Impact of Blockchain Technology in Autonomous Vehicles

Madhusudan Singh,

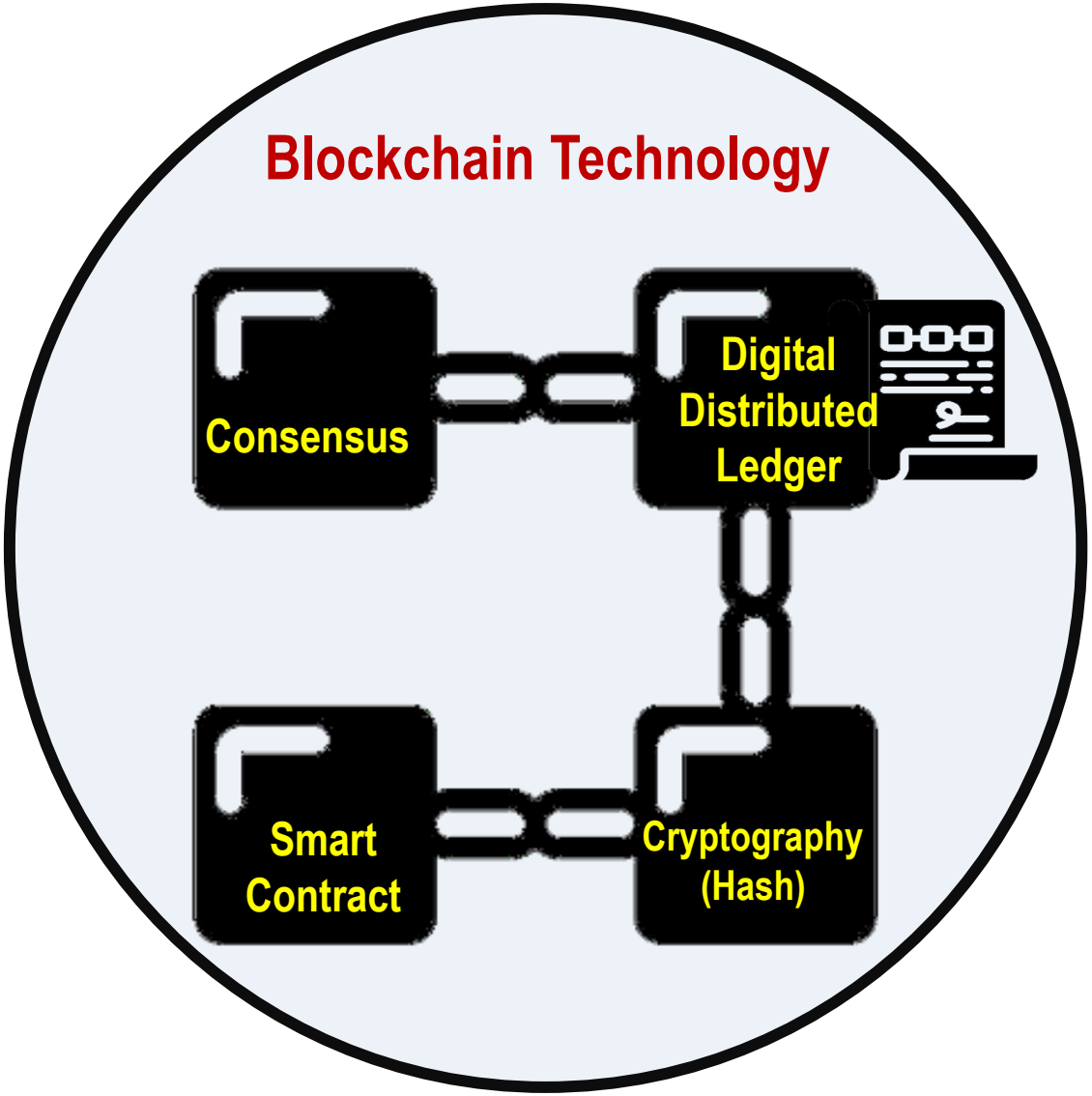
PhD, SMIEEE

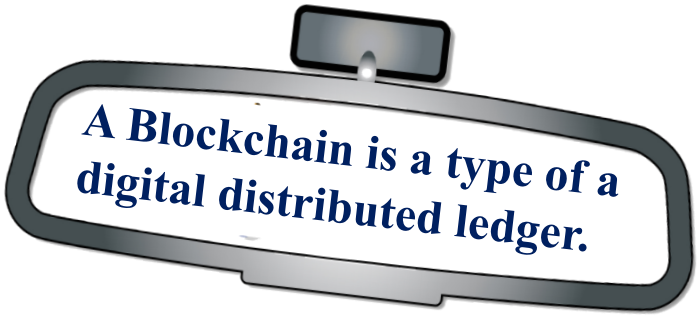
Associate Professor
Information Security Research Group
Institute of Computer Science
University of Tartu, Estonia

Contents

- Blockchain Technology
- Automotive Technology
- Automotive Technology Cyber Security
- Impact of Blockchain Technology in Autonomous Vehicles
- Blockchain Based Intelligent Vehicle Intersection:
  - A Use Case Scenario
  - Simulation Analysis of Applied Blockchain Technology Solutions

Understanding the Basics of Blockchain Technology

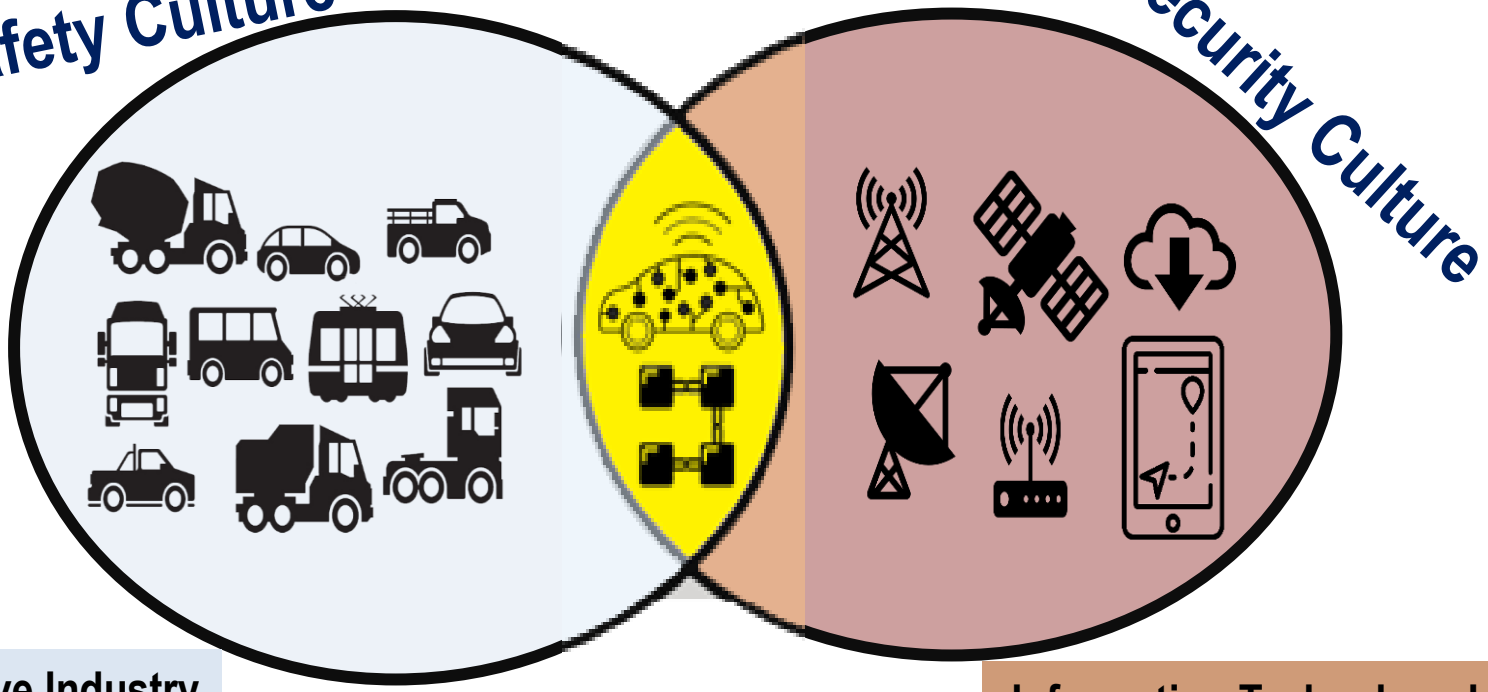




A type of distributed ledger designed to record digital interactions for the purposes of transparency, efficiency, and added security.

A consensus of replicated, shared, and synchronized digital data geographically spread across multiple sites. There is no central administrator or centralized data storage

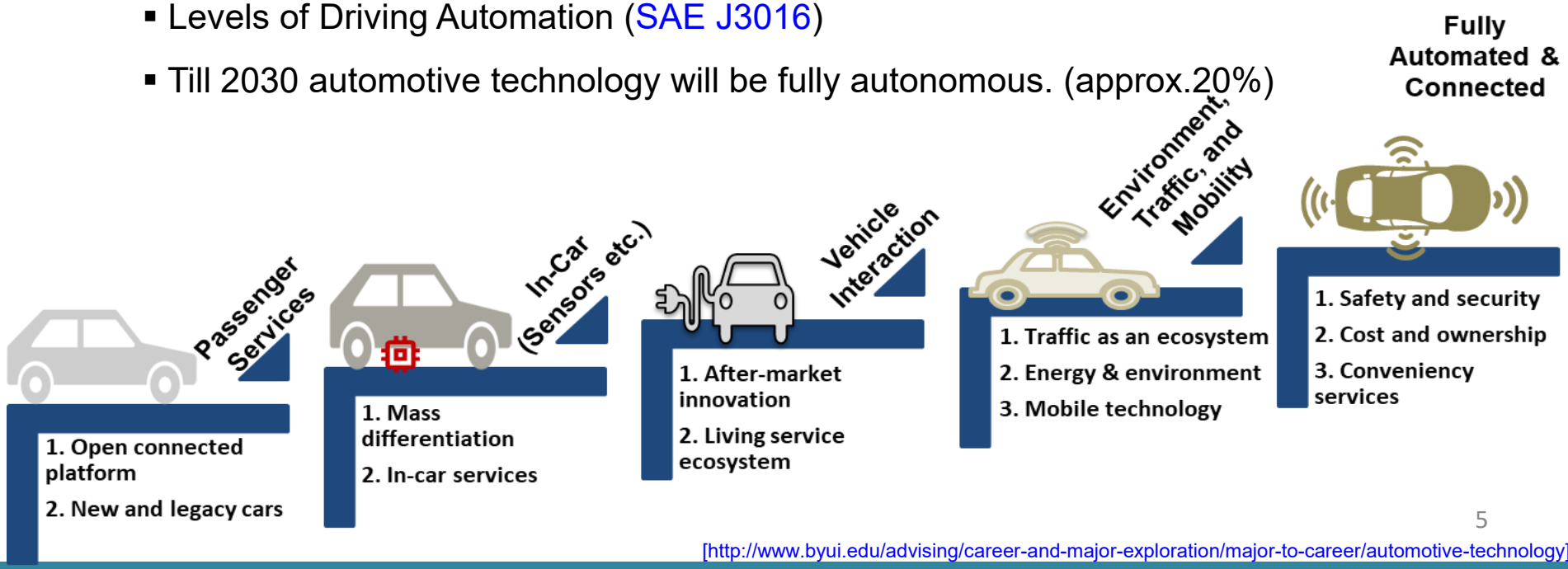
Why Blockchain and Autonomous Vehicles?



Automotive Technology Development-I

- Automotive technologies are the application of knowledge about self-propelled vehicles or machines.
- Automotive technologies are learned about engine construction, fuel and ignition systems, power trains, brakes, transmissions, electronic and diagnostic equipment, and more.

- **Automotive Technologies Development**
  - **Society of Automotive Engineers**: Standard **SAE J3016** defines classes of vehicle automation
  - Levels of Driving Automation (SAE J3016)
  - Till 2030 automotive technology will be fully autonomous. (approx.20%)



[http://www.byui.edu/advising/career-and-major-exploration/major-to-career/automotive-technology]

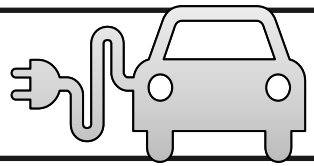
Automotive Technology Development -II

Level 0 – Driver Only →
Conventional Vehicle: Driver Manages all Aspects of Speed Direction

Level 1 - Assisted → Driver Receives Support for Specialized Task (e.g. Parking, Indicators, Back light etc.

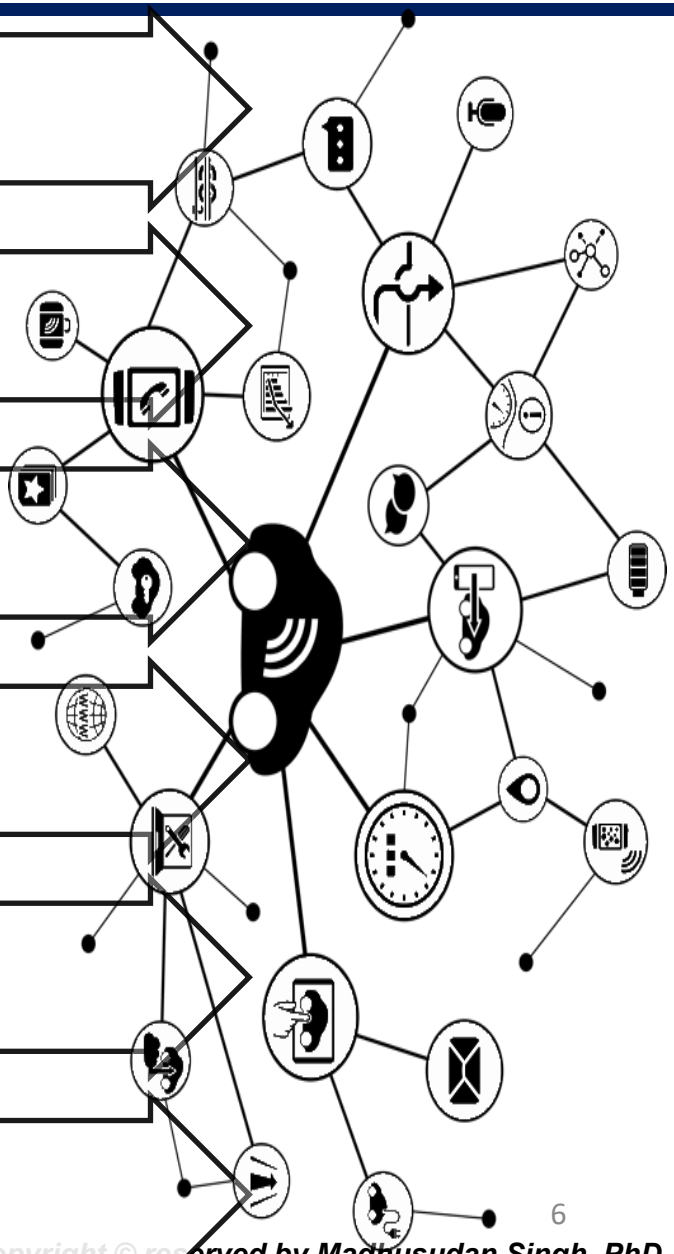
Level 2 – Partial Automation →
Driver receives support for coping with predefined scenarios (Services, traffic Jam warning & avoidance etc.)

Level 3 – Conditional Automation →
Driver can relinquish control to automated system but must be ready to take back control (e.g. Motorway Autopilot etc.)



Level 4 – Significant Automation →
Majority of Journey may automate by some driver intervention may be required (e.g. Urban Motoring

Level 5 – Complete Automation →
Complete end –to-end journey without driver intervention



Automotive Cyber Security Challenges

	Challenges Automotive Cyber Security	Possible Solutions Automotive Cyber Security
Technical Safety	• Protection against technical failures	Ensure security and safety aspect in the context of vehicle Communications Environment
Technical IT Security	• Protection against malicious manipulation & intrusion	Manage safety and security during the software development / upgradation
Quality Attributes	• End-user trust on applications and interconnected computing platforms & security-relevant organizational policies and processes	Provide trustworthy open automotive ecosystem and application store from end users centric perspective

Automotive Cyber Security Perspective

In-vehicle Security

V2X Security

V2I Security

Design

- To design Software & Hardware for Automotive Cyber security
- To create Trusted Platform
- To ensure interoperability
- To confirm Standards in Automotive Cyber Security

Build

- To build secure communication environment
- To develop dynamic environment

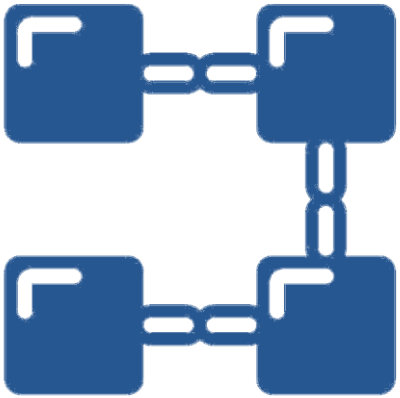
Services

- To ensure secure architecture for Connected Vehicles.
- To control vulnerabilities pre/post “threats”
- To allow users to use services at low risk

Target

- Securing content
- Authorization
- Authentication
- Message Integrity
- Protect Privacy
- Data security of vehicles & Users
- Etc.

Why Blockchain and Autonomous Vehicles?

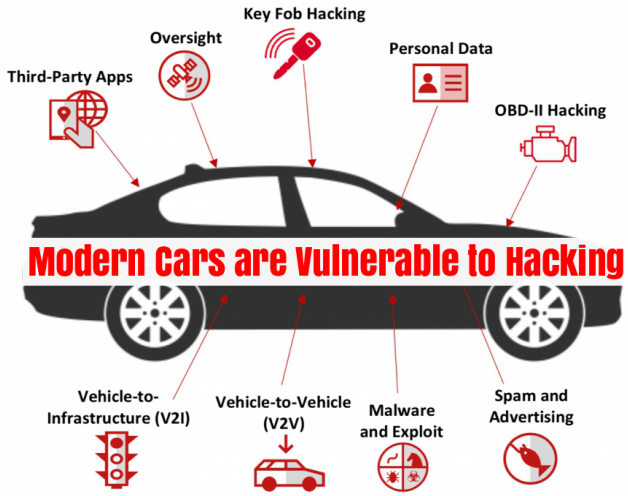


Blockchain Technology

Autonomous Vehicle Technology

Traditional Vs. Blockchain Protection

Traditional security protection



- Centralized architecture
- Heavy on resources
- Unable to protect data that is mobile
- Unable to handle large amounts of data at the same time
- No access to vehicle history
- No distributed network

Blockchain Technology Protection

- De-centralized architecture
- Low on resources
- Able to protect data that is mobile
- Able to handle large amounts of data at the same time
- Access to vehicle history
- Distributed network

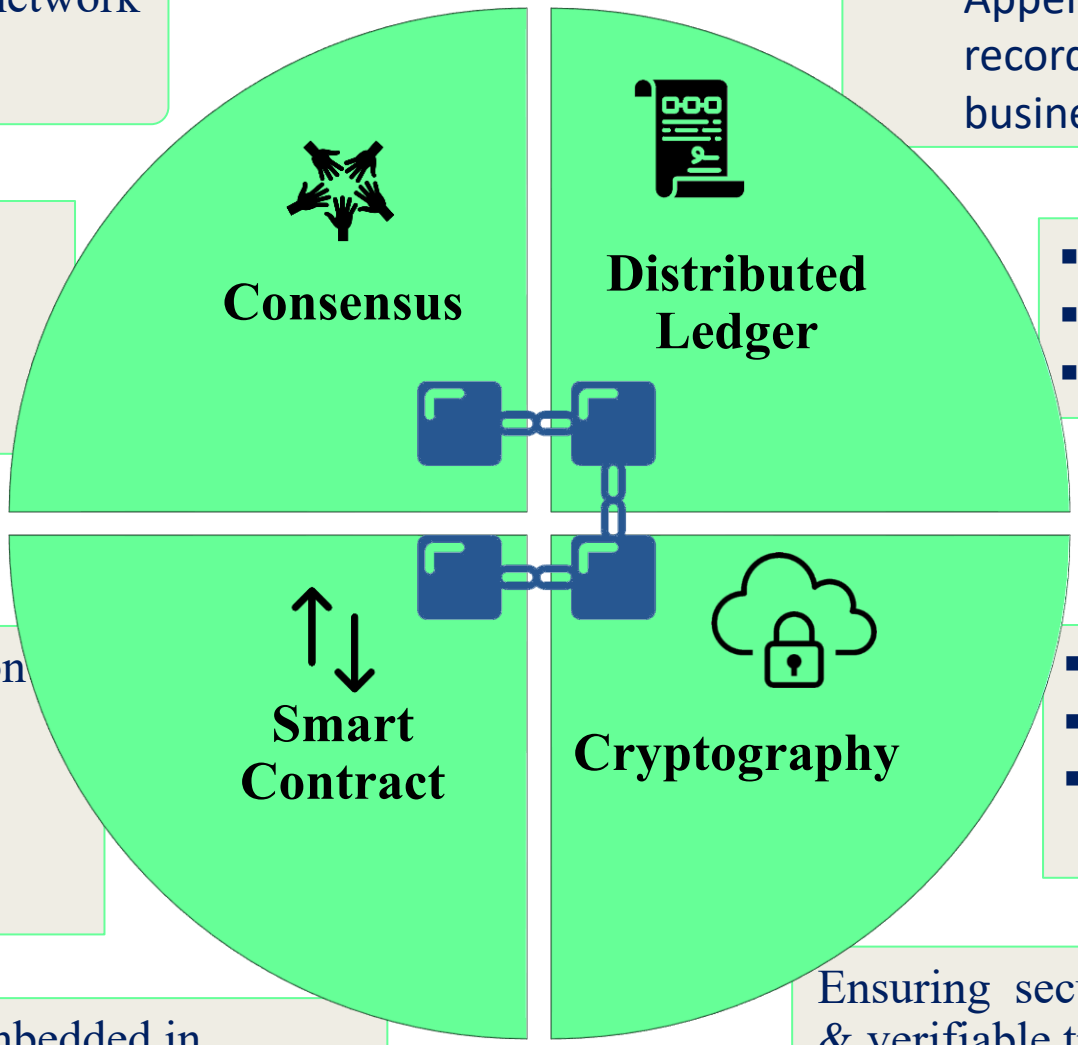
Relevant Blockchain Characteristics for Vehicles

All parties agree to network verified transaction

- Trust ability
- Liability
- Authentication /Authorization

Append-only system of record shared across business network

- Availability
- Retain ability
- Traceability



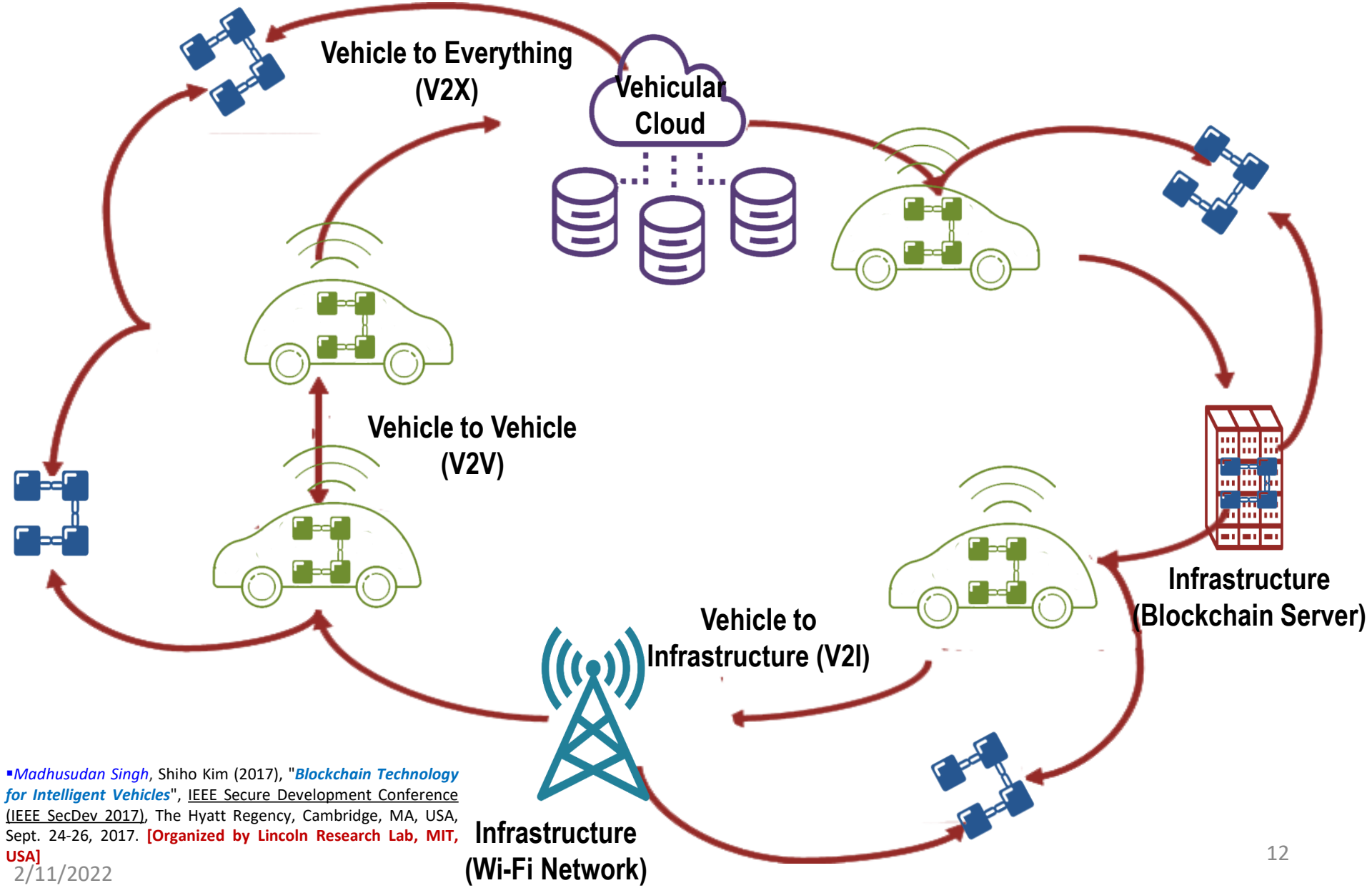
- Trust the negotiation process and final contract
- Trust ability
- Non-Repudiation

Terms embedded in transaction database & executed with transactions

- Confidentiality
- Data encryption
- Integrity (no modification)

Ensuring secure, authenticated & verifiable transactions

The Blockchain Communication Environment



▪*Madhusudan Singh*, Shiho Kim (2017), "***Blockchain Technology for Intelligent Vehicles***", IEEE Secure Development Conference (IEEE SecDev 2017), The Hyatt Regency, Cambridge, MA, USA, Sept. 24-26, 2017. **[Organized by Lincoln Research Lab, MIT, USA]**

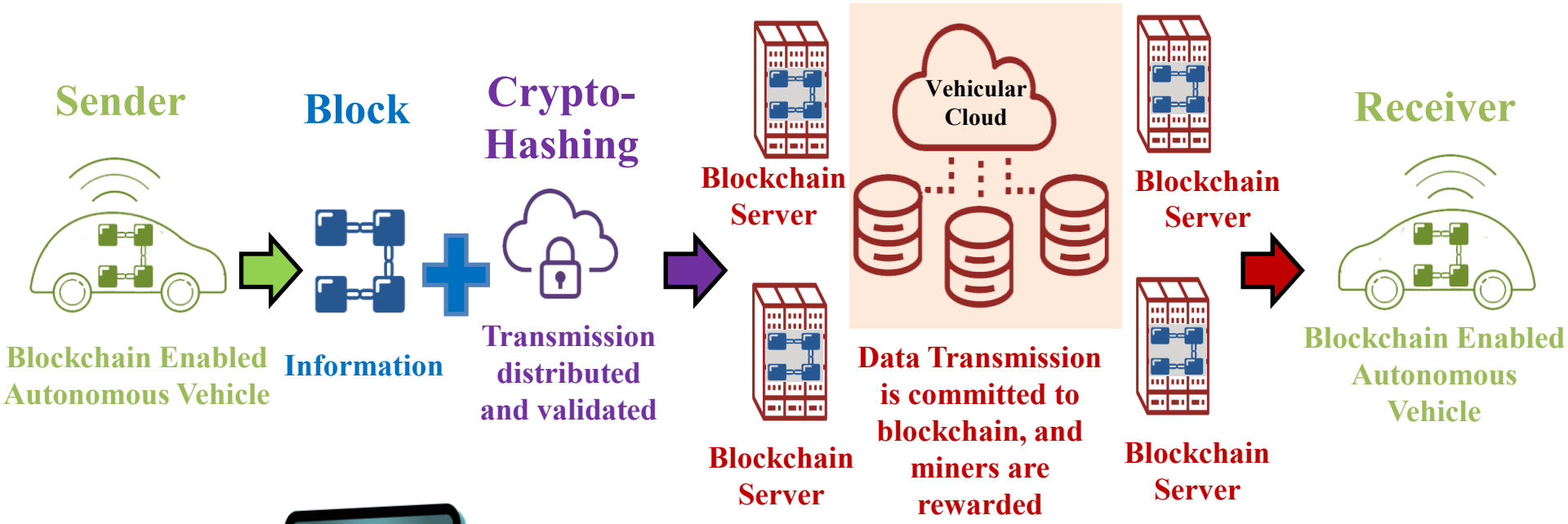
The Push for Blockchain Technology Solutions

Utilizing the Same Basic Road and Highway Infrastructure

- ⇧ Increase the Number of Passengers
- ⇧ Increase the Amount of Goods
- ⇧ Increase Average speed

- ⇩ Decrease Congestion
- ⇩ Decrease Accidents/Crashes
- ⇩ Decrease Carbon Footprint

Blockchain Technology Process in Autonomous Vehicles



The vehicular cloud is a hybrid technology that uses vehicle resources, such as computing, data storage, and internet decision-making.

A "miner" is a blockchain enabled vehicle that can validate the data transmission in the network

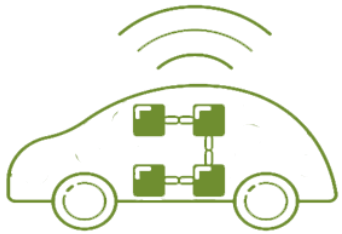
Explaining What Are Miner "Rewards"

Intelligent Vehicle Trust Point [IV-TP]

Sender

Blockchain Enabled Autonomous Vehicle

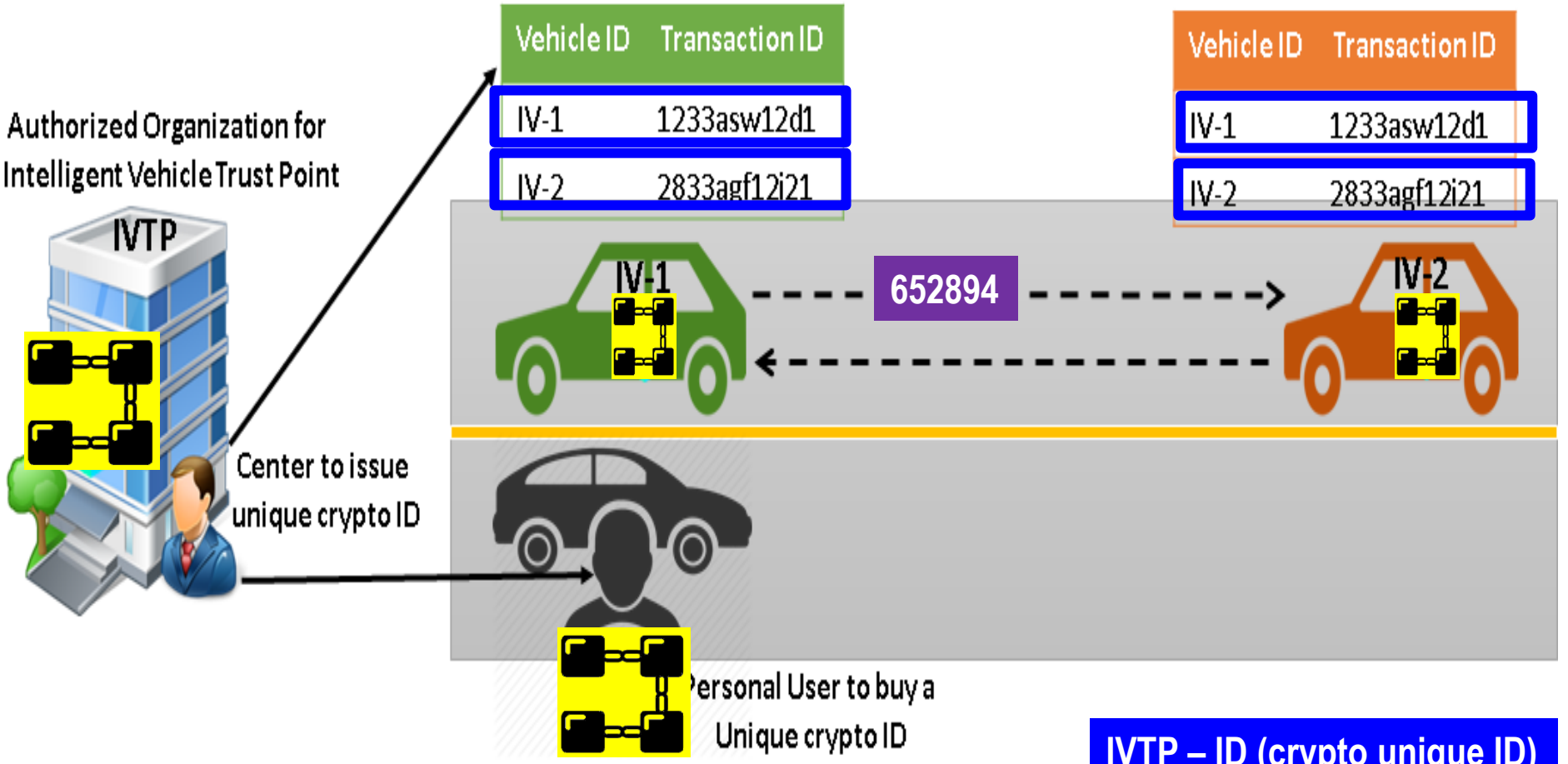
Receiver



Blockchain Enabled Autonomous Vehicle

▪*Madhusudan Singh*, Shiho Kim (2018), "*Trust Bit: Reward-based Intelligent Vehicles Communication using Blockchain*", The 4th IEEE World Forum on the Intelligent of Things (WF-IoT), Singapore, Feb. 05-08, 2018, 10.1109/WF-IoT.2018.8355227 . **[Citation: 53]**

Why Are These Rewards Important?



IVTP – ID (crypto unique ID)

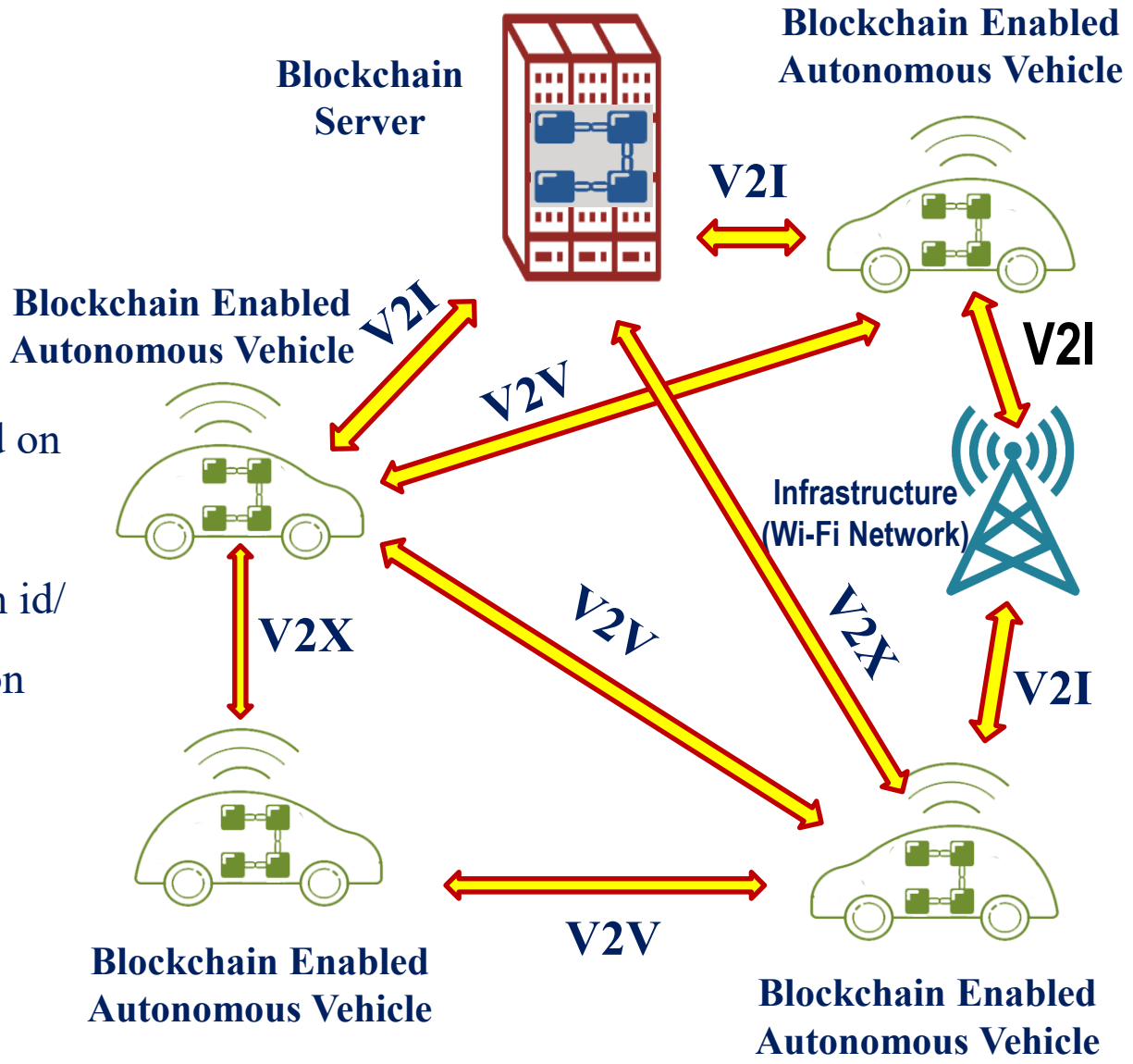
Reward IVTP unique ID

Blockchain enabled services

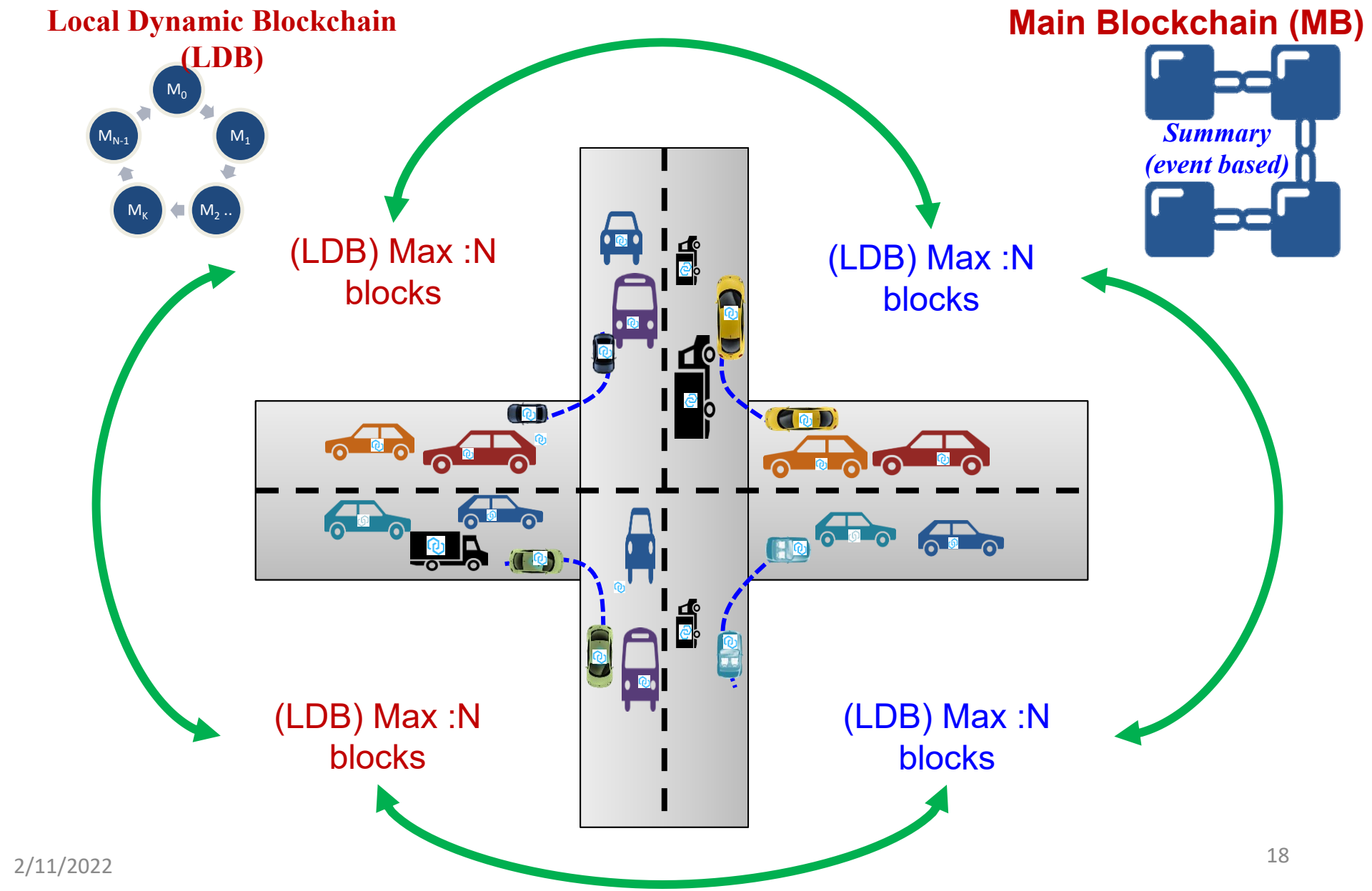
▪*Madhusudan Singh*, Shiho Kim (2018), "***Crypto Trust Point (cTp) for Secure Data Sharing among Intelligent Vehicles***", The 2018 International Conference on Electronics, Information and communication (ICEIC 2018), Sheraton Waikiki Hotel, Honolulu, Hawaii, USA, Jan. 24-27, 2018, 10.23919/ELINFOCOM.2018.8330663

Why Are These Rewards Important?

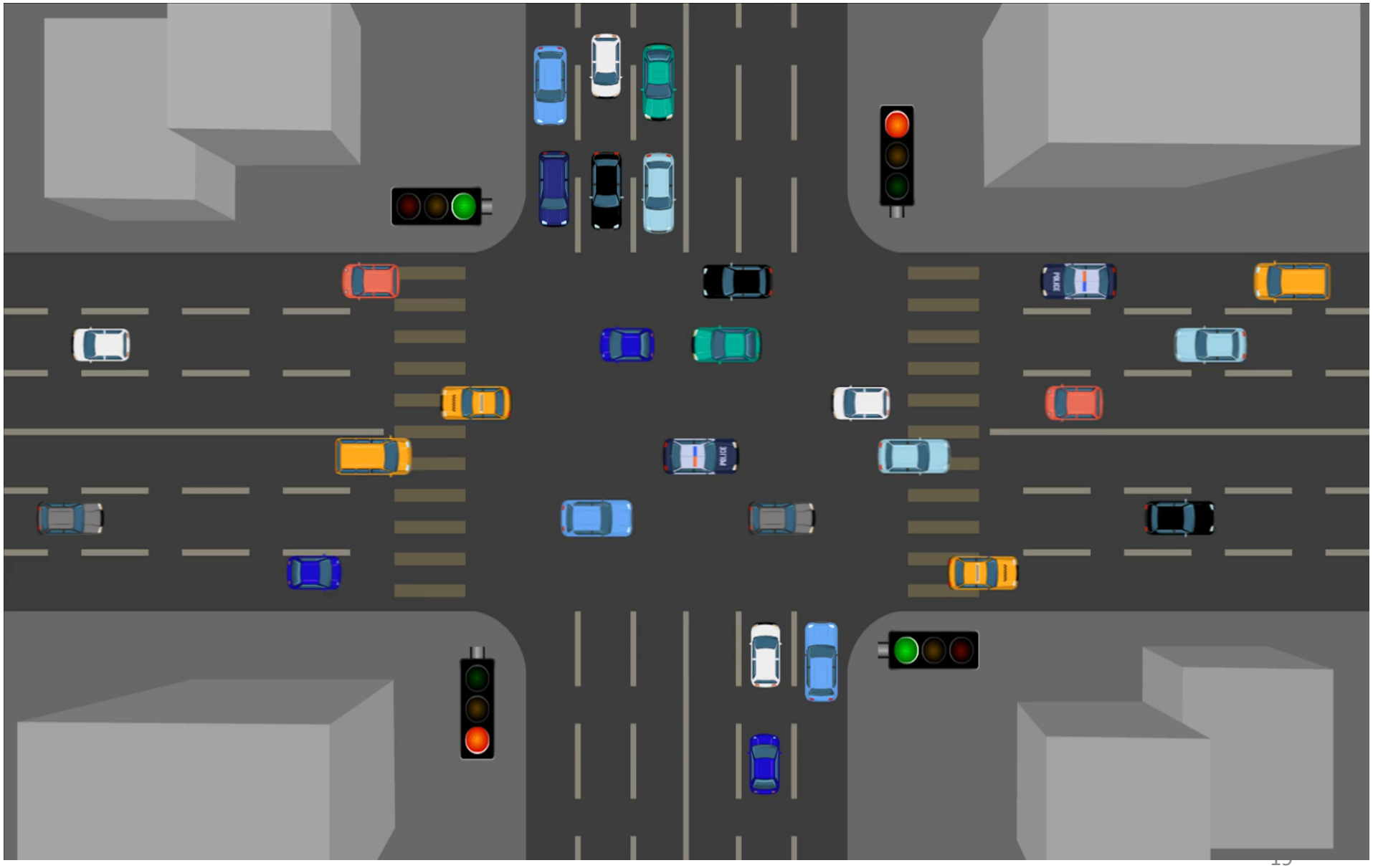
- Intelligent vehicle Trust Point (IVTP)
  - Blockchain (Block): Secure trusted communication based on blockchain Server
  - Store the vehicle hash id/ IVTP / communication details



Blockchain Technology for Vehicular communication Environment : Overview

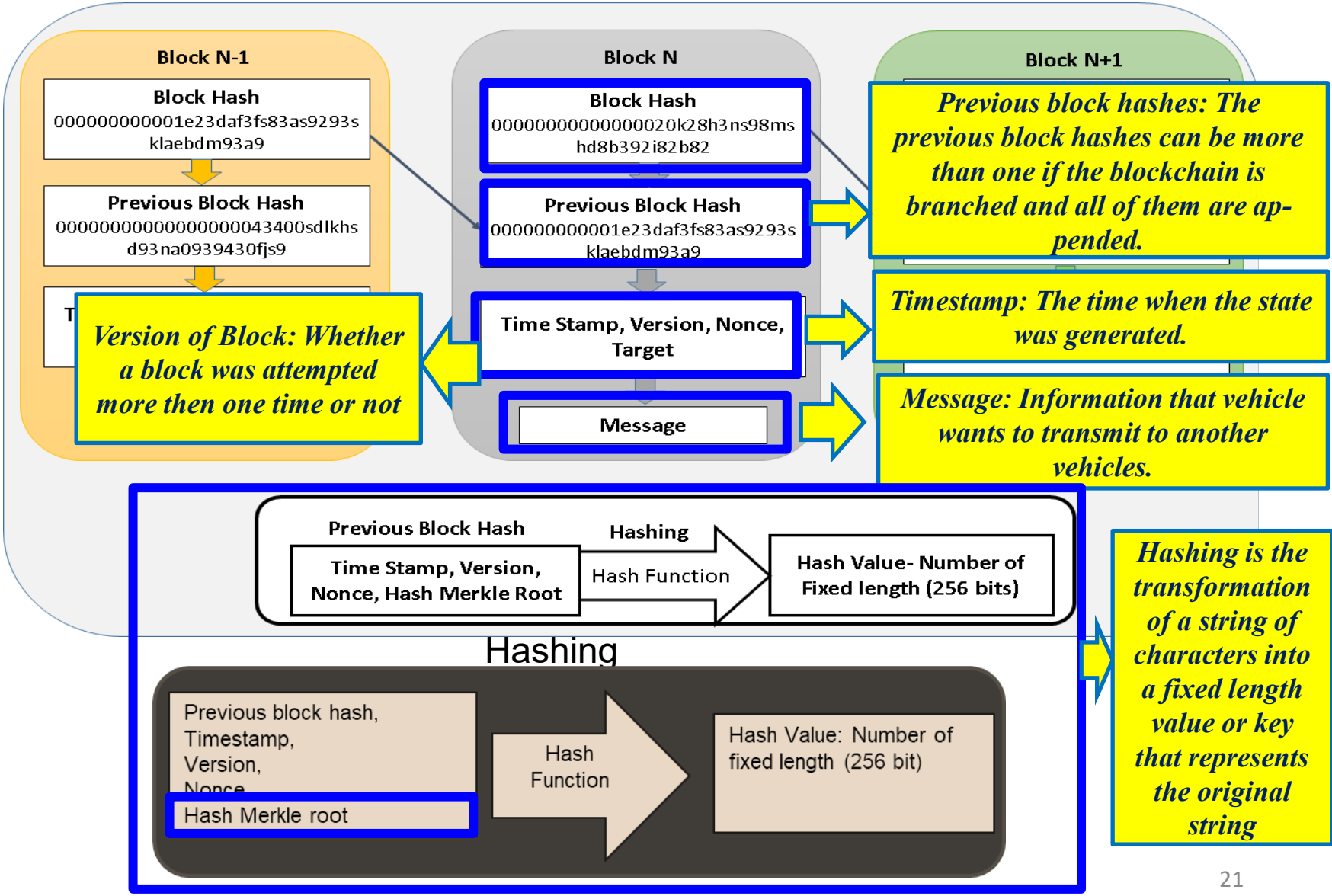


Traffic Scenario Without Blockchain



Traffic Scenario With Blockchain

Blockchain Methodology: The Structure of Blocks



Understanding State Changes of Vehicles

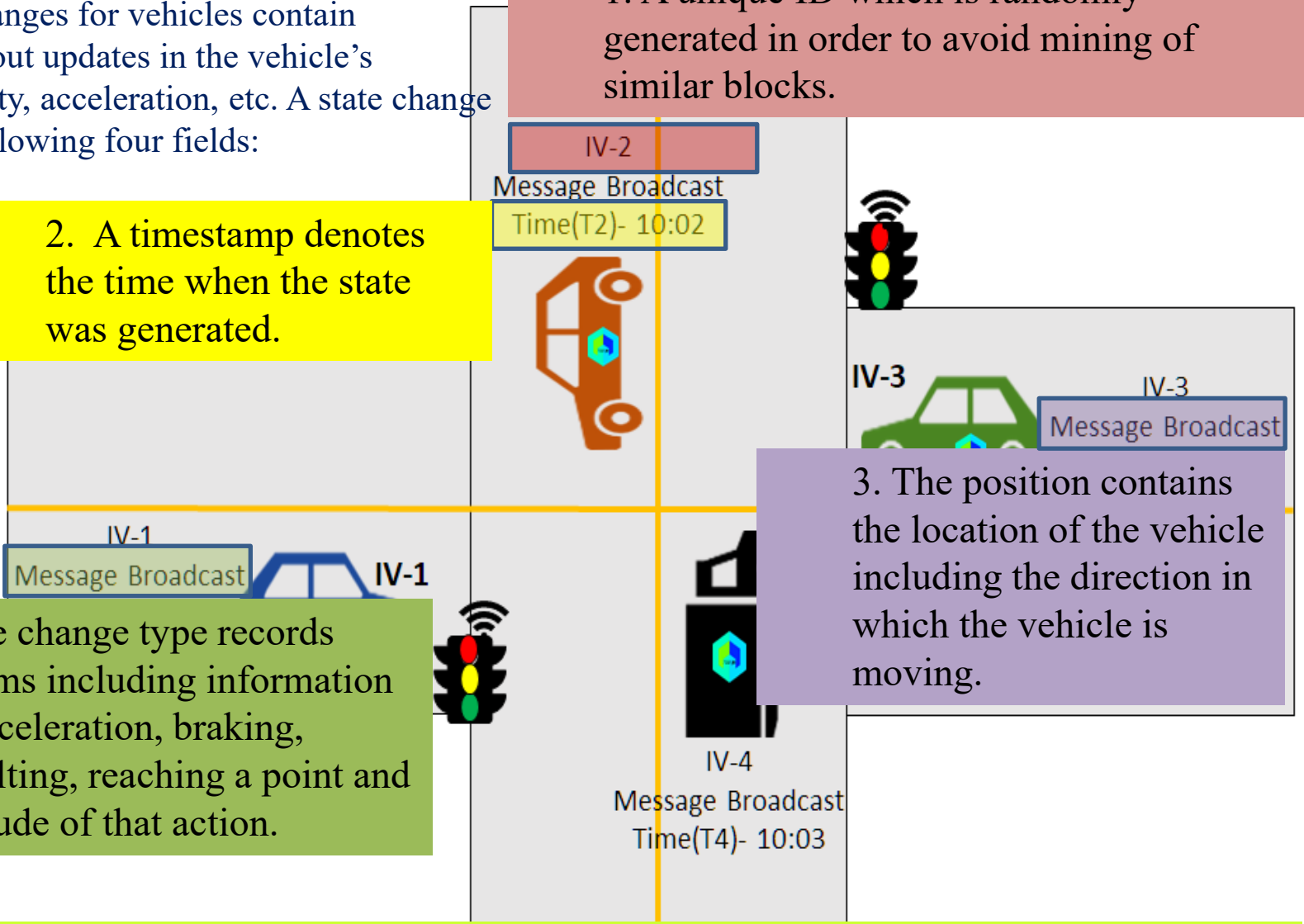
- The state of changes for vehicles contain information about updates in the vehicle's position, velocity, acceleration, etc. A state change contains the following four fields:

1. A unique ID which is randomly generated in order to avoid mining of similar blocks.

2. A timestamp denotes the time when the state was generated.

3. The position contains the location of the vehicle including the direction in which the vehicle is moving.

4. The state change type records various items including information on start, acceleration, braking, turning, halting, reaching a point and the magnitude of that action.



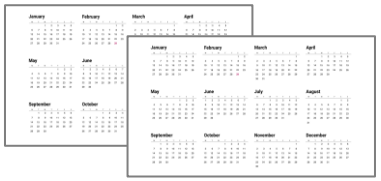
- These four values are included within the Hash block which must start with a specified nonce (number of zeroes).

Challenges with General Blockchain in Autonomous Vehicles

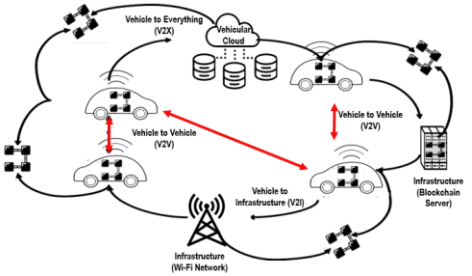
- Consumption of significant amounts of power

- Requires large-size data servers to manage information in real time

- Storage of Data needs to be stored for long periods time (more that two years).



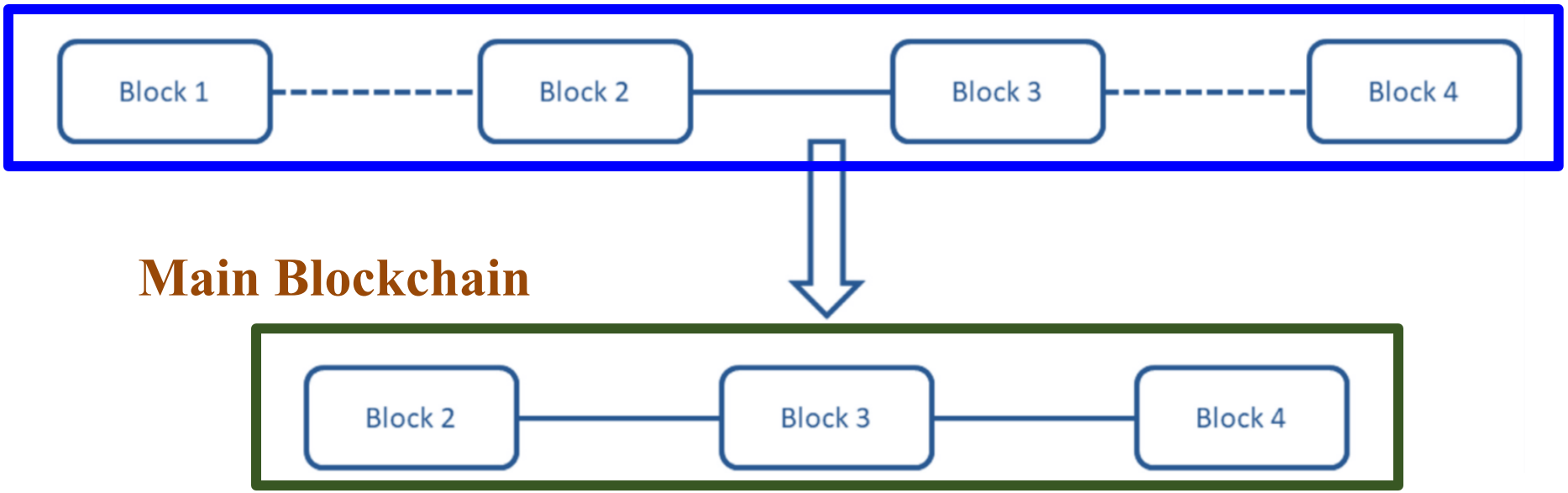
- Management of Data exchanged in a mobile and dynamic environment is difficult to manage



Local Blockchain & Main Blockchain Technology

Local Dynamic Blockchain

If it exceeds maximum length (say = 3)

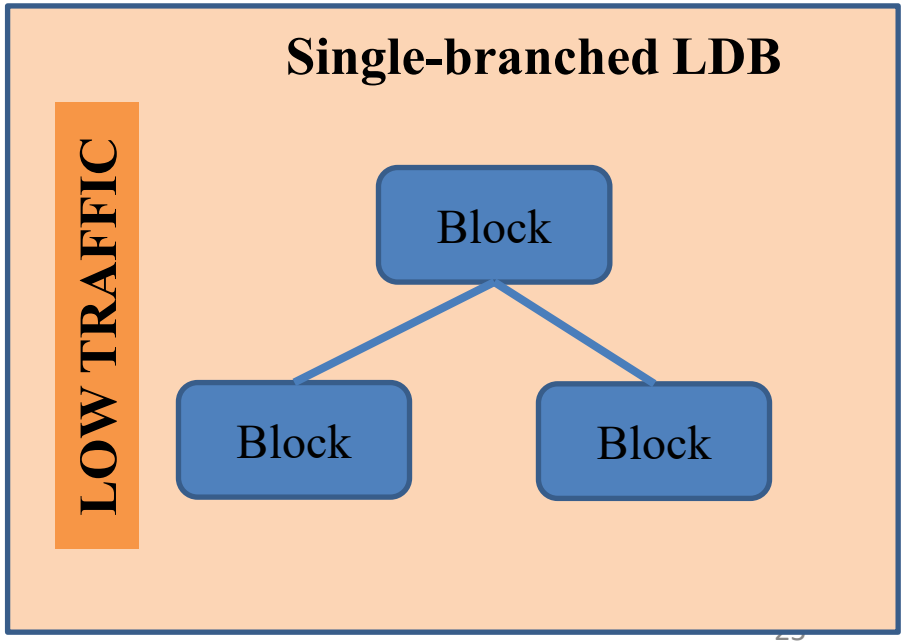


- Shiho Kim, *Madhusudan Singh*, "*비중앙집중형 자동차 보안 신뢰 네트워크 장치 및 방법* [APPARATUS AND METHOD FOR DECENTRALIZED SECURE]", Pub. No: 1020190010195, 2019.01.30, *[Granted]*, Korea Patent.

Understanding the Branching Process

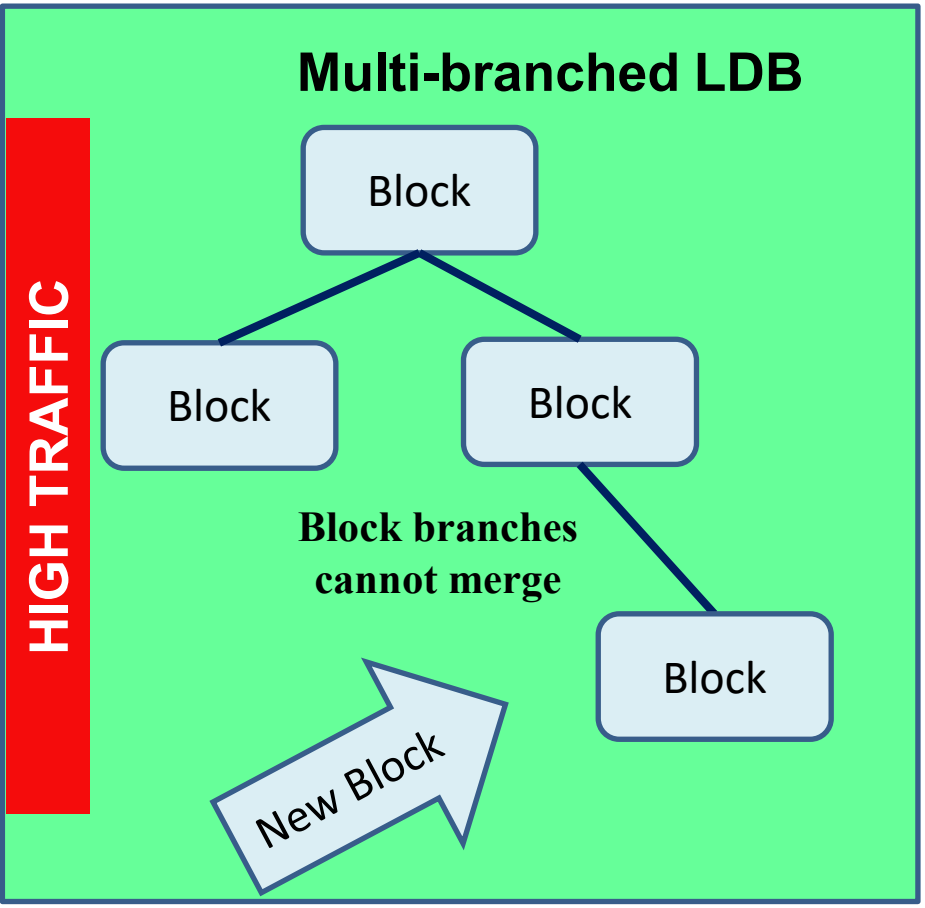
- Branching is performed by the local dynamic blockchain when the amount of traffic can be handled in real time.
- The branching process is governed by this equation, where ***DELTA 'T'*** is the average time which equals the summation of the difference between the mining time and the message broadcasting time over the total number of vehicles.

$$\Delta t_{avg} = \frac{\sum_{i=1}^{n} (t_{block\,mined} - t^{i}_{broadcast})}{n}$$



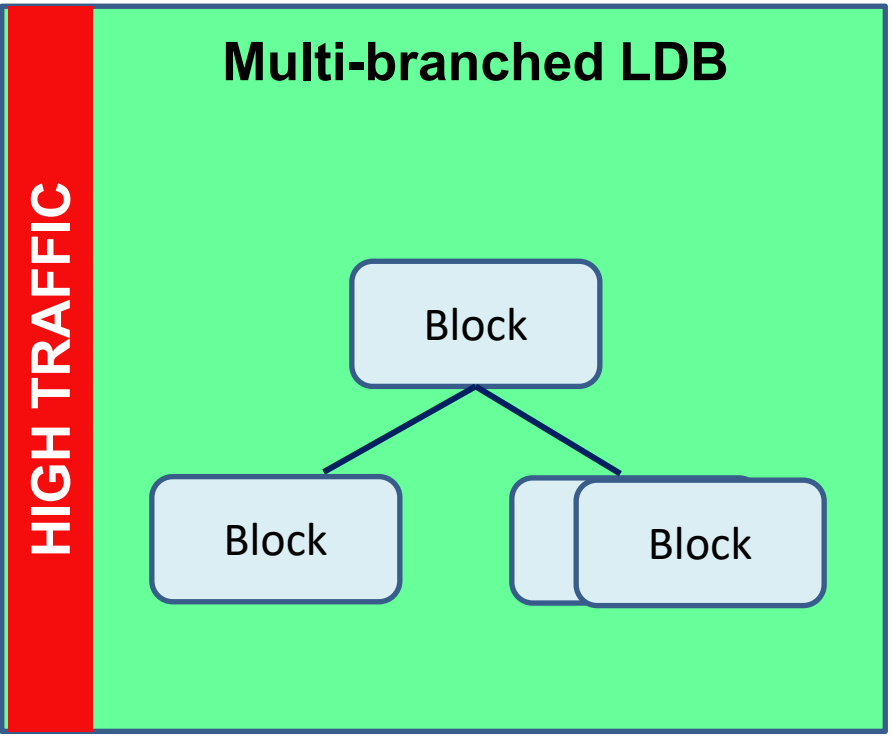
Madhusudan Singh, Shiho Kim, "***Branch Based Blockchain Technology in Intelligent Vehicle***", Computer Networks, 2018, ISSN 1389-1286, https://doi.org/10.1016/j.comnet.2018.08.016

Understanding the Branching Process



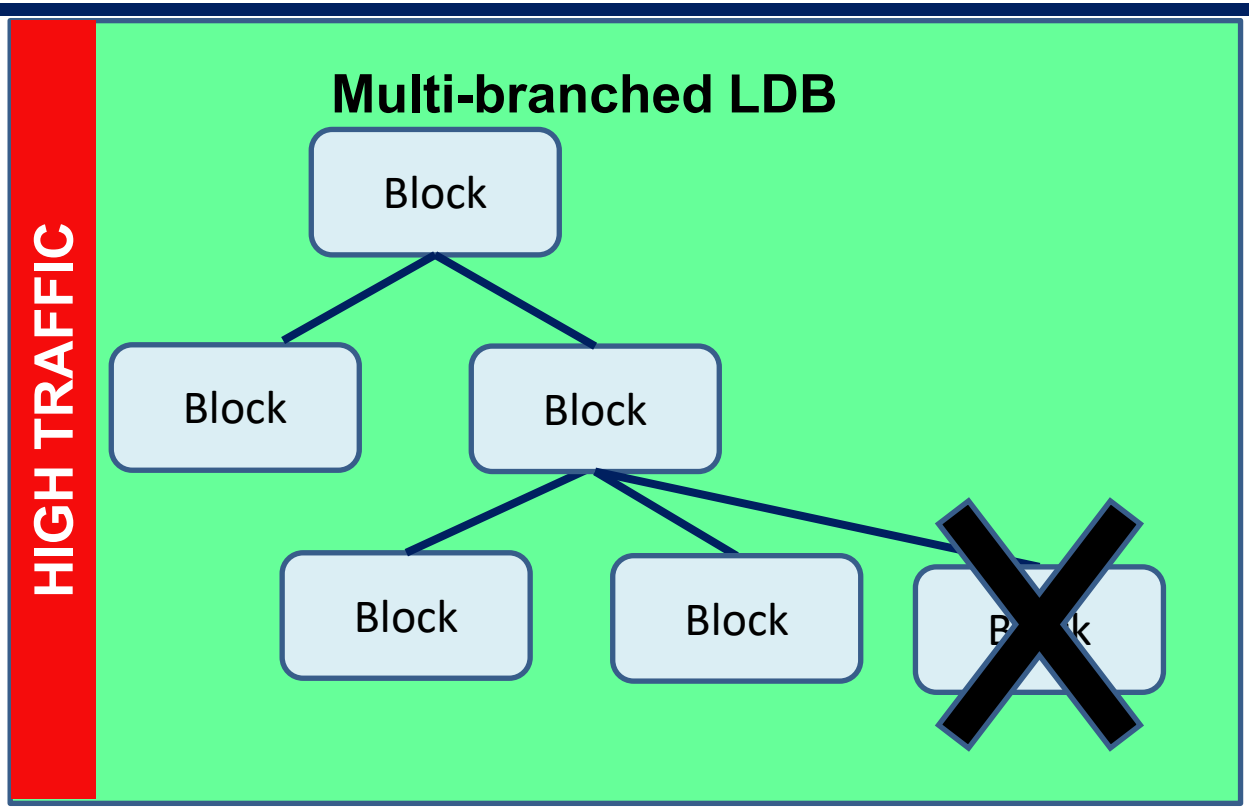
- If the LDB has branches, a block has a possibility to be added in the blockchain, hence making the process run faster.

Understanding the Branching Process



- When LDB recognizes that the traffic has decreased and can be handled by a lesser number of branches, it can merge two branches into a single branch.

Understanding the Branching Process



- A branch in LDB can only be divided into two child branches and not more.
- This blockchain is used to keep track of IV-TP transactions between two vehicles.
- This operates in a way similar to the bitcoin mechanism.
- Both in the bitcoin universe and the vehicular blockchain environment, we utilize Merkle Trees.

Construction of the Branching Process

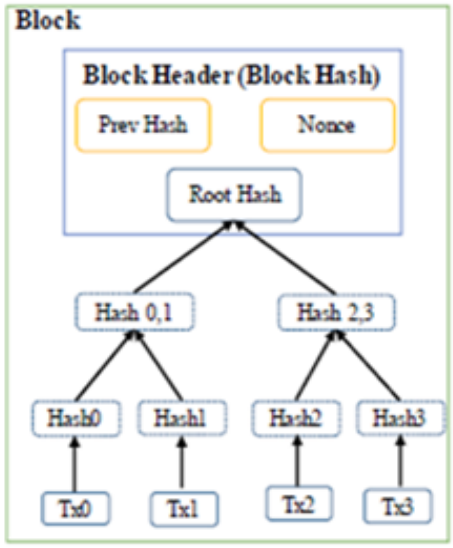
- MB is implemented using Merkle trees.

- ***Previous Branching factor > Current branching factor:***

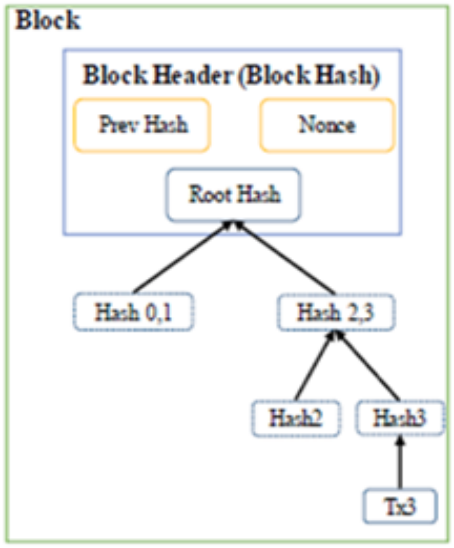
- ***Previous Branching factor < Current branching factor***

- ***Branching factor of parent*** = *Current branching factor:* Trivial case, one parent has one child.

The Merkle Tree only contains hashes, it does not contain the transaction data itself



Transactions Hashed in a Merkle Tree



After Pruning Tx0-2 from the Block

Understanding Miner Thread Pseudocode

```
function miner_thread ( )
1.    start
2.        while ( true ):
3.            if toMine is empty:
4.                continue
5.            else:
6.
7.
8.
9.
10.   end
```

The *miner_thread* function runs from the starting of the vehicle to its shutdown taking care of the mining procedure.

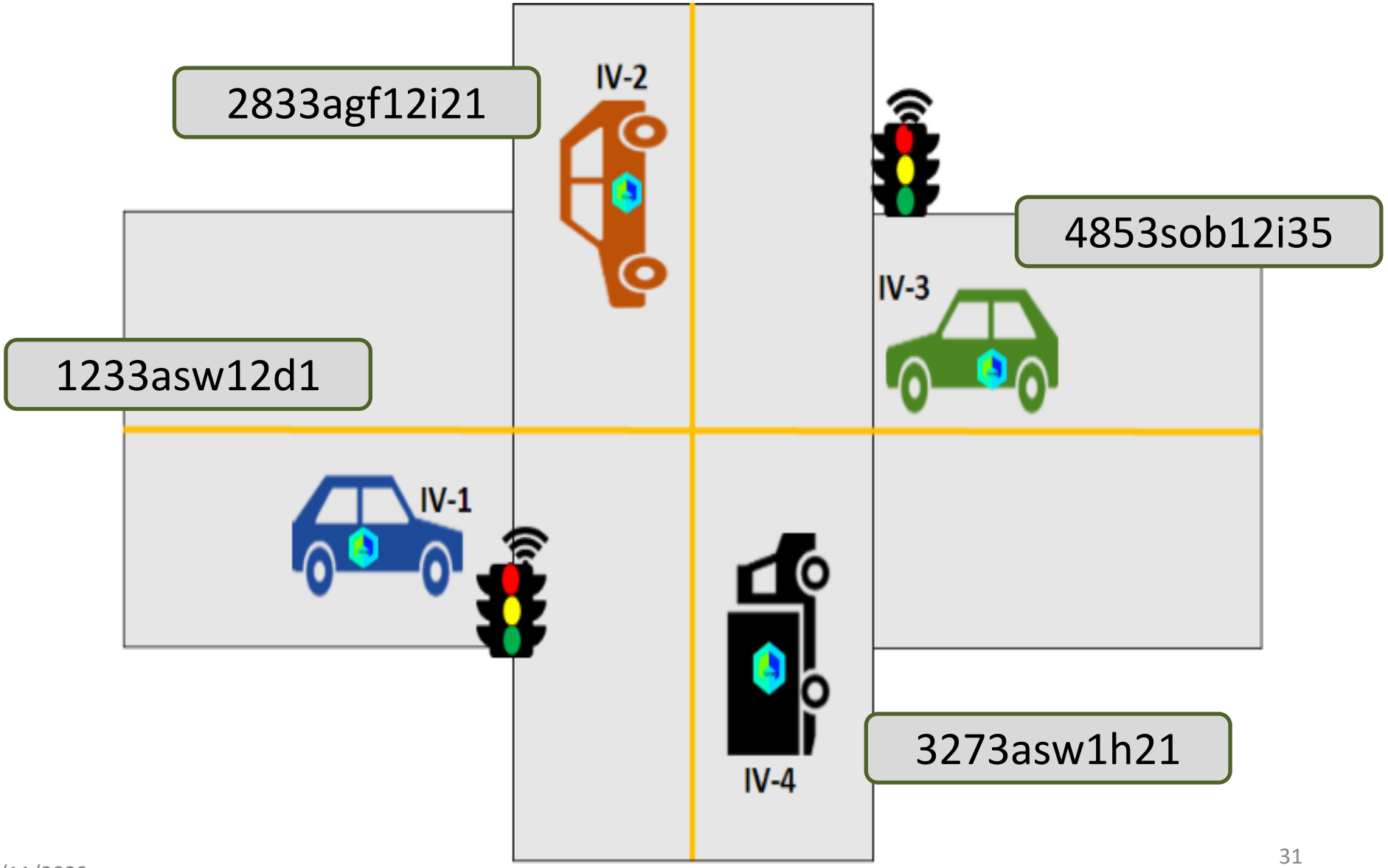
The get_template function queries the LDB for the template (a list containing information such as a version of the blockchain, parent hashes, etc.)

```
template = get_template ( )
mined_block = mine_block (toMine, template)
if add_block (mined_block) is success:
toMine.clear ( )
```

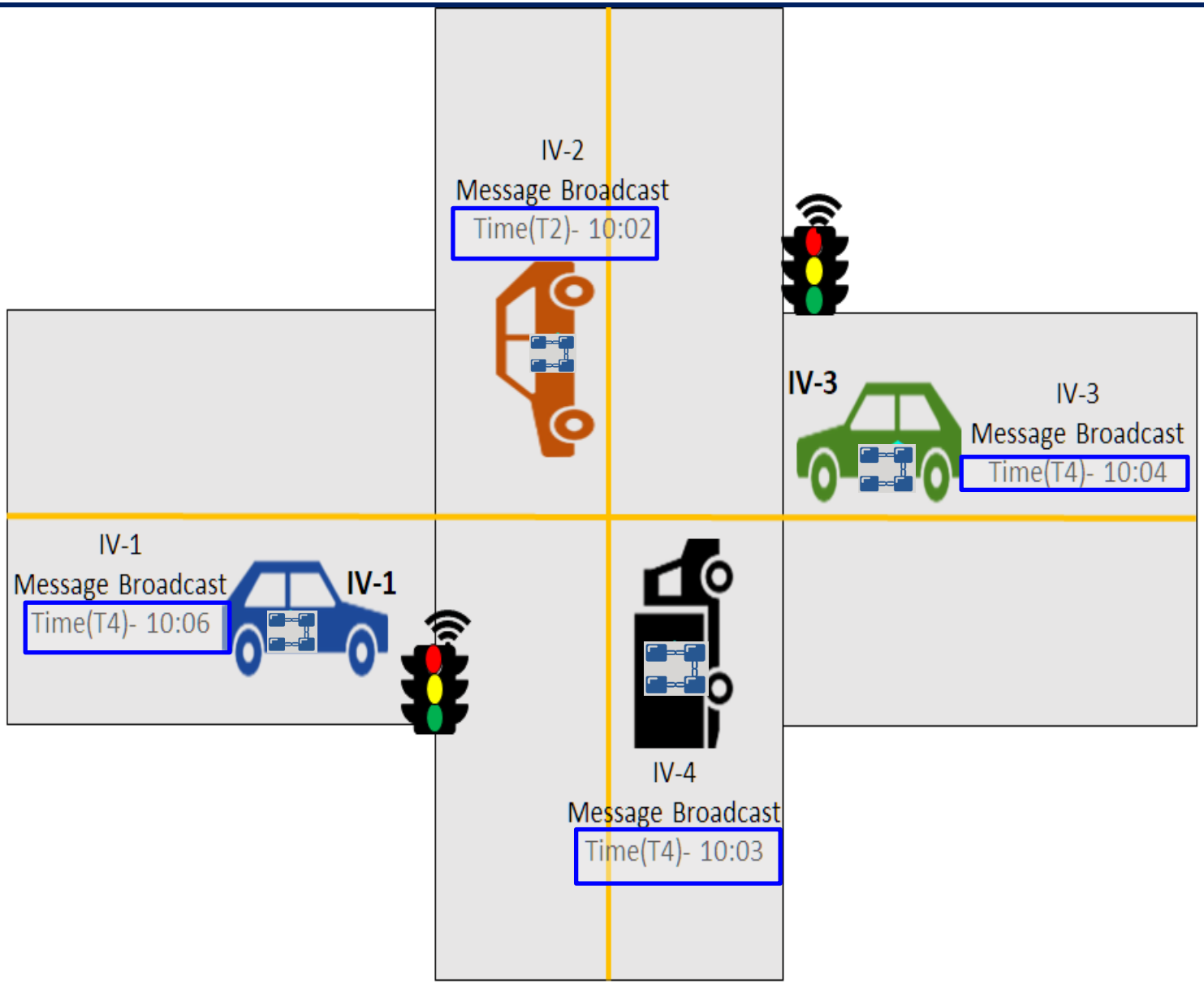
The miner_thread, along with mine_block carry out the solution of the hash function thereby generating the proof of work.

The add_block function simply sends the mined block to be added in the LDB subject to verify the proof of work (consensus mechanism).

Use Case Scenario of Blockchain Based Intelligent Intersection



Use Case Scenario of Blockchain Based Intelligent Intersection



Use Case Scenario Analysis

Intersection scenario message broadcasting time schedule by intelligent vehicles

Arrival Time of IVs	Processing Time	IVTP of IV 1	IVTP of IV 2	IVTP of IV 3	IVTP of IV 4	Remarks
	00:00:00	10	10	10	10	No vehicle issued start block
IV-1→ 10:06	00:00:05	10	10	10	10	IV 2 sends the start block, starts moving
	00:00:06	10	10	10	10	IV 3 and IV 4 send start block, start moving
IV-2 → 10:02	00:00:07	10	10	10	10	IV 1 sends start block, starts moving
	00:00:10	11	9	10	10	IV 2 reaches intersection and IV 1 mines the block, IV 2 crosses the intersection after consensus
IV-3→ 10:04	00:00:12	12	9	10	9	IV 4 reaches intersection, issues the intersection block and IV 1 mines it but cannot move since IV 2 is crossing
	00:00:15	12	9	10	9	IV 4 which came second is now able to cross
IV-4 →10:03	00:00:20	13	9	9	9	IV 3 which came in third, is now able to move, IV 1 mined this block again
	00:00:28	13	9	9	9	IV 1 which came in last, is now able to cross

Why Are These Rewards Important?

Arrival Time of IVs	Processing Time	IVTP of IV 1	IVTP of IV 2	IVTP of IV 3	IVTP of IV 4	Remarks
4	00:00:00	10	10	10	10	No vehicle issued start block
IV-1→ 10:06	00:00:05	10	10	10	10	IV 2 sends the start block, starts moving
1	00:00:06	10	10	10	10	IV 3 and IV 4 send start block, start moving
IV-2 → 10:02	00:00:07	10	10	10	10	IV 1 sends start block, starts moving
3	00:00:10	11	9	10	10	IV 2 reaches intersection and IV 1 mines the block, IV 2 crosses the intersection after consensus
IV-3→ 10:04	00:00:12	12	9	10	9	IV 4 reaches intersection, issues the intersection block and IV 1 mines it but cannot move since IV 2 is crossing
2	00:00:15	12	9	10	9	IV 4 which came second is now able to cross
IV-4 →10:03	00:00:20	13	9	9	9	IV 3 which came in third, is now able to move, IV 1 mined this block again
	00:00:28	13	9	9	9	IV 1 which came in last, is now able to cross

Reward points

Benchmark for Mining Analysis

Difficulty of proof of work

Difficulty level (number of zeros in beginning of the Hash)	Average time is taken for mining (Average after 100 tries)
Level 1(0)	0.0045
Level 2(00)	0.06705
Level 3(000)	1.03083
Level 4(0000)	11.9460
Level 5(00000)	62.9950

Simulation Analysis of Applied Blockchain Technology Solutions

Blockchain
Windows 10 on an Intel Core i7-6700HQ CPU clocked at 2.6GHz with 8GB RAM

(Intelligent Vehicle 1)
Windows 10 on an Intel Core i7-4770 CPU clocked at 3.4GHz with 16GB RAM

(Intelligent Vehicle 2)
Windows 10 on an Intel Core i7-3770 CPU clocked at 3.4GHz with 16GB RAM

(Intelligent Vehicle 3)
Ubuntu 17.04 on an Intel Core i5-4210U CPU clocked at 1.7GHz with 4GB RAM

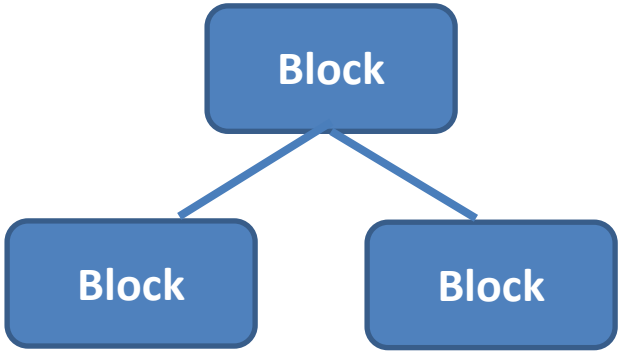
(Intelligent Vehicle 4)
Linux Mint 18.1 on an Intel Core i7-7700HQ CPU clocked at 2.8GHz with 8GB RAM

Calculation

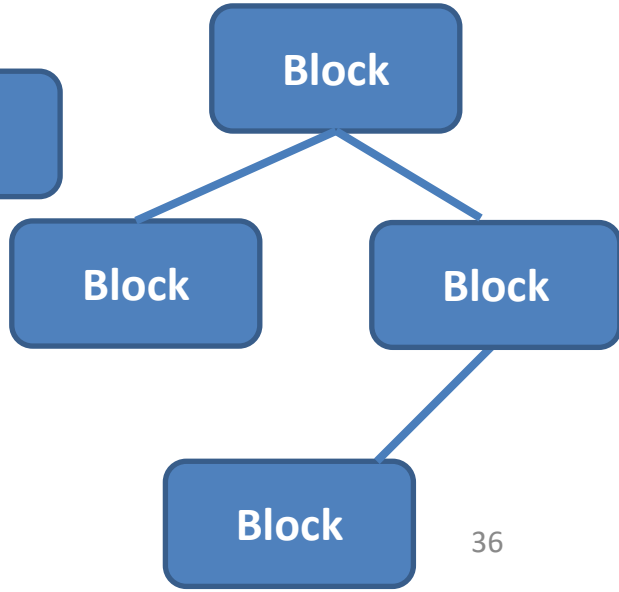
$$\frac{\text{Average Time taken for mining analysis in seconds}}{\text{Number of nonce}}$$

Level of Congestion

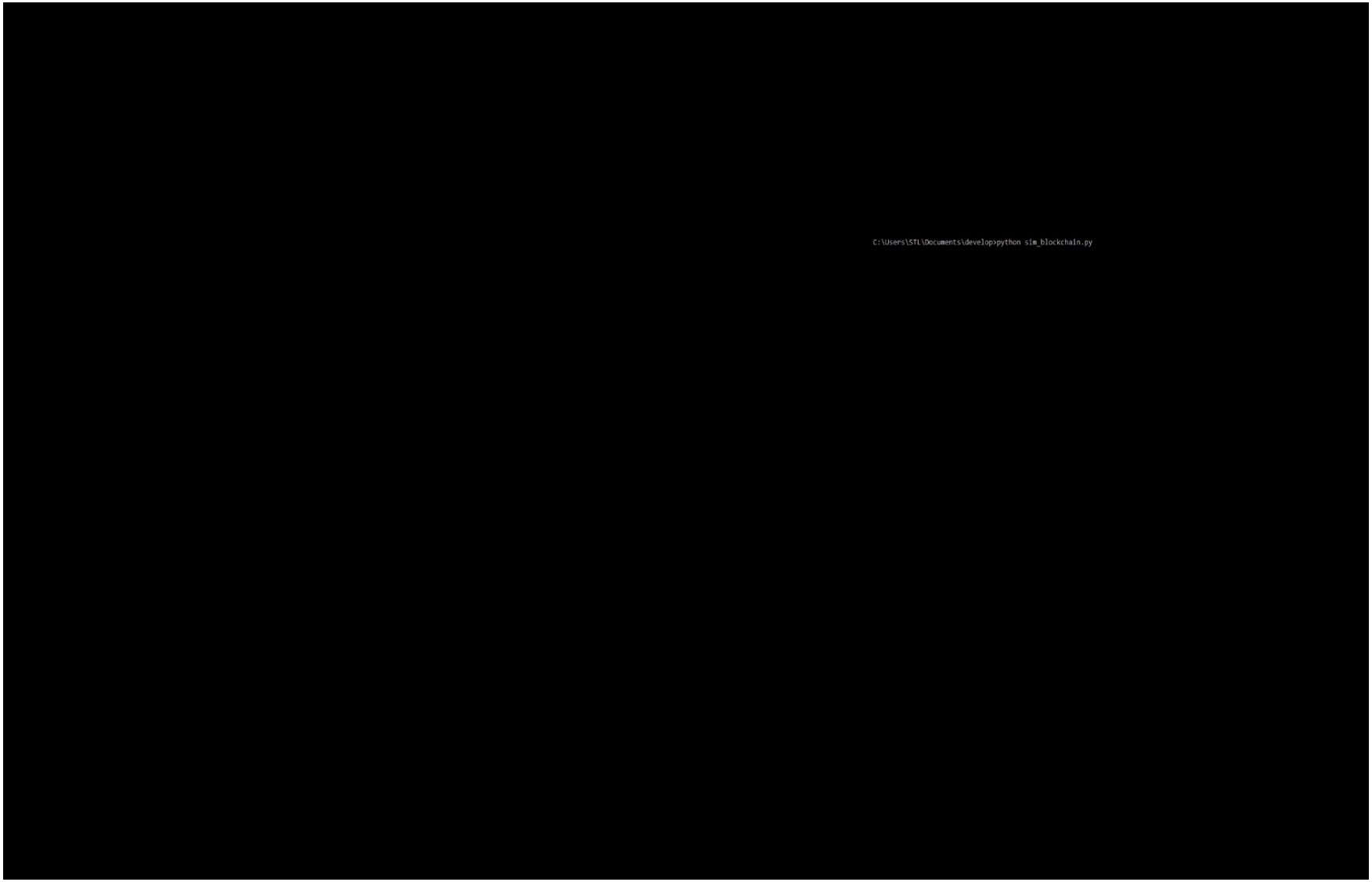
Single-branched LDB



Multi-branch LDB



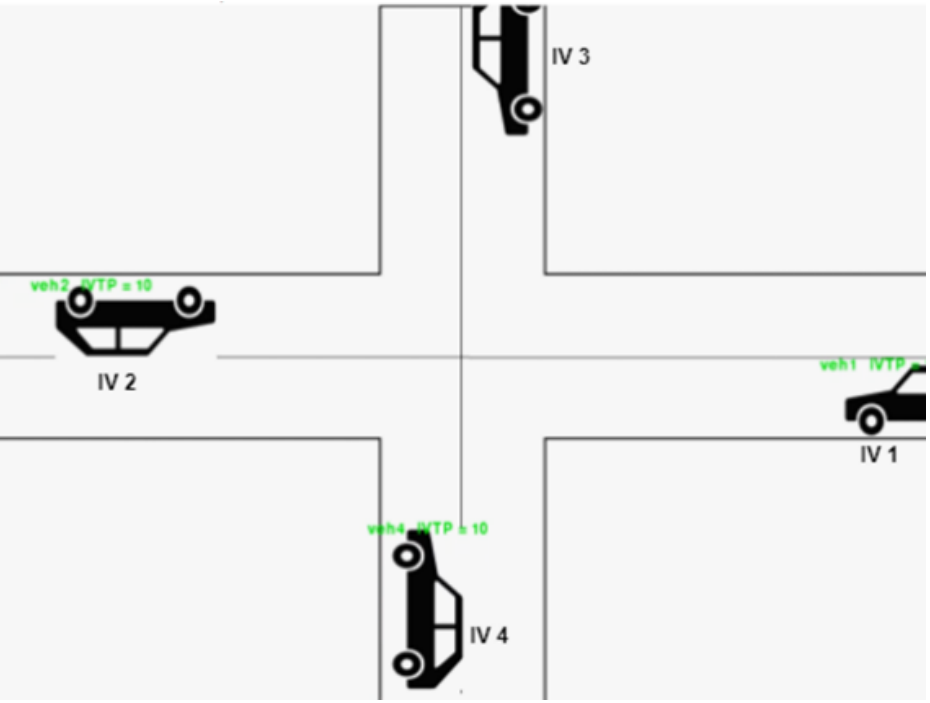
Use Case Scenario Analysis



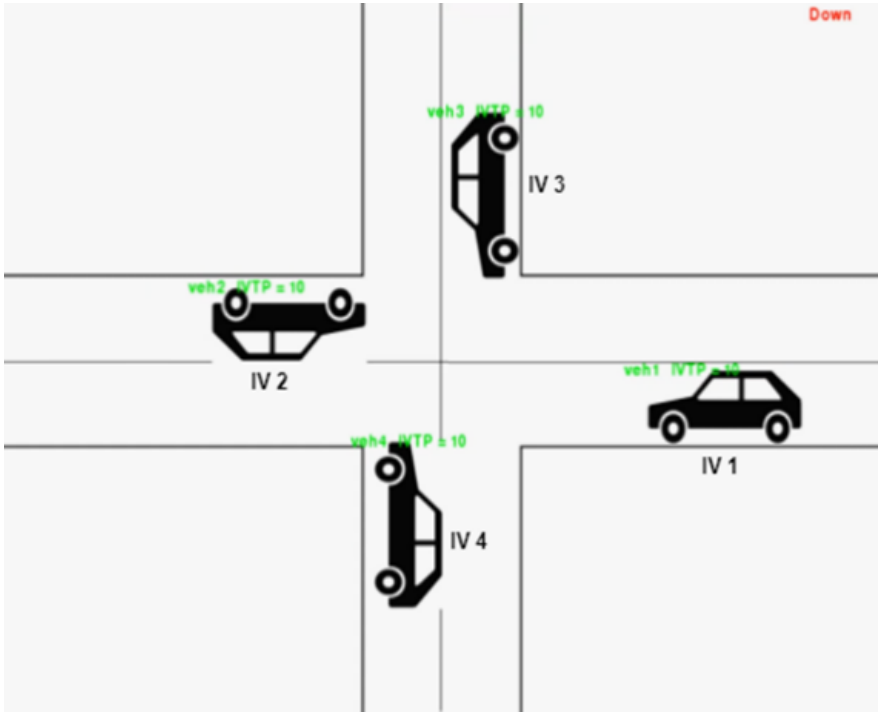
Simulation works done by our two interns from IIIT-Allahabad—Mr. Kaustubh Shamshery and Mr. Sulyab Thottungal Valapu

Use Case Scenario Analysis

Use Case Test Phase One



Use Case Test Phase Two



Level 3(000)	1.03083

Use Case Scenario Analysis

Use Case Test Phase Three

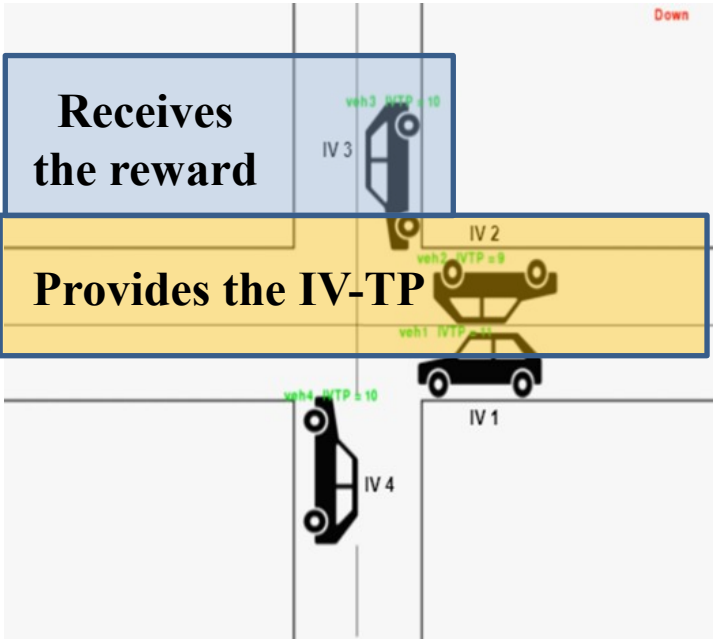
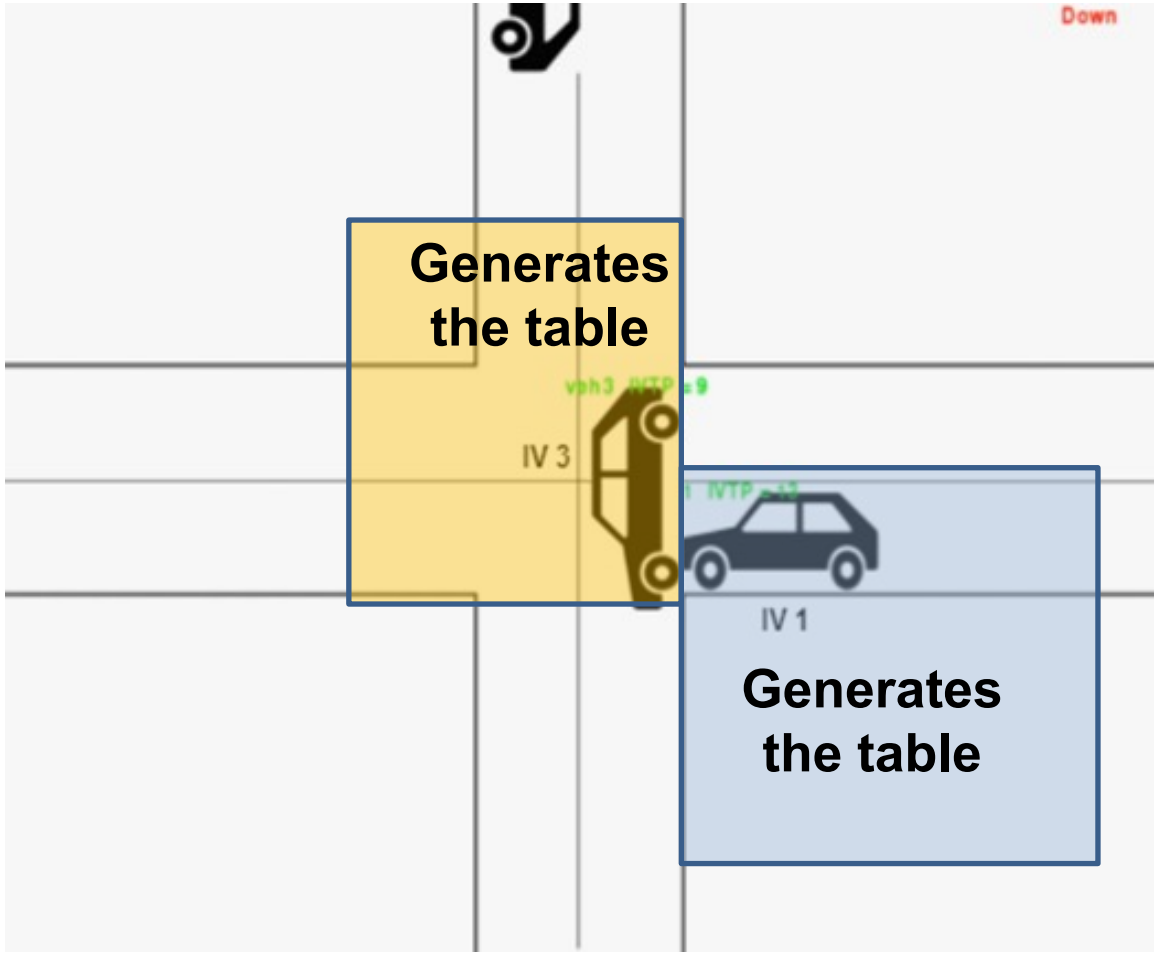


Table of Vehicles Timestamps

Arrival Time of IVs	Processing Time	IVTP of IV 1	IVTP of IV 2	IVTP of IV 3	IVTP of IV 4	Remarks
IV-1→ 10:06	00:00:00	10	10	10	10	No vehicle issued start block
	00:00:05	10	10	10	10	IV 2 sends the start block, starts moving
IV-2 → 10:02	00:00:06	10	10	10	10	IV 3 and IV 4 send start block, start moving
	00:00:07	10	10	10	10	IV 1 sends start block, starts moving
IV-3→ 10:04	00:00:10	11	9	10	10	IV 2 reaches intersection and IV 1 mines the block, IV 2 crosses the intersection after consensus
	00:00:12	12	9	10	9	IV 4 reaches intersection, issues the intersection block and IV 1 mines it but cannot move since IV 2 is crossing
IV-4 →10:03	00:00:15	12	9	10	9	IV 4 which came second is now able to cross
	00:00:20	13	9	9	9	IV 3 which came in third, is now able to move, IV 1 mined this block again
	00:00:28	13	9	9	9	IV 1 which came in last, is now able to cross

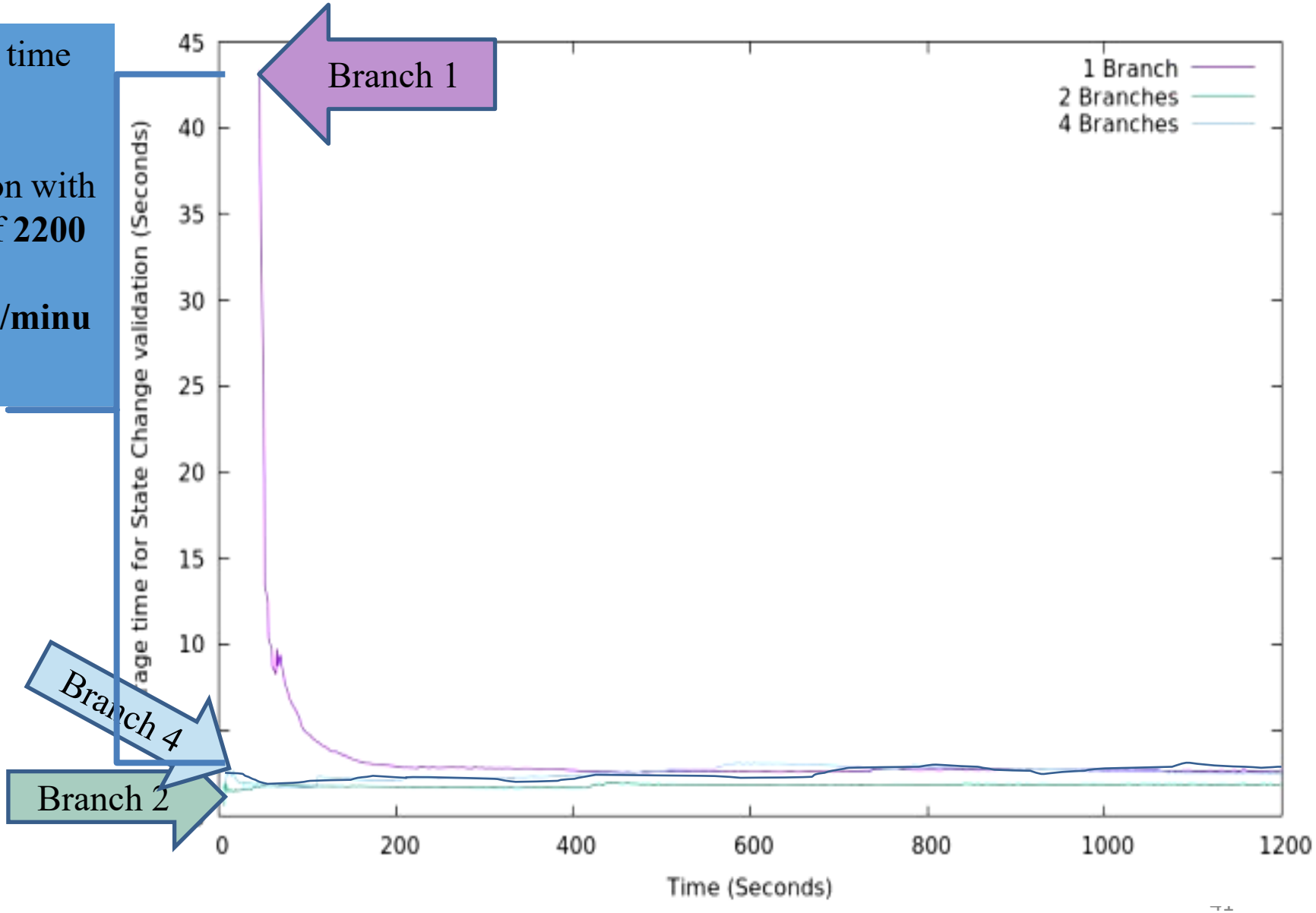
Use Case Scenario Analysis

Use Case Test Phase Four



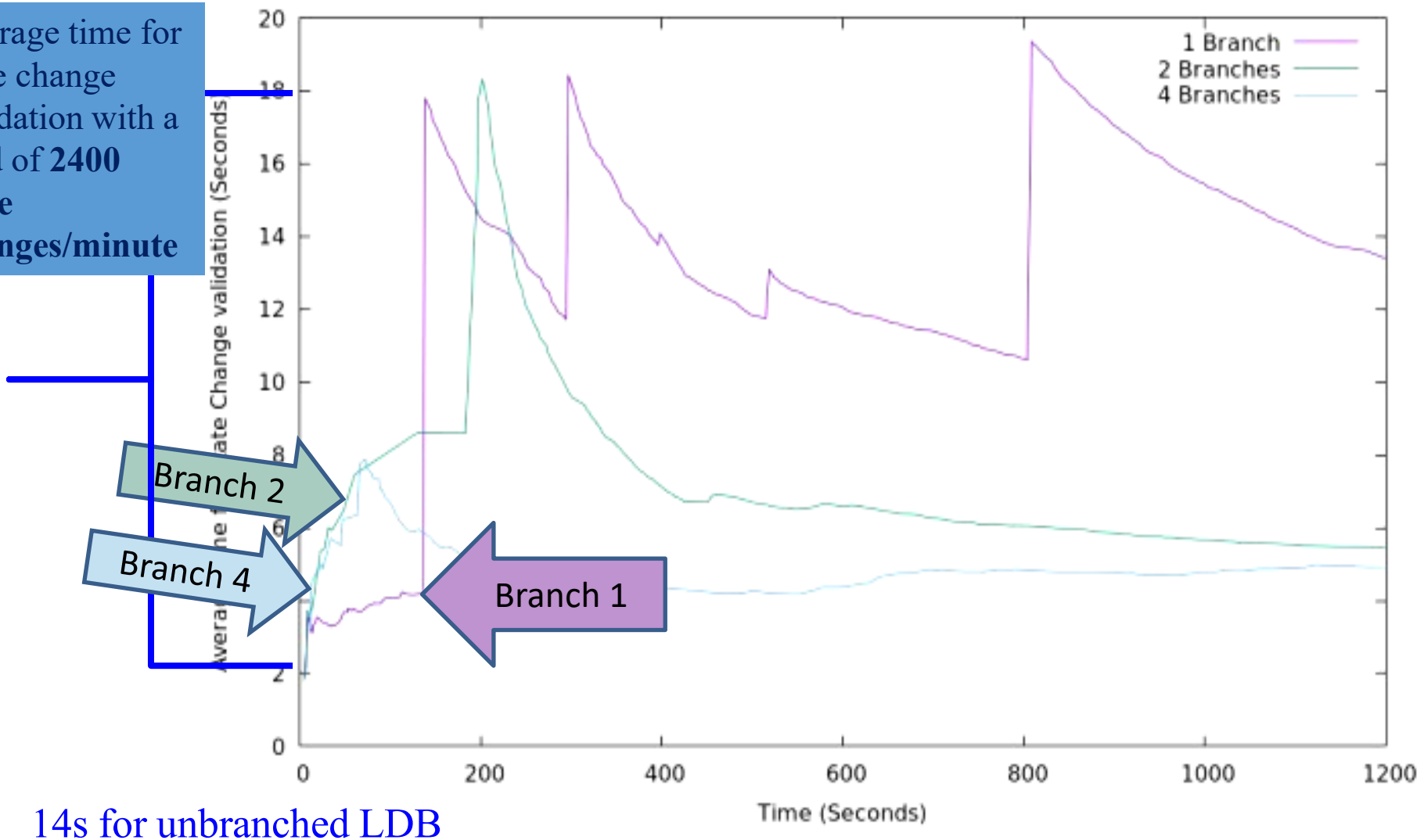
Simulation Analysis of Applied Blockchain Technology Solutions

Average time for state change validation with a load of **2200 state changes/minute**



Simulation Analysis of Applied Blockchain Technology Solutions

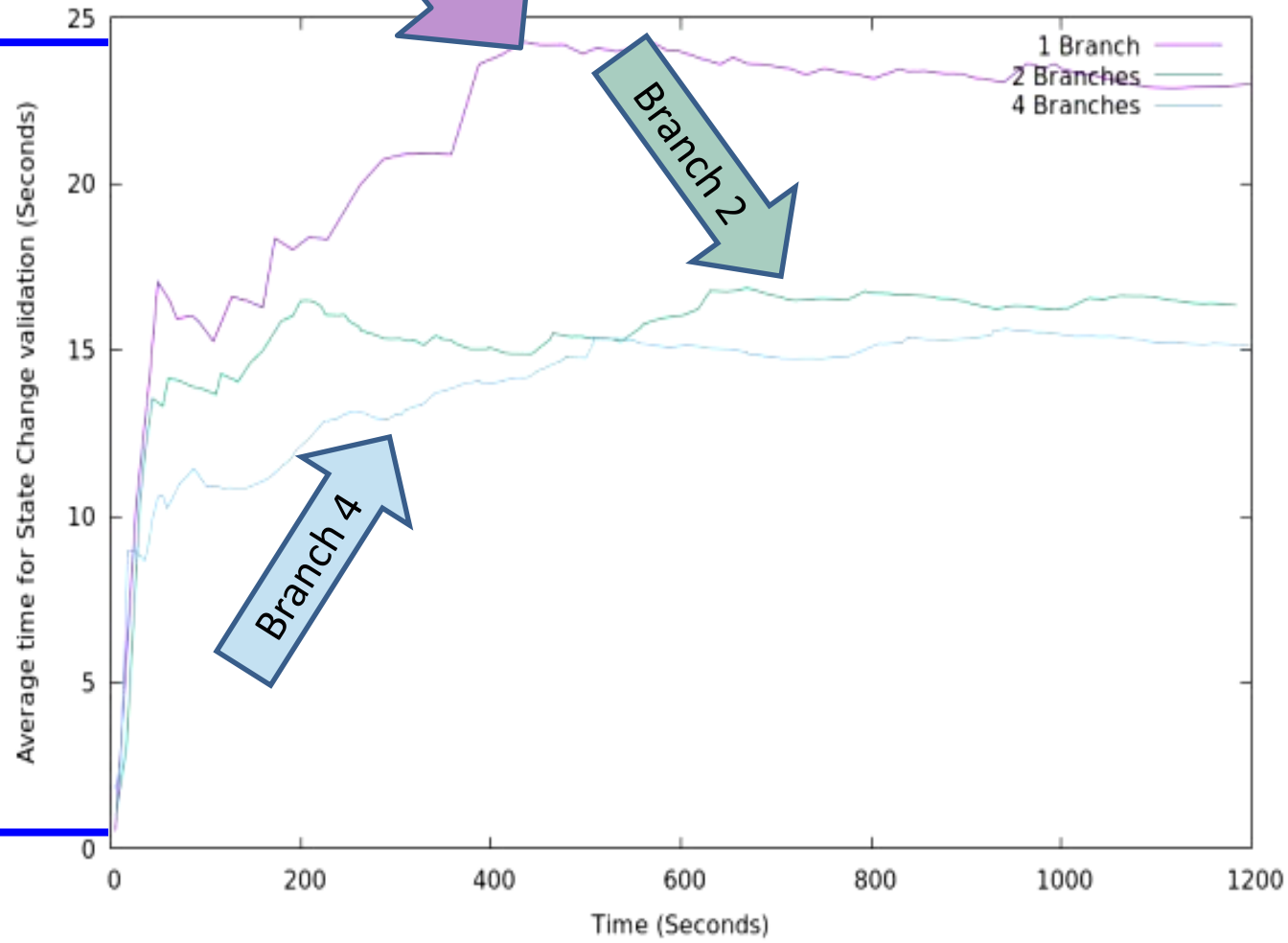
Average time for state change validation with a load of **2400 state changes/minute**



- 14s for unbranched LDB
- 6.5s for LDB with one branch
- 5.5s for LDB with 4 branches

Why Are These Rewards Important?

Average time for state change validation with a load of **3200 state changes/minute**



- 16 seconds for LDB with one branch
- 14 seconds for LDB with 4 branches

Summary

Impact of Blockchain Technology in Autonomous Vehicle

- Able to handle large amounts of data at the same time
- Access to vehicle history
  - Seamless Transportation Network
- Decentralized, Distributed secure trusted peer to peer network
- Future Work:
  - Blockchain in Emergency Vehicle scenario
  - Blockchain Computation Reduction
  - Consensus Protocol
  - Lot of research scope

References

- *Madhusudan Singh*, Hasan Tinmaz, (2021) "***Blockchain Technology in Vehicular Communication Networks***", In: Information Security of Intelligent Vehicles Communication. Studies in Computational Intelligence, vol 978. Springer, Singapore. https://doi.org/10.1007/978-981-16-2217-5_14
- *Madhusudan Singh (2020), "**Tri-Blockchain Based Intelligent Vehicular Networks**," IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workshops (INFOCOM)*, Toronto, ON, Canada, 2020, pp. 860-864, doi: 10.1109/INFOCOMWKSHPS50562.2020.9162692. **[Citation: 3]**
- Shiho Kim, *Madhusudan Singh (2019)*, "***비중앙집중형 자동차 보안 신뢰 네트워크 장치 및 방법*** [APPARATUS AND METHOD FOR DECENTRALIZED SECURE]", Patent No: 1020190010195, 2019.01.30, ***Granted*, Korea Patent. http://engportal.kipris.or.kr/engportal/search/total_search.do**
- *Madhusudan Singh*, Shiho Kim (2018), "***Branch Based Blockchain Technology in Intelligent Vehicle***", Computer Networks, 2018, ISSN -1389-1286, *https://doi.org/10.1016/j.comnet.2018.08.016* **[Citation: 163]**
- *Madhusudan Singh*, Shiho Kim (2018), "***Trust Bit: Reward-based Intelligent Vehicles Communication using Blockchain***", The 4th IEEE World Forum on the Intelligent of Things (WF-IoT), Singapore, Feb. 05-08, 2018, 10.1109/WF-IoT.2018.8355227 . **[Citation: 53]**
- *Madhusudan Singh*, Shiho Kim (2018), "***Crypto Trust Point (cTp) for Secure Data Sharing among Intelligent Vehicles***", The 2018 International Conference on Electronics, Information and communication (ICEIC 2018), Sheraton Waikiki Hotel, Honolulu, Hawaii, USA, Jan. 24-27, 2018, 10.23919/ELINFOCOM.2018.8330663 **[Citation: 30]**
- *Madhusudan Singh*, Shiho Kim (2017), "***Blockchain-based Intelligent Vehicle Data Sharing Framework***", arXiv preprint, arXiv: 1708.09721, 01 Sept. 2017. **[Citation: 117]**
- *Madhusudan Singh*, Shiho Kim (2017), "***Introduce Reward-based Intelligent Vehicle Communication Using Blockchain Technology***",14th International SoC Design Conference (ISOCC 2017), Grand Hilton Hotel, Seoul, South Korea, Nov. 5-8, 2017, 10.1109/ISOCC.2017.8368806. **[Citation: 75]**
- *Madhusudan Singh*, Shiho Kim (2017), "***Blockchain Technology for Intelligent Vehicles***", IEEE Secure Development Conference (IEEE SecDev 2017), The Hyatt Regency, Cambridge, MA, USA, Sept. 24-26, 2017. **[Organized by Lincoln Research Lab, MIT, USA]**

IEEE Online Lectures

IEEE Online Lecture, “Automotive Cyber security”

1. **Evolution of Intelligent and Autonomous Vehicles:**

   https://ieeexplore.ieee.org/courses/details/EDP585

2. **Connected Vehicle Communication :**

   https://ieeexplore.ieee.org/courses/details/EDP586

3. **Securing Intelligent Transportation Systems:**

   https://ieeexplore.ieee.org/courses/details/EDP587

4. **Using Blockchain Technology to Secure Autonomous Vehicles:**

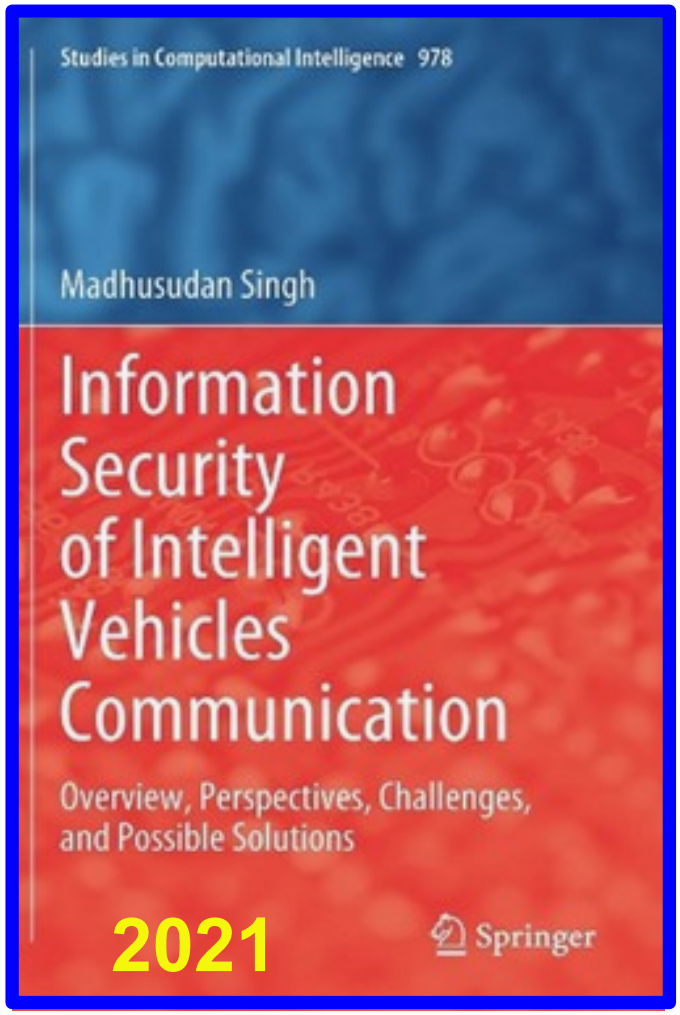
   https://ieeexplore.ieee.org/courses/details/EDP588

5. **Collecting, Analyzing, and Interpreting Vehicular Data:**

   https://ieeexplore.ieee.org/courses/details/EDP589

Books:

https://doi.org/10.1007/978-981-16-2217-5



Editor in Chief of Blockchain Technologies Book Series, Springer Nature

https://www.springer.com/series/16276

감사합니다

THANK YOU