2018 IEEE International Conference on Vehicular Electronics and Safety (ICVES)
September 12-14, 2018, Madrid, Spain

Hirofumi Onishi
*Alpine Electronics Research of America, Inc.*
Torrance (CA), USA

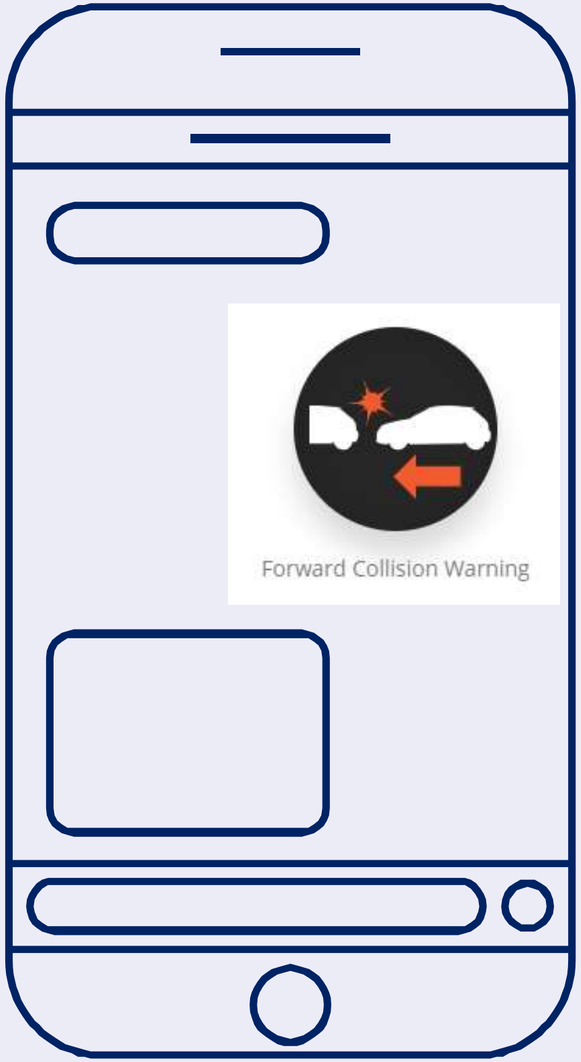
# A Survey:Engineering Challenges to Implement VANET Security

# Outline


VANET
Cyber-risks
Security mechanism
Hackers motivation
Block chain

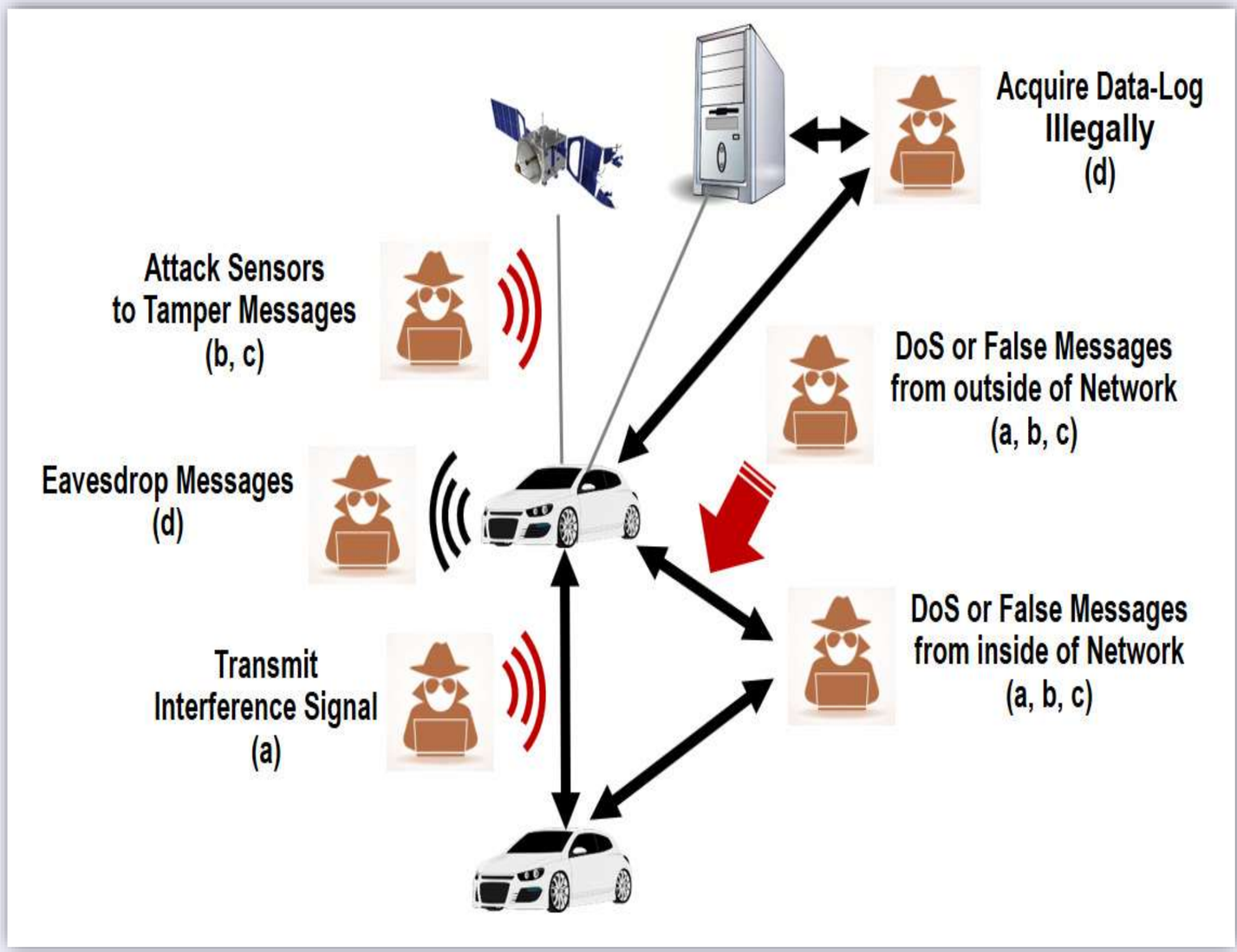
# The advancement of ICT, IoT, AI, Big Data and 5G

- Short communication latency
- High speed transmission
- More reaction time for human to confront
- For more advanced safety and convenience




Crash warning applications with VANET are not designed to control vehicles directly, therefore, they would not threaten road-users immediately [3]

# Various hackers motivations




**Attack (surface) types on VANET**

- Motivation
- Examples

**a**

- Blocking true messages.
- Radio interference
- DoS(Denial of Service)

**b**

- Sending false messages, and degrade drivers trust on these applications
- transmit false messages from the inside/outside of the network

**c**

- Sending false messages, and get unfair advantages for unscrupulous drivers
- manipulating sensors/devices that generate their messages

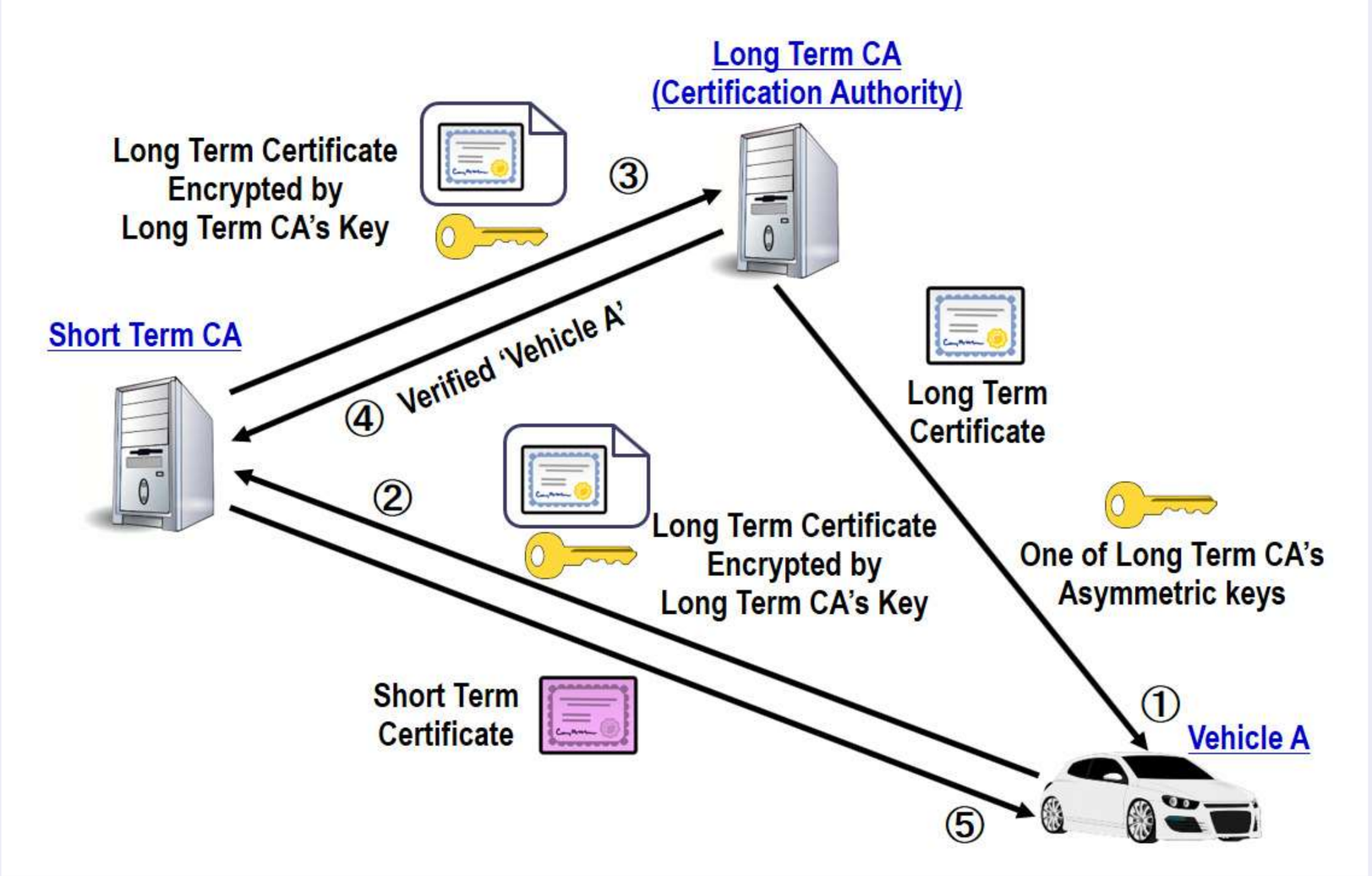
**d**

- Steal PII (Personally identifiable information),e.g. drivers driving histories
- eavesdrop messages from the target vehicle locally
- acquire the driving history of the target vehicle stored on the vehicle or a server

# Security Mechanism

## ➢ CA (Certification Authority)

- Only certified vehicles can transmit messages.
- Neighboring vehicles can easily identify if certified vehicles transmitted the message.




# Concept: Privacy protection on VANET [4]

## ➢ Certificates Revocation Lists(CRL)

- CA and vehicles monitor misbehaviors (suspicious certificates or messages)
- Detected misbehaviors are reported, and per necessity, reported vehicles' information is added on the CRL, then the CRL is circulated to all vehicles in the network.

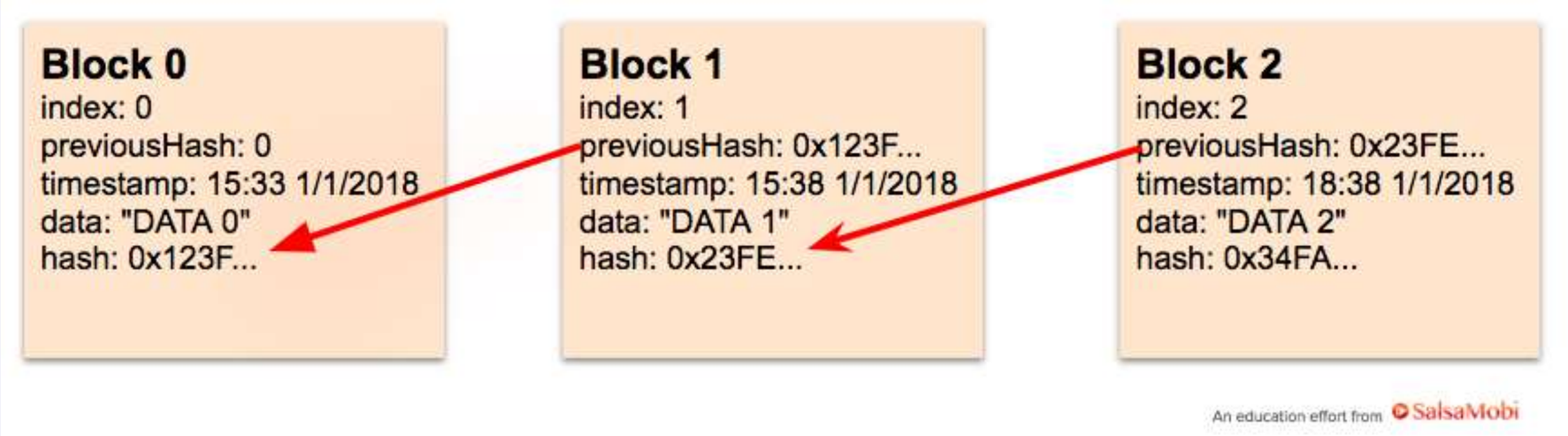
# ➢Privacy protection mechanism

- Anonymity : Messages between neighboring vehicles should not include keys
- Non-traceability : ID of adjacent node needs to be updated several times a day.
- Security : Message logs should be securely stored, and even once message logs stored on vehicles or servers were disclosed, these logs should not be abused.

# Security mechanisms Challenges

- Above mention security mechanism on VANET need centralized communication network
- Trade-off between safety and security
- Performance of encryption, decryption, and certification
- Physical-type attacks
- Privacy infringement

# Methods

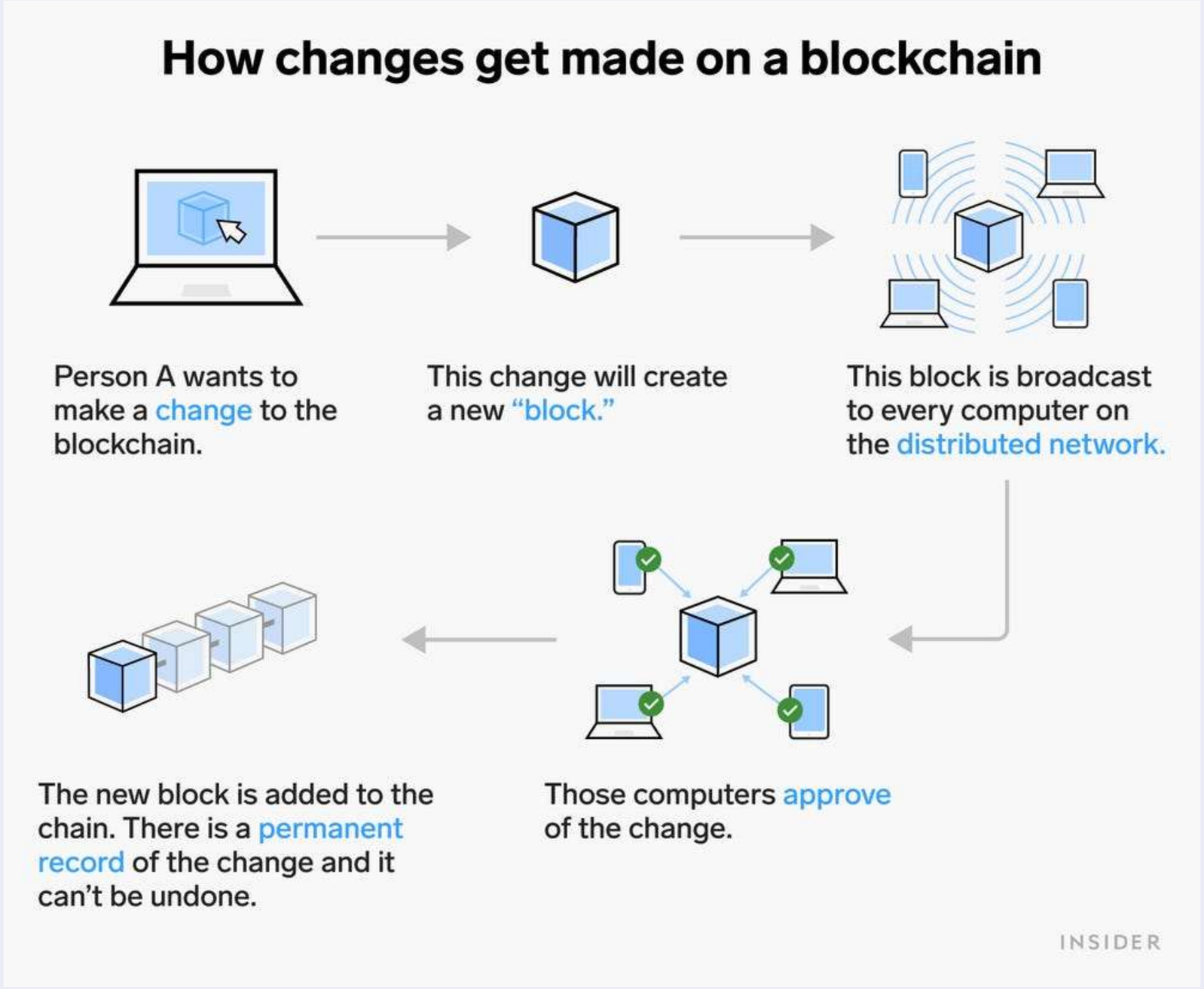



**DLT (Distributed Ledger Technologies)**

## Blockchain

- A block contains a set of transactions Creating a chain of block linked with each other[1]

- Decentralized and Immutable




Proceedings of Blockchain[2]

# Blockchain potential and application

◆ Manufacturing and logistics :

Strong resistance, lack of need of CA, record location, date, and machinery

◆ Maintenance and inspections :

repairs/inspections responding to recalls

◆ Ownership :

Control the insurance related information :

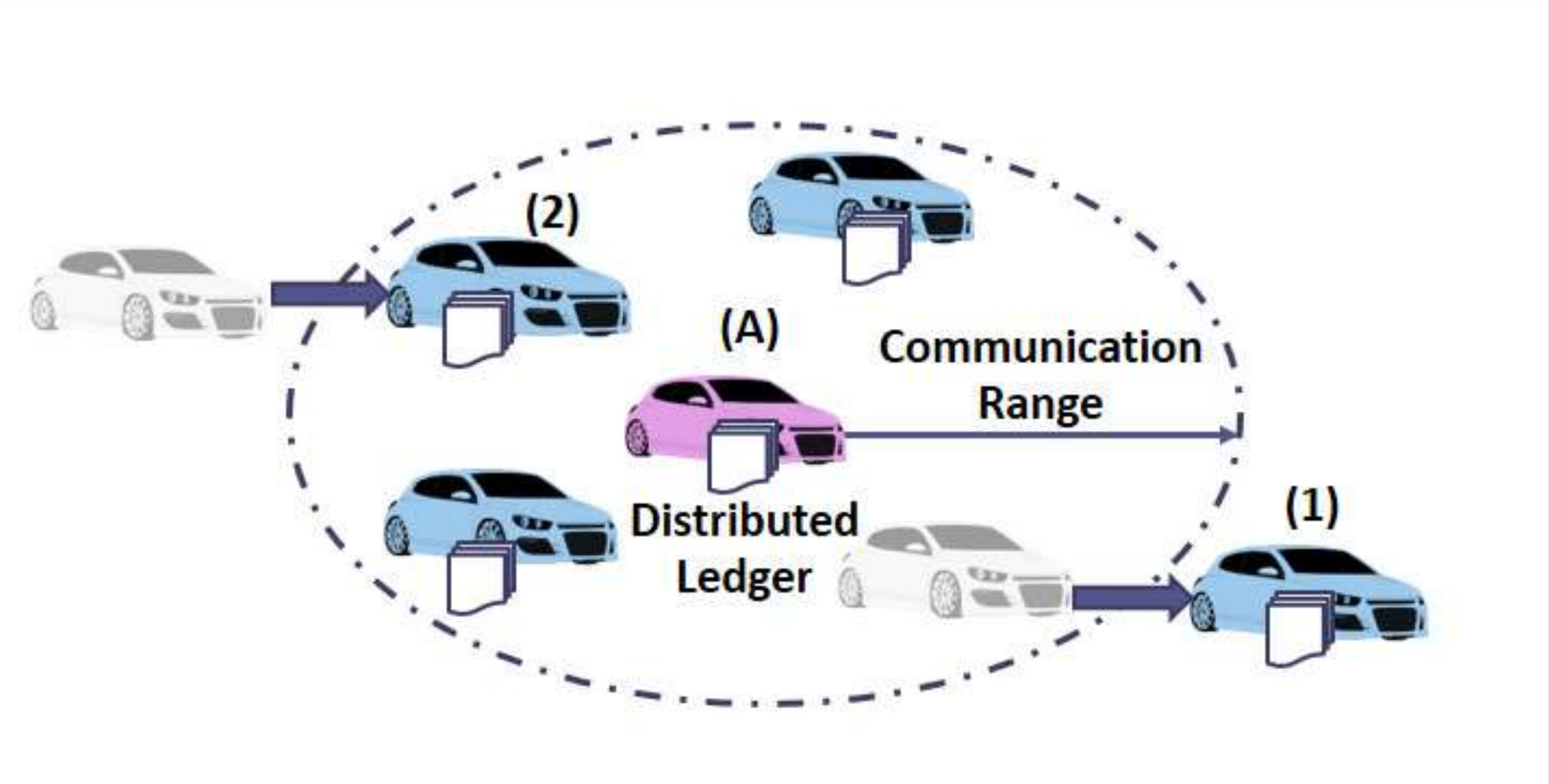
◆ Financial :

car-sharing/electric-charging/mobile payment/parking/tolling fee

# Blockchain limitations

- Power Use
- Cost
- Time-Consuming
- Immaturity
- Legal Formality

# Frequent network topology




It is difficult to synchronize distributed ledgers of individual vehicles without a centralized network which covers all vehicles in the area.

# Results

| | | VANET | VANET + (DLT)Blockchain |
|---|---|---|---|
| framework | | CA | DLT |
| Faces problems | frequent network topology | | ✓ |
| | Consensus process (Blockchain response) | | ✓ |
| | Sufficient innocent vehicles (51% ISSUE) | | ✓ |
| | Privacy protection | ✓(need) | ✓(need) (long-term, short-term certificates) |

# Discussion

Currently proposed security mechanism requires the communication infrastructure to make CAs and individual vehicles exchange certificates/security-keys.

In so doing, VANET would lose its largest advantage, i.e., not needing a network infrastructure.

# References

[1] https://miro.medium.com/max/1400/1*KYYL_lfp6tN4C9Sg_XF7xQ.webp

[2] BIOTC '21: Proceedings of the 2021 3rd Blockchain and Internet of Things Conference July 2021

[3] Armor, “The Black Market Report,” (Mar. 2018)./app/uploads/2018/03/27222933/2018-Q1-Reports-BlackMarket-DIGITAL-min.pdf

[4] K. Oka (ETAS), “Security Technique to ensure V2V and V2I Security,”(Sep. 2015), (Japanese).at monoist.atmarkit.co.jp/mn/articles/1509/16/news009.html

[5] H. Onishi, et al. “Approaches for Vehicle Cyber-Security in the US,”(20174086), International Journal of Automotive Engineering 8 (2017)1-6.at www.jstage.jst.go.jp/article/jsaeijae/8/1/8_20174086/_pdf.