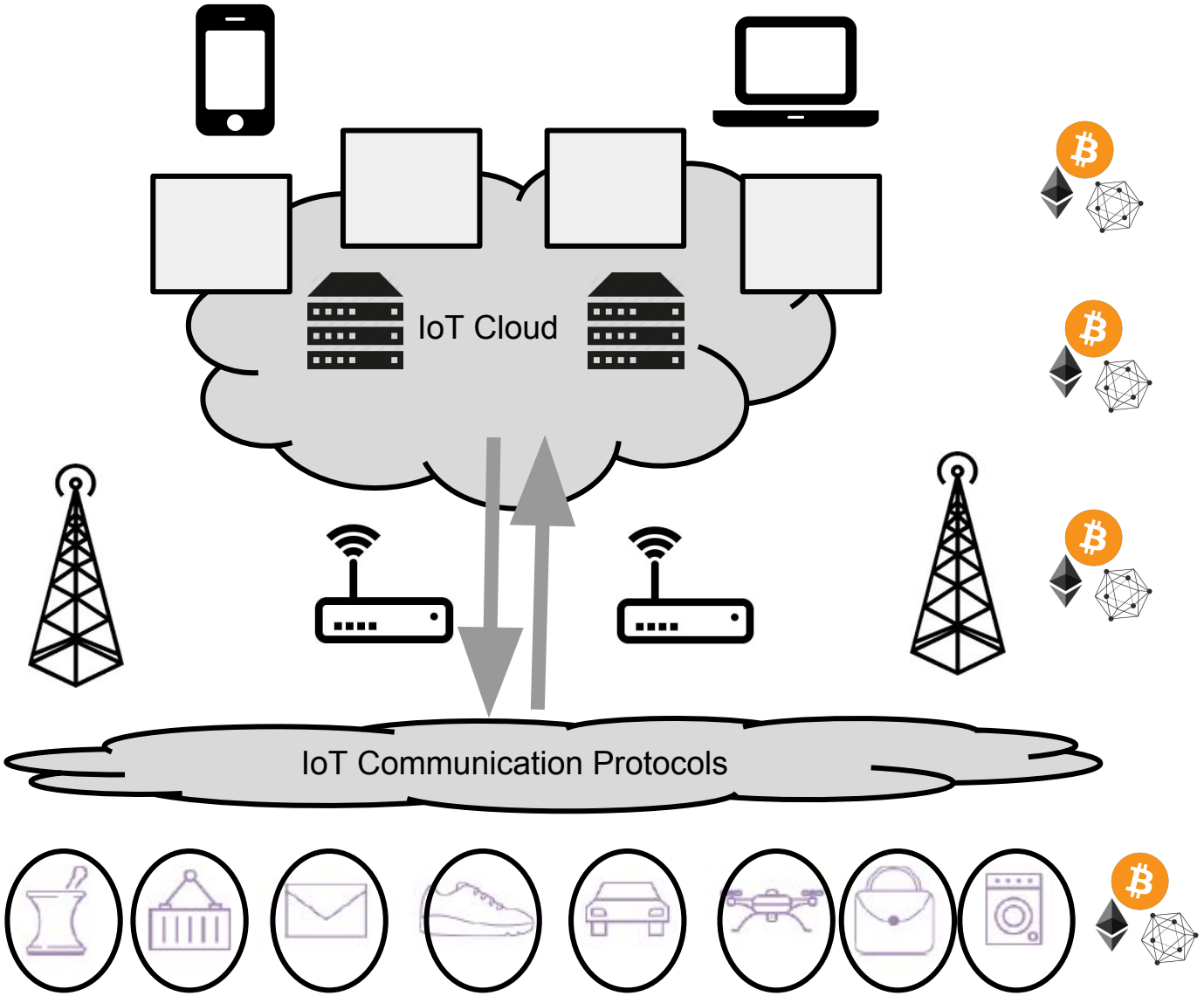
IoT Applications

Cloud infrastructure
(public, private)

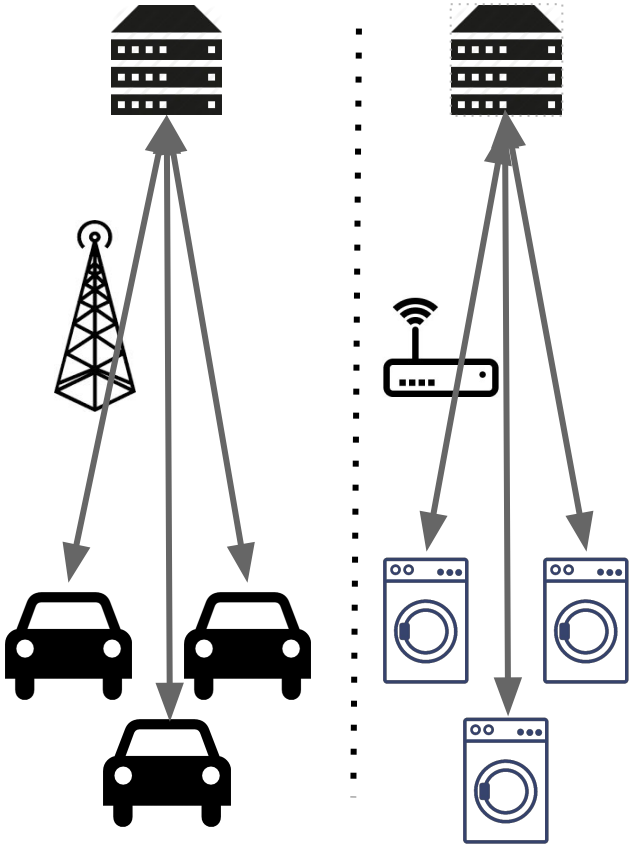
Fog/Edge Computing

Communications
- wired/wireless
- IP / No IP
- licensed/free bands

Connected Things
(sensors & actuators)

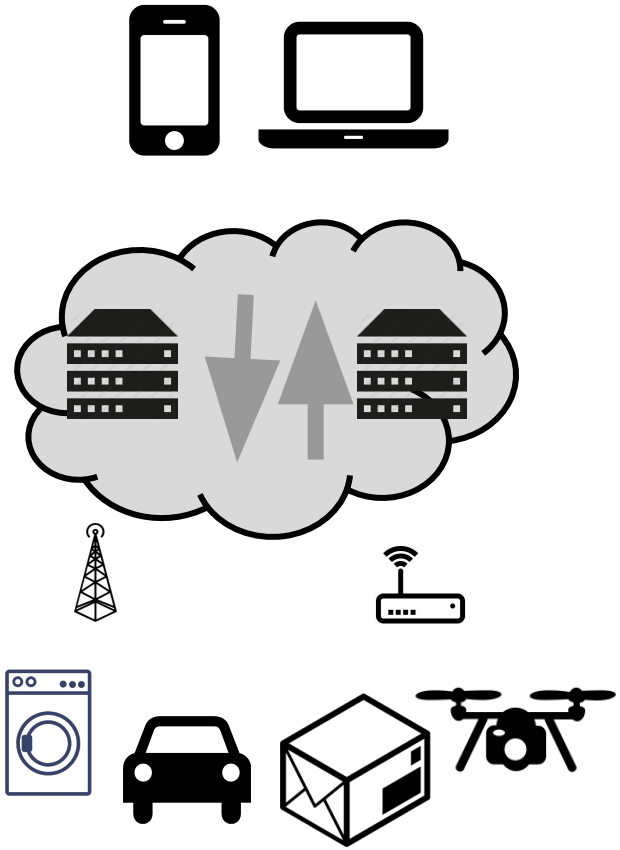


IoT systems over the years



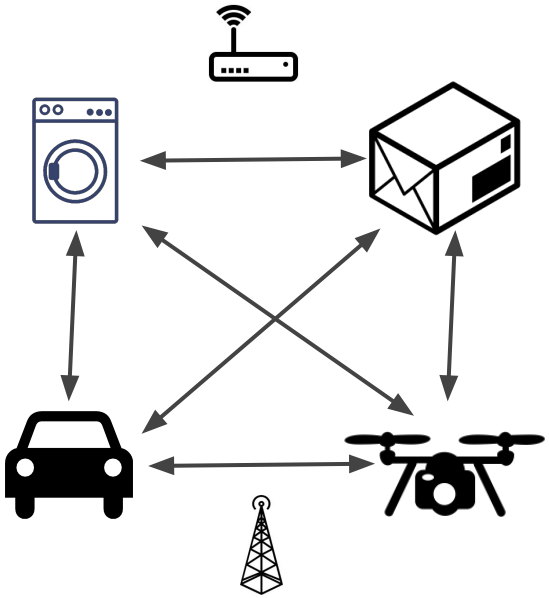
2000

Centralized & monolythic
IoT infrastructures



Today

Cloud-based & Shared
IoT infrastructures



Tomorrow (2025)

Peer-to-Peer
IoT infrastructures

Blockchain applications in IoT systems

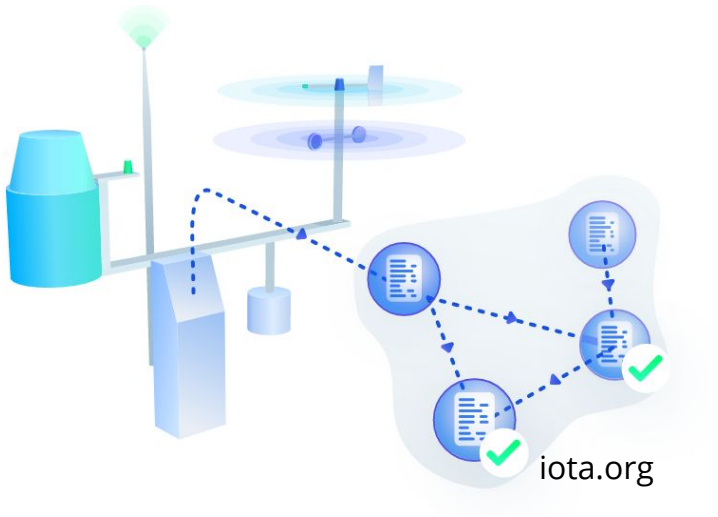
- Assets
  - Device (Endpoints, Gateways)
  - Additional services in the device
  - Measurements & Events from sensors (Data)
  - Actions on actuators (Command)
- Applications
  - Securing event loggings
  - Monetization of IoT Data (stream)
  - Device Identity
  - Device Property Titles
  - Firmware update
  - Locking/Unlocking services on Devices
  - Supply chain traceability
  - Privacy preserving
  - D2D smart contracts
  - Micro-transactions (EV charging, Open energy market)
  - Maintenance tracking and warranties
  - ...

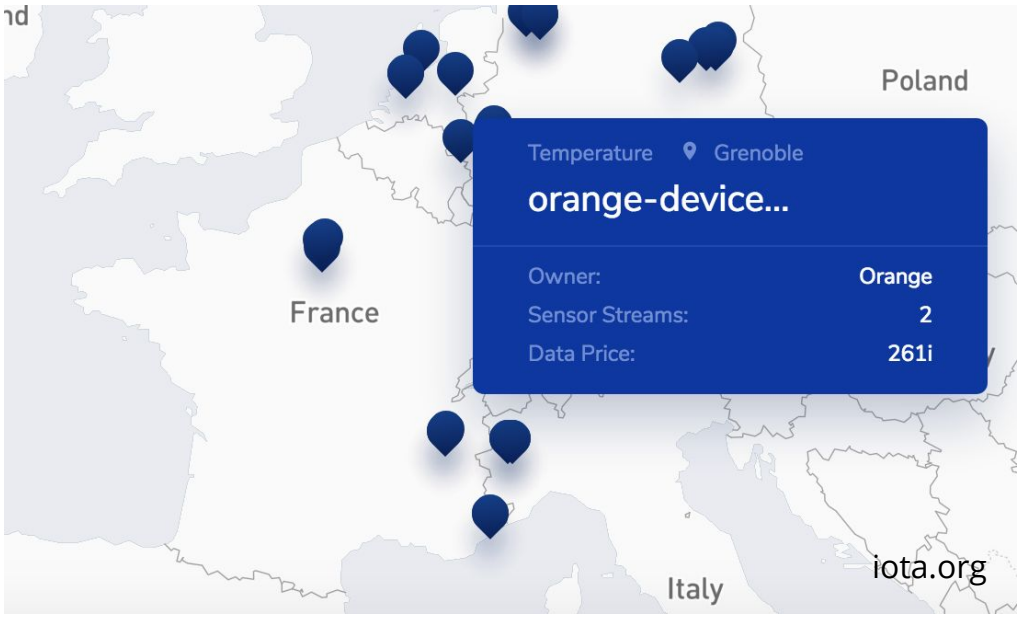
Some IoT use cases

- Sensing-as-a-Service
- Supply chain traceability
- Electric vehicle charging
- Open energy market (Microgrid)

Use case 1 : Sensing-as-a-service (S2AAS)

- securing the sensors data streams
  - Each new data is appended to the ledger (aka irrevocable time-serie DB)
- monetize sensors data streams
  - sensors are owned (and maintained) by companies and individuals
  - customers are companies, research centers, ...
  - sensors are weather station, air quality, self quantified wearables, ...

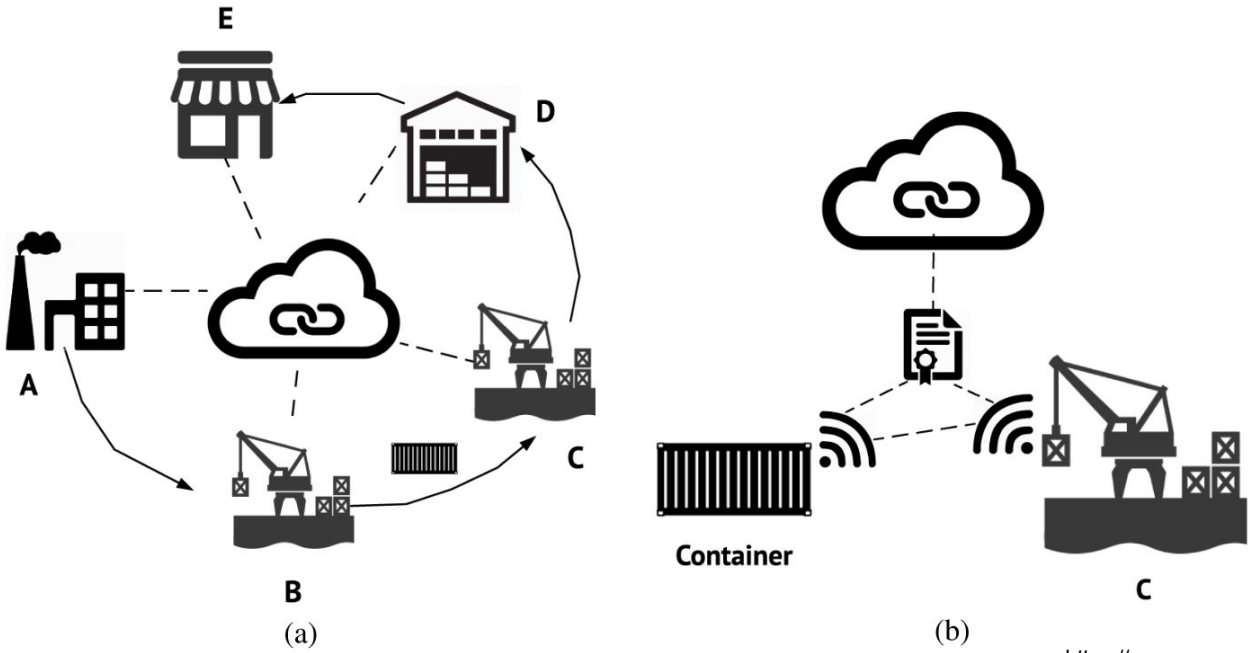




- Example: datum.iota.org

Use case 2: Supply chain traceability

- Current : EPC Global (GS1)
  - Centralized objects registry and event databases (EPCIS and ONS)
- Tracking containers and parcels
  - a) Log the events (RFID, GPS, Beacon) into the ledger
  - b) Trig the excution of smart contacts on events



https://mycourses.aalto.fi/pluginfile.php/378344/mod_resource/content/1/Christidis%20and%20Devetsikiotis.pdf

Example : Mojix’s ViZix blockchain (compliant EPCIS)

Use case 3: Open energy market

Microgrid energy productions

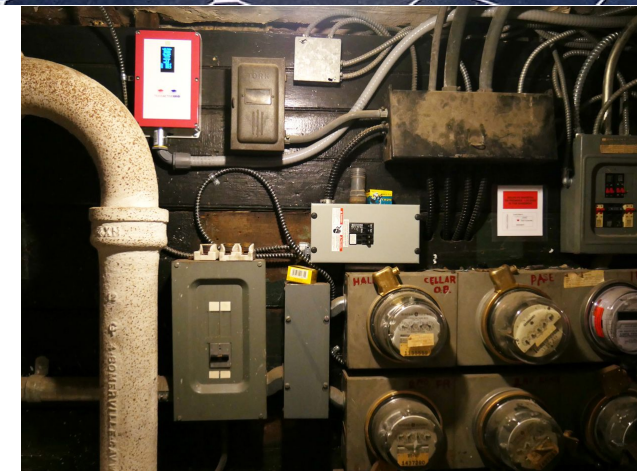
- Rooftop photovoltaic panels
  - US $30 billion in 2016 (grow 11% over 6 years)
- Residential energy storage systems
  - 95 MW in 2016 to 3700 MW by 2025

Application

- Individuals can sell stored and solar electricity to neighbours

Examples

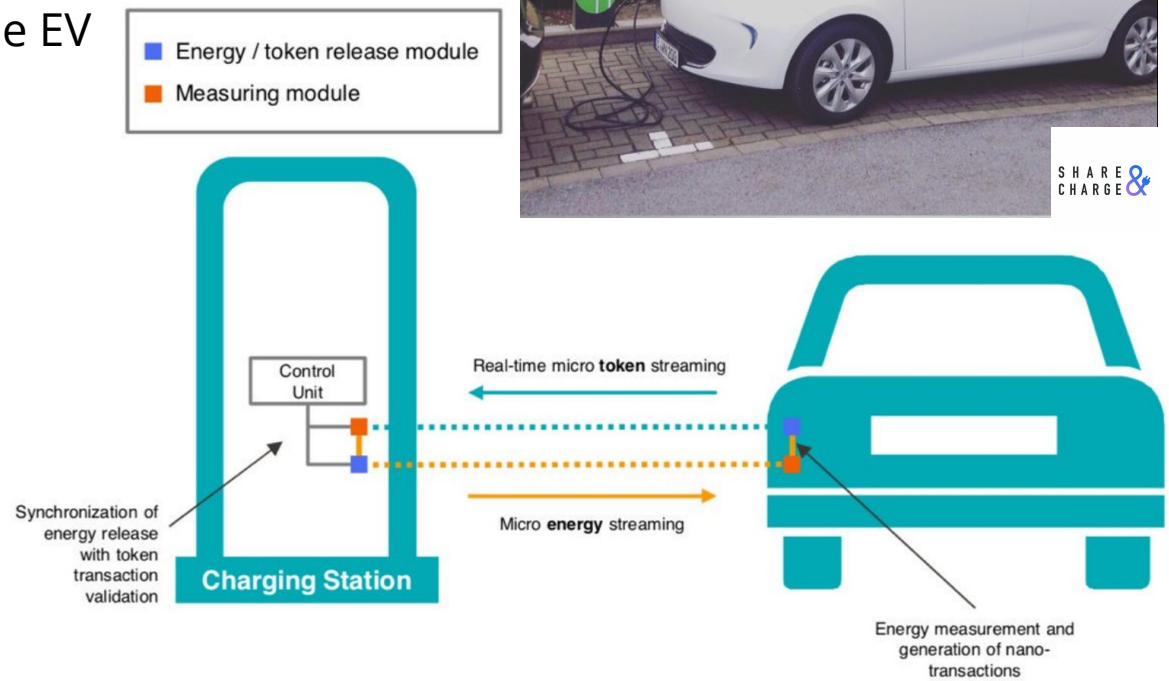
- lo3energy.com (DLT is Hyperledger Fabric)
- SolarCoin.org (Join Ethereum Alliance)



https://spectrum.ieee.org/computing/networks/blockchains-will-allow-rooftop-solar-energy-trading-for-fun-and-profit

Use case 4: Electric vehicle charging

- EV problems
  - Lack of EV charging infrastructure
  - Complex charging contracts
- Applications
  - Share EV chargers
  - Micro payment for charging the EV
- Next step
  - Autonomous car
  - Drones
- Example
  - Share&Charge
  - BlockCharge



[1] Detailed concept and specifications to be published by IOTA foundation soon

Emerging actors

- Consortiums
  - Trusted IoT Alliance
- Startups
  - IOTA
  - Slock.it
  - HAPI
  - Lo3energy
  - Filament
  - Chimera-inc
  - SolarCoin
  - Mojix
  - ...

Our work on Blockchains

Motivations

- Designing consensus protocols for permissioned blockchains

- With the following goals:
  - Versatility (Abstract framework)
  - Robustness (RBFT)
  - Efficiency, geo-replication (XFT)
  - Privacy (PAG)

Abstract framework

- “The Next 700 BFT Protocols”
  - Published in EuroSys 2010 and ACM TOCS 2015
  - Joint work with EPFL and IBM Research

- Contributions
  - Allows designing versatile BFT protocols: latency efficient, throughput efficient, robust protocols, ...
  - The paper describes two algorithms:
    - Quorum: latency optimal
    - Chain: the best throughput

- The concepts of Abstract are leveraged in Hyperledger Fabric

RBFT

- “RBFT: Redundant Byzantine Fault Tolerance”
  - Published in ICDCS 2013
  - Collaboration with CNRS Liris Lab

- Contribution
  - The most robust BFT protocol

- Used in Hyperledger Indy

XFT

- “XFT: Practical Fault Tolerance Beyond Crashes”
  - Published in OSDI 2016
  - Joint work with Eurecom and IBM Research

- Contributions
  - A novel approach to building reliable and secure distributed systems (considering network and machine faults independently)
  - XPaxos: a consensus protocol that tolerates Byzantine failures at the price of standard failures

- XFT is currently being integrated in Hyperledger Fabric

PAG

- “PAG: Private and Accountable Gossip”
  - Published in ICDCS 2016
  - Joint work with CNRS Liris Lab

- Contribution
  - The first accountable, privacy-preserving gossip protocol

- Ongoing work on the use of PAG in algorithms such as SPECTRE

Future work

Goal: being able to use permissioned blockchains at the Edge of IoT networks

How: by designing algorithms for large-scale permissioned blockchains

Thank you!