

**Sixth Regional Workshop for Africa on "Standardization of future networks: What opportunities for Africa?"
Abidjan, Cote D'Ivoire, 26 – 27 March 2018**

**Blockchain as a Trust Enabling Infrastructure
Opportunities and Challenges**

Dr. Ramy Ahmed Fathy, PhD

Director of Digital Services Planning and Risk Assessment, NTRA

Co-Chairman of ITU-T WP1/20

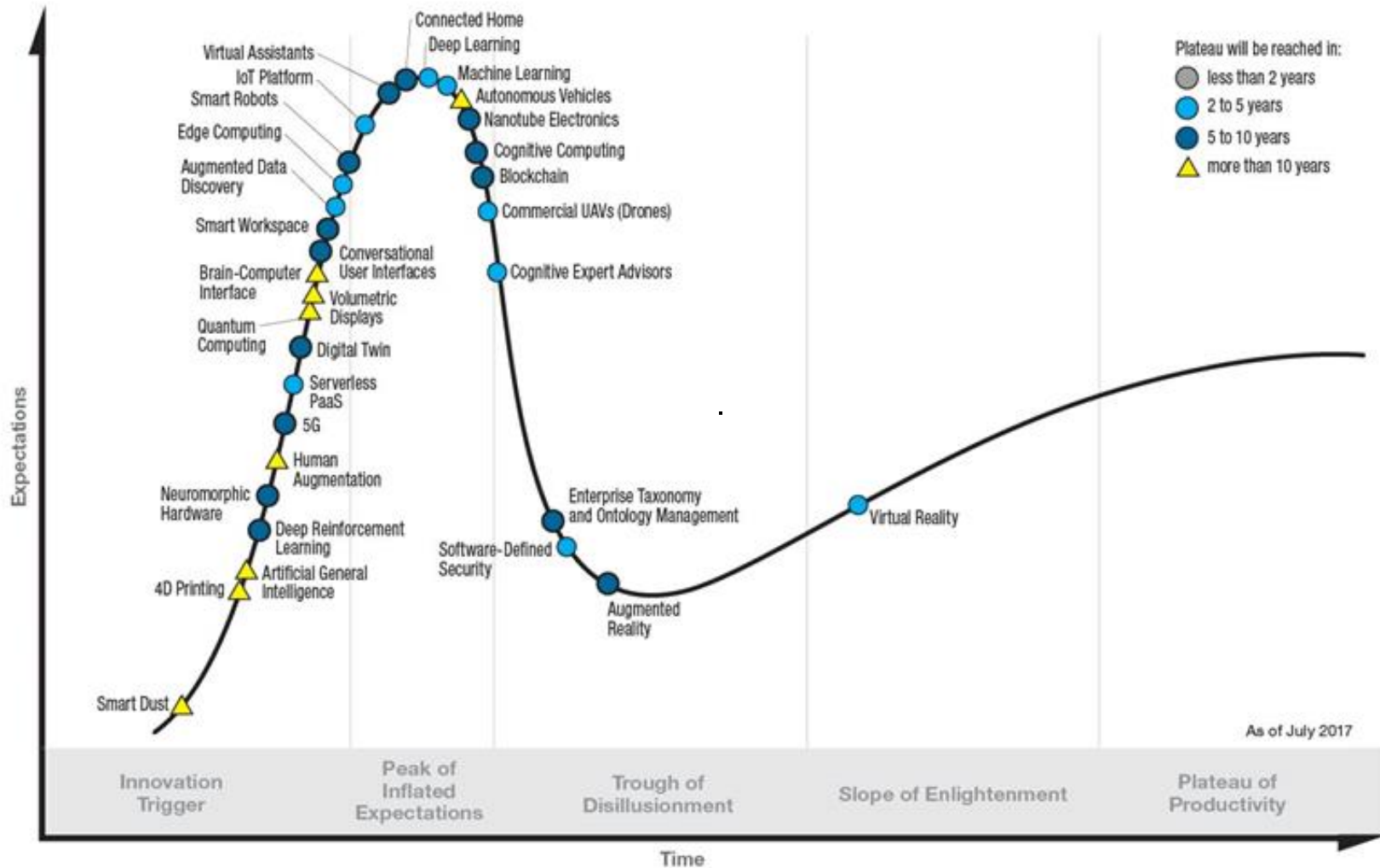
Vice Chairman of ITU-T SG20 "IoT and its Applications including Smart Cities and Communities (SC&C)"

Content

- Why Trust is Important?
- DLT Key Ideas
- DLT Challenges
- Use Cases

WHY TRUST IS IMPORTANT?

IoT, Blockchain, AI, Machine Learning, Deep Learning, AR, VR

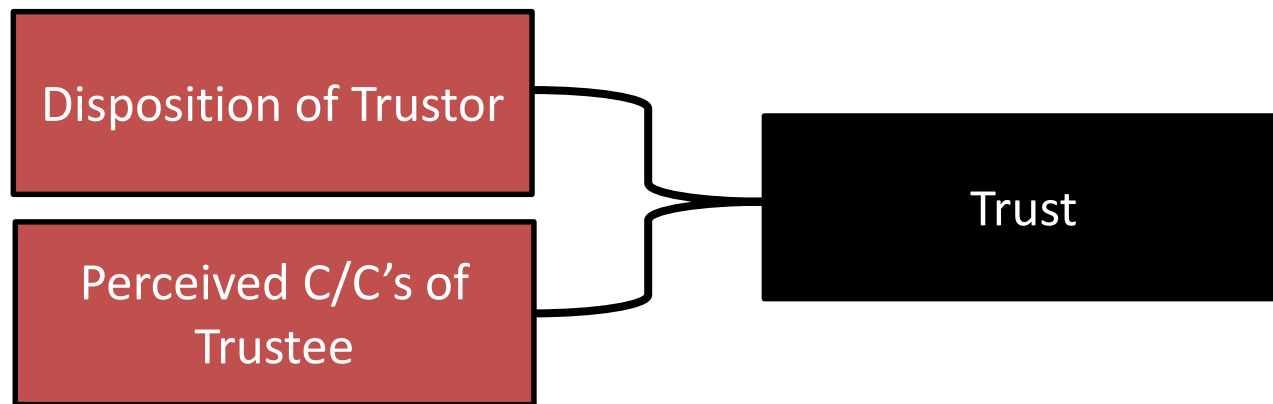


New Issues Coming Up!

- IoT: Notions of security, privacy (data), cloud security, interoperability, lock-in, identification
- Blockchain: Notions of anonymity, accountability, decentralized platform, smart contracts, permissioned vs. permission-less ledgers + money laundry issues (bitcoin and similar digital currencies)
- AI: Notions of autonomy, accountability, unknown behavior, & unpredictability will pop up → mistrust
 - New regulatory tools are needed for security, and safety checks are needed

Security leads to trust..

- Trust is “the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party”



Mayer et al. (1995)

Antecedents of Trust: Theoretical Framework

PREDICTABILITY

The degree to which a person meets the expectations of the trustor in terms of reliability and consistence of behavior

Cognitive Trust
(Schumann et al.)

ABILITY

Capability of a trustee (based on knowledge, competence, and skills) to perform tasks within a specific domain

Tripod Model
(Mayer et al.)

BENEVOLENCE

The perceived level of courtesy and positive attitude

Affective Trust
(Schumann et al.)

INTEGRITY

The intrinsic moral norms of a trustee to guard his actions with (e.g. sincerity, discretion, honesty)

Adapted from Fabio Calefato et al. (2015)

Which impacts trust more? Propensity vs. Trustee C/C's?

Propensity of Trust

High impact if no info is available on the **INTEGRITY, BENEVOLENCE, & ABILITY** of the Trustee.

No impact if these info are available.

ICT Intermediary Systems

Expert system, Trust Analysis and Management Platform (TAMP), Trust Service Broker (TSB) ...etc.

Trustee Available Info

INTEGRITY

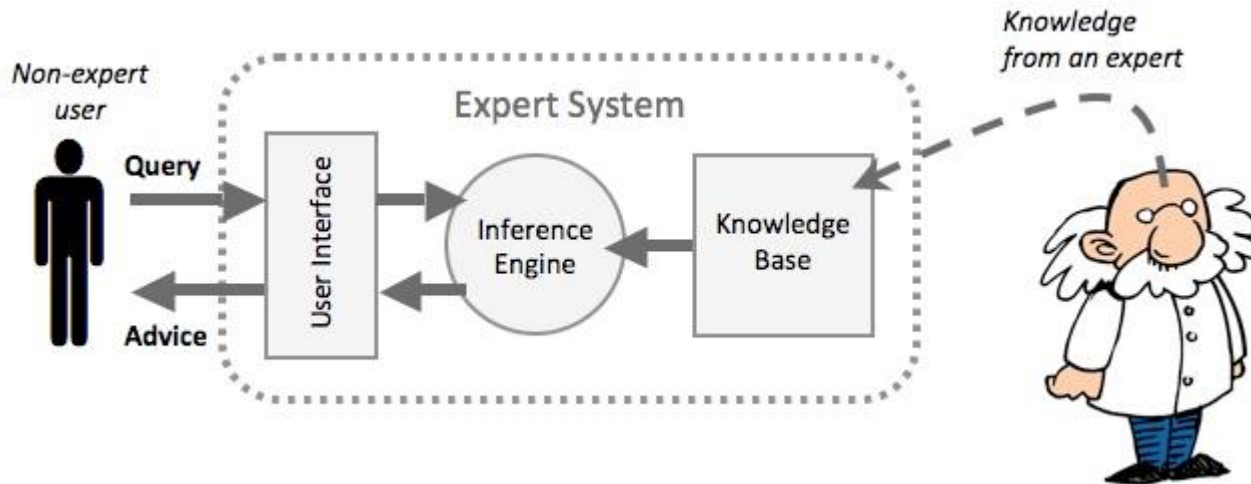
The intrinsic moral norms of a trustee to guard his actions with (e.g. sincerity, discretion, honesty)

BENEVOLENCE

The perceived level of courtesy and positive attitude

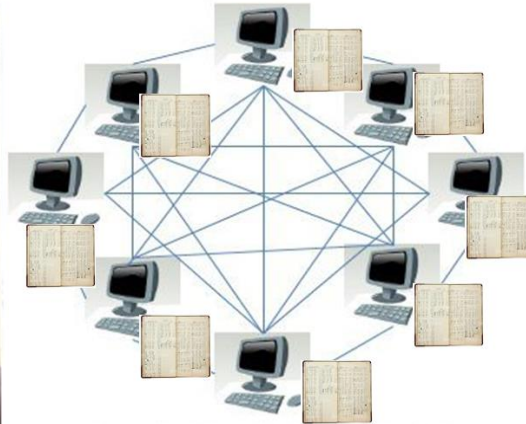
ABILITY

Capability of a trustee (based on knowledge, competence, and skills) to perform tasks within a specific domain



DLT KEY IDEAS

DLT Key Ideas



Peer-to-Peer Network Model



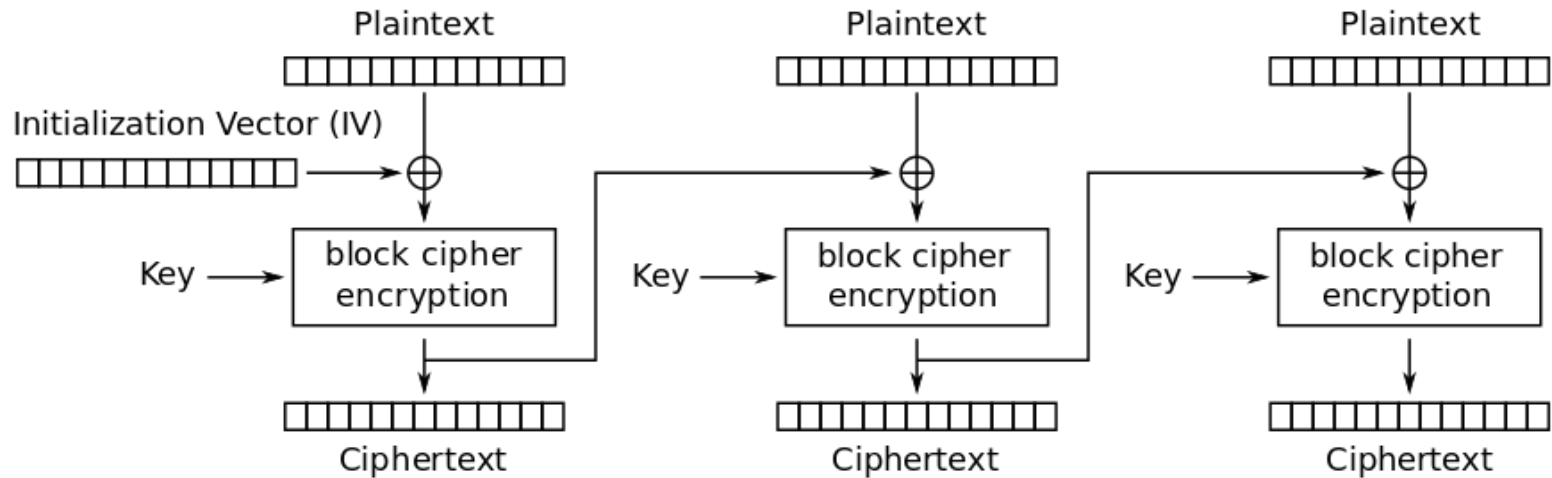
(Photo via BigStock).



"It looks like we have a consensus."

- No centralized control.. Is this the key idea?
- Consensus: Realized between equals ! ,e.g. nodes, peers, ...etc.
- Embedded software logic to perform a pre-built function in response to preprogrammed event! → Smart Contract
- Crypto for fidelity, authentication, authorization → transaction records, validation, blockchain..

Does that ring any bells?



Cipher Block Chaining (CBC) mode encryption

Ehrsam, Meyer, Smith and Tuchman invented the Cipher Block Chaining (CBC) mode of operation in 1976.

$$C_i = E_K(P_i \oplus C_{i-1}),$$

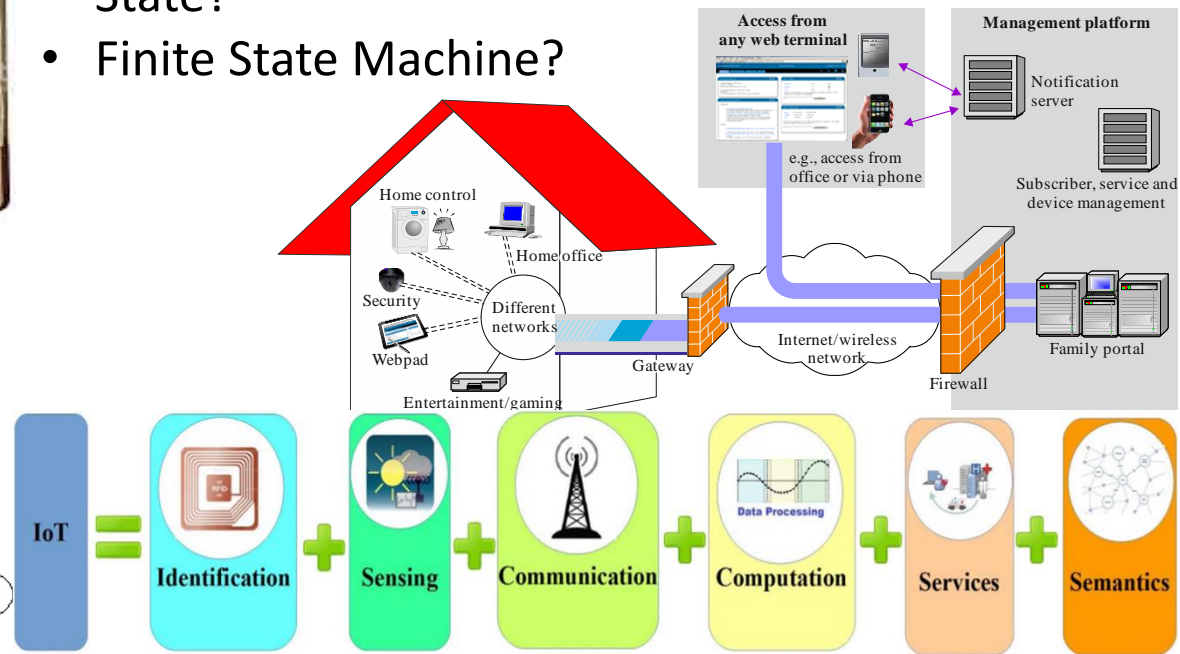
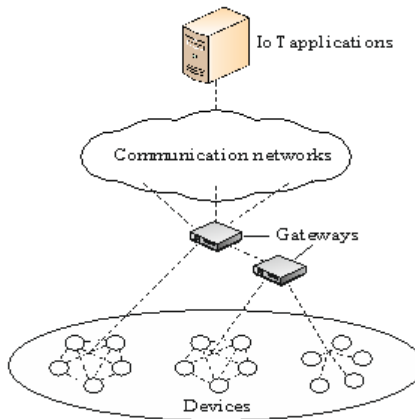
$$C_0 = IV$$

DLT is an encryption problem + P2P

DLT CHALLENGES

Let's have a closer look at the ledger!

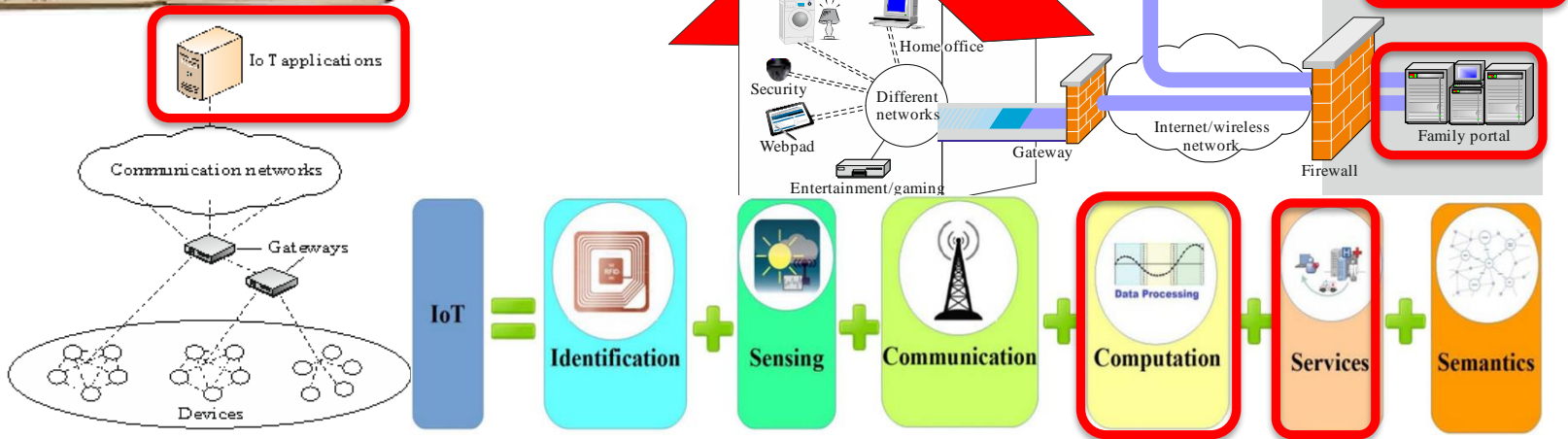
- Data?
- Transaction?
- State?
- Finite State Machine?



Let's have a closer look at the ledger!

- Data?
- Transaction?
- State?
- Finite State Machine?

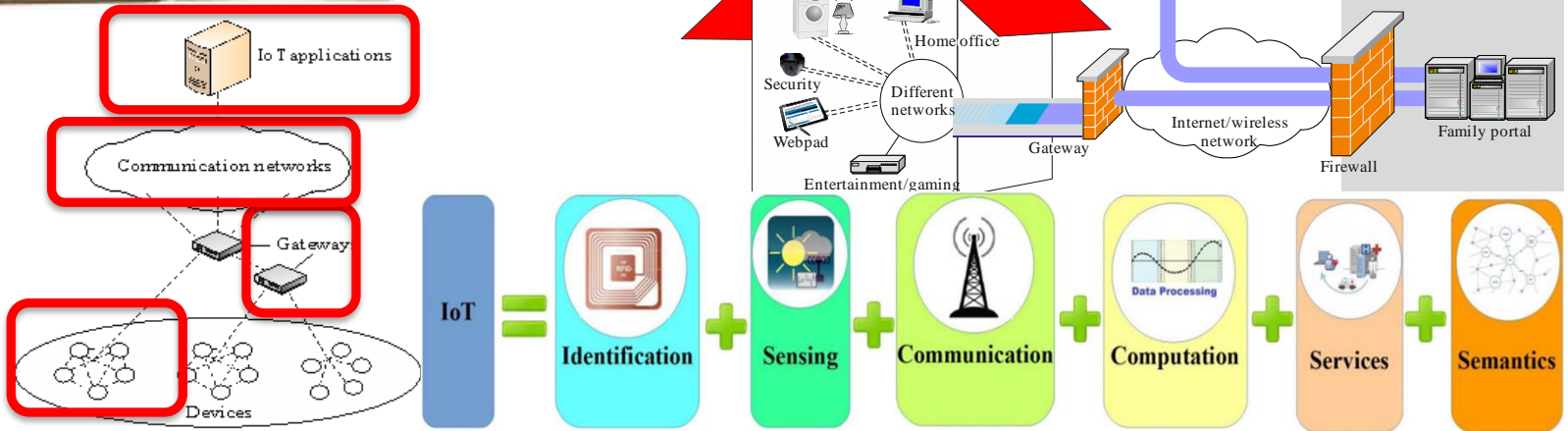
and think IoT, in terms of which element provides ledger services..



Let's have a closer look at the ledger!

- Data?
- Transaction?
- State?
- Finite State Machine?

and who maintains the ledger in a typical IoT setup..



Who is responsible for the ledger update and validation?



- Things?
 - Home appliances
 - CCTV cameras
 - Wearables
 - Medical equipment
 - Cars
 - Web services
 - Sensors/Valves
- Gateway?
- Service Enablement platforms?
- IoT Platforms?
- Software/Service?
 - Autonomous? (e.g. smart contract)
- Or a dedicated DLT asset issuer? → new elements?
- Or a dedicated DLT asset validator? → new elements?

Incentives!

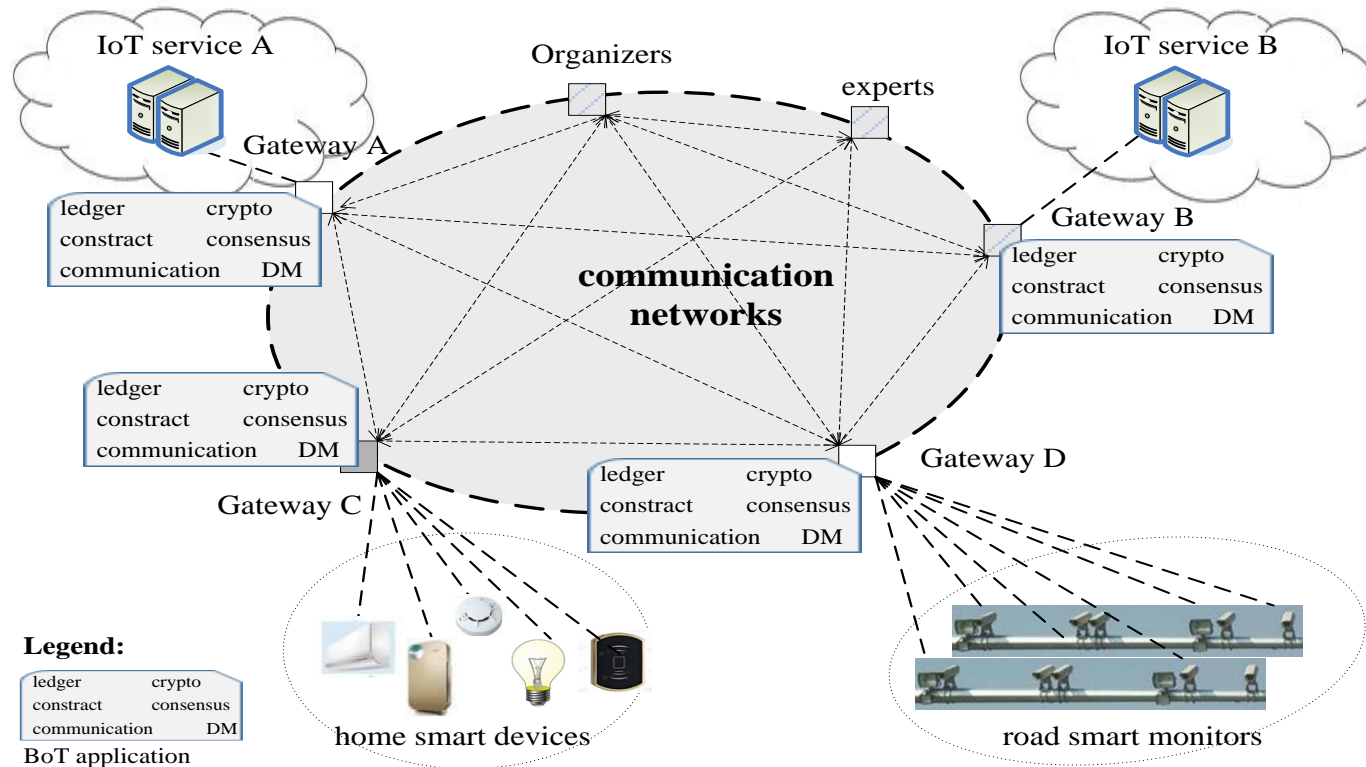
- Blockchain P2P participation depends on the idea of incentives.
- Transaction fees may not be suitable in the future, specially in micropayments cases.
- New innovative incentive protocols are needed for many type of deployments .. e.g. IoT deployments.

USE CASES

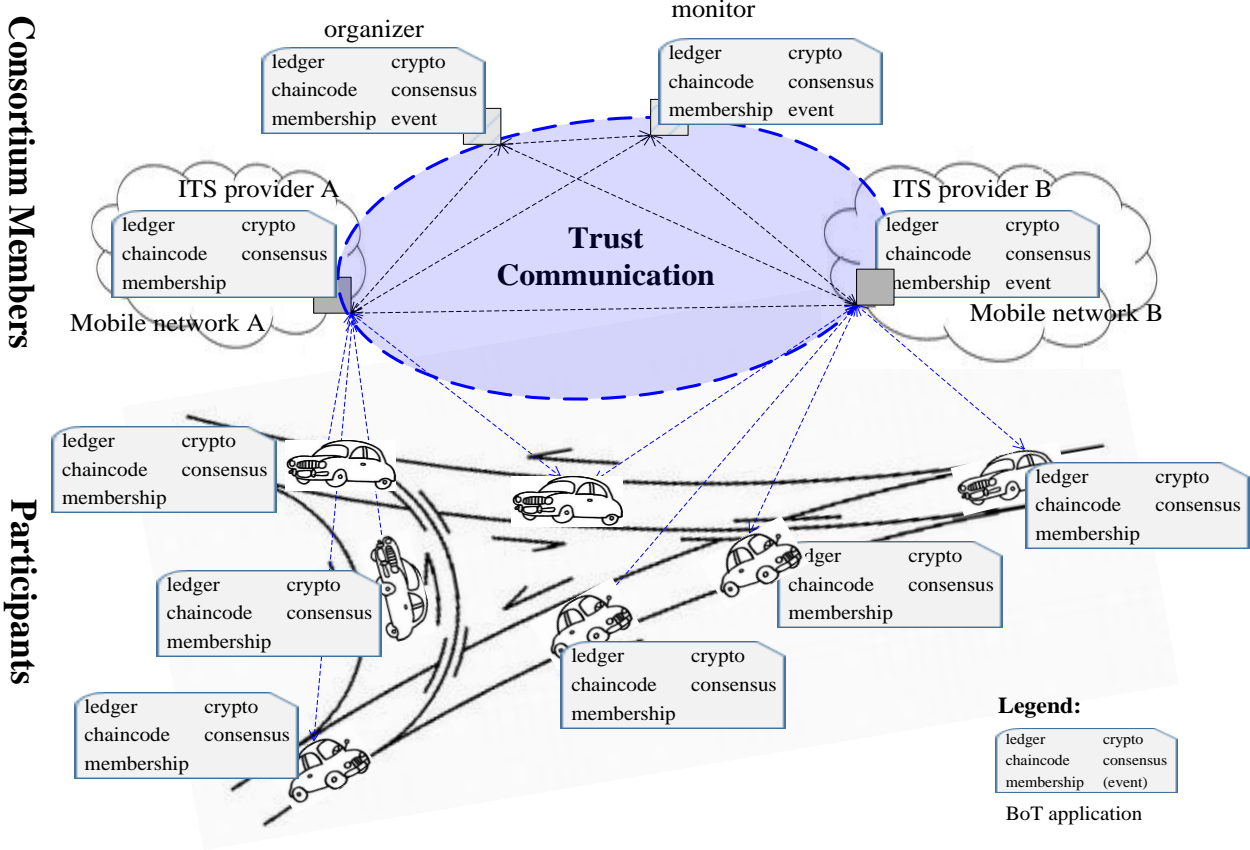
DLT Use Cases .. It really depends!

- Is it about management and control? Or about trust?
- Do we want to get rid of .. say the centralized platforms?
- Do we want to operate in trust less environment?
- DLT Client and validation protocols are needed
- Implementations in lower or upper layers
 - Lower layers need high computing capabilities!
- Platforms are needed!

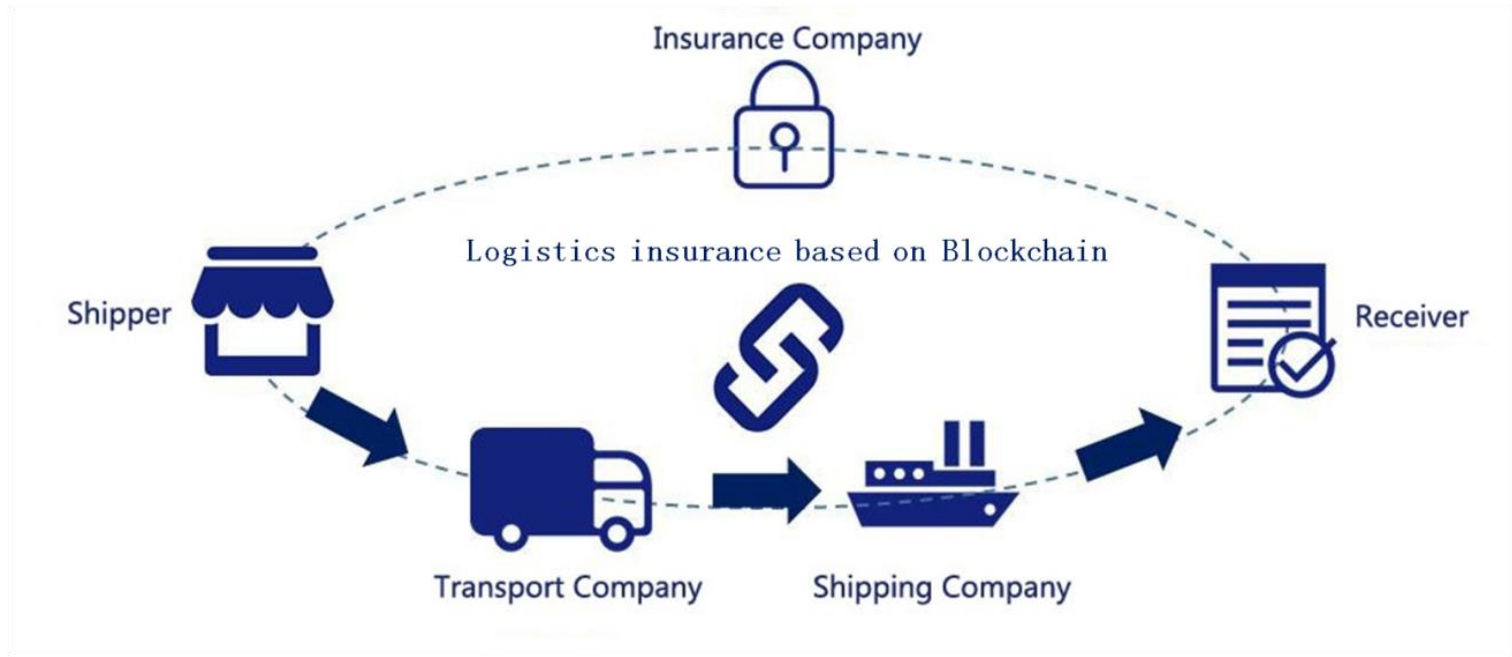
Use Case# 1: Using BoT to mitigate DDoS attacks from hijacked unsecure IoT devices



Use Case# 2: Using BoT to improve ITS for trust data exchanges



Use Case# 3: Using BoT to improve workflow and shipments transaction traceability



Thank you

Ramy Ahmed Fathy, PhD
ramy.ahmed@ieee.org