

Maintaining Trust in VANETs using Blockchain

Sarishma¹, Ravi Tomar²

*¹M.Tech. Computer Science and Engineering Faculty of Technology, Uttarakhand Technical University,
Dehradun, India sarishmasingh@gmail.com*

*²Assistant Professor School of Computer Science, University of Petroleum and Energy Studies, Dehradun, India
ravitomar7@gmail.com*

Introduction

- ▶ Introduction to VANETs
 - ▶ Issues involved in VANETs
 - ▶ Security as a key issue
 - ▶ Problem statement
- 

Blockchain

- ▶ What is blockchain?
 - ▶ Distributed ledger
 - ▶ How it works?
 - ▶ Consensus
- 

Related Work

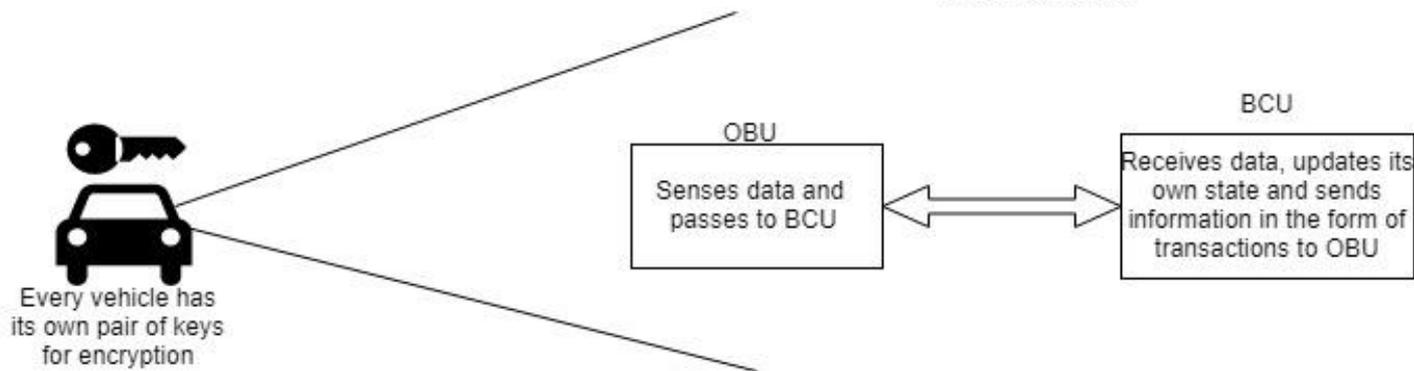
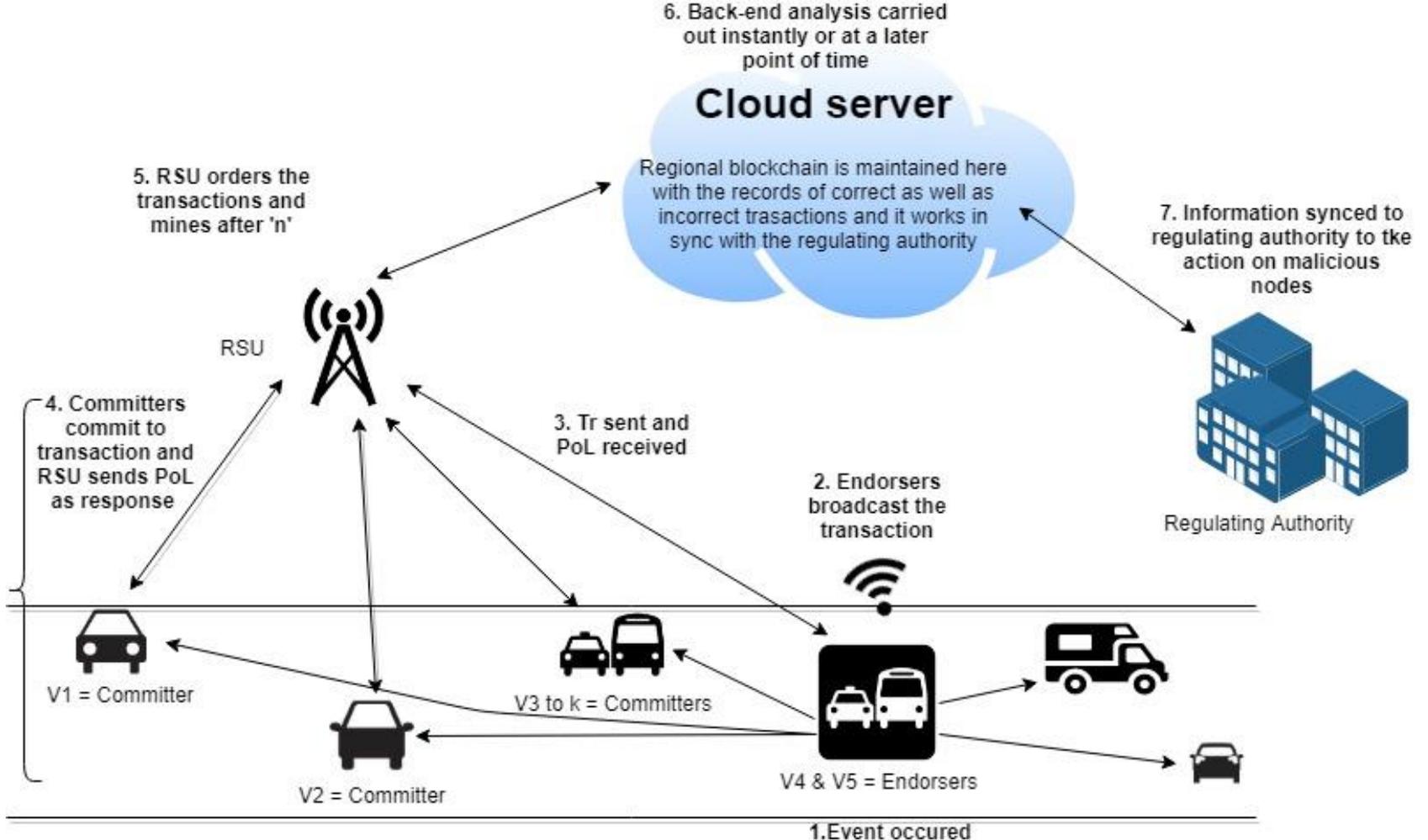
- ▶ R. Shrestha et al. – trustworthiness of messages and nodes
 - ▶ B. Leiding et al. – Traffic regulation application via Ethereum programming language
 - ▶ W. Liu et al. – BARS (reputation evaluation algorithm)
 - ▶ P. K. Sharma et al. – SmartPay
 - ▶ M. Singh et al. – Reward based system
 - ▶ SmartShare – real-time ride sharing
- 

Proposed System

- ▶ Participating network
 - ▶ Integration with existing system
 - ▶ Actors and their roles
 - ▶ Rules associated
 - ▶ Validation of data
 - ▶ Data appended at stages
 - ▶ Permission access
- 

Assumptions

- ▶ Vehicles can communicate + internet
 - ▶ Unique ID, private public keys
 - ▶ Messages are time stamped and digitally signed
 - ▶ GPS
 - ▶ BCU – BlockChain Unit
 - ▶ RSU – at least 2/3 are not malicious in nature
- 



- ▶ $\text{TrVID} = (\text{info}, x, y, z, s_1, s_2, \text{dir}, r, \text{ts}, \text{ds}, \text{hID})$
- ▶ $n = h$ (area / number of vehicles)
- ▶ $\text{Tr}_{\text{VID}} = (\text{info}, x, y, z, s_1, s_2, \text{dir}, r, \text{ts}, \text{ds}, \text{h}_{\text{ID}}, (\text{Y/N}) \text{Sign}_{\text{VID}}, \text{h}_{\text{ID}})$

Applications

- ▶ Insurance companies
 - ▶ Theft detection
 - ▶ Prediction of false behaviour
 - ▶ Clearing paths for ambulance or other emergency services
 - ▶ Traffic violation and surveillance information
 - ▶ Vehicle Tax and credit
- 

Benefits

- ▶ Security
 - ▶ Scalability
 - ▶ Accountability
 - ▶ Transparency
- 

Challenges

- ▶ Sybil attack
 - ▶ Restricted contact time
 - ▶ Prediction of behaviour
- 

Future work

- ▶ Design of BCU
 - ▶ Analysis of information
 - ▶ Division among regions
 - ▶ Information dissemination
- 

References

- ▶ [1] N. Satoshi and S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic cash system,” Bitcoin, p. 9, 2008.
- ▶ [2] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends,” Proc. – 2017 IEEE 6th Int. Congr. Big Data, BigData Congr. 2017, pp. 557–564, 2017.
- ▶ [3] R. Shrestha, R. Bajracharya, and S. Y. Nam, “Blockchain-based Message Dissemination in VANET,” Proc. 2018 IEEE 3rd Int. Conf. Comput. Commun. Secur. ICCCS 2018, pp. 161–166, 2018.
- ▶ [4] B. Leiding, P. Memarmoshrefi, and D. Hogrefe, “Self-managed and blockchain-based vehicular ad-hoc networks,” pp. 137–140, 2016.
- ▶ [5] W. Liu, Z. Lu, Z. Liu, Q. Wang, and G. Qu, “A Privacy-Preserving Trust Model Based on Blockchain for VANETs,” IEEE Access, vol. 6, pp. 45655–45664, 2018.
- ▶ [6] P. K. Sharma, S. Y. Moon, and J. H. Park, “Block-VN: A distributed blockchain based vehicular network architecture in smart city,” J. Inf. Process. Syst., vol. 13, no. 1, pp. 184–195, 2017.
- ▶ [7] M. Singh and S. Kim, “Trust Bit: Reward-based intelligent vehicle communication using blockchain paper,” IEEE World Forum Internet Things, WF-IoT 2018 – Proc., vol. 2018-Janua, pp. 62–67, 2018.
- ▶ [8] R. Shrestha, R. Bajracharya, A. P. Shrestha, and S. Y. Nam, “A new-type of blockchain for secure message exchange in VANET,” Digit. Commun. Networks, 2019.

Thank you