Blockchain for 6G & Internet of Things

NJUPT / online / 15.08.2021

Yan Zhang
University of Oslo, Norway


Iceland
Sweden
Finland
Norway
Oslo
University of Oslo (UiO)
Denmark
United Kingdom
Ireland
Belarus
Poland
Germany
Ukraine
Kazakhstan
Austria
France
Romania
Italy

Norway - fact

Population	6 million
Oslo average temperature	• Summer (16 °C) • Winter (-3 °C)
Language	• Norwegian 挪威语 • English is very popular
PhD scholarship	420000 RMB/year

挪 威 奥 斯 陆 大 学
UNIVERSITY OF OSLO
UNIVERSITETET I OSLO

建校时间：1811年

学生：40000人

诺贝尔奖：5 位

IEEE Fellow：1 位

图灵奖：2 位

全球高被引科学家：6 位

UNIVERSITY OF OSLO, NORWAY

→ → → 世 界 百 强 大 学 ← ← ←

60#

Academic Ranking of World Universities (软科世界大学排名)

ACADEMIC RANKING OF WORLD UNIVERSITIES SINCE 2003

90#

US.NEWS Best Global Universities Ranking (US.NEWS世界大学排名)

BEST GLOBAL UNIVERSITIES U.S.News & WORLD REPORT RANKINGS

OUTLINE

Blockchain

Concept
Visions
Architecture

Blockchain for 6G

AI & Data Privacy
Federated learning
Blockchain & edge

Blockchain for IoT

Asynchronous
Federated learning
Efficiency

01

BLOCKCHAIN: CONCEPTS AND PRINCIPLES

Blockchain development

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the

- In 2008, Satoshi Nakamoto proposed Bitcoin for the first time in the paper “Bitcoin: a peer-to-peer electronic cash systems”
- At time 02:15:05, 4 January 2009, Satoshi created the first block in the Bitcoin system and left the message:
  - The Times 03/Jan/2009 Chancellor on brink of second bailout for banks

Two concepts: Blockchain and Bitcoin

Bitcoin ≠ Blockchain

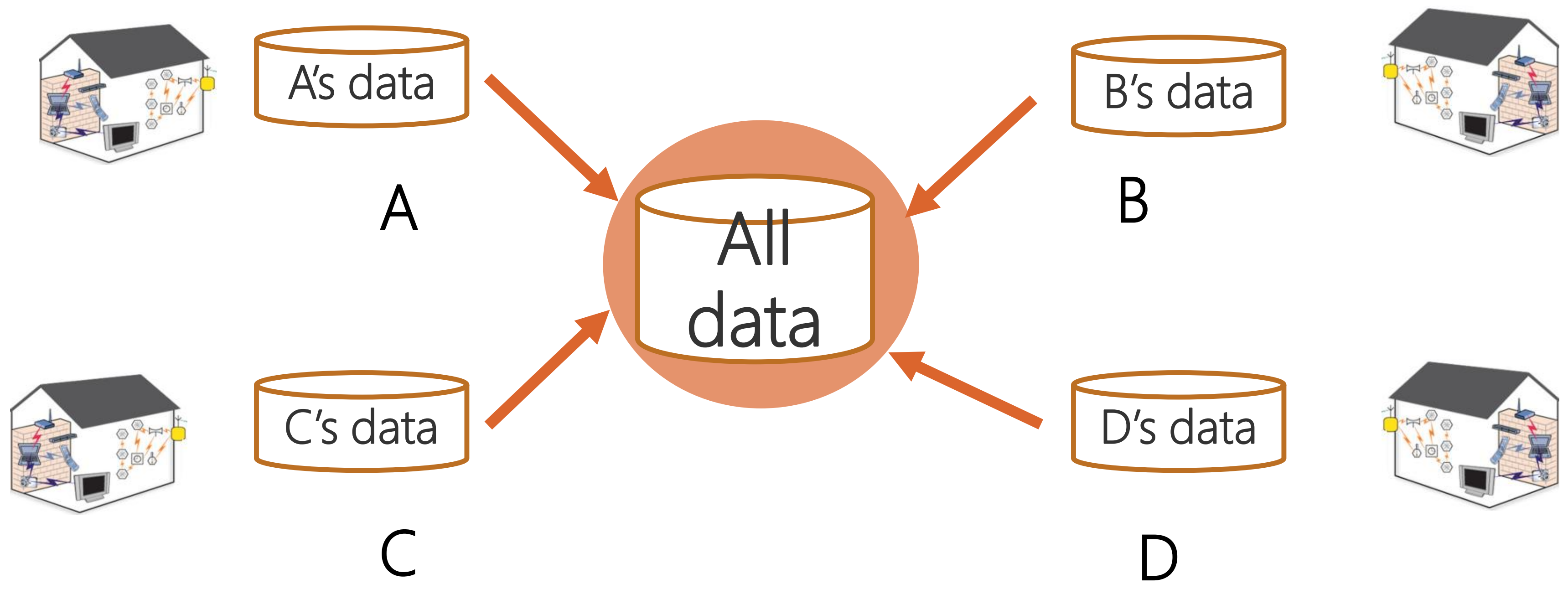
- **Bitcoin:** unregulated digital currency designed to bypass currency controls and simplify online transactions by getting rid of third-party payment processing intermediaries.
- **Blockchain and Bitcoin relationship:** Bitcoin was an application of Blockchain. Blockchain has applications far beyond Bitcoin.

中国央行即将推出数字货币DCEP （Digital Currency Electronic Payment）

- 央行将要推出的数字货币（DCEP）：基于区块链技术的全新加密电子货币体系。
- 2014 年，央行开始数字货币研发

- DCEP：不是现有货币的数字化，是流通中的现金的替代
  - DCEP 的价值只与人民币挂钩： DCEP与人民币可以1:1自由兑换
  - DCEP 具有无限法偿性: 无论支付的数额大小，收款人都不能拒绝接受
  - DCEP 不需要账户就能实现价值转移： “双离线支付”，收支双方都离线，也能进行支付
  - 资产的高度安全性： DCEP 由央行直接发行，不存在商业银行和企业倒闭的问题

Traditional central trusted authority

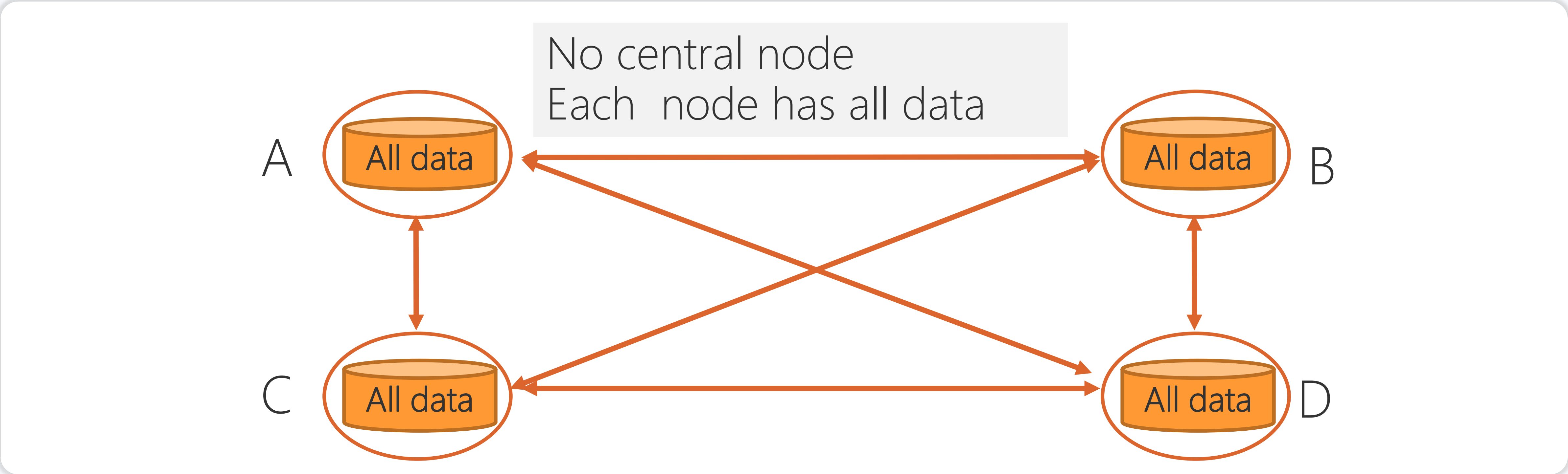


- Individual person: own her data
- Central trusted node: own all users' data, e.g., Visa, Mastercard, PayPal, banks, and Amazon. The center has full control of all data, it can search, add, delete and modify data.

Traditional central trusted authority

- A has data exchange with D (e.g., transaction)
  - A sends a request to the center
  - The center answers the request and connects D
  - Data processing
- Q: any disadvantages of such architecture?
- Very high working load in the center since all transactions go through the central node; the central tends to become malicious; the single failure point of the central node by cyber attacks.

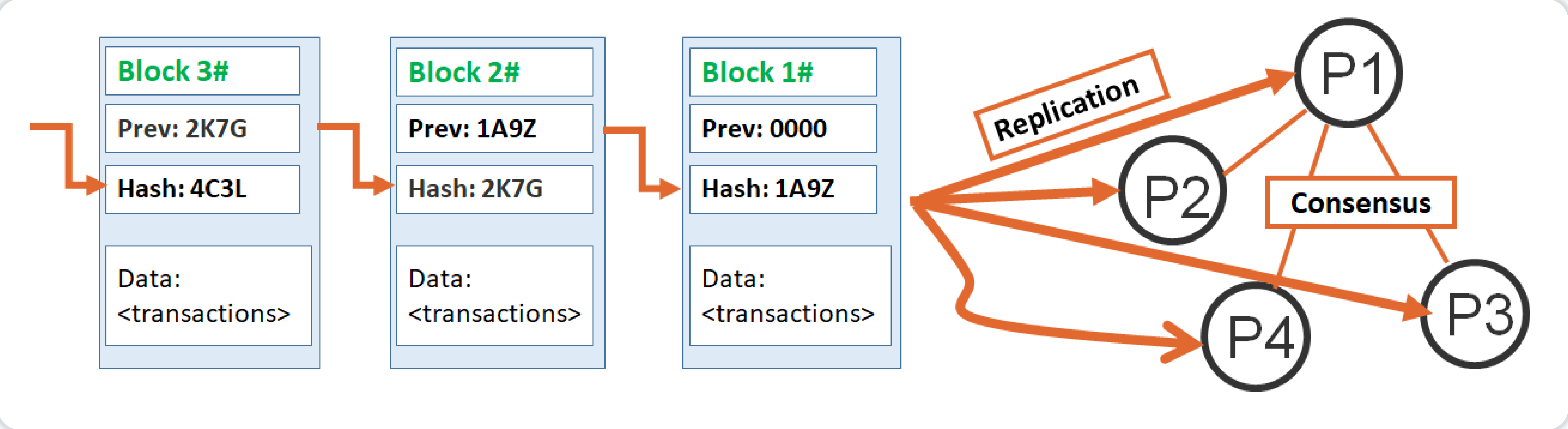
Blockchain concept



- **Blockchain:** a globally maintained and shared distributed database. Everyone has all same database and there is no central organization to manage the database.
- Blockchain records the transactions permanently. The data can only add and search; the data cannot be deleted or modified.

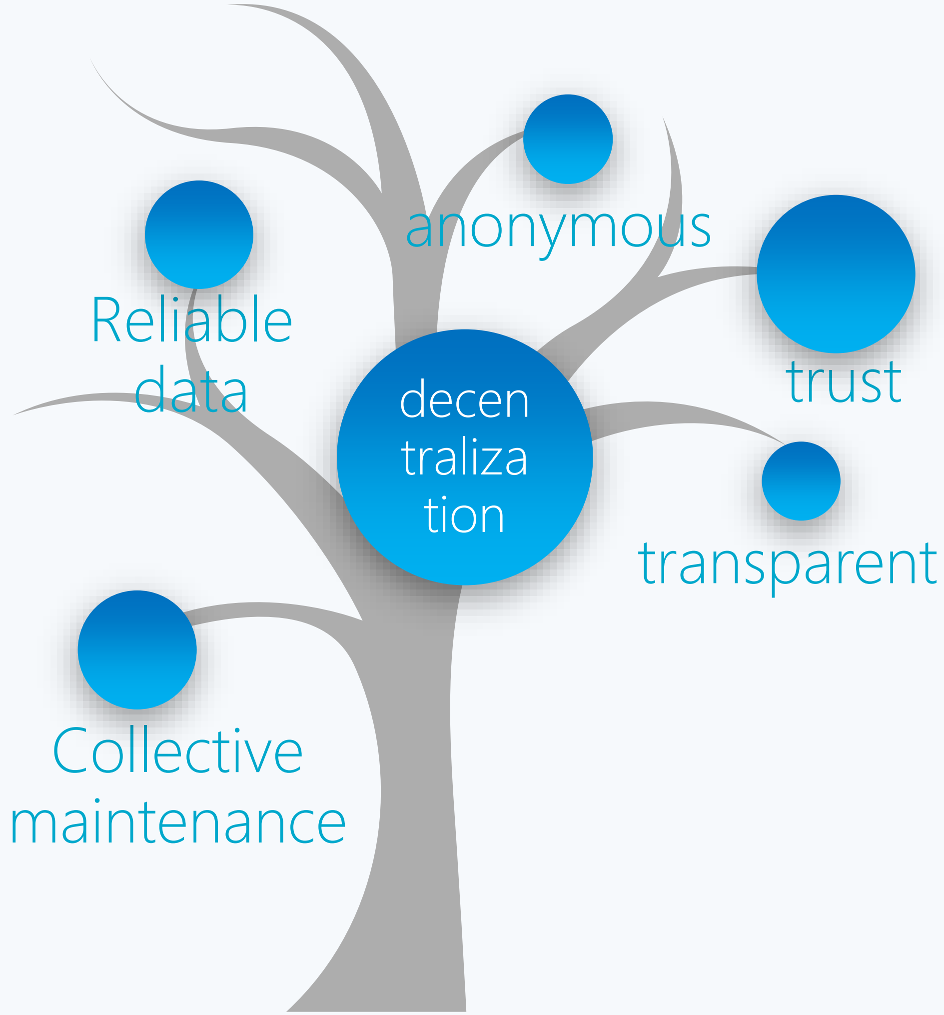
Blockchain principle

Blockchain data structure (replicated at every peer) Peer-to-Peer network



- Three types of Blockchain: public, private, and consortium blockchain
- Features: decentralization, data privacy, untamperability, diversity data source

Blockchain features



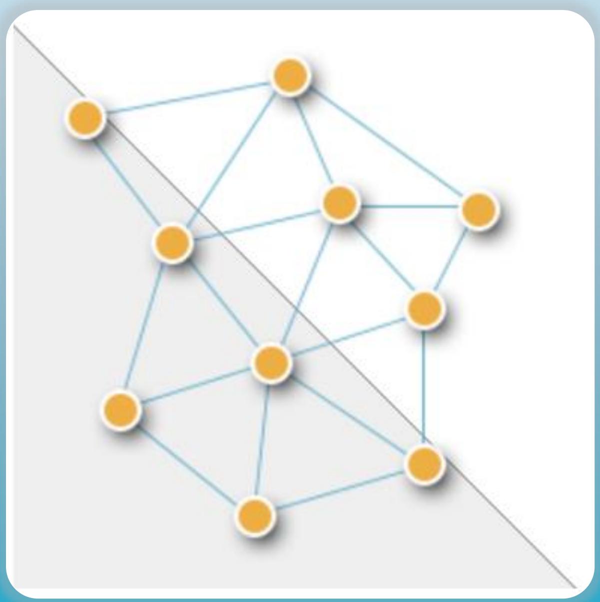
注：这一页借鉴北理工祝烈煌教授的内容

1. No central node in the network. Any two nodes are equal in terms of rights and obligations
2. The data are jointly maintained by all nodes, and each node shares rights and obligations
3. Digital signatures and consensus protocols ensure the authenticity of the data
4. Open source program ensures that ledgers and business rules can be reviewed by everyone
5. No trust issues while transactions are conducted without a third-party
6. The problem of trust is resolved, the two parties of the transaction do not need to know each other, and the transaction is conducted anonymously since the trust problem is solve

Blockchain types

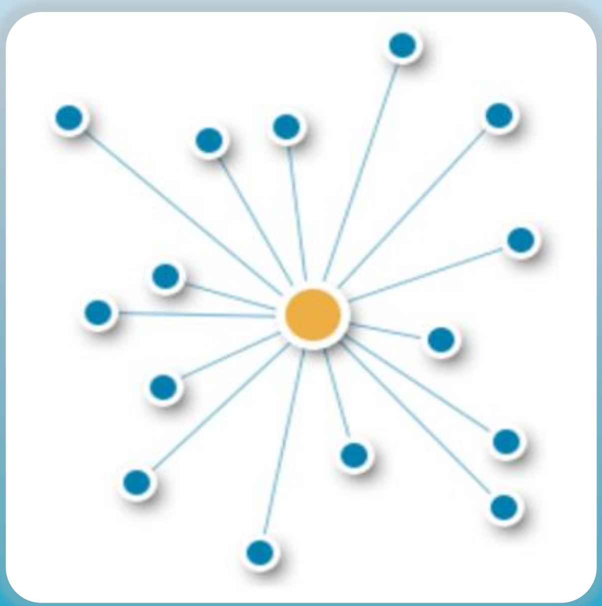
Public

- No administrator
- Permissionless
- High cost



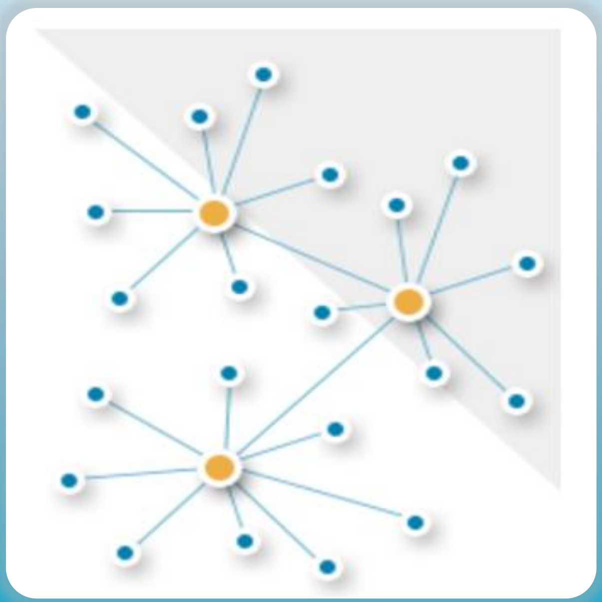
Private

- One administrator
- Permissioned
- Low cost



Consortium

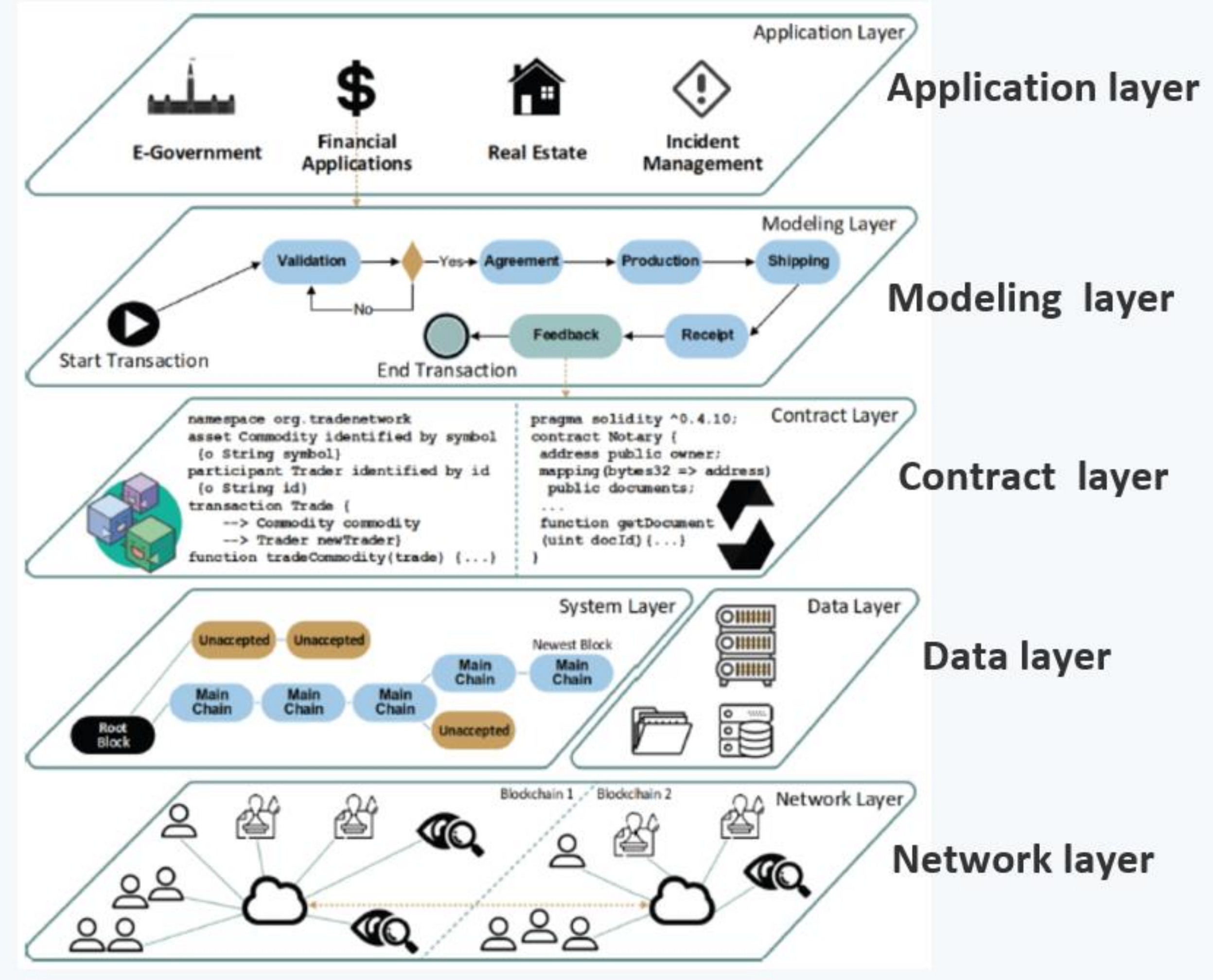
- Multi-administrator
- Permissioned
- Medium cost



Which type of Blockchain are used in the applications?

Applications		Public, Private or Consortium Blockchain
Bitcoin		Public
Bank		Private
Hospital		Private
Group of hospitals	SØRLANDET SYKEHUS  RIKSHOSPITALET	Consortium

Blockchain layered architecture

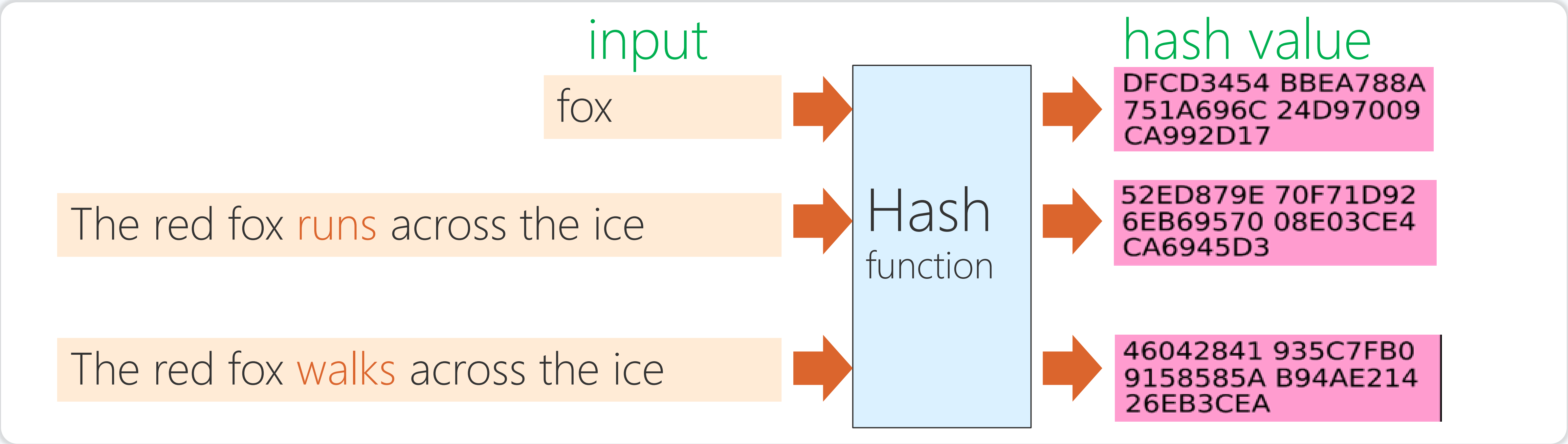


Blockchain provides
- Trust
- Security
- Scalability

Technologies

- Resource sharing
- Access control
- Content sharing
- Data sharing
- Energy trading
- Machine learning

Concept: hash function and hash value



- Hash function: takes any size input text and returns a fixed size string (i.e., hash value).
  - Easy to calculate a hash for any given data
  - Hard to calculate the original text that has a given hash
  - Two slightly different messages produce drastically different hash value
- Bitcoin uses a standard SHA-256 hash algorithm which generates a 256 bit hash value. For example: SHA256(123) = a665a45920422f9d417e4867efdc4fb8a04a1f3fff1fa07e998e86f7f7a27ae3

Blockchain data structure (I)

- **Block:** Blockchain is composed of blocks. Block refers to a group of transactions at a specific time and hash pointer of the previous block. Each block includes: header and body (i.e., data).
- Each block contains its own hash and also hash of the previous block. For instance, block 7 contains the hash of block 6, and block 6 contains the hash of block 5.
- A simple blockchain in Python: https://github.com/EricAlcaide/pysimplechain

Header

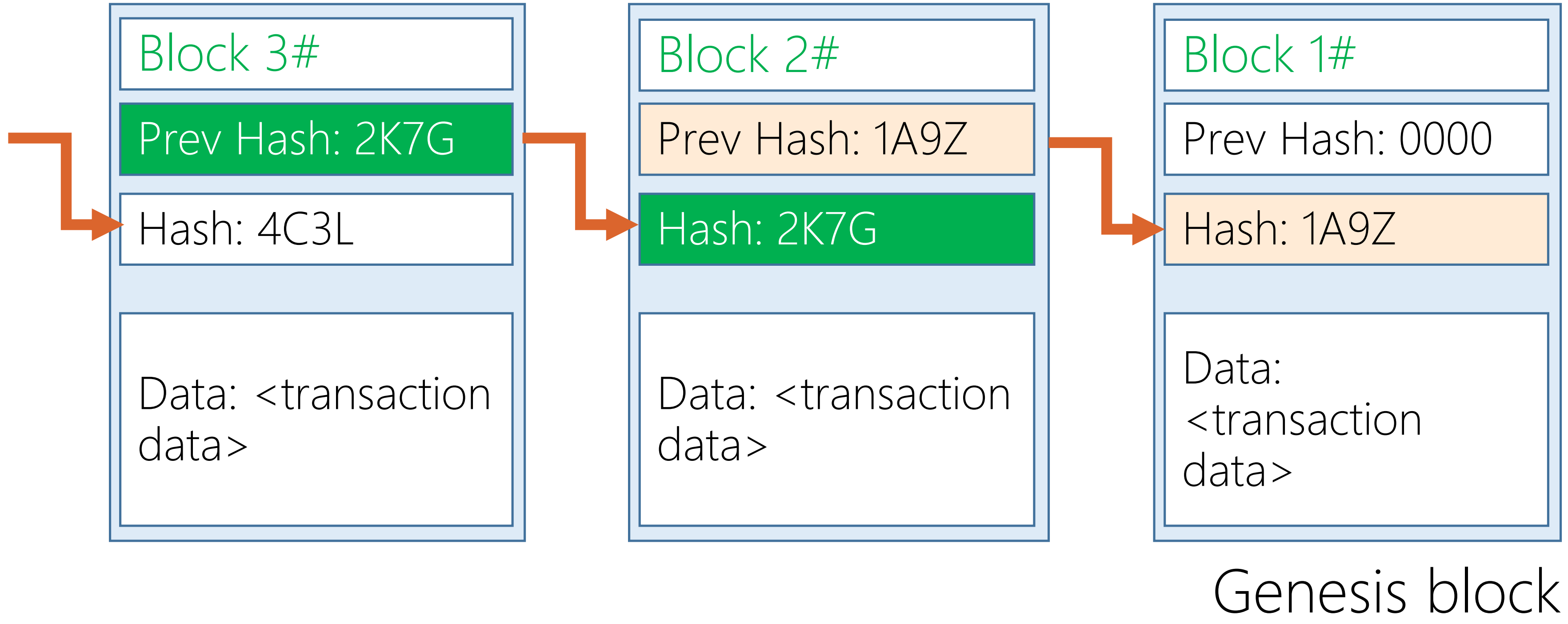
- Timestamp
- Block 6#'s hash value
- Block 7#'s hash value
- ....

Body

Transaction 1 data
Transaction 2 data
...
Transaction N data

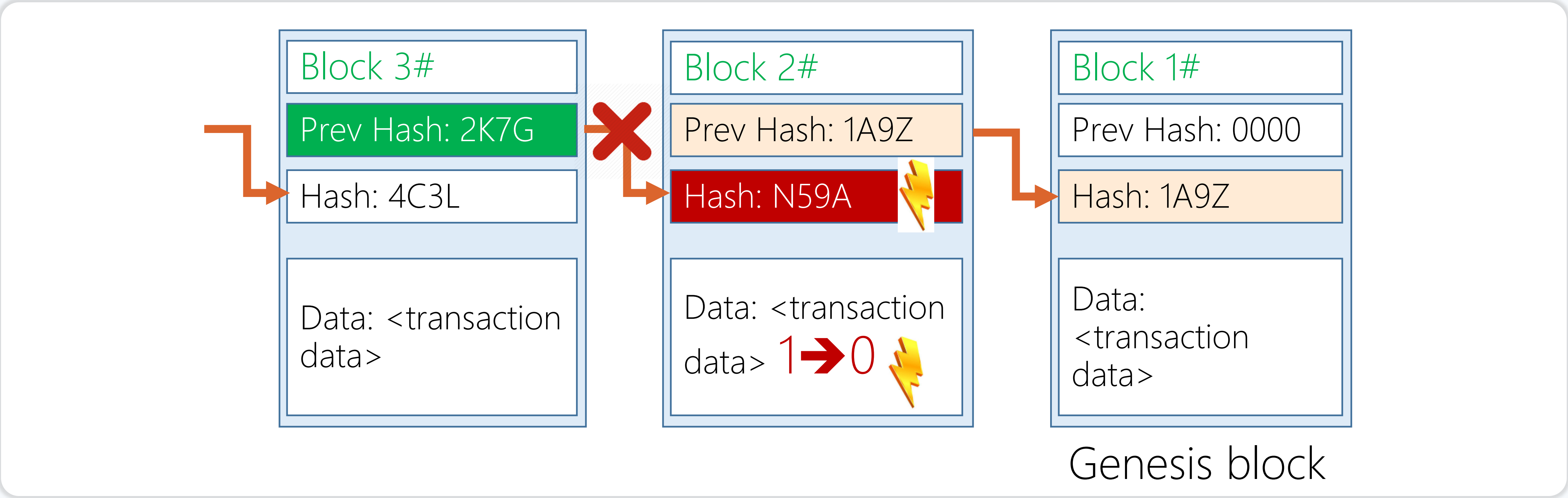
Block 7#

Blockchain data structure (II)



- Blockchain data structure: a linked list with hash pointers used to record all transactions. New blocks are added to the end of the chain.
- Hash pointer: gives you a way to retrieve data along with the hash of the data. A regular pointer only gives you a way to retrieve data.

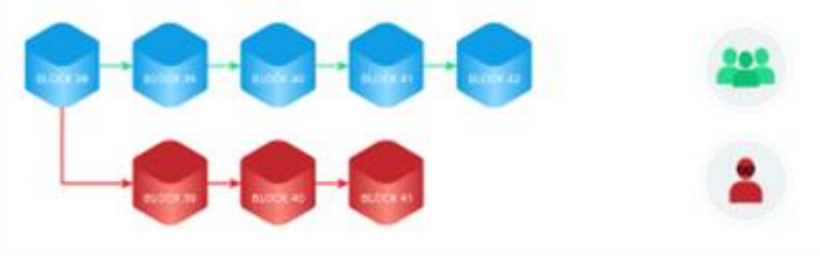
Tamper-proof mechanism



- **Tamper-proof:** an adversary is not able to tamper data in any block without getting detected.
- If anyone changes the data in Block 2, even just one bit from 1 to 0, the hash value of this block changes dramatically. Then, Block 3#'s "Prev Hash" is not same as Block 2#'s hash value, this makes the whole chain invalid.

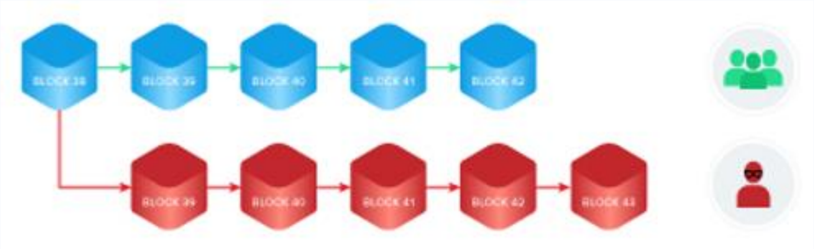
51% attack in Blockchain

- Definition: malicious attackers control a majority (51%) of the total network's computation power and collude to attack bitcoin or other crypto.

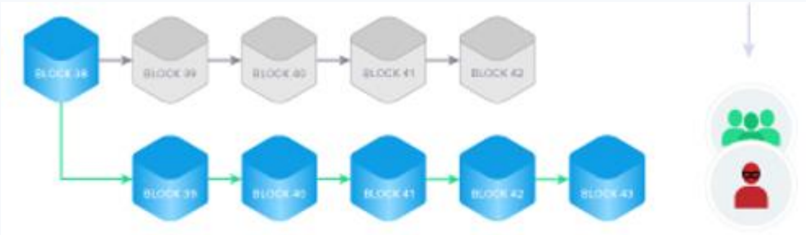


Trusted nodes add blocks by broadcasting them to the public chain

Malicious attackers add block in the private blockchain without broadcasting



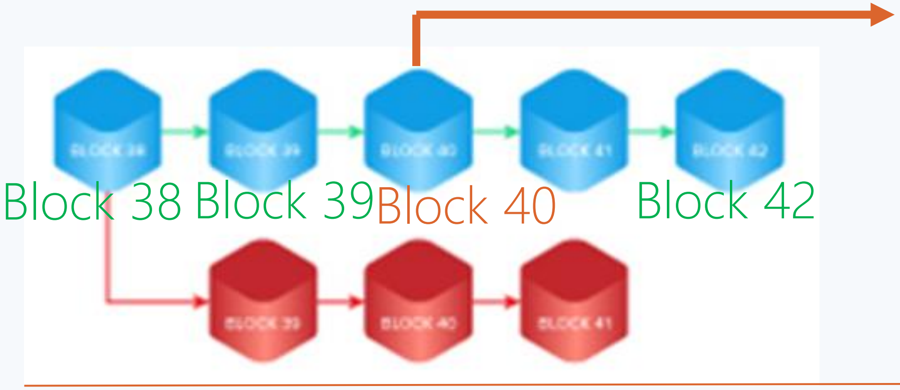
Attackers add block faster with majority computation power.
Rule in Blockchain: the longest chain wins



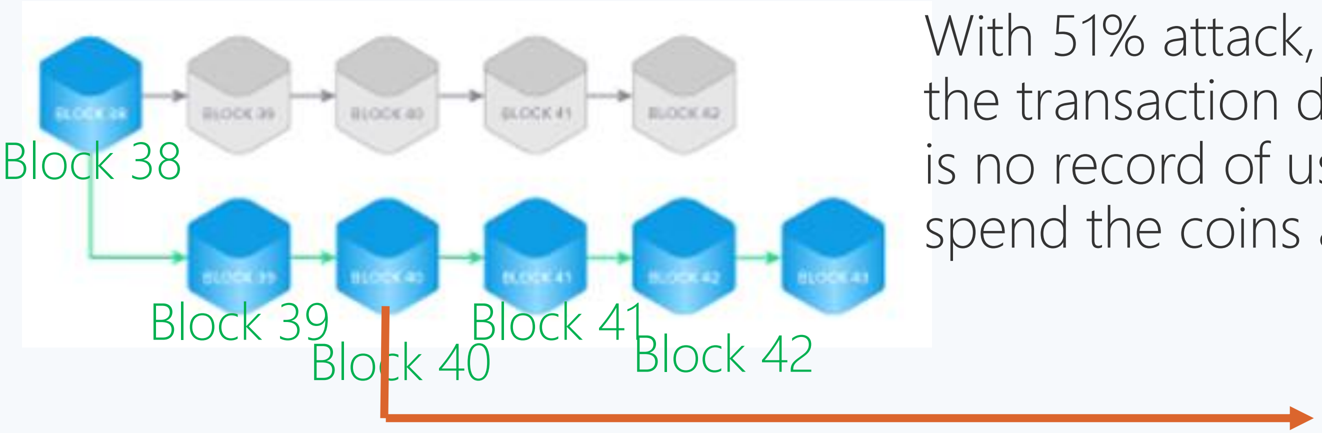
The old public chain is abandoned because it is shorter and its data is irrelevant. The attackers roll-back many blocks and start a new blockchain.

51% attack in Blockchain - consequence

- Consequence: spend coins twice (i.e., double-spending). The attacker can spend the same coins twice and buy two different cars.



Block 40 transaction data: attacker used coins to buy a car and this transaction is stored in Block 40.

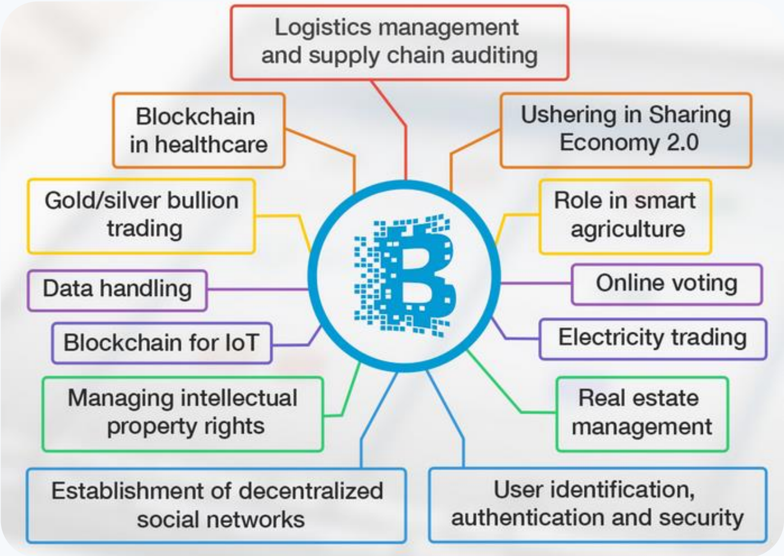


With 51% attack, the attacker starts a new Blockchain and the transaction data in the old chain is abandoned. There is no record of using the coins. The attacker can then spend the coins again to buy another car.

Blockchain applications in general

- Blockchain: decentralized database that keeps a record of all transactions.
- This provides a perfect way for systems to record transactions that should be transparent and permanent.

Sweden officially use Blockchain to register land and properties



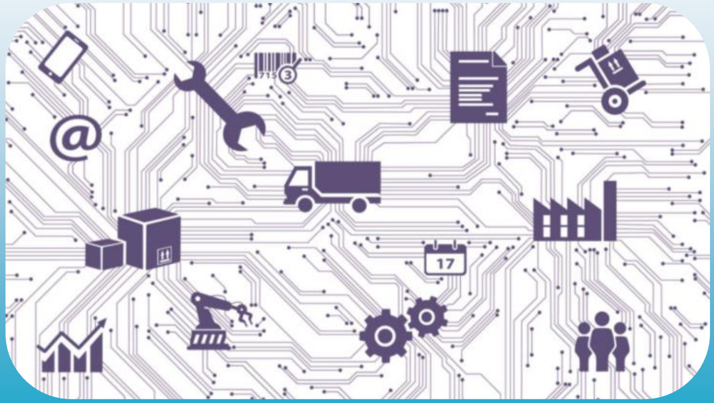
Second-hand car value certification

02

BLOCKCHAIN AND 6G AND IOT CONVERGENCE: WHAT IS THE ANGLE?

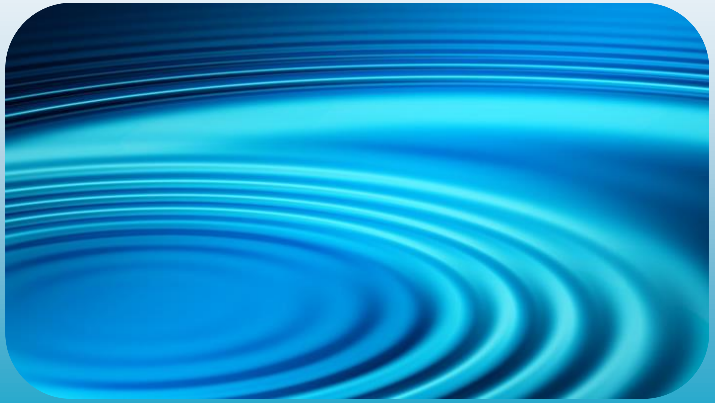
Full-* features in 6G

Full connectivity(全连接)



Full coverage (全覆盖)

Full spectrum (全频谱)

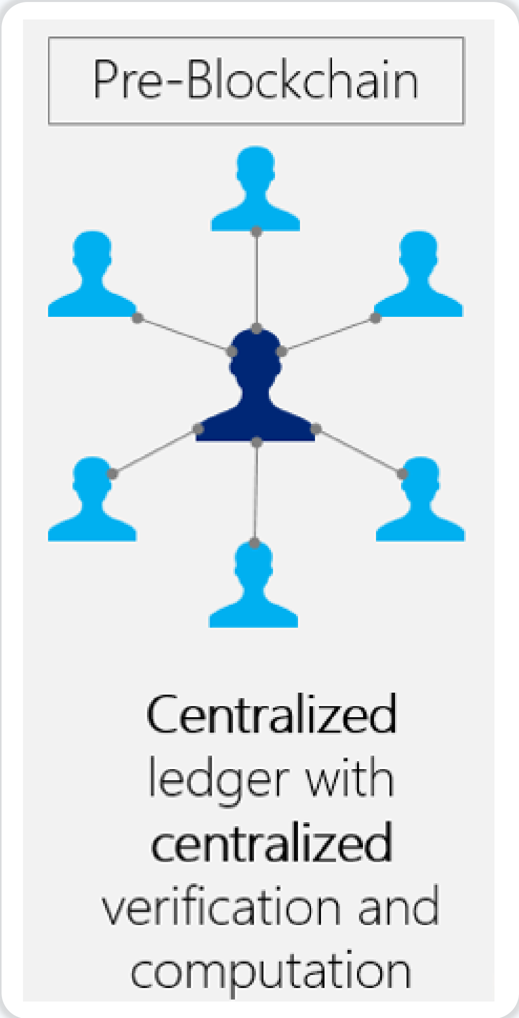


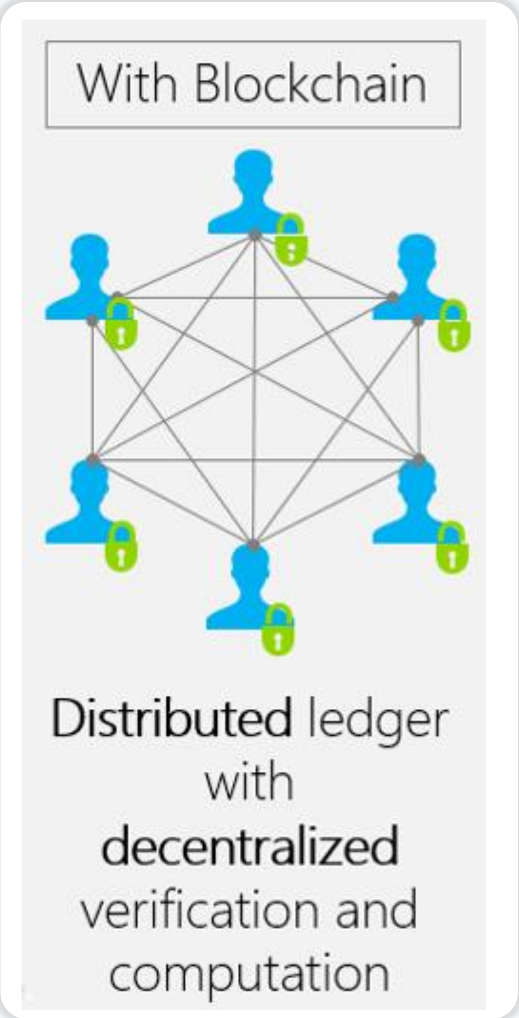
Full privacy（全隐私保护)

Full resources (全资源)

Full services (全服务)

Blockchain: centralized ➔ distributed computation and verification





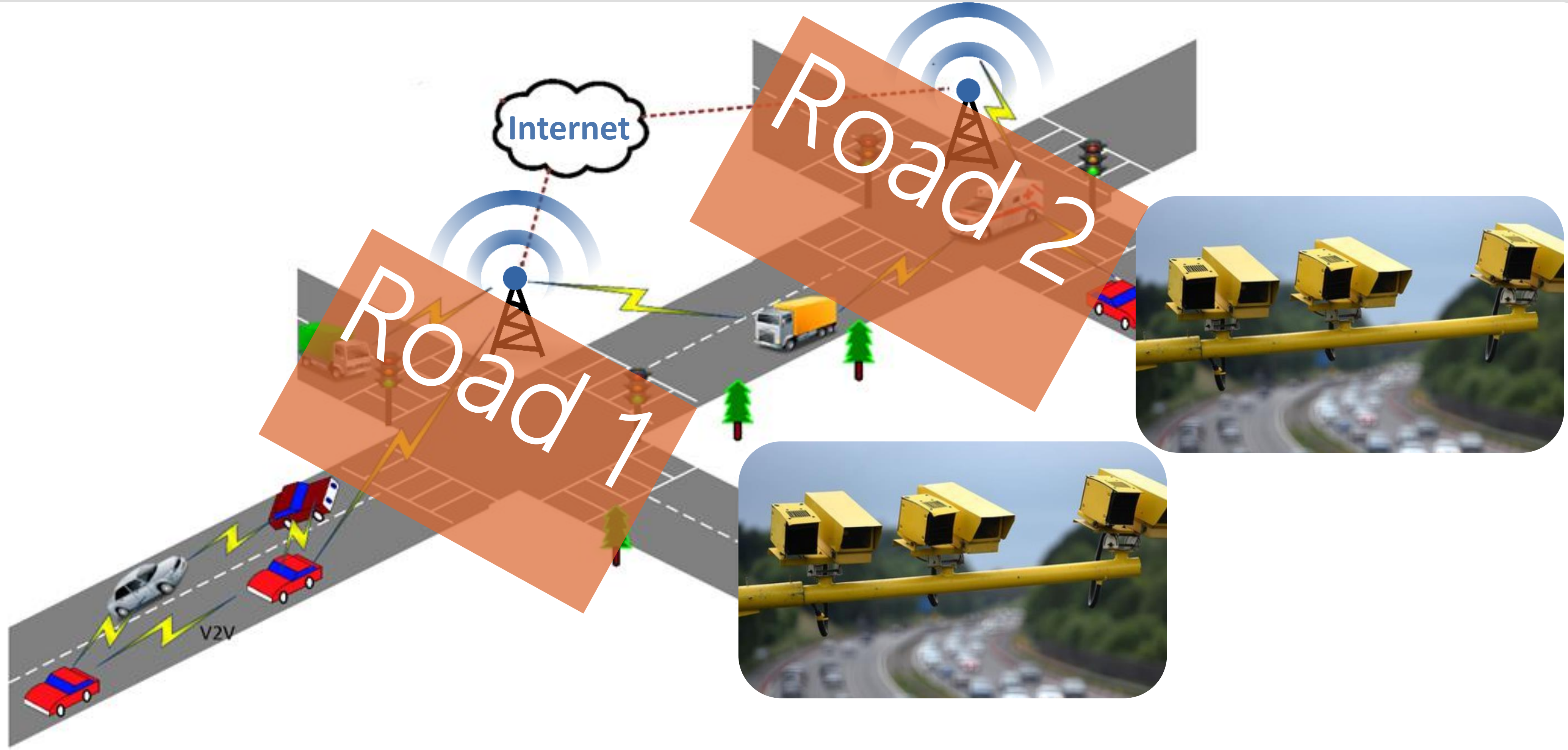
Three conditions to use Blockchain:

- distributed environment
- nodes do not trust each other
- nodes perform transactions

Role of Blockchain

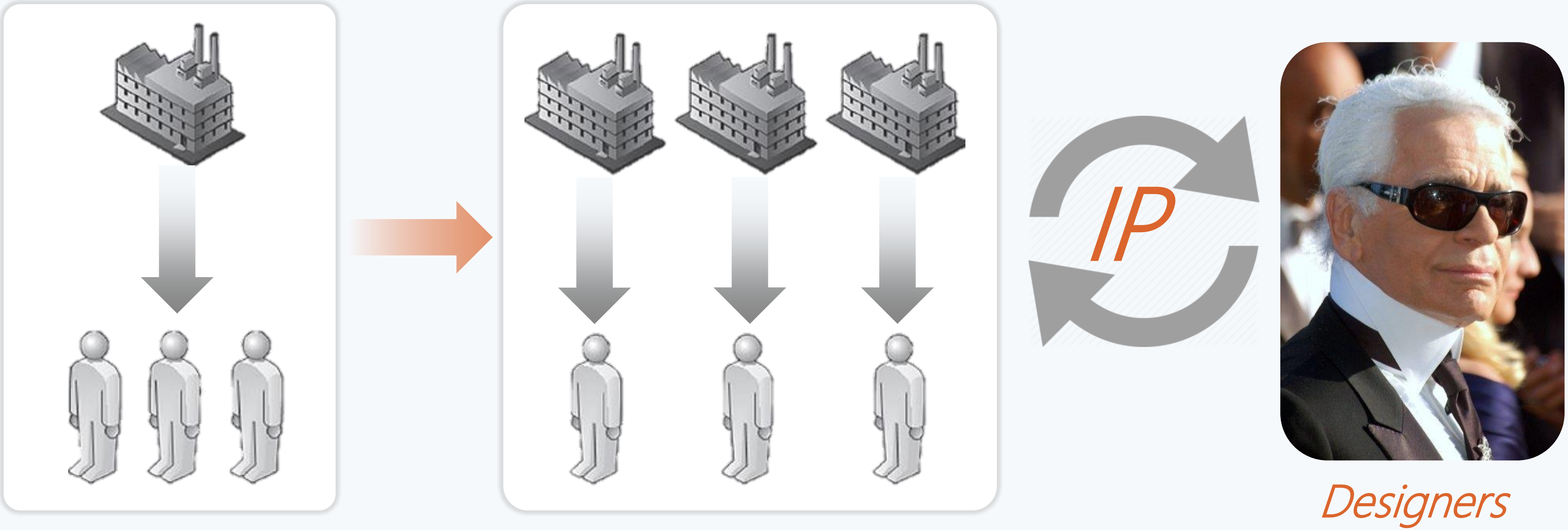
- Blockchain builds *trust* among untrusted participants in distributed environments

Centralized → decentralized operation: *transportation*



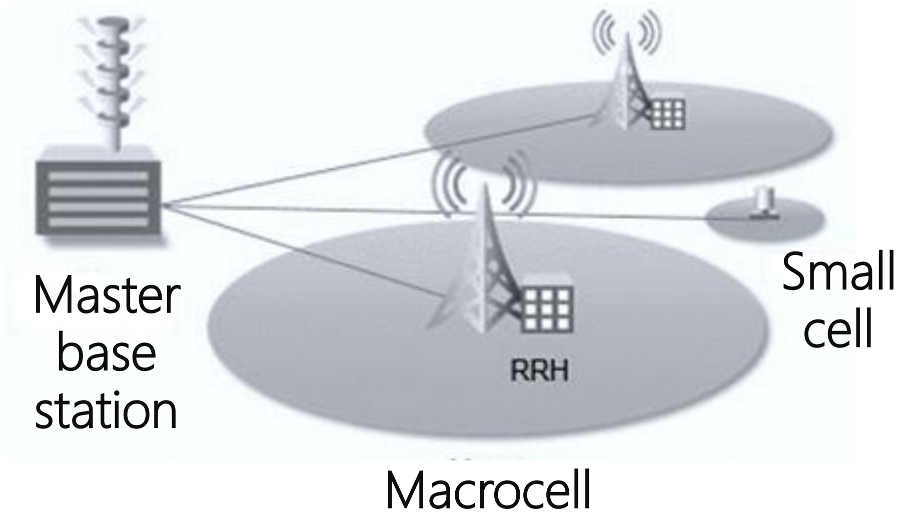
- Challenge: need new techniques to secure, store and trace the computation resources sharing in local environment

Centralized ➔ decentralized operation: *manufacturing*



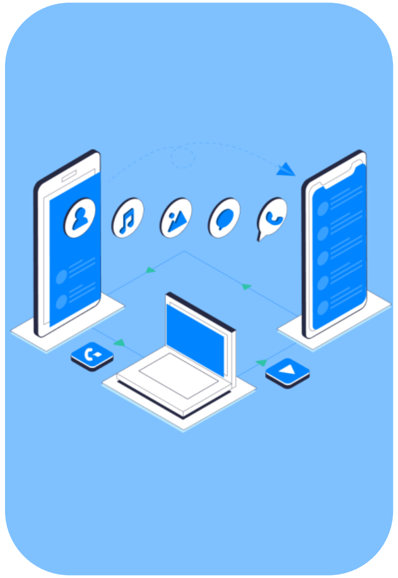
- Challenge: currently use third-party to exchange assets of value (money and intellectual property (IP) like designs or manufacturing information). We need a method to coordinate designers and customers peer-to-peer.

Centralized ➔ decentralized operation in 5G Beyond / 6G



Centralized networks

Vehicle-to-Vehicle



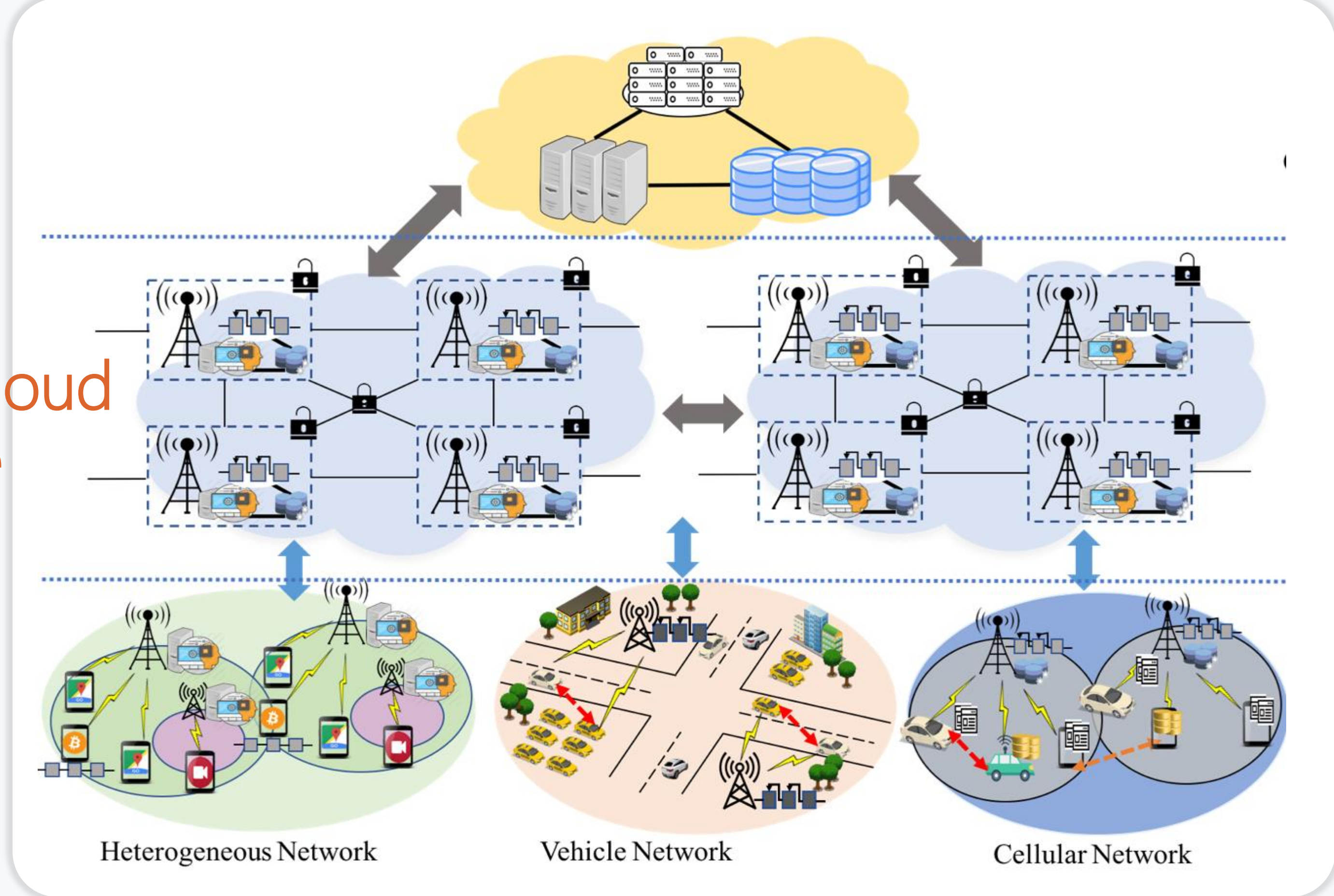
Device-to-Device

UAV-to-UAV

- **Challenge:** in distributed wireless networks, we need a method to secure the dynamic bandwidth sharing & trading among devices.

Blockchain for 6G networks: *end-edge-cloud perspective*

End-Edge-Cloud convergence



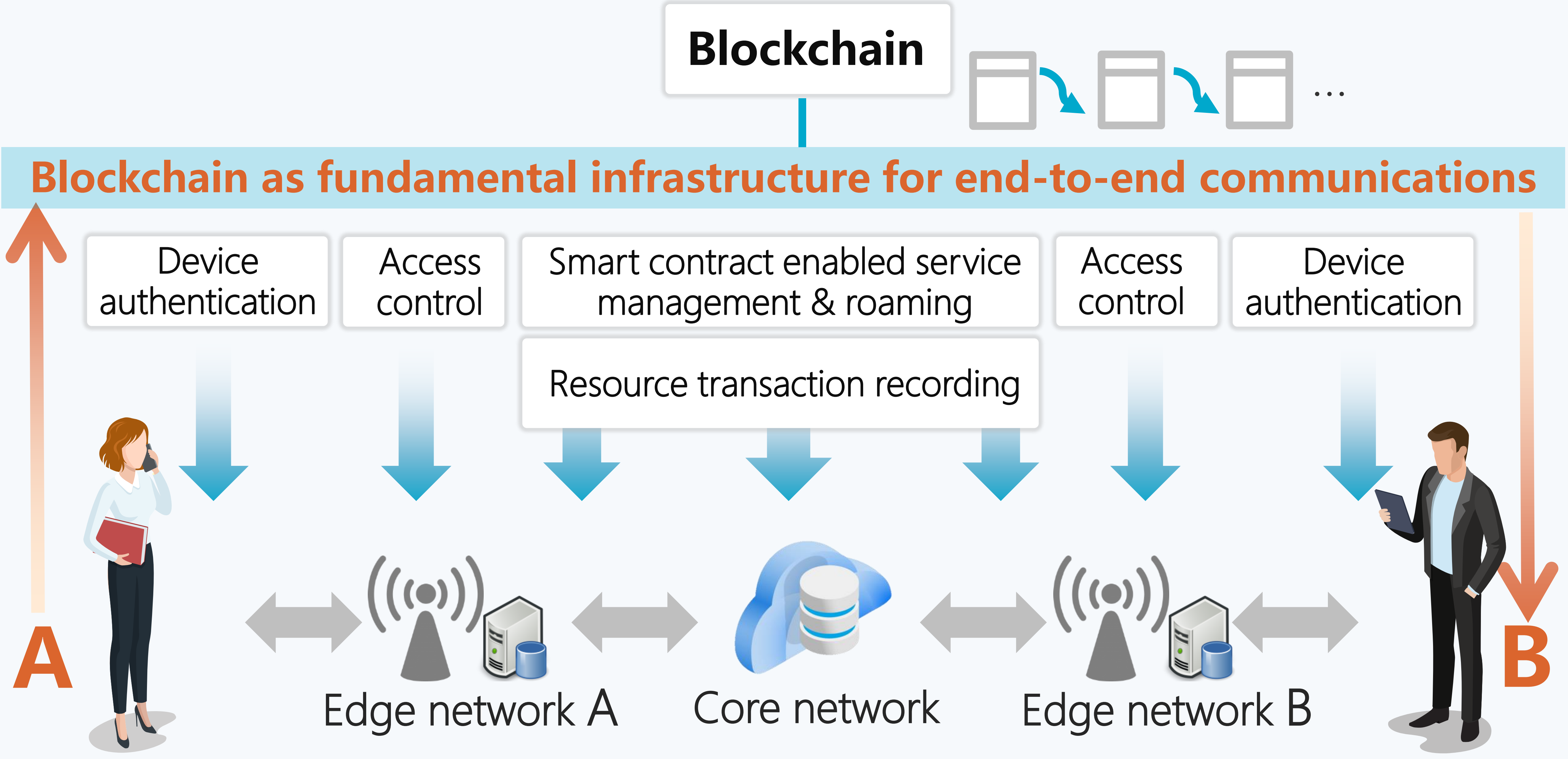
Cloud + Blockchain

Edge + Blockchain

Users + Blockchain

- End-edge-cloud integrated architecture of 6G/5G beyond network
- Blockchain enables a new secure, distributed, hierarchical networks

Blockchain for 6G: *end-to-end communications perspective*



Blockchain Research

Mainly business: bitcoin
Research focus on blockchain technology

ABCDE:
AI+Blockchain+Cloud+Digital+Edge

blockchain as fundamental infrastructure

2023?

2021

intelligent blockchain for 6G&IoT

2019.10.24: President Xi's remark

blockchain for IoT (energy, transport, UAV)

2017, since our TII paper

Our landmark study on *Blockchain for Smart Grid*

The first on Blockchain for IoT

We are *the first* to propose Blockchain for Smart Grid, and industrial IoT. This study has triggered the strong interest on Blockchain in communications society, computer society and IoT industry

The standard reference

This model is now *the standard reference* to explore Blockchain in IoT

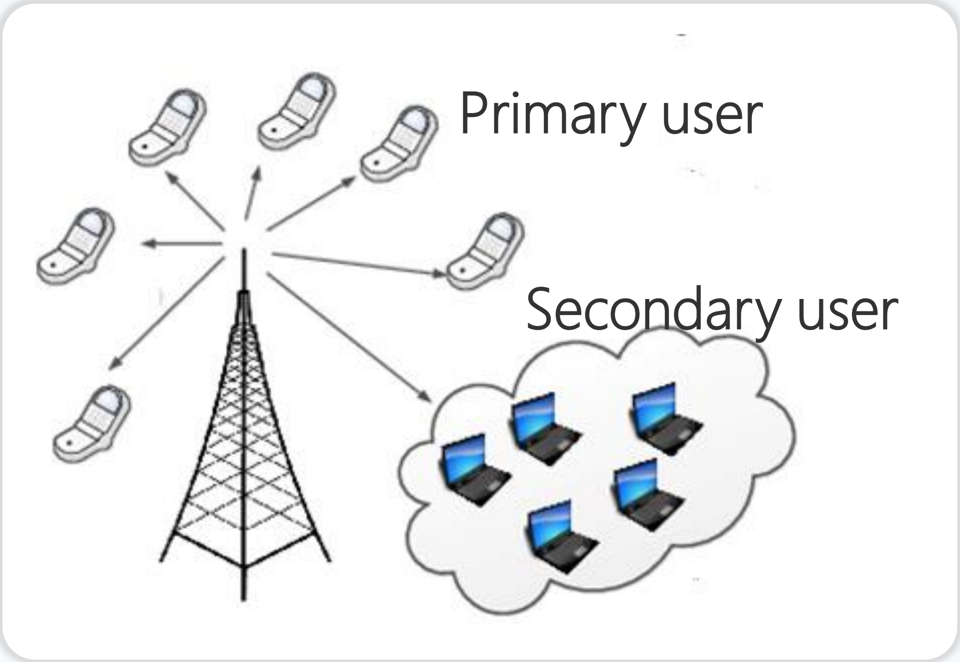
As of March/April 2019, this **highly cited paper** received enough citations to place it in the top 1% of the academic field of Engineering based on a highly cited threshold for the field and publication year.

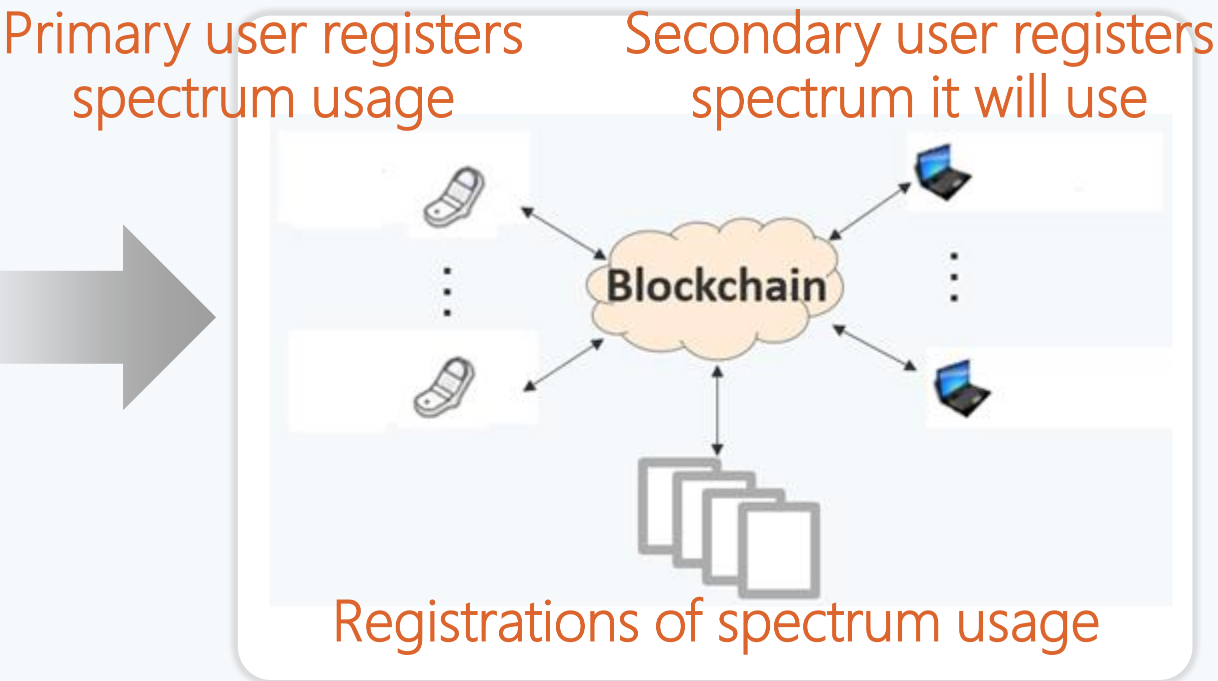
*Data from **Essential Science Indicators***

Close Window

"Enabling Localized Peer-to-Peer Electricity Trading Among Plug-in Hybrid Electric Vehicles Using Consortium Blockchain", *IEEE Trans. Industrial Informatics*, 13(6), 3154 - 3164, Dec 2017 (citations: 620+)

Blockchain + Physical Layer: *Dynamic Spectrum Sharing*





- FCC (Federal Communications Commission) Blockchain for dynamic spectrum sharing in 6G: spectrum-leasing transaction is verified and stored in Blockchain
- Blockchain as distributed ledger for communications: 1) save important data; 2) provide seamless access among different wireless networks

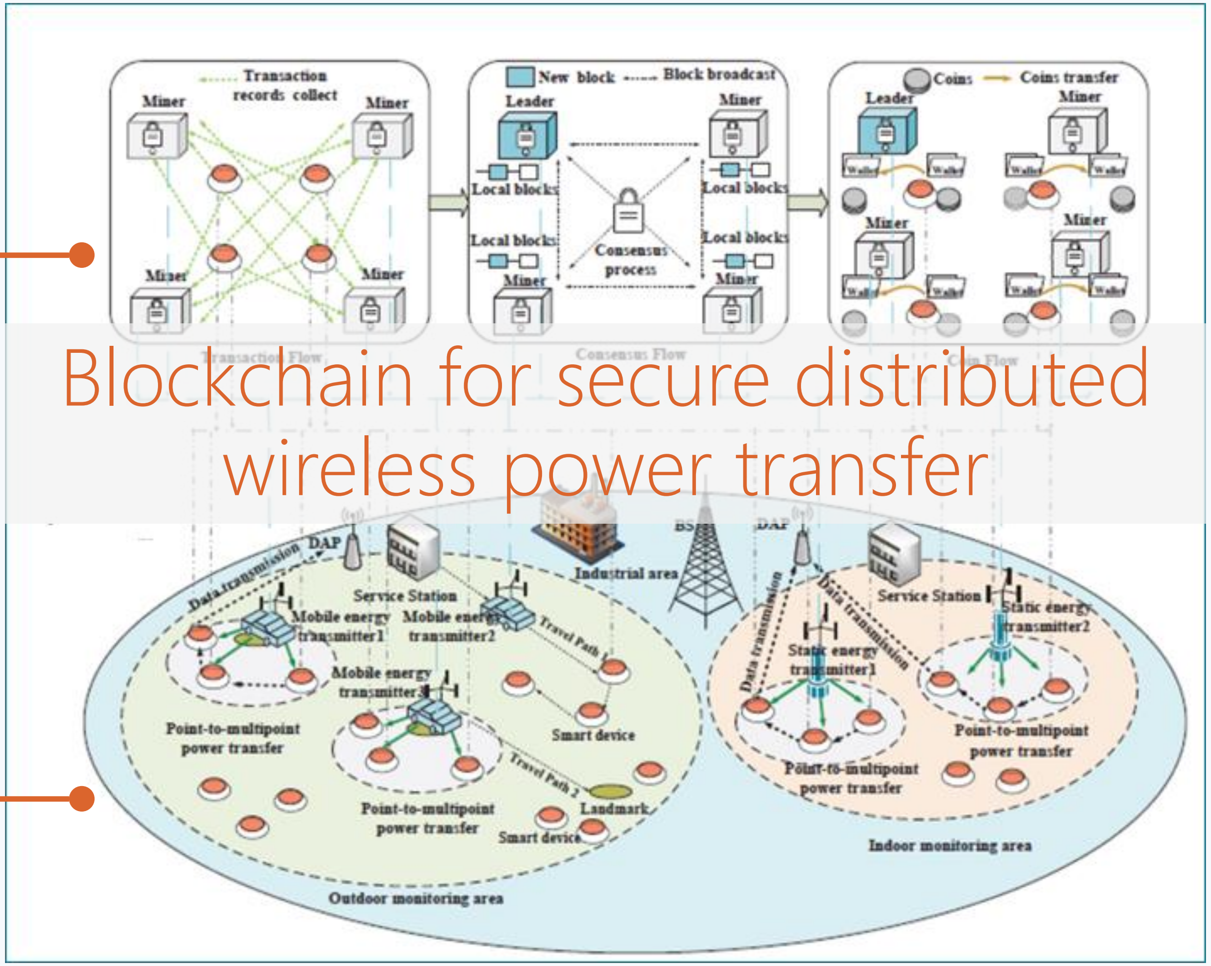
Blockchain + Physical Layer: *Wireless Power Sharing*

Blockchain Plane

DPoS based lightweight consensus scheme to achieve low overhead

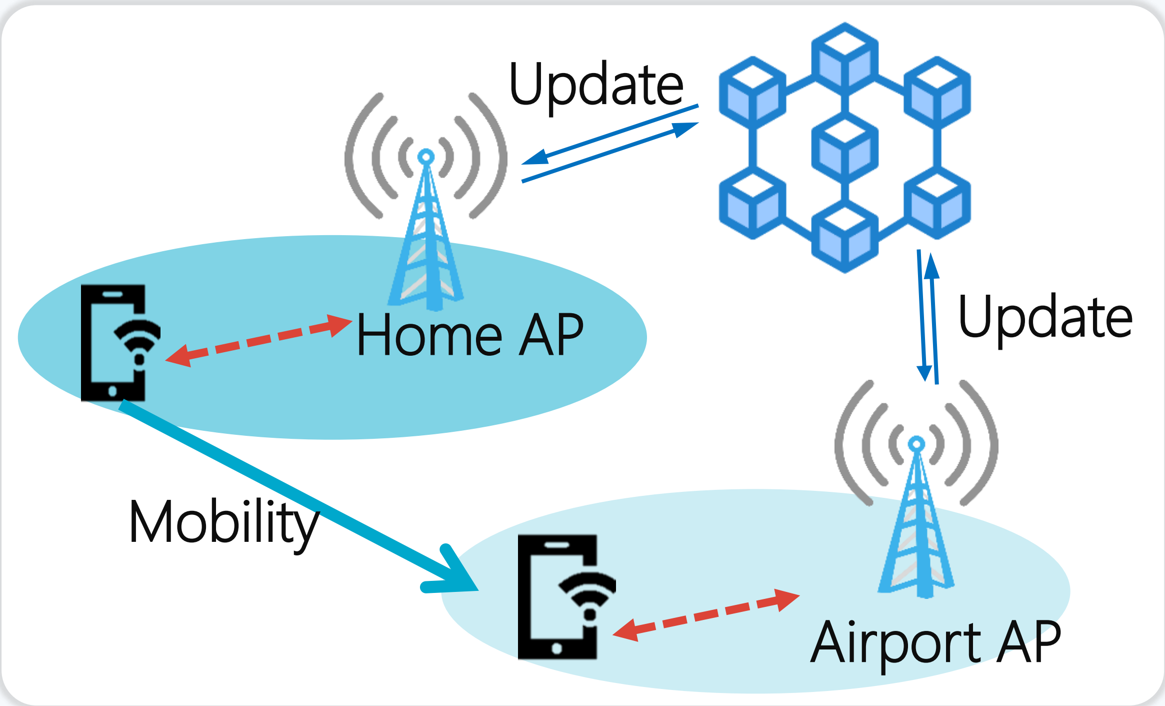
Energy Plane

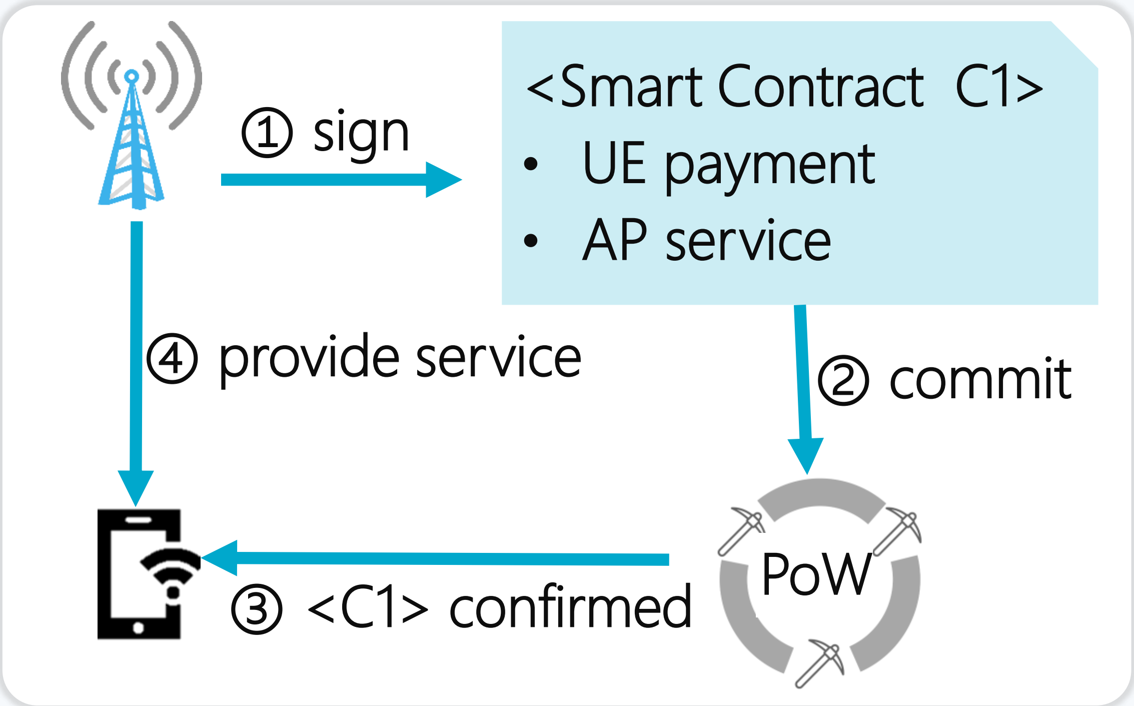
contract theory to obtain the optimal amount of transferred energy



Blockchain for secure distributed wireless power transfer

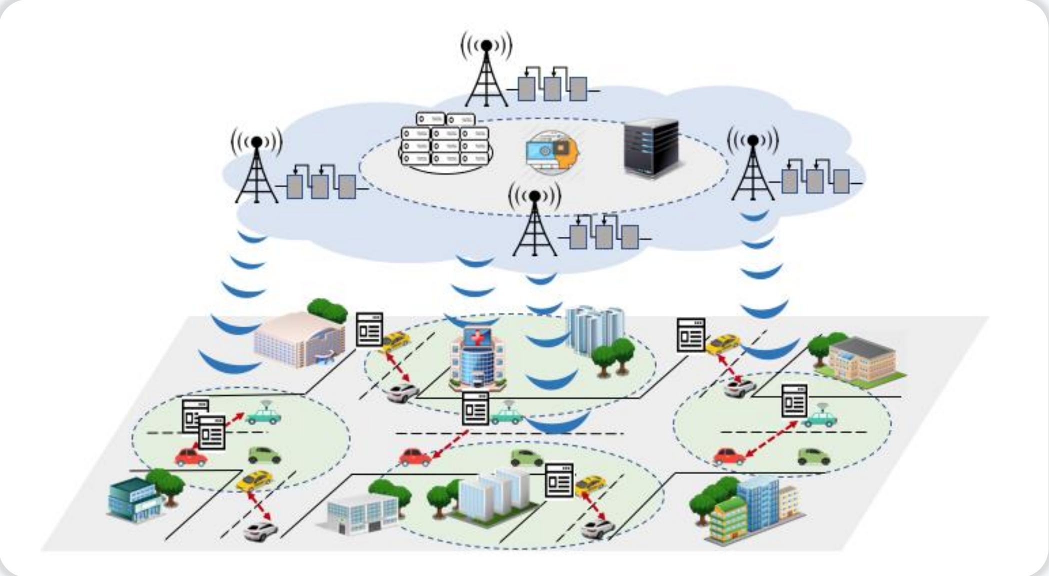
Blockchain + Data Link Layer: *Mobility Management*

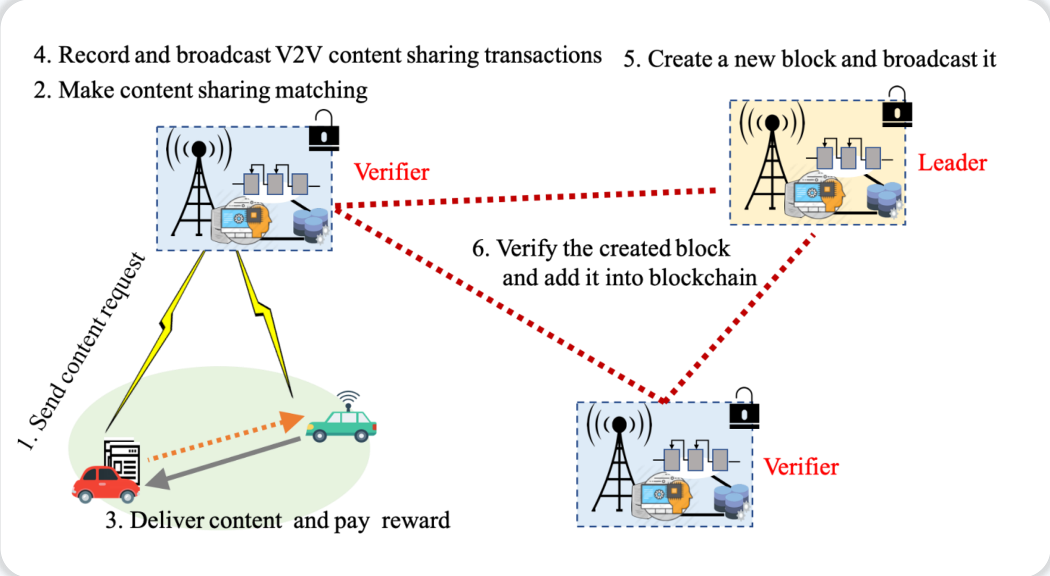




- Users and access points self-organize radio access without intermediate brokers
- Smart contract based mobility management enable cross-network roaming and establish a RAN (Radio Access Networks) among initially trustless parties

Blockchain + Application Layer: *Content Sharing*





- Vehicle Social Networks (or Vehicle Crowdsourcing Networks): Vehicles generate and request valuable content (e.g., news, videos, warnings, traffic)
- Content Sharing: devices act as caching requesters and providers to share content. Base stations maintain blockchain to record content sharing events

J. Kang, R. Yu, X. Huang, M. Wu, S. Maharjan, S. Xie and Y. Zhang, "Blockchain for Secure and Efficient Data Sharing in Vehicular Edge Computing and Networks", IEEE Internet of Things, vol.6, no.3, June 2019 (ESI "Hot Paper" "Highly Cited Paper")

Blockchain + Application Layer: *Unmanned Aerial Vehicles (UAVs)*

State-of-the-art topics

- Resource access control
- Secure content sharing
- New consensus protocol
- Edge computing for Blockchain

Innovative wireless services

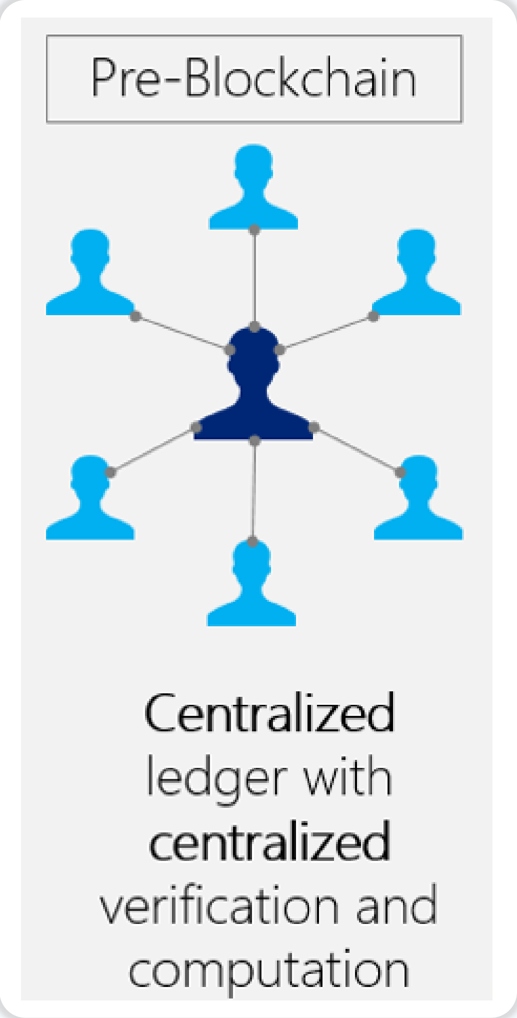
- Dynamic access network
- Environment sensing
- Proximate edge computing

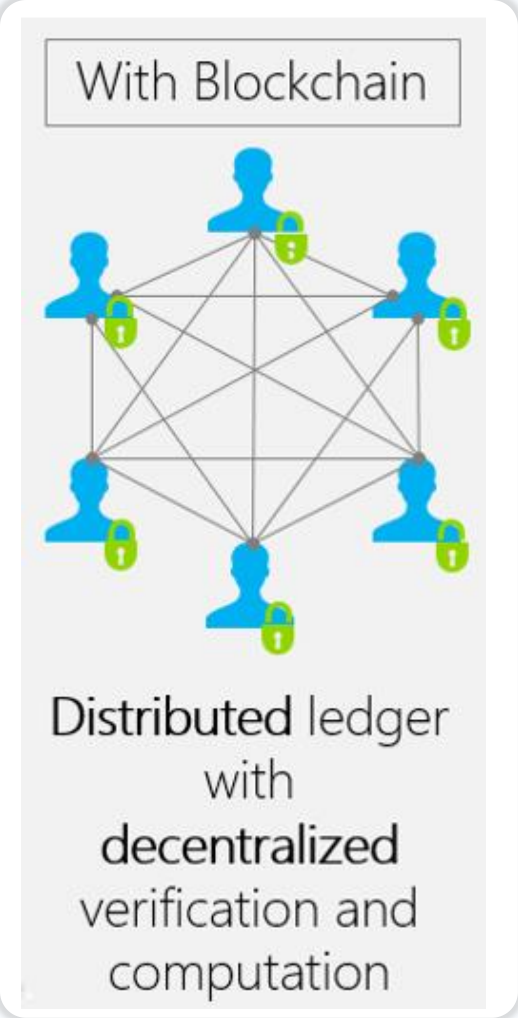
03

BLOCKCHAIN FOR SMART GRID

J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain, "Enabling Localized Peer-to-Peer Electricity Trading Among Plug-in Hybrid Electric Vehicles Using Consortium Blockchains", IEEE Transactions on Industrial Informatics, vol.13, no.6, pp. 3154 - 3164, Dec. 2017

Blockchain: centralized ➔ distributed computation and verification - recall





Three conditions to use Blockchain:

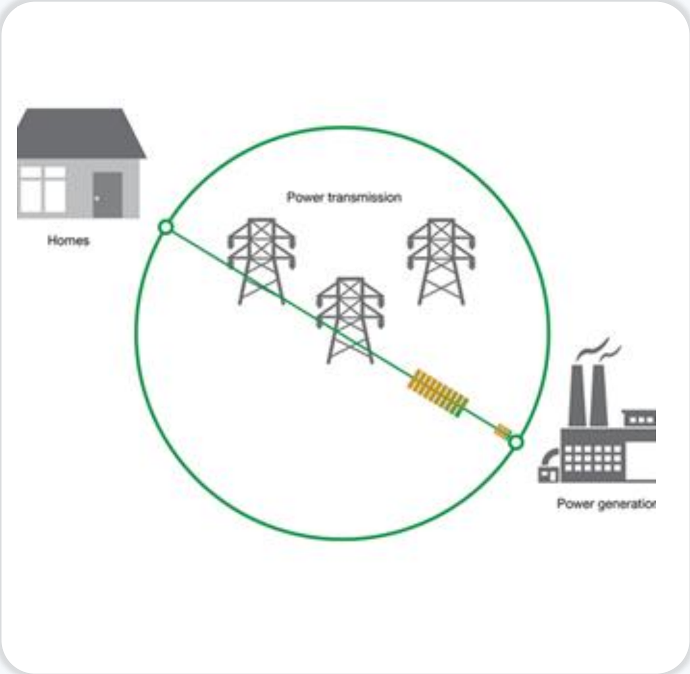
- distributed environment
- nodes do not trust each other
- nodes perform transactions

Role of Blockchain

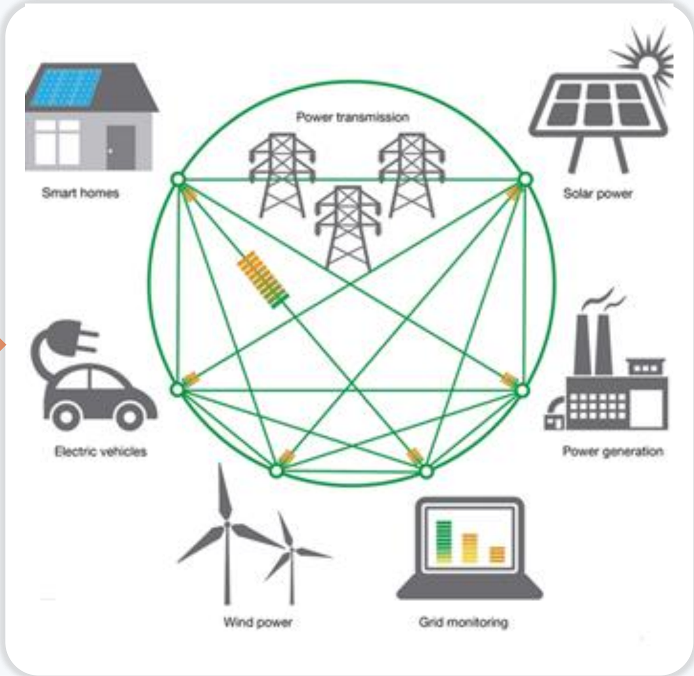
- Blockchain builds *trust* among untrusted participants in distributed environments

Centralized → decentralized operation: *smart grid*

Power grid today



Microgrid



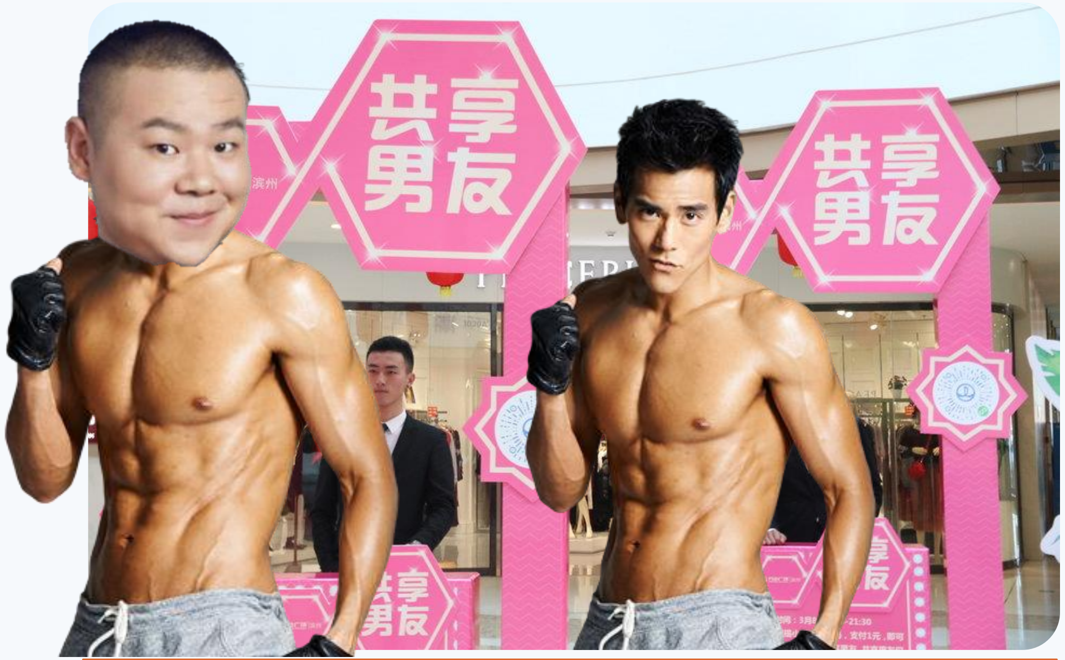
Future power grid:
network of microgrid

- Smart energy digitalization is enabled by Industrial IoT technologies for improved energy efficiency, optimization of power supply and demand, flexible integration of renewable energy resources.

Energy Sharing

Internet Sharing Economy

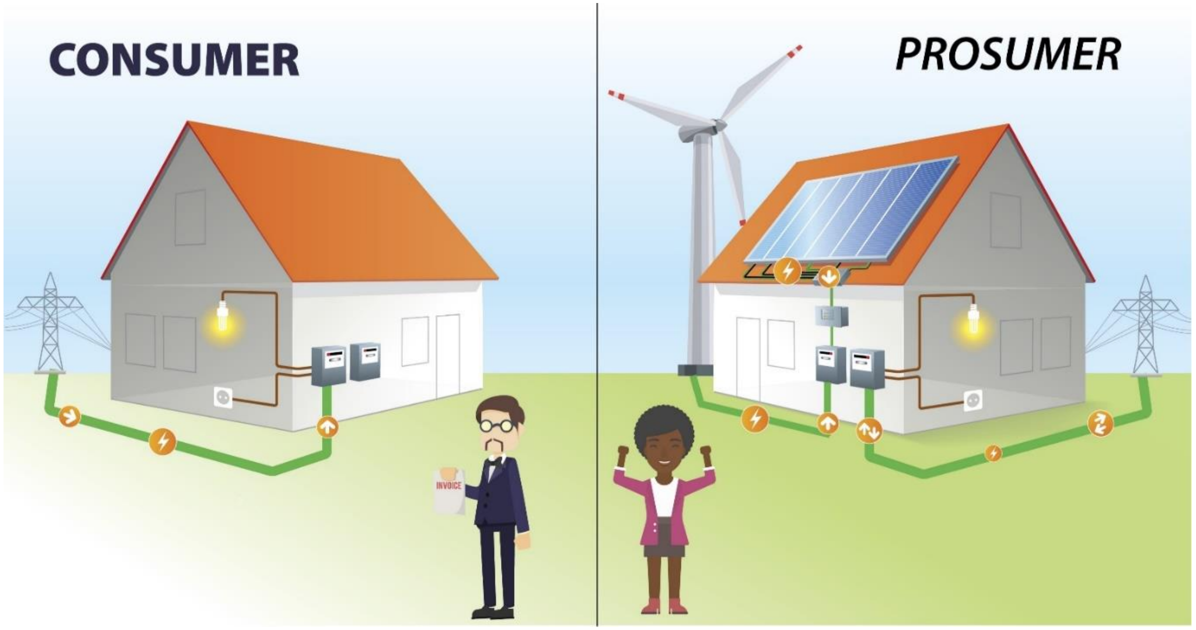
- Didi: sharing cars
- Wikipedia: knowledge sharing
- 摩拜: sharing bikes
- Airbnb: sharing houses



A natural question in Energy Sector

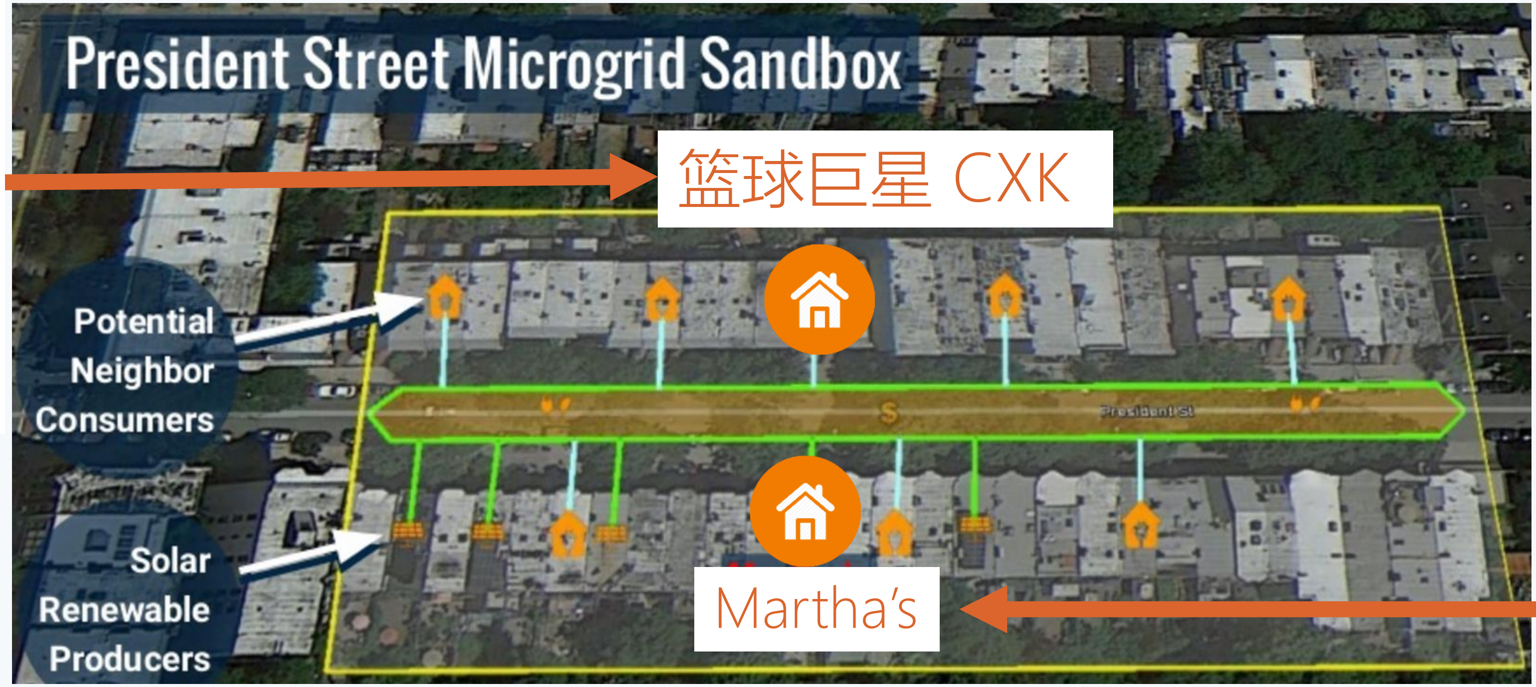
Q: How to share energy?

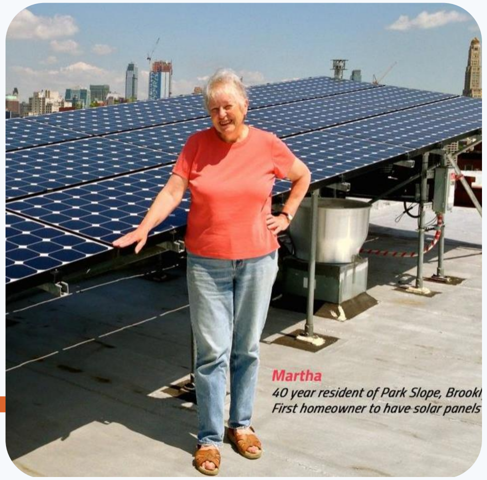
An emerging concept: *Prosumer = Producer + Consumer*



- Consumer: a house only uses electricity from power grid
- Prosumer: recently, we have renewable energy in our home, consumers are not just customer anymore. A prosumer refers to a house that can both produce and consume energy
- Energy sharing is closely related to the concept prosumer

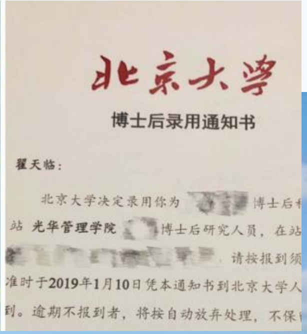
Selling your power to neighbors



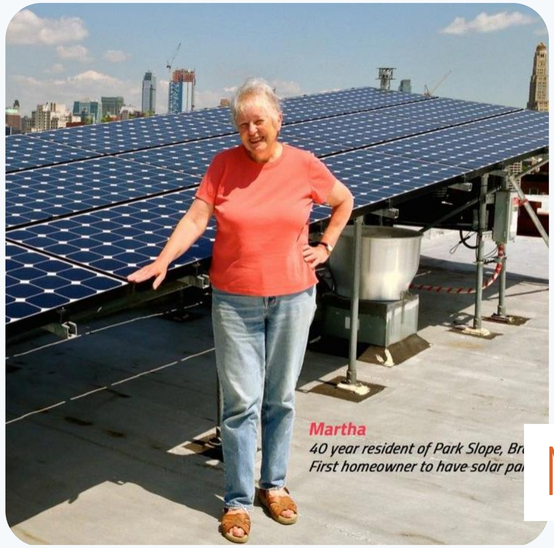


- Brooklyn Microgrid: In your house roof, you have solar power. The power can be used by yourself. If you are not able to use all power, you can sell to your neighbors, e.g., who is basketball superstar and have regular party.

Energy P2P (Peer-to-Peer) Networks



ZTL



YYQX

CXK

Martha's

- Each person can buy/sell energy from her/his neighborhood
- Very similar as P2P networks in Internet

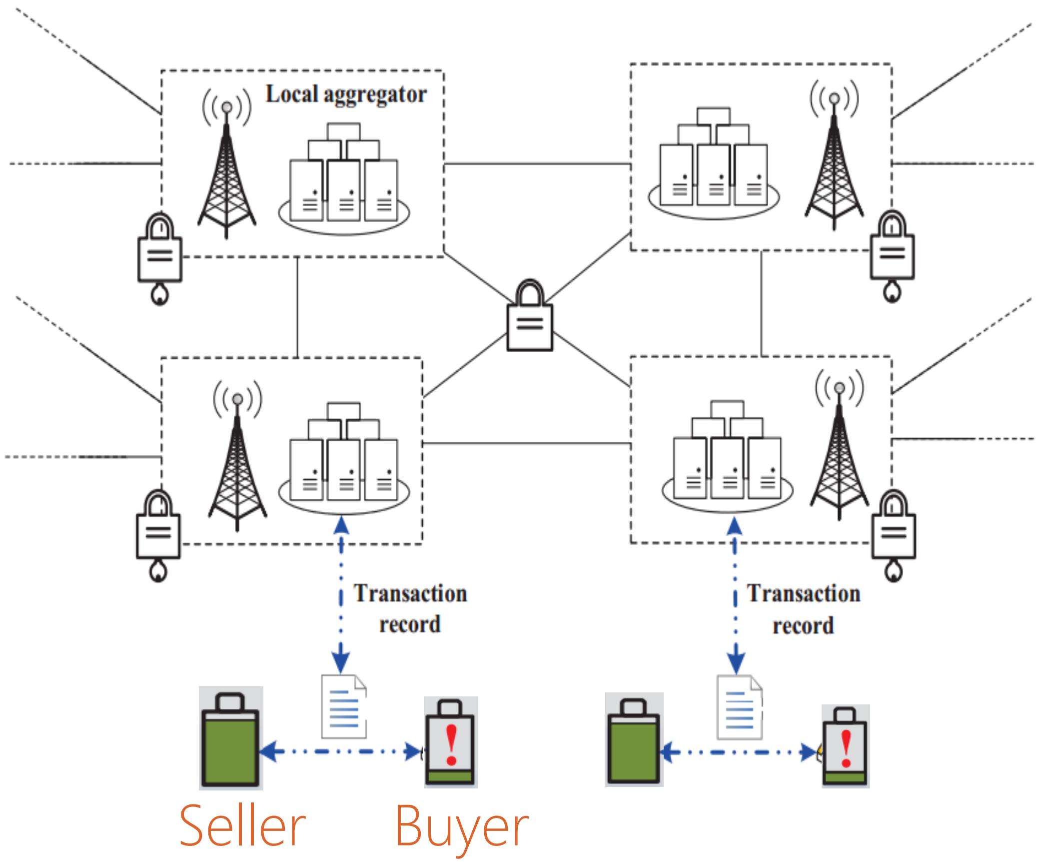
Decentralized energy trading: everyone can contribute/share power

- Feature: no need a third-party utility participating energy exchange among houses or electric vehicles

  → low cost, flexible, new business models

- Blockchain as a distributed ledger to store local energy transactions

Our Proposed Energy P2P Trading Architecture



Blockchain

Energy sharing

Our research problem and three contributions

Problem definition: need to secure a peer-to-peer energy sharing with high efficiency and private information protection

Blockchain for security

use blockchain for secure energy transaction in decentralized energy sharing scenarios

Optimization

optimize for energy balance among electric vehicles

Double auction

present an iterative double auction mechanism to hide private information but still maximize the system social welfare

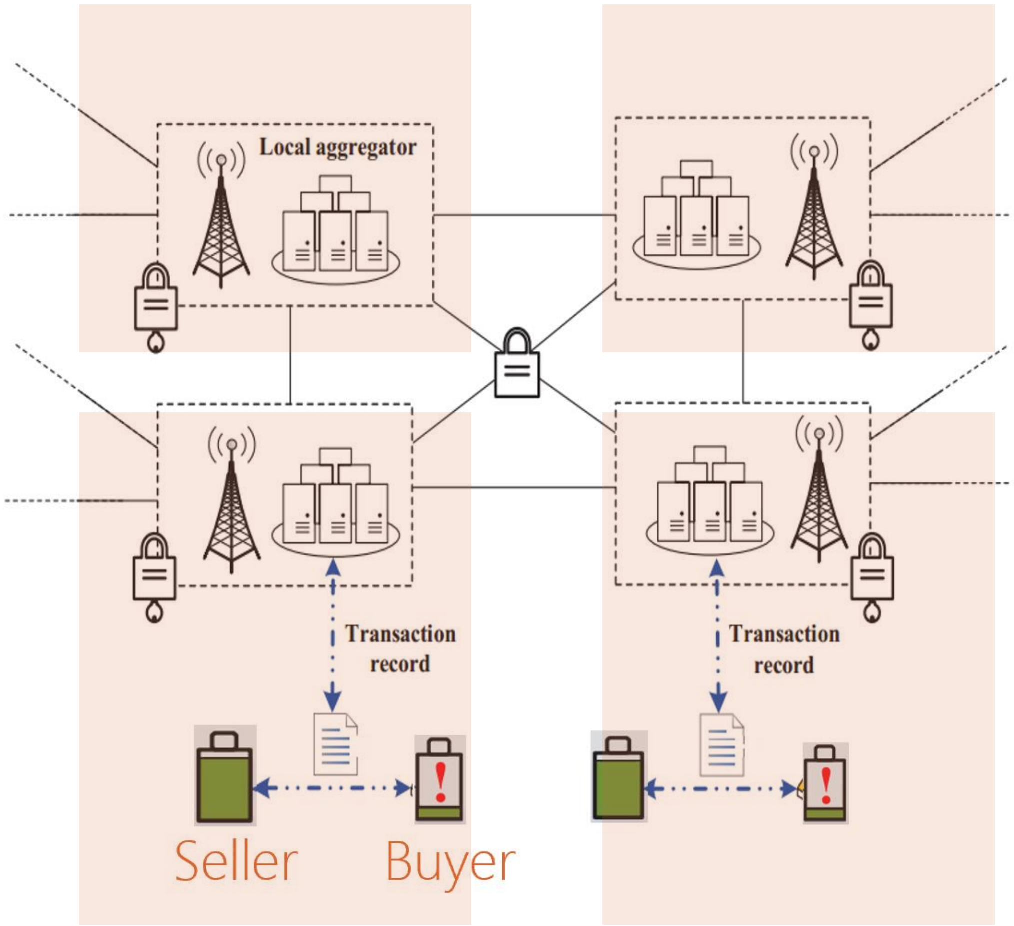
Consortium blockchain for secure energy P2P transaction

LAG (local aggregator)

- authorized nodes audit the transactions and record them into the shared ledger
- The ledger is publicly accessible

Consortium Blockchain

- blockchain with multiple authorized nodes to establish the distributed shared ledger



Blockchain enabled security features

No need 3rd party

energy P2P trading without third party to make system robust and scalable

Wallet security

Without keys, no adversary can open a wallet and steal energy coins

Transaction authentication

all transaction data is publicly audited and authenticated by authorized LAGs.

Data unforgeability

Decentralization of blockchain ensure that an adversary cannot corrupt network

No double-spending

Energy coin uses digital signatures to prevent double-spending

Privacy protection:

All energy coins accounts are pseudonymous, it can protect identity privacy

Energy sharing efficiency

Problem: decide electricity pricing and amount of traded electricity to maximize overall social welfare (i.e., the sum of nonlinear utilities).

Energy buyer:

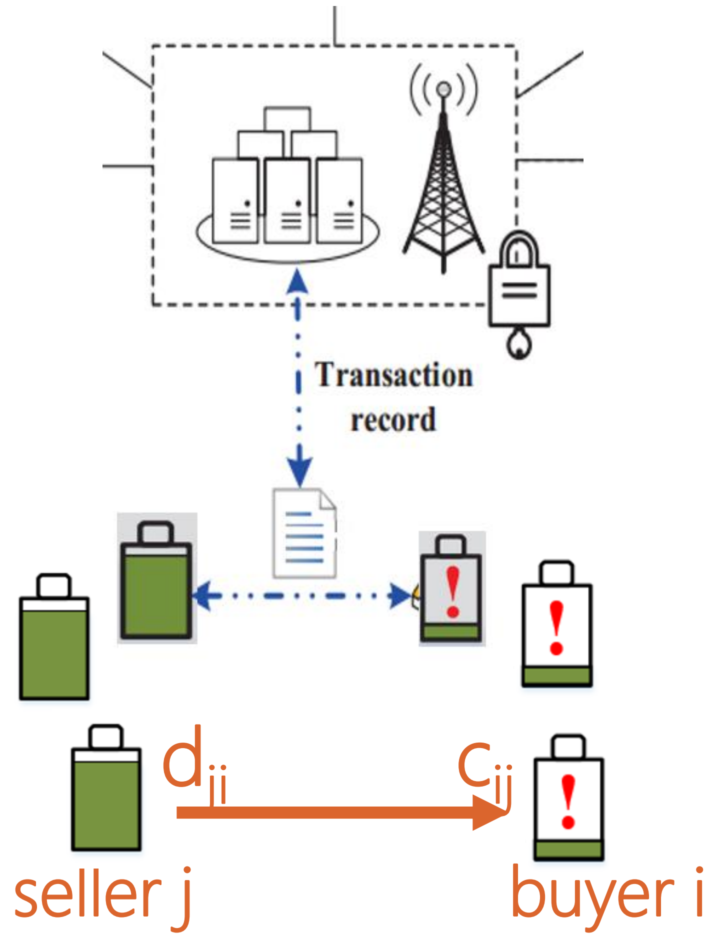
$$\upsilon \triangleq (CV_i^n | i \in \mathbb{C}, n \in \iota) \qquad \mathbb{C} = \{0, 1, 2, ..., I\}.$$

Energy seller:

$$\psi \triangleq (DV_j^n | j \in \mathbb{Z}, n \in \iota), \qquad \mathbb{Z} = \{0, 1, 2, ..., J\}.$$

Electricity demand vector of CV_i^n : $\mathbf{C_i^n} \triangleq \{c_{ij}^n | j \in \mathbb{Z}\}.$

Electricity supply vector of DV_j^n : $\mathbf{D_j^n} \triangleq \{d_{ji}^n | i \in \mathbb{R}\}.$



Problem Formulation and Electricity Trading

- Satisfaction function of CV_i^n

$$U_i(\mathbf{C_i^n}) = w_i \ln(\eta \sum_{j=1}^{J} c_{ij}^n - c_i^{n,\min} + 1),$$

$$w_i = \frac{\tau}{STO_i^n}$$

- Cost function of DV_j^n

$$L_j(\mathbf{D_j^n}) = l_1 \sum_{i=1}^{I} (d_{ji}^n)^2 + l_2 \sum_{i=1}^{I} d_{ji}^n,$$

Symbol	Interpretation
w_i	charging willingness
η	charging efficiency
c_{ij}^n	demand of CVi from discharging DVj
$c_{ij}^{n,min}$	minimum electricity demand of Cvi
STO_i^n	energy state
d_{ji}^n	energy supply from DVj to CVi in LAGn
$l_{1;}\ l_2$	cost factors

- Social welfare maximization problem: from a social perspective, the localized P2P electricity trading should maximize social welfare and achieve market equilibrium. The energy broker addresses the social welfare maximization problem to allocate energy between discharging EVs and charging EVs

Problem Formulation and Electricity Trading

$$SW : \max_{\mathbf{C^n},\mathbf{D^n}} \sum_{i=1}^{I} U_i(\mathbf{C_i^n}) - \sum_{j=1}^{J} L_j(\mathbf{D_j^n}).$$

Social welfare maximization objective function

$$\text{Subject to: } c_i^{n,\min} \leq \eta \sum_{j=1}^{J} c_{ij}^n \leq c_i^{n,\max}, \forall i \in \mathbb{C},$$

$$\sum_{i=1}^{I} d_{ji}^n \leq \mathrm{D}_j^{n,\max}, \forall j \in \mathbb{Z},$$

$$\rho d_{ji}^n = c_{ij}^n, \forall i \in \mathbb{C}, \forall j \in \mathbb{Z},$$

Energy transmission loss

$$c_{ij}^n \geq 0, \forall i \in \mathbb{C}, \forall j \in \mathbb{Z}.$$

- ρ: average electricity transmission efficiency of the local electricity trading.
- The objective function: strictly concave with compact and convex constraints, so there exists a unique optimal solution using Karush-Kuhn-Tucker (KKT) conditions.

Lagrangian function L1

$$L_1(\mathbf{C^n}, \mathbf{D^n}, \alpha, \beta, \gamma, \lambda, \mu) = \sum_{i=1}^{I} U_i(\mathbf{C_i^n}) - \sum_{j=1}^{J} L_j(\mathbf{D_j^n}) +$$
$$\sum_{i=1}^{I} \alpha_i (c_i^{n,\min} - \eta \sum_{j=1}^{J} c_{ij}^n) + \sum_{i=1}^{I} \beta_i (\eta \sum_{j=1}^{J} c_{ij}^n - c_{i,n}^{\max})$$
$$+ \sum_{j=1}^{J} \gamma_j (\sum_{i=1}^{I} d_{ji}^n - D_{j,n}^{\max}) + \sum_{j=1}^{J} \sum_{i=1}^{I} \lambda_{ij} (\rho d_{ji}^n - c_{ij}^n) -$$
$$\sum_{j=1}^{J} \sum_{i=1}^{I} \mu_{ij} c_{ij}^n.$$

- where α, β, γ, λ, μ are Lagrangian multiplier
- Then, we take derivative on L1 with respect to $c_{i,j}^n$ and $d_{j,i}^n$

Solving the problem is easy if we have sufficient information

Optimal solution of SW

- take derivative on L1 with respect to $c_{i,j}^n$ and $d_{j,i}^n$
- set two derivative functions to zero

$$\nabla_{c_{ij}^n} L_1(\mathbf{C^n},\mathbf{D^n},\boldsymbol{\alpha},\boldsymbol{\beta},\boldsymbol{\gamma},\boldsymbol{\lambda},\boldsymbol{\mu}) = \frac{\eta w_i}{\eta \sum_{j=1}^{J} c_{ij}^n - c_i^{n,\min} + 1} - \eta\alpha_i + \eta\beta_i - \lambda_{ij} - \mu_{ij} = 0,$$

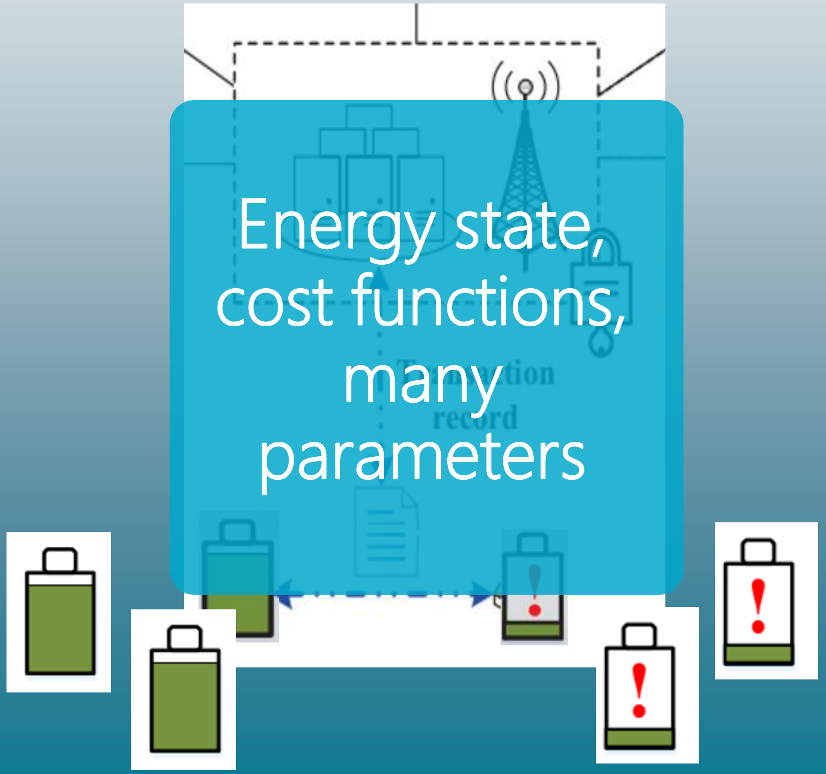
$$\nabla_{d_{ji}^n} L_1(\mathbf{C^n},\mathbf{D^n},\boldsymbol{\alpha},\boldsymbol{\beta},\boldsymbol{\gamma},\boldsymbol{\lambda},\boldsymbol{\mu}) = -2l_1 d_{ji}^n - l_2 + \gamma_j + \lambda_{ij}\rho = 0.$$

- **Difficult to solve this problem in practice**: the aggregator needs complete information of all EVs' energy state, utility and cost functions. EVs may not be willing to provide private information to the aggregator, such as energy state.

Private information protection

Complete information

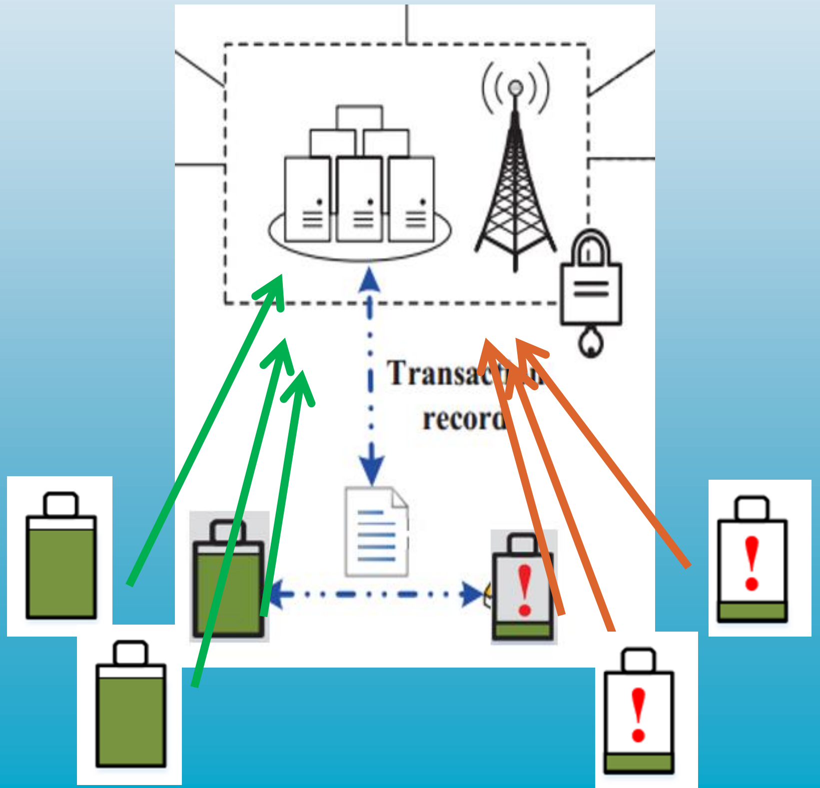
Aggregator needs all information of all houses battery, cost functions



Energy state, cost functions, many parameters

Only price information

Iterative double auction: aggregator only needs price from each house



Iterative Double Auction for energy trading

Iterative Double Auction

Many buyers and many sellers interact, facilitated by the broker, in an iterative fashion and adjust their bids until the market reaches an efficient point, i.e., the market clearing solution

- Energy sellers and buyers interact, coordinated by LAG, in an iterative fashion
- All energy entities adjust their bidding price until the market reaches an efficient point

A natural iterative double auction where

- Broker: aggregators
- Buyers: buy energy
- Sellers: sell energy to others

Iterative Double Auction Mechanism: *decide bidding price for buying (I)*

Each charging EV is selfish decides its own buying price: CVi solves the following problem to maximize its own benefit and determine its optimal bidding price

$$EB : \max_{\mathbf{B_i^n}} [U_i(\mathbf{C_i^n}) - \underline{pay_i(\mathbf{B_i^n})}], \qquad \mathbf{B_i^n} \triangleq \{b_{ij}^n | j \in \mathbb{Z}\}$$

Payment function given by the auctioneer

The payment function of CVi is given by:

$$pay_i(\mathbf{B_i^n}) = \sum_{j}^{J} b_{ij}^n,$$

Iterative Double Auction Mechanism: *decide bidding price for selling (II)*

Each discharging EV is selfish and decides its own selling price: DVj solves the following problem (ES, seller) to determine its optimal bidding price

$$ES : \max_{\mathbf{S_j^n}} [\underbrace{Rew_j(\mathbf{S_j^n})}_{} - L_j(\mathbf{D_j^n})]. \qquad \mathbf{S_j^n} \triangleq \{s_{ji}^n | i \in \mathbb{C}\}.$$

Reward function given by the auctioneer

The reward function of DVj is expressed as

$$Rew_j(\mathbf{S_j^n}) = \sum_i^I \frac{(s_{ji}^n)^2}{4l_1} + r_j^{\min}.$$

Minimum reward for a discharging EV owing to the trading participation

Iterative Double Auction Mechanism: *traded energy maximization (III)*

- The auctioneer solves problem *A* to calculate the traded energy

$$A: \max_{\mathbf{C^n},\mathbf{D^n}} \sum_{i=1}^{I} \sum_{j=1}^{J} [b_{ij}^n \ln c_{ij}^n - s_{ji}^n d_{ji}^n]$$

- Problems *A* and *SW* have the same constraints. All KKT conditions along with the steady conditions are matched. According to the Lagrangian multipliers, we obtain the bidding prices of charging EVs and discharging EVs

$$b_{ij}^n = \frac{\eta \tau c_{ij}^n}{(\eta \sum_{j=1}^{J} c_{ij}^n - c_i^{n,\min} + 1) STO_i^n}, \qquad s_{ji}^n = 2 l_1 d_{ji}^n + l_2.$$

Energy Trading Performance

Real dataset

- We evaluate the proposed iterative double auction mechanism with real dataset
- The data is from real urban area of Texas

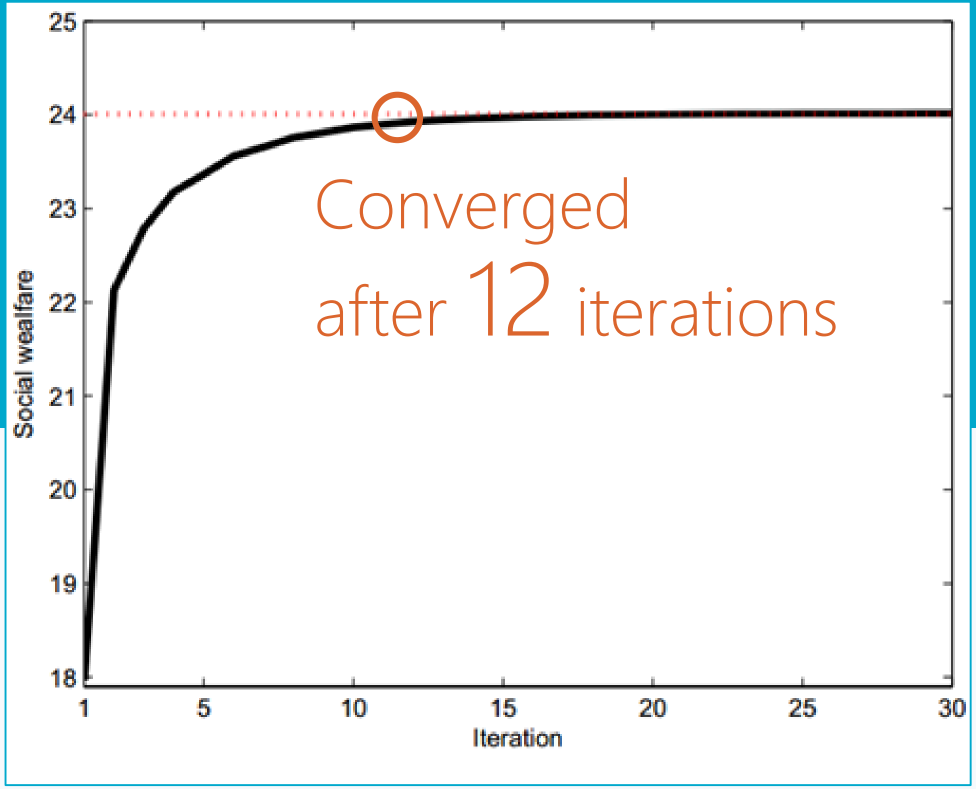
Latitude of observed area

- Latitude: 30.256 → 30.276,
- Longitude: -97.76 → -97.725

Area: 8.6 km^2

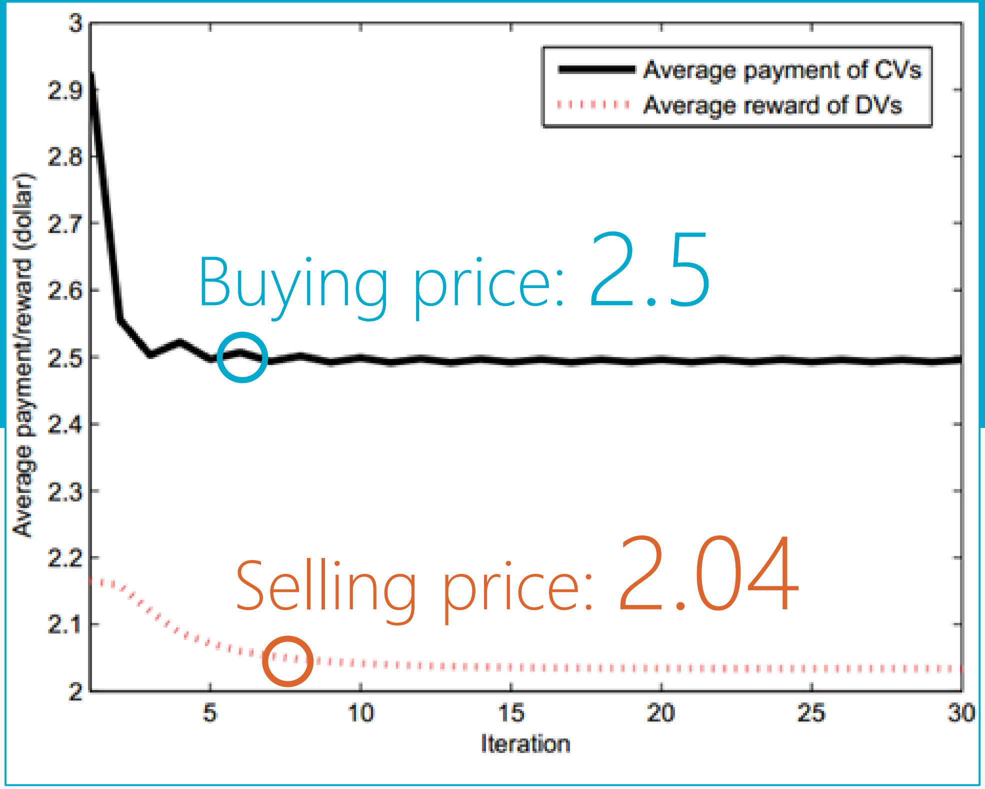
Parking lots: 58

Results for a community with 80 houses



The social welfare

rapidly converges to the optimal result



The difference between prices

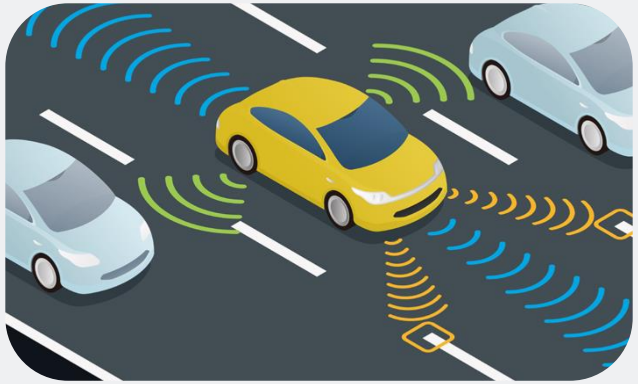
represents the benefit of the auctioner/aggregator

04

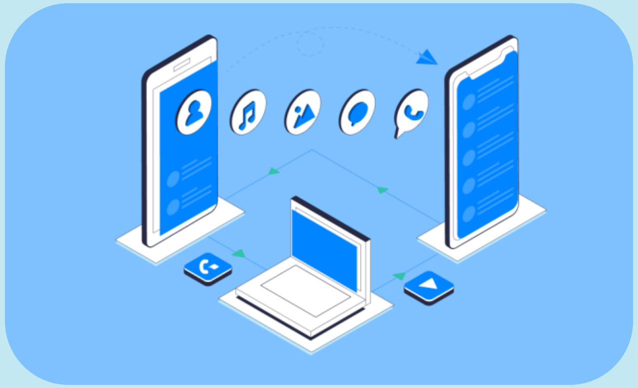
BLOCKCHAIN FOR CONTENT SHARING

- L. Jiang, S. Xie, S. Maharjan, and Y. Zhang, "Joint Transaction Relaying and Block Verification Optimization for Blockchain Empowered D2D Communication", IEEE Transactions on Vehicular Technology, vol.69, no.1, pp.828 - 841, Jan. 2020.

Data/Content sharing in D2D



Data sharing among vehicles



Device-to-Device content sharing

Data sharing among UAVs

- Data sharing (information sharing, content sharing) can take place in many scenarios, e.g., Device-to-Device (D2D), Vehicles, UAV

Consortium blockchain empowered D2D communications

D2D Pair

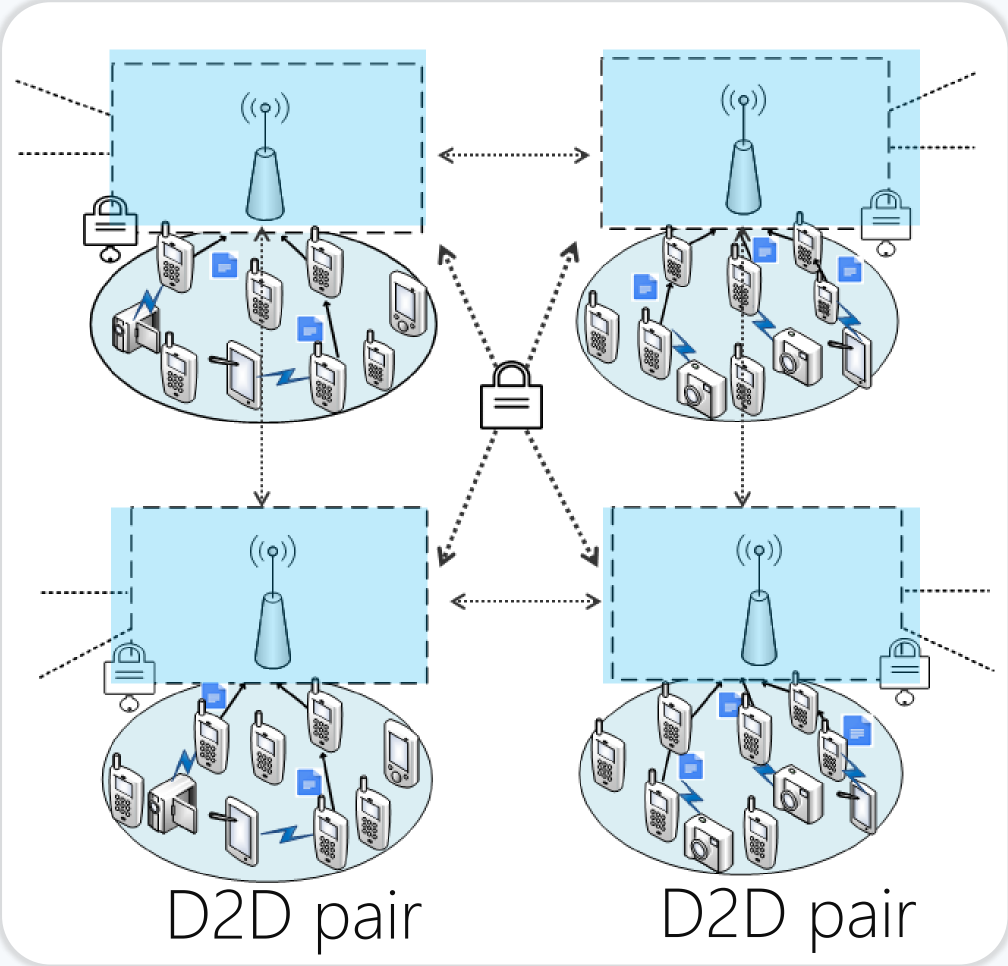
Two devices can build a pair to share content/information/data

Receiver/Transmitter

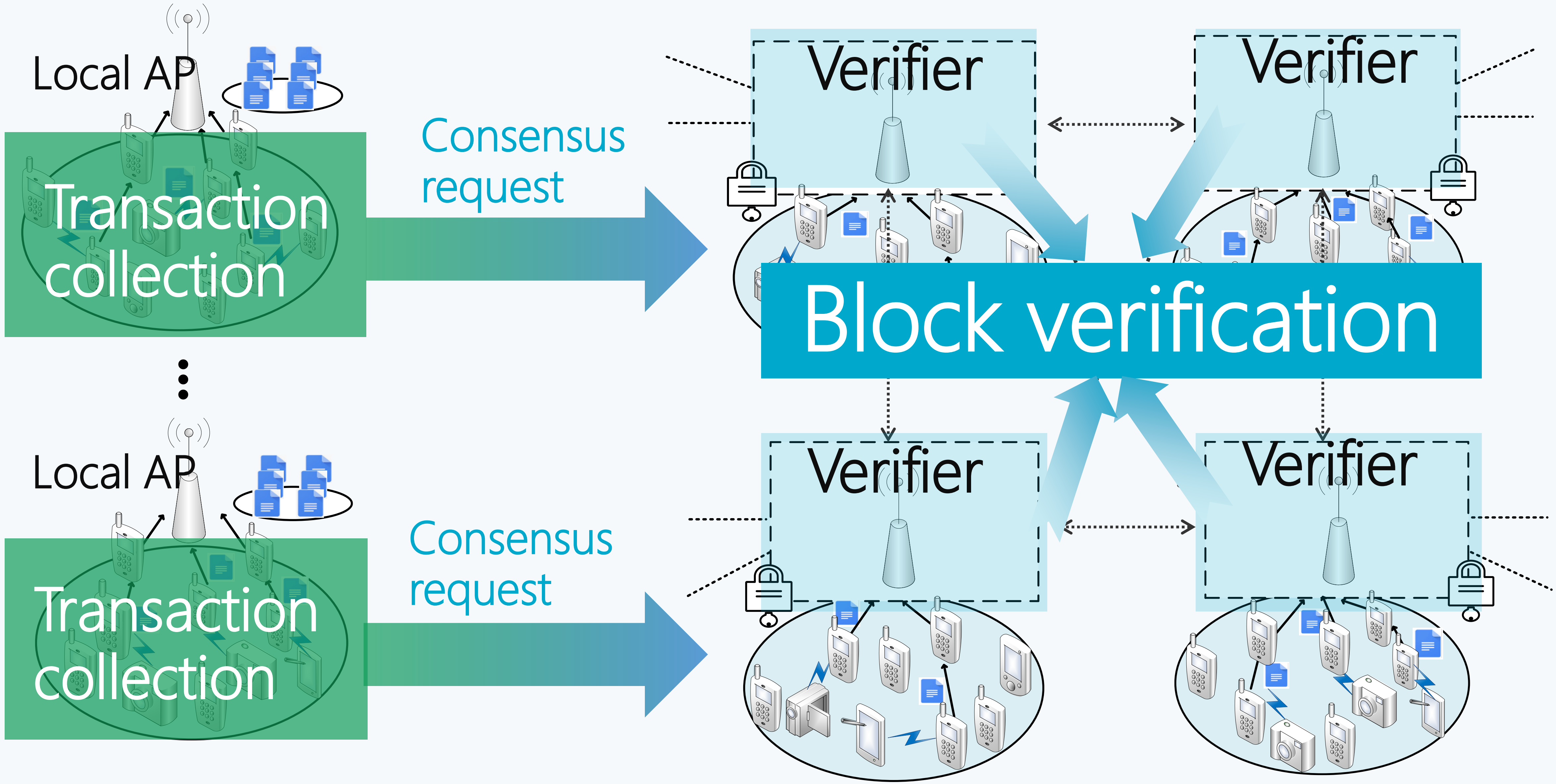
A receiver can request a transmitter nearby to provide data sharing service

Base Station/Access Point

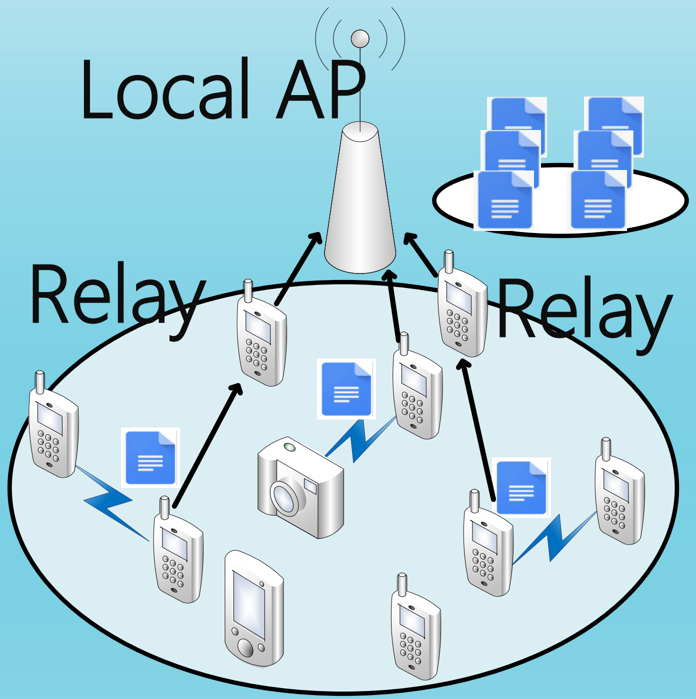
A set of APs are selected to act as verifiers and responsible for block verification

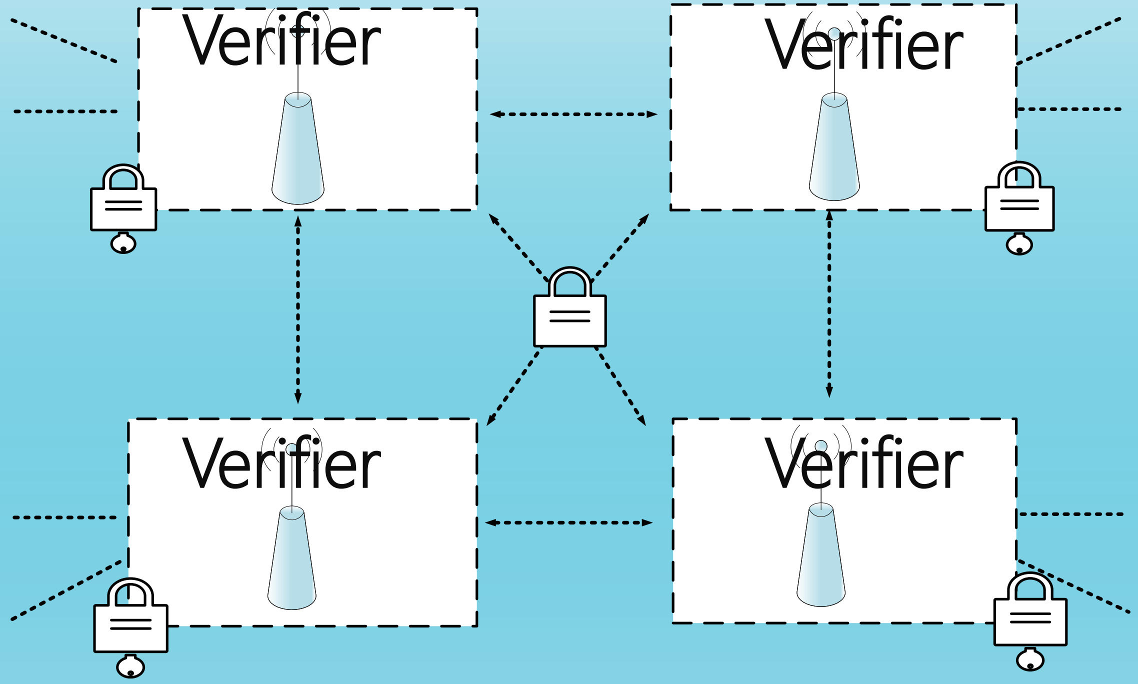


Transaction confirmation procedure



Transaction confirmation procedure





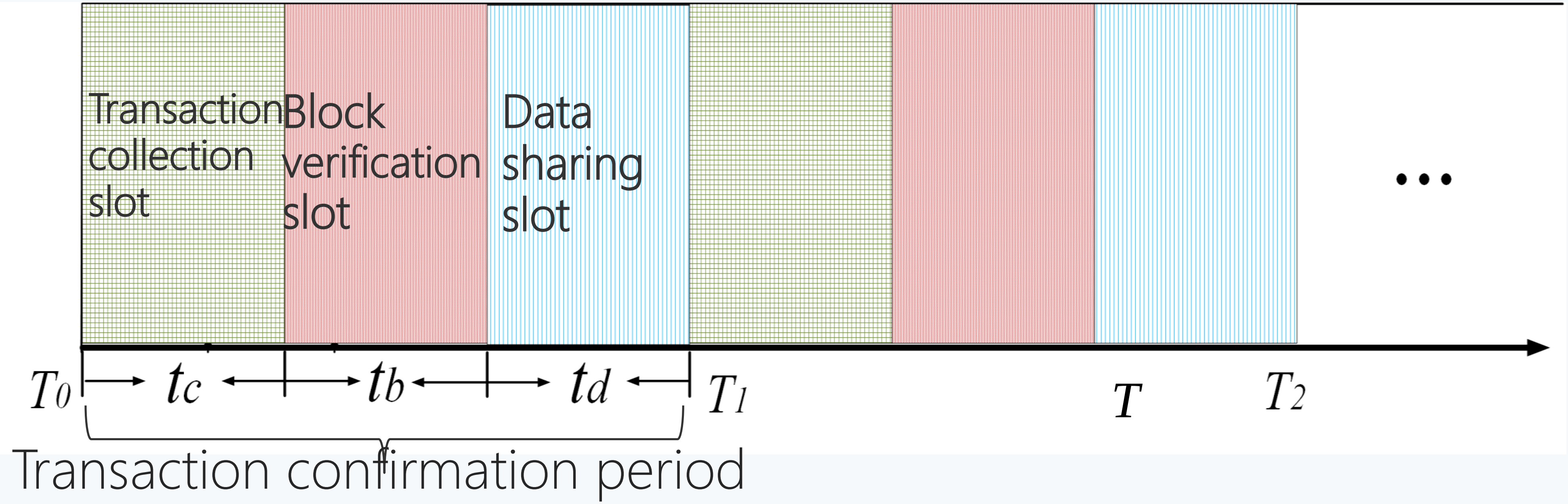
Stage 1 : Relay Selection Scheme

Relay–assisted transactions relaying scheme to select suitable relays

Stage 2 : Block Verification Procedure

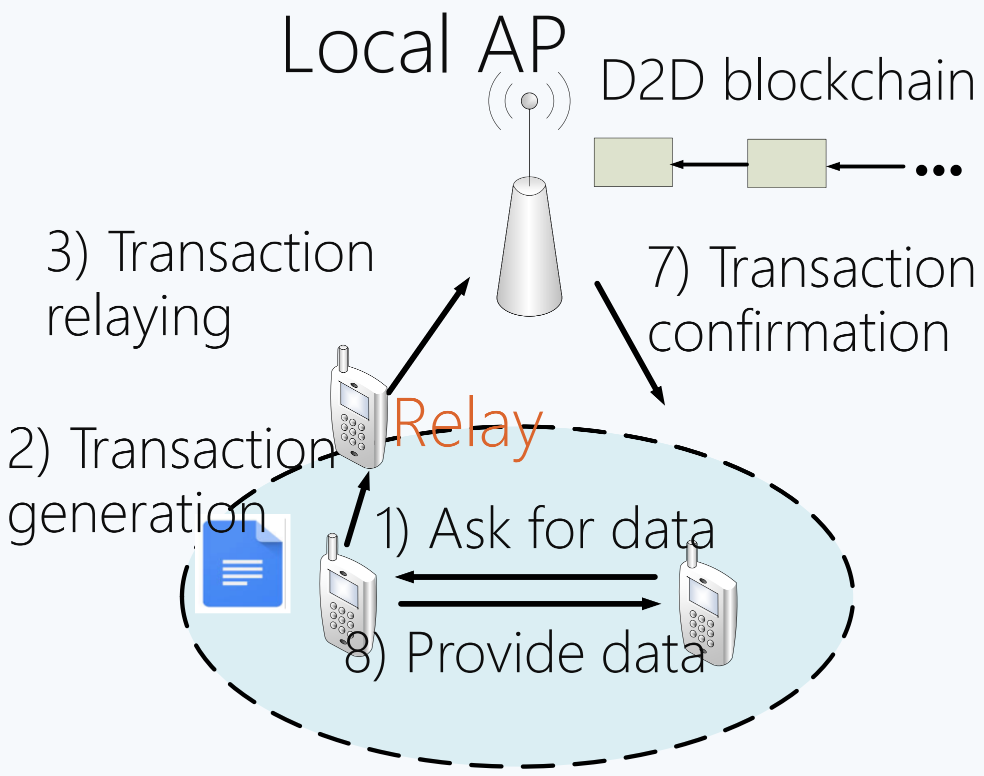
Delegated Proof-of-Stake based lightweight block verification scheme

Communications and computation issues in transaction confirmation procedure

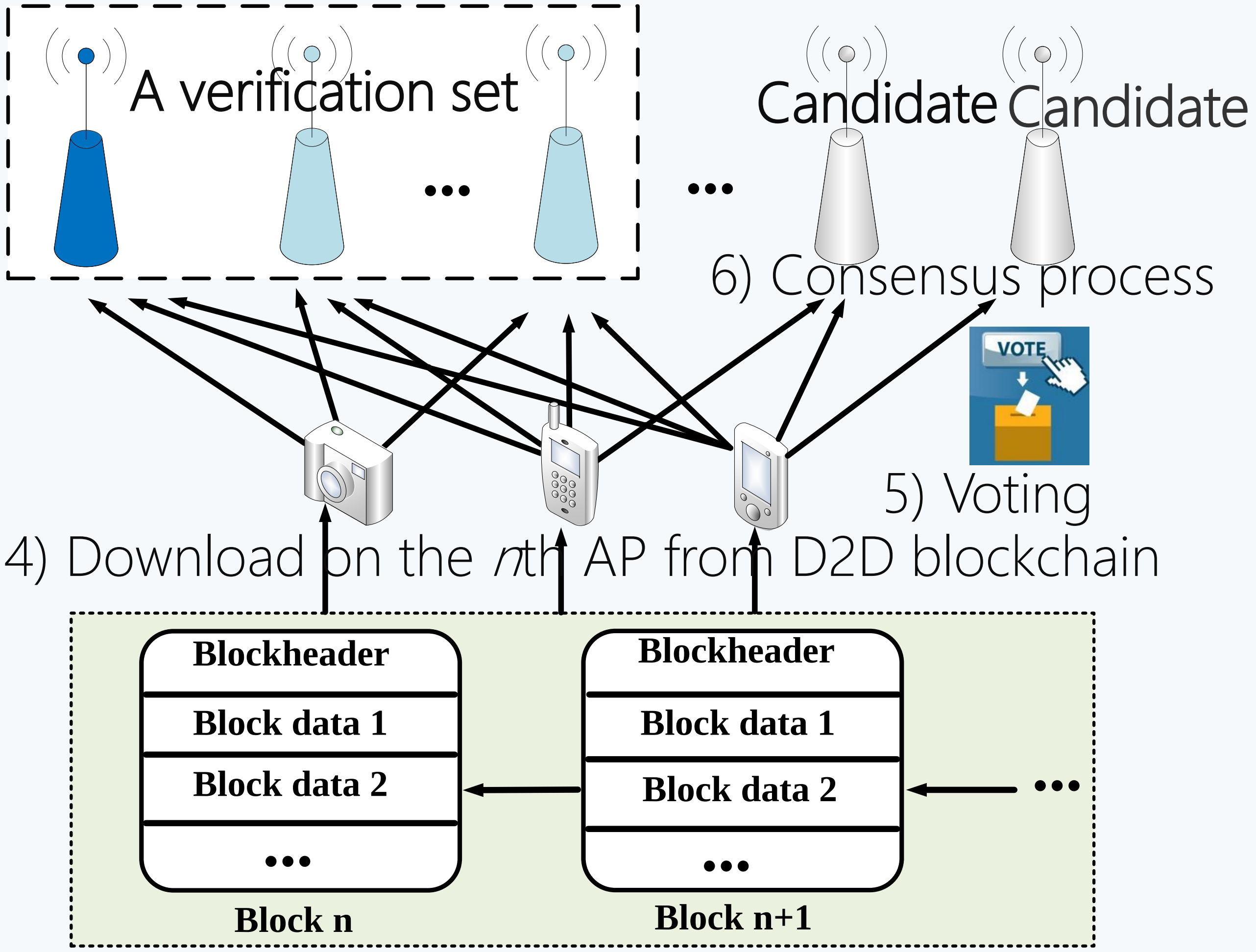


- Communications issue in stage 1: unreliable wireless channel leads to failed transmission of users' transactions to the verifiers
- Computation issue in stage 2: high computation load in verifiers (e.g., running Proof-of-Work (PoW)) in block verification slot.

Transaction relaying and DPoS based Block verification



Stage 1 : Relay Selection Scheme during transaction collection

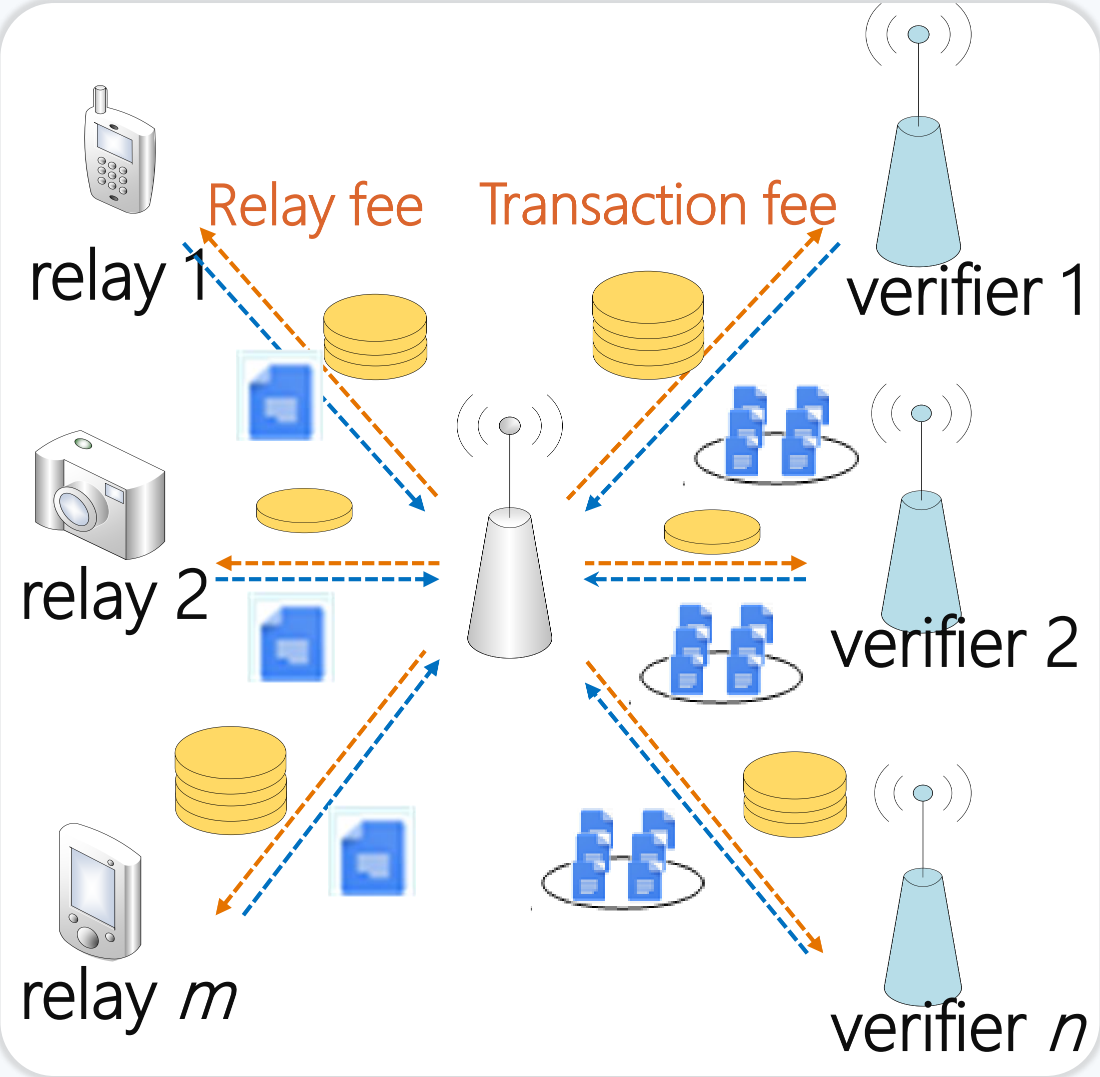


Stage 2 : DPoS-based lightweight consensus in Block Verification Procedure

Incentive mechanisms for transaction relaying and DPoS based block verification

Local APs pay relay fee and transaction fee to compensate for resources usage. The two prices are decided by

- Time-varying available resource of the relays and the verifiers
- Information asymmetry
- Long latency for transaction relaying and block verification



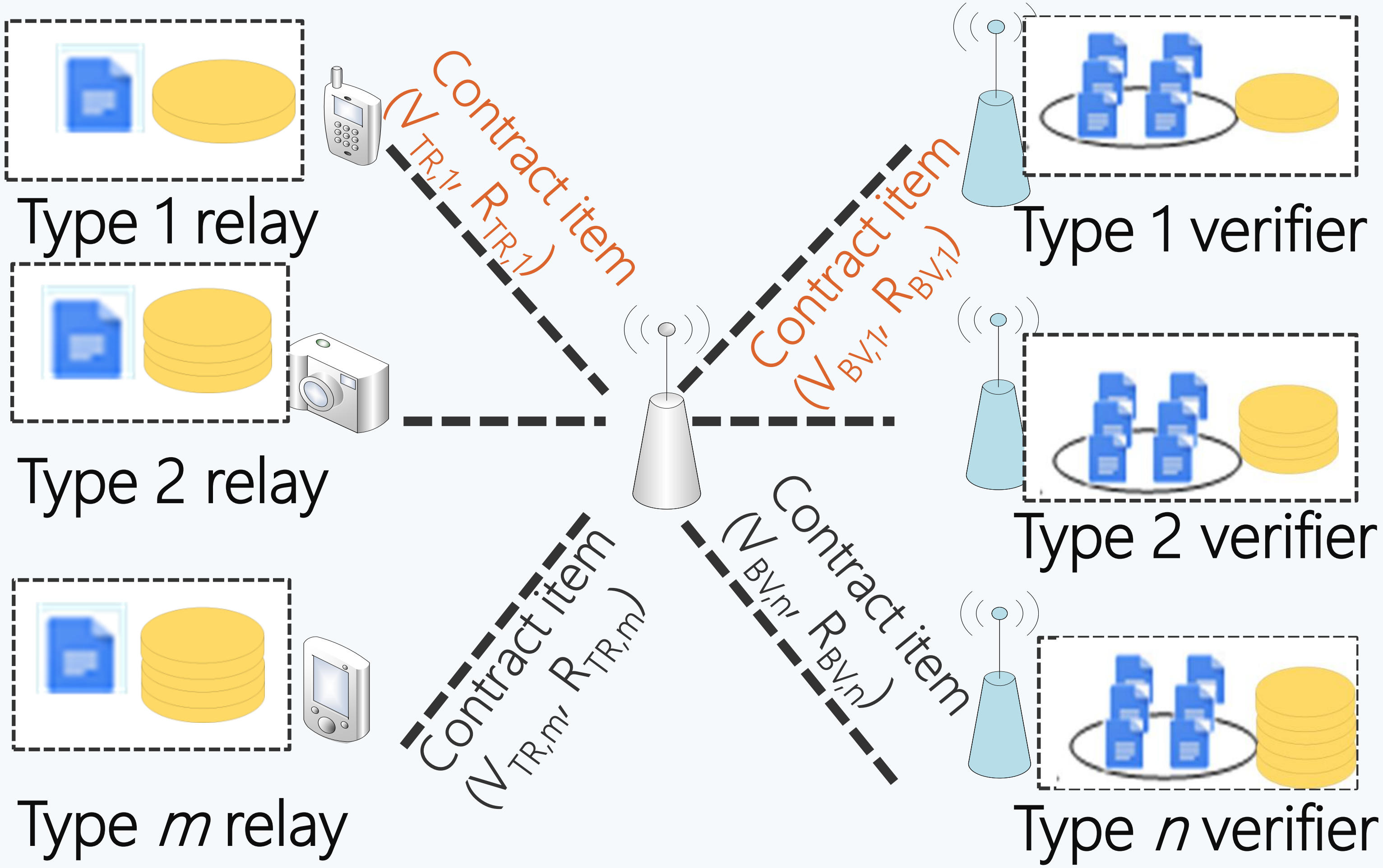
Contract theory based joint optimization for transaction relaying and block verification

- We define new terms to show the quality of relayed transaction and verified block: Value of transaction relaying (*VoTR*), Value of block verification (VoBV)

$$V_{TR,m}(t_m) = A_{TR}e^{-B_{TR}t_m},$$

$$t_m = \frac{w_{trans}}{r_m},$$

$$r_m = \frac{1}{2}b\log_2\left(1 + \frac{\beta^2 P_{user}|h_{user,m}|^2|h_{m,AP}|^2}{I+\beta^2|h_{m,AP}|^2 N_0 + N_0}\right)$$



Optimization Problem Formulation

$$\max_{\substack{(R_{TR,s},V_{TR,s}\\ R_{BV,q},V_{BV,q})}} U_{AP} = \underbrace{\sum_{s=1}^{S} \lambda_s M(V_{TR,s} - l_1 u_1 R_{TR,s})}_{\text{Utility of local AP for transaction relaying}} + \underbrace{\sum_{q=1}^{Q} \lambda_q N\left(V_{BV,q} - l_2 u_2 R_{BV,q}\right)}_{\text{Utility of local AP for block verification}}$$

s.t.

IR constraints

$$(a)\ \theta_s v_1\left(R_{TR,s}\right) - \varepsilon_1 V_{TR,s} \geq 0, \rightarrow \text{Utility of type-}s\text{ relay device}$$

$$(b)\ \psi_q v_2\left(R_{BV,q}\right) - \varepsilon_2 V_{BV,q} \geq 0, \rightarrow \text{Utility of type-}q\text{ verifier}$$

IC constraints

$$(c)\ \theta_s v_1\left(R_{TR,s}\right) - \varepsilon_1 V_{TR,s} \geq \theta_s v_1\left(R_{TR,s'}\right) - \varepsilon_1 V_{TR,s'},$$

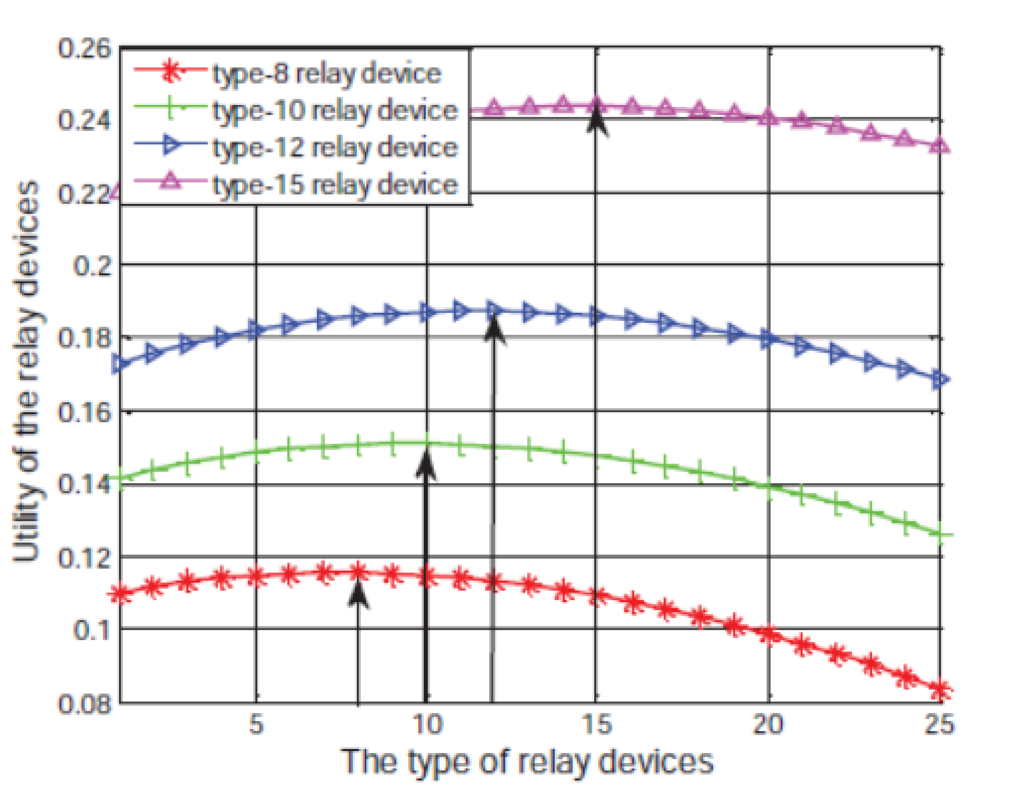
$$(d)\ \psi_q v_2\left(R_{BV,q}\right) - \varepsilon_2 V_{BV,q} \geq \psi_q v_2\left(R_{BV,q'}\right) - \varepsilon_2 V_{BV,q'},$$

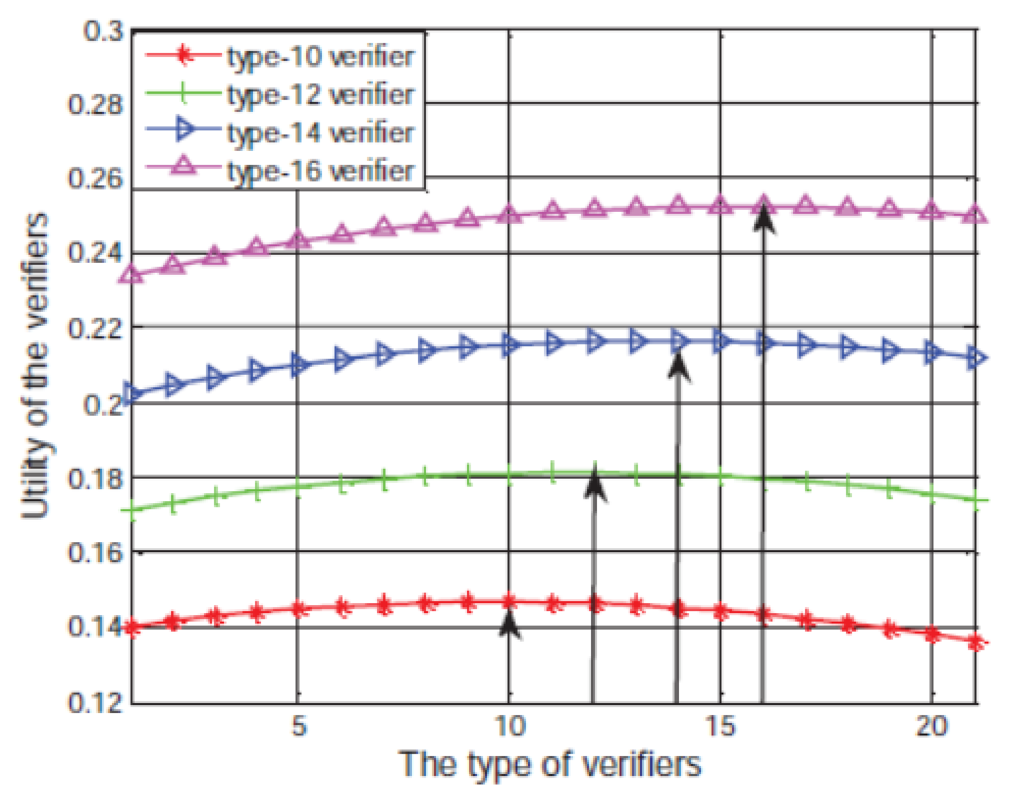
$$(e)\ \sum_{s=1}^{S} \lambda_s M R_{TR,s} + \sum_{q=1}^{Q} \lambda_q N R_{BV,q} \leq R_{max}, \rightarrow \text{Maximum reward provided by the local AP}$$

$$(f)\ l_1 + l_2 = 1, \rightarrow \text{Weight constraint of the relay fee and the transaction fee}$$

$$\forall s, s' \in \{1,\ldots,S\}, s \neq s', and\ \forall q, q' \in \{1,\ldots,Q\}, q \neq q'.$$

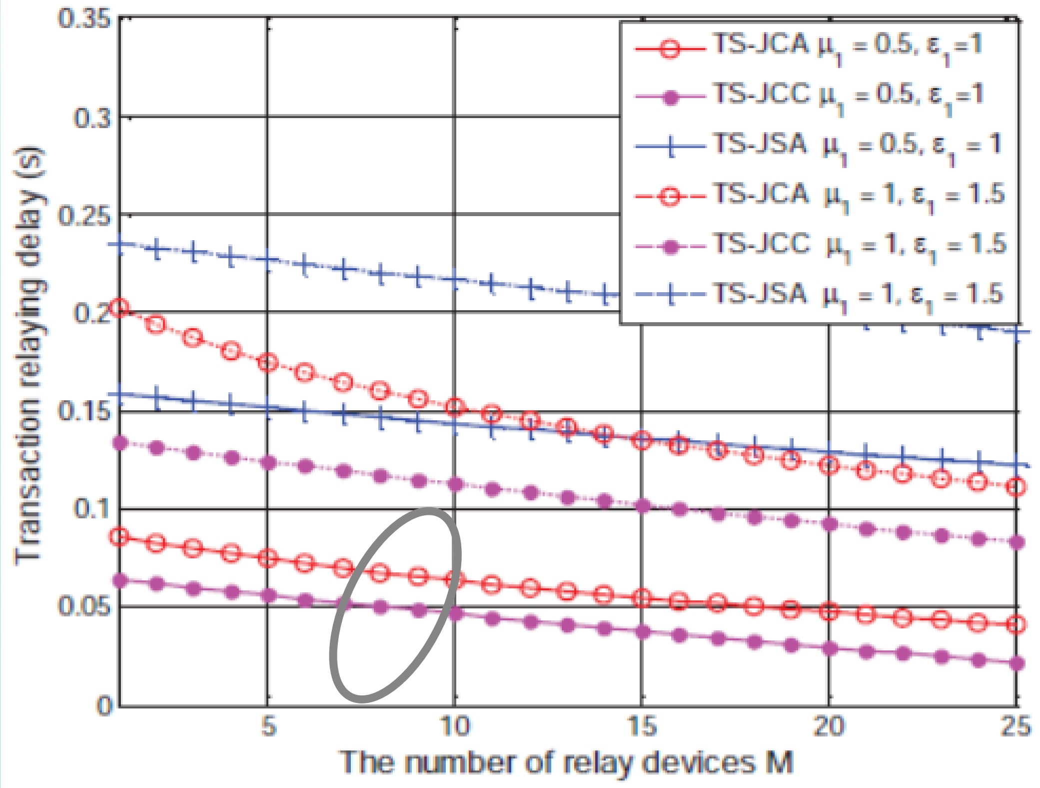
Utilities of relay device and verifier

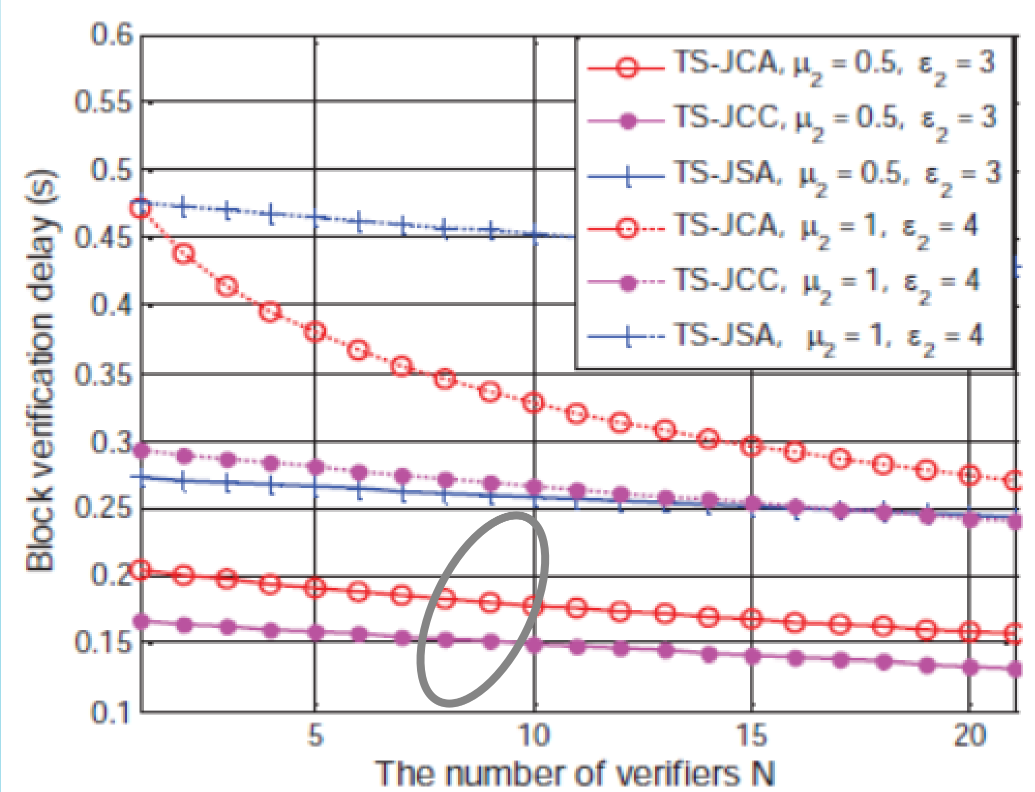




- Relays and verifiers maximize utility if selecting contract for their own types
- Overcoming information asymmetry: relay devices and verifiers will reveal their types truthfully after selecting the contract designed for their own types

Relaying delay and block verification delay





- Delay decreases with the increasing number of relay devices or verifiers.
- Transaction relaying delay and block verification delay of our TS-JCA scheme is only slightly inferior to TS-JCC (TS-JCC: scheme with complete information)

05

BLOCKCHAIN AND FEDERATED LEARNING: *PRIVACY*

- Y. Lu, X. Huang, Y. Dai, S. Maharjan and Y. Zhang, "Blockchain and Federated Learning for Privacy-preserved Data Sharing in Industrial IoT", IEEE Transactions on Industrial Informatics, vol.16, no.6, pp.4177-4186, June 2020

Observations/motivations

Privacy protection is becoming extremely important worldwide

GDPR (EU General Data Protection Regulation)

July 8, 2019, British Airline faces 183Million GBP fines
2019年7月8日，英国航空收到1.83亿英镑（约16亿人民币）巨额罚单

CCPA (California Consumers Privacy Act)

Effective from January 2020
美国加州消费者隐私法案2020年1月起开始生效

罚款: 7500USD/California customer

CES (Consumer Electronics Show) 2020

In CES 2020 at Las Vegas, data privacy is the hottest topic presented by Apple, Facebook, Amazon, Google

Federated learning: concept

Centralized learning

all data are sent to the central server, which train the centralized datasets.

$$D = D_1 \cup D_2 \cup \ \ldots \ \cup D_n$$

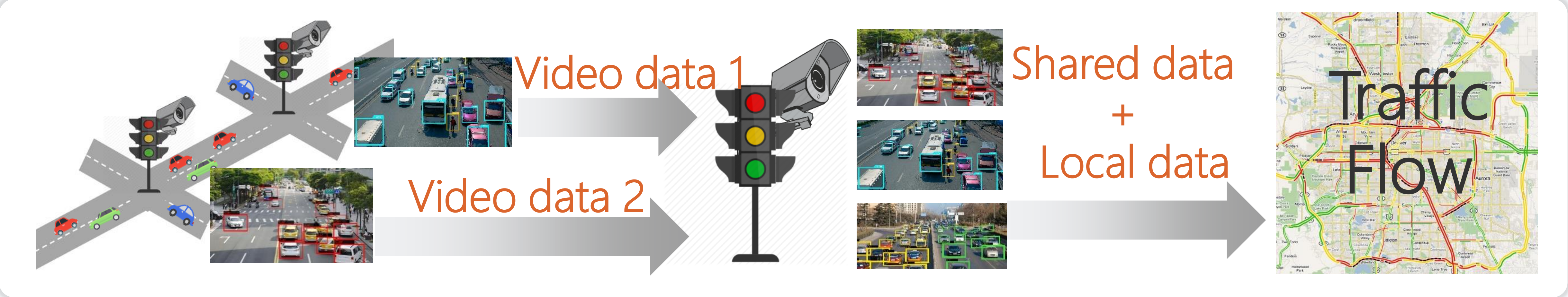
Federated learning

users train a model and send it to the central. Personal data are kept locally.

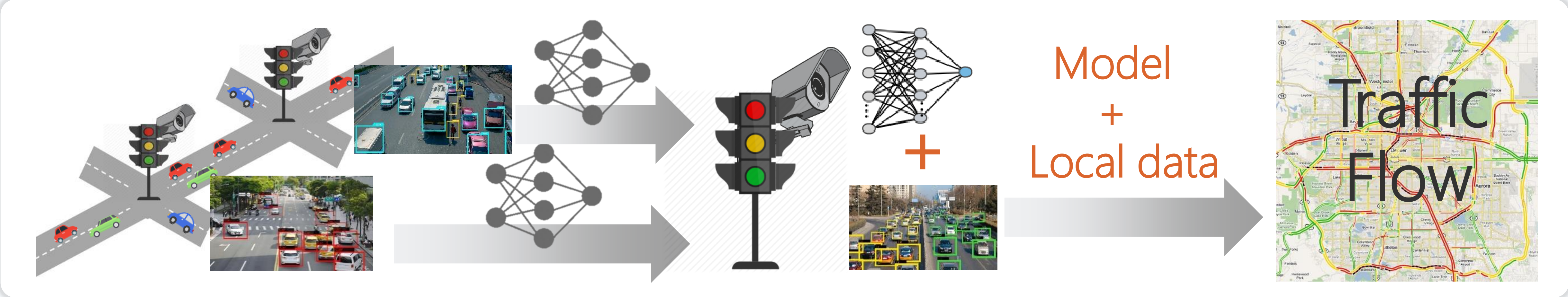
$$W = W_1 \cup W_2 \cup \ \ldots \ \cup W_n$$

Federated Learning for Transport: *example*

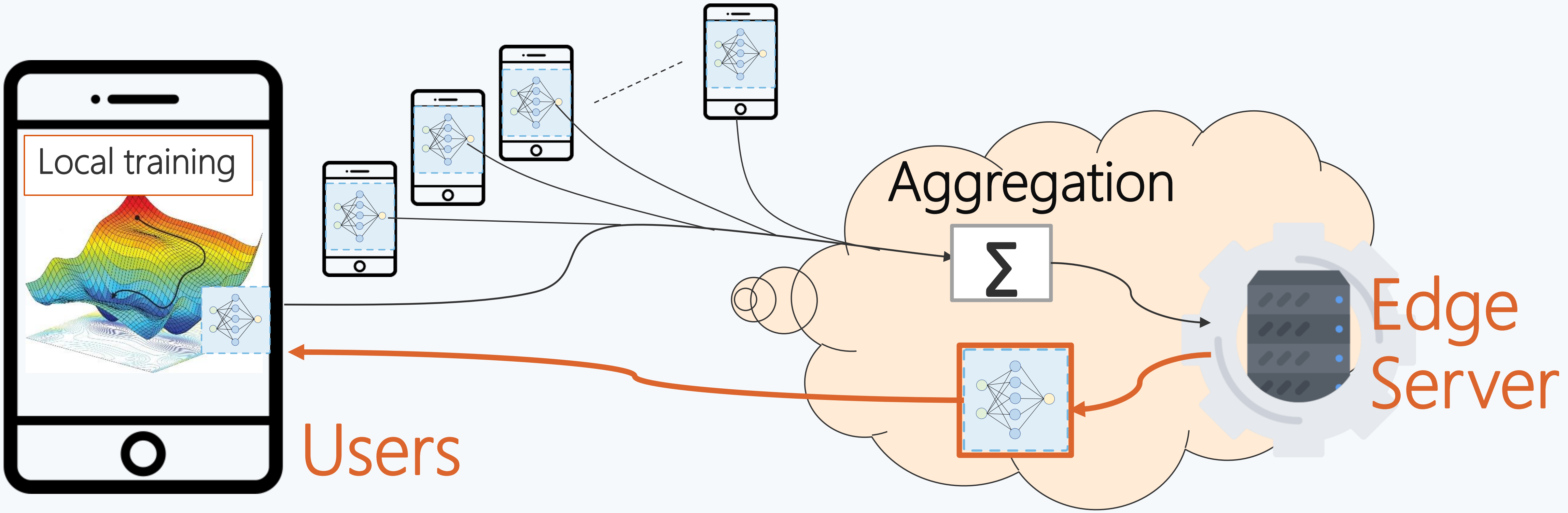
Traditional video data sharing



Federated Learning for model sharing



Federated learning: *3-step principle*



01 **computation:** all nodes make the local training and build model

02 **communications:** all nodes transmit model parameters to the server

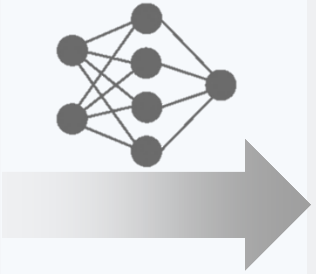
03 **aggregation:** aggregates the local models into a global model

Federated learning: model

Each device: local training

- Local model parameters $\boldsymbol{w_t}$
- Loss function $\boldsymbol{L(w_t)}$
- Find optimal $\boldsymbol{w_t}$ to minimize $\boldsymbol{L(w_t)}$, through gradient descent

Update



Edge server: global aggregation

- The server aims at minimizing the global loss function
- For example: averaging aggregation

$$\boldsymbol{w_t = w_{t-1} + \alpha_t \cdot \nabla L_i(w_t)}$$

Model parameters in iteration t

Gradient of loss function

$$\boldsymbol{W_G(t) = \frac{1}{N} \sum_{i=1}^{N} w_i(t)}$$

Global model parameters

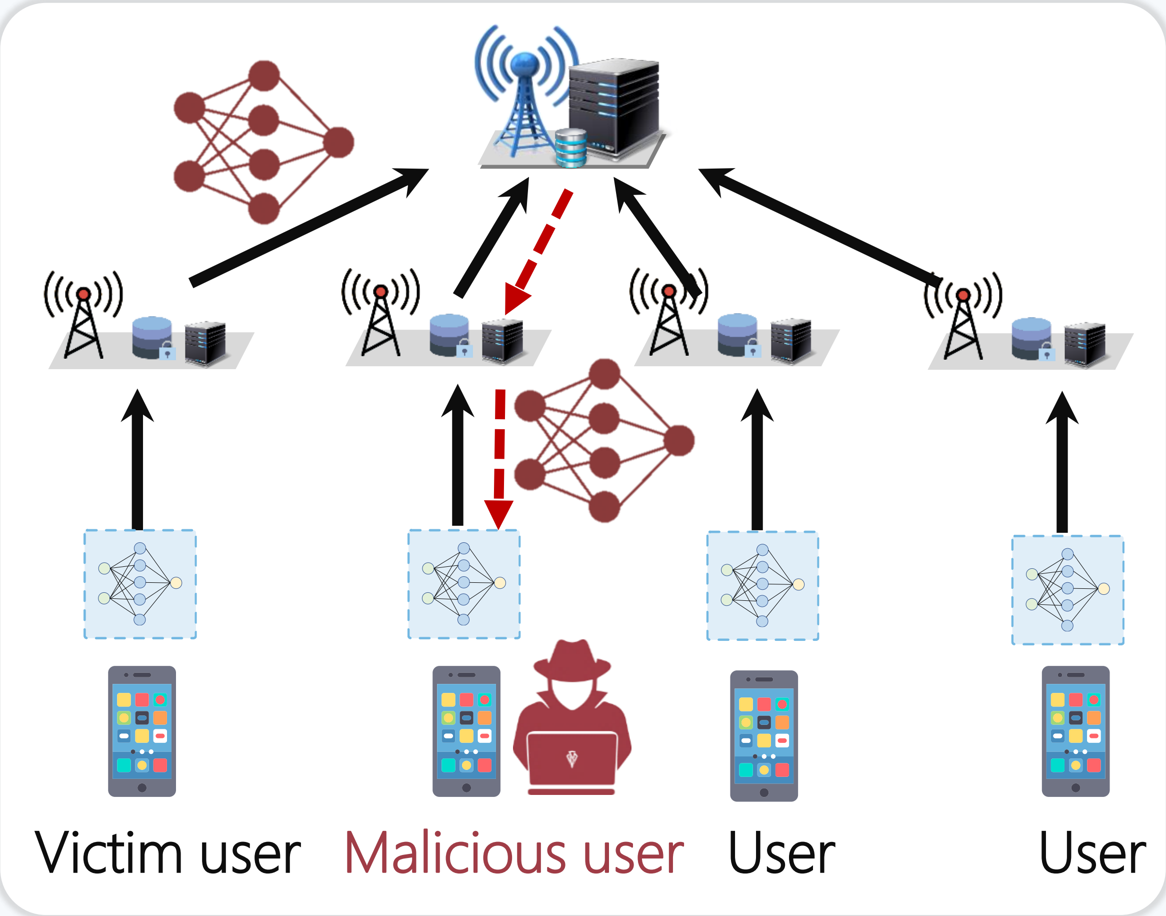
Federated learning: *benefits & challenges*

BENEFITS

- **Privacy:** protect user privacy since raw data is kept in the local environment
- **Performance:** can easily extend the scale of training data

TWO CHALLENGES

- **Privacy**: parameters privacy
- **Efficiency**: communications and computation efficiency in aggregation



Parameters/Models privacy

Federated learning: *key research questions*

ENHANCE PRIVACY AND SECURITY

Protect the privacy of parameters. Build trust mechanisms among users

Our focus

VULNERABILITIES OF THIRD-PARTY

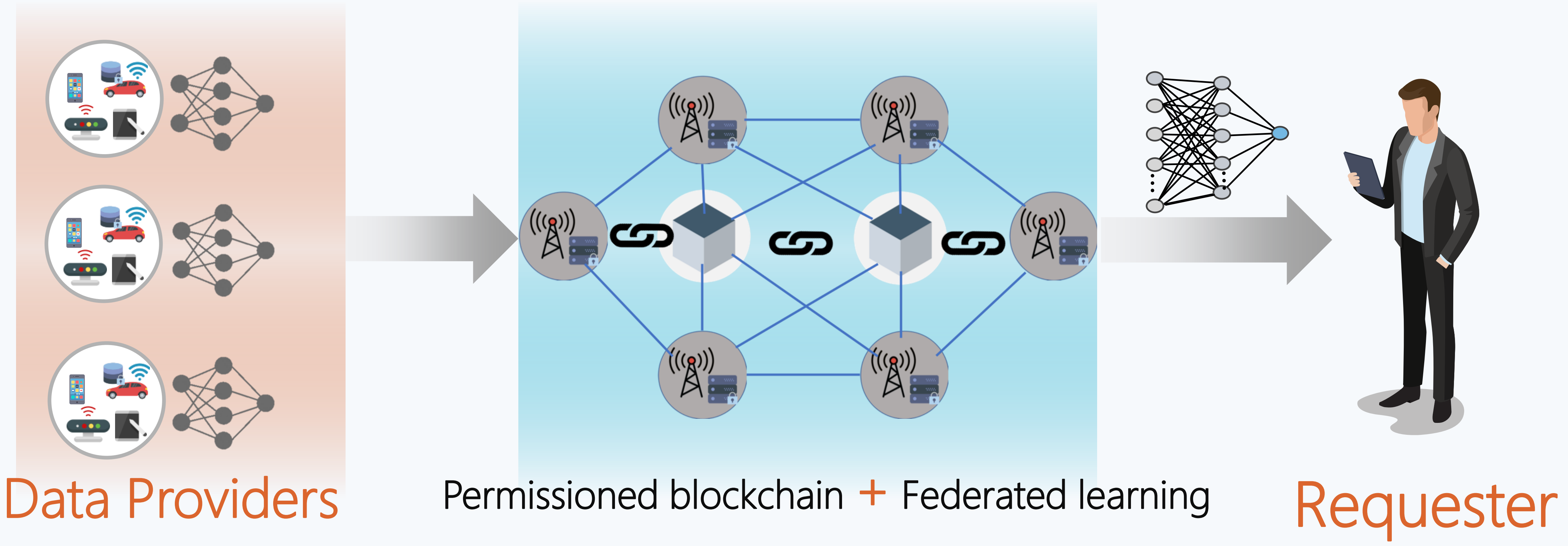
In case of single point failure, learning process is failed and leaks data

IMPROVE EFFICIENCY

Reduce wireless communications and computation cost

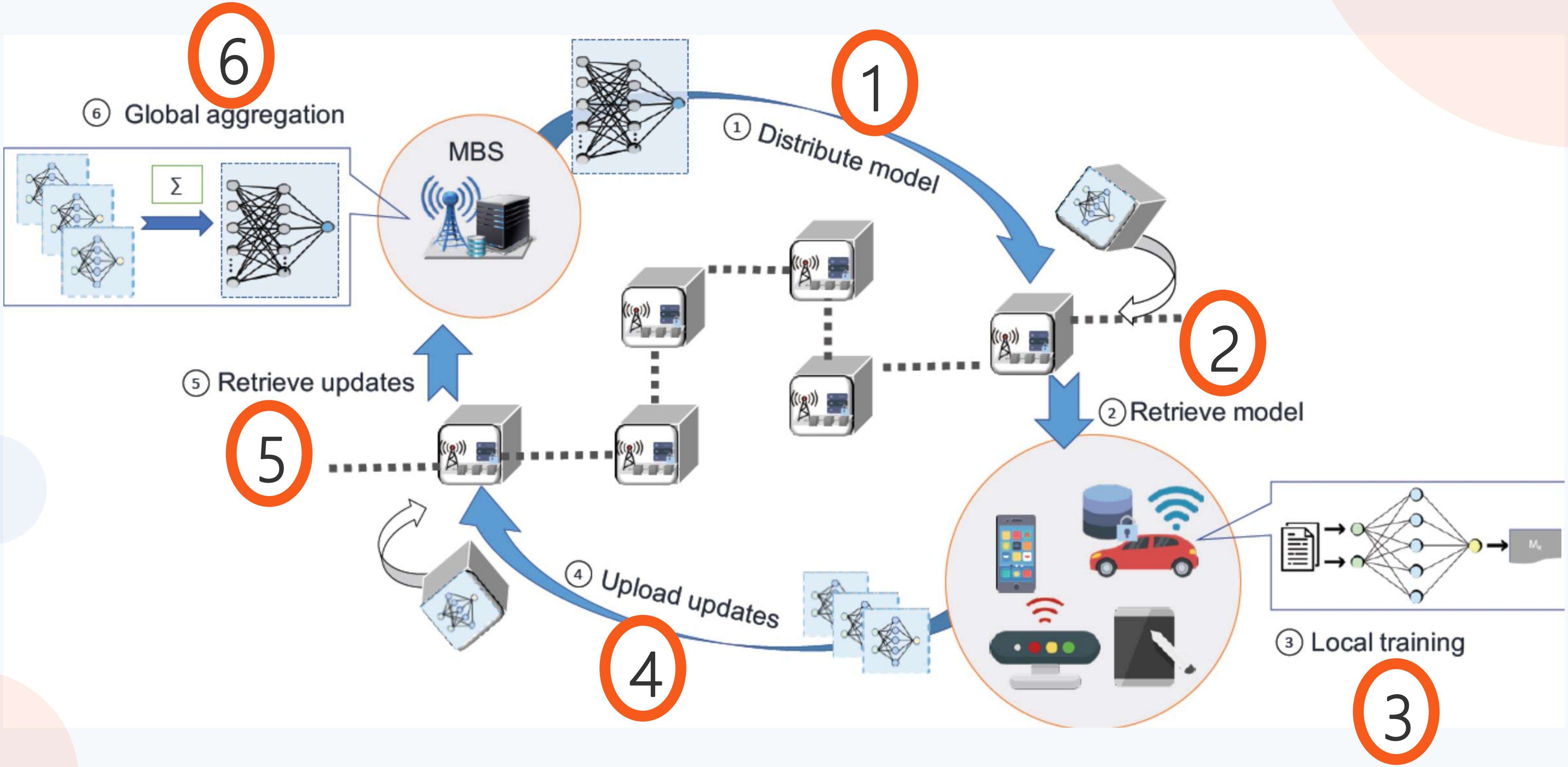
Our focus: need to build trust among users, protect the parameters, and avoid the vulnerability of the third-party servers → perfectly Blockchain principle

Blockchain + Federated Learning for data privacy



- **Data requester:** data users, IoT devices
- **Data providers (IoT devices):** register to blockchain with data profiles, and run local training
- **Parameter blockchain:** records and retrieve data and parameters/models, verify models

Model sharing process



Federated learning: *determine multiparty for data retrieval*

Select data providers

- Include more relevant providers to improve accuracy
- Refer to registered data in Blockchain, e.g., data size, data type, we can classify the data providers based on node similarity

Select training data

- Each provider selects training data
- Local training with Differential Privacy (DP): add noise to local parameters

Training quality based consensus

Main Idea

Replace the PoW mining work with model verification work

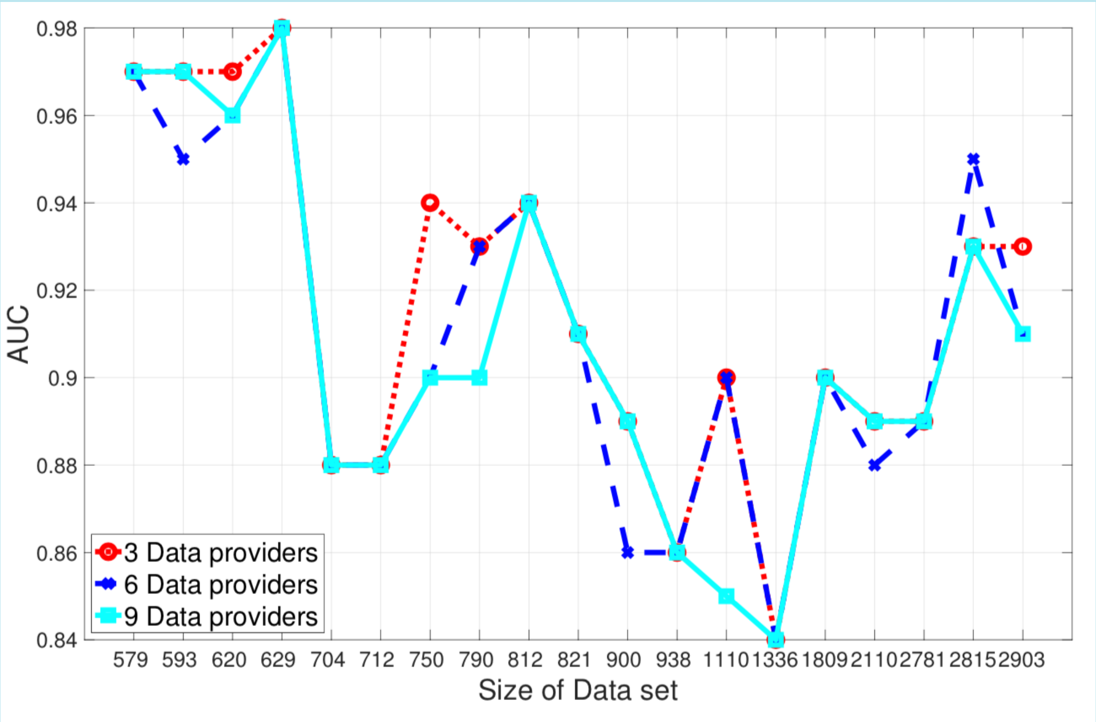
Consensus execution by verifiers

- Select a subset of participants as verifiers
- Verify the model quality based on federated learning results through the metric *mean absolute error (MAE).*

$$\mathrm{MAE} = \frac{1}{n}\sum_{j=1}^{n}|y_j - \hat{y}_j|$$

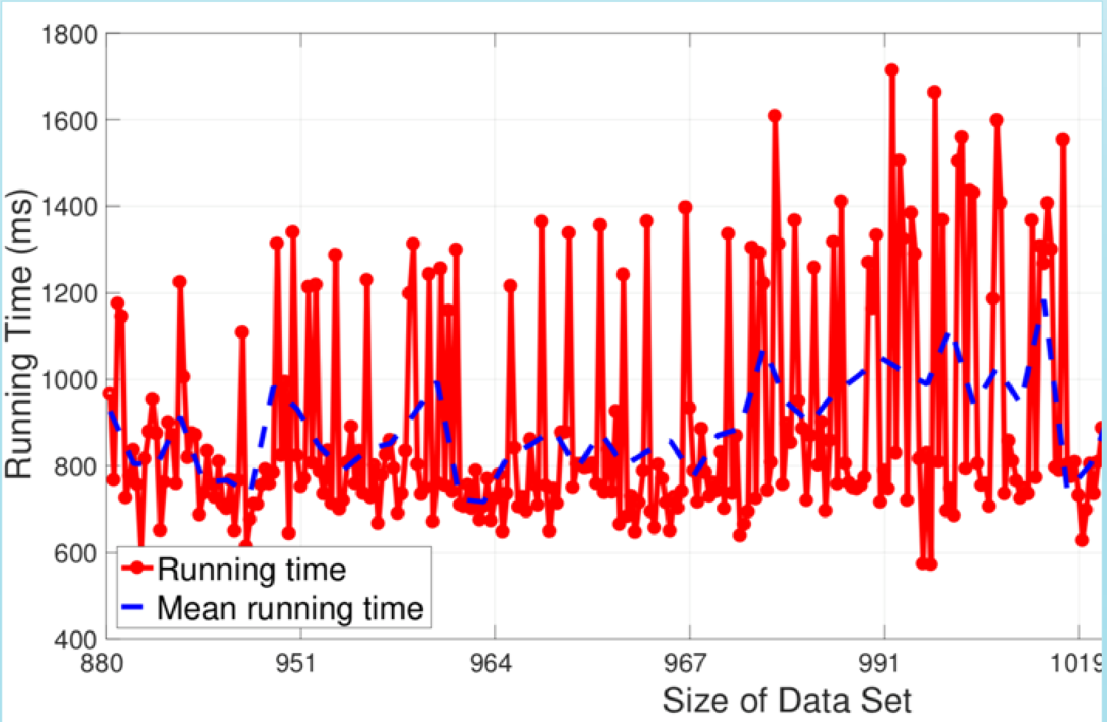
- If the accuracy satisfies the lower limit, the verifier will approve the transaction

Illustrative Results - *positive*



The proposed scheme with blockchain and federated learning

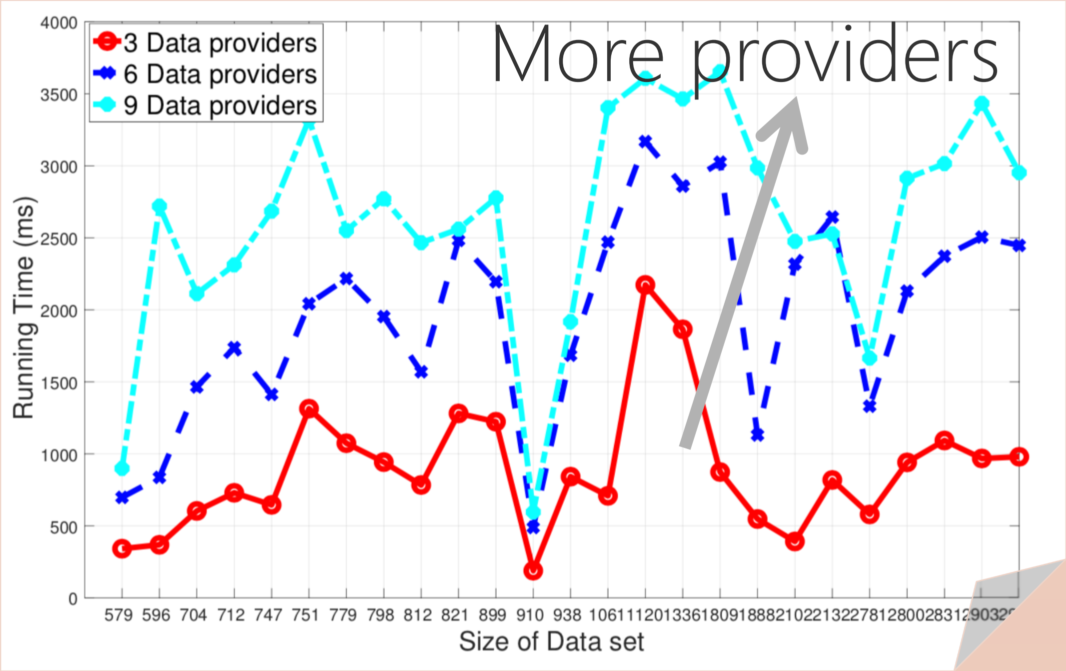
Achieves: high learning accuracy with various providers



The proposed scheme with blockchain and federated learning

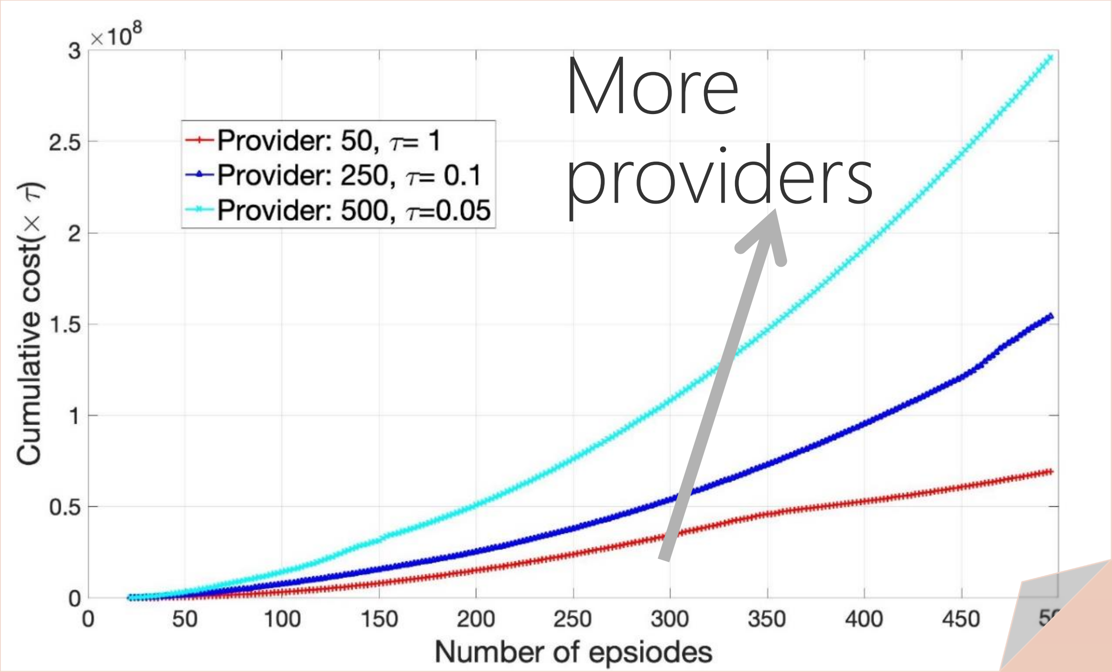
Achieves: good running time performance, from milliseconds to seconds

Illustrative Results - *negative*



Running time increases as the number of data providers increases.

Reason: the more providers, the more updated models need to be transmitted and processed, which is time consuming



Cost of maintaining the blockchain increases with more providers

Reason: we did not the communications cost in our proposed scheme. Needs improvement in the future work

06

BLOCKCHAIN AND FEDERATED LEARNING: *EFFICIENCY*

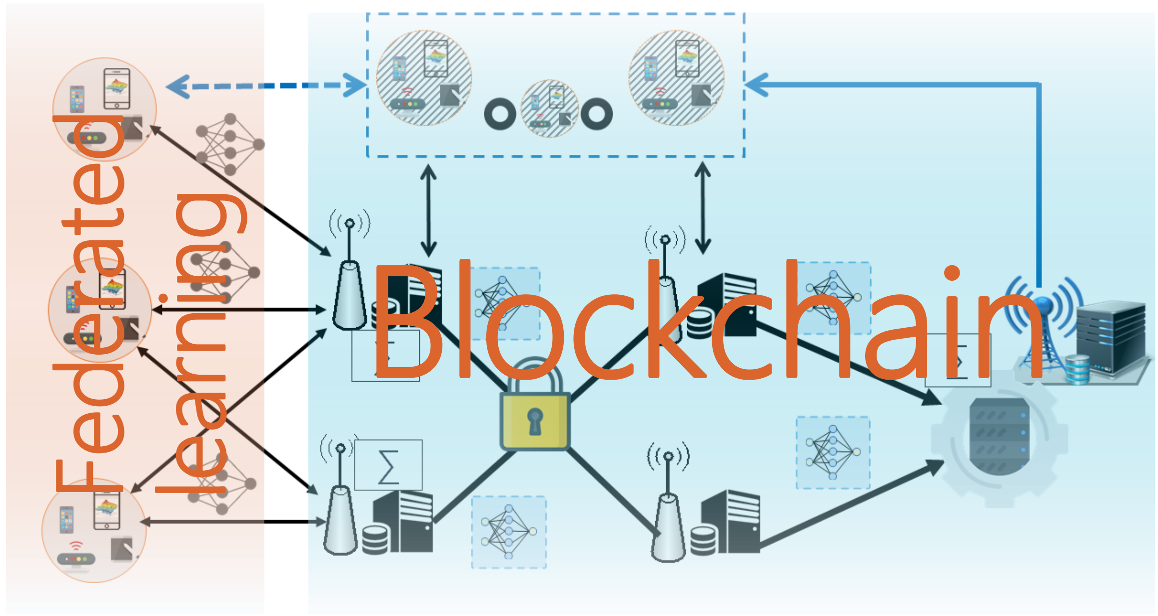
Federated learning and Blockchain: model

FEDERATED LEARNING

- Local training for model
- Transmit model parameters
- Model should be protected

CONSORTIUM BLOCKCHAIN

- Collect model parameters and store them as transactions
- Consortium blockchain verifies global model through consensus

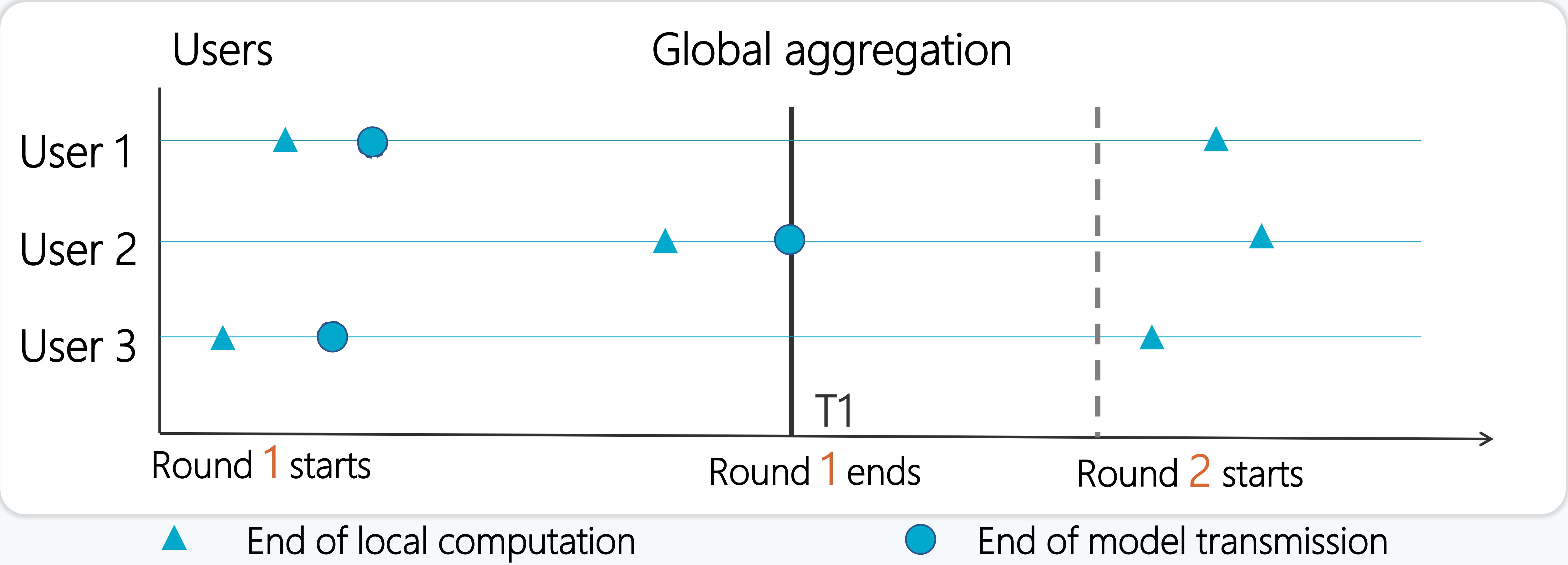


06.01

COMPUTATION EFFICIENCY

- Y. Lu, X. Huang, K. Zhang, S. Maharjan and Y. Zhang, "Blockchain Empowered Asynchronous Federated Learning for Secure Data Sharing in Internet of Vehicles", IEEE Transactions on Vehicular Technology, vol.69, no.4, pp.4298-4311, April 2020

Challenge: computation efficiency



Computation efficiency unbalance: user 2 is computing very slow and we may simply discard user 2

Asynchronous federated learning

Federated learning

- All users participate in the global aggregation in each round
- Limitation: long waiting cost due to different running/training time

Asynchronous federated learning

- Select part of users to participate in global aggregation
- The other users can continue the local training

Two research questions

01 how to decide the users to participate?

02 how to improve the training quality of the unselected nodes?

Asynchronous federated learning - *process*

We propose *node selection scheme* and *local aggregation* to address these two research questions

01 **Local training for all nodes**: train models based on gradient descent

02 **Node selection scheme**: choose the nodes with sufficient resources to participate the global aggregation

03 **Global aggregation**: RSUs perform global aggregation based on models from selected nodes

04 **Local aggregation**: execute local aggregation on nearby models for unselected nodes

Asynchronous federated learning

Node selection: Deep Reinforcement Learning

$$M = (S, \lambda, P_\lambda, C_\lambda)$$

State, action, probability, cost

Local training: use gradient descent to minimize loss function

$$\arg\min_{w} F(w)$$ loss function

$$w_t = w_{t-1} - \eta \nabla F_i(w_t)$$

Global/Local aggregation

perform aggregation based on models from local training

$$w(t) = \frac{1}{D} \sum_{i=1}^{N} D_i w_i(t)$$

Research problem

Problem definition: find the nodes selection policy λ^t that minimizes system cost c^t which consists of computing cost, communication cost, and training loss

$$\min_{\boldsymbol{\lambda}^t} \quad c^t(\boldsymbol{\lambda}^t)$$
$$\text{s.t.} \quad \lambda_i^t \in \{0,1\}, \forall i,$$
$$|p_{i|\lambda_i=1}(t) - p_c(t)| \leq r_0^2$$

System cost

The vehicles are within distance range $\mathbf{r}$

$$c^t(\lambda^t) = c^t_{te} + c^t_q$$

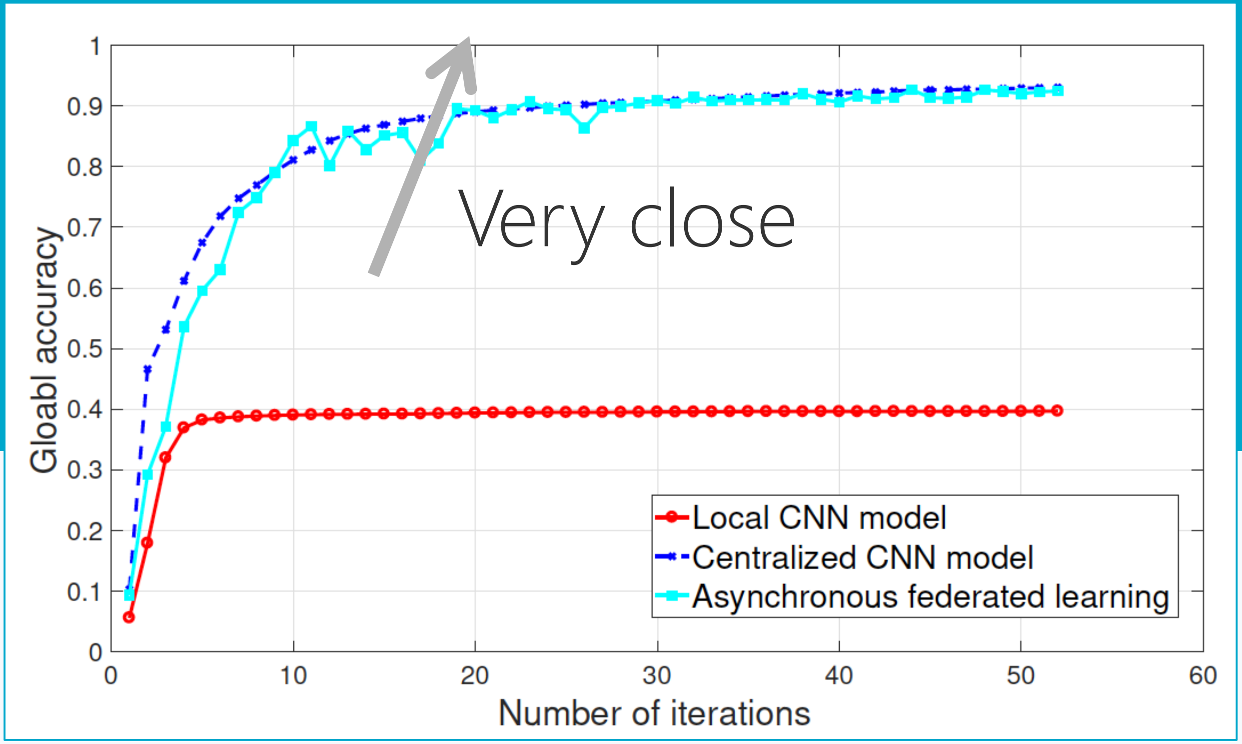
Computation and communication cost

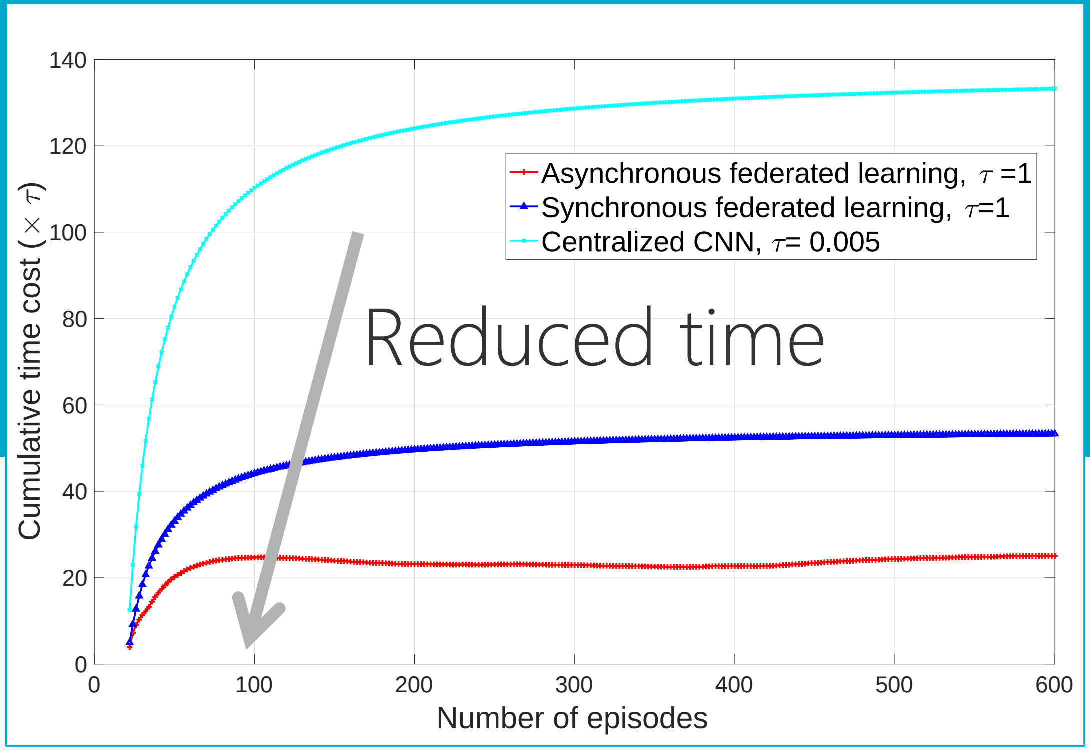
Learning accuracy loss

$$c_q^t = \sum_{i \in V_P} \sigma_i^t(w^t, d_i) = \sum_{i \in V_P} \sum_j L(y_j - \hat{w}^t(x_j))$$

learning loss function of models

Illustrative Results





Our asynchronous federated learning

smaller accuracy and convergence rate than benchmark, but the results are very close

Our asynchronous federated learning

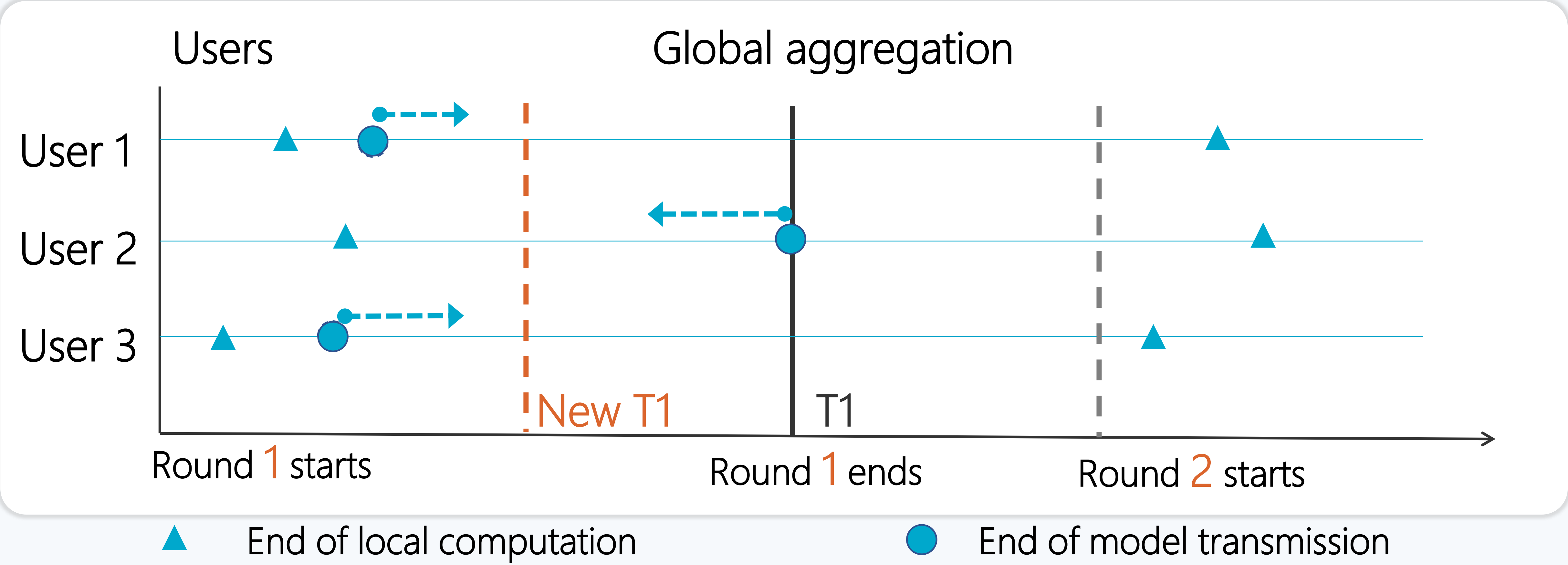
the time cost is reduced which optimally selects the participants based on their resources and training losses

06.02

COMMUNICATIONS EFFICIENCY

- Y. Lu, X. Huang, K. Zhang, S. Maharjan, and Y. Zhang, "Communication-Efficient Federated Learning for Digital Twin Edge Networks in Industrial IoT", IEEE Transactions on Industrial Informatics, DOI: 10.1109/TII.2020.3010798

Challenge: communication efficiency



Idea to mitigate the performance unbalance: Assign slow user 2 with more resources, while assign fast users 1 and 3 with less resources.

Research problem: execution time imbalance

Minimize the execution time imbalance under constraints of energy consumption, communication and computation capabilities

$$\min_{\boldsymbol{f},\boldsymbol{\lambda},\boldsymbol{\theta}} \frac{1}{\sum_{i=1}^{N} \lambda_i} \sum_{i=1}^{N} \lambda_i (T_i(\theta, t) - T_{ave}(\boldsymbol{\lambda}, \boldsymbol{\theta}, t))^2$$

Computation subproblem

- minimize the energy cost and computation time

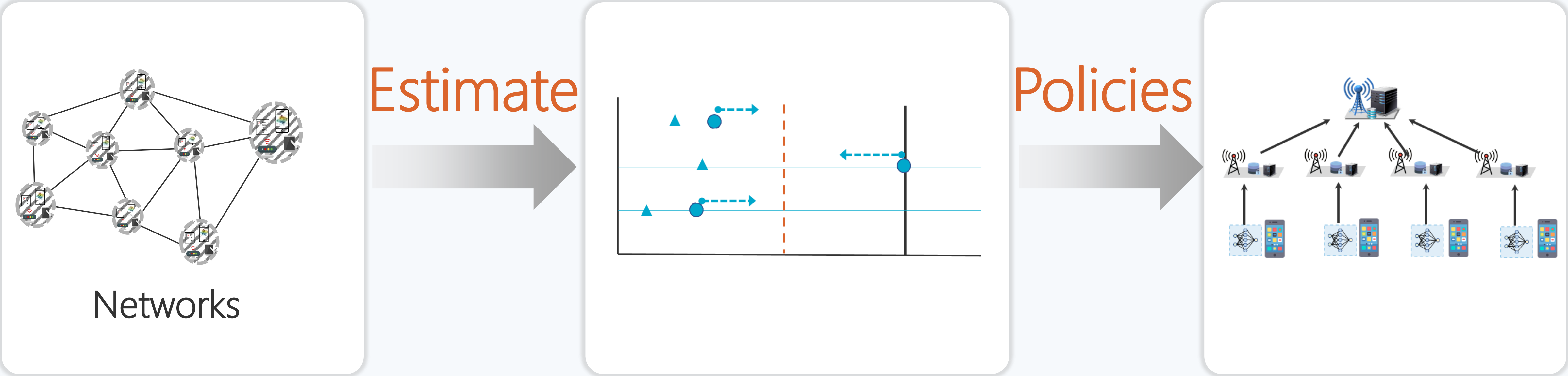
$$\min_{\boldsymbol{f}_i} \sum_{i=1}^{N} E_n^{cmp}(f_i) + \gamma T^{cmp}$$

Communications subproblem

- minimize the execution time difference under energy constraints

$$\min_{\boldsymbol{\lambda},\boldsymbol{\theta}} \sum_{i=1}^{N} \lambda_i (T_i^{com}(\theta, P_i, t) + T_i^{cmp} - T_{ave})^2$$

Resources optimization

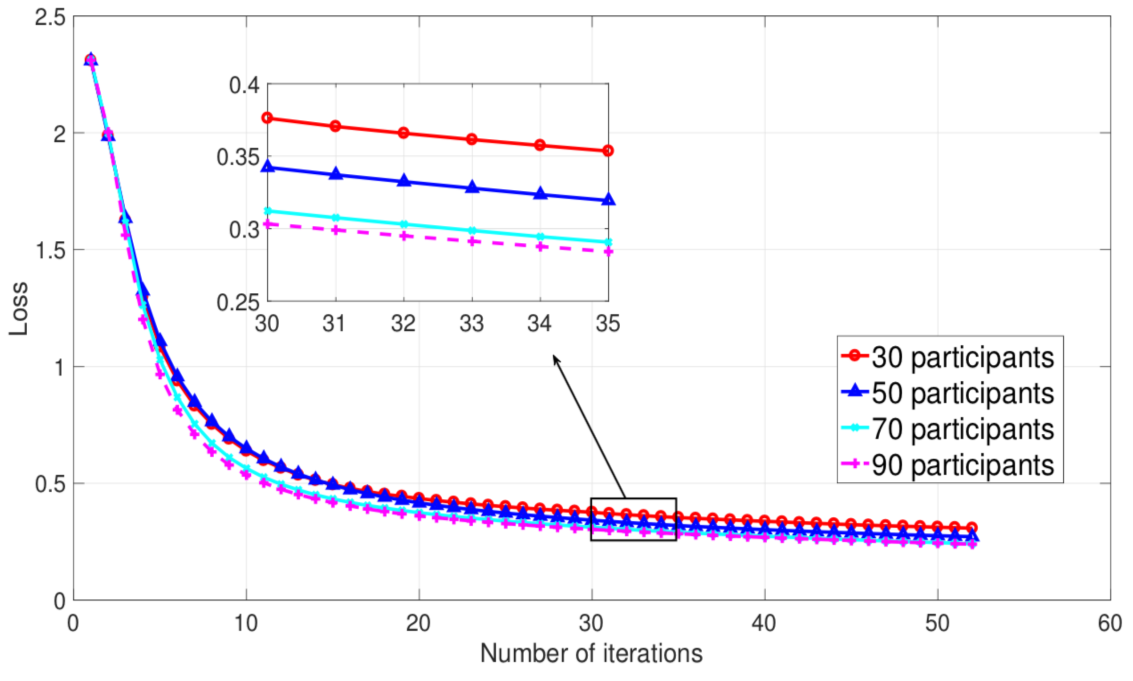


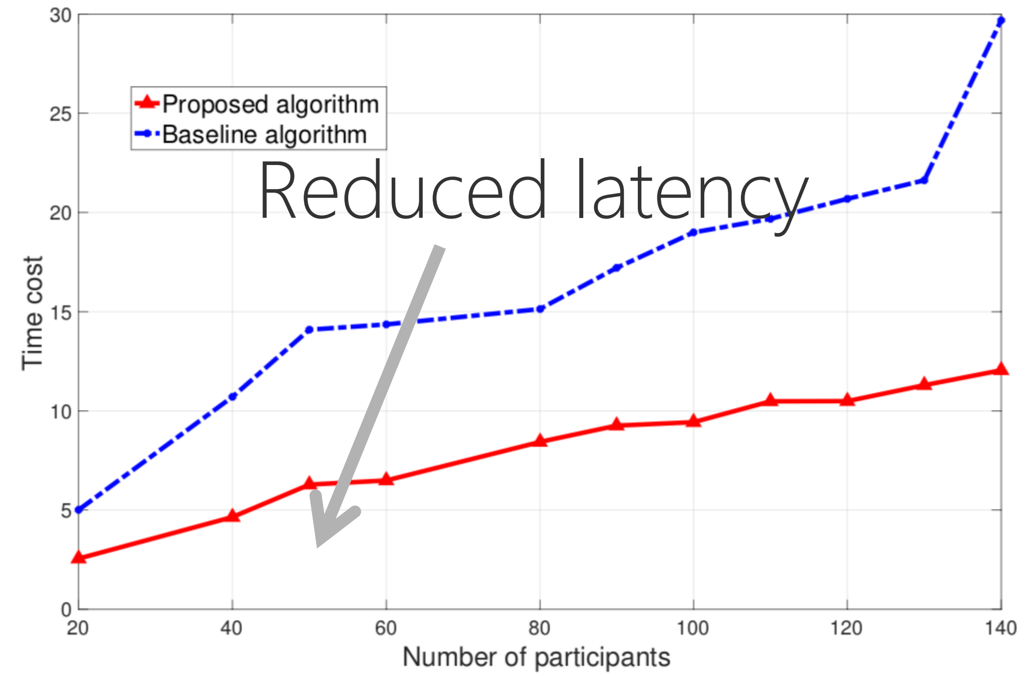
01 **Initialization:** assigning good channels and more resources to slow users

02 **Networks:** estimate time cost and user's own time; then assign channels to minimize the difference between these two times.

03 **Policy**: minimize system overall cost via DNN to find the optimal policy.

Illustrative Results





The proposed scheme with federated learning

Achieves: good learning accuracy

The proposed scheme with federated learning

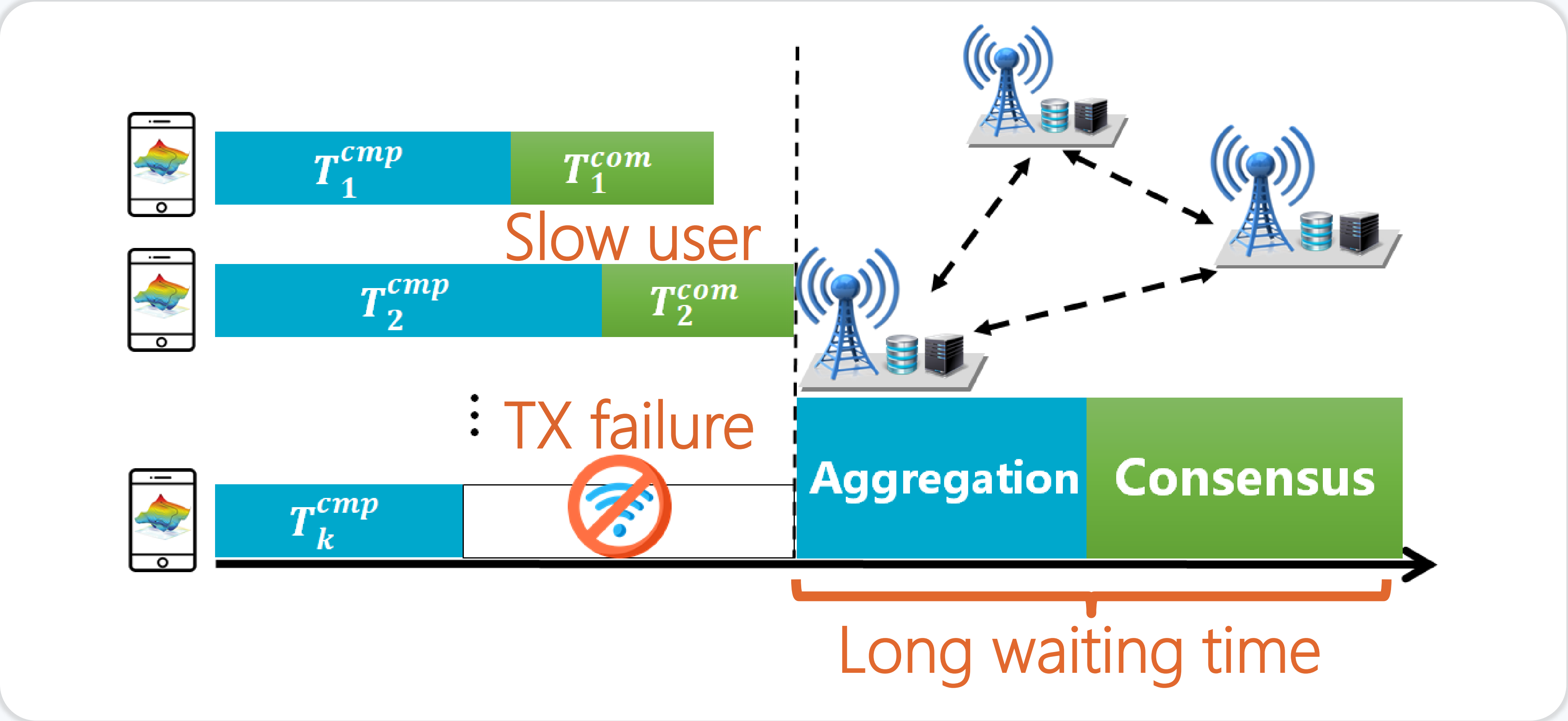
Achieves: lower latency

06.03

COMMUNICATIONS-COMPUTATION EFFICIENCY

- Y. Lu, X. Huang, K. Zhang, S. Maharjan, and Y. Zhang, "Communication-efficient Federated Learning and Permissioned Blockchain for Digital Twin Edge Networks", IEEE Internal of Things Journal, DOI: 10.1109/JIOT.2020.3015772

Federated learning and Blockchain



- **Research challenge:** slow users in federated learning and blockchain consensus may lead to communication congestion, long waiting time and high latency

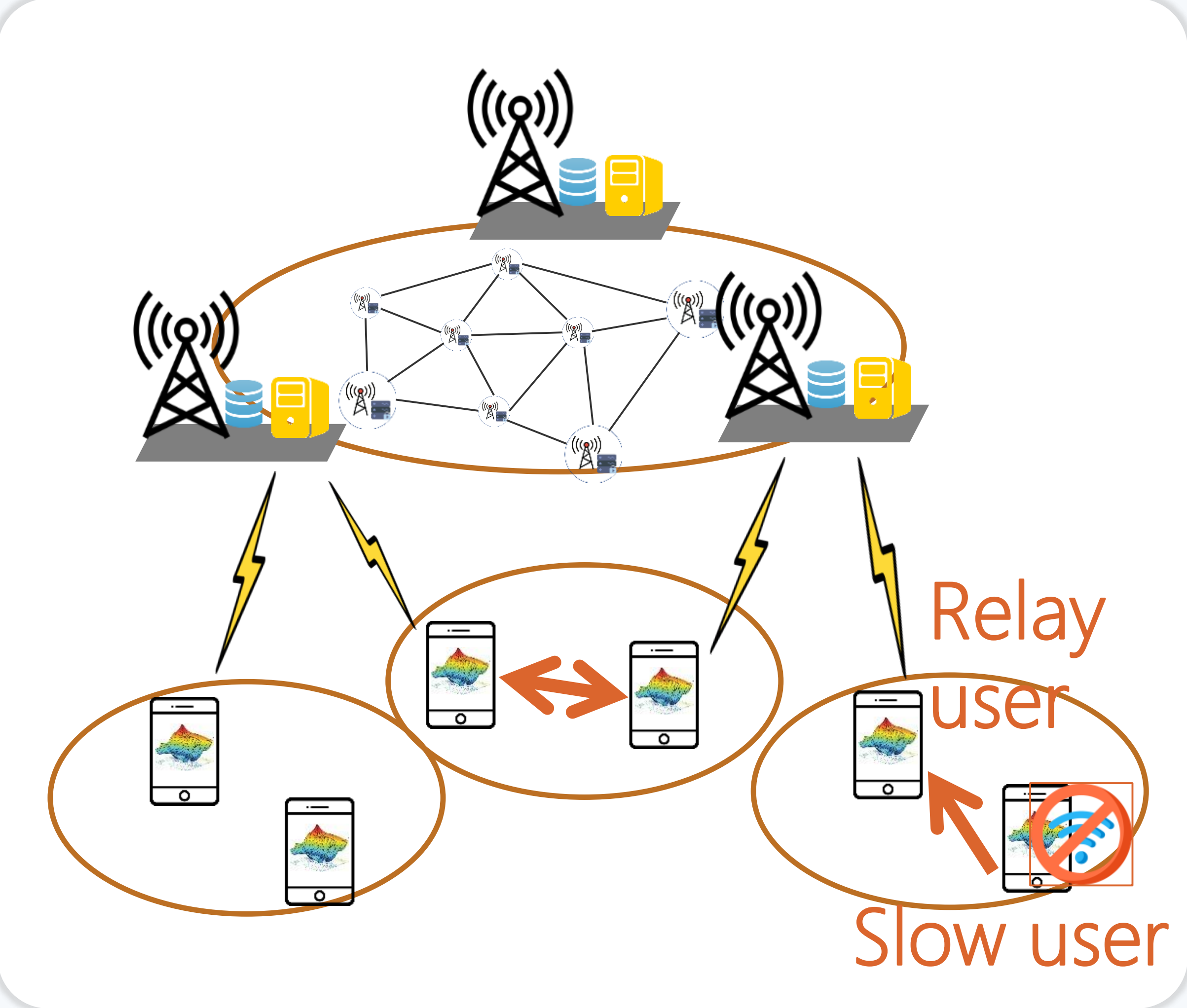
Research problem: optimal relay selection

Main observation

- Slow users: compute the training models, but unable to transmit parameters timely
- Relay users: have good communication capabilities

Optimal relay

- Select optimal relay users to help slow users $< \boldsymbol{u_i}, \boldsymbol{u_j} >$ to transmit models with minimal system cost



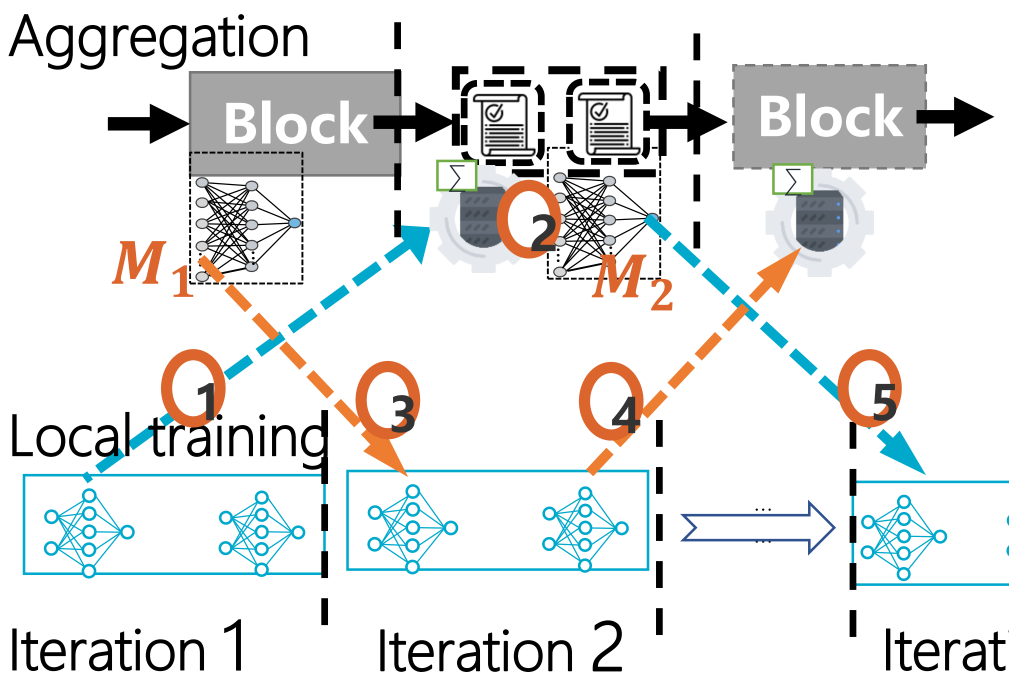
Reducing latency in Blockchain consensus

Blockchain

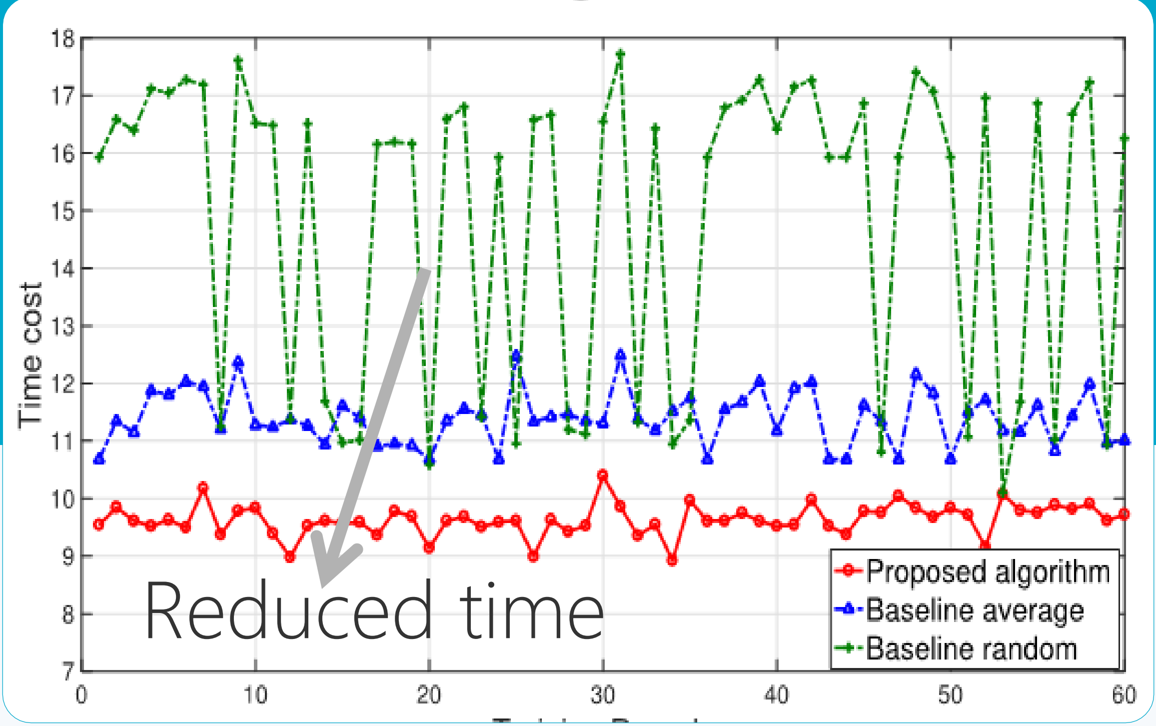
- Global states, devices behavior
- Store and verify models

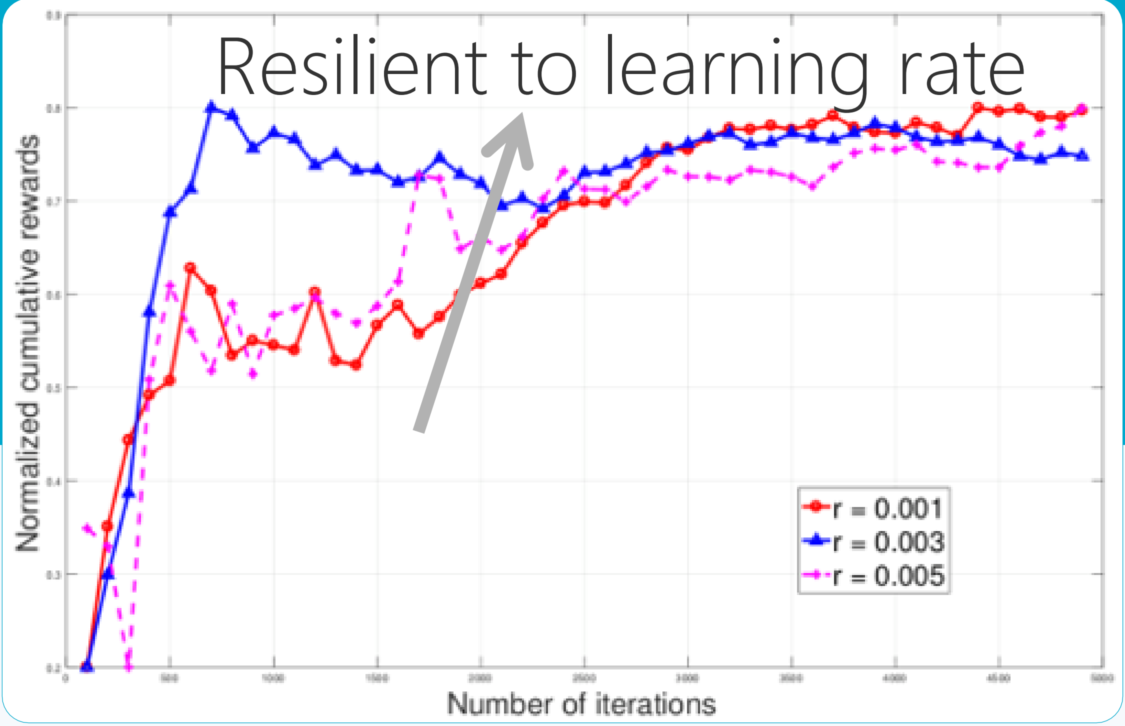
Reducing latency in consensus

- In iteration 2, system retrieves verified model M_1 from Blockchain for local training instead of waiting for M_2 to be verified
- This can greatly reduce latency



Illustrative Results





The proposed scheme with blockchain and federated learning

Achieves: reduced time cost

The proposed scheme with blockchain and federated learning

Achieves: good training policy performance

Thanks!
Q & A?

Yan Zhang
University of Oslo, Norway

yanzhang@ieee.org


Welcome to Visit Norway

Welcome to Visit Oslo

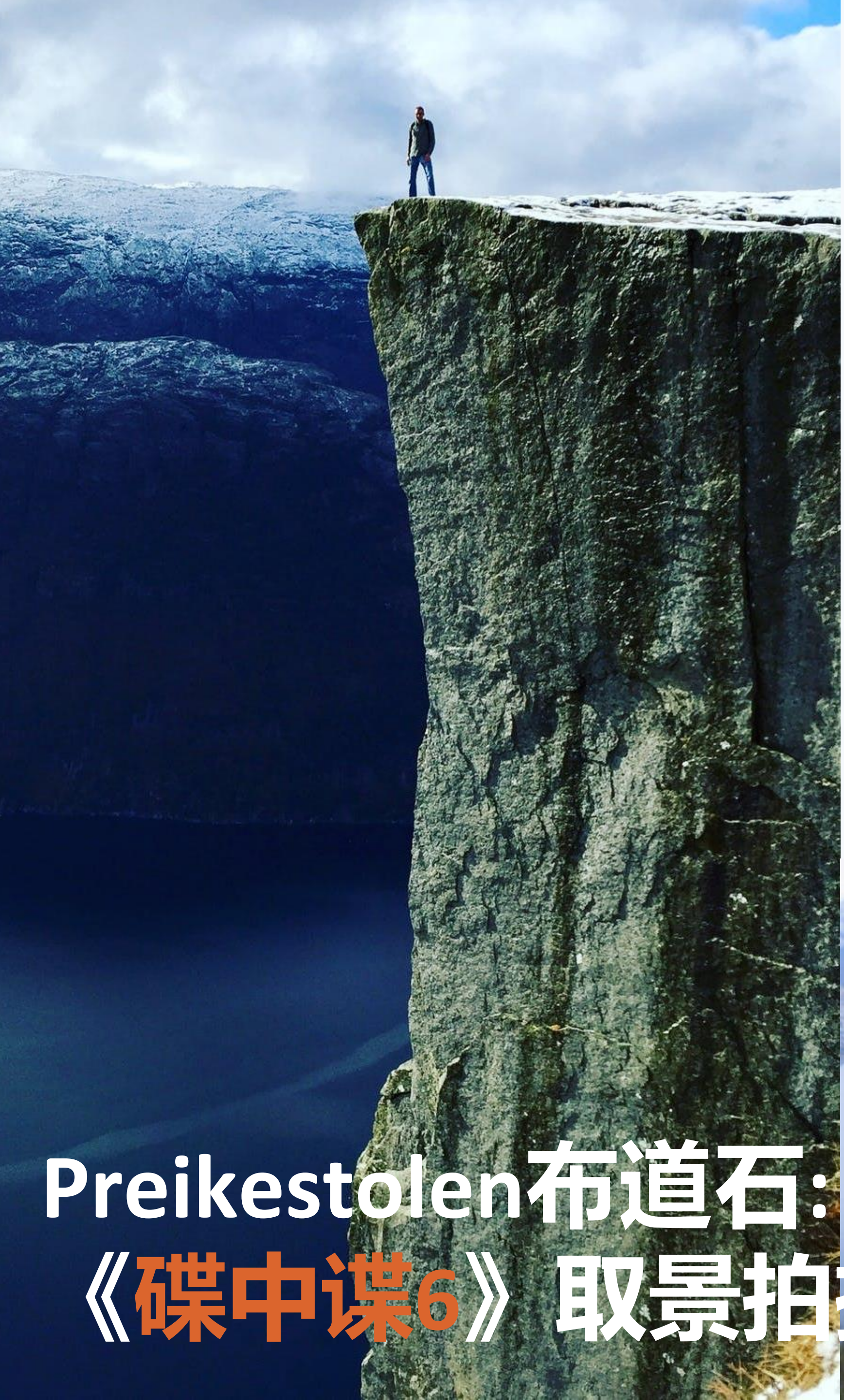








恶魔之舌 (Trolltunga)



Preikestolen布道石:
《碟中谍6》取景拍摄