Using Blockchain to Securely Communicate Autonomous Vehicles' Current Location with Vehicles Nearby

Category: Engineering and Technology, Chemistry, and Physical Sciences

Rohini Das

42075 Loudoun Academy Dr, Leesburg, VA 20175

Acknowledgements

This research was conducted from August 2020 to March 2022 at the Engineering Lab at the Academies of Loudoun under the guidance of Sundar Thirukkurungudi, the Engineering Research teacher. Throughout the duration of the research, equipment was used from the Engineering Lab and assistance was received from Mr. Thirukurungudi in order to use materials and software safely. Furthermore, Mr. Thirukkurungudi assisted in finding online sources to gain background information on areas of the research project. The remainder of the research, including completing the method, collecting data and results, and writing this paper was done by Rohini Das, the student conducting this project.

Table of Contents **Page**

1 Introduction

1.1 Autonomous Vehicles

Each day, over a billion people travel on the roads of the world. As these people travel, two common traffic issues are congestion and human error. On an average, drivers spend 47 extra hours per year on the road, and 94% of deadly car crashes are caused by human error. Autonomous vehicles are a possible solution to these problems. An autonomous vehicle navigates around its environment with little to no human involvement using software that communicates to sensors and actuators. Currently, companies such as Tesla, NuTonomy, and AutoX are building autonomous vehicles and developing self-driving technology using artificial intelligence (Schroer, 2020). Since these vehicles operate on a machine-based system and determine the most efficient routes while traveling, they reduce human error and traffic congestion, resulting in fewer car accidents and increased human efficiency.

1.2 Future Location Communication

However, despite the shift towards autonomous vehicles (AVs), these two issues are still prevalent. A proposed solution to this problem lies with communication between AVs. Along with communication between the different components of a single AV, separate AVs will communicate with each another. Specifically, they'll communicate their future locations with one another. By knowing the locations of the vehicles nearby, AVs can utilize this information to efficiently determine driving routes, reducing traffic congestion and accidents. One way to predict the future location of an AV is through a machine learning algorithm that uses a vehicle's current location and speed to predict its nearest future location. Furthermore, the technology that

will enable the communication of this future location with other vehicles is known as vehicular ad-hoc networks or VANETs.

A VANET is comprised of stationary and moving vehicles that are connected via a wireless network. Until now, the primary use of VANETs was providing comfort and safety to drivers. However, research is now being conducted to utilize this technology towards enabling intelligent transportation systems where vehicles are connected and communicate using smart devices. One application of VANETs is connected autonomous vehicles (CAV) in which vehicles utilize sensors and adapters to communicate with their surroundings (Rathee et al., 2019). Connected autonomous vehicles can be characterized into four categories: vehicle to vehicle, vehicle to infrastructure, vehicle to pedestrian, and vehicle to everything. As their name suggests, these forms of CAV are the communication between a vehicle and vehicle, infrastructure, pedestrian, and everything respectively. With CAVs, autonomous vehicles will be able to share and retrieve the future locations of the vehicles nearby to efficiently determine driving routes. As more AV's join this network of communication, fewer AVs will be at the same location at the same time, reducing traffic congestion. Furthermore, accidents will be reduced as AVs will be informed when nearby AVs change lanes or speed.

However, since the VANET network, which is the enabling technology behind this communication, is centralized, the vehicular communication is subject to cyber-attacks and spreading disinformation among networks (Khan et al., 2019). Hackers can break into the autonomous vehicle's communication system and alter data, alter signals, or send incorrect signals, endangering the life of the passengers and nearby environment. In order for communication between autonomous vehicles to be integrated into the daily lifestyle of the people, it must be made secure. To ensure secure communication, this research proposes the integration of the machine learning algorithm with a Blockchain network.

1.3 Blockchain Network

Blockchains are distributed ledgers that allow transactions to be recorded globally on several servers in the form of interconnected blocks. Using a decentralized, peer-to-peer system, anyone on the blockchain network can view everyone else's entries and transactions. Each block in the blockchain is composed of three components: data, the hash of the block, and the hash of the previous block. The data stored in the block depends on the type of blockchain (Koduri et al., 2020). For example, the data stored in a Bitcoin blockchain is information about a transaction such as the sender, receiver, and number of coins. The next element in a block is the hash. Similar to a fingerprint, the hash identifies the block and its contents and is always unique. It is a function that converts an input of letters and numbers into an encrypted output and is calculated once the block is created. Altering something inside of the block changes the hash as well, making hashes extremely useful for detecting changes as once the hash is changed, it is no longer the same block. Finally, the third component in a block is the hash of the previous block, which creates a chain of blocks and makes blockchains so secure. For example, in a blockchain containing three blocks, along with containing its hash and data, the third block would also contain the hash of the second block. Similarly, the second block would contain the hash of the first block. Tampering with the second block would result in a change in its hash as well. As a result, the third block and all of the following blocks would be invalid as they would no longer

store a valid hash of the previous block. Thus, changing the contents of a single block results in the following blocks being invalid.

Along with hashes, a mechanism known as the proof-of-work is used to mitigate the tampering of blocks. This mechanism slows down the creation of new blocks, making it difficult to tamper with the blocks as altering one block would mean recalculating the proof-of-work for all of the following blocks. The final security measure in blockchains is its decentralized network that anyone can join. Each node in the blockchain receives a copy of the blockchain that automatically updates when a new block is added. When someone creates a new block, the block is sent to everyone on the network. Then, each node in the blockchain validates the block to ensure it has not been tampered with. If the nodes vote that the block is indeed valid, each node adds this block to its blockchain. Else, the block is not added to the blockchain. These properties of a blockchain make it nearly impossible to tamper with and extremely secure (Dorri et al., 2017; Reiff, 2020).

1.4 Smart Contracts

One of the more recent developments of blockchains is smart contracts. A smart contract is a computer protocol that digitally enforces the negotiation or performance of a contract. It allows for transactions without any third parties. Smart contracts can be compared to a vending machine. When money is dropped into a vending machine, it triggers the machine to release the desired product. In a smart contract, the money put in is the terms and conditions that result in the smart contract executing respective actions. Since smart contracts are stored in a blockchain, they are immutable and are distributed. As they are immutable, they cannot be altered once they are created. Furthermore, as they are distributed, the output of the smart contract can be validated by anyone. Thus, tampering with smart contracts is nearly impossible, making it secure. Currently, Ethereum is the largest open-source, blockchain-based distributed computing platform that is specifically designed to support smart contracts. These smart contracts can be programmed using the programming language Solidity (Frankenfield, 2019).

In this research, communication between AVs will be integrated with a Blockchain network. By integrating the two together, the blockchain network will validate the information about an autonomous vehicle that is communicated with the vehicles nearby by storing this information in the form of transactions. With the decentralized blockchain network validating the current location of AVs, future machine learning algorithms can utilize accurate current location data and accurately predict the vehicle's future location.

1.5 Current Research

Several studies have also addressed the issues of security amongst AVs by proposing a blockchain framework using IoT devices. An IoT device is a system that retrieves and transfers data over a network without human interaction. As an autonomous vehicle would travel, its IoT device would track its location and send this location to nearby vehicles to validate and add to the blockchain as a record. To test the effectiveness of the blockchain framework in increasing security, the researchers conducted a simulation of an autonomous cab booking system. In the online service, users would choose a cab of their choice and their entire ride would be monitored

by the nodes in the blockchain to ensure their security. Any malicious activity by the cab detected by the nodes would lower the cab's ratings. This approach is effective for current cab services that pose security risks for passengers, as passengers are not provided the details of the driver or the traveling route to their destination. Such a system that provides transparency to the rider would address these issues and reduce security risks (Rathee et. al., 2019).

While this research utilizes a blockchain network to provide security to passengers in autonomous vehicles, it solely focuses on the security of cab services and does not acknowledge the risks of personal vehicles. While autonomous cab services incorporate multiple vehicles with the same function, private vehicles do not have this common function. In addition, while incorporating autonomous vehicles with a blockchain network addresses the issue of safety, it doesn't increase efficiency or reduce traffic congestion. The research in this paper provides a solution to both current security risks and traffic congestion. By validating vehicles' current locations using Blockchain, future research can use these validated locations to the predict the future locations of these AVs. Such a secure and efficient system will increase the adoption of these self-driving vehicles in society. It will increase efficiency, reduce carbon emissions, and generate new avenues for economic growth, particularly for those kept off the roads due to physical disabilities.

2 Materials and Method

We created a simulation of interaction between autonomous vehicles using four Raspberry Pi 3 B+. We set up each Raspberry Pi using the Raspbian operating system and connected the Pi to a central computer. Next, we installed the GPS-based app What 3 Words on each Pi to retrieve its location and used the SCP command-line utility to send this location to the other Pi and central computer. After, we used Solidity to code the smart contract that validated the locations of the four Pi. Then, we shifted the Pi around to generate trials of suspicious and not suspicious behavior. Finally, the nodes in the network (the four Pi and central computer) used the smart contract to validate each trial as having suspicious or no suspicious behavior.

2.1 Setting Up Raspberry Pi

This research proposed the sharing of autonomous vehicles' locations with vehicles nearby. As mentioned above, IoT devices are the technology that retrieve such information about vehicles. To simulate this interaction, Raspberry Pi were used to represent AVs as both are essentially computers. Furthermore, a GPS-based app was used to model IoT devices and retrieve the locations of the Pi.

A Raspberry Pi is a low cost, small sized computer that plugs into a computer monitor and uses a standard keyboard and mouse for function. In this research, four Raspberry Pi were used to represent four autonomous vehicles. Each Pi was set up by first formatting its respective 32 GB SD card as FAT 32 using the SD Card Formatter application. Next, the Raspbian operating system was installed on each Pi using the Raspbian image and Etcher. After setting up

the four Pi, each device was connected to a monitor using an HDMI cord to display its contents. The images below show the set-up of the Pi.

Image 1: Set-up of one Raspberry Pi

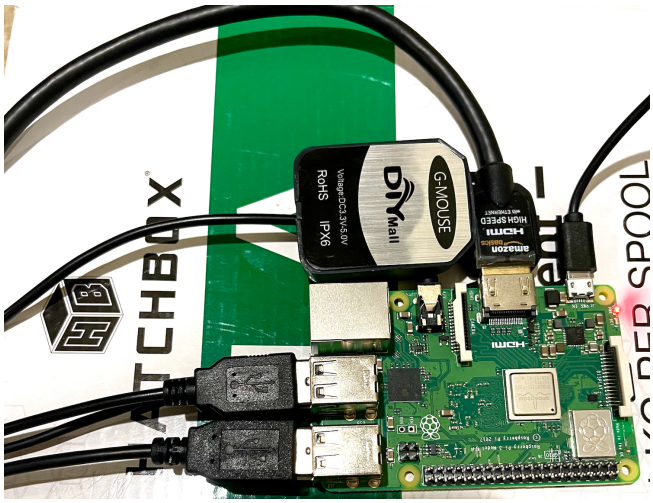
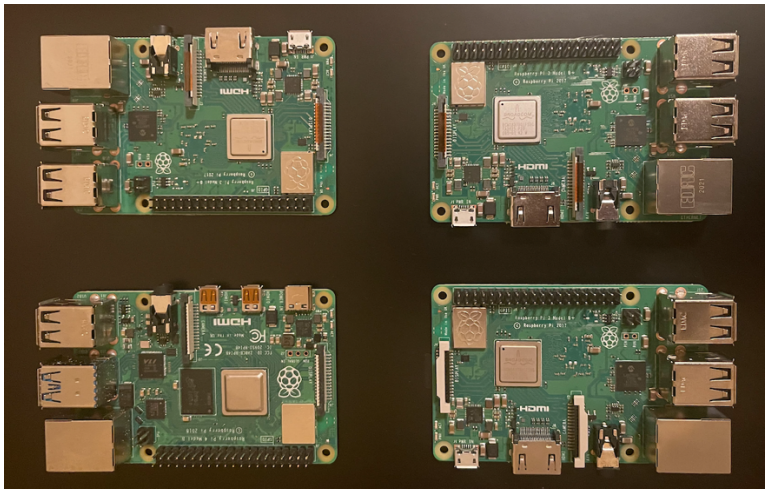


Image 2: Default placement of the four Raspberry Pi



2.2 Setting Up What 3 Words

After the four Pi were running on Raspbian, their individual locations were retrieved using the What 3 Words app. What 3 Words is a geocode system that divides the world into a grid of 57 trillion 3-by-3-meter squares that each have a unique three-word address. It uses an

API for bidirectional conversion between what3words addresses and latitude and longitude coordinates. The three-word addresses are available in forty-seven languages with each language using a list of 25,000 words to remove any risk of having two places with the same three-word address. Unlike standard GPS-based systems that are accurate to the nearest eleven meters, What 3 Words is accurate to the nearest 3 meters. Since the area encompassed by the components in this research was less than 11 meters, locations collected from a standard GPS-based system would be inaccurate. Furthermore, along with outputting locations in a form easy to remember, this app has error prevention technology that helps users quickly identify and correct input mistakes.

To install What 3 Words on a Raspberry Pi, since the app is only supported by Android and iOS, Android was installed on the Pi by installing Balena Etcher flashing software and Lineage OS 18.1 software. After installing the software, Lineage OS was flashed to the Pi's SD card with the Balena Etcher software. These steps were completed for all four Pi, so each Pi had the Android operating installed. After Android had been installed on the Pi, What 3 Words was installed on Google Play. Finally, the app was tested by seeing how shifting the Pi to different locations affected the outputted three-word string. At this point, the locations of all four Pi could be determined by the app. After, each Pi sent its location to the remaining three Pi and central computer using the SCP command-line utility, which could transfer files between Pi on the same Wifi network.

2.3 Setting Up Blockchain Network

After installing What 3 Words on the Pi and using SCP to communicate this location with the remaining Pi and central computer, the blockchain network was created. In this research, the blockchain network was comprised of five nodes: the four Raspberry Pi and the central computer. As these nodes received the locations of the four Pi, they would use the smart contract to validate these locations as having suspicious or no suspicious behavior based on the validating criteria. Currently, the only validating criteria is if the location of all four Pi aren't all different, and if the locations of any Pi change abruptly. Theoretically, the locations of more than one vehicle should only be the same in the case of an accident where they are on top of one another. So, in case of a situation other than an accident, this would signal suspicious behavior. In this research, this situation of suspicious behavior was simulated by placing multiple Pi directly on top of one another. Additionally, while the locations of vehicles change as they move, sudden changes in location would also signal suspicious behavior. In this research, this situation of suspicious behavior was simulated by suddenly shifting the position of Pi. As the prior validated locations of the Pi are stored in the blockchain, the smart contract can compare the older validated locations to the new current location to detect any sudden changes in location. While these two situations would represent suspicious behavior, any other situations would currently represent not suspicious behavior.

The first step to setting up the blockchain network was installing Ethereum on the four Pi and central computer. After Ethereum was installed on the Pi and central computer, it could synchronize with the live chain. Next, two miners that would later add validated locations of the Pi as transactions in the Blockchain were installed. Both miners were initialized by specifying their own target folder, creating the blockchain. After, default accounts were created for both

miners to run the two nodes in the blockchain. These accounts would receive the ethers created by the miners in the blockchain. After preparing both miners, ethers were sent within the accounts of the two miners to ensure that each mining node was properly installed and functioning. After synchronizing the two miners, these miners were synchronized with the four Raspberry Pi and central computer that each acted as nodes in the blockchain. This was done by initializing the blockchain on each Pi. Similar to the miners, default accounts were created for all four Pi and the central computer to run the nodes on the blockchain. Finally, ethers were sent between the miners and Pi to ensure all four Pi were properly installed and functioning.

At this point, the blockchain network was set up with the four Raspberry Pi nodes, the central computer, and the two miners. Furthermore, What 3 Words was set up to retrieve the current location of its respective Pi which was then sent to the remaining Pi using SCP. The final part of the method before collecting data was creating the Blockchain's smart contract that would validate the current locations of the Pi using Solidity. To develop and deploy the smart contract, Truffle, a development framework for Ethereum, was installed on the nodes. The contract had two functions. The first was to validate the four locations as having suspicious or no suspicious behavior based on the validating criteria mentioned above. The second function of the smart contract was peer-to-peer communication between the nodes where each node sent its validation to the remaining nodes. The nodes' validations of suspicious or no suspicious behavior were compared for each trial with the majority output being noted as the blockchain's experimental output for the trial. Ultimately, as the nodes are able to accurately validate the Pi's location with these two criteria, additional criteria will be incorporated into the contract.

3 Data

After coding the smart contract using Solidity, the smart contract was tested by generating 60 data trials. In 30 of the trials, the four Pi were shifted around the testing space to generate suspicious behavior using the two parameters specified above. While 25 of the trials tested the first condition of Pi being at identical locations, 5 of the trials tested the second condition of Pi locations suddenly changing drastically. After shifting the Pi, their respective What 3 Words app would retrieve and send their location to the remaining Pi which were nodes in the Blockchain network. The nodes would then validate these four locations as having suspicious or no suspicious behavior using the criteria mentioned above. Ideally, in these trials, the blockchain network would also output suspicious behavior as this would mean the network was accurately able to validate the locations of the Pi. In the remaining 30 trials, the four Pi were shifted around the testing space to generate no suspicious behavior. Similarly, in these trials, the network would ideally output no suspicious behavior amongst the Pi.

Table 1: Experimental vs actual output for not suspicious behavior

Trial	Current Location (Pi 1)	Current Location (Pi 2)	Current Location (Pi 3)	Current Location (Pi 4)	Experimental Output	Actual Output
1	dabbing.towers.microwaves	coping.reality.wipes	commented.conflicted.rooms	stewardness.cycles.hostels	Not suspicious	Not suspicious
2	radio.snooty.accused	shelving.jolt.contest	habitat.congratulations.milkman	appeals.fiction.checklists	Not suspicious	Not suspicious
3	wades.desired.elbowed	lengthy.butter.starter	found.undercover.relates	phrases.kettle	Not suspicious	Not suspicious
4	radio.snooty.accused	dabbing.towers.microwaves	dusted.roofed.influential	bulges.rowers.jars	Not suspicious	Not suspicious
5	cheese.bypasses.transformed	café.adamant.freezers	inspected.legions.former	salvage.rectangular.buzzards	Not suspicious	Not suspicious
6	breezes.degrading.refined	amongst.luxury.honeycomb	knee.impress.introduces	slyly.luckily.resign	Not suspicious	Not suspicious
7	movement.private.weaving	sues.helicopters.piles	appeals.fiction.checklists	salvage.rectangular.buzzards	Not suspicious	Not suspicious
8	lift.soldiers.braves	chunks.remain.capillary	craving.probing.wagers	extends.goal.hesitate	Not suspicious	Not suspicious
9	harmless.optical.kettles	cross.scenic.objection	dusted.roofed.influential	coping.reality.wipes	Not suspicious	Not suspicious
10	admits.panic.unsafe	crated.pyramid.diligently	truck.parents.taxable	illustrates.cowboys.amazed	Not suspicious	Not suspicious
11	subjecting.leaflet.copiers	enclosures.objective.swaps	unduly.tramps.nutrients	traces.broadens.madness	Not suspicious	Not suspicious
12	habitat.congratulations.mlkman	sourced.offered.jackets	stewardness.cycles.hostels	converting.revise.sprawls	Not suspicious	Not suspicious
13	protections.reporting.weeded	owned.geared.secures	processes.proper.equator	prices.bossy.influential	Not suspicious	Not suspicious
14	sues.helicopters.piles	towers.charms.editor	massive.barricades.wriggled	truck.parents.taxable	Not suspicious	Not suspicious
15	packaging.using.beliefs	pastry.upwardly.contents	thumbs.schematic.plea	milestones.global.secretly	Not suspicious	Not suspicious
16	tulips.punters.acknowledge	unduly.tramps.nutrients	encoded.lances.garage	drilled.firelight.pottery	Not suspicious	Not suspicious
17	merchandise.whisk.forcefully	knee.impress.introduces	citizenship.obvious.interacted	forcfully.workroom.snug	Not suspicious	Not suspicious
18	automobiles.subsystem.radio	hospitality.balconies.kitchens	upbringing.schooling.though	includes.server.purified	Not suspicious	Not suspicious
19	stewardness.topical.snares	amongst.luxury.honeycomb	appeals.fiction.checklists	appeals.fiction.checklists	Not suspicious	Not suspicious
20	crated.pyramid.diligently	sues.helicopters.piles	traces.broadens.madness	tulips.punters.acknowledge	Not suspicious	Not suspicious
21	inspected.legions.former	habitat.congratulations.mlkman	automobiles.subsystem.radio	salvage.rectangular.buzzards	Not suspicious	Not suspicious
22	alarms.forging.biologist	doodle.roses.spring	octagon.cooling.captain	birthmark.salt.withdraws	Not suspicious	Not suspicious
23	task.contracting.departments	vegetarian.hedged.certain	guilty.headstone.certain	impulses.sitcom.parents	Not suspicious	Not suspicious
24	costumes.scoring.puppet	bounce.guide.spirits	cigar.iconic.denistry	depart.gates.joked	Not suspicious	Not suspicious
25	tulips.punters.acknowledge	knee.impress.introduces	packaging.using.beliefs	milestones.global.secretly	Not suspicious	Not suspicious
26	unsecured.quaint.blurts	awaits.burying.clearcut	niece.offend.calms	scorpions.likely.spills	Not suspicious	Not suspicious
27	weeknight.couple.galas	perceptual.factored.billiard	charge.triumphant.shops	wobbling.misled.aimed	Not suspicious	Not suspicious
28	dispenser.daytime.foils	ritual.clustering.situation	arranges.nicknames.listeners	relocating.threading.headboard	Not suspicious	Not suspicious
29	mattress.counters.concessions	guilty.headstone.certain	weeknight.couple.galas	drilled.firelight.pottery	Not suspicious	Not suspicious
30	traces.broadens.madness	amongst.luxury.honeycomb	tulips.punters.acknowledge	thumbs.schematic.plea	Not suspicious	Not suspicious

The table above displays the experimental vs actual output during the 30 trials where there was no suspicious behavior. Columns 2-5 include the current locations of the four Pi during each trial. The experimental and actual outputs can be compared using columns 6-7.

Table 2: Experimental vs actual output for suspicious behavior (first condition)

Trial	Current Location (Pi 1)	Current Location (Pi 2)	Current Location (Pi 3)	Current Location (Pi 4)	Experimental Output	Actual Output
1	wades.desired.elbowed	wades.desired.elbowed	wades.desired.elbowed	wades.desired.elbowed	Suspicious	Suspicious
2	cheese.bypasses.transformed	cheese.bypasses.transformed	cheese.bypasses.transformed	cheese.bypasses.transformed	Suspicious	Suspicious
3	breezes.degrading.refined	breezes.degrading.refined	breezes.degrading.refined	breezes.degrading.refined	Suspicious	Suspicious
4	café.adamant.freezers	café.adamant.freezers	café.adamant.freezers	café.adamant.freezers	Suspicious	Suspicious
5	movement.private.weaving	movement.private.weaving	movement.private.weaving	movement.private.weaving	Suspicious	Suspicious
6	salvage.rectangular.buzzards	salvage.rectangular.buzzards	salvage.rectangular.buzzards	salvage.rectangular.buzzards	Suspicious	Suspicious
7	dusted.roofed.influential	dusted.roofed.influential	dusted.roofed.influential	dusted.roofed.influential	Suspicious	Suspicious
8	unduly.tramps.nutrients	unduly.tramps.nutrients	unduly.tramps.nutrients	unduly.tramps.nutrients	Suspicious	Suspicious
9	traces.broadens.madness	traces.broadens.madness	traces.broadens.madness	traces.broadens.madness	Suspicious	Suspicious
10	processes.proper.equator	processes.proper.equator	processes.proper.equator	processes.proper.equator	Suspicious	Suspicious
11	pastry.upwardly.contents	pastry.upwardly.contents	truck.parents.taxable	truck.parents.taxable	Suspicious	Suspicious
12	truck.parents.taxable	truck.parents.taxable	merchandise.whisk.forcefully	merchandise.whisk.forcefully	Suspicious	Suspicious
13	merchandise.whisk.forcefully	merchandise.whisk.forcefully	sues.helicopters.piles	sues.helicopters.piles	Suspicious	Suspicious
14	sues.helicopters.piles	sues.helicopters.piles	upbringing.schooling.though	upbringing.schooling.though	Suspicious	Suspicious
15	upbringing.schooling.though	upbringing.schooling.though	dispenser.daytime.foils	dispenser.daytime.foils	Suspicious	Suspicious
16	includes.server.purified	includes.server.purified	dispenser.daytime.foils	dispenser.daytime.foils	Suspicious	Suspicious
17	crated.pyramid.diligently	crated.pyramid.diligently	includes.server.purified	includes.server.purified	Suspicious	Suspicious
18	relocating.threading.headboard	relocating.threading.headboard	crated.pyramid.diligently	crated.pyramid.diligently	Suspicious	Suspicious
19	found.undercover.relates	found.undercover.relates	relocating.threading.headboard	relocating.threading.headboard	Suspicious	Suspicious
20	costumes.scoring.puppet	costumes.scoring.puppet	found.undercover.relates	found.undercover.relates	Suspicious	Suspicious
21	costumes.scoring.puppet	alarms.forging.biologist	alarms.forging.biologist	costumes.scoring.puppet	Suspicious	Suspicious
22	alarms.forging.biologist	cigar.iconic.denistry	cigar.iconic.denistry	alarms.forging.biologist	Suspicious	Suspicious
23	cigar.iconic.denistry	bounce.guide.spirits	bounce.guide.spirits	cigar.iconic.denistry	Suspicious	Suspicious
24	bounce.guide.spirits	guilty.headstone.certain	guilty.headstone.certain	bounce.guide.spirits	Suspicious	Suspicious
25	guilty.headstone.certain	movement.private.weaving	movement.private.weaving	guilty.headstone.certain	Suspicious	Suspicious

The table above displays the experimental vs actual output during 25 of the 30 trials where there was suspicious behavior. During these trials, two or more Pi were placed on top of each other to generate suspicious behavior. Columns 2-5 include the current locations of the four Pi during each trial. The experimental and actual outputs can be compared using columns 6-7.

Table 3: Experimental vs actual output for suspicious behavior (second condition)

Trial	Current Location (Pi)	Initial Location	Final Location	Experimental Output	Actual Output
1	Current Location (Pi 1)	dusted.roofed.influential	unduly.tramps.nutrients		
	Current Location (Pi 2)	**cheese.bypasses.transformed**	**guilty.headstone.certain**	Suspicious	Suspicious
	Current Location (Pi 3)	wades.desired.elbowed	dusted.roofed.influential		
	Current Location (Pi 4)	unduly.tramps.nutrients	wades.desired.elbowed		
2	Current Location (Pi 1)	café.adamant.freezers	unduly.tramps.nutrients		
	Current Location (Pi 2)	**cheese.bypasses.transformed**	**guilty.headstone.certain**	Not Suspicious	Suspicious
	Current Location (Pi 3)	movement.private.weaving	processes.proper.equator		
	Current Location (Pi 4)	processes.proper.equator	café.adamant.freezers		
3	Current Location (Pi 1)	dusted.roofed.influential	cheese.bypasses.transformed		
	Current Location (Pi 2)	pastry.upwardly.contents	truck.parents.taxable		
	Current Location (Pi 3)	**cheese.bypasses.transformed**	**dusted.roofed.influential**	Not Suspicious	Suspicious
	Current Location (Pi 4)	truck.parents.taxable	breezes.degrading.refined		
4	Current Location (Pi 1)	pastry.upwardly.contents	habitat.congratulations.milkman		
	Current Location (Pi 2)	cigar.iconic.denistry	guilty.headstone.certain		
	Current Location (Pi 3)	automobiles.subsystem.radio	pastry.upwardly.contents		
	Current Location (Pi 4)	**habitat.congratulations.mlkman**	**unsecured.quaint.blurts**	Suspicious	Suspicious
5	**Current Location (Pi 1)**	**amongst.luxury.honeycomb**	**stewardness.topical.snares**	Not Suspicious	Suspicious
	Current Location (Pi 2)	sues.helicopters.piles	cigar.iconic.denistry		
	Current Location (Pi 3)	costumes.scoring.puppet	sues.helicopters.piles		
	Current Location (Pi 4)	vegetarian.hedged.certain	amongst.luxury.honeycomb		

The table above displays the experimental vs actual output during 5 of the 30 trials where there was suspicious behavior. During these trials, the Pi were shifted with columns 3-4 displaying the initial and final locations of the Pi. In each trial, one of the four Pi were moved to a drastically different location to simulate abnormal driving data. This Pi is bolded in each trial. The experimental and actual outputs can be compared using columns 5-6.

Results

To compare the blockchain's experimental output in validating suspicious and no suspicious behavior, a 2x2 contingency table was created. This table included the number of trials where the blockchain correctly validated suspicious behavior, correctly validated not suspicious behavior, incorrectly validated suspicious behavior, and incorrectly validated not suspicious behavior. Such a table would depict how closely the experimental data determined by the blockchain network aligned with the actual data and display information such as if the blockchain was more accurate at validating a certain type of behavior. The table blow displays the 2x2 contingency table.

Table 4: 2x2 Contingency table displaying relationships between experimental vs actual output across trials

	Experimental Suspicious Behavior	Experimental No Suspicious Behavior	Total
Actual Suspicious Behavior	27	3	30
Actual No Suspicious Behavior	0	30	30
Total	27	33	60

Looking at the table above, the blockchain network was able to accurately validate trials with no suspicious behavior in all 30 trials. So, there were no instances where the network incorrectly validated a case of no suspicious behavior as having suspicious behavior. Thus, the blockchain network was able to successfully able to validate no suspicious behavior. However, in the 30 trials that contained suspicious behavior, the blockchain network only validated 27 of trials correctly. So, there were three instances where the network incorrectly validated a case of suspicious behavior as having no suspicious behavior. Thus, while the network was able to correctly validate most instances of suspicious behavior, it had a higher accuracy in validating trials containing no suspicious behavior.

Going back to the hypothesis, since the blockchain network correctly validated the locations of the Pi in all 30 trials of no suspicious behavior, there was no significant difference between the actual and experimental output during these trials. However, since the blockchain only correctly validated 27 of the 30 trials of suspicious behavior, a two-tailed t-test was conducted to the compare the experimental and actual outputs for this set of 30 trials to see if there was a significant difference between the outputs for suspicious behavior. While conducting the t-test, trials where the experimental and actual data aligned were noted as 1 while trials where they didn't align were noted as 0. Furthermore, the data was compared to the hypothetical mean of 1. The results for the t-test are shown below.

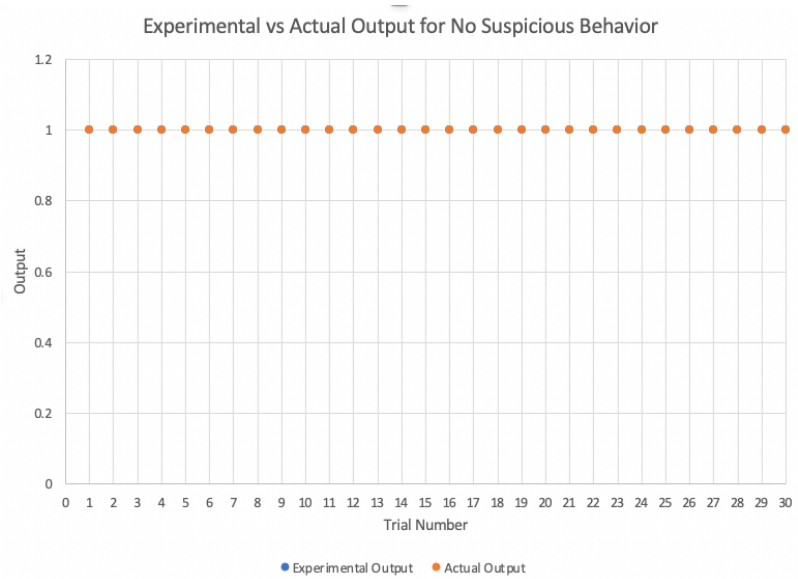
Table 5: Two-tailed t-test values comparing experimental vs actual output for suspicious behavior

p-value	0.0831
95% confidence interval	[0.7861, 1.014]
Mean	0.9
Standard Deviation	0.3051
Standard Error	0.05571

Looking at the results of the t-test above, it can be seen that the p-value is 0.0831. Since the p-value of 0.0831 is greater than the significance level of 0.05, the null hypothesis cannot be rejected. Thus, there isn't a significant difference between the actual and experimental output for suspicious behavior, indicating that the blockchain network was able to accurately validate suspicious behavior amongst the Pi. Furthermore, looking at the values above, the 95% confidence interval is [0.7861, 1.014], the mean is 0.9, the standard deviation in 0.3051, and the standard error is 0.05571.

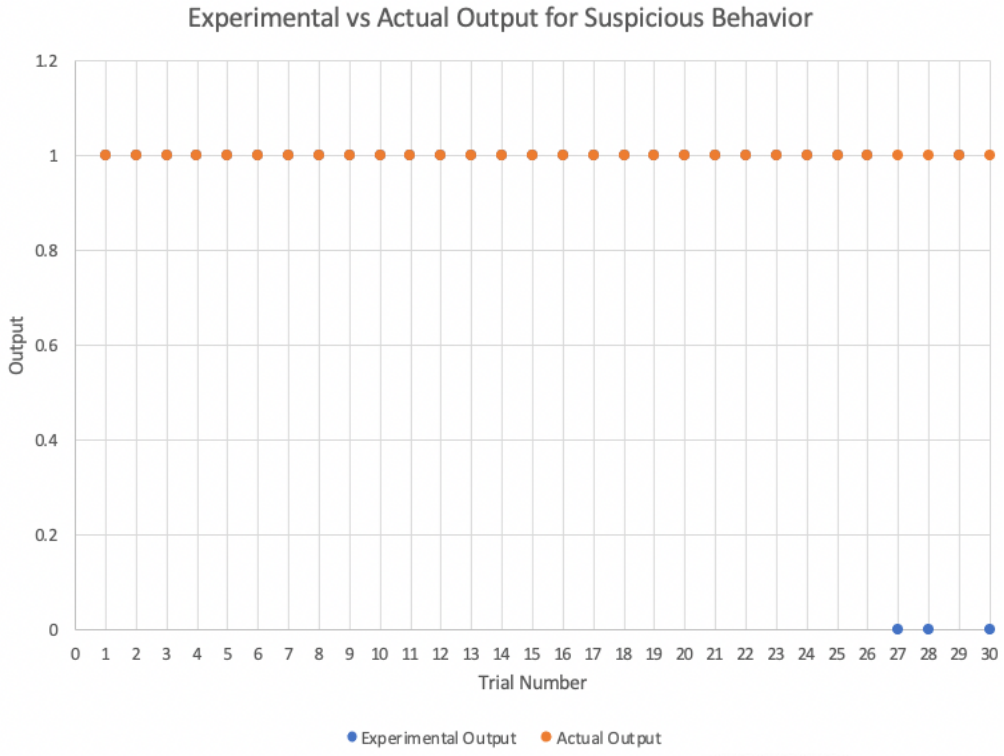
Finally, the graphs below display how closely the experimental and actual outputs align for suspicious and not suspicious behavior in a more visual form. While trials with only one point signify that both outputs aligned, trials with two points signify that the outputs differed from one another.

Graph 1: Experimental vs Actual Output for No Suspicious Behavior



Looking at the graph above, since the experimental and actual outputs were identical for all 30 trials of no suspicious behavior, there is only one point for each trial.

Graph 2: Experimental vs Actual Output for Suspicious Behavior



Looking at the graph above, since the experimental and actual outputs were only identical for 27 trials of suspicious behavior and differed for 3 trials, there are three trials containing two points. The remaining 27 trials only contain one point.

Discussion

The purpose of this research was to securely communicate autonomous vehicles' current location with vehicles nearby. As these vehicles become integrated into society, they must be made secure. As vehicle-to-vehicle interaction continues to advance, this communication must be made secure. Passengers and drivers must feel safe when traveling in these vehicles. The proposed solution to the integration of this communication with a blockchain network that will validate the information communicated between vehicles. One such example of communication information is the current location of vehicles. By knowing the locations of the vehicles nearby, autonomous vehicles can utilize this information to make efficient driving decisions. By validating this information through a Blockchain network, this vehicular communication will become secure as the information AVs receive will be accurate and not tampered.

To do this, a simulation of interaction between Raspberry Pi was created in this research. In this research, 60 trials of suspicious and not suspicious behavior were generated by shifting the Pi in a testing space. As the Pi were shifted, their respective GPS-based What 3 Words app retrieved and sent their location to the Blockchain network to validate. After collecting data for

all 30 trials of suspicious behavior and 30 trials of not suspicious behavior as seen in Tables 1-3, the actual and experimental outputs were compared in Table 4-5 and Graphs 1-2. As seen in the tables and graphs, the blockchain network was able to accurately validate trials with no suspicious behavior in all 30 trials. So, there were no instances where the network incorrectly validated a case of no suspicious behavior as having suspicious behavior. Thus, the blockchain network was able to successfully able to validate no suspicious behavior. However, in the 30 trials that contained suspicious behavior, the blockchain network only validated 27 of trials correctly. So, there were three instances where the network incorrectly validated a case of suspicious behavior as having no suspicious behavior. Thus, while the network was able to correctly validate most instances of suspicious behavior, it had a higher accuracy in validating trials containing no suspicious behavior.

Going back to the hypothesis, since the blockchain network correctly validated the locations of the Pi in all 30 trials of no suspicious behavior, there was no significant difference between the actual and experimental output during these trials. However, since the blockchain only correctly validated 27 of the 30 trials of suspicious behavior, a two-tailed t-test was conducted to the compare the experimental and actual outputs for this set of 30 trials to see if there was a significant difference between the outputs for suspicious behavior. Since a two-tailed t-test comparing the blockchain's experimental output and the actual output displayed no significant difference between the two outputs, the decentralized system accurately validated the locations for suspicious behavior as well.

In this research, a blockchain network was created that accurately validated the locations of Pi as having suspicious or no suspicious behavior. In the future, this blockchain network will be integrated with a linear regression algorithm to predict the future locations of the Pi and ultimately, vehicles. This integration of blockchain will help ensure that information communicated between self-driving vehicles is accurate, reducing traffic congestion and accidents. Future work will focus on using blockchain to securely communicate vehicles' future location over a designated time interval.

Literature Cited

Dorri, A., Steger, M., Kanhere, S., & Jurdak, R. (2017). BlockChain: A Distributed Solution to Automotive Security and Privacy. *IEEE Communications Magazine*, 55(12), 119-125. doi: 10.1109/MCOM.2017.1700879

Eloudrhiri, S. (2017, February 24). *Create a private Ethereum blockchain with IoT devices*. ChainSkills. https://chainskills.com/2017/02/24/create-a- private-ethereum-blockchain-with-iot-devices-16/

Frankenfield, Jake. "Smart Contracts: What You Need to Know." *Investopedia*, Investopedia, 7 May 2020, www.investopedia.com/terms/s/smart-contracts.asp.

Khan, A.S., Balan, K., Javed, Y., Tarmizi, S., Abdullah, J. (2019) Secure Trust-Based Blockchain Architecture to Prevent Attacks in VANET. *Sensors 2019,* 19(22), 4954. doi: 10.3390/s19224954

M, V., Koduri, R., Nandyala, S., & Manalikandy, M. (2020). Secure Vehicular Communication Using Blockchain Technology. *SAE Technical Paper,* doi: 10.4271/2020-01-0722

Rathee, G., Sharma, A., Iqbal, R., Aloqaily, M., Jaglan, N., & Kumar, R. (2019). A Blockchain Framework for Securing Connected and Autonomous Vehicles. *Sensors 2019*, 19(14), 3165. doi: 10.3390/s19143165

Reiff, Nathan. "Blockchain Explained." *Investopedia*, Investopedia, 5 Feb. 2020, www.investopedia.com/terms/b/blockchain.asp.

Schroer, Alyssa. “Artificial Intelligence in Cars Powers an AI Revolution in the Auto Industry.” *Built In*, builtin.com/artificial-intelligence/artificial-intelligence-automotive-industry .