Securing Autonomous Vehicle Interactions with Blockchains

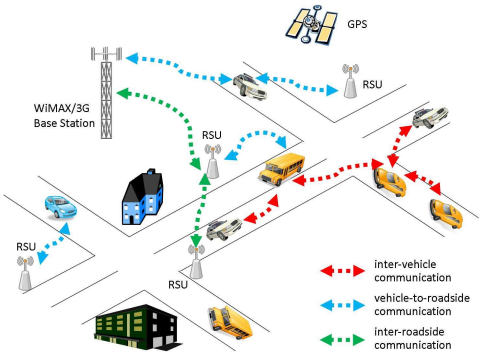
Matthew Wagner, Dr. Bruce McMillin
Department of Computer Science
Missouri S&T University of Science & Technology

Objective

Secure platoons of self-driving vehicles within a vehicular ad-hoc network (VANET) by using distributed blockchains.

Background

A VANET is a system where vehicles communicate with one-another for an application. There are multiple types of communication paths possible.



Source: http://www.cs.nthu.edu.tw/~jungchuk/research.html

Public Key Infrastructure (PKI)

Currently most solutions to security involve some variation of a PKI. A PKI includes:

- Every vehicle has certificates and keys that they use to create and authenticate messages.
- A large infrastructure is required.
- Constant communication with the infrastructure to revoke misbehaving users and maintain the systems integrity is required.

Blockchains

Blockchains are a digitally signed computationally immutable ledger. They consist of:

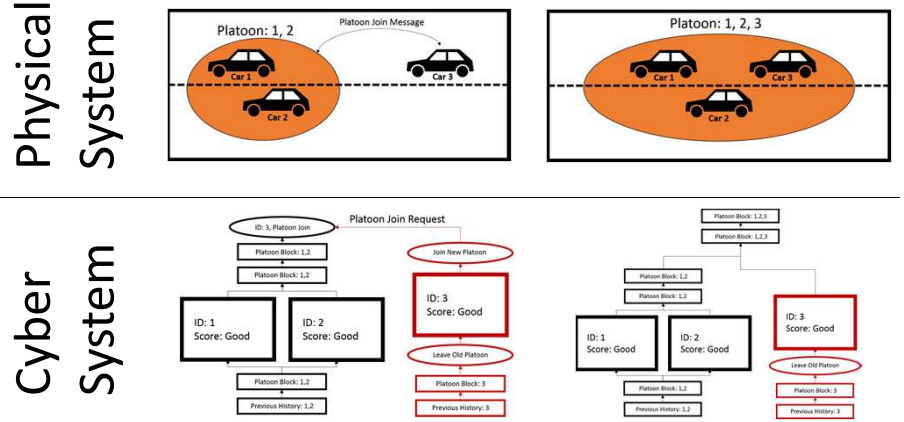
- Transactions that are digitally signed by a sender.
- Blocks that consist of a group of transactions that are publicly verified.
- A chain of blocks that are tied together by including the hash of the previous block within the current block. These serve as an agreed upon history.

Current Use: Blockchains are used primarily in digital currency. Chains such as Bitcoin and Ethereum use a blockchain in a distributed system as a form of a distributed ledger. However, blockchains can realistically be applied to any system where there is a group of peers that must collaborate on some task and agree on a system state. However, there must be a mechanism to determine the ground truth of the system.

Our Proposed Solution

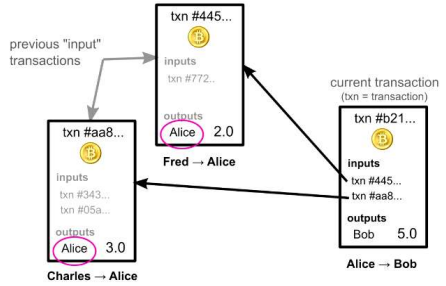
Our solution is to use blockchains as a building block for trust between vehicles. Our solution is as follows:

- Every vehicle certifies with a certificate authority which creates their genesis block.
- Every vehicle maintains its own blockchain.
- Blockchains are used as a token to allow vehicles to participate in high-risk activities.
- The vehicles make evaluations of other vehicles' actions. Platoons create blocks out of these evaluations and use these as the agreed upon state.



Verifiability

In Bitcoin, transactions are verified as by checking that someone sent the sender coin previously.



In the purposed system, transactions are verified by leveraging the physical system and the vehicles sensing capabilities.

Conclusions

By using blockchains we believe that we can create an immutable history of behavior that can serve as a token to detect correct or incorrect behavior locally. If we are able to successfully apply blockchains to our application while preserving the security properties then we will be able to extend this to the Internet of Things (IoTs) as a whole. This would allow us to be able to build trust in any application between peers that requires the cooperation of its peers in order to perform a critical task and agree on the state of the system.

This research is funded by the Missouri S&T's Chancellor's Distinguished Fellowship Program.