A system to ensure robust, honest reporting of sensor data

Md. Adib Muhtasim
Department of Computer Science
mdadib.muhtasim1@ucalgary.ca

UNIVERSITY OF CALGARY

Introduction

- Sophisticated and autonomous devices becoming indispensable part of our lives
- Integrity of their reported data

2

Data Tampering

Security issues with devices and sensors

Manipulation or falsification of system or sensor data

Privacy of the data owner

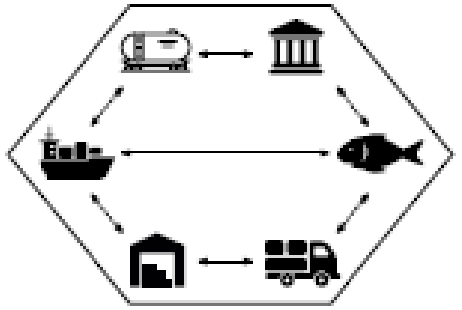
Problem

- Lack of proper monitoring and auditing system
- Lack of ESOs (Environmental Situation Oracles)
  - ESOs are assumed to be honest and truthful source of sensor data

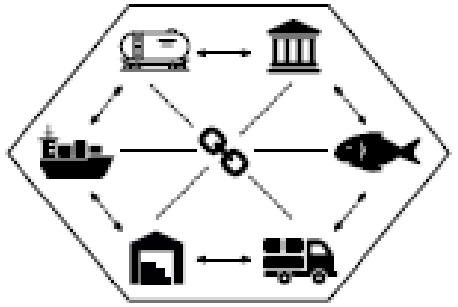
5

Some examples of data manipulation

Blockchain powered Supply Chain Management

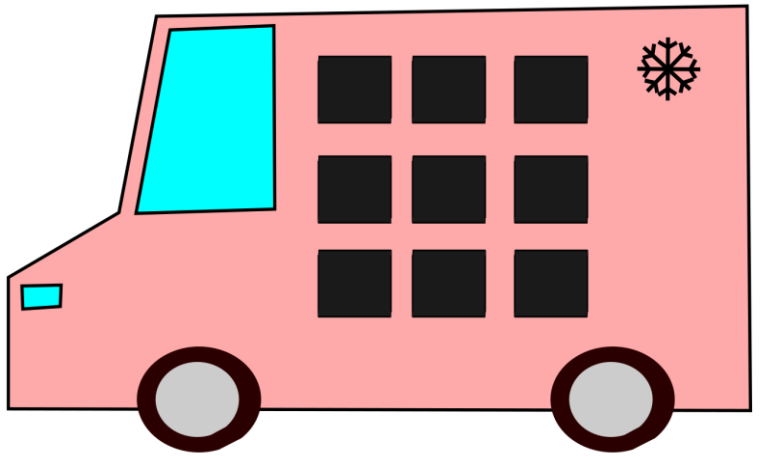


Traditional SCM

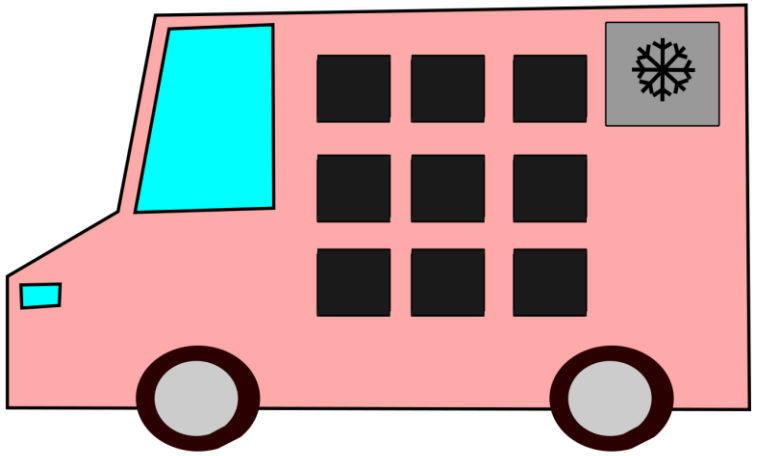


Blockchain powered SCM

Blockchain powered Supply Chain Management



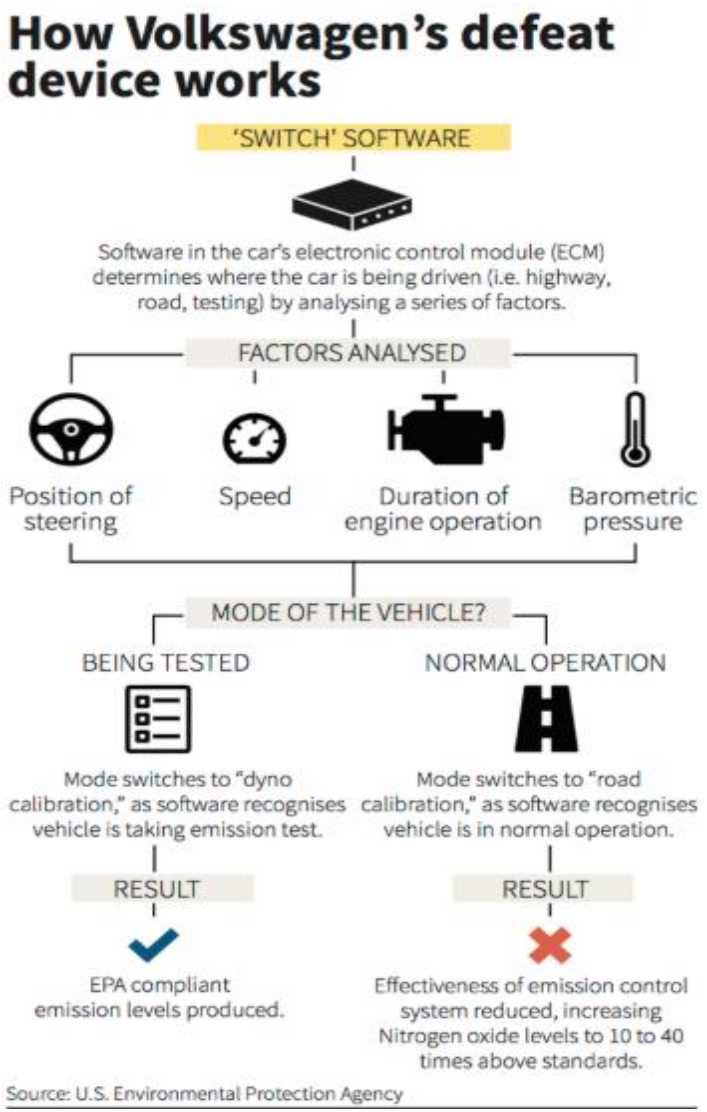
Intended scenario



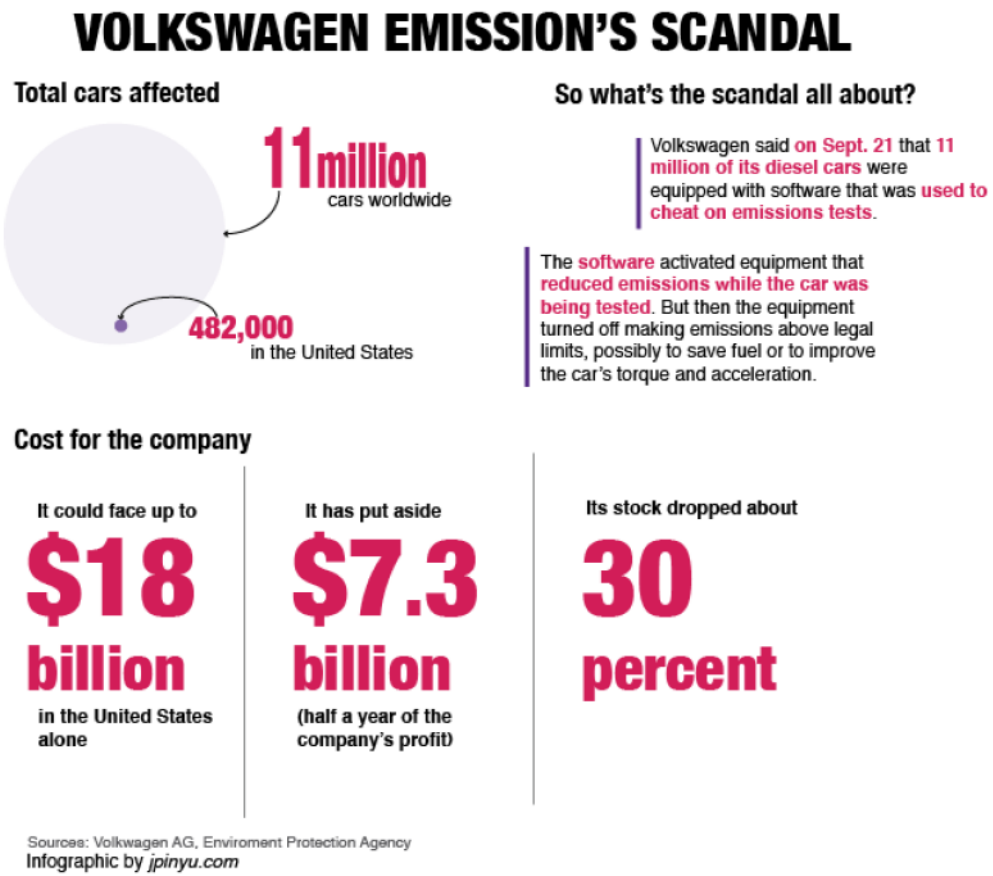
Attack scenario

Volkswagen emissions scandal

Volkswagen emissions scandal



Volkswagen emissions scandal

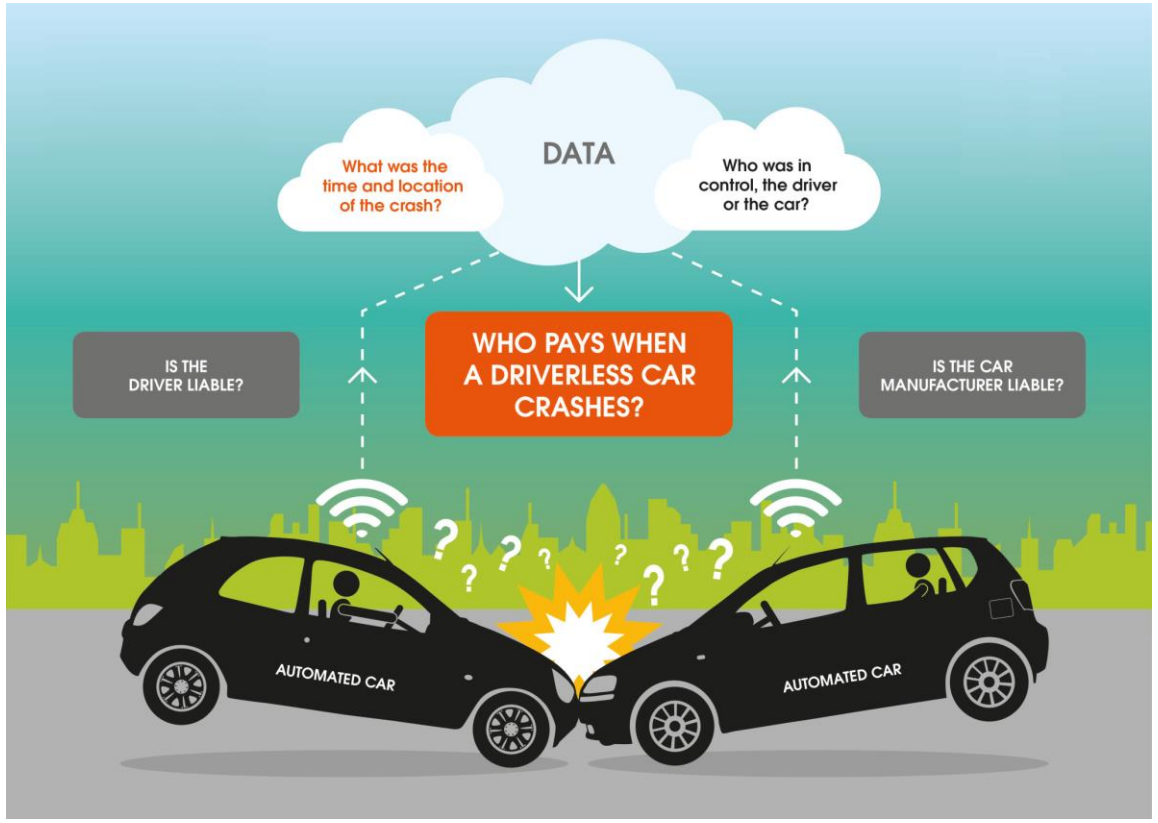


Autonomous car crashes

Uber’s self-driving car crash

Tesla’s model X car crash

Who is to blame?



Goals

Our goal is to prevent

- Prevent a system or a sensor from performing unethical behaviours
- Retain the privacy

Goals

Our goal is to prevent

- Prevent a system or a sensor from performing unethical behaviours
- Retain the privacy

Proposed System

- Ensure robust, honest reporting of sensor data

Autonomous Vehicles

Feasibility and Efficiency

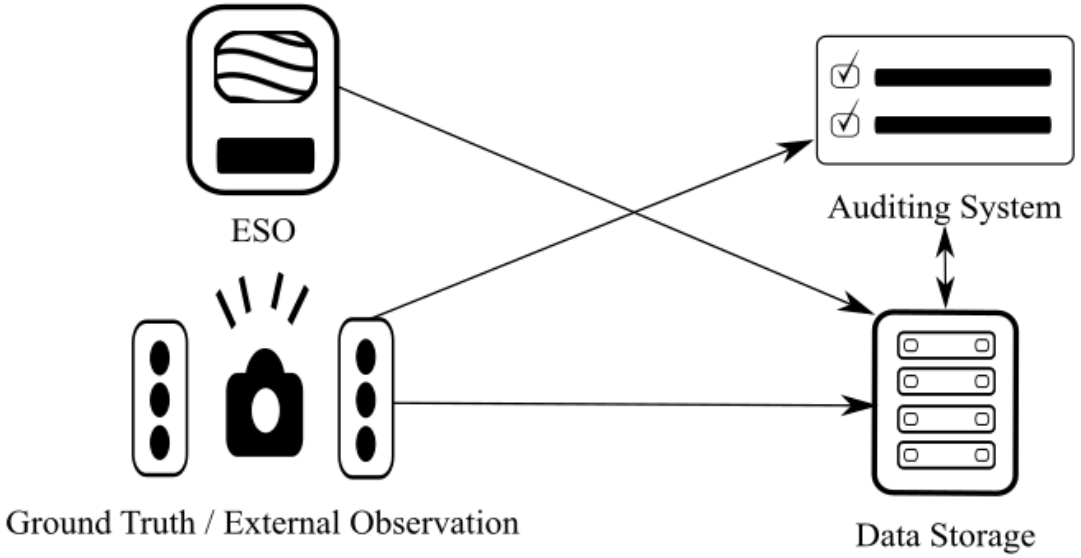
Measure

- Amount of time it takes to catch a *cheater*

Predict

- Amount of network traffic it has to handle in a real-world implementation

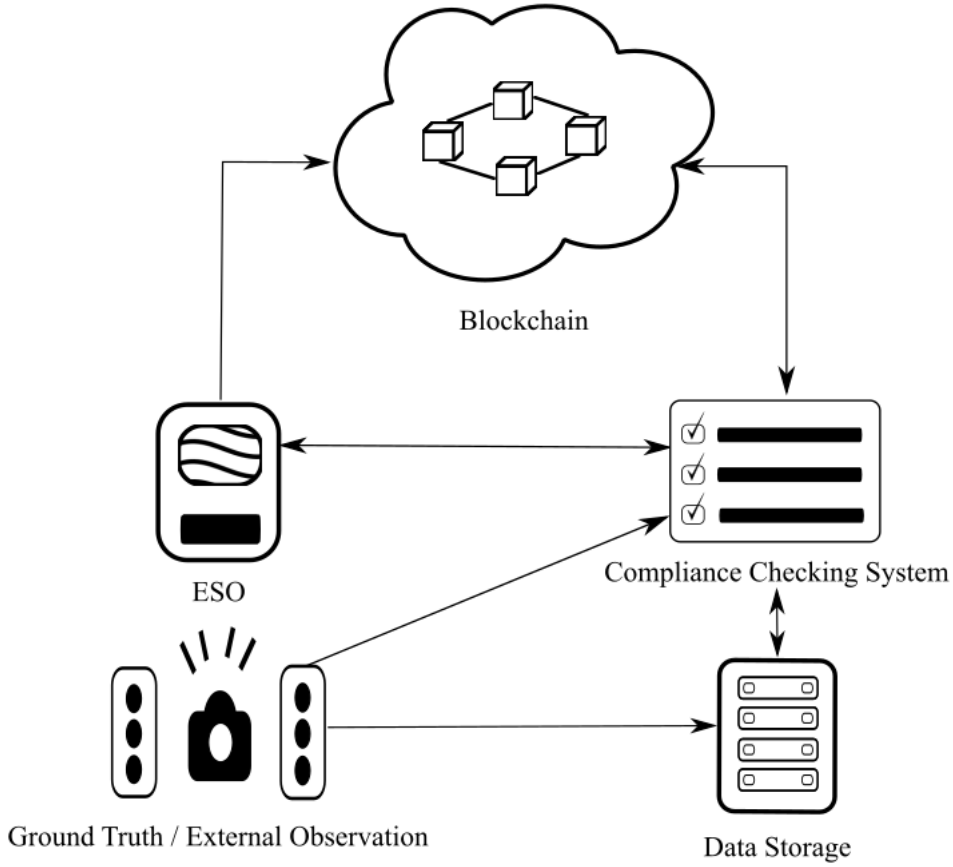
A typical solution



How can we prevent a system from

manipulating its data and retain its privacy at the same time?

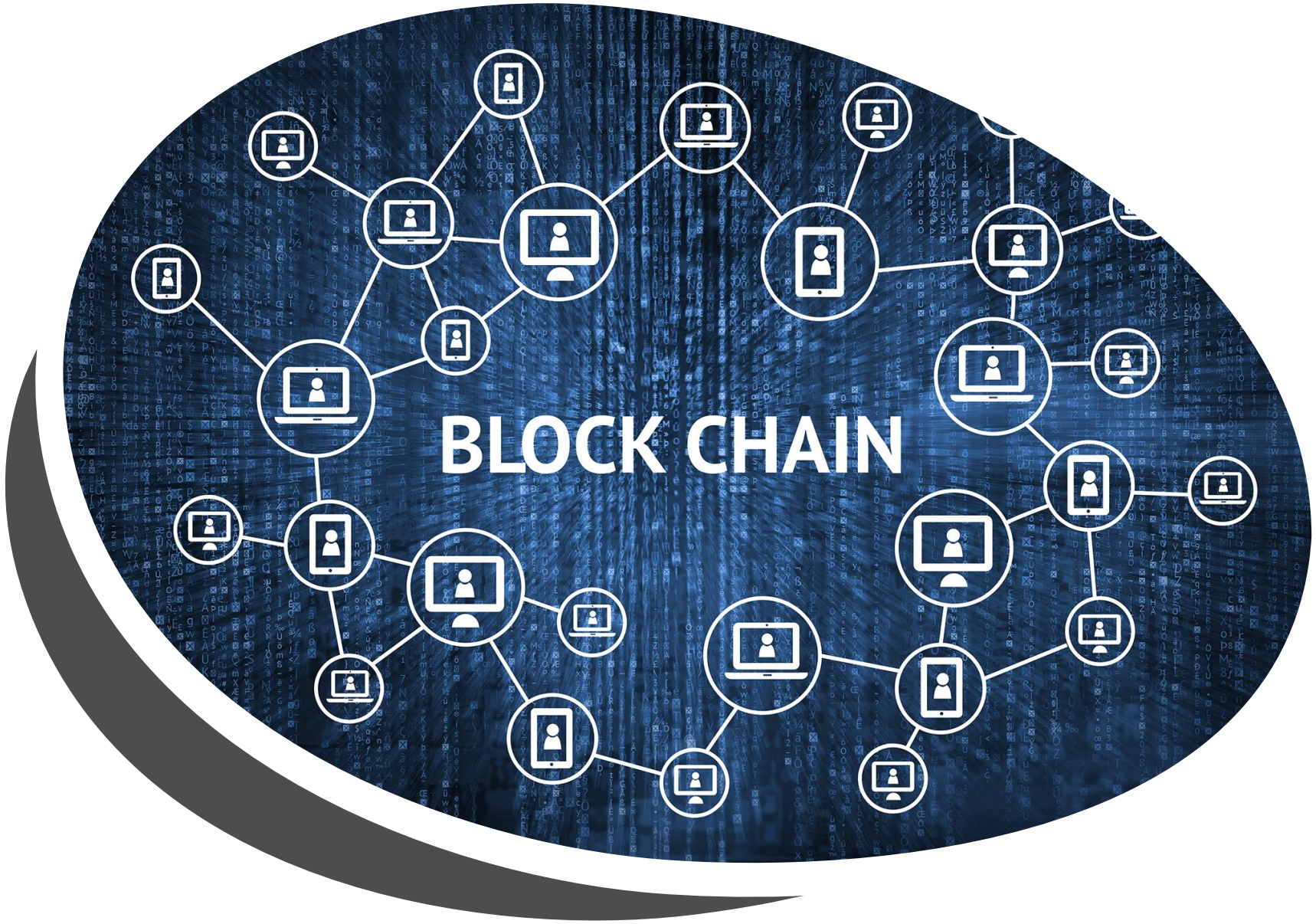
High level view of our system



Black Box or Event Data Recorder

	vehicle_id	Location - x	Location - y	Location - z	Speed	Time	Salt	Seat Belt	Brake	Gear	Steer	Throttle	RPM
1	120	240.82	53.59	-0.02	0.44	11:58:43	0a4902fe....	ON	0.0	0	-0.0	0.7	3878
2	120	240.82	53.58	0.01	0.0	11:58:44	59512fe3....	OFF	0.0	0	-1e-06	0.7	4069
3	120	240.85	52.31	0.01	14.99	11:58:45	cd25734d....	ON	0.0	1	-5e-06	0.7	4729
4	120	240.98	47.12	0.01	21.55	11:58:46	469e6be2....	OFF	0.0	1	-7e-05	0.590837	1623
5	120	241.14	40.89	0.01	23.22	11:58:47	39f1585f....	ON	0.0	2	-0.000222	0.401105	2116
6	120	241.29	34.93	0.01	22.5	11:58:48	61ea38e0....	OFF	0.0	2	-0.000417	0.447416	1872
7	120	241.45	28.37	0.01	23.2	11:58:49	45840d23....	ON	0.0	3	-0.000263	0.370856	1207
8	120	241.6	22.1	0.01	22.86	11:58:50	a2c65760....	OFF	0.0	3	-0.000164	0.371081	1672
9	120	241.75	15.6	0.01	22.68	11:58:51	1634447e....	ON	0.0	3	-5.6e-05	0.37459	1474
10	120	241.9	9.33	0.01	22.49	11:58:52	6d07f7eb....	OFF	0.0	3	-1.2e-05	0.368118	3378
11	120	242.04	3.19	0.01	22.3	11:58:53	d75b75c2....	OFF	0.0	3	5e-06	0.371429	3278
12	120	242.18	-2.95	0.01	22.19	11:58:54	f5b94c4e....	OFF	0.0	3	6.9e-05	0.366604	1360
13	120	242.33	-9.23	0.01	22.05	11:58:55	6ccd57a8....	ON	0.0	3	0.000142	0.365385	2289
14	120	242.48	-15.4	0.01	21.93	11:58:56	1a9df82a....	ON	0.0	3	0.000183	0.367335	2405
15	120	242.63	-21.59	0.01	21.83	11:58:57	726abb87....	ON	0.0	3	0.000149	0.364966	4322
16	120	242.77	-27.36	0.01	21.73	11:58:58	ad548c36....	ON	0.0	3	8.6e-05	0.369287	3054
17	120	242.93	-33.6	0.01	21.65	11:58:59	b64d0fdc....	OFF	0.0	3	2.3e-05	0.364132	3507
18	120	243.08	-39.63	0.01	21.58	11:59:00	1ca84f67....	ON	0.0	3	-1e-06	0.364037	2216
19	120	243.23	-45.49	0.01	21.45	11:59:01	e98398b2....	OFF	0.0	3	-8e-06	0.367964	4150
20	120	243.38	-51.48	0.01	21.46	11:59:02	cda24859....	ON	0.0	3	-7.8e-05	0.363167	3419
21	120	243.53	-57.41	0.01	21.4	11:59:03	dfa231de....	OFF	0.0	3	-0.000125	0.357872	3870
22	120	243.68	-63.51	0.01	21.4	11:59:04	e8b4e601....	ON	0.0	3	-0.000173	0.358241	3184
23	120	243.82	-69.22	0.01	21.25	11:59:05	6c79213f....	OFF	0.0	3	-0.000118	0.371811	1652
24	120	243.97	-75.4	0.01	21.26	11:59:06	cce50b25....	OFF	0.0	3	-0.000133	0.376727	2791
25	120	244.11	-81.24	0.01	21.23	11:59:07	a01a22de....	ON	0.0	3	-7.8e-05	0.371786	4080
26	120	244.25	-87.2	0.01	21.16	11:59:08	1ef5a133....	OFF	0.0	3	-2.7e-05	0.36628	4744
27	120	244.39	-93.09	0.01	21.24	11:59:09	a5fc5b08....	OFF	0.0	3	-6e-06	0.36605	1349
28	120	244.52	-98.84	0.01	21.24	11:59:10	6eebd9cd....	OFF	0.0	3	0.0	0.361748	4633
29	120	244.66	-104.68	0.01	21.16	11:59:11	fa068a34....	OFF	0.0	3	4.2e-05	0.362767	1148
30	120	244.81	-110.86	0.01	21.02	11:59:12	522a11c6....	OFF	0.0	3	4e-05	0.37325	2532

Car data


BLOCK CHAIN

Notable properties of blockchain technology

- Decentralization
- High availability
- Tamper resistant

Hashing

Input	Hash
Calgary	4dcbd74fcbd08192a287425acff97cfc3c8cf3dd46486d07669b2380d927cdcf
Autonomous Vehicle	5afd05e393e8e5d65b382c1b63a24a347eb7b6ba7e92a1703c311fbf04f59e10
Compliance Checker	ebca86cbf85493b2159e2f34a2ef33a51774be9600612aa0138c7aec3d6b3dd6

Hashing using SHA-256

Input	Hash
Calgary	4dcbd74fcbd08192a287425acff97cfc3c8cf3dd46486d07669b2380d927cdcf
calgary	e00b3c76911327ca972f10e1a457772e345be7dd0b9ed6cb0c6643023176409c

Avalanche effect

Types of blockchains

Public blockchain

Private blockchain

Hybrid blockchain

Salting

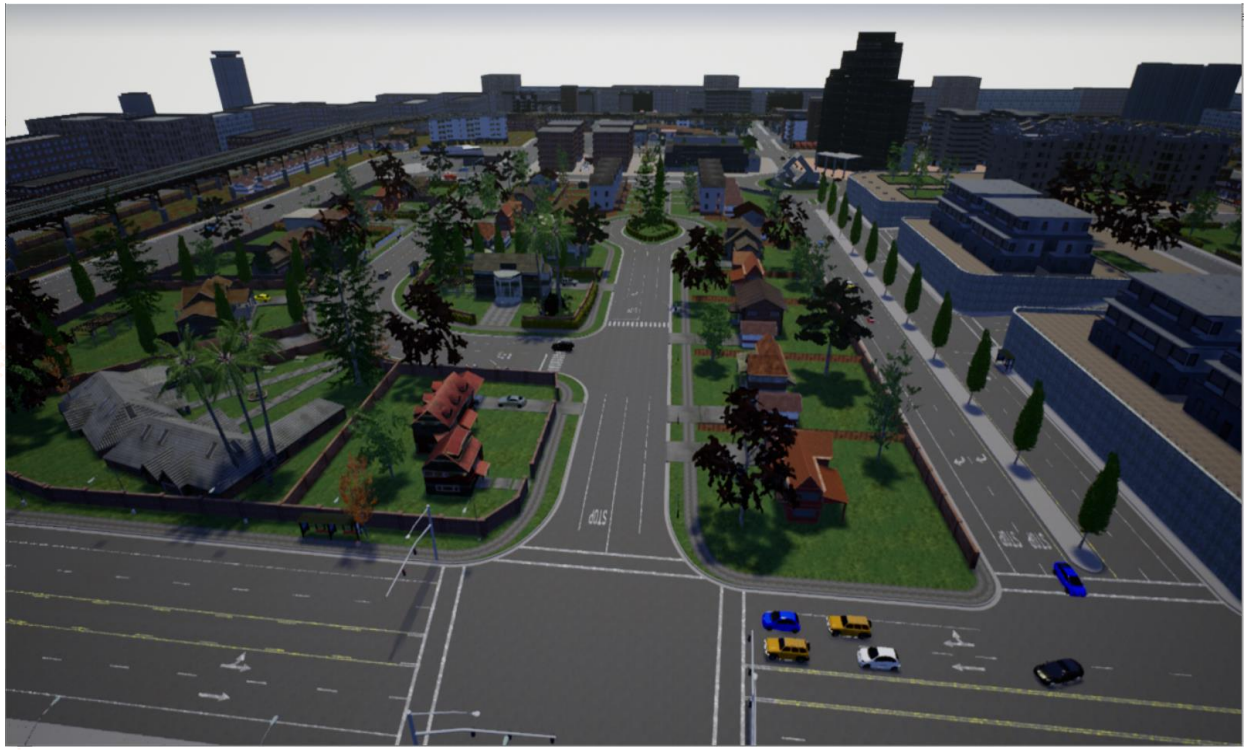
Die Roll (Plain-text)	Hash
1	6b86b273ff34fce19d6b804eff5a3f5747ada4eaa22f1d49c01e52ddb7875b4b
2	d4735e3a265e16eee03f59718b9b5d03019c07d8b6c51f90da3a666eec13ab35
3	4e07408562bedb8b60ce05c1decfe3ad16b72230967de01f640b7e4729b49fce
4	4b227777d4dd1fc61c6f884f48641d02b4d121d3fd328cb08b5531fcacdabf8a
5	ef2d127de37b942baad06145e54b0c619a1f22327b2ebbcfbec78f5564afe39d
6	e7f6c011776e8db7cd330b54174fd76f7d0216b612387a5ffcfb81e6f0919683

Salting

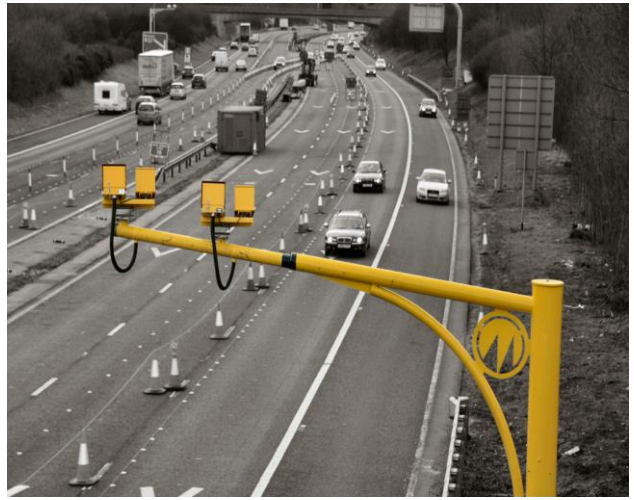
Die Roll (Plain-text) + Random Salt	Hash
1 + 7902699be42c8a8e46fbbb4501726517e86b22c56a189f7625a6da49081b2451	60222d661a930f6e234eb8d150bb94b4c83ced7259d99ee05f711045815fd19e
2 + 2c624232cdd221771294dfbb310aca000a0df6ac8b66b696d90ef06fdefb64a3	bab1572cf479a6619df2da843751630077bcceb65fa4618a17810895b6ba22f9
3 + 19581e27de7ced00ff1ce50b2047e7a567c76b1cbaebabe5ef03f7c3017bb5b7	6a62d83b295cdea7c3c82961485836dded55a885617412eb0727fc26459b75b6
4 + 4a44dc15364204a80fe80e9039455cc1608281820fe2b24f1e5233ade6af1dd5	c09ce97f618ec8bacd33ee70ca65a42b249e1689c0cc0de8f93a8c59cd7b57d2
5 + 4fc82b26aecb47d2868c4efbe3581732a3e7cbcc6c2efb32062c08170a05eeb8	0f69bc351f4259ba53966907ec867b58af4f0da818ff7c2d4aa8609b81b57cc9
6 + 6b51d431df5d7f141cbececcf79edf3dd861c3b4069f0b11661a3eefacbba918	6ef9c9f8d21df962a9bfac2c8985ad43d0f95d67cfcd1db6e70a74a52efdaa44

CARLA

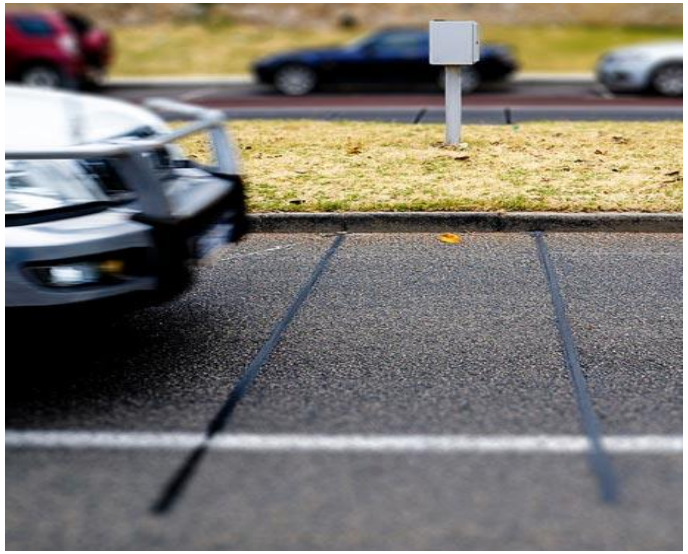
an open urban driving simulator



Traffic cameras



Embedded road sensors

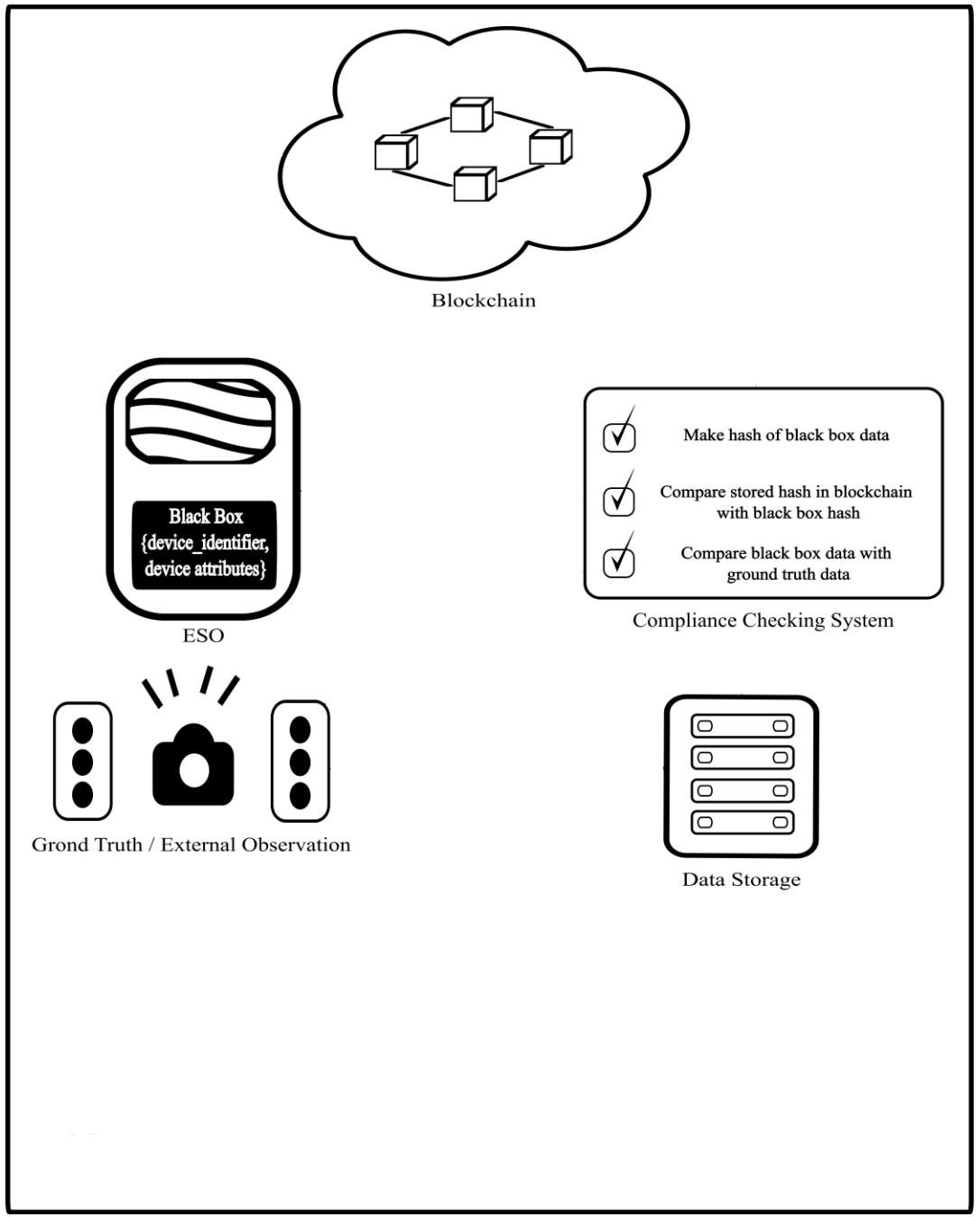


Piezoelectric sensor

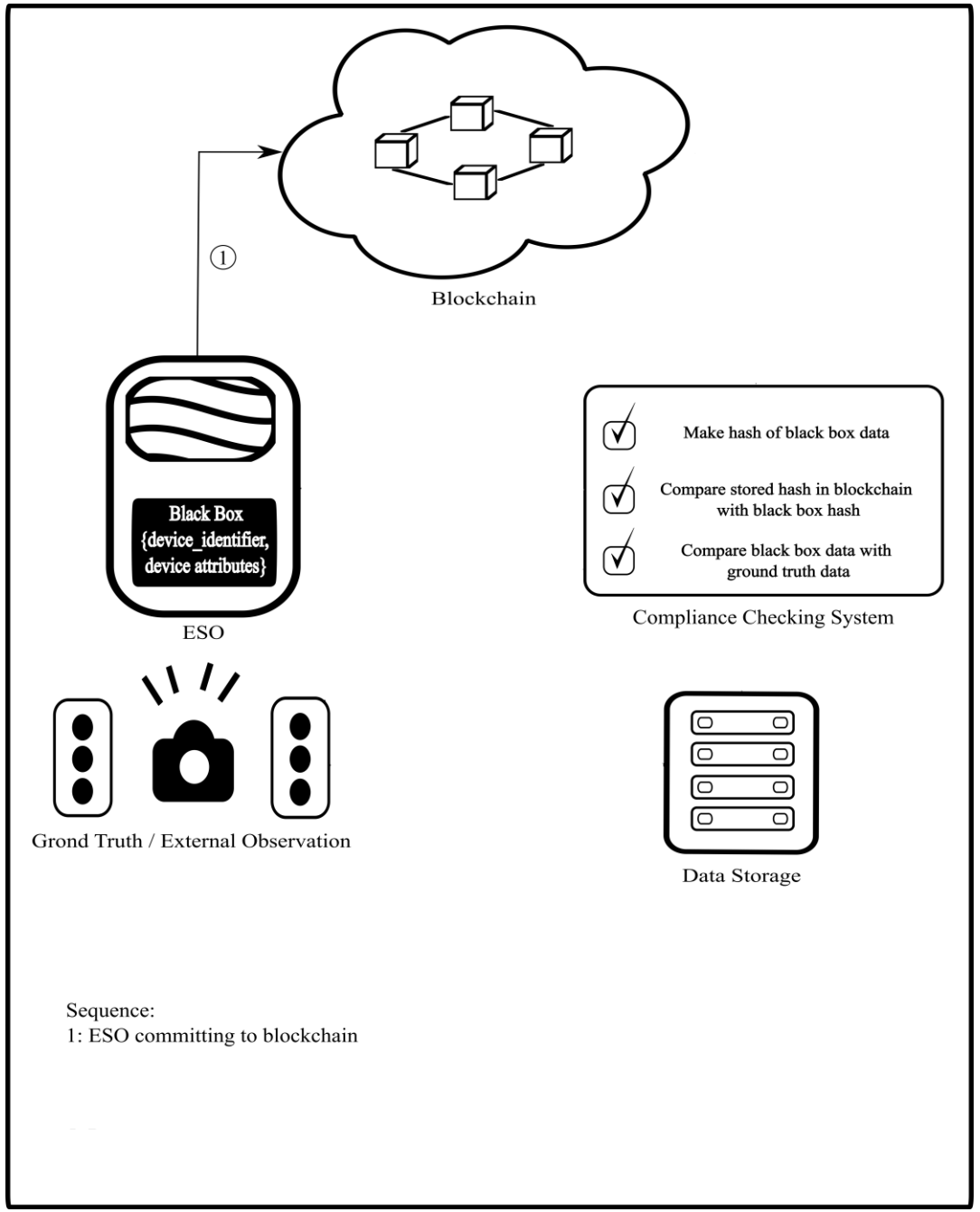
Inductive loop

Pneumatic road tube

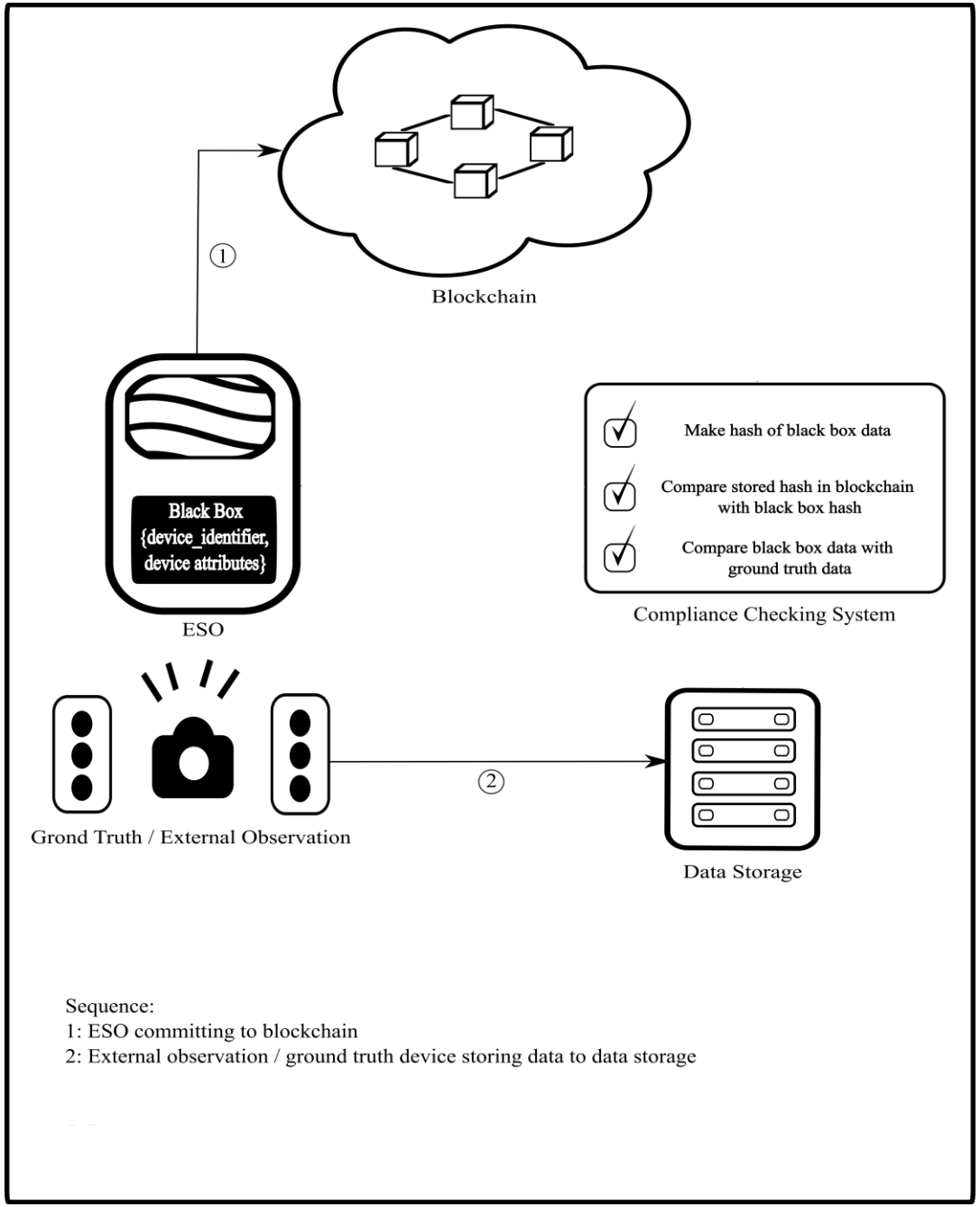
System Design



System Design

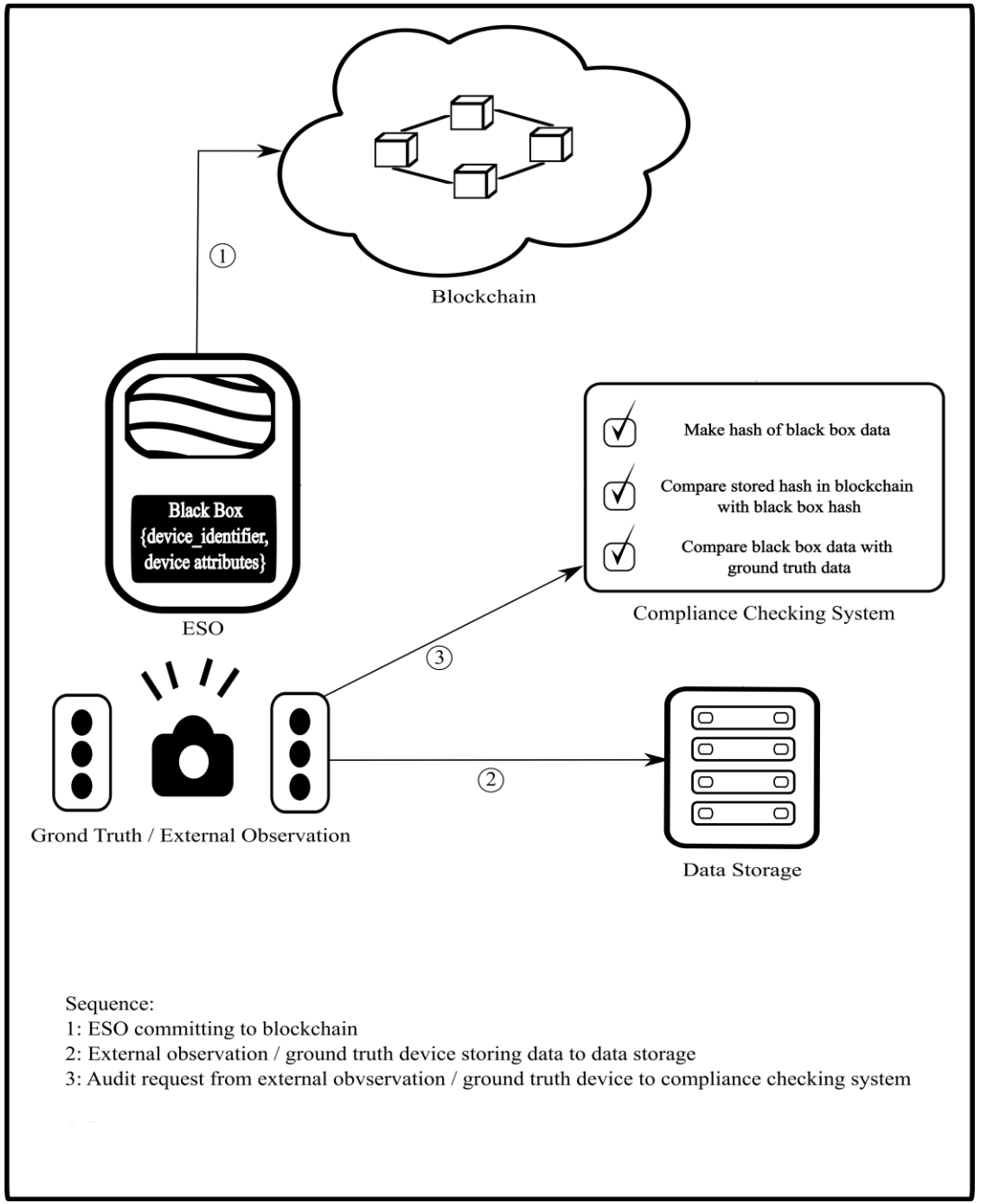


System Design



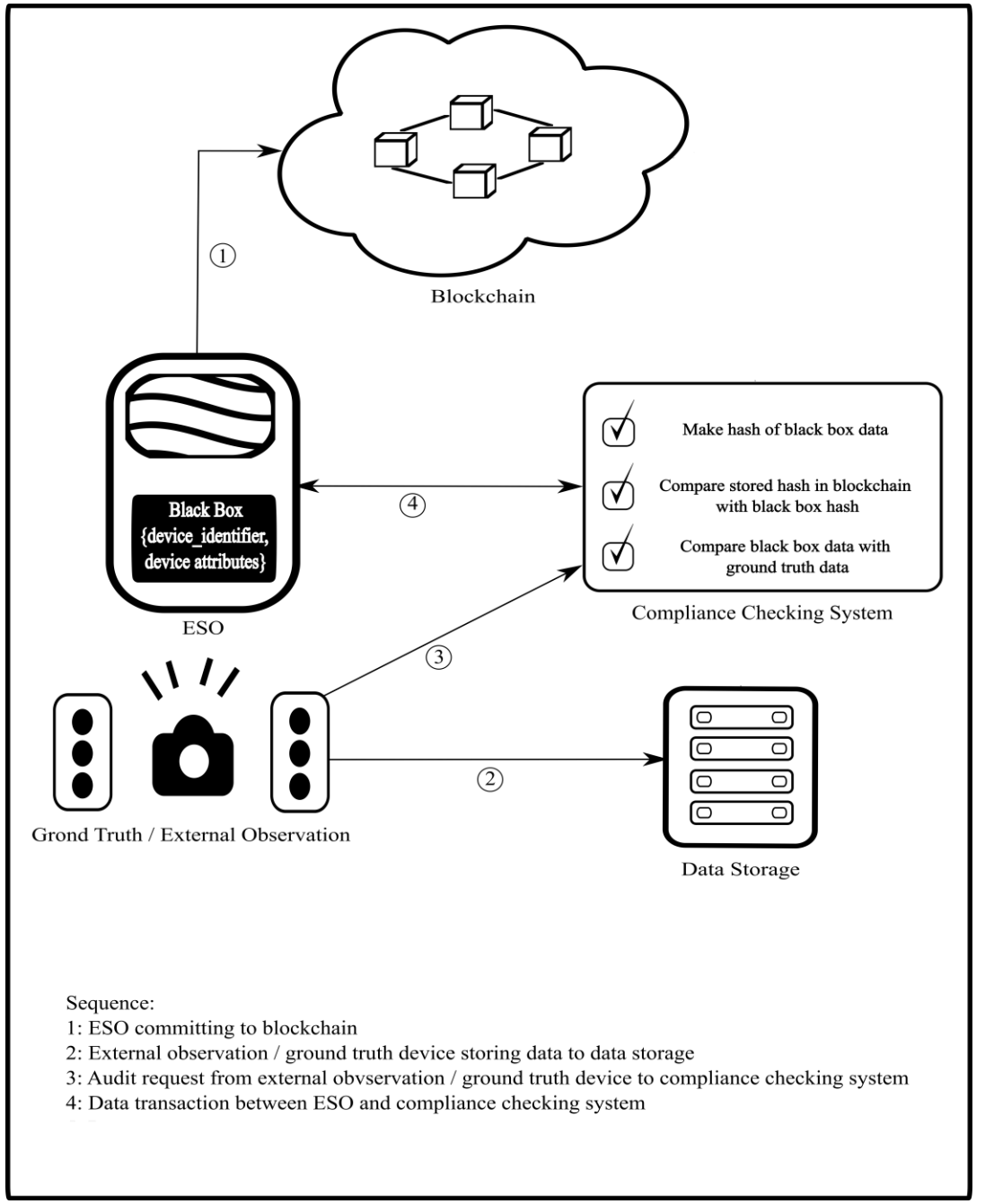
Sequence:
1: ESO committing to blockchain
2: External observation / ground truth device storing data to data storage

System Design



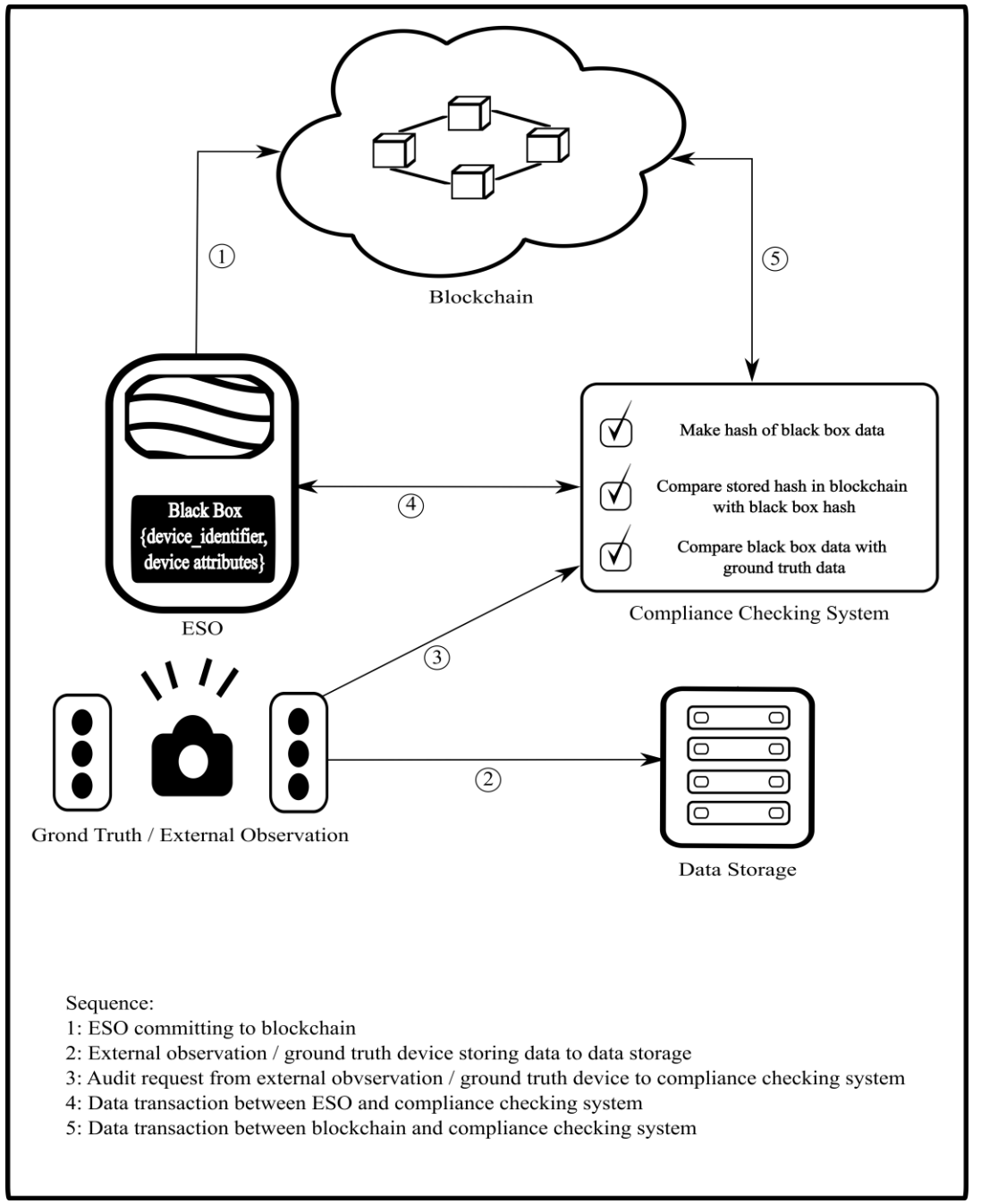
Sequence:
1: ESO committing to blockchain
2: External observation / ground truth device storing data to data storage
3: Audit request from external obvservation / ground truth device to compliance checking system

System Design



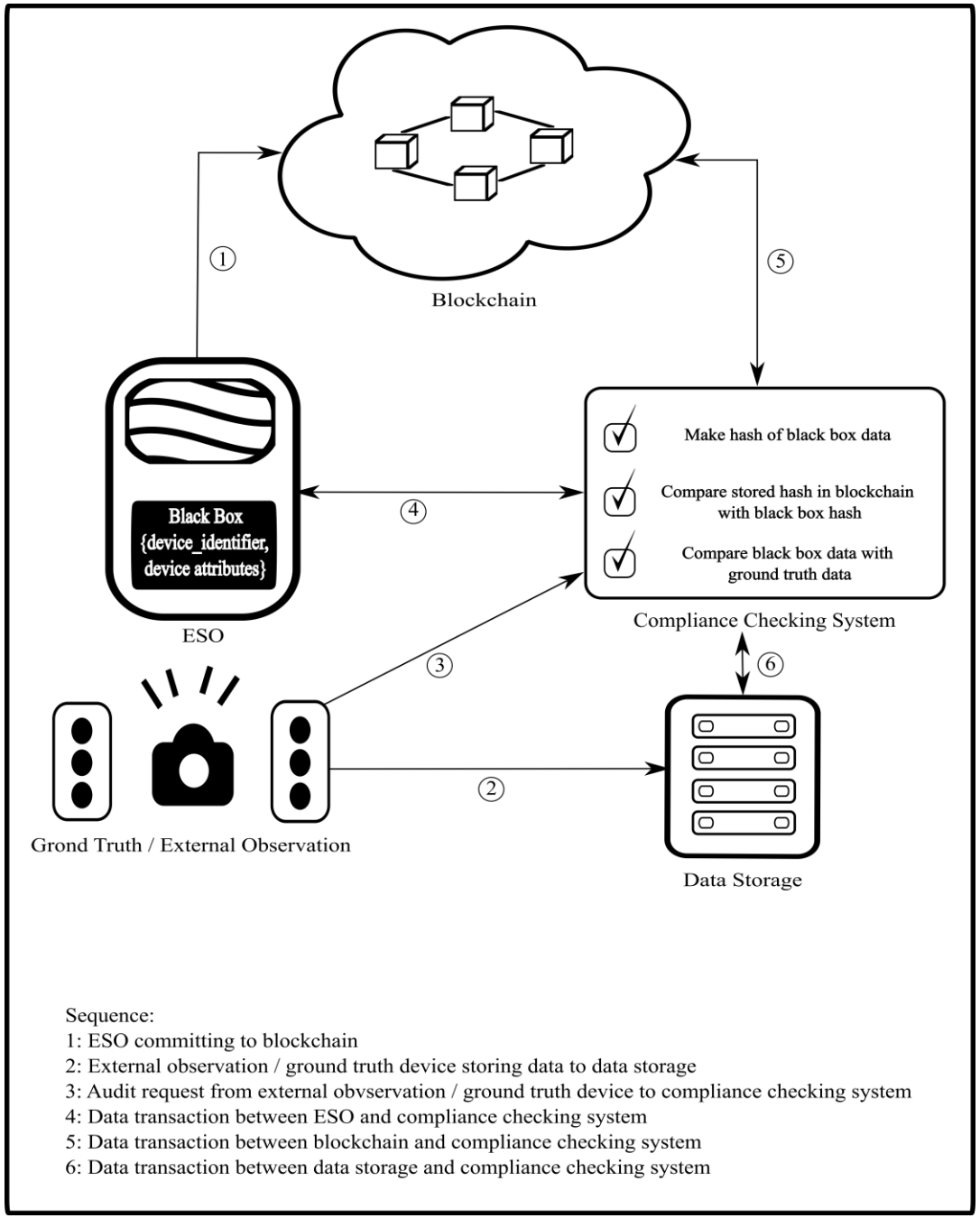
Sequence:
1: ESO committing to blockchain
2: External observation / ground truth device storing data to data storage
3: Audit request from external obvservation / ground truth device to compliance checking system
4: Data transaction between ESO and compliance checking system

System Design



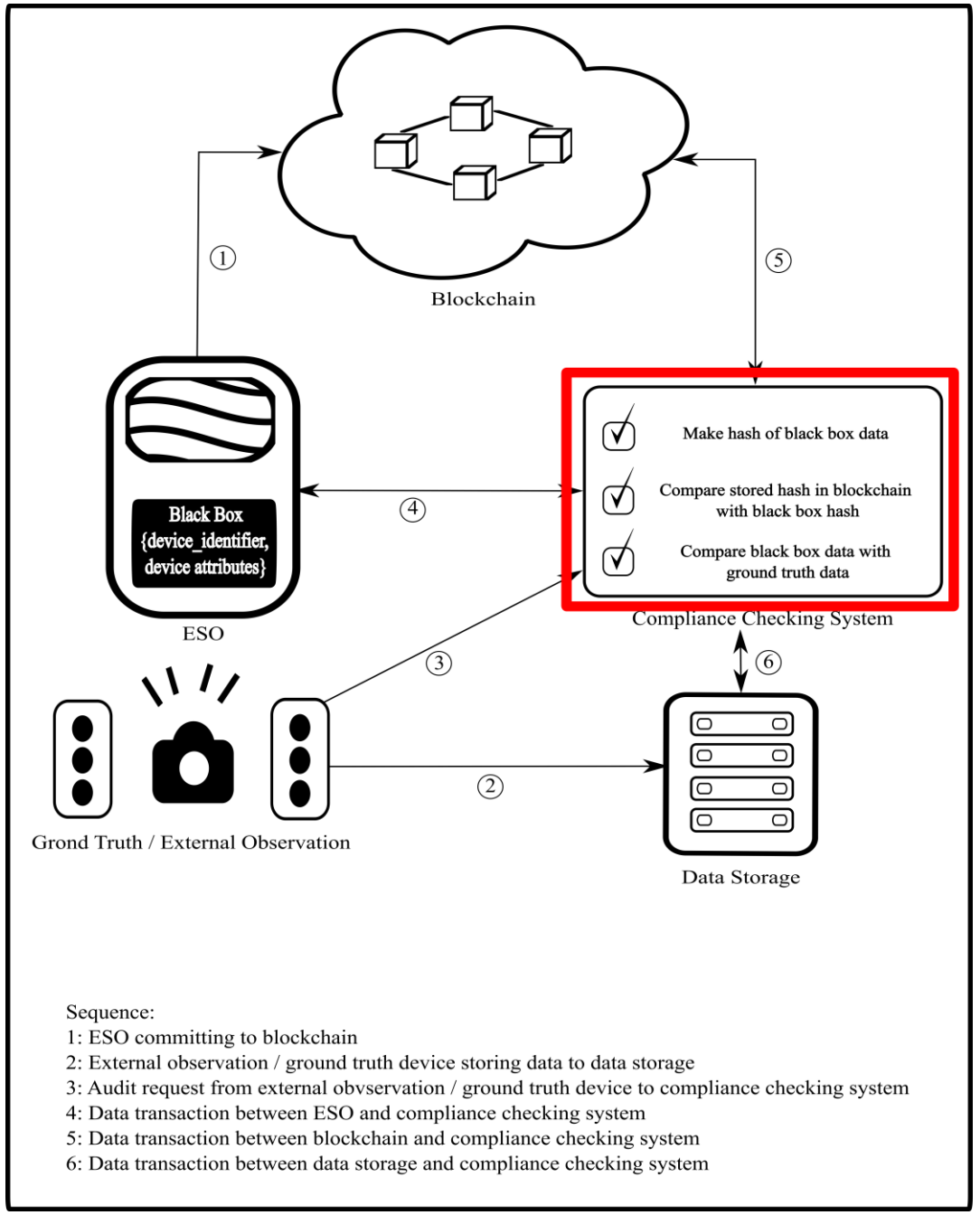
Sequence:
1: ESO committing to blockchain
2: External observation / ground truth device storing data to data storage
3: Audit request from external obvservation / ground truth device to compliance checking system
4: Data transaction between ESO and compliance checking system
5: Data transaction between blockchain and compliance checking system

System Design



Sequence:
1: ESO committing to blockchain
2: External observation / ground truth device storing data to data storage
3: Audit request from external obvservation / ground truth device to compliance checking system
4: Data transaction between ESO and compliance checking system
5: Data transaction between blockchain and compliance checking system
6: Data transaction between data storage and compliance checking system

System Design (Auditing)



Sequence:
1: ESO committing to blockchain
2: External observation / ground truth device storing data to data storage
3: Audit request from external obvservation / ground truth device to compliance checking system
4: Data transaction between ESO and compliance checking system
5: Data transaction between blockchain and compliance checking system
6: Data transaction between data storage and compliance checking system

Security Analysis

Our proposed system is comprised of the following security mechanisms:

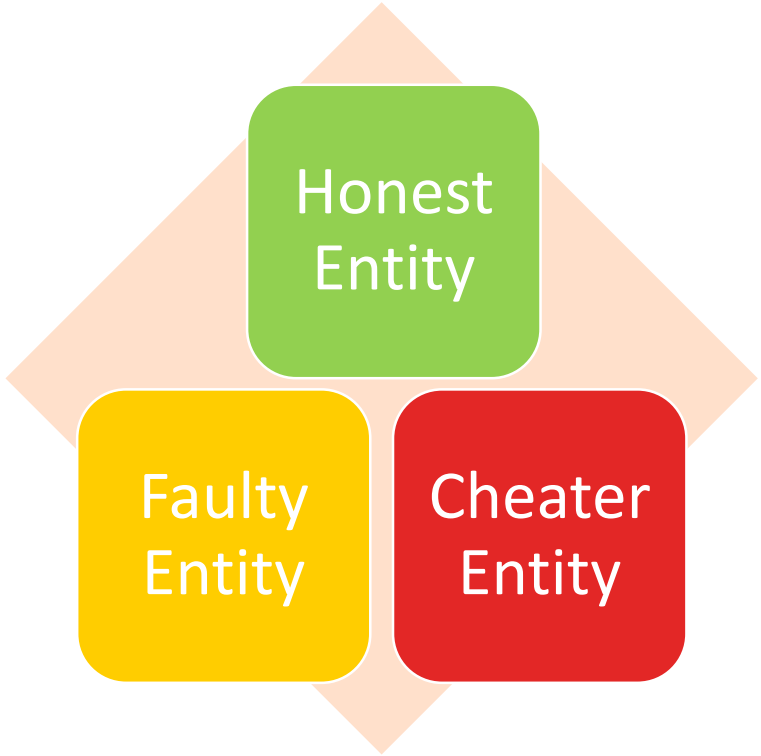
Hashes

Commitments

Random Audits

Security Analysis

Based on their characteristics, the following three types of entities can be found in our system:



Security Analysis Matrix

	Correct report of black box data	Incorrect report of black box data
Correct commit of black box hash in blockchain	• *Honest Enitity* • Expected Behaviour • No cheating	• *Faulty Entity* • Lies about black box content • Honest about blockchain commitment • Hash does not match
Inorrect commit of black box hash in blockchain	• *Faulty Entity* • Lies about blockchain commitment • Honest about black box content • Hash does not match	• *Cheater Entity* • Lies about data and commitment • Set fraudulent data at the time of collection • Random audit will reveal that the data that has been committed to, does not match reality

Prototype Implementation

Blockchain activation

CARLA simulator activation

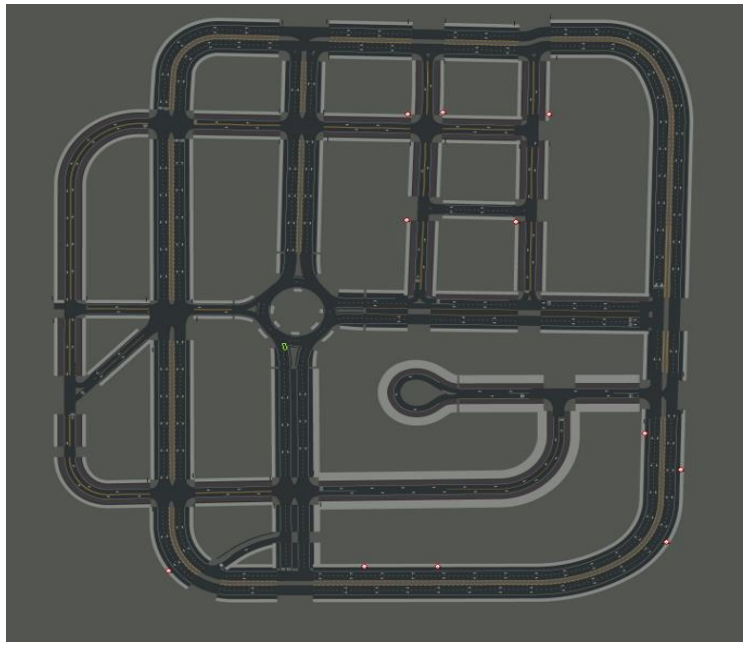
Autonomous vehicles generation

Cheater vehicle generation

Compliance Checking System activation

Traffic Cameras activation

Prototype Implementation



Map of Town03

Cheater vehicle

Location of traffic cameras

Result

Simulation No.	No. of captures	No. of audits	Audit percentage
1	110	51	46.36%
2	32	14	43.75%
3	25	18	72%
4	25	15	60%
5	40	25	62.50%
6	21	15	71.43%
7	46	27	58.70%
8	24	18	75%
9	47	29	61.70%
10	24	13	54.17%
Average	39.4	22.5	60.56%

Audit report of the *cheater* vehicle

Result

Simulation No.	Transmitted data (MiB)
1	147.819
2	201.225
3	211.716
4	139.236
5	133.514
6	145.912
7	130.653
8	171.661
9	198.364
10	113.487
Average	159.359

Network traffic during simulation

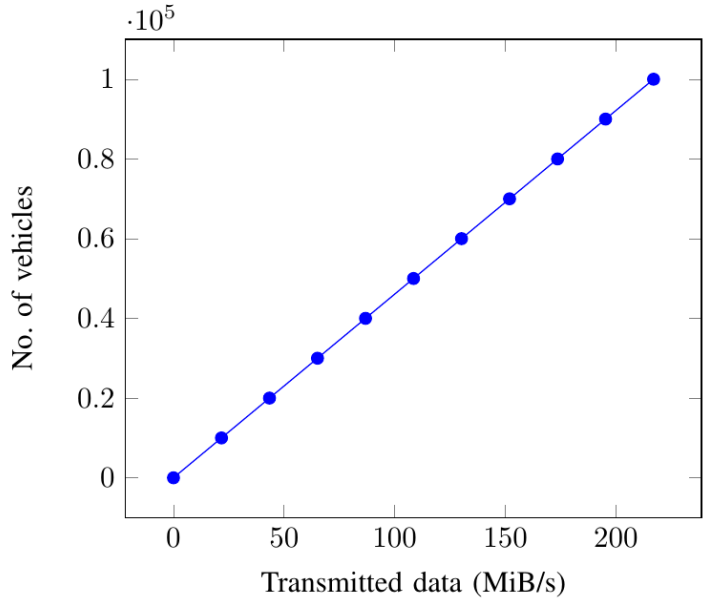
Duration (s)	Transmitted data (MiB)
1800	159.359
1	0.089

Data transmission of 41 vehicles

Result

No. of vehicles	Transmitted data (MiB/s)
1	0.00217
10,000	21.7
20,000	43.4
30,000	65.1
40,000	86.8
50,000	108.5
60,000	130.2
70,000	151.9
80,000	173.6
90,000	195.3
100,000	217

Network traffic prediction



No. of vehicles vs Transmitted data (MiB/s)

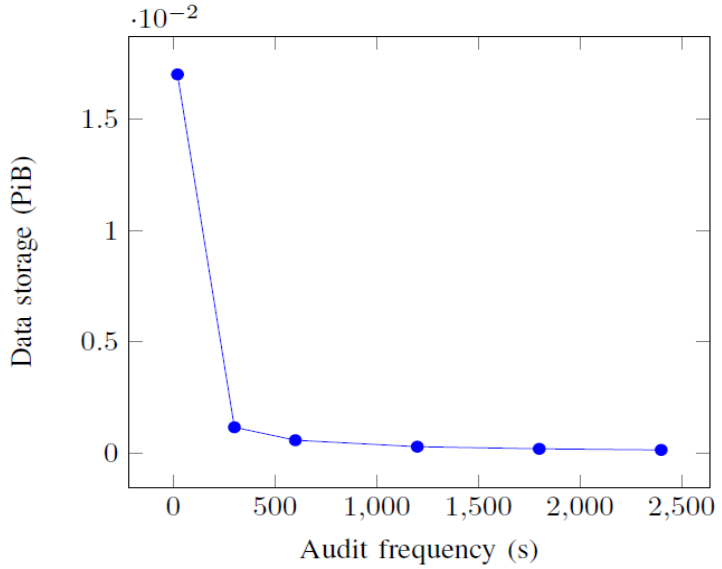
Result

Audit frequency (s)	Total number of audits in 24 hours	Data storage (PiB)
20	4320	6.13
300	288	0.40668

Audit frequency and data storage for the total number of registered vehicles in Canada (35,108,602)

Audit frequency (s)	Total number of audits in 24 hours	Data storage (PiB)
20	4320	0.017
300	288	0.00116
600	144	0.000579
1200	72	0.000289
1800	48	0.000193
2400	36	0.000144

Audit frequency and data storage for 100,000 vehicles



Data storage (PiB) vs audit frequency (s) for 100,000 vehicles

Summary

- Auditing and monitoring system
  - Prevents a system or a sensor from modifying its data
  - Retain the privacy
- Prototype implementation
  - monitor and audit autonomous vehicles
- Measure
  - Amount of time it takes to catch a *cheater*
- Predict
  - Amount of network traffic our system has to handle in a real-world implementation

Future Work and Conclusion

- Access to real-world devices and sensors
- Implement our model to monitor and audit autonomous vehicles in a modern city
- Implement our model to other use case scenarios
- Compare the performance among different use cases

THANK YOU

Q & A

Bibliography

- Crowdwiz, “What is blockchain and why is it the most secure way to exchange tokens?”[Accessed: 29-Sep-2018]. [Online]. Available: https://medium.com/@Crowdwiz.io/what-is-blockchain-and-why-is-it-the-most-secure-way-to-exchange-tokens-4c0f78edeede/
- R. Schuster, V. Shmatikov, and E. Tromer, “Situational access control in the internet of things,” in Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, 2018, pp. 1056–1073.
- K. W¨ust and A. Gervais, “Do you need a blockchain?” in 2018 Crypto Valley Conference on Blockchain Technology (CVCBT). IEEE, 2018, pp. 45–54. G. Smith and R. Parloff, “Inside volkswagen’s diesel fraud,” Fortune, Mar 2016, [Accessed: 29-Sep-2018]. [Online]. Available: http://fortune.com/inside-volkswagen-emissions-scandal/
- “Dieselgate - the ethical cycle,” Coursera, [Accessed: 01-Oct-2018]. [Online]. Available: https://www.coursera.org/lecture/ethics-technology-engineering/dieselgate-Rfpdc
- C. Gartenberg, “Safety driver of fatal self-driving uber crash was reportedly watching hulu at time of accident,” The Verge, Jun 2018, [Accessed:29-Sep-2018]. [Online]. Available: https://www.theverge.com/2018/6/22/17492320/safety-driver-self-driving-uber-crash-hulu-police-report
- Y. Heisler, “Tesla shares plummet by nearly 9% in wake of fatal Model X crash,” Bgr, Mar 2018, [Accessed: 29-Sep-2018]. [Online]. Available: https://bgr.com/2018/03/27/tesla-crash-model-x-fire-ntsb-investigation-stock/
- J. Hruska, “Tesla blames driver in Model X autopilot crash,” April 2018, [Accessed:29-Sep-2018]. [Online]. Available: https://www.extremetech.com/extreme/267417-tesla-blames-driver-in-model-x-autopilot-crash

- “Airplane black boxes and car black boxes: What are their similarities and differences?”Feb 2015, [Accessed: 29-Sep-2018]. [Online]. Available: https://www.telematics.com/airplane-black-boxes-and-car-black-boxes-what-are-their-similarities-and-differences/
- “Black box 101: Event data recorders - consumer reports,” Apr. 2014, [Accessed: 11-May-2020]. [Online]. Available: https://www.consumerreports.org/cro/2012/10/black-box-101-understanding-event-data-recorders/index.htm
- B. Canis and D. R. Peterman, “” black boxes” in passenger vehicles: Policy issues,” Congressional Research Service, Tech. Rep., 2014.
- N. E. W. Group et al., “Event data recorders-final rule,” NHTSA, US DOT, 2006.
- A. Rosic, “What is blockchain technology? a step-by-step guide for beginners,” 2016, [Accessed: 11-May-2020]. [Online]. Available: https://blockgeeks.com/guides/what-is-blockchain-technology/
- A. M. Antonopoulos, Mastering bitcoin: Programming the open blockchain. ” O’Reilly Media, Inc.”, 2017.
- I. Bashir, Mastering Blockchain: Distributed ledger technology, decentralization, and smart contracts explained. Packt Publishing Ltd, 2018.
- “4 different types of blockchain technology & networks,” Apr. 2020, [Accessed: 11-May-2020]. [Online]. Available: https://101blockchains.com/types-of-blockchain/
- D. Tapscott and A. Tapscott, “How blockchain will change organizations,” MIT Sloan Management Review, vol. 58, no. 2, p. 10, 2017.

- G. Greenspan, “Blockchains vs centralized databases. multichain,” Accessed on October, vol. 24, no. 2017, pp. 1–6, 2016.
- “What is a merkle tree and how does it affect blockchain technology?” Selfkey, Nov. 2019, [Accessed: 11-May-2020]. [Online]. Available: https://selfkey.org/what-is-a-merkle-tree-and-how-does-it-affect-blockchain-technology
- P. Nohe, “The difference between encryption, hashing and salting,” Dec. 2018, [Accessed: 11-May-2020]. [Online]. Available: https://www.thesslstore.com/blog/difference-encryption-hashing-salting/
- A. O’Donnell, “Rainbow tables: Your password’s worst nightmare,” Lifewire, Nov. 2019, [Accessed: 11-May-2020]. [Online]. Available: https://www.lifewire.com/rainbow-tables-your-passwords-worst-nightmare-2487288
- G. Greenspan, “Multichain private blockchain-white paper,” https://www.multichain.com/download/MultiChain-White-Paper.pdf
- A. Dosovitskiy, G. Ros, F. Codevilla, A. Lopez, and V. Koltun, “Carla: An open urban driving simulator,” arXiv preprint arXiv:1711.03938, 2017.
- J. Guerrero-Ib´a˜nez, S. Zeadally, and J. Contreras-Castillo, “Sensor technologies for intelligent transportation systems,” Sensors, vol. 18, no. 4, p. 1212, 2018.

- “Statistics canada. table 23-10-0067-01 vehicle registrations, by type of vehicle,” [Accessed:11-May-2020]. [Online]. Available: https://www150.statcan.gc.ca/t1/tbl1/en/tv.action?pid=2310006701
- “Google, how much data do you handle?” Guidesify, Jun. 2017, [Accessed: 11-May-2020]. [Online]. Available: https://guidesify.com/much-data-google-handle/