Forensic-blockchains for autonomous vehicles: Incentives and attacks

Bhavya Gulati, Ritesh Ahuja
Viterbi School of Engineering

Introduction

One of the critical technological challenges in widespread adoption of driverless technology is the development of trustable dispute and liability resolution in the event of traffic collisions or environmental accidents. The data collected from sensors can be instrumental in detecting the faulty party in post accident scenarios.

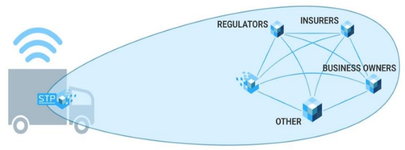


Figure 1 : Data Environment

Benefit of Blockchain

Features	Traditional EMS Systems	Permissioned Blockchain System
Storage	Black boxes have limited storage	Use fragmented ledger with cloud storage
Decentralized	Have to trust a third party to obtain the data	Everyone has access of all the data
Availability	No common umbrella for data from all the parties	Shared ledger of hashes of data
Validity	Validity of data based on trust	Data can be validated by all the validators
Immutability	Data can be tampered after accident	Data once recorded in blockchain can not be updated
Hit & Run is not traceable	Vehicle can get away as data is not shared on blockchain	V2V and V2I capture interaction data as witnesses

Data Flow

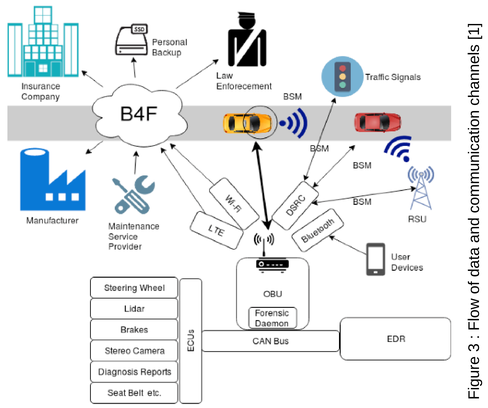


Figure 3 : Flow of data and communication channels [1]

System Overview (Permissioned Blockchains)

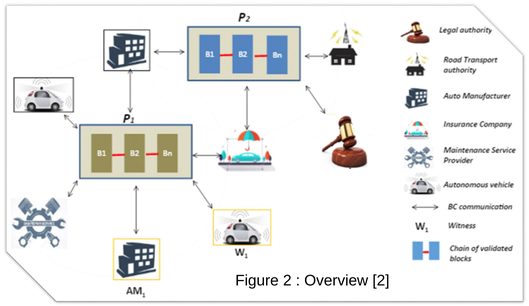
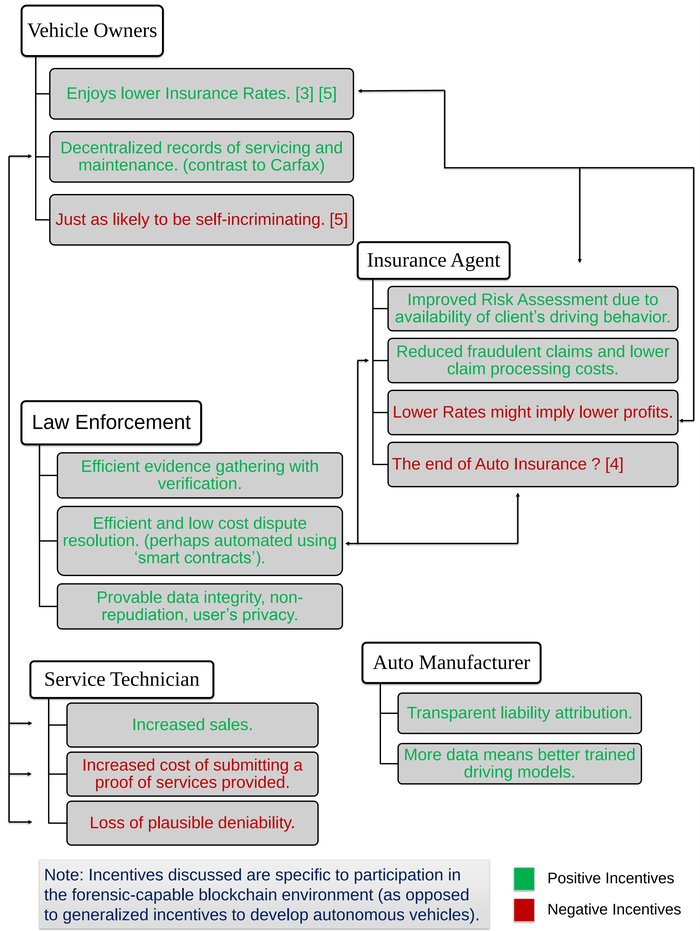


Figure 2 : Overview [2]

Role	P1: Operational Partition	P2: Decision Partition
Proposer	Autonomous vehicle, Service technician, Auto manufacturer	Insurance company, Auto manufacturer
Validator	Insurance company, Service technician, Auto manufacturer	Government transport authority, Legal authority

Incentives to participate in the system.



Potential Attacks

Q1. What if Autonomous vehicles falsify data?

❑ Could use Physical Unclonable Functions in controllers coupled with tamper proof storage.

❑ Verify vehicle data against witnesses vehicles, etc) and environmental data (road signal, object positions, etc) .

Q2. Can transactions be tampered? How to avoid it?

❑ At any point in time when current block has not reached it's maximum size, potential liable parties can deny transactions from the final block.
❑ A Potential Solution [6]: Dynamic block size validation. Each micro transaction builds on hash of previous set of micro transactions which are validated and immutable..

Q3. Can a party deny evidence when requested?

S1. **If raw data is submitted** as a transaction on the block chain, we can not have denial of evidence. However, this imposes an unreasonable cost of data storage on all parties.

S2. **If hash of raw data is submitted** as a transaction on the chain. The raw data is kept in a fragmented ledger where each party only stores data that it requires.. We solve the storage problem with the risk of denial of evidence.

Q4. What if multiple parties collude to evade liability?

Assumption: Law enforcement agents are honest.

If either the Auto Manufacturer or the Insurance Agent colludes with the vehicle owner to deny liability, then the non colluding validators can detect the malicious party by checking timestamps and signatures of data provided.

Q5. What if Law enforcement, AM and IC collude ?

A5. Revolution!

Literature Cited

[1] Cebe, Mumin, et al. "Block4Forensic: An Integrated Lightweight Blockchain Framework for Forensics Applications of Connected Vehicles." arXiv:1802.00561 (2018).
[2] Oham, Chuka, et al. "A Blockchain Based Liability Attribution Framework for Autonomous Vehicles." arXiv preprint arXiv:1802.05050 (2018).
[3] NY Lawmakers Propose Insurance Discount For Dash Cam-Equipped Cars ." CBS News, June 30, 2016 , http://newyork.cbslocal.com/2016/06/30/dash-cam-insurance-discount/
[4] Light, Donald (8 May 2012). A Scenario" The End of Auto Insurance (Technical report). Celent.
[5] "Autonomous cars: Bring 'em on, drivers say in Insurance.com survey". Insurance.com. 28 July 2014. Retrieved 29 July 2014.
[6] Min, Xinping, et al. "A permissioned blockchain framework for supporting instant transaction and dynamic block size." Trustcom/BigDataSE/I SPA, 2016.

Acknowledgement

This poster is created as part of CSCI 599 course taught by Dr. Bhaskar Krishnamachari

Contact Info

For further information contact:.
Bhavya Gulati <bgulati@usc.edu>
Ritesh Ahuja <riteshah@usc.edu>

Conclusion & Future Work

Incentive mechanisms: Extending the idea presented, we can incentivize car vehicles for driving safe and sharing their data by granting them tokens. This way, vehicles would not need insurances, all they need is to share their data and in case of an accident, utilize these tokens for repairs.
Technical solutions to privacy: Use of Vehicle Public Key as pseudonyms to keep the identity of vehicle anonymous.
Experiments: The system proposed needs to be tested for huge amounts of fast incoming real-time data ingestion.