Examining Distributed Ledger Technology (DLT) for Autonomous Vehicle Communications Using The IOTA Framework

Author

James O'Connor

Masters in Engineering (MEng) in Connected and Autonomous Vehicles

Institute of Technology, Sligo

Supervisor of Research: Dr. Donny Hurley

Submitted to the Quality Qualifications Ireland (QQI)

December, 2021

Table of Contents

List of Figures

List of Tables

STUDENT DECLARATION

or another college.

Signed: **James O'Connor** Date: 19/10/2021

Ethical Considerations (where applicable)

I will follow the conditions of the Ethical Conduct for research involving humans. If required, Ethical approval for this research will be obtained from the Institute of Technology Sligo Ethics Committee

CHAPTER ONE

Introduction

1.1 Problem Statement

With driverless cars already operational in a number of countries, autonomous driving systems are rapidly becoming a reality as a mode of intelligent transportation. It has been predicted that by 2025 there will be over eight million vehicles on our roads with level three and above autonomy [1], based on the SAE definitions for automation systems for on-road motor vehicles [2]. Vehicle-to-everything (V2X) communication is an over-arching term that encapsulates vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I) and vehicle-to-pedestrian (V2P). With the projected rate of growth in vehicles of this magnitude, finding a way for these vehicles to communicate with each other, with users and with their environment that is secure, scalable and standardised remains an open research question [3]. From a security perspective, a number of challenges still exist including availability (flooding, blackhole and greyhole attacks), data privacy (eavesdropping, location tracking, non-repudiation), data integrity (injection, replay and spoofing attacks) and authenticity (Sybil and man-in-the-middle attacks) [3]. In terms of scalability it is estimated that 125 million cars with embedded connectivity will ship between 2018 and 2022, which will lead to higher traffic and usage of autonomous vehicle services and applications and their supporting Dedicated Short Range Communication (DSRC) and Cellular-V2X (C-V2X) protocols. In addition to this, as the industry moves towards autonomy, these supporting services and applications will also need to be autonomous to capture the benefits and opportunities of autonomous vehicles. In terms of standardisation, there is no universal standardised framework for V2X integration. Many of the standards for 5G communication are still under development, and standards differ across countries, geopolitical areas and consortiums [4]. The lack of operability among heterogeneous devices poses a challenge to adoption rates of autonomous vehicles [3].

1.2 Rationale For Research

Approximately 94% of all serious accidents on roads are due to human error [5]. Autonomous vehicles have the capability to dramatically increase safety on our roads, which is beneficial on both an economic and societal level. From an environmental perspective autonomous vehicles can provide smooth traffic control, a reduction in traffic congestion and vehicle ownership, cutting fuel cost and vehicle emissions [5]. The current challenges for V2X communication outlined in the problem statement hinder the rollout and adoption of autonomous vehicles and inevitably the benefits that come with them. To solve for these issues a ubiquitous communication platform for frictionless data and value transfer between machines and humans that is secure, scalable and standardised may be a solution to this problem.

The IOTA framework is a relatively new Distributed Ledger Technology (DLT), a term synonymous with the recent blockchain paradigm. A distributed ledger is a database of recorded transactions between two parties that is shared and synced across multiple sites, institutions or geographies that is accessible by multiple people. The IOTA Foundation (a non-profit organization and creator of IOTA) defines it as the first distributed ledger technology solution built for the "Internet of Everything" that enables relationships between machines and humans through a network designed for exchanging value and data [6]. The core components of the IOTA framework are expanded upon in Section 2.2.

From a security perspective, DLTs provide accurate and immutable records for data exchanges and interactions between users, vehicles and infrastructure. They are more resistant than the traditional client-server architectures to the aforementioned cyber-attacks such as Sybil and man-in-the-middle attacks due to the removal of the centralised server as a single point of failure [7]. Once a transaction is confirmed and added to the network, it cannot be modified or tampered with. Each time a transaction is added to the network, a cryptographic problem needs to be solved, which requires some computational power. This is called "Proof-of-Work" (PoW). The IOTA network uses PoW to discourage spamming through adapting the difficulty of the cryptographic problem to be solved if a node tries to spam the network. This has the potential to reduce the likelihood of brute-force and Distributed Denial-of-Service (DDoS) attacks on Autonomous Vehicles (AVs) and their supporting infrastructure.

From a scalability perspective, the IOTA network is stated to operate in such a way that it is more performant the more nodes participate in the network. In essence, it gets faster as more users are added to the network [8].

From a standardisation perspective, the IOTA framework is open-source, feeless and can be run on any type of computing device that is connected to the internet. This is in contrast to the current state-of-the-art in V2X communication protocols. Already there are two protocols for V2X communications, namely the DSRC protocol developed in the US [9] and the ITS-G5 protocol developed to be the European standard [10], showing a divergence in approaches on a global level.

In recent years, DLT networks, particularly PoW networks have faced scrutiny over the energy cost of running their underlying networks. Each time a transaction is added to the network, a cryptographic problem is presented to the network to be solved or “mined” by a “miner”, which requires computational power and thus consumes energy. As a reward for this work, the miner that solves the problem first gets rewarded with cryptocurrency. Most notably, the Bitcoin network has been estimated to consume between 73 and 78.3 terrawatts-hours (TWh) per year due to this mining approach [11]. The IOTA network, by comparison, has no miners and all PoW is done on the node where the transaction originates, thus resulting in a drastic reduction in energy consumption to run the network. Sori *et al.* [12] classified the IOTA network as “exceptional” when comparing the network to other networks and payment protocols such as Bitcoin, Ethereum, VISA and Mastercard.

The IOTA framework has already been proven to work in a number of use cases, and this is further expanded upon in the Literature Review. However, as of September 2021 the IOTA foundation launched IOTA 2.0 in beta with a number of radical upgrades, including a fully decentralized network, more robust security features, marking an important milestone in the IOTA foundation history [13]. The IOTA foundation have also, as of 2021, introduced a number of key features and products such as smart contract capabilities, new communication protocols called “Streams” and identity access management tool called “Access” [14]. Smart contracts are digital contracts stored on a blockchain that automatically get executed when predetermined conditions are met [15]. Combining the IOTA framework with smart contract functionality and these other services may have potential for automating service and applications within the autonomous vehicle eco-system. As of today this space has been relatively unexplored.

1.3 Purpose and Scope

This research has a number of purposes. The main goal is to examine and demonstrate the benefits and limitations of the IOTA Framework for V2X communication. To be specific, this research aims to answer the following research question:

"Can the IOTA framework be used as a viable communication layer for secure and scalable data transfer for autonomous V2X applications?"

Four objectives were outlined to help answer the research question:

1) Compare DLT to the current state-of-the-art to traditional architectures.
2) Identify the benefits and limitations of the IOTA Framework for autonomous vehicle communication.
3) Quantify the ease of developing decentralized applications using IOTA framework.
4) Highlight future applications and areas for future research.

The scope of this research will be limited to a simple use-case scenario: an application that publishes data to the IOTA network, aggregates vehicle data and publishes messages to vehicles to warn about potential road hazards. Warning messages that are currently available in the OBU include heavy braking, wiper (high), traction control, severe bounce and antilock brakes. The IOTA Framework will act as a communication platform for the vehicles. The data that will be published to test the IOTA framework is the traction control warning. Once this data is published to the network, it will be aggregated and analysed to find anomalies in locations where traction control is activated. In theory, this should enable the fast detection of adversarial road conditions, enabling authorities to act accordingly.

The scope of this research will be limited to a python-based scenario simulation and the development of a lightweight pub/sub application to publish messages to the IOTA network.

1.4 Hypothesis

In order to examine the new IOTA framework and its applications in detail, the following hypothesis is proposed:

The IOTA framework can be used as a viable V2X communication layer that allows for secure and scalable OBU data transfer between autonomous vehicles using the IOTA network.

CHAPTER TWO

Literature Review

The following literature review examine four key areas; distributed ledger technology, the IOTA framework, V2X communication and the rationale for the chosen use case. A number of seminal papers in these areas were examined, along with recently published articles and technical documentation. It begins with Section 2.1, a general discussion of how DLT is playing a role in the advancement of the AV industry. Blockchain is the most widely used DLT currently, and this is expanded upon. The IOTA framework, while also considered a DLT, is different from blockchain in a number of key areas. Section 2.2 includes an in-depth analysis of these differences along with a discussion of the core IOTA technologies and products. In Section 2.3, V2X communication is discussed in detail. To understand how this messaging protocol could be integrated and what it would mean from a feasibility and an implementation perspective, the state-of-the-art in V2X communication is investigated. V2X standards are discussed as well as the technologies used to secure communications between vehicles and their surroundings. Finally, Section 2.4 expands on the rationale for the use case; transmitting OBU messages using the IOTA communication protocol. This section deals with why the use case was chosen and examines similar work done in the area.

2.1 Distributed Ledger Technology

The definition of DLTs is not an easily defined concept. Definitions can be wide-varying and often conflicting, depending on the author, audience and industry in which it is defined. Some definitions are more ontological with others being more technical.

Rauchs *et al* [16] defines DLT as a consensus machine; a system with multiple actors who agree on a set of shared data and its validity, in the absence of a centralized coordinator. In comparison to traditional databases, both distributed and centralized, DLTs key features are rooted in data integrity in an adversarial environment. It is a system of electronic records that enables a network of participants (nodes) to reach a consensus on the authoritative order of transactions, which are linked using cryptographic hashes and persisted across all nodes of the network. This multi-party consensus produces a ledger, which is the authoritative version of a transaction history.

In the financial realm, the European Central Bank defines DLTs as a technology that enables users to store and access information relating to one or more assets in a shared database of transactions and balances [17]. A transaction is a cryptographically signed authorised attempt to change the status of this database. It allows users to reach a consensus on a specific version of the ledger, meaning that with enough actors, there cannot be any manual alteration of the ledger. Cryptographic solutions with economic incentives replace the concept of central validation.

2.1.1 Blockchain as a Form of DLT

DLT has been around in concept since the mid 1990s, built on a thought experiment on a consensus mechanism called "The Byzantine Generals' Problem" created in 1982 [18]. In many cases the terms DLT and blockchain are used interchangeably. In some sense this is true, blockchain is a type (and most popular form) of DLT. Bitcoin, which is a cryptocurrency developed in 2008 under the pseudonym Satoshi Nakamoto [19], made use of the blockchain protocol and brought the technology into mainstream focus for the first time.

2.1.2 DLT in the AV Industry

Although research into DLTs has been increasing rapidly over the last ten years, the research within the connected and autonomous vehicles (CAV) space, seems to be lagging behind other industries such as the financial, healthcare and education.

Rathee *et al* [20] looked at using a blockchain framework for securing CAVs from smart device tampering by malicious attackers looking to compromise the communication channels of the vehicles. Using a blockchain framework, where vehicles operate as both nodes in the network, (much like the structure of today's VANETs[1]), each vehicle is

[1] VANET stands for vehicular ad hoc network which is a group of vehicles connected by a wireless network

aware of all valid actors and devices in the network. Any alteration or deletion of information to vehicle data or user data will come to the notice of other devices. This approach showed a 79% success rate in the detection of malicious attacks when compared to the traditional VANET architecture.

Pustisek *et al.* [21] highlight the need for novel Machine-to-Machine (M2M) communication paradigms to connect energy producers, consumers and providers. They state that blockchain transactions could be fundamental to energy trading applications and platforms. This paper highlights the possibility for the use of the Ethereum platform to build this trading application. They conclude by highlighting the abundance of additional service applications that could be built on top of this using the Ethereum platform including reservation of charge points, selection based on traffic conditions, battery status, charging intensity.

Indicative of the advance in the technology, five years since Pustisek *et al.* [21] outlined a conceptual model, Khan *et al.* [22] built on this idea by creating a fully-fledged P2P payment and energy trading system using IBM blockchain technology. This solution aims to reduce the level of human interaction and increase privacy, transparency and trust among EV participants. Scalability was also highlighted as another key benefit of blockchain technology, in this instance, optimal transaction confirmations of 825 per second were observed.

From a security perspective, Gupta *et al.* [23] explore the use of blockchain to increase the robustness of AV security to cyberattacks. The study proposes that the majority of solutions to current cybersecurity threats to AVs today are based on centralized hub-and-spoke architecture which creates a single point of failure and that blockchain-based solutions. Research challenges highlighted include system throughput, scalability, and proper authentication of nodes prior to joining the network.

Modern vehicles purport to have over a hundred million lines of code [24],which will need to be maintained and updated regularly. Baza *et al.* [25] designed a blockchain-based firmware update scheme for autonomous vehicles, utilising the decentralised architecture to use AVs to push updates to other required vehicles. Interestingly, with the use of smart contracts, the AVs get compensated by the manufacturers for participating through a rewarding system.

Ethereum is another open-source blockchain protocol second in popularity and similar to the Bitcoin protocol, but with the addition of smart contract functionality. Smart contracts are codified business rules that automatically execute on network nodes allowing the network to operate in a fully autonomous and decentralized manner [26].

2.1.3 Summary

In this section, the concept of DLTs was introduced. The concept of this technology is fundamentally different from the centralised hub-and-spoke architectures (server-client architecture) that have been used up to this point. It is such a paradigm shift that it is being hailed “Web 3.0” [27]. From initial literature research, DLTs, specifically blockchains have shown potential in their applications in terms of security and scalability. Similarly from a use-case perspective, blockchain technology has shown to have wide-varying applicability in the AV industry. While the IOTA framework is also considered a type of DLT, there were a number of design decisions that were made during its development that differentiated it from other blockchains. This will be discussed in the next section.

2.2 The IOTA Framework

The IOTA framework was created in 2015. The IOTA Foundation defines IOTA as “an open, feeless data and value transfer protocol”. It is based on DLT principles and was originally built specifically for the IoT industry. While also considered a DLT, its underlying ledger data structure is not based on a chain of blocks but rather a Directed Acyclic Graph (DAG) data structure. Coined by the foundation, “the Tangle” is a moniker for this DAG data structure on which the network is based [28].

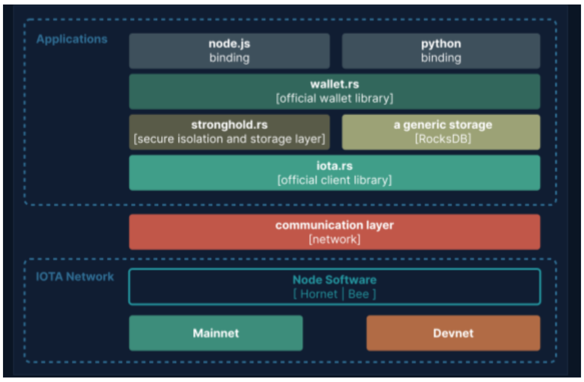


Figure 1: The IOTA Ecosystem [29]

At the core of all DLTs is a *ledger*, a *network of nodes* and *transactions*. In the following sections, the words transaction and message, as well as the words ledger and “the Tangle” are used interchangeably. These concepts are outlined in the below three sections.

2.2.1 The Tangle (The IOTA Ledger)

The Tangle is the ledger for storing these transactions in such a way that they become immutably and cryptographically linked in a tree-like graph (See Figure 2). This graph consists of vertices and directed edges and grows in only one direction (“Directed”) and vertices never directly or indirectly reconnect with themselves (“Acyclic”). IOTA takes advantage of this structure, combined with numerous cryptography techniques to create its ledger of transactions. Each vertex in the graph represents a transaction and each directed edge represents a transaction confirmation.

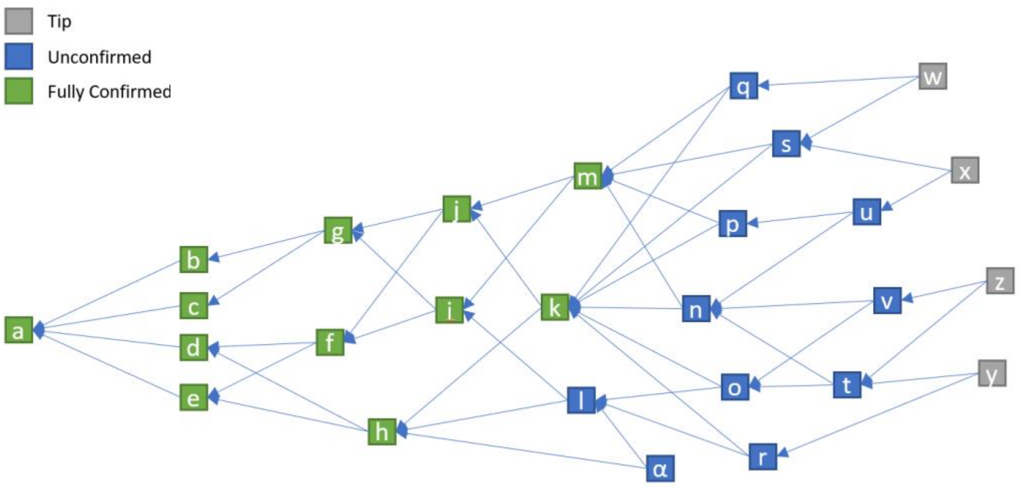


Figure 2: The Tangle Data Structure [30]

The main idea of the tangle is as follows; to create a new transaction on the Tangle (represented as vertices in Figure 2), users must work to approve two other transactions on the Tangle (represented as edges in Figure 2). All of this is done using the nodes on the network. Nodes use the Markov Chain Monte Carlo (MCMC) algorithm to randomly select a tip from the tangle. A tip represents unapproved transactions in the Tangle graph [26].

As the network is asynchronous, all participating nodes do not see the same set of transactions at any point in time. Therefore, it is possible that conflicting transactions will exist in the tangle. An example of this is if person A had 100 coins in total and sent 100 coins to person B and shortly after sent 100 coins to person C, before the first A-B transaction could be confirmed. This is a conflicting transaction and is called "double-spending". The job of the nodes is to decide which of these transactions "make the most sense" through consensus. The way in which consensus is achieved is through an algorithm called Fast Probabilistic Consensus (FPC) [31], whereby if a node detects a conflicting transaction, it will query other random nodes multiple times for their opinion. If a supermajority of nodes prefer one transaction, then the final consensus is 1 with high probability [31]. Transactions that do not meet the consensus of nodes get orphaned and are not confirmed.

Transactions have two properties – *weight* and *cumulative weight*. The weight of a transaction refers to how much PoW was done by the issuing node and can only have values in the set 3^n (1, 3, 9.., 3^n). A higher number representing a greater degree of work, and hence importance. Cumulative weight is the transactions own weight in addition to the sum of the weights of the transactions that directly or indirectly approve the transaction. For example, in Figure 3, the weight of transaction A, C, D and E is 1. The weight of F and B is 3, indicating more PoW was done by the issuing node. Also in Figure 3, F has a cumulative weight of 9 as it is directly and indirectly referenced by A, B, C and E which have weights of 1, 3, 1 and 1 respectively. Therefore the cumulative weight of F is 1 + 3 + 1 + 1 + 3 (own weight of F) = 9. Transactions with high cumulative weights are usually older, have more verifications and can be trusted with greater confidence [28].

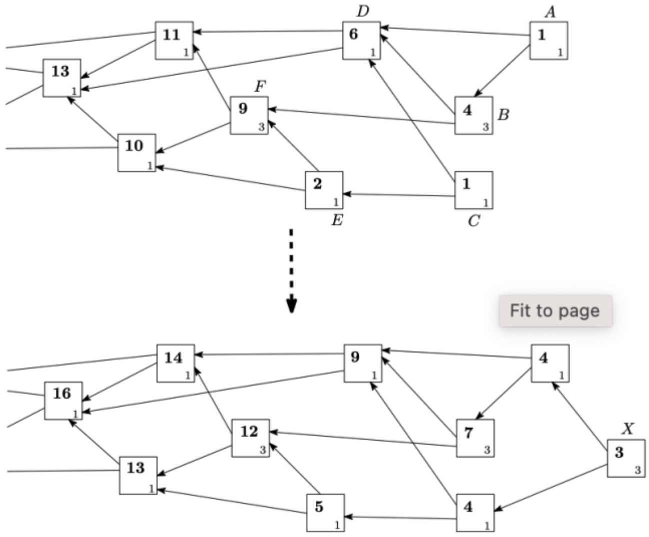


Figure 3: Tangle Transaction Cumulative Weights [28]

2.2.2 IOTA Nodes

Nodes are computers that provide the network computation and storage, and are connected in a peer-to-peer (P2P) manner. Nodes act as gatekeepers to the Tangle. As of December 2021, there are currently 327 nodes running the network [32]. Nodes in the IOTA network run the core software and have three main functions:

1) To validate incoming transactions and add them to the shared ledger
2) To enable read/write access to the Tangle

3) To store the ledger and keep it in sync with the rest of the network

Nodes relay information across the network using a gossip protocol. This involves participating nodes receiving messages from a neighbouring node and forwarding them to other neighbouring nodes. Using this gossip protocol allows all participating nodes to be aware of new transactions and updates to the ledger.

As the network scales, congestion becomes an issue, much like an internet server crashing if too much web traffic is directed at it. Blockchain technologies solve this congestion problem in a number of ways. Both the Bitcoin and Ethereum protocols have a similar solution, using miners as leaders to organise and validate blocks of transactions before they are added to the network ledger. As IOTA does not use blocks or miners to run the network, to solve this problem, nodes employ the IOTA congestion control algorithm (ICCA) [33]. This algorithm uses a scheduler to determine which transactions are written to the ledger, a blacklister function to censor malicious nodes and a rate setter to adjust the rate at which messages can be added to the network. This makes nodes resistant to DDoS attacks – as it does not allow a single node to spam the network with messages.

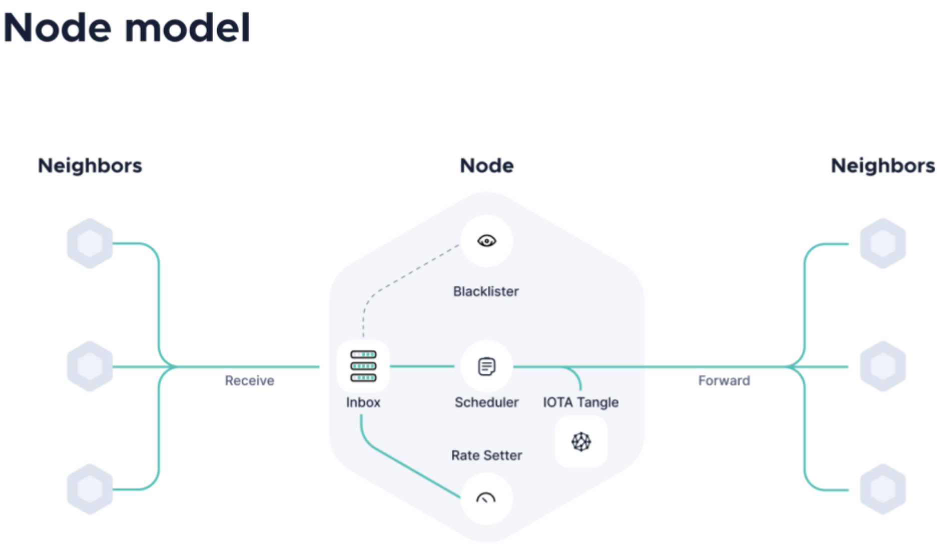


Figure 4: An IOTA Node [33]

As IOTA began with IoT in mind, these nodes were designed to run on all types of devices. Sori *et al.* [12] measured the computational cost of validating a transaction on an

IOTA node, and gave it an exceptional rating in comparison to other protocols such as Bitcoin, Ethereum and Visa.

Devices do not necessarily have to run as *full nodes* (nodes that validate transactions and store the ledger state) to contribute to the network; devices can connect to any full node as an endpoint using the IOTA client libraries. These are called *light nodes*. Distributing these connections among full nodes becomes an issue for network optimisation. In recognising this limitation, Hellani *et al.* [34] created a load balancer for IOTA light nodes balance message approval requests among full nodes based on number of current active connections, managing to improve balancing of data traffic among nodes in the network.

In the context of V2X technologies, vehicles could operate as either a light node or a full node in the IOTA network, allowing themselves to submit transactions to read and write messages to the tangle.

2.2.3 IOTA Transactions (Messages)

A transaction, or message to use the IOTA term, is an information object broadcast and gossiped around the network to enable the transfer data or value (or both) between two participating entities within the network. Unlike blockchain technologies like Bitcoin and Ethereum, adding messages to the Tangle ledger is feeless. Blockchain mining is computationally and financially expensive. In comparison to these aforementioned blockchain technologies where users can pay a transaction fee incentivising miners to include their messages on the blockchain ledger, IOTA does not use miners, hence no transaction fees, making micro-transactions between entities economically viable.

Message objects are created on devices using IOTA client libraries and sent to network nodes for validation. A message object has a number of requirements, most notably the message cannot exceed 32KiB, it must be signed with the devices private key and must include in its payload a reference to between 2-8 parent message IDs already confirmed on the tangle. The node selects these messages IDs using an algorithm called Uniform Random Tip Selection (URTS), and provides them to the client. Once the node receives the formatted message from the client, it has to solve a cryptographic puzzle in the form of a hash function, to produce a hash value that meets the requirements defined by the IOTA. Korotkyi *et al.* [35] tested the speed of producing this hash value by an IOTA node using hardware accelerators and showed transaction confirmation times of 0.42 seconds. This is orders of magnitudes faster than the Bitcoin transaction time, which takes 25 minutes on average to confirm transactions [36]. As the rate of messages being sent to nodes for validation increases, the hash function difficulty also increases. This makes it exponentially harder to produce a valid hash value, creating a natural DDoS and Sybil attack prevention for the network nodes.

Value transfers are enabled by transferring IOTAs native cryptocurrency called MIOTA. MIOTA (or 1 million IOTA tokens) can be bought using other cryptocurrencies or *fiat* currency[2]. There is a fixed amount of IOTA tokens in circulation, and at all times, the sum of all tokens recorded on the ledger must equal the original amount minted when the network was created. This is managed by the network nodes and ensures that IOTA tokens cannot be double-spent or forged.

Data transfers work in much the same way as value transfers, without the exchange of IOTA tokens. The ability to transfer data for free is a major differentiator between them and other DLT technologies, the IOTA foundation claims [33].

2.2.4 IOTA Products

In the past two years, the IOTA Foundation have released a number of different products built on top of the core components of framework to expand the eco-system and make it easier for developers to build new decentralised applications. In this section, two products called IOTA Streams and IOTA Identity are discussed.

2.2.4.1 *IOTA Streams*

IOTA Streams is an open-source message-oriented cryptographic protocol for decentralized data encryption and streaming. The final alpha version of this product was released on October 15th 2020 [37]. It allows devices to communicate securely and

[2] Fiat is a term used in the cryptocurrency industry to define a currency backed by a government or economic bodies e.g. US Dollar, Euro.

privately on the Tangle, and in theory ensuring communication data is stored in an immutable, decentralized and tamper-proof way on the ledger. Streams are comprised of two roles: Authors and Subscribers. An Author can create a channel and share session key information with Subscribers allowing both parties to interact privately and securely. IOTA Streams is implemented using the Rust language and has multiple bindings including C and NodeJS [38].

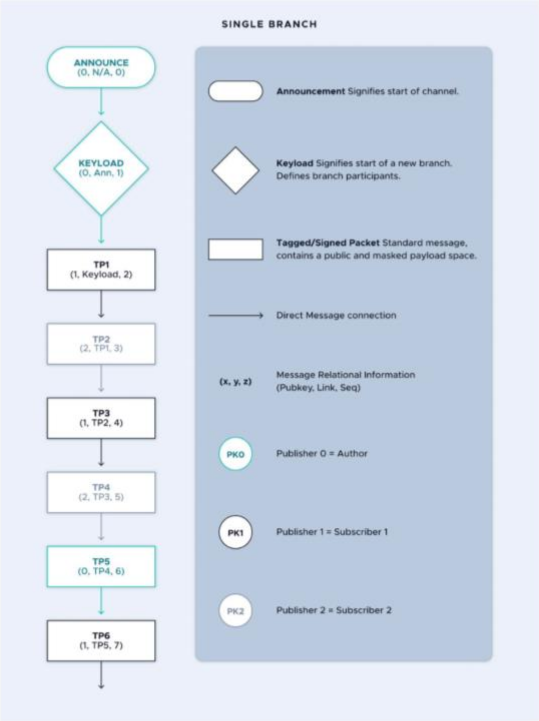

SINGLE BRANCH
ANNOUNCE (0, N/A, 0)
KEYLOAD (0, Ann, 1)
TP1 (1, Keyload, 2)
TP2 (2, TP1, 3)
TP3 (1, TP2, 4)
TP4 (2, TP3, 5)
TP5 (0, TP4, 6)
TP6 (1, TP5, 7)
Announcement Signifies start of channel.
Keyload Signifies start of a new branch. Defines branch participants.
Tagged/Signed Packet Standard message, contains a public and masked payload space.
Direct Message connection
(x, y, z)
Message Relational Information (Pubkey, Link, Seq)
PK0
Publisher 0 = Author
PK1
Publisher 1 = Subscriber 1
PK2
Publisher 2 = Subscriber 2

Figure 5: The IOTA Streams Framework Architecture [39]

Figure 5 demonstrates the process flow of IOTA Streams framework. A channel gets created and announced by an author, the author then creates a new branch with a keyload identifier, to which the channel author can publish messages. Subscribers can request to join the channel using the announcement link. Once the subscription has been processed, both authors and subscribers can publish encrypted messages to the channel and listen for messages from the author or other subscribers. Messages that get sent using the IOTA Streams protocol get packetized into IOTA transactions before getting sent to an IOTA node for attachment to the Tangle.

To date, there has been no major studies on IOTA Streams, due to the product being in its nascence. Other studies have been conducted using the legacy version of IOTA Streams called Masked Authenticated Messaging (MAM). Lamtzidis *et al.* [40] created a distributed sensor node system to collect store and process data using MAM and IOTA protocol to enable M2M transactions of value and data. However, MAM has been criticized for a number of limitations, which led to the creation of IOTA Streams. This research will focus on the IOTA Streams framework to test the capabilities of IOTA as an encrypted data transportation layer for vehicular communications.

2.2.4.2 *IOTA Identity*

IOTA Identity is a decentralized digital identity service. The service implements the W3C Decentralized Identifiers (DID) standard with the idea that it can be used to create and authenticate digital identities [41]. There are many instances where using this service could prove useful in the AV industry. As an example, prior to the release of this product, multiple papers were published in the V2X space regarding the use of IOTA for streamlining Public Key Infrastructure [42, 43]. These studies bootstrapped the IOTA framework to build a product that operates in much the same way. Further research in this area could focus on extending and streamlining these studies to include the IOTA identity product.

2.2.5 Current IOTA Use Cases

The IOTA framework has already demonstrated value in a number of areas. In [44] a DLT-based charging and billing mechanism for EAVs was proposed to demonstrate machine-to-machine (M2M) micropayments for electric vehicles. The study conceptualised the charger-to-vehicle relationship using a Raspberry Pi and a temperature sensor; and created a framework that demonstrated the viability of using the Tangle for transferring value from one machine to another. In [45] the authors examined the Tangle as a viable alternative to the shortcomings of traditional blockchains for vehicular applications, namely large transaction confirmation times, concluding smaller transaction delays as well as high performance using the encryption mechanism provided by the Tangle.

From an implementation perspective, Jaguar Land Rover, in collaboration with the Mobility Open Blockchain Initiative (MOBI) have demonstrated a system using the IOTA framework that allows drivers to earn cryptocurrency by allowing their cars to report useful road conditions including potholes and traffic congestion to authorities and navigation providers [46]. Another interesting project based on the IOTA framework was carried out by the research institute ElaadNL who have created “the first ever IOTA-based EV charging station” [47]. This research group built both the charging station hardware as(information which would traditionally be stored on a centralized server) was investigated. Both studies proved that the framework was lightweight enough to create a decentralized and scalable access control framework solution for IoT devices.

2.2.6 Summary

In this chapter, the core technologies and products created by the IOTA Foundation were discussed. The approach that was taken to create the tangle is fundamentally different to many other DLT technologies operating in this space. As the technology is only a few years old, it is a relatively new and unproven at scale. Many of the case studies examined in this section were proof-of-concept and small scale implementations. That being said, each of the case studies successfully demonstrated implementations of the IOTA technology in the autonomous vehicle industry. However, as IOTA is rapidly developing new features, including IOTA Streams, IOTA Identity and IOTA Smart Contracts, there have been no studies to date examining the potential applications of these for V2X communication. This research will look at using IOTA Streams as a V2X communication protocol using the underlying tangle technology.

2.3 V2X Technology

V2X technology is synonymous with connected vehicles. It defines as the wireless technology that enables data exchange between vehicles and their surroundings. Without the ability to connect vehicles to each other and their surroundings in a secure, private and low-latency manner, applications of connected vehicles will be limited. In this section V2X standards, secure V2X communication and enabling technologies are examined in detail.

2.3.1 OBU

Modern vehicles use an On-Board Unit (OBU) to communicate with other vehicles that are also equipped with an OBU and communicate with the infrastructure (V2I) by connecting to Road Side Units (RSUs) and other networks (V2N). Host vehicles (HVs) and remote vehicles (RVs) communicate using Basic Safety Messages (BSM), which are standardised packets of data transmitted and received between vehicle OBUs. These messages are decoded and used for multiple applications including predicting crashes and alerting drivers of any imminent dangers. This standard ensures that all vehicles can "speak the same language", which will enable developers and manufacturers to develop safety applications to reduce fatalities and crashes [48]. Typically, an OBU has a GPS/GNSS receiver, a Dedicated Short Range Communication (DSRC) radio for reception and transmission, a processor, and obtains vehicle data through interfacing with modules such as the CANBus, Security, Ethernet or GPS. Figure 6 shows a breakdown of the main OBU components for a DSRC-based system.

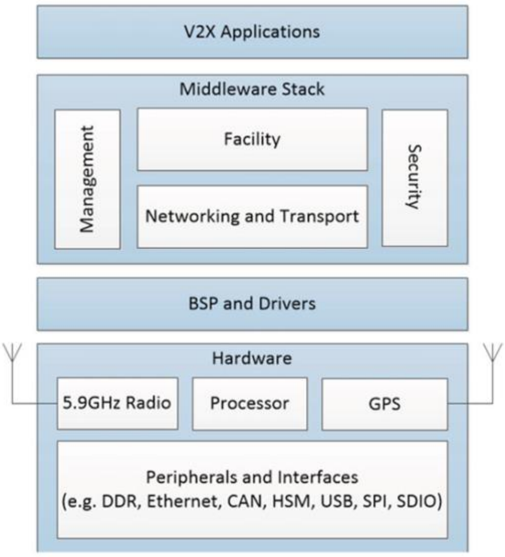


Figure 6: A DSRC-Based OBU [48]

2.3.2 V2X Standards

As with many technologies, the approach to V2X standards and protocols has varied. Two major standards have emerged. The first protocol, DSRC originated when the US Federal Communications Commission (FCC) licensed 75MHz of bandwidth in the 5.9 GHz region for use in automotive applications and developed the standard based on the IEEE802.11p physical access layer standard developed for vehicular networks [49]. A similar standard was adapted by the European Telecommunications Standards Institute (ETSI) called ITS-G5, which also operates at the same frequency. The second and more recent standard developed is the Cellular-V2X (C-V2X), which is a new approach built for the advent of 5G-enabled devices. There are two schools of thought in the automotive industry about the best standard for V2X communication; DSRC and C-V2X.

2.3.3 DSRC vs C-V2X

DSRC allows for *direct* communication (i.e. it does not use any cellular infrastructure) between OBUs and RSUs only. This makes it easy to secure, and very low-latency. When the DSRC protocol was originally developed, the state-of-the-art cellular technology was 3G which could not provide the latency required for high-speed and secure communication between vehicles, as it had to pass via a cellular tower, therefore was not considered an option for this application. Since then, cellular technology has evolved over two radical generations, namely 4G-LTE and 5G. For context, 4G is approximately 500 times faster than 3G, and 5G is purported to be 100 times faster than 4G, with higher peak capacity, larger bandwidth and lower latency [50]. This has allowed the cellular C-V2X standard to emerge as a contender, however, it is a relatively new technology with the first specification released in 2016 and earliest trial only taking place in 2017 [51]. For reference, Figure 7 gives a conceptual overview of the two system architectures.

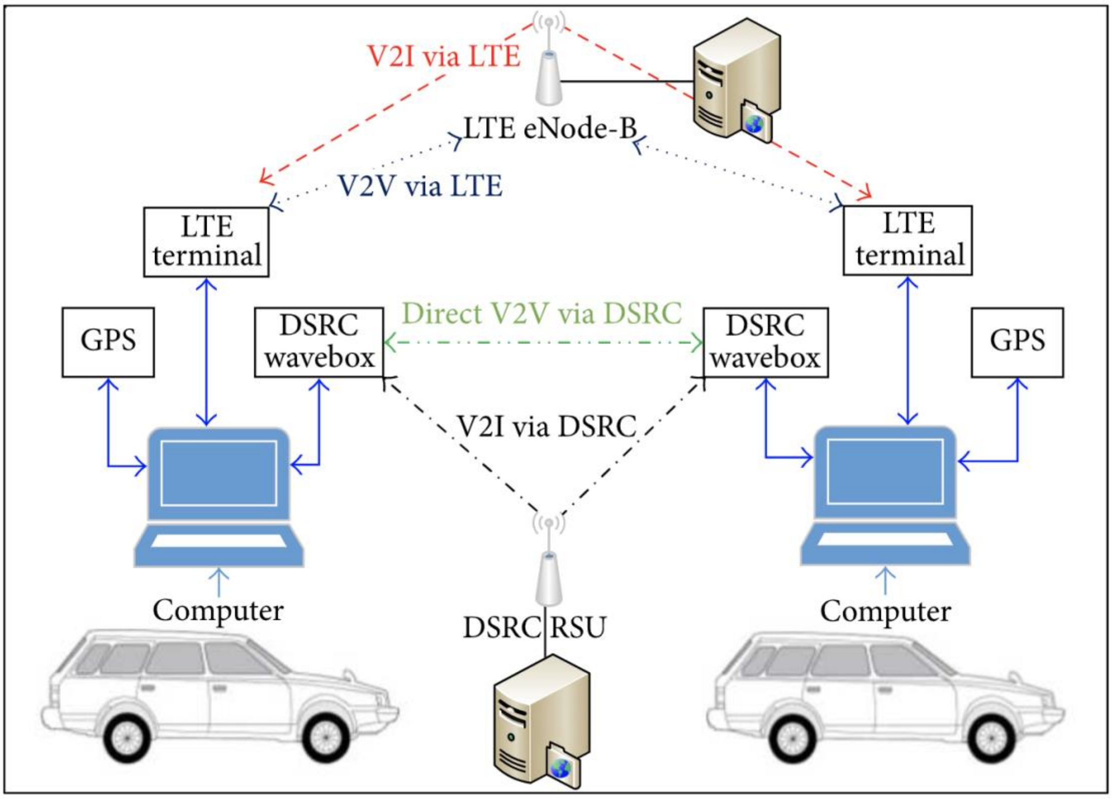


Figure 7: DSRC Versus Cellular Concept [52]

More recently, the Third Generation Partnership Project (3GPP) 4G Release 14 allowed for direct device-to-device communication [53]. In the context of V2X communication, this meant that cellular networks could be used in the same way that traditional DSRC operates, by jumping between devices *without* first hitting the cellular tower for low latency mission-critical vehicle sensor connectivity.

Mannoni et al. [44] completed a study comparing the two V2X systems. This study showed that in general C-V2X performed better than its older ITS-G5 counterpart. Interestingly, however, this study showed that this is only the case when there are less than 150 users per km^2 and after this the performance of the C-V2X system deteriorates faster than the ITS-G5 system, indicating that there is no clear winner. A key performance indicator for V2X system performance is latency, however this study was inconclusive in naming the optimal solution as it is highly dependent on operating range and user density. Similar studies evaluating the two systems were undertaken [52, 54] with the former showing that in 2017 DSRC outperforms C-V2X and the latter contradicting that opinion showing a preference for C-V2X in 2019.

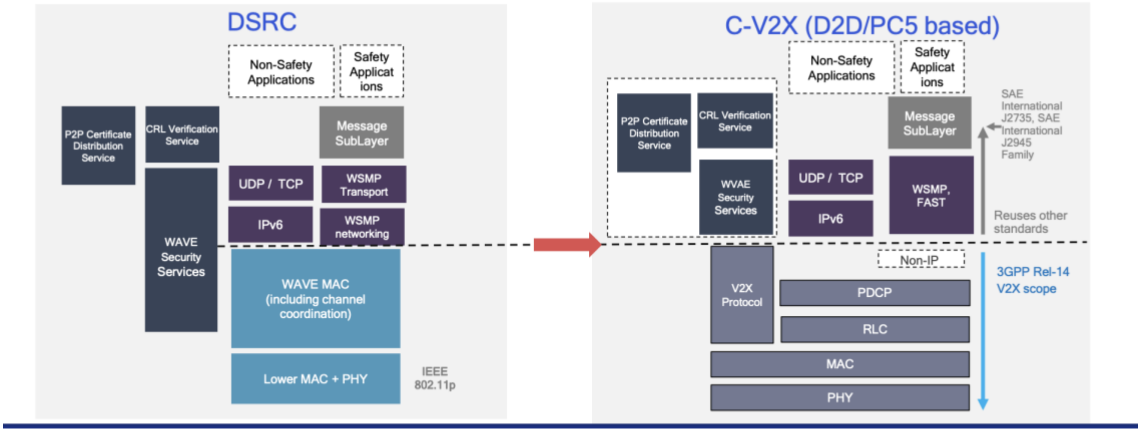


Figure 8: DSRC Versus C-V2X Architecture Comparison [55]

In relation to IOTA and the use case for this research, passing vehicle data from the OBU to the IOTA network is not considered a mission-critical application. Both C-V2X and DSRC based systems offer TCP/IP and IPv6 connections which can be used to connect the IOTA network via the OBU.

2.3.4 Secure V2V Communication

Securing communications is one of the most important elements in V2X communication. The leading technology solution to date is the Security Credential Management System (SCMS) [56] developed by security and automotive experts alongside the US Department of Transport in 2016. Gaining access to a vehicles OBU allows a malicious actor in the network to gain full control of the vehicle. Once a BSM is received from a remote vehicle, the vehicles must establish that a message has come from another trustworthy certified onboard device. Due to the latency requirements of mission-critical V2X systems (sometimes within 5ms) validating requests using a third-party is not possible. Therefore, pre-validated certificates, called pseudonym or ephemeral certificates are loaded onto these devices and can be used to quickly validate BSMs as they are received.

SCMS is used to secure communication between devices [56]. Vehicles need to be able to make sure that the BSM is authentic and from another certified on-board device. They also need to be able to ensure that the message was not altered during transmission. If a false message was inserted, this could influence applications, cause crashes and a host of other malicious behaviours. Each participating vehicle and infrastructure node that sends and receives BMSs is issued a digital certificate and this is used to create a secure communication channel between devices. All devices sign the BSM digitally and then the receiving vehicle checks the signature before acting on it to make sure it is legitimate.

The requirements for secure V2X communication outlined in [48] are as follows:

- Message Integrity – make sure the message was not changed.
- Message Authenticity – make sure the message is legitimate.
- No PII data gets broadcast to the network.
- No data that allows for long-term tracking/ data mining of our vehicle gets broadcast to the network.
- Certificates can be actively and passively revoked
    - Active is when devices are informed about no longer trustworthy devices
    - Passive means untrustworthy devices no longer can update their credentials

SCMS uses private key infrastructure (PKI) principles and cryptography to manage these issued certificates and maintain the security requirements above. It is designed to partition functionality and distribute it among the system components, separated organizationally to avoid insider attacks. This organizational separation prevents a single organization in the SCMS from linking certificates to specific devices. An exhaustive description of SCMS can be found in [56].

However, SCMS, like many of the components of V2X technology, is a relatively new and unproven system at scale.

Tesei *et al.* [42] proposed a DLT-based vehicle public key infrastructure based on the current SCMS for V2X communication. The goal of this research was to use IOTA as a DLT implementation to eliminate the single point of failure and scalability issues that exists in the form of Certificate Authority (CA). SCMS was designed to obfuscate data in such a way that no one organisation can link a certificate to a specific vehicle, which proves cumbersome in practice. IOTA implementation used to offer Masked Authenticated Message (MAM) channels that nodes could use to communicate anonymously. Each channel has three modes – Public, Private and Restricted. The Restricted channel is protected by a key, which the channel owner can use to authorise channel subscribers. When a new vehicle is added to the network, it negotiates a symmetric key with the CA and instantiates a secure communication channel where certificates can be registered and updated. Once registered, the CA records a hash of the issued certificate and sends the link to the vehicle, which can be used to sign messages so other vehicles can validate it on the IOTA ledger as proof that the certificate was issued.

A follow-on study on certificate revocation using IOTA was presented by Tesei *et al.* [43]. This research was focused on replicating the Resolution Authority (RA) and Misbehaviour Authority (MA) elements of the SCMS using IOTA framework. The RA validates and processes requests from devices and the MA processes misbehaviour reports to identify misbehaving or malfunctioning devices, revokes access and adds them to a Certificate Revocation Link (CRL). Once a vehicle is found to be compromised by the MA, this information is published on the IOTA Tangle ledger using a zero-value transaction. This solution managed to reduce the vulnerability window (i.e. time between compromised device and certificate revocation) down to 18.57 second. This is markedly lower than the vulnerability window in the current SCMS standards, which can take up to three months to revoke a certificate.

2.3.5 V2X for Non-Safety Critical Applications

It is worth noting that for the purpose of this research, using the IOTA protocol for autonomous vehicle communication is not being considered for “mission-critical” applications currently handled by DSRC/ C-V2X. This is due to the inherit network latency of the IOTA protocol which is built using internet technologies and is not anticipated to be comparable to the latency of DSRC technologies. This is because the two approaches are fundamentally different, and have different use-cases. DSRC is ultra-low latency, short range and infrastructure-less (i.e. data gets transmitted directly between vehicles using radios) and the other uses internet protocols and infrastructure to send and receive data between two points. As the use of autonomous vehicles become more ubiquitous in the coming years, it is estimated that approximately 30% of V2X applications will be non-safety related by 2027 [57]. Therefore there is merit in exploring new ways that vehicles can communicate for non-safety-critical V2X applications, securely, ubiquitously and at scale. This research will deal with examining the IOTA protocol within this context.

2.3.6 Summary

V2X communication is, from an automotive industry perspective, a newer technology. There have been a number of major advancements in this area over the past number of years including the development of SCMS, C-V2X as well as DSRC improvements. This has largely been helped by the advancement of 5G cellular technologies, allowing for much lower latency and larger bandwidths in which vehicles can communicate. However, 5G is still a new technology. This is not the only issue. For one, the development of competing standards between the US and the EU has the potential to hinder progress in the area. Also, the convoluted, inefficient and centralised structure of the SCMS PKI highlights the needs for an alternative solution to private key management. Allowing compromised edge devices to operate for months after an anomaly has been detected highlights this issue. A decentralized and trustless network to manage message integrity, authenticity and anonymity for V2X communications could be a viable solution to some of these issues.

2.4 Conclusion

DLTs are an exciting new approach to decentralized applications and communication. In comparison to the financial industry where DLTs first emerged, the use of this technology has been relatively unexplored. DLT offers a number of unique advantages over centralised hub-and-spoke network architectures including transparency (as the ledger is public), traceability, data immutability, resistance to cyber-attacks like DDoS as well as the ability to create decentralised autonomous organisations using smart contracts. However, these advantages come at a cost. DLTs, in particular the ones that use PoW algorithms consume significant amounts of energy during the mining process. Similarly, scaling some DLTs has proven to be challenging, for example the Bitcoin and Ethereum networks with high transaction fees as these networks become congested.

IOTA was designed to alleviate a number of the drawbacks of traditional blockchains. With the exclusion of miners in the process, this drastically increases the throughput rate of transactions, enabling device communication. It also drastically reduces the environmental cost of running the network. It is also argued that the process of mining blocks was included in blockchains for a reason, and its exclusion makes the decentralized network less secure. It has also yet to be proven at scale and adoption of the technology seems to be lagging. There are a small number of nodes (<500) globally running the network. However, recent developments to improve the core technology and create new products signals a push for increased adoption and encouraging developers to create new products using the IOTA framework.

V2X communications has a number of potential applications that could drastically improve road safety. The generational improvements of cellular technology over the past few years to reduce latency has enabled new opportunities for V2X communication that up to now were not possible. Security is a seen as key concern. A malicious device or node in a vehicle network could create a number of dangerous situations for road users. The SCMS is an extensive PKI system, designed to provide anonymity, organisational separation and unlinkability of devices participating in V2X communication to maintain integrity and security. However, the research suggests that maintaining the integrity and authenticity of device certificates is inefficient. A number of studies presented in the literature review show potential in using DLTs to improve this process.

To conclude, each of the technologies discussed in this paper are relatively new and are in their own stages of rapid development. The research suggests that many of the current limitations and issues with V2X technologies could benefit from the value proposition of DLTs; technology that is secure, scalable and standardised. The research however, is not universally conclusive on this and there is still much to be researched.

CHAPTER THREE

Research Design

3.1 Introduction

To recap on the research question/ hypothesis:

“The IOTA framework can be used as a viable V2X communication layer that allows for secure and scalable data transfer within the autonomous vehicle environment using the IOTA network.”

To answer this research question, the research was decomposed into topics and sub-topics that provided enough coverage of the IOTA framework to enable us to answer the research question. Multiple research approaches were evaluated that holistically evaluate open-source software (OSS) to decide what these topics would be. Xiaozhou et al. [58] examined the factors and metric to select open source software components for integration within the software industry and used the following topics as key to OSS adoption: *Community Support and Adoption, Documentation, License, Operational SW Characteristics, Maturity, Quality, Risk (Perceived risks), Trustworthiness*. Zhao *et al.* [59] carried out a systematic empirical study identifying indicators for evaluating open-source software (OSS) from numerous papers over the last 20 years. From this, five types of indicators commonly used to evaluate were found. They were: *code, license, popularity, developer and sponsorship*. This research conducted was largely quantitative and focused primarily on data extracted from online repositories such as GitHub and GitLab. It also cited another more common evaluation perspective to assessing OOS, broken into four indicators:

1) Quality – software’s ability to user’s needs or expectations in use.
2) Reliability – the probability that OSS can maintain unobstructed operation in the pre-scribed tests.
3) Maturity – technical or application characteristics that can be achieved
4) Vulnerability – the existence of defects in the software

As demonstrated, there are various ways to quantify OSS. As the hypothesis for this research pertains to the autonomous vehicle and its ability to act as a V2X communication protocol, as well as the scope of this research being limited for this research, these headings were consolidated and combined into the following topics to be used as the basis of this study.

#	Topic	Sub Topic
1	Quality	Network Latency
		Usability
		Documentation
2	Reliability	Network Uptime & Availability
3	Security	Trustworthiness & Vulnerability

Table 1: Research Topics and Sub Topics

The rest of this chapter will discuss the approach to designing the research around the five sub-topics within the context of the three main topics. The aim was to provide quantitative and qualitative data to facilitate a discussion on the IOTA framework and its potential applications in the autonomous vehicle industry. The “Research Onion” approach was followed to structure the design of the research. The following section breaks down the three topics of quality, reliability and security and how the research was designed around them.

3.2 Research Philosophy

The first step in research design was to decide the research philosophy. This enabled the definition of the set of beliefs on which this research is based and guide future research design decisions. There are two main points of view; ontological and epistemological. Saunders *et al.* [60] define ontological research as being “the researcher’s view of the nature of reality or being” and epistemological research as being “the researcher’s view regarding what constitutes acceptable knowledge”. Fundamentally, a new technology (IOTA Framework) was being evaluated for its potential application within an industry, therefore this research was be ontological (based on reality). Four of the main research philosophies were examined – positivism, realism, interpretivism and pragmatism. To decide on the most apt research philosophy, the research topics defined in the previous section were revisited.

#	Topic	Philosophy	Data Collection
1	Quality	Positivism and Interpretivism	Quantitative + Qualitative
2	Reliability	Positivism	Quantitative
3	Security	Positivism and Interpretivism	Quantitative + Qualitative

The study of our topics and research question suggested a mixed philosophical approach. Saunders *et al.* [60] suggests that if the research question does not unambiguously suggest either a positivist or interpretivist philosophy, adopting the position of the pragmatist makes the most sense. Data collection techniques most often used for pragmatistic research are both qualitative and quantitative. Therefore this research will adopt a pragmatic philosophy.

3.3 Research Approach

The next phase of the research design was to decide the research approach, of which there are two main options – deductive and inductive research. Saunders *et al.* [60] states that defining a research approach is critically important as it enables a more informed decision about research design, and outlines the differences in the two approaches. Deductive research is broadly defined as scientific research; the process of determining causal relationship between two or more variables in a deducted hypothesis. Quantitative data is most often used with this approach. Induction involves building theory from a less rigid methodology. It allows for context and more often uses qualitative data over quantitative. Existing data on the subject is often limited with inductive research.

As previously defined, to test the research hypothesis, various quantitative and qualitative data will be required to test the three topics of quality, reliability and security of the IOTA OSS. Where possible, hypotheses within these topics that can be tested using purely quantitative will use a deductive approach. Other hypotheses within these topics that cannot be explicitly proven through quantitative data, such as usability and documentation, will adopt an inductive approach and use qualitative data. These hypotheses will be combined together to give the overall picture. Therefore defining the viability of OSS could be done through simply a deductive approach so a combined research approach was required.

3.4 Research Purpose, Plan and Strategy

3.4.1 Research Purpose

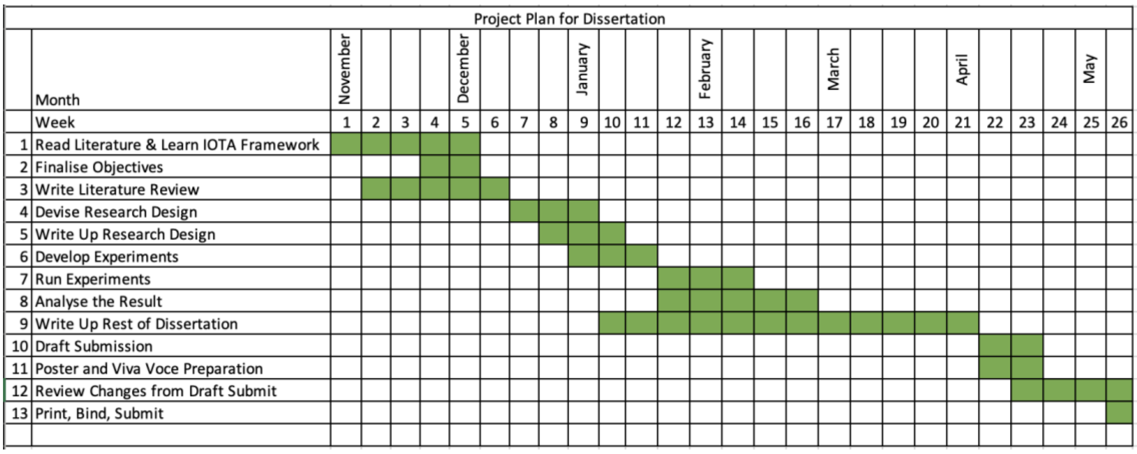
The research question and objectives were used to define the purpose of the research and as the basis for designing the research strategy. The research question is as follows:

"Can the IOTA framework be used as a viable communication layer for secure and scalable data transfer for V2X applications?"

Understanding the purpose of the research project i.e. is it descriptive, explanatory or exploratory, or a combination of all helped guide the design of the research strategy. Saunders *et al.* [60] gives general definitions of the three: exploratory research is a means of generating new insights by asking questions, descriptive research is the portrayal of persons, events or situations and explanatory research is figuring out causal relationships between variables. Again, as the research topic are multi-faceted, no distinct research purpose emerged. However, the research question is centred on determining the viability of OSS for a particular application, it will be mostly descriptive followed by exploration – generating data from experiments using the IOTA technologies as well as aggregating other recent studies on IOTA, and then exploring these to generate new insights.

3.4.2 Research Plan

Other factors considered during research strategy design were time and data constraints. For time, a research plan was followed, outlined in Figure 9 below.



Project Plan for Dissertation

	Month	November				December				January				February				March				April				May	
	Week	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
1	Read Literature & Learn IOTA Framework	🟩	🟩	🟩	🟩	🟩																					
2	Finalise Objectives				🟩	🟩																					
3	Write Literature Review		🟩	🟩	🟩	🟩	🟩																				
4	Devise Research Design							🟩	🟩	🟩																	
5	Write Up Research Design								🟩	🟩	🟩																
6	Develop Experiments									🟩	🟩	🟩															
7	Run Experiments												🟩	🟩	🟩												
8	Analyse the Result												🟩	🟩	🟩	🟩	🟩										
9	Write Up Rest of Dissertation										🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩					
10	Draft Submission																						🟩	🟩			
11	Poster and Viva Voce Preparation																						🟩	🟩			
12	Review Changes from Draft Submit																							🟩	🟩	🟩	🟩
13	Print, Bind, Submit																										🟩

Figure 9: Research Plan

Access to data was also considered. For some parts of the research, data will be generated from interacting with the IOTA technologies and discussion drawn from that. From the research plan, there was an eight week period to design, run and evaluate the results of the research.

3.4.3 Research Strategies

Following the approach from Saunders et al. [60] now that the research purpose and plan were defined, a number of research strategies were explored including: *experiment, survey, case study, action research, grounded theory, ethnography and archival research*. There were a number of factors that determined how the research sub-topics from section 3.1 would be studied. Some of the research strategies mentioned were more suitable for the purpose of this research. For example, as the viability of a new technology is being studied, and the technology is open-source, tests could be designed and executed to generate quantitative data on the performance of the software, in particular network latency, network uptime and availability. Therefore the preferential research strategy was an experimental approach. For determining the usability of IOTA, a qualitative study of its users was required, and so a survey of this population was the most suitable research strategy.

The final topic that had to be researched was security. As time was limited, as well as expertise in the area of decentralized application security, a review of data from existing literature was chosen as the most suitable research strategy.

Therefore the research strategies for all the sub-topics are outlined in Table 2.

Research Topic	Sub Topic	Research Strategy
Quality	Network Latency	Experiment
	Usability	Survey
Reliability	Network Uptime & Availability	Experiment
Security	Trustworthiness & Vulnerability	Secondary Data Analysis

Table 2: Research strategies for each sub-topic

3.5 Techniques and Procedures

Code for each of these experiments can be found at:
https://github.com/jameseoconnor/meng-project-iota-saev

3.5.1 Quality - Network Latency

In order for the IOTA protocol to be useful for autonomous vehicle communication, the speed of end-to-end communication is an important metric in assessing what type of applications it can be used for. For mission-critical applications, due to latency requirements the main form of V2V communication is based on direct short-range wireless communication. These channels have ultra-low latency requirements (between 5-100ms latency). However, as previously stated in the literature review, this research is not intended to compare the IOTA protocol to the network latency of short-range wireless communication. Instead, this research is focused on the use of the IOTA protocol as a viable communication protocol for non-mission critical applications. A more useful comparison is between the IOTA protocol and a popular request-response software architecture styles such as REST or SOAP that might be used to develop such an application in the absence of an alternative. Therefore to test the network latency against a benchmark, two simple applications will be developed, one using a RESTful framework benchmarked against another using the IOTA framework. Each application will send a simple message and await a response. Packets of timestamped data of varying sizes will then be transmitted and the Round Trip Time (RTT) will be measured for both applications. This is the duration in milliseconds (ms) it takes for a network request to go from a starting point to a destination and back again to the starting point [61].

Designing the Network Latency Test Applications

The overall architecture for the network latency experiment is outlined in Figure 10. A t3 medium Linux EC2 instance was launched in the Northern California Amazon Web Services (AWS) availability region. Security groups were added to allow public access to the EC2 instance. An IOTA node was installed on the EC2 instance, enabling read/write access to the IOTA Tangle. There are publicly availably IOTA nodes that can be used but are located in Germany and are behind load balancing machines. Therefore for consistency a dedicated node was created for this research at http://54.177.214.21:8081/.

The first application was developed using NodeJS and the bindings for the IOTA Streams client libraries. This application:

1) Creates an IOTA streams author instance on the client machine for the IOTA network and announces author channel to the network
2) Creates a subscriber instance on the IOTA network on the client machine and subscribes to the newly created channel that has just been announced.
3) A random bytes payload is generated by the application which contains a UNIX timestamp $t1$ of when the message was sent.
4) Subscriber instance sends the payload to the IOTA node to be added to the Tangle.
5) Author polls the network for the newly created message from the subscriber.
6) Once the payload from Step 4 is received by the author, the server calculates the time between the current UNIX timestamp $t2$ and $t1$ from the subscriber payload.
7) The RTT from subscriber to author can then be calculated as $t2 - t1$.

A second NodeJS application was developed and deployed on the same machine. This application worked as follows:

1) The client application creates a HTTP POST request
2) The client sends a message to the server application. A random bytes payload is generated by the client application which contains a UNIX timestamp $t1$ of when the message was sent.
3) The server application accepts the HTTP POST request at the endpoint http://54.177.214.21/post/

4) When the message reaches the server the server calculates the time between the current UNIX timestamp $t2$ and $t1$ from the request body.

5) The server returns a HTTP response to the client machine containing the value $t2 - t1$ as the RTT for the message to be delivered.

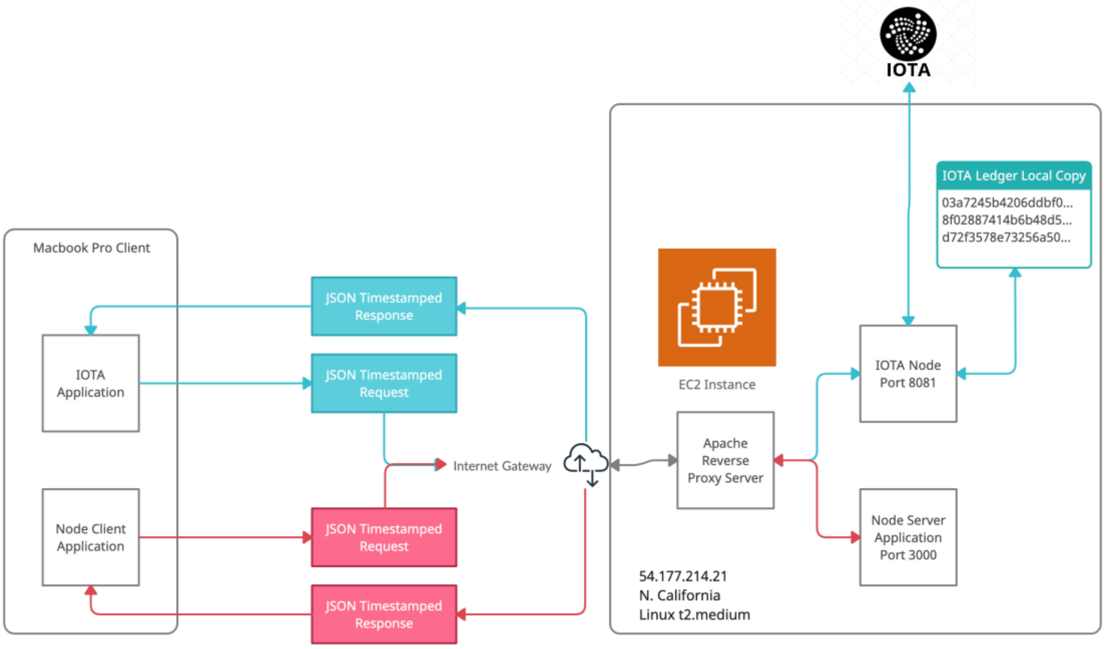


Figure 10: Architecture For Network Latency Test

Controlling Variables

For most communication applications there are generally two main actors – the "publisher" and the "subscriber" – the publisher being the actor that broadcasts the message and the subscriber the one that receives it. However, testing the RTT between a publisher and subscriber is not straightforward as there are a number of variables to consider when testing the RTT. These include:

Variable 1: Type of network transport protocol used (e.g. TCP/UDP/ICMP).

Variable 2: Local and wide area network speed.

Variable 3: Geographical distance between the publisher and subscriber.

Variable 4: CPU availability on pub/ sub machines.

Variable 5: Number of network hops during round-trip journey.

Variable 6: Compiler/ interpreter used for building the applications

Variable 7: Total packet size being sent.

The RTT experiment needed to be designed in such a way that these variables could be controlled. To control variable 1, TCP was chosen as the communication protocol. To control variable 2, all data was gathered at the same time using the same internet connection and location. To control variable 3, both applications were installed on the same server as seen in Figure 10. Again as in Figure 10, to control variable 4, the same client machine was used to send requests to the server and receive responses (2 GHz Quad-Core Intel Core i5 16GB RAM). Controlling variable 5 was not an option as the server was hosted within an AWS environment on an EC2 instance, but the same general path should be taken between the two machines as the same LAN and AWS infrastructure are being used. To control variable 6, the same runtime was used for developing both applications (NodeJS). Variable 7 is the variable that will be changed to measure network latency at different packet sizes.

3.5.2 Quality - Usability

The ease-of-use/ usability also needed to be researched. Various techniques were looked at to identify a valid method of quantifying the usability of a piece of open-source software.

One such method is the System Usability Scale (SUS), was developed in 1996 by John Brooke [62]. This method is self-described as “a reliable, low-cost usability scale that can be used for global assessments of systems usability.” Also self-described as a “quick and dirty” usability scale, the technique is a very popular in measuring the usability of a system, in this case the IOTA technologies and products. Empirical evidence shows this method is very effective despite being relatively short and high-level [62]. Due to time constraints and resource availability this approach was chosen as a suitable method to measure the usability of the IOTA technologies and products.

System Usability Scale (SUS)

The system usability scale works as follows: it is a ten part questionnaire (see Appendix 1) with five possible answers to each question:

1) Strongly Agree – 5 Points
2) Agree – 4 Points
3) Neither Agree or Disagree – 3 Points

4) Disagree – 2 Points
5) Strongly Disagree – 1 Point

The steps to calculate the overall SUS score for each response are as follows:

- If the question is an odd-numbered question, 1 is subtracted from the answer to give the result for that question.
- If the question is an even-numbered question, the answer is subtracted from 5 to give the result for that question.
- Each result is added together, and then multiplied by 2.5 to give the overall SUS score.

Once the overall SUS score has been calculated, the adjective rating for usability can be calculated as per Table 3 below.

SUS Score	**Grade**	**Adjective Rating**
>80.3	A	Excellent
68 – 80.3	B	Good
68	C	Okay
51 – 68	D	Poor
<51	F	Fail

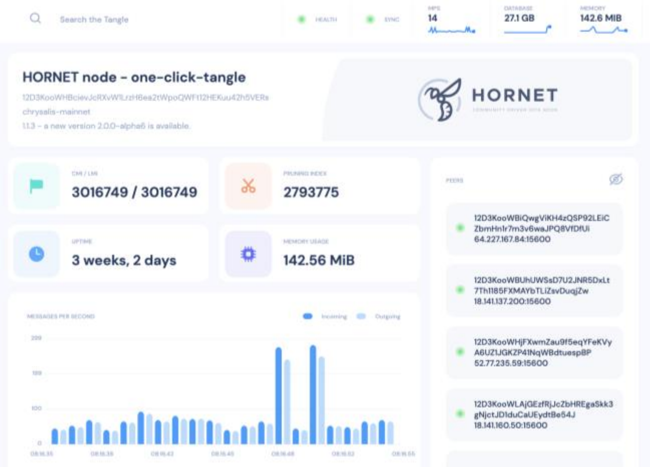
Table 3: Scoring system for SUS

Target Population

In order to conduct the survey, a population familiar with the IOTA products and technology was required. IOTA technologies and products have yet to reach mainstream adoption. Therefore, research into the IOTA communities online was undertaken to find a concentrated population who interact with the IOTA technologies and products on a regular basis. There were a number of potential platforms being used like GitHub, Twitter, Reddit and Discord. While GitHub is a very active platform from the perspective of the IOTA Foundation and its developers, Discord appeared to be the primary communication platform between the IOTA Foundation and the online IOTA community and users when compared to the other platforms. Discord is an instant messaging and digital distribution platform and has between 2000 – 3500 IOTA community members online at any one point, discussing the various aspects of the IOTA platform was chosen as the best option for launching the questionnaire and conducting the survey.

3.5.3 Reliability - Network Uptime & Availability

Interacting with the IOTA network is done via network nodes, which are the gatekeepers of the Tangle shared ledger. It is where transactions are validated and PoW takes place. Nodes are connected to neighbour nodes through peer-to-peer (P2P) connections and each time a new transaction gets added to the ledger, this information gets gossiped around the nodes through these connections, keeping the network in sync. If a node is not connected to other nodes, or is out of sync with other nodes, then this node cannot participate in the sending and receiving of data to the network. Therefore to maintain access to the network, nodes must remain connected to their peers and in sync with the network. Figure 11 shows the dashboard of a node that is healthy, in sync, connected to four peers and participating in the network.



HORNET node - one-click-tangle

12D3KooWHBcievJcRXvW1LzH6ea2tWpoQWFt12HEKuu42h5VERs

chrysalis-mainnet

1.1.3 - a new version 2.0.0-alpha6 is available.

MPS 14

DATABASE 27.1 GB

MEMORY 142.6 MIB

CMI / LMI 3016749 / 3016749

PRUNING INDEX 2793775

UPTIME 3 weeks, 2 days

MEMORY USAGE 142.56 MiB

PEERS

12D3KooWBiQwgViKH4zQSP92LEiCZbmHn1r7m3v6waJPQ8VfDfUi
64.227.167.84:15600

12D3KooWBUhUWSsD7U2JNR5DxLt7Th1185FXMAYbTLiZsvDuqjZw
18.141.137.200:15600

12D3KooWHjFXwmZau9f5eqYFeKVyA6UZ1JGKZP41NqWBdtuespBP
52.77.235.59:15600

12D3KooWLAjGEzfRjJcZbHREgaSkk3gNjctJD1duCaUEydtBe54J
18.141.160.50:15600

Figure 11: Screenshot of IOTA Hornet Node Dashboard

To test for this, the below architecture was devised to test network uptime and availability over an extended period of two weeks. A simple application was developed to ping the node once every ten minutes to determine if the node is available, healthy and in sync. The results were then stored in a local database. Much of the existing architecture from the network latency testing ins section 3.5.1 was reused for this experiment.

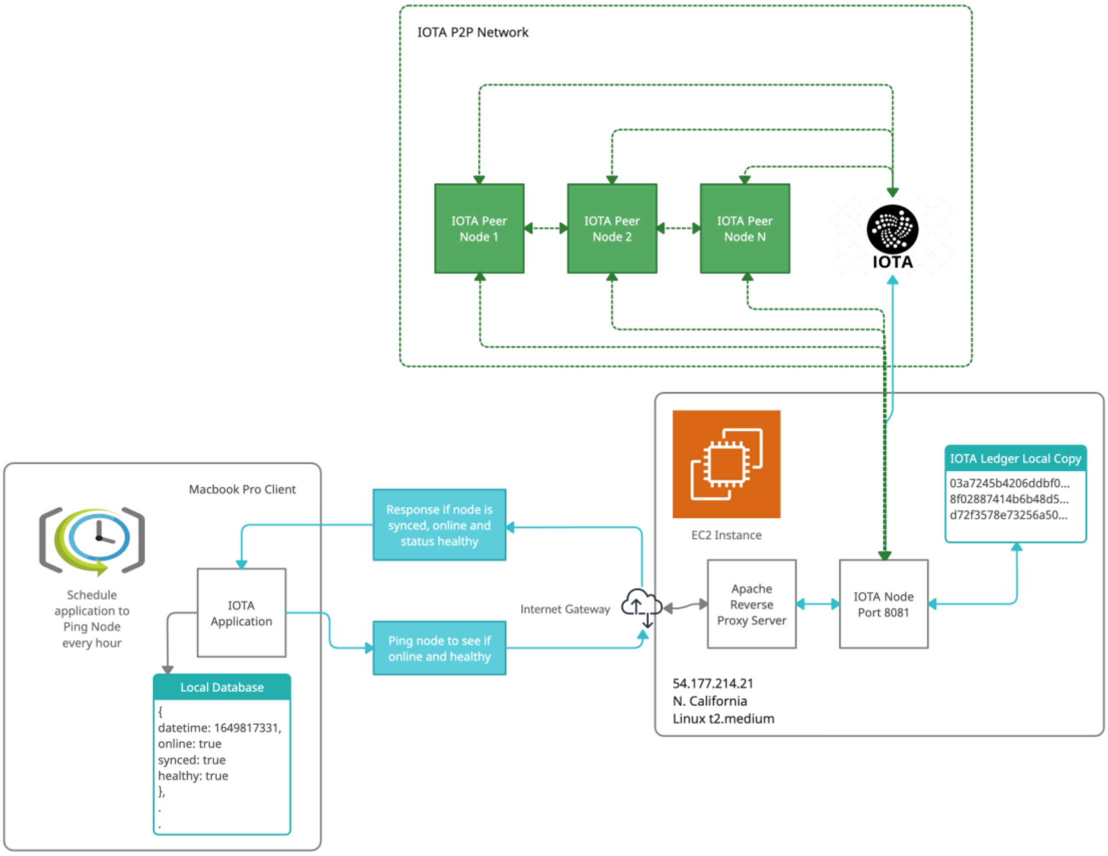
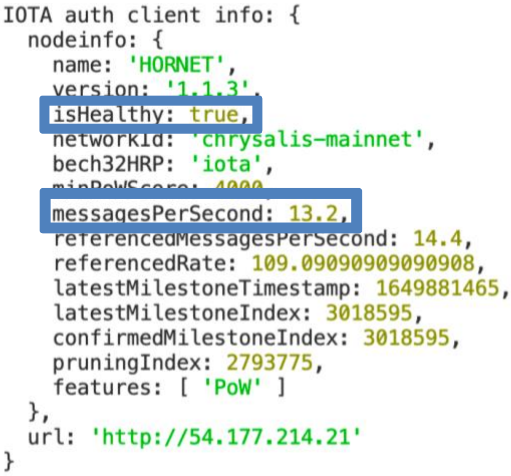


Figure 12: Architecture for Network Reliability Experiment

The response from the node contains the data that is needed. Example below:



```
IOTA auth client info: {
  nodeinfo: {
    name: 'HORNET',
    version: '1.1.3',
    isHealthy: true,
    networkId: 'chrysalis-mainnet',
    bech32HRP: 'iota',
    minPoWScore: 4000,
    messagesPerSecond: 13.2,
    referencedMessagesPerSecond: 14.4,
    referencedRate: 109.09090909090908,
    latestMilestoneTimestamp: 1649881465,
    latestMilestoneIndex: 3018595,
    confirmedMilestoneIndex: 3018595,
    pruningIndex: 2793775,
    features: [ 'PoW' ]
  },
  url: 'http://54.177.214.21'
}
```

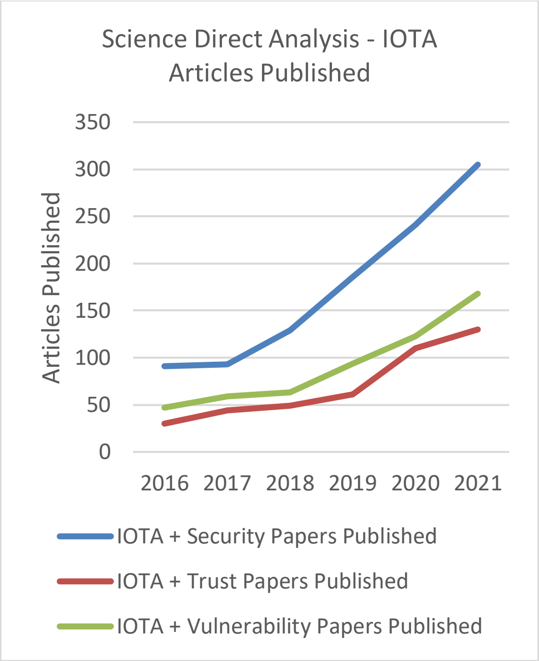
Figure 13: Response from node using get_info() function

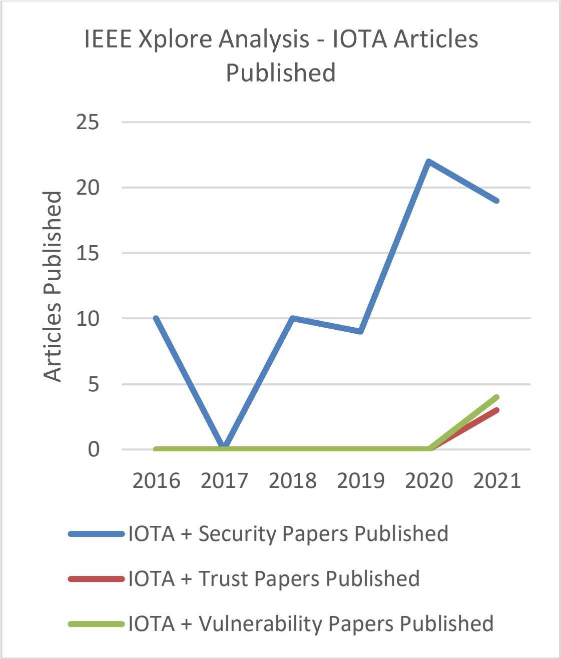
Each time the response was returned, the relevant data was stored in a local database.

After a two week period, the results of the experiment could be collated and analysed.

3.5.4 Security - Trustworthiness & Vulnerability

Security is one of the key attractions to DLTs. They are secure by design and have inherent security advantages over more centralised architectures. To investigate the state-of-play of IOTA security, a literature review of IOTA security features and issues was designed. As the IOTA Foundation was only founded in 2015, research around the topic was limited. Keywords were chosen for the search were “IOTA”, “Security”, “Trust” and “Vulnerability”. ScienceDirect and IEEEXplore were chosen as the academic databases and the article type was filtered to research articles and conference proceedings.





Initial research on publications over the last six years indicated a rate of growth of research in this area. These publications will be examined for quantitative and qualitative data and findings about the security benefits and limitations of IOTA discovered over this time period.

CHAPTER FIVE

Results

The following chapter will document the results of the three experiments, the survey and the literature review outlined in the previous chapter.

4.1 Speed/ Network Latency

The first experiment that was run was to test the speed of the message being delivered using an application built on the IOTA Streams communication protocol. It was then compared to a similar application using a more traditional approach (REST). The results are as follows:

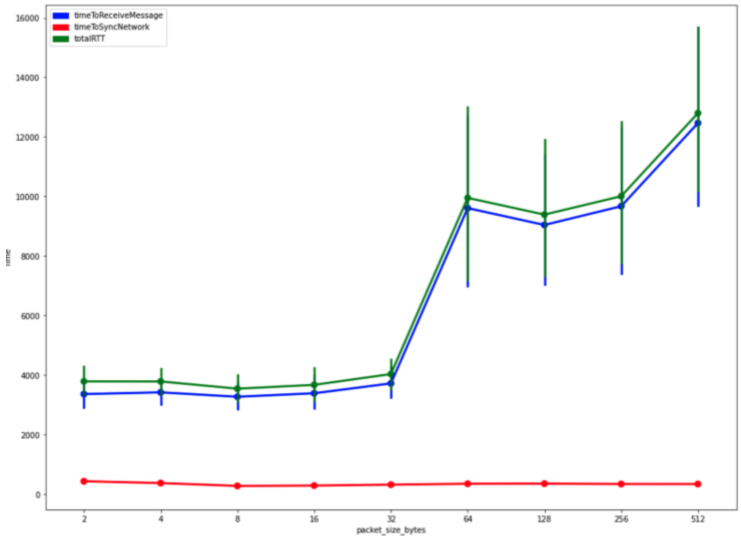


Figure 14: Total RTT for IOTA messages

From 2 to 32 bytes, the total RTT for a message was ~4 seconds. A degradation in delivery time was recorded as the packet size being sent was larger than 32 bytes at >10 seconds.

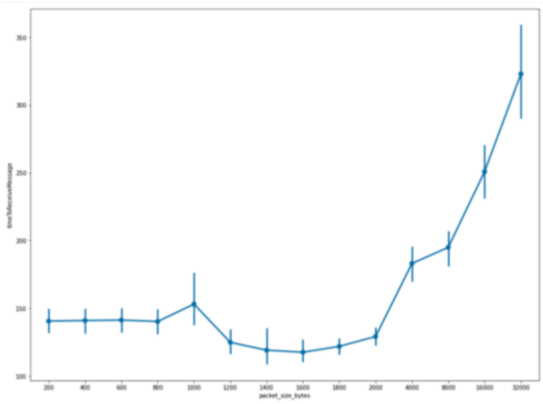


Figure 15: Total RTT for NodeJS Application

Up to 2Kb (200bytes), RTT remained under 150ms approximately for request and response. Above 2Kb, up to 32Kb the RTT increased to 350ms. Testing less than 200 bytes, like the IOTA application test above did not show any significant difference due to the inherent latency of the system.

4.2 Usability Results

SUS

The Google Forms questionnaire that was devised was posted in the IOTA Discord group in a channel called "#promote-your-project". The questionnaire had a total response of 12 people. An Excel tool was devised to calculate the individual scores of each respondent.

The answers to the ten question in Appendix 1 were as follows:

	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10
Strongly Disagree	0.0%	8.3%	8.3%	8.3%	8.3%	25.0%	0.0%	16.7%	8.3%	8.3%
Disagree	0.0%	58.3%	41.7%	8.3%	0.0%	50.0%	25.0%	50.0%	8.3%	0.0%
Neither Disagree or Agree	25.0%	0.0%	16.7%	25.0%	25.0%	8.3%	25.0%	25.0%	16.7%	8.3%
Agree	33.3%	25.0%	33.3%	41.7%	33.3%	0.0%	41.7%	8.3%	58.3%	58.3%
Strongly Agree	41.7%	8.3%	0.0%	16.7%	33.3%	16.7%	8.3%	0.0%	8.3%	25.0%

Table 4: SUS Questionnaire Responses

The average SUS was 58.125. This correlates to a "Poor" rating on the System Usability Scale.

Question		Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	SUS
Response 1		3	2	1	1	1	5	2	3	3	4	37.5
Response 2		4	4	2	5	4	2	2	3	4	5	42.5
Response 3		5	2	4	4	3	1	3	2	4	5	62.5
Response 4		5	2	4	4	3	1	3	2	4	5	45
Response 5		3	4	2	5	3	2	5	3	3	4	65
Response 6		5	2	3	4	5	2	3	2	4	4	65
Response 7		5	1	4	3	4	3	2	2	4	4	75
Response 8		4	2	3	3	5	1	4	2	5	3	67.5
Response 9		5	2	2	4	5	2	4	1	4	4	50
Response 10		4	4	2	3	5	2	4	4	2	4	37.5
Response 11		3	5	2	4	4	5	4	1	1	4	77.5
Response 12		4	2	4	2	4	2	4	2	4	1	72.5
												58.125

Table 5: Overall SUS Calculation

Mean, variance and standard deviation calculations for each question are outlined in Table 6. Question 6 had the highest variance and standard deviation.

Question	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10
Mean Value	4.17	2.67	2.75	3.50	3.83	2.33	3.33	2.25	3.50	3.92
σ^2	0.70	1.52	1.11	1.36	1.42	1.88	0.97	0.75	1.18	1.17
σ	0.83	1.23	1.06	1.17	1.19	1.37	0.98	0.87	1.09	1.08

Table 6: Mean, Var, Std for Questionnaire Answers

4.3 Reliability – Network Uptime and Availability

Samples to test for node reliability and uptime were taken at 10 minute intervals over a period of two weeks. The results are as follows:

1997 samples were taken. Out of these samples, the network was available and the node was synced and healthy for message processing in 99.29% of cases.

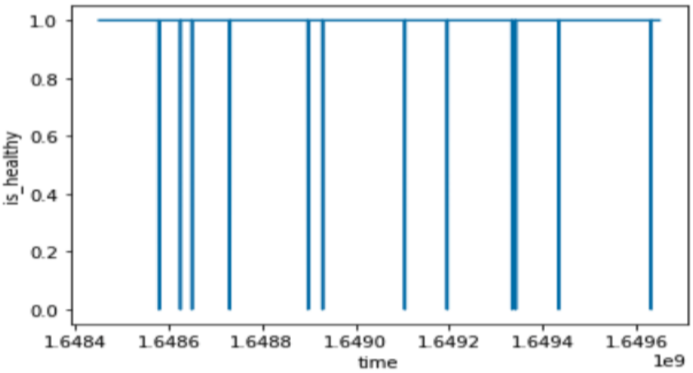


Figure 16: IOTA Node Network Uptime (2 Weeks)

A second metric gathered from each response was the messages per second that the node was processing. Out of the 1997 samples taken, the mean message-per-second value was 13.089 with a standard deviation of 3.24. This means that for the dedicated node that was created, the node was available 99.29% of the time over a two week period, processing on average 13.089 messages per second.

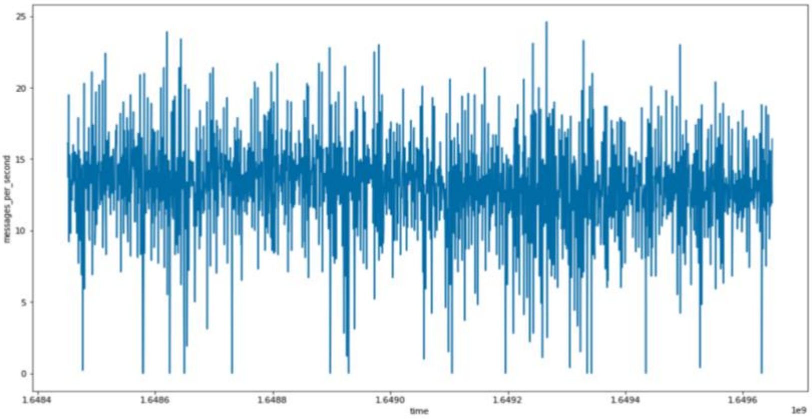


Figure 17: Average Messages Per Second Processed on IOTA Node

4.4 Security – Trustworthiness and Vulnerability

As the time for experimentation was limited, a literature review of papers published addressing the security of the IOTA services. The result of the literature review is outlined below:

IOTA Maturation

It is worth noting that the IOTA framework that is rapidly developing, and many of the issues highlighted in some papers more than 3 years old have already been addressed.

Once such paper by Conti *et al.* [63] highlights this relationship between the maturation of the IOTA technology and the security issues present. In the original version of the IOTA protocol, released in 2015, the paper identifies 22 potential attack vectors for IOTA 1.0 with 18 resolutions, five attacks and resolutions in IOTA 1.5 and eleven attacks and resolutions in IOTA 2.0.

The four attacks yet to be resolved are:

1) Eclipsing – where attackers aim to attack one user rather than whole network
2) Byzantine Node Creation - A node that does not forward messages to other participants and sends conflicting messages.
3) Sybil Identities – Forging multiple fake identities to gain control over the p2p network.
4) Failure of the Coordinator – taking down the coordinator stops the entire tangle from operating

Currently, the IOTA network is governed by what is called a "Coordinator" which is a centralized node run by the IOTA foundation, and is the executor node in deciding which transactions and messages are to be added to the ledger [64]. The presence of the Coordinator to provide consensus is a point of criticism among the community as with it, the network is not technically fully decentralized. IOTA 1.5 or "Chrysalis" (which is the version currently running the mainnet) was released in April 2021 as an intermediary step to optimise the network prior to the launch of IOTA 2.0 or "Coordicide" [64]. With this new release, a number of new security features were added. The Ed25519 signature scheme replaced the Winternitz One Time Signture (W-OTS) scheme which allowed for the reuse of private keys and addresses. This was previously not available with W-OTS as part of the private key got exposed when a transaction was created, exposing the private key to brute-force attacks.

Coordicide

From a security perspective, as outlined by Conti *et al.* [63] the existence of the coordinator creates an attack plane that is single point of failure in the network of nodes. IOTA 2.0, dubbed "Coordicide", is a new version of the protocol that is designed to remove the Coordinator from the network, allowing for full decentralization. Another interesting addition was the concept of Mana, which is a solution that is aimed to support participating node reputation and sybil protection.

Saha *et al.* [65] studied the concept of the Mana reputation system in great detail. Each time a node adds a valid transaction to the ledger, it is assigned a difficult-to-obtain network resource called mana. The more mana a node has, the more trustworthy it becomes as a good actor. However, a number of pitfalls were already identified with this approach:

1) There is the ability for a single node to monopolise the system for more control
2) High mana nodes communicate with nodes of similar levels, making it harder for newly joined nodes to accumulate reputation.
3) High mana nodes are more utilised as a result of being a good actor, which could undermine the node availability.
4) Dependency on a single reputation parameter makes it easier for nodes to legitimise themselves.

This study presented an improved solution called eMana, which is a more holistic behavioural reputation model for the network, reducing biases and the likelihood of monopolies developing, and increasing fairness for all participating nodes.

Threat Modelling

Ullah *et al.* [66] explored and highlighted some security vulnerabilities of IOTA using existing literature and online blogs. Six vulnerabilities were identified and scored using the Common Vulnerability Scoring System, which is an open industry standard for assessing severity of system security vulnerabilities. The results discovered the existence of the Coordinator in the network as the biggest security threat to the IOTA network as seen in Table 7.

Vulnerability	**CVSS Score**	**Rating**
Curl-P hashing	2.6	Low
Replay attack	2.6	Low
Double spending attack	3.1	Low
Splitting attack	3.1	Low

34% attack and necessity of an “assiduous honest majority”	4.2	Medium
Centralization/ Coordinator	8.7	High

Table 7: IOTA Vulnerabilities Identified by [66]

DDoS Attacks

One of the most studied security threats within the DLT space is Distributed Denial-of-Service, as it is a type of attack the technology was specifically designed to avoid. In 2002, Back [67] introduced a mechanism called “hashcash” as a denial-of-service countermeasure, a mechanism referenced heavily in the original whitepaper for bitcoin, the first and most popular DLT [19]. Brightene *et al.* [68] explored the vulnerability of the IOTA network to SYN flooding through port-based attacks on IOTA nodes. SYN flooding is a type of DDoS attack that works by exploiting the handshake process of TCP connections. Each node has a number of ports open at any one time to perform various tasks like auto-peering, gossiping and FPC. This study revealed that the gossip protocol, which is the protocol used by nodes for peer-to-peer communicate, was vulnerable to this type of DDoS attack. Nodes were unable to create a list of neighbouring nodes while under attack and thus unable to communicate. This study suggested the implementation of a noise protocol to replace TCP for all exposed ports.

Conti *et al.* [63] also points to the vulnerability of nodes to spam attacks. With specialised FPGA hardware, it is theoretically possible to complete PoW in a short period of time and flood the node, even in the presence of the Adaptive PoW algorithm, which was introduced in IOTA 1.5. Brady *et al.* [69] confirmed this by attempting a DOS attack on the IOTA network. Based on their analysis, managed to drop the transaction conformation rate on a node by 58% by adding significant load onto the server, suggesting a weakness in the IOTA implementation. Additionally, as IOTA is designed to run on low-powered devices, for example a Raspberry Pi, this research suggested attacks like this could halve the battery life of such devices.

User Error & Social Engineering

Users of the IOTA network pose one of the greatest security vulnerabilities, specifically when it comes to storage and transfer of MIOTA, the token used for value transfer within the IOTA network. There is more user agency and personal responsibility with DLTs as users have to manage their private keys or seeds, and recovery phrases. In April 2020, there was a breach of the Trinity software wallet ,where IOTA users store IOTA tokens. Code that was downloaded from a third-party service called “Moonpay” had been maliciously altered to give hackers access to users software wallets once it was opened by them. Funds were stolen from user accounts, up to a value of approximately 2 million dollars at the time. Since then, the Trinity wallet has since been deprecated and replaced by a new and more secure wallet with the IOTA 1.5 release.

CHAPTER SIX

Discussion of Results

This chapter discusses the results of the analysis of the IOTA framework in terms of speed, reliability and security from Chapter 4. These results are then used to contextualise the use of this communication technology for autonomous vehicle communication. Other points of interest that emerged during the research process are expanded upon at the end of the chapter.

5.1 Speed/ Network Latency

The network latency experiment testing end-to-end communication using the IOTA Streams framework yielded some interesting results. Total round-trip-time for the IOTA application was considerably slower at sending packet sizes of less than 32 bytes in comparison to the NodeJS application. There was a considerable delay in message delivery time for the IOTA Application when the packet size increased past 32 bytes up to 512 bytes.

It is worth noting here that communication with a payload of less than 32 bytes is very limiting (approximately 64 character hexadecimal value). Taking an example in the context of V2X, the BSMs used in V2X short range communication, which have been specifically designed to minimize message size to reduce DSRC channel congestion are a minimum 39 bytes [70]. This only accounts for BSM I data elements and frames which is the mandatory part of the BSM. Additional data can be added to the BSM (BSM II) which can make the message size much larger. By comparison, the NodeJS application delivered a much larger payload (approximately 1000 times larger) at a much faster RTT (by approximately 10-50 times). A faster RTT was expected for the NodeJS application, considering it does not need to go through the same cryptographic protocols as the IOTA Streams message, nor does it need to wait for network nodes to sync or for the message to be added to a ledger before responding. However the difference in time here can be considered as the time taken to complete these actions, and the difference is considerable.

There are some improvements that could be made to improve the network latency. A more efficient IP transport protocol could be used instead of TCP, for example User Diagram Protocol (UDP, if data integrity was not a design requirement. UDP is an alternative transport protocol used to establish low-latency loss tolerant connections and is often used for media streaming.

Ultimately if small network latency and transfer of packets of >32 bytes are design requirements for AV applications, then the IOTA framework does not seem to be a good fit.

5.2 Network Uptime & Availability

The second experiment demonstrated a stable network, with an healthy, synced node with 99.29% availability over a two week period. To remain healthy and in sync, nodes must retain relationship with other synced and healthy nodes, and this appeared to be the case. In an ideal situation, if the IOTA technology was used by autonomous vehicles, node software would be installed within the vehicle and it would operate as a node on the IOTA network. This would give applications that use the IOTA protocol a dedicated node within the vehicle which can be used to interact with the IOTA ledger and reduce the reliance on external infrastructure. It also minimises that chance that a single node could become overloaded, as demonstrated by Brady *et al.* [69], if it were being used by multiple users or vehicles.

However, for a node to operate, unlike DSRC communication, the node must be connected to the internet in order to work. This may not have been reflected fully in the results from this experiment as the Hornet node was installed on a server with wired connectivity. In reality, access to the network would depend on cellular connectivity which is less predictable or reliable, especially in more rural situations where cellular infrastructure is less proximal. However this is the same problem for all IP-based communication and not necessarily isolated to IOTA.

Also, AV compute and storage resource availability need also to be considered. IOTA Facts [71] alluded to a possible issue with lighter nodes (e.g. a Raspberry Pi) becoming unavailability at around 40% of the average network transactions per second due to lack of computational power, indicating a level of computational power is required for a node to function properly. The IOTA Foundation recommend recommendations for running a Hornet node are a dual core CPU with 2GB of RAM. From a storage perspective, a copy of the shared ledger needs to be stored on the node machine. Over the course of the two weeks when the network uptime and availability experiment was carried out, the ledger data grew from 4GB to 27GB. The IOTA Foundation have implemented functionality to configure the max size of the ledger. However, there is a trade-off between reducing the ledger size and access to historical data. Once the historical data is pruned from the ledger, it is no longer available on the node for referencing. Therefore adding resources to the technology stack that consumes the AV compute and storage resources would need to be weighted with the benefits on offer.

Finally, the IOTA Foundation state that the network gets faster and more reliable as more nodes get added. This makes sense – if there are more nodes, there are more peers to connect with and more compute power for the network. Therefore the reliability and availability links directly to the number of nodes running the network, so node running adoption is critical. However, IOTA lacks incentive for users to run their own node. For many DLTs, running a node is incentivised usually in the form of cryptocurrency rewards, as is the case when running a Bitcoin node. IOTA, by comparison, has very little incentives to keep a node running, apart from having controlled and dedicated access to the Tangle. The introduction of "mana" being introduced in IOTA 2.0 version is a form of reputational reward mechanism for running a healthy node. The IOTA Foundation states that in the future, this earned mana could be leased for high-priority access to the network [72] but as of today it is unclear how this translates into real rewards for users . Running a node can be costly for the owner. Approximate costs of running a Hornet node on AWS infrastructure during this research was €35 for one month, or €210 annually. Also, question X of the questionnaire indicated that the majority of users did not currently run a node or plan to run a node in the future.

5.3 Security

Security remains one of the most debated topic around IOTA. Like all DLTs, it is a technology rooted in cryptography and the integrity of its protocols are a critical component. DLTs are secure by design . The literature review from the research results indicate that there are a number of security issues that have yet to be resolved including some exposure to DDoS attacks, one of the major selling points of DLTs. However, while still exposed to these types of spam attacks, the research suggests that even though the network performance could be compromised and parts of the network could be attacked, it is much harder to take down the entire network in comparison to a more centralised architecture.

The literature review and review of the GitHub repository where the code is hosted highlighted the speed at which the IOTA Foundation have rolled out upgrades and patches to security concerns since the launch of the original IOTA in 2015, with a very active development community.

The existence of the coordinator surfaced many times in the research as the “Achilles heel” of the technology. Interestingly, it served as the trip-switch to halt all transactions when the network was hacked during the Trinity Wallet attack in 2020. In reality, IOTA cannot be considered as a true decentralized network like Ethereum or Bitcoin with the existence of a single node making the executive decision on all transactions. The IOTA 2.0 “Coordicide” release is highly anticipated in the IOTA community and is not without scepticism whether or not true decentralization is possible for the technology. And with a single point of failure or attack plane, the network remains vulnerable to many types of attacks.

5.4 Other Factors

5.4.1 Payments

There are other factors to be considered regarding the benefits of adoption of the IOTA Framework for autonomous vehicle usage. One benefit that has not been examined in detail in this research, and one of the core features of the IOTA technology, is the ability for it to be used as a payment gateway. While the results of the network speed experiment determines that the IOTA Streams communication may not be a suitable candidate for real-time V2X communication, payment processing is an example of a use-case where network latency is less critical. This has already proven at a small scale [22, 46]. Emerging research has also suggested that the IOTA protocol is much more energy efficient than centralized payment gateway services like Visa, Mastercard, Stripe and PayPal. Other payment gateway alternatives. Furthermore, the IOTA was designed to allow micro-transactions in a machine-to-machine economy, something that is not possible with the aforementioned centralized payment gateways. Currently, 1 MIOTA (which is the unit of measurement for 1 million IOTA tokens) is $0.66. The smallest unit of value transfer is 1 IOTA token, meaning a transaction can be very small fractions of a cent. This micro-payment features opens a new set of use cases for connected machines, to serve as a payment gateway for a unique set of AV applications. In addition to this, value transfers between users are also stated to be “feeless”, unlike most other payment gateways where fees can be between 1.3 – 3.5% of a transaction [73], and other blockchain technologies where fees increase in relation to traffic congestion. Feeless transactions translates to financial savings for AV owners and encourage the use of applications that can exchange value and data for free between machines for goods and services.

5.4.2 Potential Use Case – Publishing Warning Messages in the OBU using IOTA

It is estimated that 1.3 million people die each year as a result of road traffic crashes which is the leading cause of death for children and young adults aged between 5-29 years [74]. Over 90% of these incidents occur in low- to middle-income countries. There are many factors that influence levels of road fatalities, most notably driving under the influence, speeding, distraction as well as inadequacies in road infrastructure, vehicle condition, post-crash care and law enforcement. As an example, in the United States alone, there are over 150,000 accidents with over 1,800 deaths every year due to icy road conditions [75].

Electronic Stability Control (ESC) or Traction Control (TC) as it is better known is a safety feature which was first brought to the automotive market in the early 1990s and is incorporated into the majority of vehicles on the market today. Traction control works by sensing when a vehicle is about to lose control by comparing the expected versus actual wheel behaviour, and intervenes accordingly to stabilise the vehicle.

Other studies not involving dangerous road conditions have also been undertaken. Zhang *et al.* [76] examined traffic signal light management using a consortium blockchain and OBU messages. The idea was as the road gets congested, the host vehicle sends road condition messages to a traffic department, which adjusted signal light duration automatically using a smart contract.

Baruah *et al.* [77] proposed a secure road condition monitoring system. This study addressed some of the underlying security issues with publishing vehicle data to cloud-based monitoring applications, including RSU collusion attacks and lack of anonymity.

Chowdhury *et al.* [78] examined the use of OBU message data to create a trust model to measure the trustworthiness of autonomous vehicles. This trust model could potentially be used to detect malicious or corrupt vehicles as part of an entity-centric trust model.

CHAPTER SEVEN

Conclusions and Future Research

Autonomous vehicle or V2X communication is a multi-faceted area of research that spans from ultra-low latency DSRC communication where information exchange happens at a millisecond level up to IP-based communication using various internet protocols. This research focused on one type of IP-based communication protocol called the IOTA framework, a distributed ledger technology created in 2015. Various aspects of this open-source technology were tested including network speed, network reliability and security using various research methods. From this research it is clear that the technology has come a long way since its inception, while also having a long way to go to achieve the objectives outlined in its technology roadmap. As stated, it is estimated that over 30% of V2X applications will be non-safety critical by 2027 and built by third-party developers using IP-based communication. The security, reliability and speed of the technologies and protocols that underpin these applications is a large area of research today. Decentralized leger technologies are fundamentally different from the centralized or federated architecture approach and offer a host of new security features. In the case if the IOTA framework, from the network latency test, it appears to not be the best use case for real-time communication. It shows promise in a multitude of use cases where real-time processing is less critical, like payment processing for AV services. In terms of reliability, the network was measured to be very stable and highly available. Multiple security concerns have been highlighted by various researchers over the past few years, which the IOTA Foundation seem to be incrementally addressing through new releases. This is apparent in the online community of developers which are very active and engaged with the development of the technology. The future of the IOTA framework, hinders it seems, on the successful release of IOTA 2.0, the journey towards a fully decentralized network. Finally, there is potential for this technology to also play a part in the future of the AV industry.

6.1 Future Research

There are many directions that this research can take. One thing that this research prove is that the IOTA framework is unsuitable for safety-critical application that require real-time processing. Focus for this technology should be on use-cases and testing in a real-world situation. Applications that could benefit from the advantage of distributed ledger for example - vehicle ownership and transfer of ownership, audit trails for vehicle actions, machine-to-machine payments / micropayments, identity access management. More rigorous testing of the topics presented in this paper should be undertaken once the IOTA 2.0 Coordicide release.

References

[1] ABIResearch. "ABI Research Forecasts 8 Million Vehicles to Ship with SAE Level 3, 4 and 5 Autonomous Technology in 2025." https://www.abiresearch.com/press/abi-research-forecasts-8-million-vehicles-ship-sae-level-3-4-and-5-autonomous-technology-2025/ (accessed October 31, 2020, 2020).

[2] *Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles*, S. International, 2021. [Online]. Available: https://www.sae.org/standards/content/j3016_202104/

[3] A. Alnasser, H. Sun, and J. Jiang, "Cyber security challenges and solutions for V2X communications: A survey," *Computer Networks*, vol. 151, pp. 52-67, 2019-03-01 2019, doi: 10.1016/j.comnet.2018.12.018.

[4] A. Moubayed and A. Shami, "Softwarization, Virtualization, & Machine Learning For Intelligent & Effective V2X Communications," *IEEE Intelligent Transportation Systems Magazine*, pp. 0-0, 2020-01-01 2020, doi: 10.1109/mits.2020.3014124.

[5] NHTSA. "Automated Vehicles for Safety." NHTSA. https://www.nhtsa.gov/technology-innovation/automated-vehicles-safety/ (accessed 19th Oct, 2021).

[6] I. Foundation. "What is IOTA." The IOTA Foundation. https://www.iota.org/get-started/what-is-iota (accessed October 19th 2021).

[7] R. Zhang, R. Xue, and L. Liu, "Security and Privacy on Blockchain," *ACM Computing Surveys*, vol. 52, no. 3, pp. 1-34, 2019-07-27 2019, doi: 10.1145/3316481.

[8] Interestingengineering.com. "IOTA : A Cryptocurrency With Infinite Scalability And No Fees." https://interestingengineering.com/iota-a-cryptocurrency-with-infinite-scalability-and-no-fees (accessed October 19th, 2021).

[9] K. Abboud, H. A. Omar, and W. Zhuang, "Interworking of DSRC and Cellular Network Technologies for V2X Communications: A Survey," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 12, pp. 9457-9470, 2016-12-01 2016, doi: 10.1109/tvt.2016.2591558.

[10] R. F. Atallah, M. J. Khabbaz, and C. M. Assi, "Vehicular networking: A survey on spectrum access technologies and persisting challenges," *Vehicular Communications*, vol. 2, no. 3, pp. 125-149, 2015-07-01 2015, doi: 10.1016/j.vehcom.2015.03.005.

[11] L. Badea and M. C. Mungiu-Pupazan, "The Economic and Environmental Impact of Bitcoin," *IEEE Access*, vol. 9, pp. 48091-48104, 2021-01-01 2021, doi: 10.1109/access.2021.3068636.

[12] A. A. Sori, M. Golsorkhtabaramiri, and A. M. Rahmani, "Cryptocurrency Grade of Green; IOTA Energy Consumption Modeling and Measurement," in *2020 IEEE Green Technologies Conference(GreenTech)*, 2020-04-01 2020: IEEE, doi: 10.1109/greentech46478.2020.9289803.

[13] T. I. Foundation. "IOTA 2.0: Details on Current Status and Next Steps." https://blog.iota.org/iota-2-0-details-on-current-status-and-outlook/ (accessed.

[14] T. I. Foundation. "IOTA Smart Contracts Protocol Alpha Release." The IOTA Foundation. https://blog.iota.org/iota-smart-contracts-protocol-alpha-release/ (accessed October 21st 2021).

[15] IBM. "What are smart contracts on blockchain?" IBM. https://www.ibm.com/topics/smart-contracts (accessed October 21, 2021).

[16] M. Rauchs *et al.*, "Distributed Ledger Technology Systems: A Conceptual Framework," *SSRN Electronic Journal,* 2018-01-01 2018, doi: 10.2139/ssrn.3230013.

[17] A. Pinna and W. Ruttenberg, "Distributed ledger technologies in securities post-trading," ed: European Central Bank, 2016.

[18] L. LAMPORT, R. SHOSTAK, and M. PEASE, "The Byzantine Generals Problem," *ACM Transactions on Programming Languages and System,* vol. 4, pp. 382-401, 1982.

[19] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008,

[20] Rathee, Sharma, Iqbal, Aloqaily, Jaglan, and Kumar, "A Blockchain Framework for Securing Connected and Autonomous Vehicles," *Sensors,* vol. 19, no. 14, p. 3165, 2019-07-18 2019, doi: 10.3390/s19143165.

[21] M. Pustisek, A. Kos, and U. Sedlar, "Blockchain Based Autonomous Selection of Electric Vehicle Charging Station," in *2016 International Conference on Identification, Information and Knowledge in the Internet of Things (IIKI),* 2016-10-01 2016: IEEE, doi: 10.1109/iiki.2016.60.

[22] W. Khan, "Blockchain-Based Peer-to-Peer Energy Trading and Charging Payment System for Electric Vehicles," *Sustainability 2021,* 2021.

[23] R. Gupta, S. Tanwar, N. Kumar, and S. Tyagi, "Blockchain-based security attack resilience schemes for autonomous vehicles in industry 4.0: A systematic review," *Computers & Electrical Engineering,* vol. 86, p. 106717, 2020-09-01 2020, doi: 10.1016/j.compeleceng.2020.106717.

[24] T. Review. "Many Cars Have a Hundred Million Lines of Code." https://www.technologyreview.com./2012/12/03/181350/many-cars-have-a-hundred-million-lines-of-code/ (accessed.

[25] M. Baza, M. Nabil, N. Lasla, K. Fidan, M. Mahmoud, and M. Abdallah, "Blockchain-based Firmware Update Scheme Tailored for Autonomous Vehicles," in *2019 IEEE Wireless Communications and Networking Conference (WCNC)*, 2019-04-01 2019: IEEE, doi: 10.1109/wcnc.2019.8885769.

[26] V. Buterin. "A Next-Generation Smart Contract and Decentralized Application Platform." https://ethereum.org/en/whitepaper/ (accessed Nov 20th, 2021).

[27] F. A. Alabdulwahhab, "Web 3.0: The Decentralized Web Blockchain networks and Protocol Innovation," in *2018 1st International Conference on Computer Applications & Information Security (ICCAIS)*, 2018-04-01 2018: IEEE, doi: 10.1109/cais.2018.8441990.

[28] S. Popov, "The Tangle," Berlin, 2018. [Online]. Available: http://www.descryptions.com/Iota.pdf

[29] T. I. Foundation. "The IOTA Wallet Library." https://wiki.iota.org/chrysalis-docs/guides/exchange (accessed April 10, 2022).

[30] Nonymous. "Blockchain-Based Peer-to-Peer Energy Trading and Charging Payment System for Electric Vehicles." https://github.com/noneymous/iota-consensus-presentation (accessed Nov 30th, 2021).

[31] S. Popov and W. J. Buchanan, "FPC-BI: Fast Probabilistic Consensus within Byzantine Infrastructures," *Journal of Parallel and Distributed Computing,* vol. 147, 2019.

[32] thetangle.org. "Public IOTA nodes." https://thetangle.org/nodes (accessed November 22, 2021).

[33] T. I. Foundation. "Explaining the IOTA Congestion Control Algorithm." https://blog.iota.org/explaining-the-iota-congestion-control-algorithm/ (accessed December 1, 2021).

[34] H. Hellani, L. Sliman, A. E. Samhat, and E. Exposito, "Computing Resource Allocation Scheme for DAG-Based IOTA Nodes," *Sensors*, vol. 21, no. 14, p. 4703, 2021-07-09 2021, doi: 10.3390/s21144703.

[35] I. Korotkyi and S. Sachov, "Hardware Accelerators for IOTA Cryptocurrency," in *2019 IEEE 39th International Conference on Electronics and Nanotechnology (ELNANO)*, 2019-04-01 2019: IEEE, doi: 10.1109/elnano.2019.8783449.

[36] S. S. Hazari and Q. H. Mahmoud, "A Parallel Proof of Work to Improve Transaction Speed and Scalability in Blockchain Systems," in *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, 2019-01-01 2019: IEEE, doi: 10.1109/ccwc.2019.8666535.

[37] T. I. Foundation. "Final Alpha Release for IOTA Streams." https://blog.iota.org/final-alpha-release-for-iota-streams-5a4cfeca506c/ (accessed December 3, 2021).

[38] I. Foundation. "IOTA Streams." https://github.com/iotaledger/streams/tree/develop/bindings (accessed.

[39] I. Foundation, "Streams Specification," 2021. [Online]. Available: https://github.com/iotaledger/streams/blob/develop/specification/Streams_Specification_1_0A.pdf

[40] O. Lamtzidis and J. Gialelis, "An IOTA Based Distributed Sensor Node System," in *2018 IEEE Globecom Workshops (GC Wkshps)*, 2018-12-01 2018: IEEE, doi: 10.1109/glocomw.2018.8644153.

[41] I. Foundation. "Identity.rs." https://github.com/iotaledger/identity.rs/ (accessed Dec 4th, 2021).

[42] A. Tesei, L. Di Mauro, M. Falcitelli, S. Noto, and P. Pagano, "IOTA-VPKI: A DLT-Based and Resource Efficient Vehicular Public Key Infrastructure," in *2018 IEEE 88th Vehicular Technology Conference (VTC-Fall)*, 2018-08-01 2018: IEEE, doi: 10.1109/vtcfall.2018.8690769.

[43] A. Tesei, D. Lattuca, P. Pagano, M. Luise, J. Ferreira, and P. C. Bartolomeu, "A Transparent Distributed Ledger-based Certificate Revocation Scheme for VANETs," 2020-10-23T15:12:07 2020.

[44] D. Strugar, R. Hussain, M. Mazzara, V. Rivera, J. Young Lee, and R. Mustafin, "On M2M Micropayments: A Case Study of Electric Autonomous Vehicles," in *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 2018-07-01 2018: IEEE, doi: 10.1109/cybermatics_2018.2018.00283.

[45] P. C. Bartolomeu, E. Vieira, and J. Ferreira, "IOTA Feasibility and Perspectives for Enabling Vehicular Applications," in *2018 IEEE Globecom Workshops (GC Wkshps)*, 2018-12-01 2018: IEEE, doi: 10.1109/glocomw.2018.8644201.

[46] J. L. Rover. "ON THE MONEY: EARN AS YOU DRIVE WITH JAGUAR LAND ROVER." https://www.jaguarlandrover.com/news/2019/04/money-earn-you-drive-jaguar-land-rover (accessed October 19th, 2021).

[47] Elaad. "IOTA Charging Station." https://www.elaad.nl/projects/iota-charging-station/ (accessed.

[48] R. Miucic, *Connected Vehicles: Intelligent Transport Systems*. Detroit: Springer, 2019.

[49] V. Mannoni, V. Berg, S. Sesia, and E. Perraud, "A Comparison of the V2X Communication Systems: ITS-G5 and C-V2X," in *2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring)*, 2019-04-01 2019: IEEE, doi: 10.1109/vtcspring.2019.8746562.

[50] Verizon. "What is the difference between 3G, 4G and 5G?" https://www.verizon.com/about/our-company/5g/difference-between-3g-4g-5g (accessed November 25, 2021).

[51] Continental. "Continental Invests in Cellular-V2X Technology and Announces C-V2X Trials." https://www.continental.com/en/press/press-releases/continental-invests-in-cellular-v2x-technology-and-announces-c-v2x-trials/ (accessed.

[52] Z. Xu, X. Li, X. Zhao, M. H. Zhang, and Z. Wang, "DSRC versus 4G-LTE for Connected Vehicle Applications: A Study on Field Experiments of Vehicular Communication Performance," *Journal of Advanced Transportation*, vol. 2017, pp. 1-10, 2017-01-01 2017, doi: 10.1155/2017/2750452.

[53] L. Miao, J. J. Virtusio, and K.-L. Hua, "PC5-Based Cellular-V2X Evolution and Deployment," *Sensors*, vol. 21, no. 3, p. 843, 2021-01-27 2021, doi: 10.3390/s21030843.

[54] R. Sattiraju , D. Wang, A. Weinand, and H. D. Schotten, "Link Level Performance Comparison of C-V2X and
ITS-G5 for Vehicular Channel Models," *Wireless Communication & Navigation*, 2020.

[55] Qualcomm, "ITS Stack," 2020. [Online]. Available: https://www.qualcomm.com/media/documents/files/c-v2x-its-stack.pdf

[56] (2016). *Security Credential Management System
Proof–of–Concept Implementation*. [Online] Available: https://pronto-core-cdn.prontomarketing.com/2/wp-content/uploads/sites/2896/2019/04/SCMS_POC_EE_Requirements.pdf

[57] A. Research. "By 2027, 30% of V2X Applications will be Non-safety Related, Driven by Third-party Developer Ecosystem." https://www.abiresearch.com/press/by-2027-30-of-v2x-applications-will-be-non-safety-/ (accessed Dec 12, 2021).

[58] X. Li, S. Moreschini, Z. Zhang, and D. Taibi, "Exploring Factors and Measures to Select Open Source Software," 2021-02-19T15:18:03 2021.

[59] Y. Zhao, R. Liang, X. Chen, and J. Zou, "Evaluation indicators for open-source software: a review," *Cybersecurity*, vol. 4, no. 1, 2021-12-01 2021, doi: 10.1186/s42400-021-00084-8.

[60] M. Saunders, P. Lewis, and A. Thornhill, *Research Methods for Business Students* 5ed. Pearson Education, 2009.

[61] CloudFlare. "What is Round Trip Time (RTT)." https://www.cloudflare.com/en-gb/learning/cdn/glossary/round-trip-time-rtt/ (accessed.

[62] J. R. Lewis and J. Sauro, "The Factor Structure of the System Usability Scale," in *Human Centered Design*: Springer Berlin Heidelberg, 2009, pp. 94-103.

[63] M. Conti, G. Kumar, Vigneri, Luigi, and R. Saha, "A survey on security challenges and solutions in the IOTA," *Network ad Computer Applications*, 2021.

[64] T. I. Foundation. "Fully Decentralized IOTA 2.0." https://blog.iota.org/fully-decentralized-iota-explained-in-under-3-minutes/ (accessed.

[65] R. Saha, G. Kumar, A. Brighente, and M. Conti, "Towards An Enhanced Reputation System for IOTA’s Coordicide," in *2021 Third International*

Conference on Blockchain Computing and Applications (BCCA), 2021-11-15 2021: IEEE, doi: 10.1109/bcca53669.2021.9656975.

[66] I. Ullah, G. De Roode, N. Meratnia, and P. Havinga, "Threat Modeling—How to Visualize Attacks on IOTA?," *Sensors*, vol. 21, no. 5, p. 1834, 2021-03-06 2021, doi: 10.3390/s21051834.

[67] A. Back, "Hashcash - A Denial of Service Counter-Measure,"

[68] A. Brighente, M. Conti, G. Kumar, R. Ghanbari, and R. Saha, "Knocking on Tangle's Doors: Security Analysis of IOTA Ports," in *2021 IEEE International Conference on Blockchain (Blockchain)*, 2021-12-01 2021: IEEE, doi: 10.1109/blockchain53845.2021.00067.

[69] M. A. Brady, I. Ullah, and P. J. M. Havinga, "DOSing Distributed Ledger Technology: IOTA," in *2021 IEEE 5th International Conference on Cryptography, Security and Privacy (CSP)*, 2021-01-08 2021: IEEE, doi: 10.1109/csp51677.2021.9357600.

[70] NHTSA, "Development of a Basic Safety Message for Tractor-Trailers for V2V Communications," 2016. [Online]. Available: https://www-esv.nhtsa.dot.gov/proceedings/24/files/24ESV-000379.PDF

[71] I. Facts, "IF exaggerates Chrysalis TPS by 4x," ed, 2021.

[72] T. I. Foundation. "Incentives to Run an IOTA Node." https://blog.iota.org/incentives-to-run-an-iota-node/ (accessed.

[73] Fool.com. "Average Credit Card Processing Fees and Costs in 2021." https://www.fool.com/the-ascent/research/average-credit-card-processing-fees-costs-america/ (accessed.

[74] W. H. Organization. "Road traffic injuries." https://www.who.int/news-room/fact-sheets/detail/road-traffic-injuries (accessed December 3, 2021).

[75] T. Zebra. "Winter Driving Statistics in 2021." https://github.com/iotaledger/streams/tree/develop/bindings (accessed.

[76] X. Zhang and D. Wang, "Adaptive Traffic Signal Control Mechanism for Intelligent Transportation Based on a Consortium Blockchain," *IEEE Access,* vol. 7, pp. 97281-97295, 2019-01-01 2019, doi: 10.1109/access.2019.2929259.

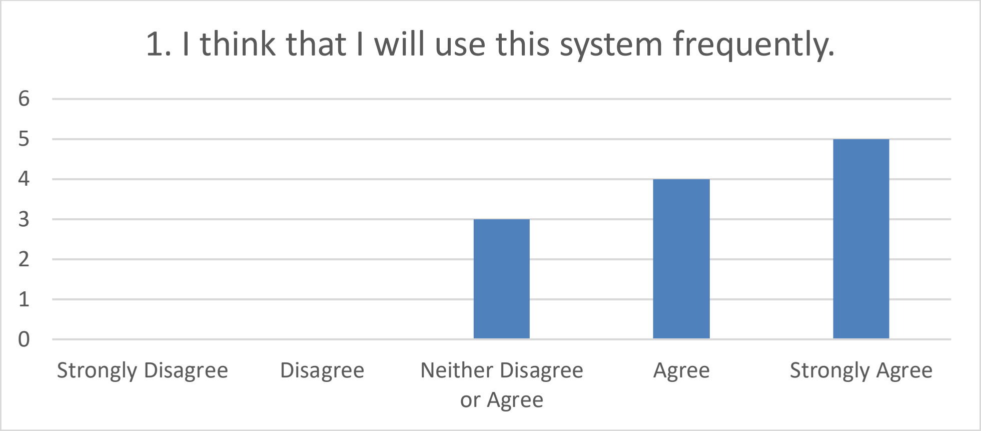
[77] B. Baruah and S. Dhal, "A Secure and Privacy-Preserved Road Condition Monitoring System," in *2020 International Conference on COMmunication Systems & NETworkS (COMSNETS)*, 2020-01-01 2020: IEEE, doi: 10.1109/comsnets48256.2020.9027482.

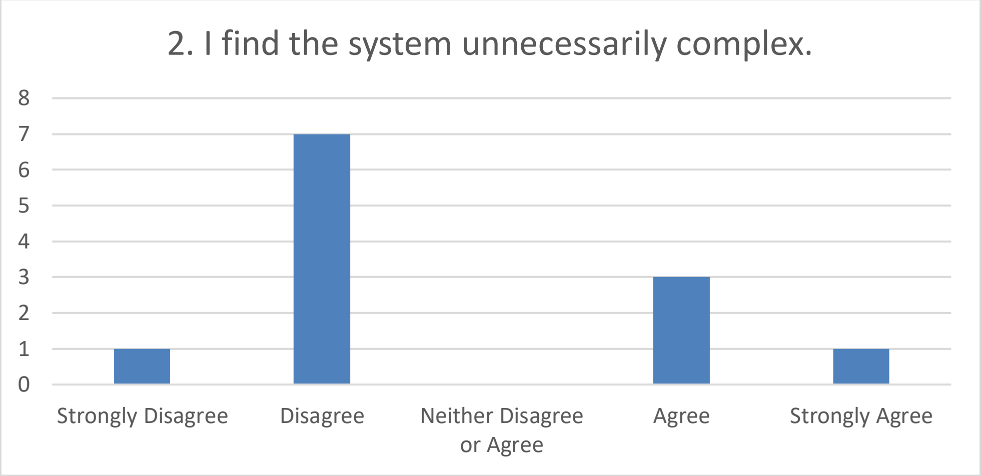
[78] A. Chowdhury, G. Karmakar, J. Kamruzzaman, and S. Islam, "Trustworthiness of Self-Driving Vehicles for Intelligent Transportation Systems in Industry Applications," *IEEE Transactions on Industrial Informatics,* vol. 17, no. 2, pp. 961-970, 2021-02-01 2021, doi: 10.1109/tii.2020.2987431.

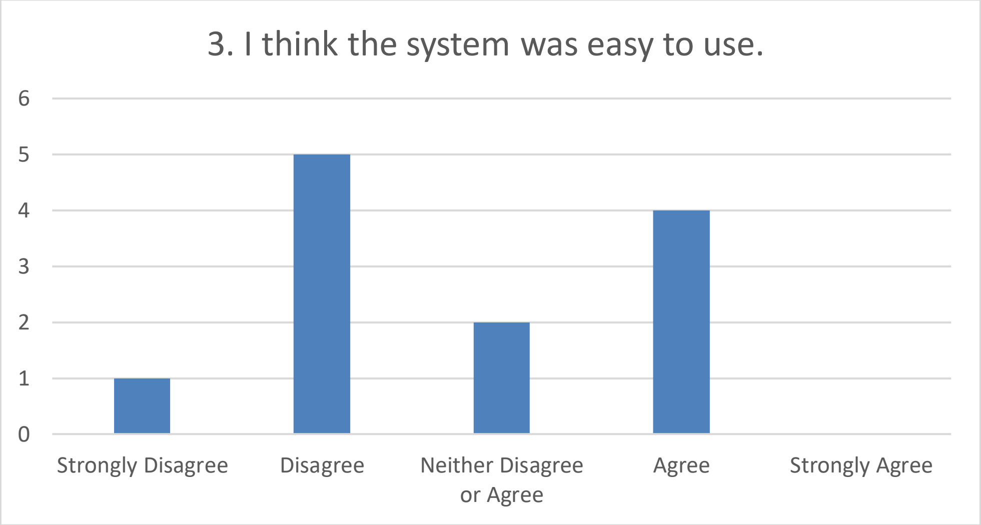
Appendix 1

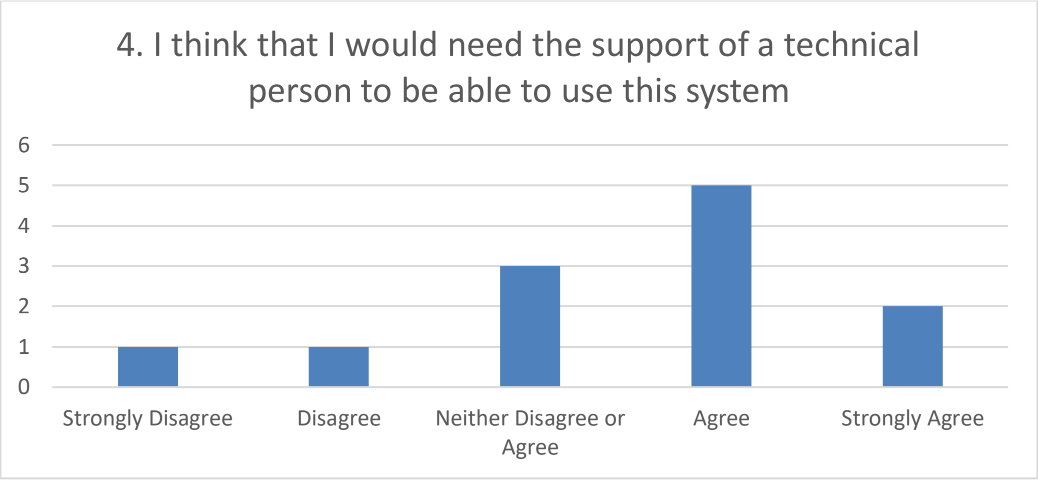
1) I think that I will use this system frequently.
2) I find the system unnecessarily complex.
3) I think the system is easy to use.
4) I think that I would need the support of a technical person to be able to use this system.
5) I find the various functions in this system were well integrated.
6) I think there was too much inconsistency in this system.
7) I would imagine that most people would learn to use this system very quickly.
8) I find the system very cumbersome to use.
9) I feel very confident using the system.
10) I needed to learn a lot of things before I could get going with this system.

Appendix 2 – Answers to the SUS Questionnaire

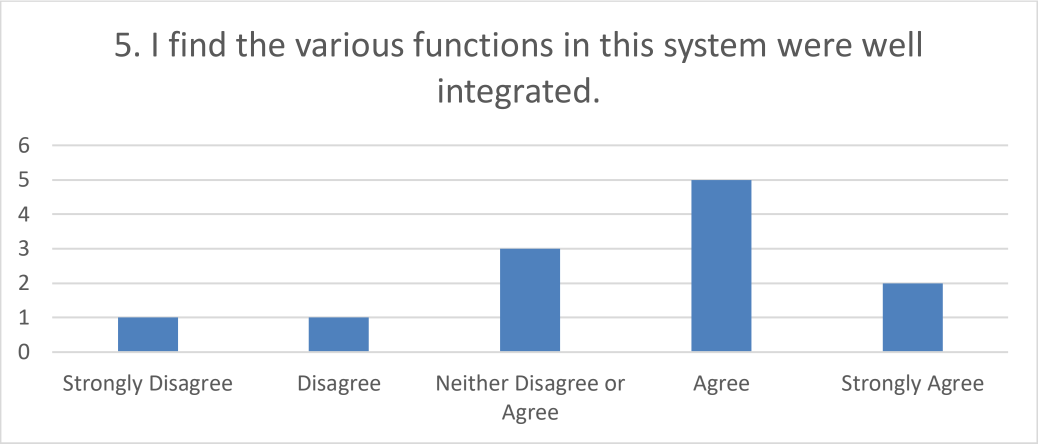




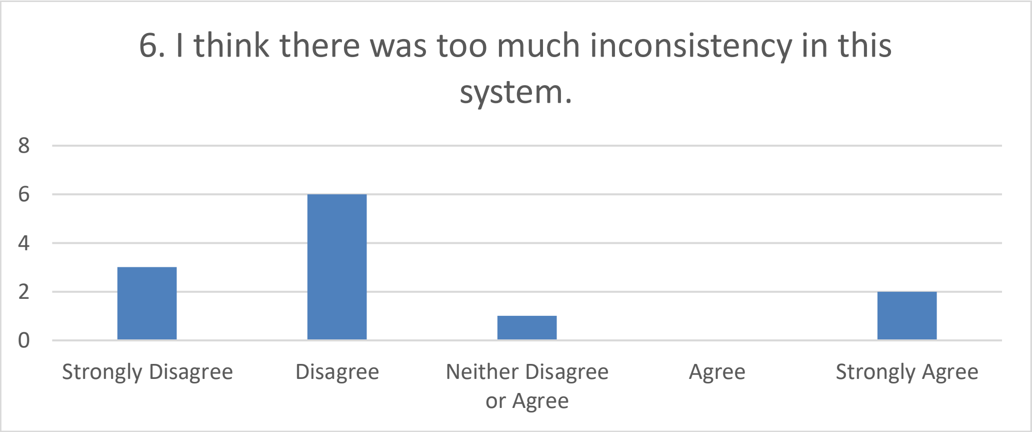




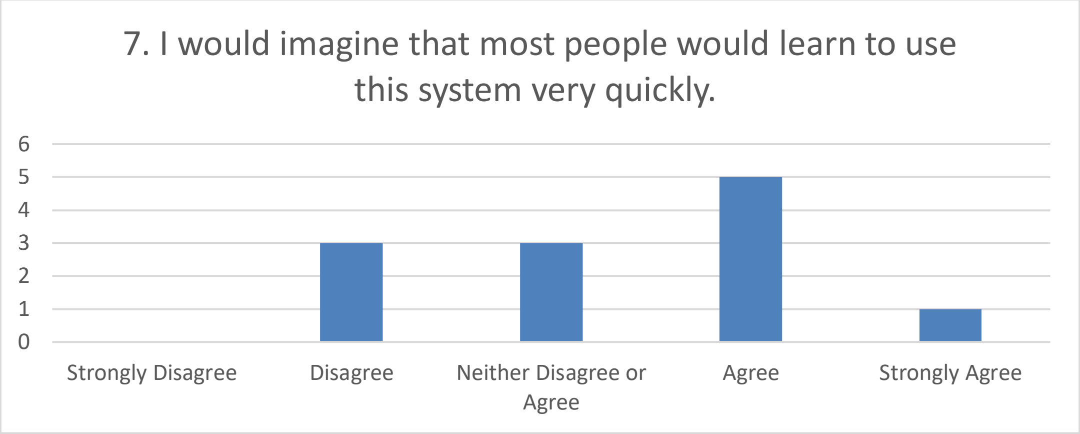
4. I think that I would need the support of a technical person to be able to use this system

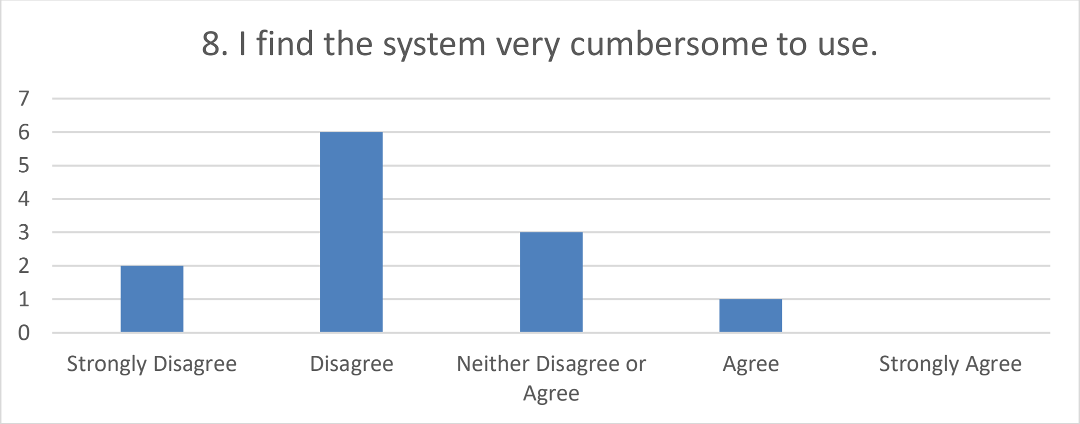


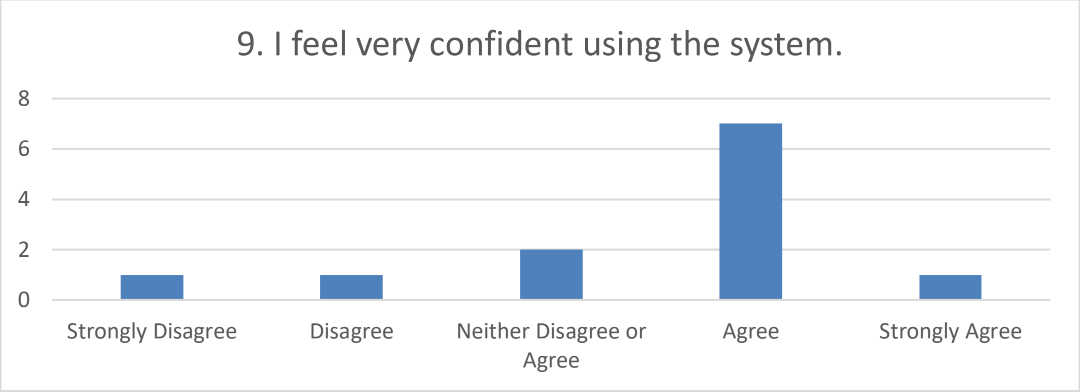
5. I find the various functions in this system were well integrated.

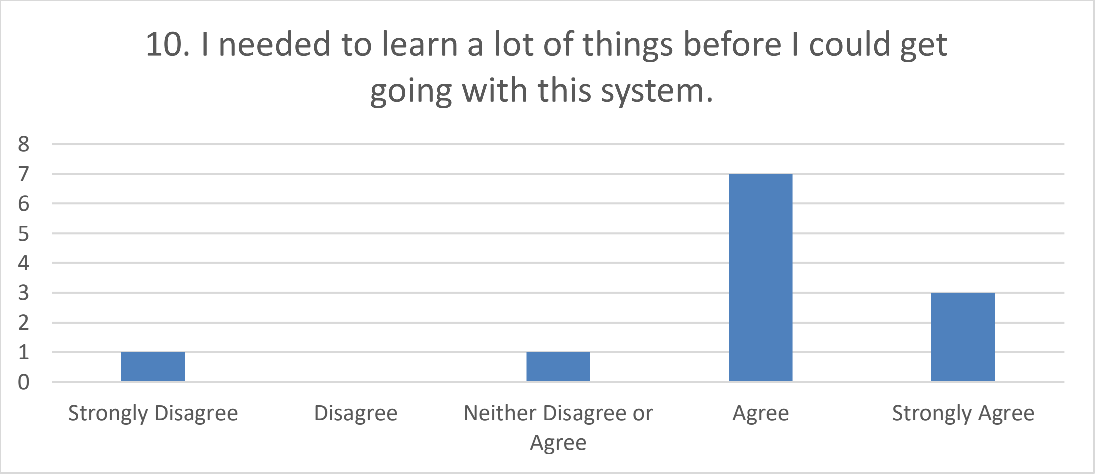


6. I think there was too much inconsistency in this system.


7. I would imagine that most people would learn to use this system very quickly.
6
5
4
3
2
1
0
Strongly Disagree
Disagree
Neither Disagree or Agree
Agree
Strongly Agree


8. I find the system very cumbersome to use.
7
6
5
4
3
2
1
0
Strongly Disagree
Disagree
Neither Disagree or Agree
Agree
Strongly Agree


9. I feel very confident using the system.
8
6
4
2
0
Strongly Disagree
Disagree
Neither Disagree or Agree
Agree
Strongly Agree


10. I needed to learn a lot of things before I could get going with this system.
8
7
6
5
4
3
2
1
0
Strongly Disagree
Disagree
Neither Disagree or Agree
Agree
Strongly Agree