NANYANG TECHNOLOGICAL UNIVERSITY

When Internet of Vehicles Meets Blockchain: A Perspective of Consensus Optimization

Jiawen Kang

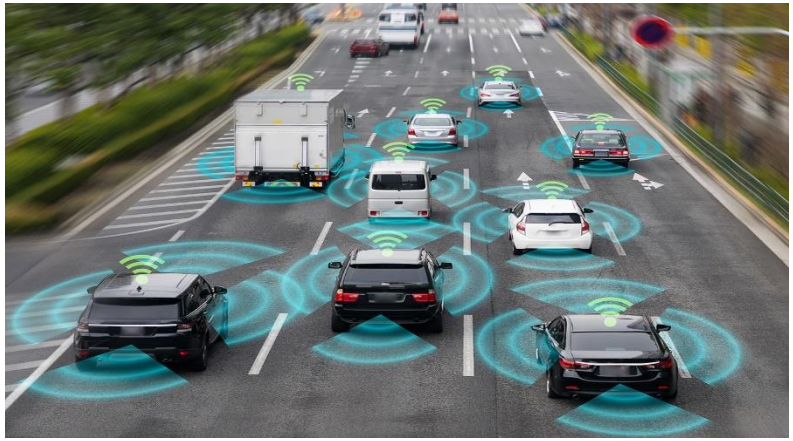
Nanyang Technological University

Ref. [1]: J. Kang, Z. Xiong, D. Niyato, D. Ye, D. I. Kim and J. Zhao, "Toward Secure Blockchain-Enabled Internet of Vehicles: Optimizing Consensus Management Using Reputation and Contract Theory," in *IEEE Transactions on Vehicular Technology*, vol. 68, no. 3, pp. 2906-2920, March 2019.

Outline

- **Preliminary: Internet of Vehicles Meets Blockchains**
  - Internet of Vehicles
  - Blockchain
  - Delegated Proof of Stake (DPoS)
  - Security Challenges for DPoS
  - Solutions for DPoS challenges
- **Reputation for Secure Block Verification**
  - Reputation
  - Subjective Logic Model for Reputation Calculation
- **Contract Theory based Incentive Mechanism**
  - Contract Theory
  - Problem Formulation and Solution
- **Performance Evaluation**
- **Summary**

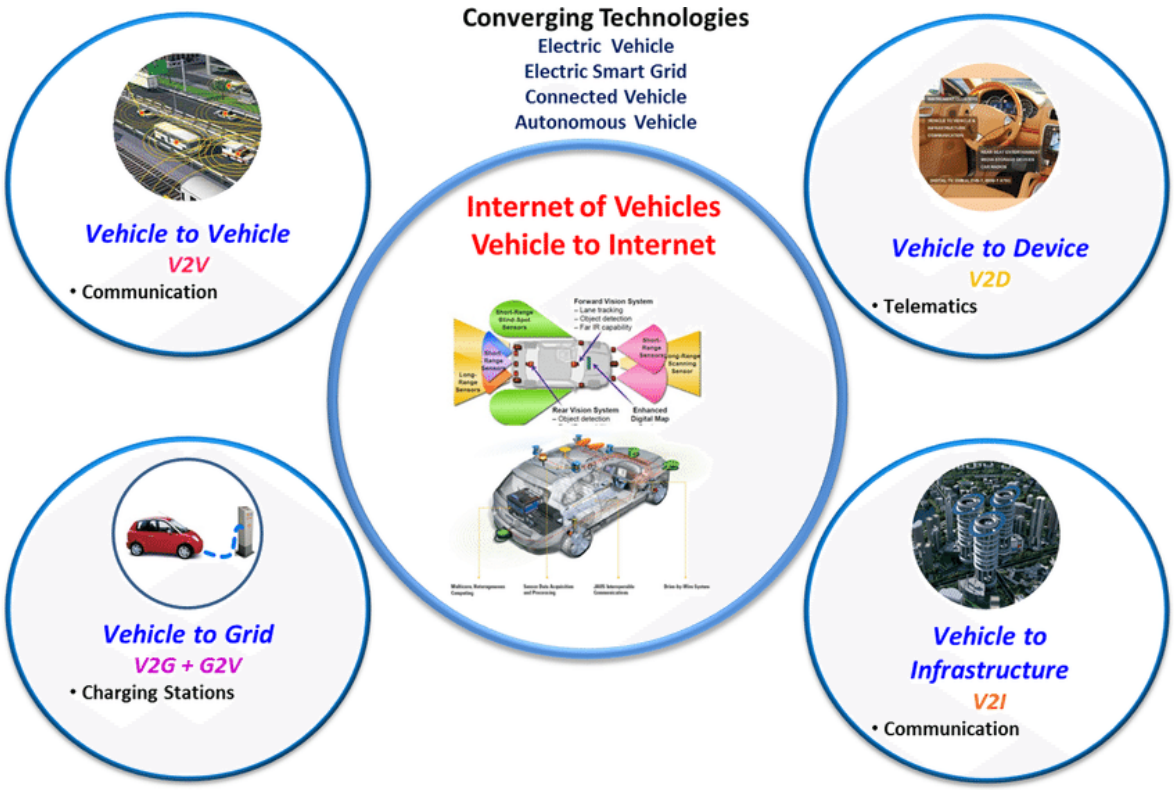
Internet of Vehicles



- The new era of the Internet of Things is driving the evolution of conventional Vehicle Networks into the Internet of Vehicles (IoV).
- Being in generation of Internet connectivity, there is a need to stay in safe and hassle free environment.
- According to recent predictions, 25 billion “things” will be connected to the Internet by 2020, of which vehicles will constitute a significant portion.

Internet of Vehicles

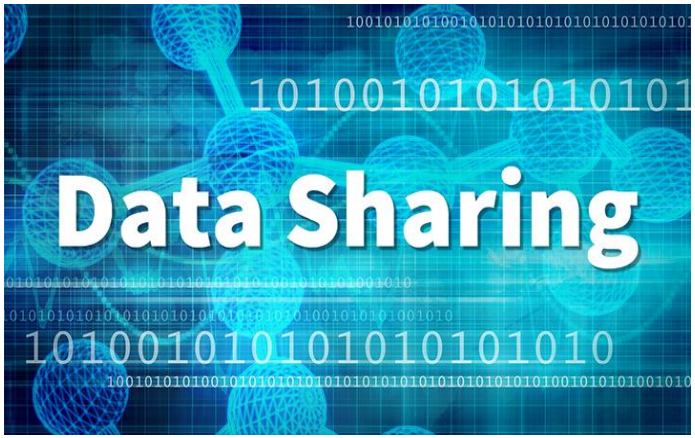
- IoV is basically INTERNET of VEHICLES, a strong network between vehicles and living.
- Vehicles-To-X Types:
  - Vehicles-To-Vehicles
  - Vehicles-To-Infrastructure
  - Vehicles-To-Cloud
  - Vehicles-To-Grid
  - Vehicles-To-Device



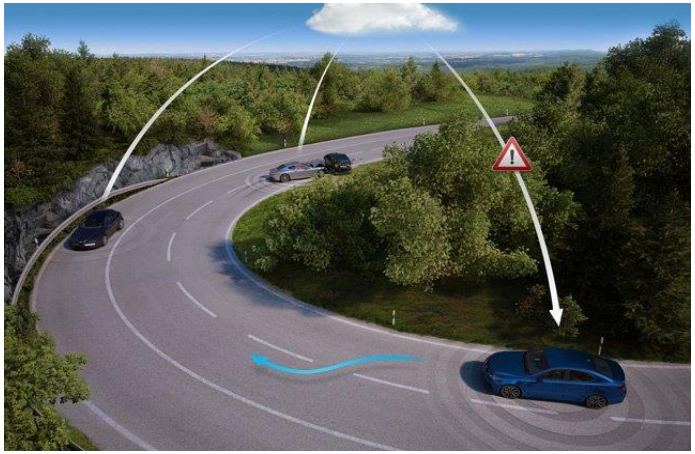
Internet of Vehicles

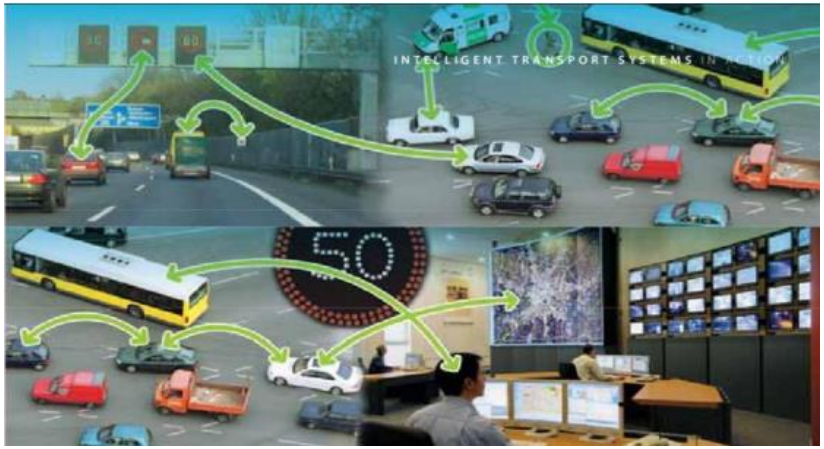
- Benefits
- Smart City
- Advanced Navigation
- Real time traffic Information
- Driver & Passenger Safety
- Fuel & Cost Efficiency
- Less traffic blocks …

Data Sharing in Internet of Vehicles



- Vehicles can cooperatively collect and share data of common interest, such as road conditions, and parking lot occupancy.
- These data can improve driving safety and enhance vehicular services

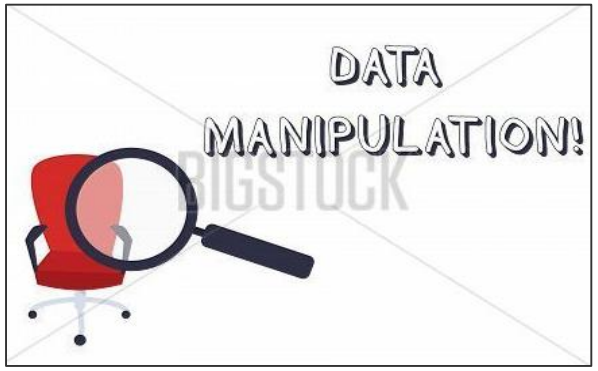




Critical Challenges in Data Sharing

- **Challenges:**

- Centralized management: single point of failure and personal data manipulation

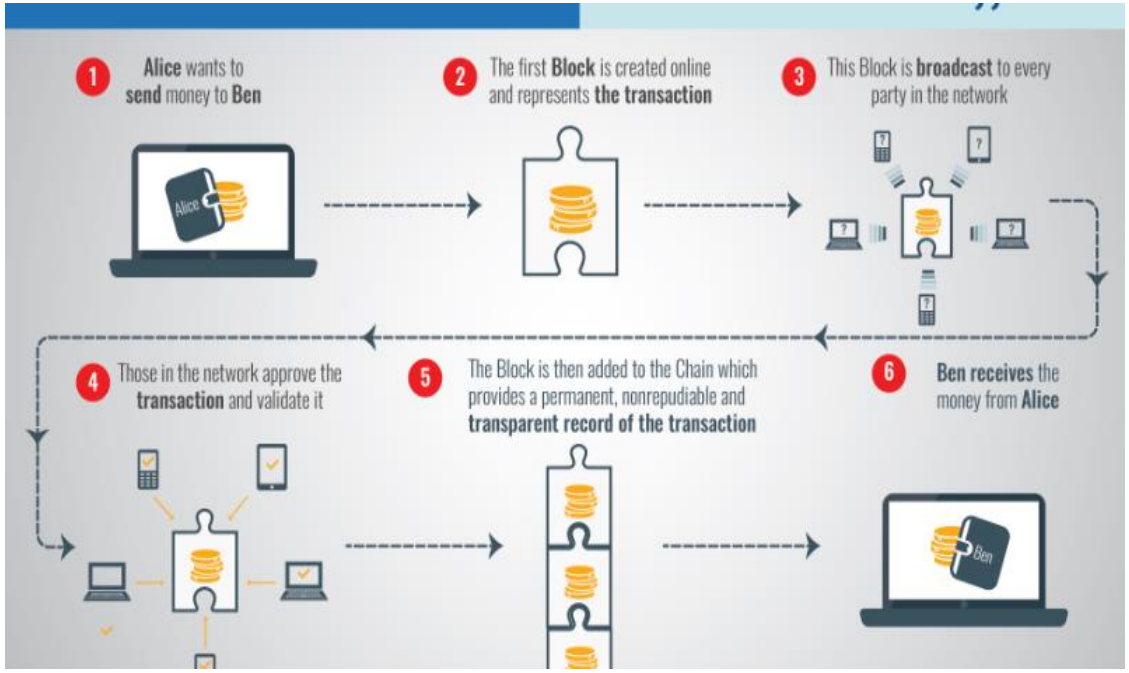


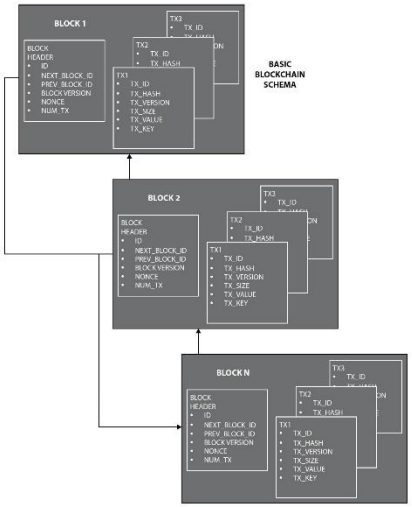
- Decentralized management: data access without authorization and security protection in a decentralized architecture

- The challenges adversely affect the circulation of vehicle data and hinder the future development of Internet of Vehicles

Blockchain

- Blockchain represents novel approach to the landscape of information collection, distribution, and governance
  - Add new and undeletable transactions and organize them into blocks.
  - Cryptographically verify each transaction in the block.
  - Append the new block to the end of the existing immutable blockchain.

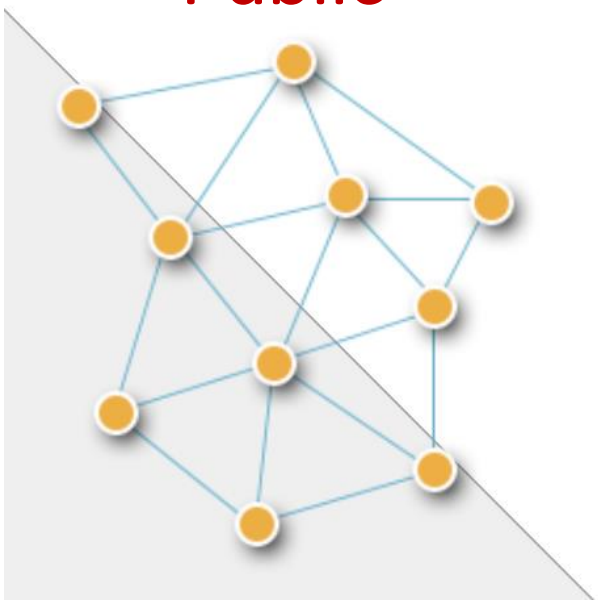




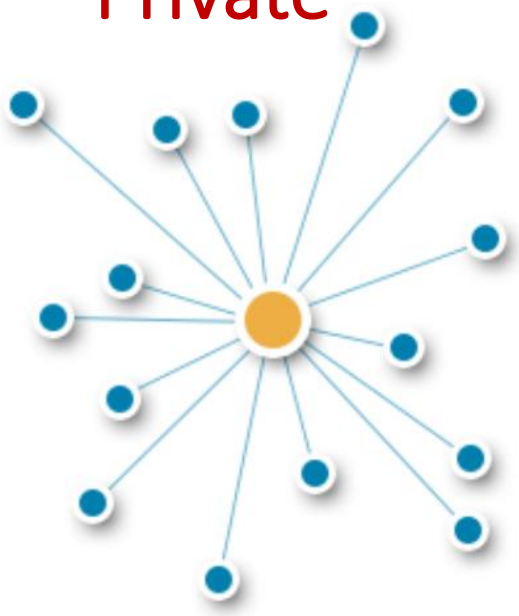
https://https://www.linkedin.com/pulse/securing-internet-things-iot-blockchain-ahmed-banafa/

Blockchain types

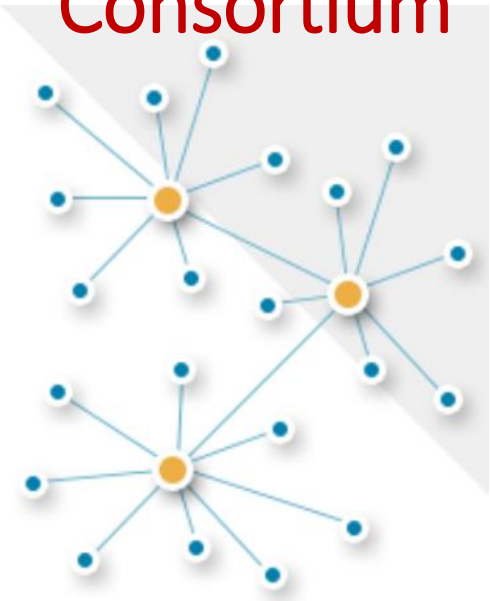
Public



Private



Consortium



	Public	Private	Consortium
Administration	No administrator	Single	Multiple
Access	Open read/write	Permission	Permission
Confidence of participation	Low	High	Medium
Computation cost	High	Low	medium

Blockchain for Internet of Vehicles

- Solution for the Challenges: new techniques to organize, secure and trace the peer-to-peer data sharing record → blockchain is the key!
- Blockchain: provides a perfect way for distributed systems to record transactions that is designed to be transparent, permanent, auditable.

Volkswagen and Ford use blockchain for secure vehicular communication

Second-hand car value certification

Related Work

- A secure, trusted, and decentralized intelligent transport ecosystem is established by blockchain to solve vehicle data sharing problems [1], [2].
- Yang et al. in [3] proposed a decentralized trust management system for vehicle data credibility assessment using blockchain with joint Proof-of-Work (PoW) and Proof-of-Stake (PoS) consensus schemes.
- An intelligent vehicle-trust point mechanism using proof-of-driving-based blockchain is presented to support secure communications and data sharing among vehicles [4], [5].
- Li et al. [6] proposed a privacy-preserving incentive announcement network base d on public blockchain. The Byzantine fault tolerance algorithm is adopted to incentivize vehicles to share traffic information.

[1] L. Yue, H. Junqin, Q. Shengzhi, and W. Ruijin, “Big data model of security sharing based on blockchain,” in Big Data Computing and Communications (BIGCOM), 2017 3rd International Conference on, pp. 117–121, IEEE, 2017.
[2] Y. Yuan and F. Y. Wang, “Towards blockchain-based intelligent transportation systems,” in 2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC), pp. 2663–2668, Nov 2016.
[3] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. Leung, “Blockchain-based decentralized trust management in vehicular networks,” IEEE Internet of Things Journal, 2018.
[4] M. Singh and S. Kim, “Intelligent vehicle-trust point: Reward based intelligent vehicle communication using blockchain,” CoRR, vol. abs/1707.07442, 2017.
[5] M. Singh and S. Kim, “Blockchain based intelligent vehicle data sharing framework,” CoRR, vol. abs/1708.09721, 2017.
[6] L. Li, J. Liu, L. Cheng, S. Qiu, W. Wang, X. Zhang, and Z. Zhang, “Creditcoin: A privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles,” IEEE Transactions on Intelligent Transportation Systems, 2018.

Consensus Schemes for Blockchain-based Internet of Vehicles

- The existing blockchain-based vehicular networks do not work well due to exorbitant cost to build a blockchain in resource-limited vehicles using computation intensive PoW or unfair PoS.

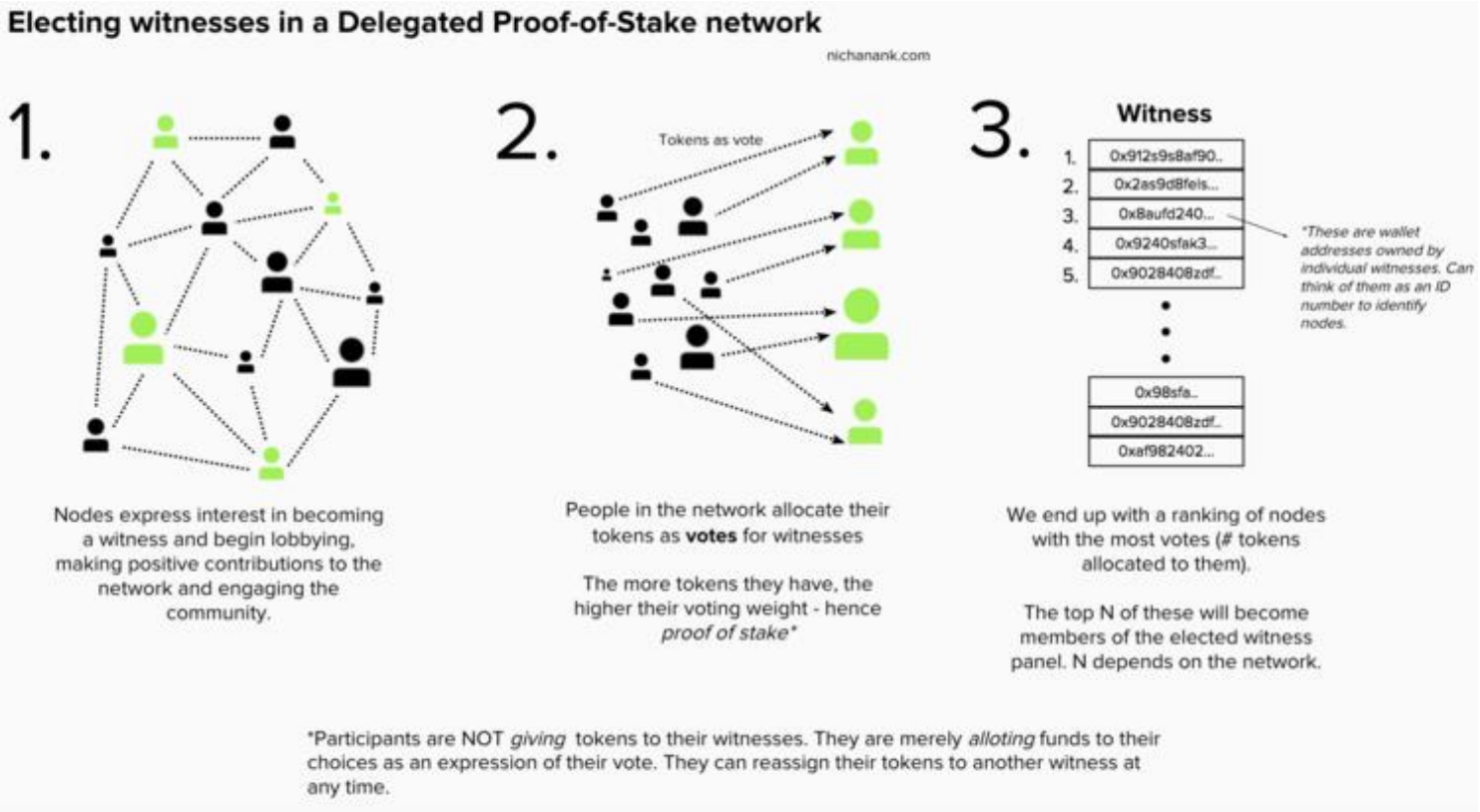
- The Delegated Proof-of-Stake (DPoS) scheme is particularly suitable and practical for vehicular network [7], which performs the consensus process on pre-selected miners with moderate cost.

Some DPoS-based tokens and systems

[7] Y. Yuan and F.-Y. Wang, "Towards blockchain-based intelligent transportation systems," in Intelligent Transportation Systems (ITSC), 2016 IEEE 19th International Conference on, pp. 2663–2668, IEEE, 2016.

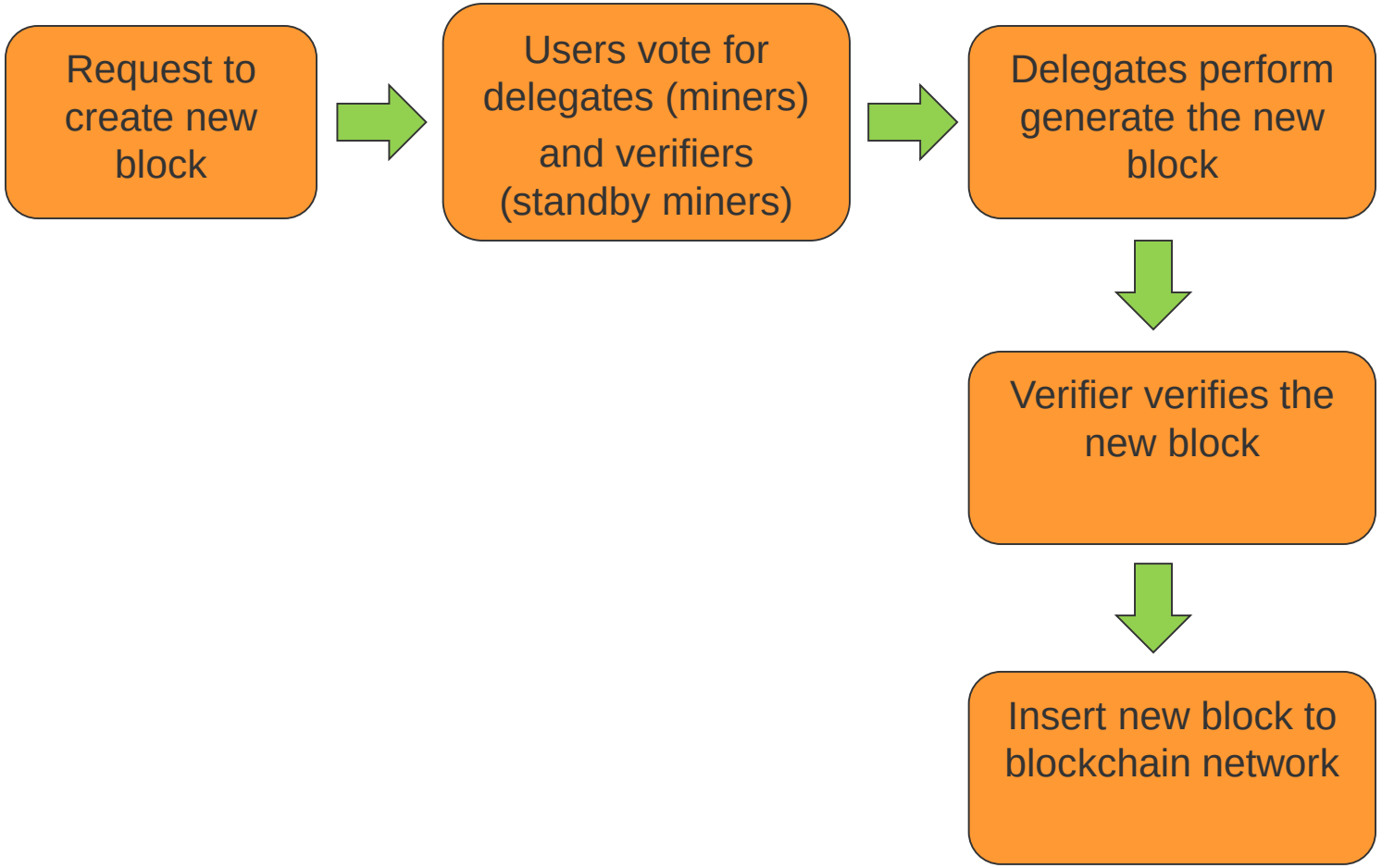
Delegated Proof-of-Stake (DPoS)

- DPoS is an effective consensus mechanism that requires users to vote for “delegates”, who are then responsible for validating transactions and maintaining the blockchain.
- Delegated Proof of Stake is mostly maintained through the election process. Active users of DPoS-based blockchain are voting for “verifiers (witnesses)” and “delegates” with placing their tokens on the name of their candidate.



Delegated Proof-of-Stake (DPoS)

- Process



Security Challenges for DPoS

- Miners in DPoS schemes are selected by stake-based voting. The stakeholders with more stake have higher voting power.
- In BIoV, as RSUs acting as miner candidates may be distributed along the road without sufficient security protection, they are semi-trusted and may be vulnerable to be directly compromised by attackers.
- Miner Voting Collusion: Malicious RSUs collude with compromised high-stake stakeholders to be voted as miners. These malicious miners may falsely modify or discard transaction data during its mining process.
- Block Verification Collusion: Malicious miners may internally collude with other miners to generate false results in the block verification stage, even to launch double-spending attack, which is also challenging.

It is necessary to design an enhanced DPoS consensus scheme with secure miner selection and block verification to defend against the collusion attacks in BIoV

Our Work 1

- **Motivation:** The traditional miner selection is based on stake voting. For fair and reliable miner selection, it is necessary to design a reliable and fair miner selection scheme to defend against the **Miner Voting Collusion**. Reputation is utilized to select active miners that is a time-accumulated metric to indicate trustworthiness of entities according to their past behaviors.

- **Ideas:**
  - We introduce a secure and efficient reputation management scheme by using a **multi-weight subjective logic model**. Miners are selected by reputation-based voting for decreasing collusion between stakeholders with a lot of stake and miner candidates.
  - Reputation opinions of miner candidates are recorded into a blockchain system named **vehicular blockchain**. These reputation opinions on the vehicular blockchain are persistent and transparent evidence when disputes and destruction occur.

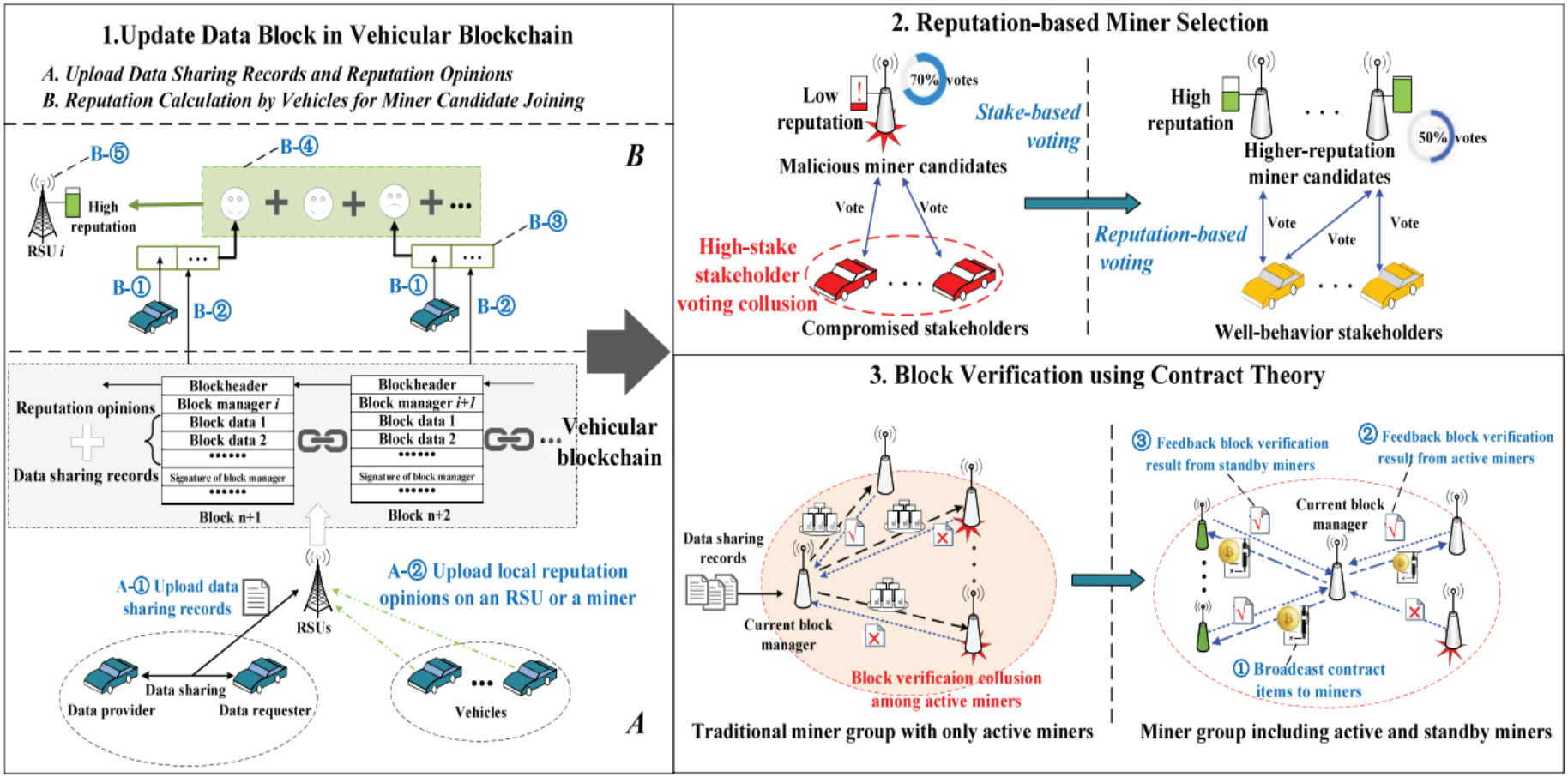
Our Work 2

- **Motivation:** Due to limited number of active miners, attackers are easy to launch the **Block Verification Collusion** that asks the compromised active miners to generate false verification result for a certain block. It is necessary to design an enhanced DPoS consensus scheme with secure block verification to defend against the block verification collusion attack.

- **Ideas:**
  - **The more participating miners can lead to the more secure block verification**. We design an incentive mechanism using **contract theory** to motivate both active miners and standby miners to participate in the block verification.
  - High reputation miners are more likely to generate right verification results. The verifiers that contribute more should be rewarded more.

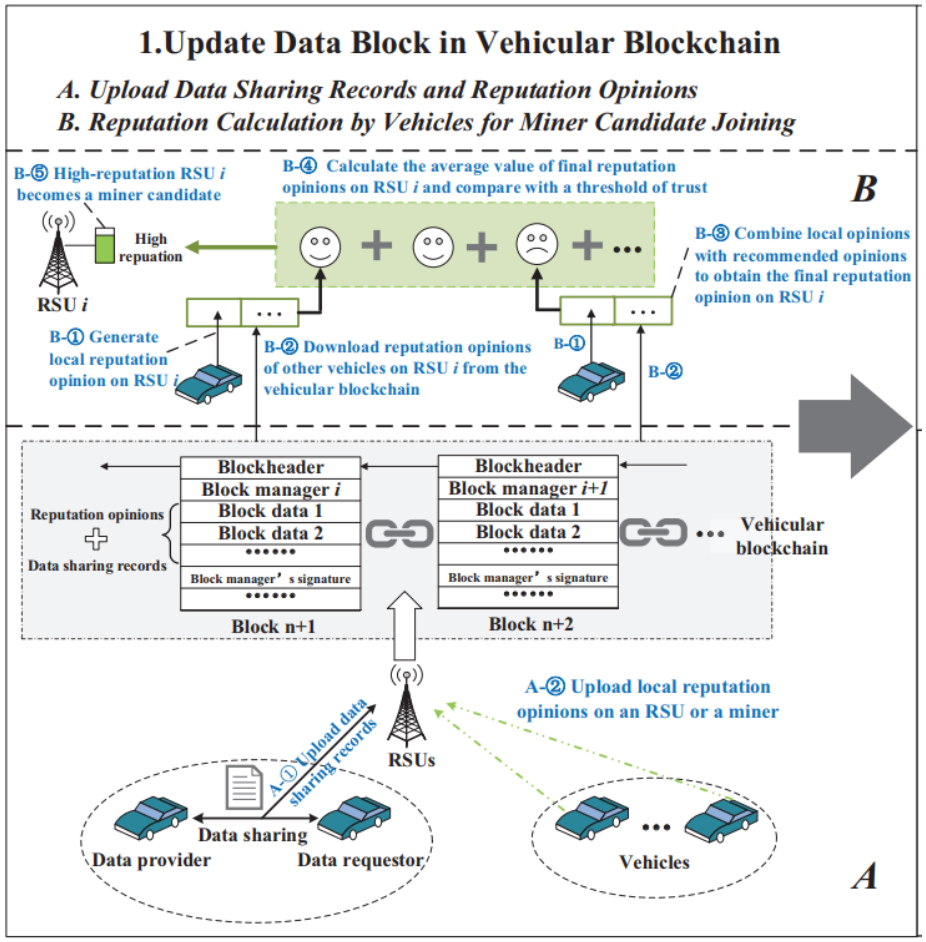
- **Objective:** To reduce information asymmetry between the block managers (active miners) and verifiers (standby miners) and encourage high reputation miners to participate in block verification.

The Proposed Framework



- Reputation based miner selection: reputation calculation using multi-weight subjective logic model + blockchain
- Block verification using contract theory: incentive mechanism using contract theory

Vehicular Blockchain for Reputation Management

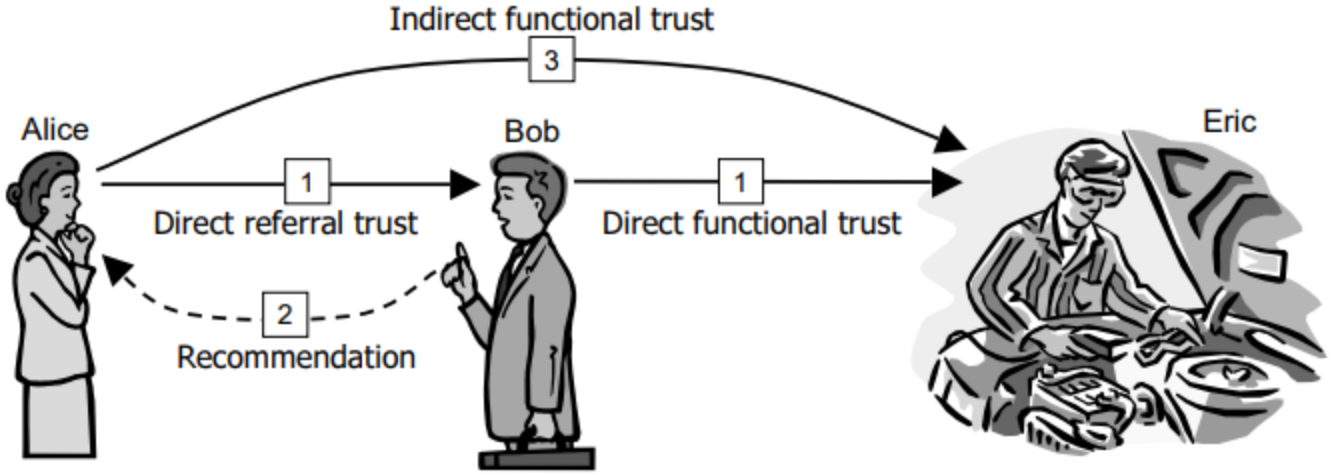


- Upload local reputation opinions:
  - Vehicles upload local reputation opinions for an RSU to the miners
  - The miners perform consensus process using enhanced DPoS consensus scheme
  - The mined block data with reputation opinions is added into the vehicular blockchain
- Reputation calculation
  - Generate local reputation opinion on a certain RSU
  - Download the latest block data with reputation opinions of the RSU, and treat these opinions as recommended opinions
  - Based on subjective logic model, combine recommended opinions with local opinions to obtain the final reputation opinions

The vehicular blockchain is a public ledger that records vehicles' reputation opinions for RSUs and miners into the block data. These reputation opinions are persistent and transparent evidence when disputes and destruction occur.

Reputation Calculation using Subjective Logic Model

- **Subjective Logic** is utilized to formulate individual evaluation of reputation based on past interactions and recommended opinions.
- The subjective logic utilizes the term “opinion” to denote the representation of a subjective belief, and models positive, negative statements and uncertainty.



Transitive trust principle

Multi-weight Subjective Logic Model

- Traditional subjective logic is evolved towards multi-weight subjective logic when considering weighting operations.

- Interaction Frequency: The higher interaction frequency means that vehicle V_i has more prior knowledge about RSU RU_j (miner candidate).

- Interaction Timeliness: In BIoV, an RSU is not always trusted and reliable because the widely distributed RSUs may lack sufficient security protection and are vulnerable to be compromised. Both the trustfulness and reputation of V_i to RU_j are changing over time.

- Interaction Effects: Positive interactions increase RSUs' reputation and negative interactions decrease the reputation of RSUs.

Multi-weight Subjective Logic for Reputation Calculation

Local opinions for subjective logic

A local opinion vector of V_i to RU_j :

$$\omega_{i\to j}=\{\mathrm{b}_{i\to j},d_{i\to j},u_{i\to j}\},\ \text{where}\ \ \mathrm{b}_{i\to j}+d_{i\to j}+u_{i\to j}=1,\ \{\mathrm{b}_{i\to j},d_{i\to j},u_{i\to j}\}\in[0,1].$$

$$\begin{cases} b_{i\to j}=(1-u_{i\to j})\frac{\alpha_i}{\alpha_i+\beta_i}, \\ d_{i\to j}=(1-u_{i\to j})\frac{\beta_i}{\alpha_i+\beta_i}, \\ u_{i\to j}=1-s_{i\to j}. \end{cases}$$

$b_{i\to j}$: belief
$d_{i\to j}$: distrust
$u_{i\to j}$: uncertainty

α_i : The number of positive interactions between the vehicle *i* and the RSU *j*
β_i : The number of negative interactions between the vehicle *i* and the RSU *j*
$s_{i\to j}$:The communication quality of a link between the vehicle *i* and the RSU *j* i.e., the successful transmission probability of data packets, determines the uncertainty of local opinion vector $u_{i\to j}$

Multi-weight Subjective Logic for Reputation Calculation

- **Three-weight local opinions for subjective logic**

(1) Interaction Frequency ($IF_{i\to j}$)

The ratio of the number of times that V_i interacts with RU_j to the average number of times that V_i interacts with other RSUs during a time window T.

$$\mathrm{IF}_{i\to j} = \frac{N_{i\to j}}{\overline{N_i}}, \text{ where } N_{i\to j} = (\alpha_i + \beta_i), \text{ and } \overline{N_i} = \frac{1}{|S|}\sum_{s\in S} N_{i\to s}.$$

S is the set of all RSUs interacting with vehicle V_i during the time window. The higher interaction frequency leads to a higher reputation.

(2) Interaction Timeliness

The recent interactions and past interactions have different weights on the local opinions of vehicles. The parameter ζ represents the weight of recent interactions, and σ represents the weight of past interactions. ζ + σ = 1, ζ > σ.

Multi-weight Subjective Logic for Reputation Calculation

(3) Interaction Effects

Positive interactions increase RSUs' reputation and negative interactions decrease the reputation of RSUs.

The positive interactions have a higher weight on the local opinions of vehicles than that of the negative interactions. Here, the weight of positive interactions is χ, and the weight of negative interactions is τ, where $\chi + \tau = 1$, $\tau < \chi$.

The weights of interaction timeliness and interaction effects are combined together to form a new interaction frequency as follows:

$$\begin{cases} \alpha_i = \zeta\chi\alpha_1^i + \sigma\chi\alpha_2^i, \\ \beta_i = \zeta\tau\beta_1^i + \sigma\tau\beta_2^i. \end{cases}$$

α_1^i β_1^i : The number of positive and negative recent interactions, respectively.

α_2^i β_2^i : The number of positive and negative past interactions, respectively.

Therefore, the interaction frequency between V_i to RU_j is updated as follows:

$$\mathrm{IF}_{i\to j} = \frac{N_{i\to j}}{\overline{N_i}} = \frac{\chi(\zeta\alpha_1^i + \sigma\alpha_2^i) + \tau(\zeta\beta_1^i + \sigma\beta_2^i)}{\frac{1}{|S|}\sum_{s\in S} N_{i\to s}}.$$

Multi-weight Subjective Logic Model

- The overall weight of reputation for local opinions is $\delta_{i\to j} = \rho_i * IF_{i\to j}$, where $0 \le \rho_i \le 1$ is a pre-defined weight parameter for reputation calculation.

- After being weighted, the recommended opinions are combined into a common opinion in the form of $\omega_{x\to j}^{rec} := \{b_{x\to j}^{rec}, d_{x\to j}^{rec}, u_{x\to j}^{rec}\}$

$$\begin{cases} b_{x\to j}^{rec} = \frac{1}{\sum_{x\in X} \delta_{x\to j}} \sum_{x\in X} \delta_{x\to j} b_{x\to j}, \\ d_{x\to j}^{rec} = \frac{1}{\sum_{x\in X} \delta_{x\to j}} \sum_{x\in X} \delta_{x\to j} d_{x\to j}, \\ u_{x\to j}^{rec} = \frac{1}{\sum_{x\in X} \delta_{x\to j}} \sum_{x\in X} \delta_{x\to j} u_{x\to j}, \end{cases}$$

where $x \in X$ is a set of recommenders, i.e., the other vehicles that have interacted with RU_j.

The subjective opinions from different recommenders are combined into one single opinion, which is called the recommended opinion according to each opinion's weight.

Multi-weight Subjective Logic Model

- To avoid being cheating by the recommenders, a vehicle should take both its own local opinion and the recommended opinions into consideration when form the final reputation opinion for an RSU.
- The final reputation opinion of V_i to RU_j is formed as $\omega_{x\to j}^{final} := \{b_{x\to j}^{final}, d_{x\to j}^{final}, u_{x\to j}^{final}\}$

According to subjective logic model, we have

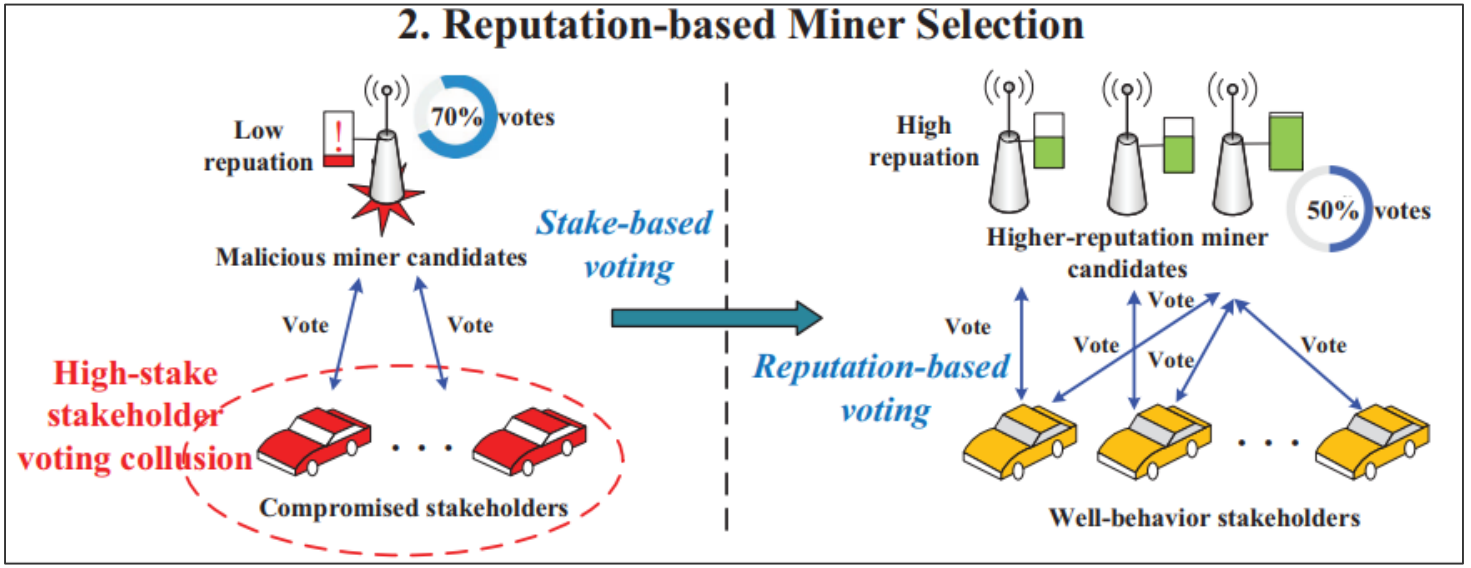
$$\begin{cases} b_{i\to j}^{final} = \frac{b_{i\to j}u_{x\to j}^{rec} + b_{x\to j}^{rec}u_{i\to j}}{u_{i\to j} + u_{x\to j}^{rec} - u_{x\to j}^{rec}u_{i\to j}}, \\ d_{i\to j}^{final} = \frac{d_{i\to j}u_{x\to j}^{rec} + d_{x\to j}^{rec}u_{i\to j}}{u_{i\to j} + u_{x\to j}^{rec} - u_{x\to j}^{rec}u_{i\to j}}, \\ u_{i\to j}^{final} = \frac{u_{x\to j}^{rec}u_{i\to j}}{u_{i\to j} + u_{x\to j}^{rec} - u_{x\to j}^{rec}u_{i\to j}}. \end{cases}$$

The reputation value $T_{i\to j}$ represents the expected belief of vehicle V_i that RSU RU_j is trusted and behaves normally during a consensus process, which is denoted by

$$T_{i\to j} = b_{i\to j} + \gamma u_{i\to j}.$$

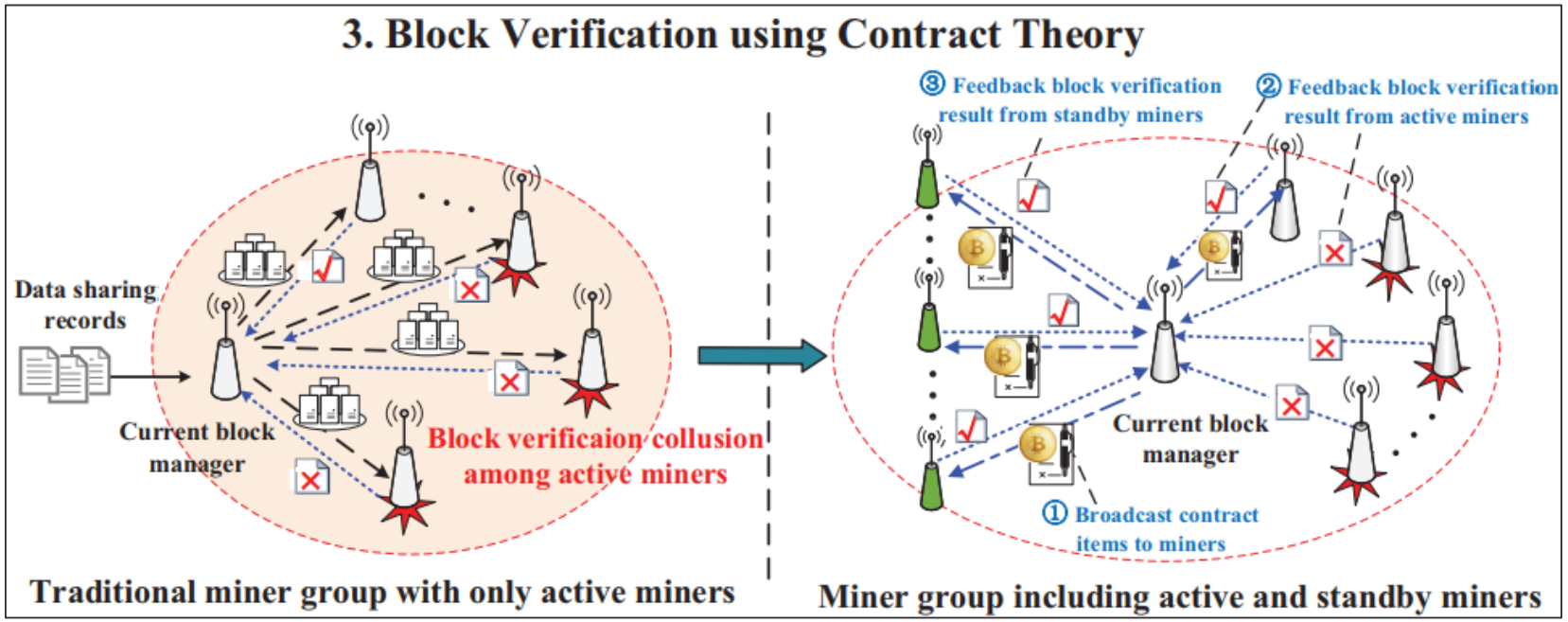
- After obtaining the final reputation opinion on an RSU, vehicles will upload and store their final reputation opinions as recommended opinions for other vehicles in the vehicular blockchain.
- Finally, miner candidates with high-reputation are voted as the miners for secure block verification.

Overview of Reputation-based Miner Selection



- According to the final reputation opinions, as shown in the figure, each stakeholder （vehicle） votes for *y* candidates as the miners according to its ranking of the final reputation opinions for the candidates.
- Unlike traditional DPoS schemes, all the vehicles have the same weight in miner voting (same voting power) even though some stakeholders owning larger stake.
- The top *k* miner candidates with the highest reputation are selected to be active miners and ($y - k$) miner candidates can be standby miners. The active miners and standby miners form a miner group in vehicular blockchain. Here $y < k$, and k is an odd integer, such as 21 in EoS and 101 in Bitshares.

Overview of Block Verification using Contract Theory



- In traditional DPoS, due to the limited number of active miners, malicious active miners may launch the block verification collusion attack to generate false block verification results.
- The miners including active miners and standby miners can act as verifiers and join the block verification process, especially the high-reputation miners, which can prevent the block verification collusion among the active miners.
- We then design an incentive mechanism by using contract theory to encourage high-reputation miners to participate in the block verification. In the incentive mechanism, the active miner acts as the block manager and the contract designer to broadcast contract items to miners. Meanwhile, the standby miners choose and sign their best contract items.

Incentive Mechanism using Contract Theory

- For secure block verification, we aim to design an **incentive mechanism** to motivate more miners (**both active miners and standby miners**) to participate in the block verification. Every **block manager** will offer a part of the transaction fee as a reward to verifiers that participate in block verification and accomplish the tasks in time.

- There exist **information asymmetry issues** between miners and the block managers.
  - The block manager does not have prior knowledge about which miners would like to participate in verification.
  - It does not have an accurate reputation value of a verifier.
  - It does not know the amount of resource that each verifier can contribute. The information asymmetry between the block manager and verifiers may incur too much cost for the block manager to give an incentive to the verifiers.

- The best strategy for the block manager is to design an incentive mechanism that can reduce the impact of information asymmetry. Moreover, the verifiers that contribute more should be rewarded more.

Contract theory!!!

Model Formulation using Contract Theory

- **Latency in block verification**

The local verification time of this block

$$L_q(c_m^k, I_k, O_k) = \frac{I_k}{r_m^d} + \frac{\mathrm{Task}_m^k}{c_m^k} + \psi I_k \left|\mathbb{M}\right| + \frac{O_k}{r_m^u}$$

The time of verification feedback

Delay of unverified block transmission from the block manager to verifiers

Delay of verification result broadcasting and verification result comparison among verifiers

- **The uplink/ downlink transmission rate between the verifiers and block manager**

$$r_m^u = r_m^d = B\log_2(1 + \frac{\varpi_m |h_m|^2}{\sum_{m^- \in \mathbb{M}\setminus\{m\}} \varpi_{m^-} |h_{m^-}|^2 + N_0 B})$$

Model Formulation using Contract Theory

- **The profit of the block manager:**

$$\max_{(\mathrm{R_q},\mathrm{L_q^{-1}})} U_{bm} = \sum_{q=1}^{Q} |\mathbb{M}| p_q [g_1 e_1 (\theta_q |\mathbb{M}| p_q)^{z_1} - g_1 e_2 (\frac{L_q}{T_{\max}})^{z_2} - l R_q]$$

The cost of the block manager

The benefit of the block manager regarding a security-latency metric for type-*q* verifier

$$\begin{aligned}
&\text{s.t.} \\
&\theta_q \eta(R_q) - l' L_q^{-1} \geq 0, \forall q \in \{1, \ldots, Q\}, \\
&\theta_q \eta(R_q) - l' L_q^{-1} \geq \theta_q \eta(R_{q'}) - l' L_{q'}^{-1}, \forall q, q' \in \{1, \ldots, Q\}, \\
&q \neq q', \\
&\max\{L_q\} \leq T_{\max}, \forall q \in \{1, \ldots, Q\}, \\
&\sum_{q=1}^{Q} |\mathbb{M}| p_q R_q \leq R_{\max}, \forall q \in \{1, \ldots, Q\},
\end{aligned}$$

L_q: latency of block verification for type-q verifiers
R_q: incentive for type-q verifier

- **Security-latency metric:** The more verifiers participating in block verification leads to more secure block verification stage. However, this causes larger latency since the verifiers may need to communicate with verifiers through multi-hop relays. We define this metric to balance the network scale and the block verification time for type-q verifier.

- **The utility of type-q verifier:**

$$\max_{(\mathrm{R_q},\mathrm{L_q^{-1}})} U_q = \theta_q \eta(R_q) - l' L_q^{-1}, \forall q \in \{1, \ldots, Q\}.$$

The type of verifier: reputation. More details about reputation calculation can be found in Ref. [1]

Ref. [1]: J. Kang, Z. Xiong, D. Niyato, D. Ye, D. I. Kim and J. Zhao, "Toward Secure Blockchain-Enabled Internet of Vehicles: Optimizing Consensus Management Using Reputation and Contract Theory," in *IEEE Transactions on Vehicular Technology*, vol. 68, no. 3, pp. 2906-2920, March 2019.

Solution

- **Solution**

$$\max_{(\mathrm{R_q},\mathrm{L_q^{-1}})} U_{bm} = \sum_{q=1}^{Q} |\mathbb{M}| p_q [g_1 e_1 (\theta_q |\mathbb{M}| p_q)^{z_1} - g_1 e_2 (\frac{1}{L_q^{-1} T_{\max}})^{z_2}]$$
$$- |\mathbb{M}| l \sum_{q=1}^{Q} f_q L_q^{-1},$$
$$\text{s.t.} \quad L_q^{-1} \geq \frac{1}{T_{\max}}, \forall q \in \{1, \ldots, Q\},$$
$$|\mathbb{M}| \sum_{q=1}^{Q} f_q L_q^{-1} \leq R_{\max}, \forall q \in \{1, \ldots, Q\}.$$

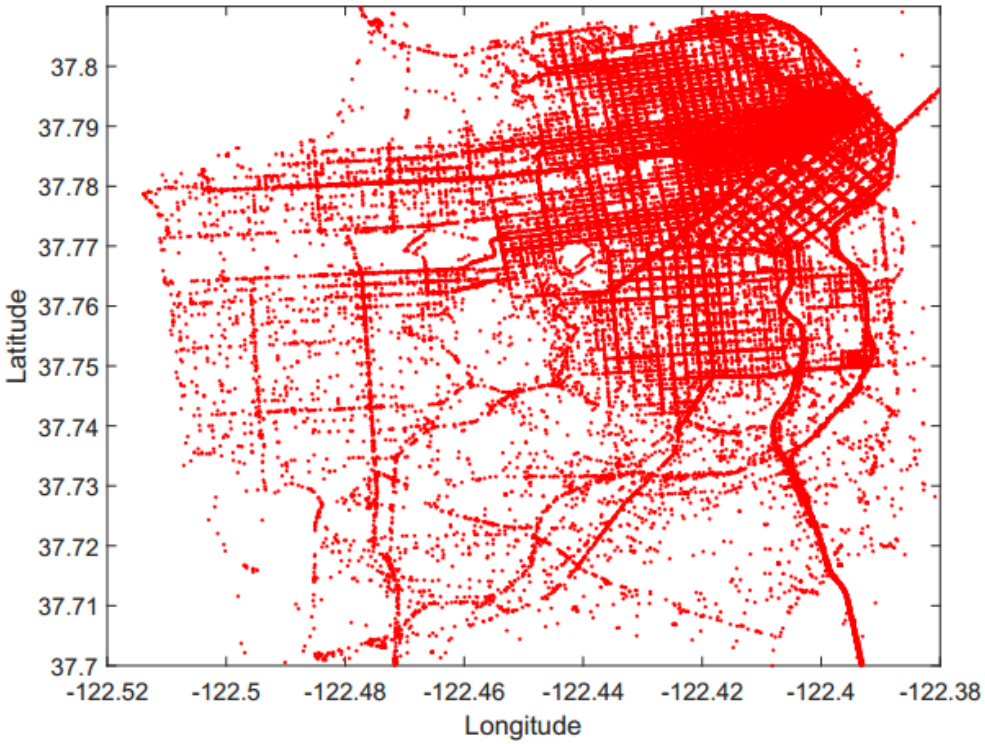
Where,

$$f_q = \begin{cases} \frac{l' p_q}{\theta_q} + \left(\frac{l'}{\theta_q} - \frac{l'}{\theta_{q+1}}\right) \sum_{i=q+1}^{Q} p_i, & if \ q < Q, \\ \frac{l' p_Q}{\theta_Q}, & if \ q = Q. \end{cases}$$

The above problem is a convex optimization problem because the summation of concave functions (U_{bm}) is still a concave function, and the constraints are affine. We can obtain the optimal latency requirement L_q^{-1*} and the corresponding incentive R_q* by using convex optimization tools, e.g., **CVX**.

Simulation Setting

- We first evaluate the performance of the **Multi-Weight Subjective Logic (MWSL) scheme** based on a real-world dataset of San Francisco Yellow Cab.
- Next, we evaluate and compare the performance of the **incentive mechanism** based on contract theory.
- We observe 200 taxis running in an urban area, whose latitude and longitude are from 37.7 to 37.81 and from -122.52 to -122.38, respectively.



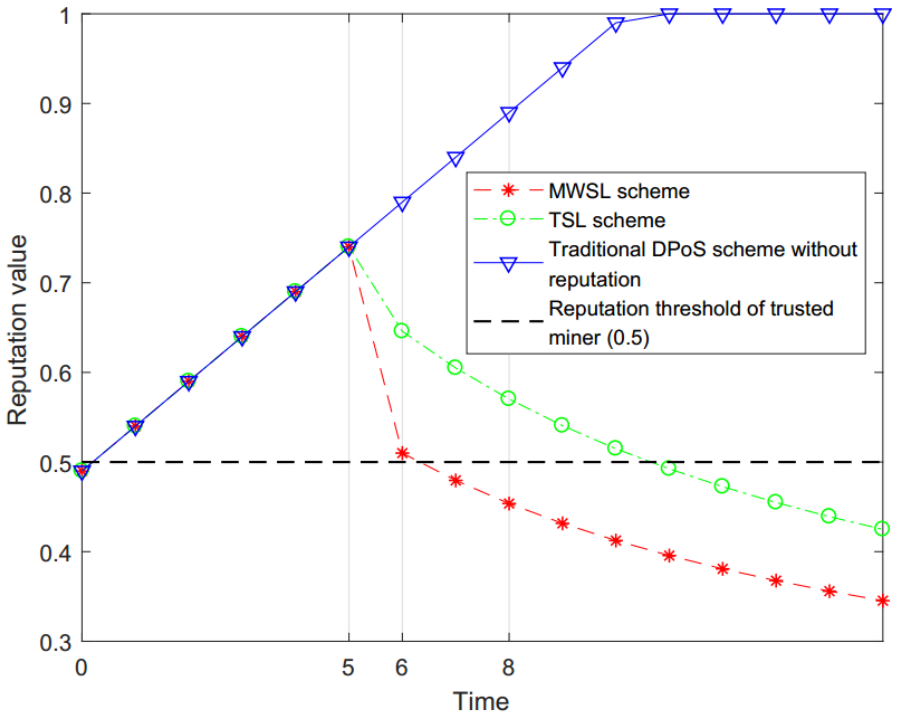
Spatial distribution of vehicle trace points.

Simulation Setting

Parameter	Setting
Interaction frequency between vehicles and RSUs	[50, 200] times/week
Coverage range of RSUs	[300, 500] m
Speed of vehicles	[50, 150] km/h
Weight parameters	$\chi = 0.4$, $\tau = 0.6$, $\zeta = 0.6$, $\sigma = 0.4$, $\rho = 1$
Time scale of recent and past events t_{recent}	three days
Rate of compromised vehicles	[10%, 90%]
Successful transmission probability of data packets	[0.5, 1]
Vehicle to RSU bandwidth	20 MHz
Noise spectrum density	-174 dBm/Hz
Transmission power	[10, 23] dBm
Receiver power	14 dBm
Computation resource	$[10^3, 10^6]$ CPU cycles/unit time
Input/output block data size	[50, 500] KB
Pre-defined parameters	$g_1 = 1.2$, $e_1 = 15$, $e_2 = 10$, $z_1 = 2$, $z_2 = 1$, $l = 5$, $l' = 1$, $T_{max} = 300$ s, $R_{max} = 1000$, $\psi = 0.5$

- These miner candidates are classified into 10 types according to their reputation values, wherein the probability for a candidate belonging to a certain type is 0.1.
- Major parameters used in the simulation are given in the Table.

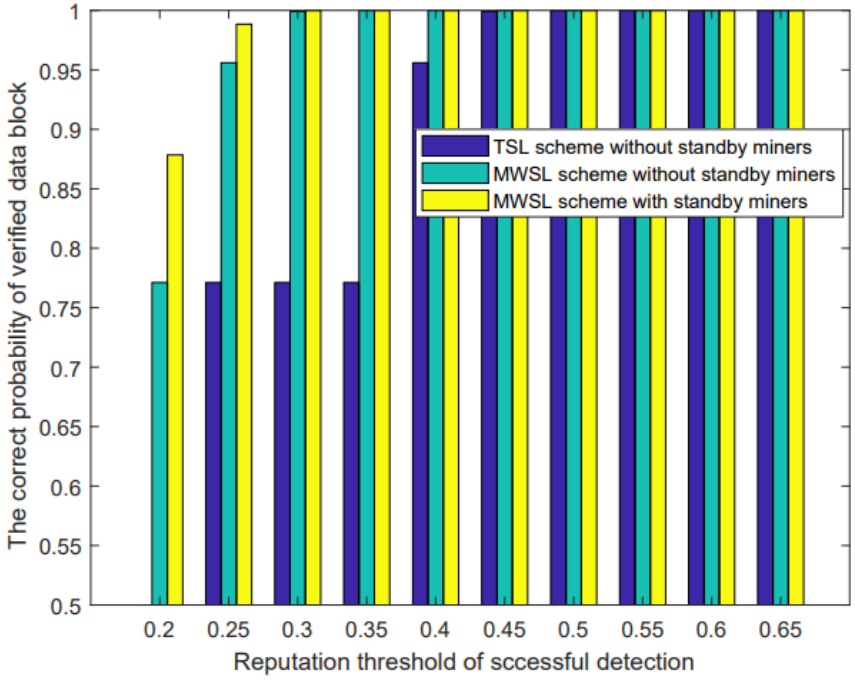
Performance of Proposed Reputation Scheme



The reputation values of a malicious miner.

- In the traditional DPoS scheme without reputation, the reputation value of the malicious candidate evaluated by the vehicle is linearly increasing because the well-behaved vehicle cannot detect the candidate's misbehaviors for other well-behaved vehicles.
- For the TSL and our MWSL schemes, the reputation values of the candidate sharply decrease because of recommended opinions from other vehicles. Our MWSL scheme achieves more accurate reputation calculation, and this therefore leads to more secure miner voting.

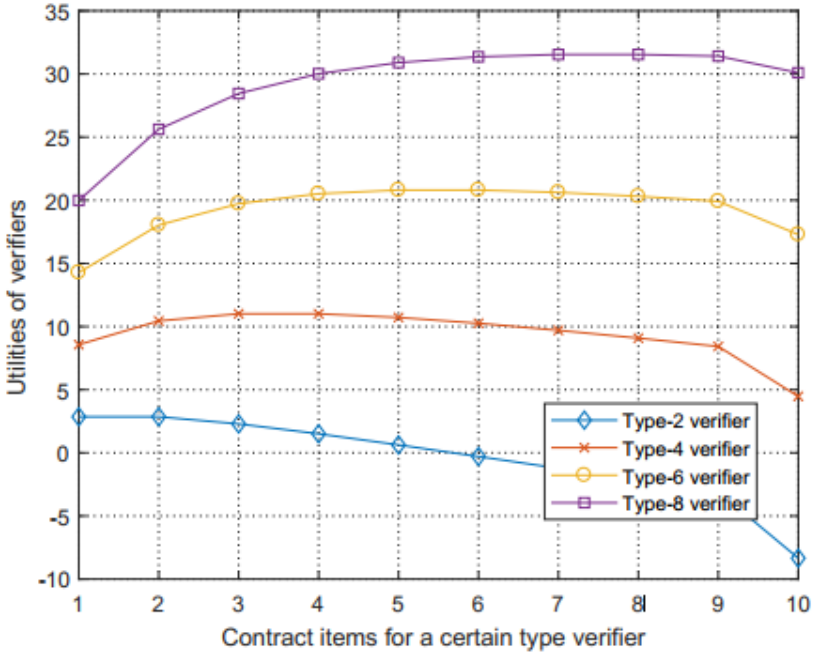
Performance of Proposed Reputation Scheme



Probability of corrected data blocks under different threshold values of trusted miners

- Correct probability of verified block: The data block is correctly verified without the effects of the verification collusion attack.
- The proposed MWSL can ensure a secure block verification, even when attackers launch internal active miner collusion.

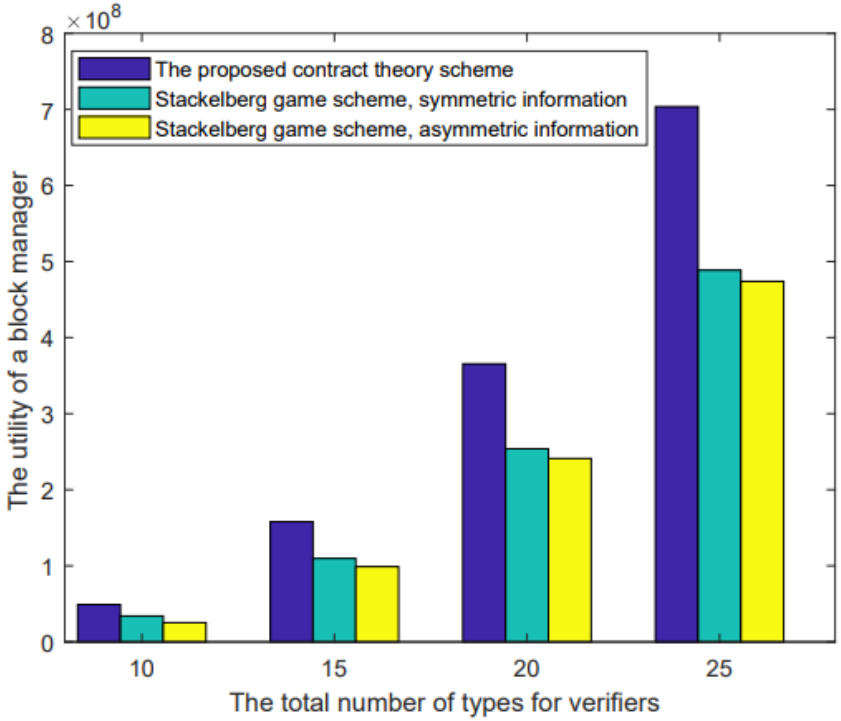
Performance of Incentive Mechanism



Utilities of verifiers under different contract items.

- This figure shows the utilities of verifiers with type 2, type 4, type 6 and type 8. Each type of verifiers obtains the maximum utility while selecting the contract item exactly designed for its type, which explains the IC constraint.
- All types of verifiers choose the contract items corresponding to their types with non-negative utilities, which validates the IR constraint.

Performance of Incentive Mechanism



The utility of a block manager under different total number of verifier types.

- We compare the profit of a block manager obtained from the proposed contract model, and Stackelberg game models.
- It shows that the profit of a block manager increases with the total number of verifier types. The more verifier types bring both more verifiers and contract item choices for high-type (high-reputation) verifiers, leading to the more secure block verification. The utility of the proposed contract model has better performance than that of the Stackelberg game model.

Summary

- We propose an enhanced DPoS consensus scheme to establish blockchain-enabled Internet of Vehicles for secure vehicle data sharing.
- This DPoS consensus scheme has been improved by a two-stage soft security enhancement solution: (1) select miners by reputation-based voting. A multi-weight subjective logic scheme has been utilized to calculate securely and accurately the reputation of miner candidates. (2) incentivize standby miners to participate in block verification using contract theory, which can further prevent internal collusion of active miners.
- Numerical results have indicated that our multi-weight subjective logic scheme has great advantages over traditional reputation schemes in improving detection rate of malicious miner candidates. Likewise, the proposed contract-based block verification scheme can further decrease active miners collusion and optimize the utilities of both the block manager and verifiers to further improve the security of vehicle data sharing.

More details can be found in the journal paper:

J. Kang, Z. Xiong, D. Niyato, D. Ye, D. I. Kim and J. Zhao, "Toward Secure Blockchain-Enabled Internet of Vehicles: Optimizing Consensus Management Using Reputation and Contract Theory," in *IEEE Transactions on Vehicular Technology*, vol. 68, no. 3, pp. 2906-2920, 2019.

NANYANG TECHNOLOGICAL UNIVERSITY

Thank you!

Contact: Kavinkang@ntu.edu.sg