Blockchain-based Secure Decentralization for the Internet-of-Things

Dr. Vasos Vassiliou

University of Cyprus

Dr. Vasos Vassiliou
University of Cyprus

- Prof. of Computer Networks
- Working on mobile, wireless sensor networks, IoT, and Security for the last 15 years
- Passionate about all things connected and robots
- Co-founder of VIRIDOM
- Definitely not a blockchain expert !!!

Introduction

- IoT is a natural evolution
- Devices have always been connected
- Novelty relates to

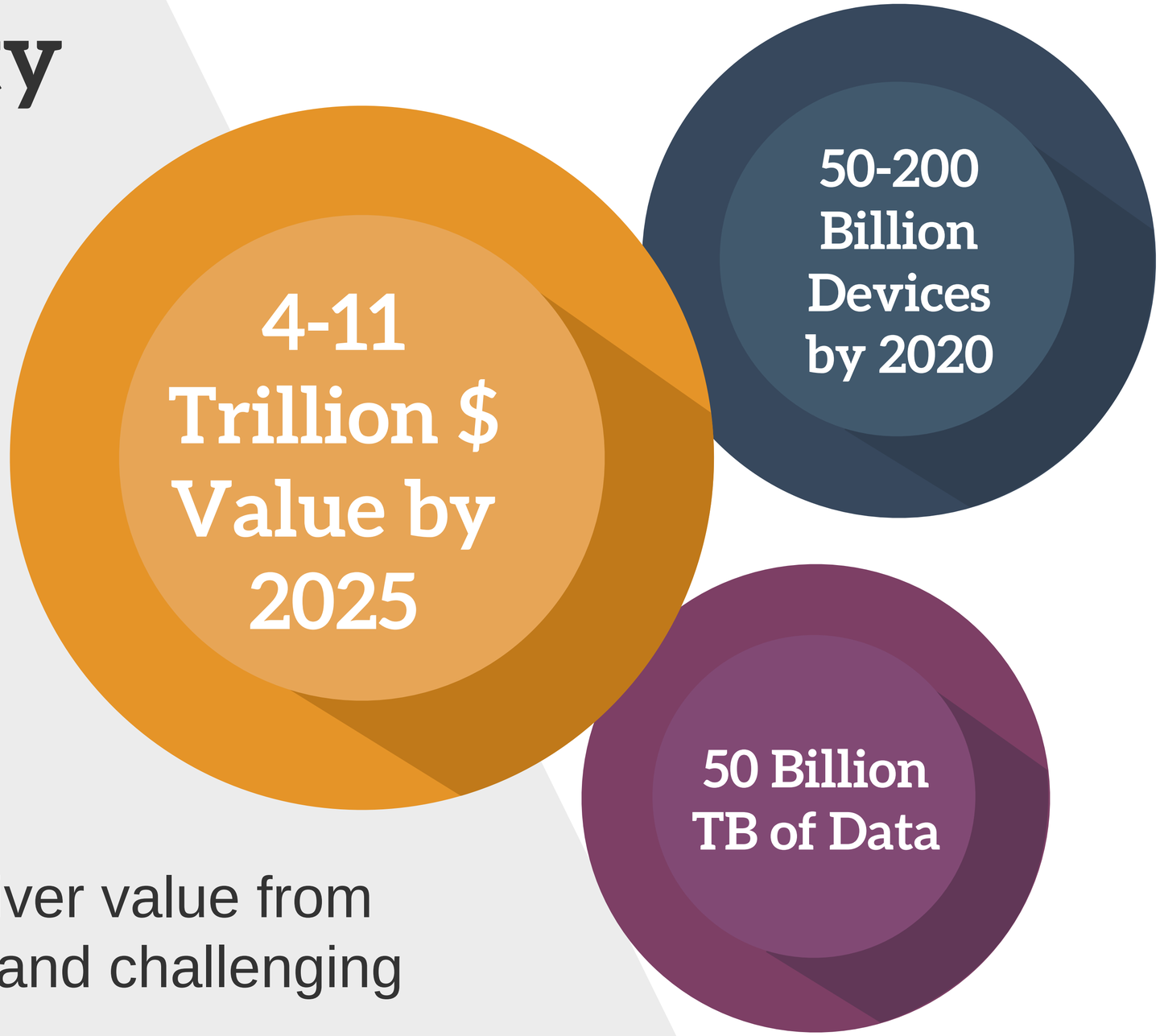
Smaller Size

Better Design

Faster Connectivity

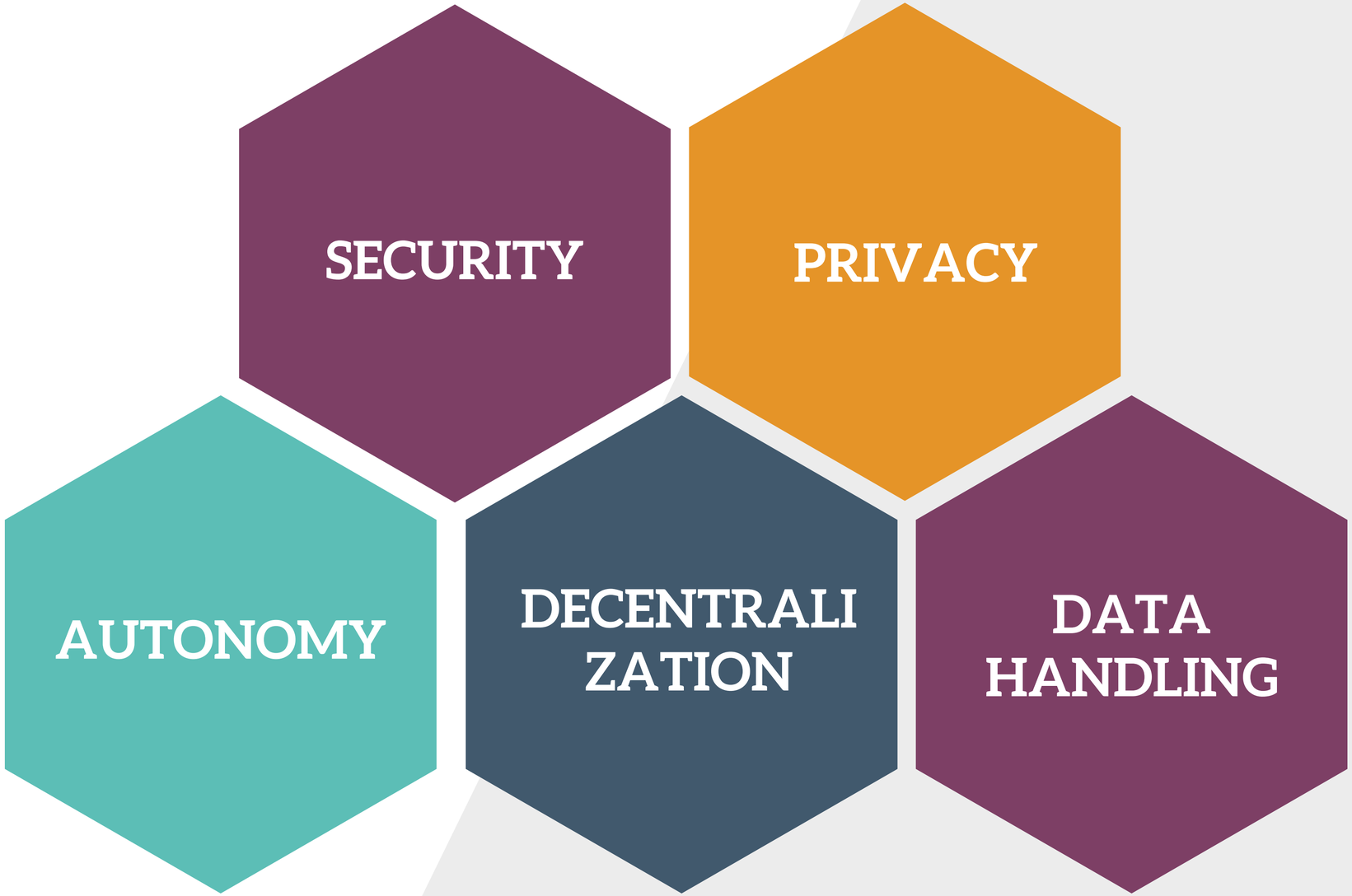
Mobile Operation

Opportunity



Unlocking IoT to deliver value from the data is complex and challenging

Challenges


SECURITY
PRIVACY
AUTONOMY
DECENTRALI
ZATION
DATA
HANDLING

Talk Objective

Is Blockchain the security solution for IoT?

When and how do the two coincide?

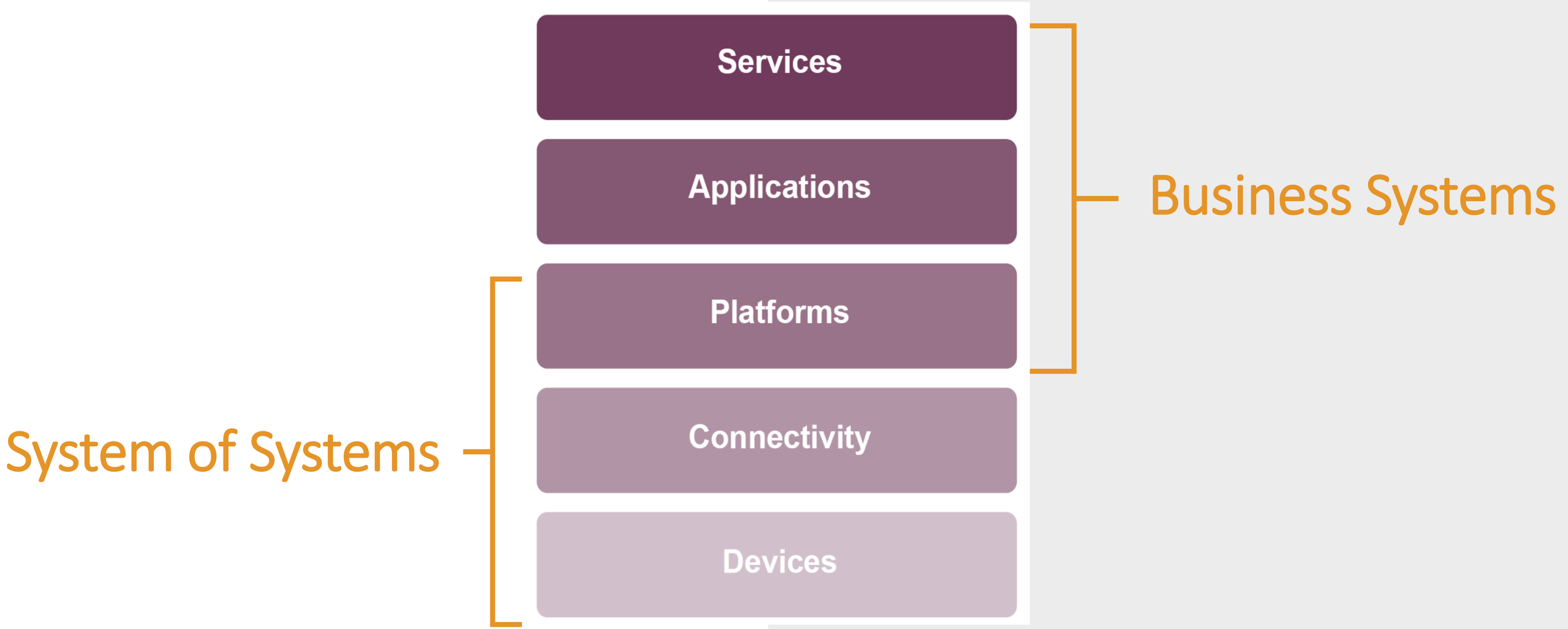
What is IoT?

- The **Internet of things** (**IoT**) is the **network of physical devices** (vehicles, home appliances, and other embedded devices). Each thing is **uniquely identifiable** and able to inter-operate within the existing Internet infrastructure. [Wikipedia]

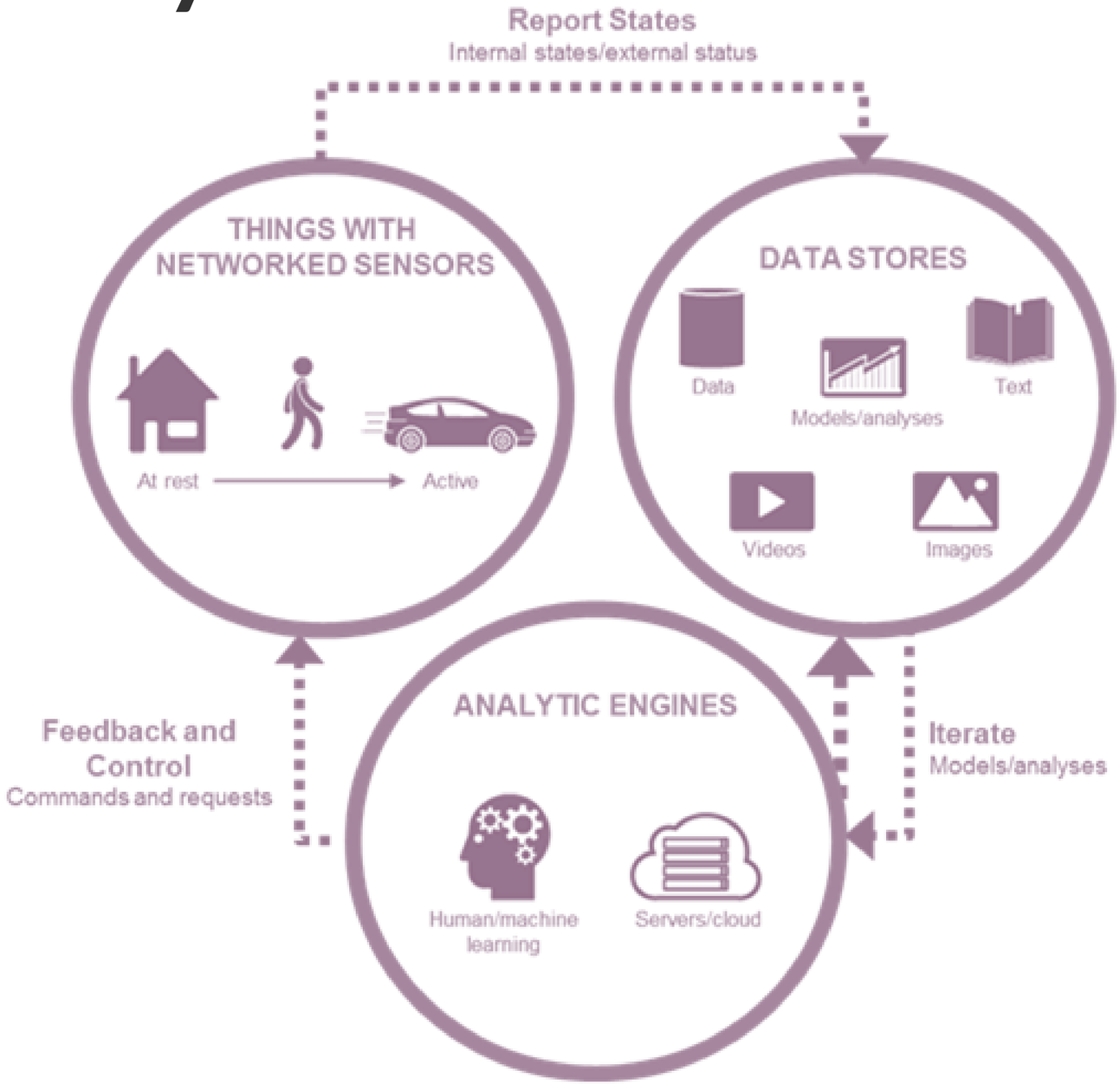
- The Internet of Things (IoT) is a **system** of interrelated computing **devices**, mechanical and digital machines, objects, animals or people that are provided with **unique identifiers** and the ability to **transfer data** over a network without requiring human-to-human or human-to-computer interaction. [TechTargets]

- Internet of Things is the concept of connecting **any device** to the **Internet** and to other connected devices – all of which **collect and share data** about the way they are used and about the **environment** around them. [IBM]

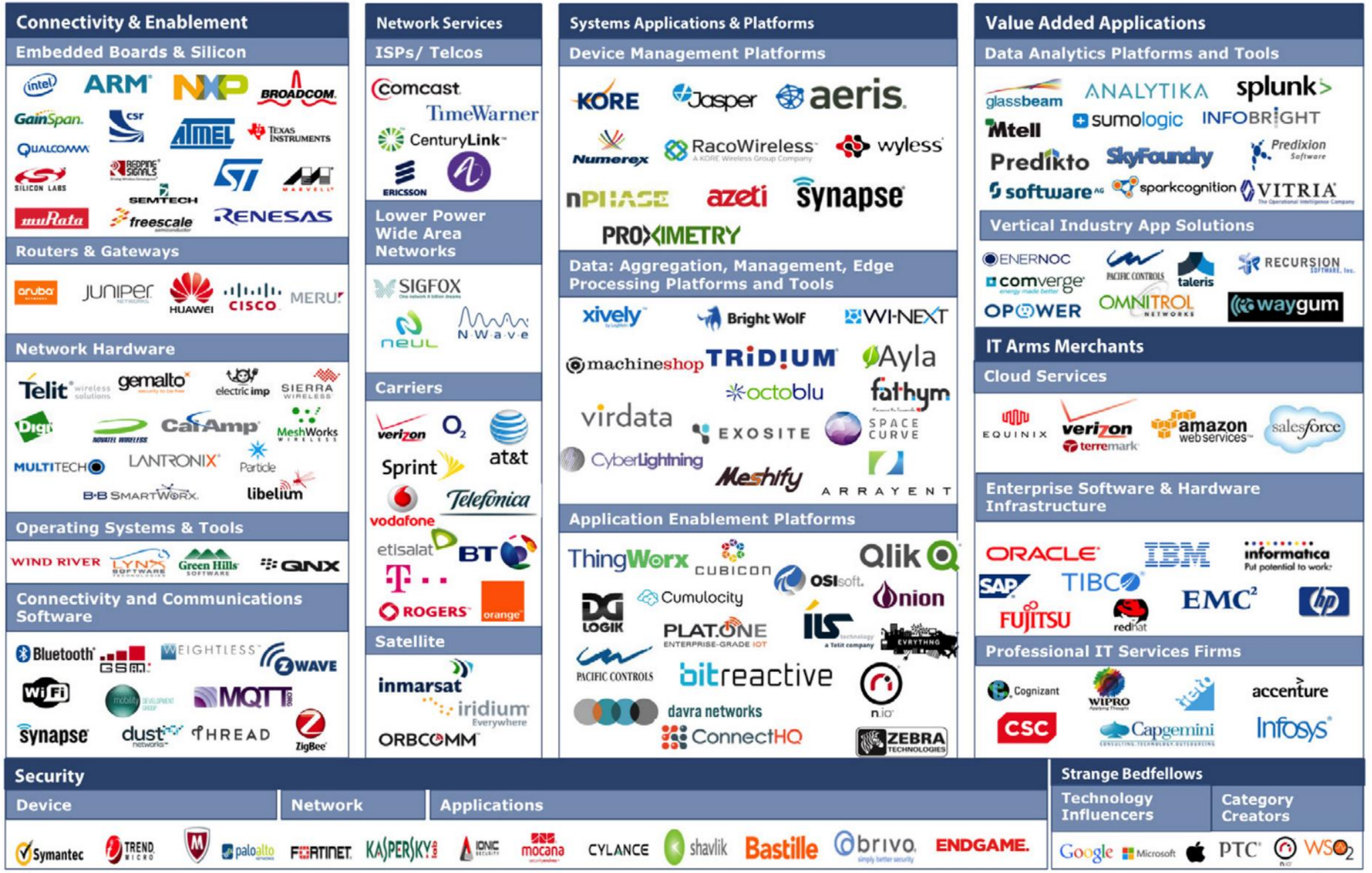
The Different Visions of IoT



The IoT Ecosystem



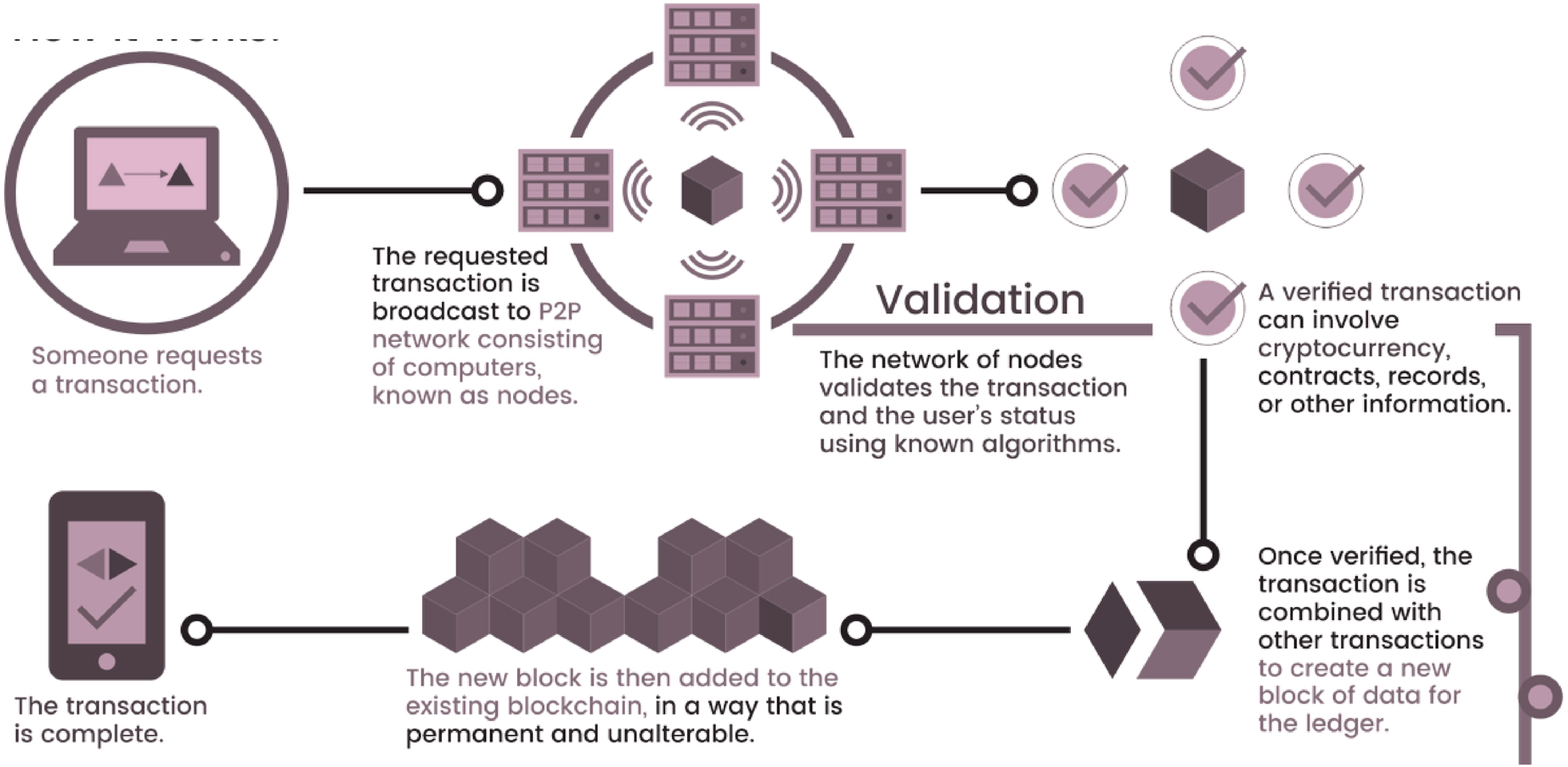
The Internet of Things Technology Landscape



Internet of Things Technology Landscape. Harbor Research 2016

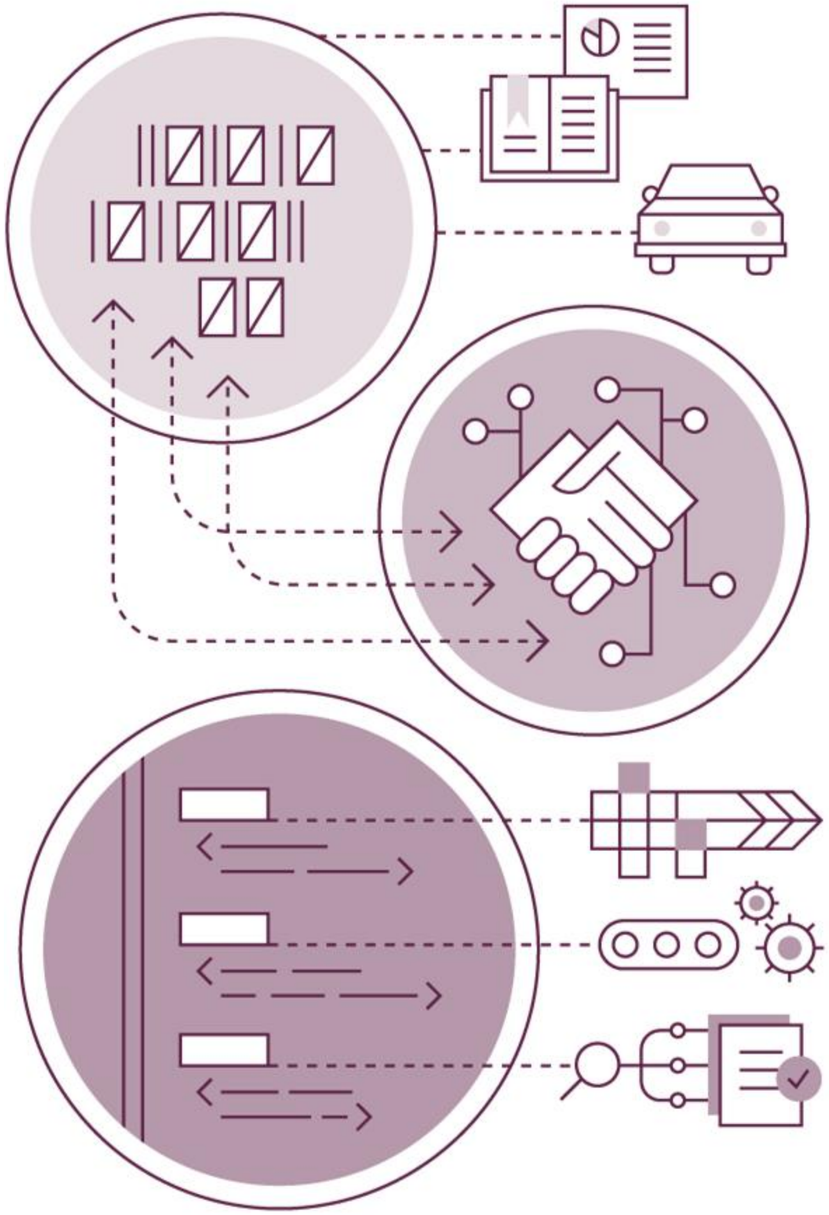
Harbor Research

What is Blockchain?



Adapted from : BlockGeeks

Why Blockchain



1 Storing digital records

Blockchain allows unprecedented control of information through secure, auditable, and immutable records of not only transactions but digital representations of physical assets.

---

2 Exchanging digital assets

Users can issue new assets and transfer ownership in real time without banks, stock exchanges, or payment processors.

---

3 Executing smart contracts

Self-governing contracts simplify and automate lengthy and inefficient business processes.

Ground rules Terms and conditions are recorded in the contract's code.

Implementation The shared network automatically executes the contract and monitors compliance.

Verification Outcomes are validated instantaneously without a third party.

Blockchain and IoT: How exactly?

Source: IBM

Blockchain and IoT: How exactly?

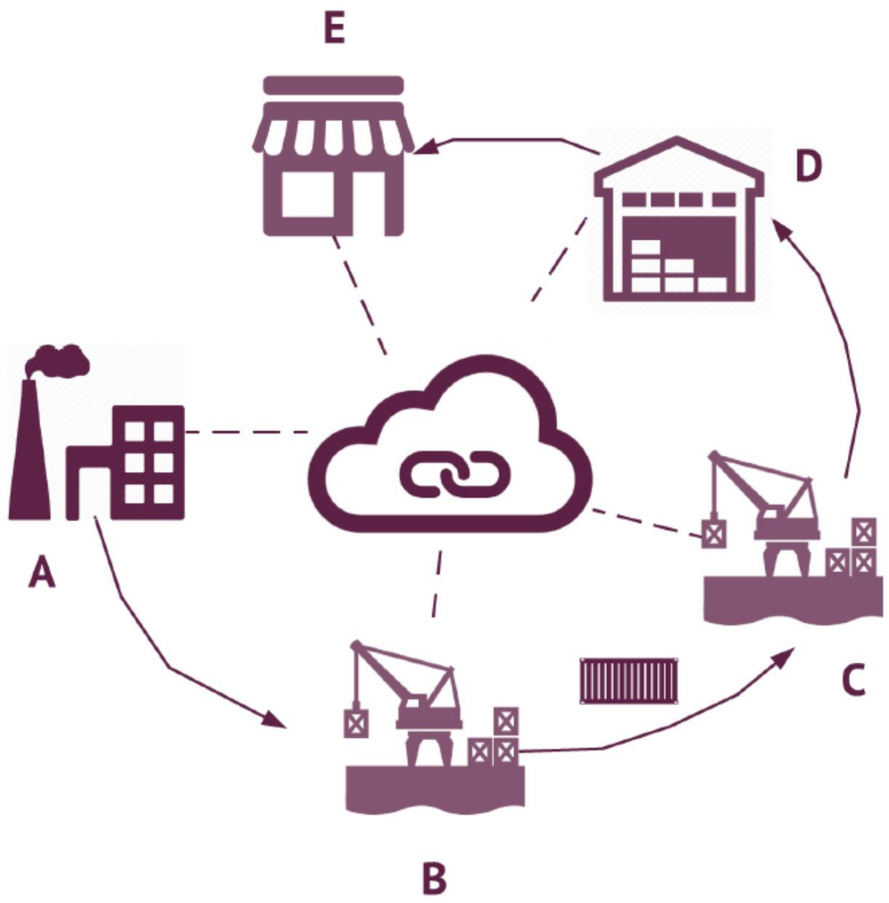
Challenge	Explanation	Potential blockchain solution
Costs and capacity constraints	It is a challenge to handle exponential growth in IoT devices: by 2020, a network capacity at least 1,000 times the level of 2016 will be needed.	No need for a centralized entity: devices can communicate securely, exchange value with each other, and execute actions automatically through smart contracts.
Deficient architecture	Each block of IoT architecture acts as a bottleneck or point of failure and disrupts the entire network; vulnerability to distributed denial-of-service attacks, hacking, data theft, and remote hijacking also exists.	Secure messaging between devices: the validity of a device's identity is verified, and transactions are signed and verified cryptographically to ensure that only a message's originator could have sent it.
Cloud server downtime and unavailability of services	Cloud servers are sometimes down due to cyberattacks, software bugs, power, cooling, or other problems.	No single point of failure: records are on many computers and devices that hold identical information.
Susceptibility to manipulation	Information is likely to be manipulated and put to inappropriate uses.	Decentralized access and immutability: malicious actions can be detected and prevented. Devices are interlocked: if one device's blockchain updates are breached, the system rejects it.

How can Blockchain help IoT?

- Blockchain can be used in an industrial cyber protection context
  - providing a secure means of storing data as transactions
  - with smart contracts providing the details for
    - what data is to be collected
    - how it will be used, and
    - what kinds of transactions are allowed.

Forms the basis for machine-based trust, since all nodes in a network are authenticated and each transaction is verified

Asset Tracking Example



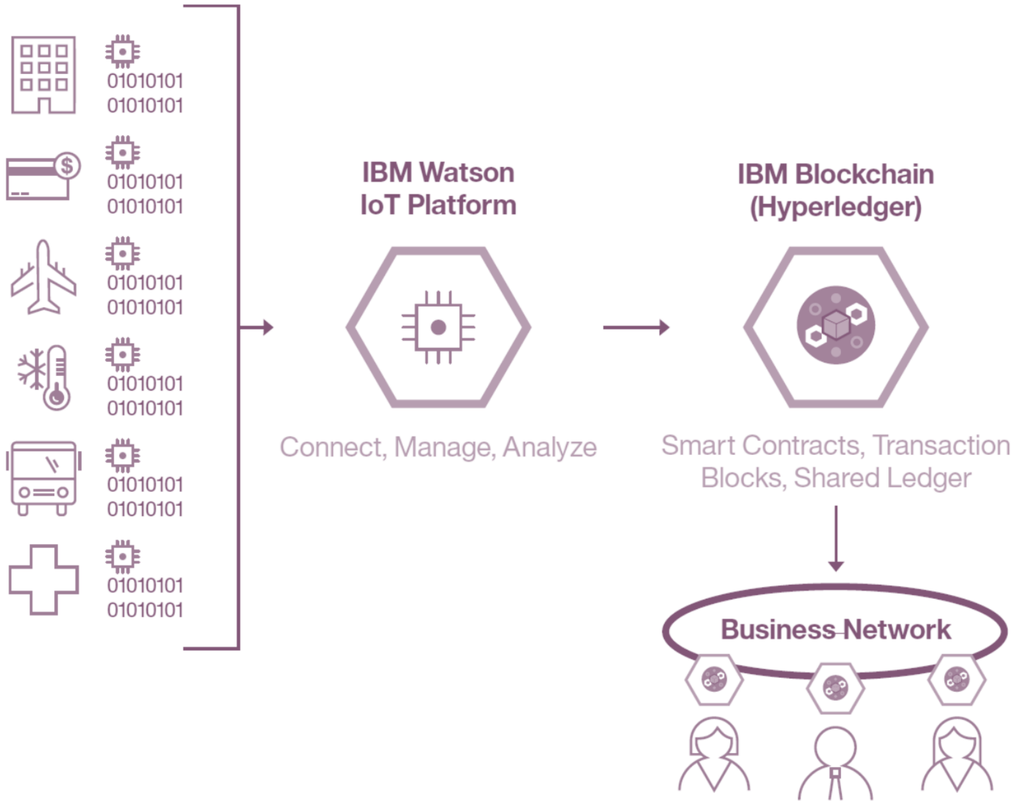
- Shipping carrier reaches destination port and sends a signed message to a predetermined and agreed-upon smart contract to allow everyone on the chain to know that the container is now at point C.
- Since the transaction is signed, it acts as a cryptographically verifiable receipt of the shipping company's claim that the container has reached the destination port.
- The receiver at the port posts to same smart contract to confirm that it is in possession of the container.

Food Safety Tracking

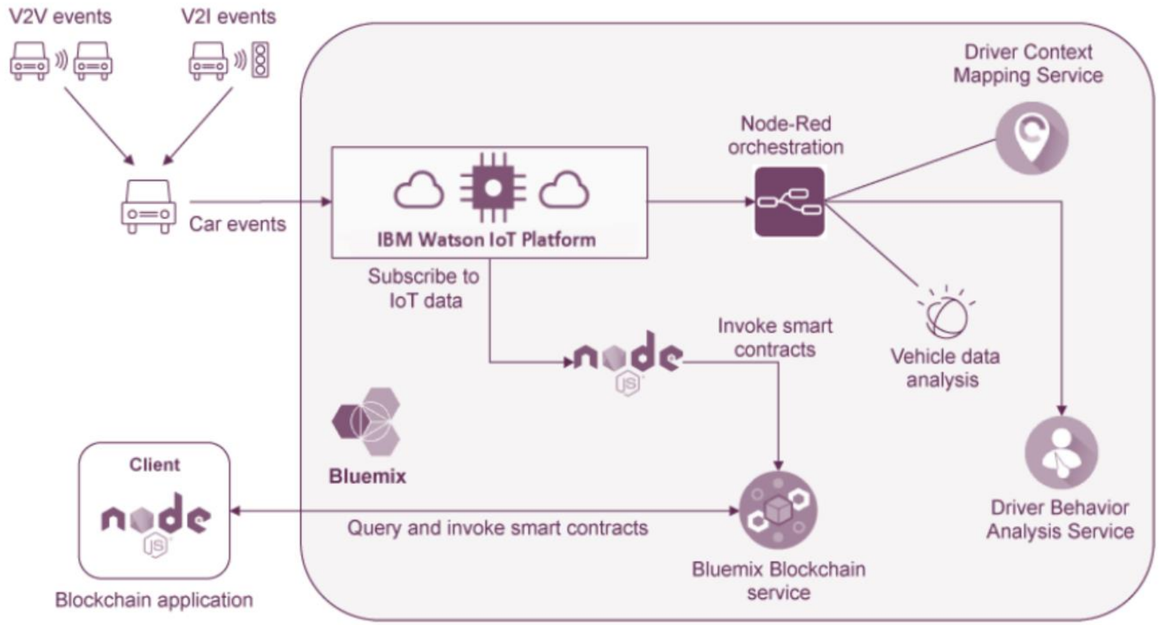
- IBM hopes blockchain will enable food providers and distributors to trace contaminated product to its source in a short amount of time so that it can be disposed of quickly and the source of contamination can be monitored, or removed from the supply chain.

[Enterprise IoT Insights Article, 23 Aug. 2017]

The IBM Concept



Architecture



Intelligent Transportation Example

Instruction Integrity

- Device hashes information it wants to send to another device and places the hash into a Blockchain
- The receiver of the information hashes the same information
- if the hash matches the hash on the Blockchain then the information has not changed in transit.

- Similar to traditional message integrity checking solutions

Device Identity Protocol

- Each device has a Blockchain public key.
- Devices encrypt messages to each other (challenge/ responses) to ensure the device is in control of its own identity.
- This is not far from existing digital signature solutions

Device Registration Systems

- Acertification agency for devices which audits the new device and then gives it an identity on the Blockchain.
- Oncethe device is historically 'born on the Blockchain' the device’s identity will be irreversible.
- Environmental inputs that are unique to an individual sensor, such as GPS, temperature/humidity, etc., be used in conjunction with IMEI & OEM firmware hashes to create the ultimate in tamper-resistant unique device identification

Device Firmware Hashing

- Device firmware can be hashed into a Blockchain on a continual basis.
- If the firmware state changes (by even a single digit) due to malware altering the firmware code, can the hash failure will alert the device owners to foul play.

- This is not dissimilar to an immune system flagging a foreign body.

Distribution of Software Updates

- All the IoT devices of a manufacturer operate on the same blockchain network.
- The manufacturer deploys a smart contract that allows them to store the hash of the latest firmware update on the network.
- The devices either ship with the smart contract's address baked into their blockchain client, or they find out about it via a discovery service.
- They can then query the contract, find out about the new firmware, and request it by its hash via a distributed peer-to-peer filesystem

Applying Blockchain for IoT security

- Blockchain doesn’t solve every security problem for IoT devices, such as the hijacking of IoT devices for use in DDoS botnets
- It just helps protect data from malicious actors.

False Claims

- ADEPT (IBM & Samsung)
  - Use of bitcoins to pay for goods
- TILEPAY
  - Sell data for digital currency
- SOLAR
  - energy produced by IoT solar panels generates cryptocurrency value that is registered on the blockchain

Shortcomings

Processing Power

Storage

Legal and Compliance

Energy Consumption

Conclusion

- IoT, Blockchain **and AI** will be the winning trio
- Transition to decentralized network not always makes sense
- Blockchain not be able to fulfill all items in “wish-list”
- Blockchains and smart contracts bring a slew of advantages, but they also come with a bag of disadvantages

Contact

Dr. Vasos Vassiliou

Networks Research laboratory
Dept. of Computer Science
University of Cyprus

vasosv

vasosv@ucy.ac.cy

+357 22892750