inlecom

"Enhancing innovation capacity through digital ecosystems"

Blockchain and IoT Convergence Challenges

Konstantinos Loupos, MEng, MSc, PMP, MBA

Head of R&D Program

INLECOM Group: *Enhancing innovation capacity through digital ecosystems*

- Founded: 1996
- Offices: Athens (GR), Brussels (BE), London (UK)

- Main Expertise:
  - Project Management, Governance & OPEX
    - End to end life cycle management of ICT projects
  - Logistics (transport), IoT (ICT, SEC, ..)
  - Cyber security
  - IoT, Analytics, Cloud, Big Data & Blockchain
  - System Integration and Validation
  - Solution Design, Prototyping
  - Security & Compliance
  - Innovation Management & IP Protection

  - Website: http://www.inlecom.eu/

inlecom

R&D Program: Technologies and Domains

- Strong engagement into EC Research Programs (FP6-FP7-H2020)
- Technologies:
  - IoT
  - Blockchain
  - Big Data
  - Communication Systems
  - Embedded Systems
  - Sensing Technologies
  - Analytics
- Topics/Sectors:
  - Transport/Logistics
  - Security
  - Health
  - ICT & Robotics
  - Environment
  - Circular Economies
  - Other: GSRT, MED, Interreg

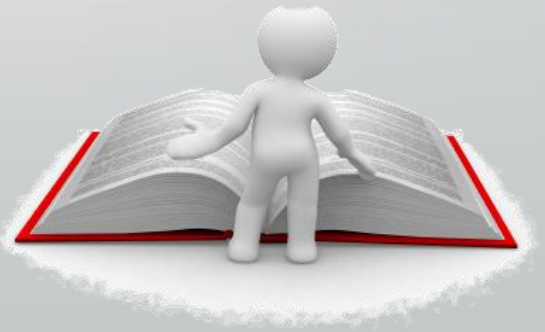
Definitions and Alignment

- Blockchain:

  "a cryptographically-secured distributed electronic ledger that contains tamper-proof records, autonomously built up and hosted by participating nodes through a decentralized consensus mechanism"

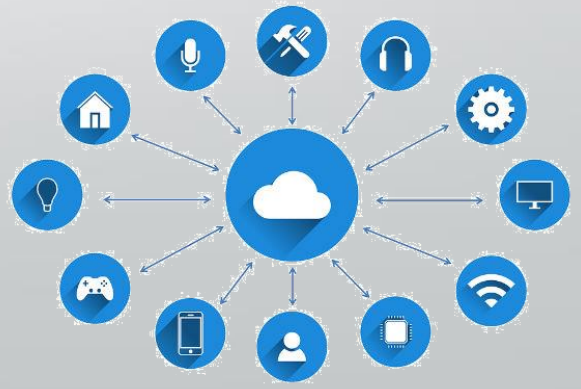
- Distributed Secure Ledger (DSL):

  "a consensus of replicated, shared, and synchronized digital data geographically spread across multiple parties, without any form of central administration or data storage"



Internet Of Things (IoT)

- **Internet of Things:** the internet inter-connection of computing devices/nodes embedded in ordinary items/devices enabling them to send and/or receive data
- Within the most disruptive technologies of the century
- Natural evolution of Internet (simple computers) to ***embedded and cyber-physical systems*** ("things")
- At this level of interconnected things, information is collected at a **greater granularity**
- The complexity, continuous increase and density of data penetrating our every-day lives raises **serious security, safety and privacy concerns**
- **Applications**: smart-life, smart-mobility, smart-city, smart-manufacturing/production and many more…

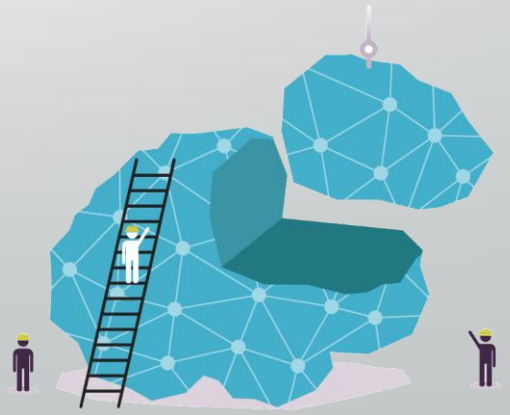


IoT Today

- Internet of Things (IoT) exponentially grows in research and industry
- Still suffering from privacy/security vulnerabilities
- Existing conventional security/privacy approaches seem not applicable for IoT
  - decentralized topology and
  - resource-constraints (devices majority)

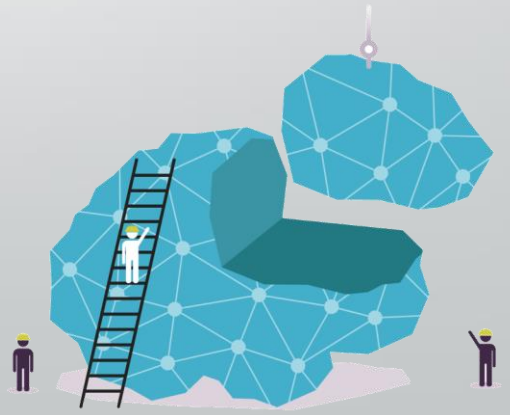
IoT Industrial Challenges 1/2

- **Conventional Cyber-security control unable to keep up with rapidly evolving IoT market**
  - New products, merges/acquisitions, market expansion
  - Continuous software upgrades, proprietary software, non-disclosed source code
- **Multi-branch Networks** (and sub-networks of networks)
  - Complex infrastructures, cloud computing etc
  - Circuitous information flows, indirect communications
- **Commercially available applications communicating with IoT networks**
  - Social apps, geo-location mapping etc
  - Malicious apps, vulnerabilities



Industrial Challenges 2/2

- **IoT Sensor wireless capabilities**
  - Opens up new opportunities for cyber-attack vectors
- **Legislations, Governance and Compliance**
  - Data accumulation under different levels of scrutiny
- **Information Privacy and Protection**
  - Uncontrolled propagation of private/personal information within IoT networks
  - Undetectable/uncontrolled data breaches



Benefits of using Blockchain and DSL 1/2

- **Secure message exchanges:** model agreement between the two (or more) parties
  - Secure M2M communication: Device authentication & peer-to-peer messaging
- **Decentralization:** Lack of central control ensuring scalability and robustness by using resources of all nodes and eliminating many-to-one traffic flows
  - Eliminates many-to-one traffic flows & single points of failure enabling M2M interactions & inter-device agreements
- **Anonymity (privacy):** suited for most IoT use cases where the identity of the users must be kept private
  - Blockchain subnetworks can specify access control to crucial operational data, controlling information flows locally/offline
- **Smart Contracts**
  - Nick Szabo introduced the concept of Smart Contracts as an alternative to traditional paper-based contracts

Benefits of using Blockchain and DSL 2/2

- **Security:** Realization of a secure network over untrusted parties
  - Needed in IoT with numerous/heterogeneous devices, such as a house-blocks with multiple fire-detectors
- **Aided autonomous decision making automating decision mechanisms**
  - Autonomous Device Coordination: Resource negotiations in case of an emergency, where unnecessary sensors stop transmitting data & instead let the emergency sensor be prioritized
- **Record transactions for account and audit**
  - Data from IoT applications transported through infrastructure owned by multiple organizations.

IoT Challenges over DLTs (and blockchain) 1/3

- **Resource constraints:**
  - IoT platforms have **limited resources for computation, communication and storage**,
  - Blockchain technologies demand excessive Resources
- **Bandwidth requirements:**
  - Blockchain Platforms have to interact with other platforms in the network to participate in the consensus process
- **Security:**
  - All the devices in the network coordinate and cooperate with each other through pre-defined protocols
  - Devices stay connected to the blockchain network for participating in the consensus process making IoT devices potentially more susceptible to security attacks

IoT Challenges over DLTs (and blockchain) 2/3

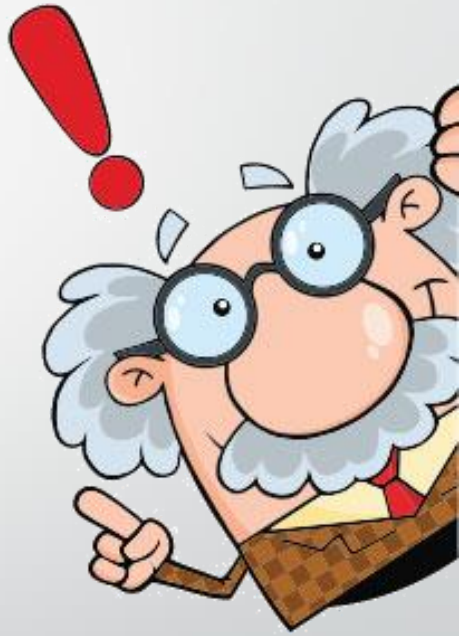
- **Latency demands:**
  - IoT systems consist of a collection of data producers and data consumers and data consumers react to an event and perform an actuation.
  - Blockchain may reduce responsiveness of the data consumer
  - Consensus needs to conclude before reacting to an event
- **Transaction fees:**
  - IoT devices cannot store all transaction data (at least not always)
- **Permissioned vs public:**
  - Public blockchains (Bitcoin and Ethereum) no authorization needed
  - Permissioned blockchains consist of authorized network members

IoT Challenges over DLTs (and blockchain) 3/3

- **Tolerance for intermittently connected devices:**
  - IoT applications at devices with intermittently connection
  - End-devices running on batteries use duty cycling to prolong lifetime
  - Devices operating on the wireless bands regulated by ETSI and FTC need to adhere to the bandwidth limitations enforced federal authorities
- **Transaction Volumes:**
  - Limiting volume of IoT devices in the network (and blockchain)
- **Physical interface weakness:**
  - As cyber-physical systems, individual sensors and actuators can be hacked or misused to report false or erroneous data that gets logged on to the blockchain in an immutable fashion

Conclusions

- **Various challenges (still) exist**
- **Blockchain and DLT still prove very promising towards:**
  - Security
  - Privacy
  - Trust
- **Especially in multi-party applications**



Thank you!

Konstantinos Loupos

MEng, MSc, PMP, MBA

konstantinos.loupos@inlecomsystems.com

Head of R&D Program

INLECOM Innovation

www.inlecom.eu