

SpicyChicken: A block chain based persistence implementation for safety information in VANETs

Zhuoer Tong, Uttie Gumbula, Binshuai Wang, Wenjing fan, Yue Wu
Computer Science @ UC Davis

Abstract

VANETs provide a new way of transmitting information, particularly for safety for drivers and vehicles on the road. This also comes with challenges of ensuring authorship of data, need for secure communication, in a highly dynamic network topology whose members are mostly ephemeral. This paper details these challenges and how block chain technologies can be leveraged to address these concerns.

1 Introduction

Historically, networks have relied on a client-server model, where both end points were geographically fixed, and centralized. As the need for fault tolerant services grew, the paradigm of decentralization took a greater hold. Yet even in this, the nature of the network topology was fairly static. The way distributed systems and networking are employed is changing rapidly with ever advancing and adoption of novel technologies. Given the growth of ubiquitous computing, increasing power of small form factor and proliferation of faster networking devices everywhere, there are new frontiers that need novel solutions.

In the recent decades, with computing devices becoming smaller, powerful and increasingly more mobile, this presumption does not hold. There is a need to study and consider how distributed systems will operate in a highly dynamic topology with little implicit trust in the network, and yet deliver a reliable and secure method to transmit data.

The field of Mobile ad hoc network (MANET) studies these concerns, and a subset of which, and the focus of this paper is Vehicular Ad hoc Network (VANET), its applications. VANETs are essentially decentralized at their core because they establish a local peer to peer links to communicate. This feature makes VANETs critically useful for various types of communications. These can be classified into two; primarily for safety applications and secondarily for entertainment/comfort applications. The domain of safety includes conveying information about accident detection and avoidance, warnings about upstream traffic events, sign extension and even critical vehicle information. [3]

The uses of entertainment include being able to run trivial applications for chatting, video and other services targeted toward comfort in travel. [1].

Historically, the most common VANET-type networks have been provided by the government (Self-managed paper). This presents many problems, but the centralization of such systems can cause single point of failures, and highly prized targets for attackers, and given the span of control, raises concerns about government surveillance on the users. [4]

Therefore, a decentralized approach is warranted for further study. Though this is not without its own challenges. There's an imminent need to address security concerns of Isolate safety related Application Units (AUs) and its data from other non-critical AUs. Furthermore, we'd need to validate

We'd need to authenticate the validity and origin of the data. Furthermore, given the dynamic nature of VANET topology, care needs to be taken when routing packets so as to not expose any identifiable sender and recipient information.

This problem makes it very amenable to utilizing block-chain technologies to address these problems of Vehicle to Infrastructure (V2I) and Vehicle to vehicle (V2V) communication in ensuring provenance of data while offering security and reliability in a decentralized manner.[5]

We plan on detailing the safety concerns and best practice guides, and implementing 2 applications units (AUs) as proof-of-concept that will work on On-Board Units (OBUs), provide a safety oriented service to Roadside Units(RSUs) that will persist data on a commodity block chain and future venues for further research. [4][2]

References

- [1] S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, and H. Zedan. A comprehensive survey on vehicular ad hoc network. *Journal of network and computer applications*, 37:380–392, 2014.
- [2] T. Jiang, H. Fang, and H. Wang. Blockchain-based internet of vehicles: distributed network architecture and

performance analysis. *IEEE Internet of Things Journal*, 6(3):4640–4649, 2018.

- [3] V. Kumar, S. Mishra, N. Chand, et al. Applications of vanets: present & future. *Communications and Network*, 5(01):12, 2013.
- [4] B. Leiding, P. Memarmoshrefi, and D. Hogrefe. Self-managed and blockchain-based vehicular ad-hoc networks. In *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct*, pages 137–140, 2016.
- [5] A. P. S. Y. Rakesh Shrestha, Rojeena Bajracharya. A new type of blockchain for secure message exchange in vanet. *Digital Communications and Networks Digital Communications and Networks*, 2019.