Examining Distributed Ledger Technology (DLT) for V2X Communication: Road Condition Monitoring and Alerting System using the IOTA Framework

Author

James O'Connor

Masters in Engineering (MEng) in Connected and Autonomous Vehicles

Institute of Technology, Sligo

Supervisor of Research: Donny Hurley

Submitted to the Quality Qualifications Ireland (QQI)

December, 2021

Table of Contents

List of Figures

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 the 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 operates in such a way that it is more performant the more nodes participate in the network. In essence, it gets faster the more users it has [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 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 will:

1) Compare DLT to the current state-of-the-art to traditional architectures.
2) Identify the benefits and limitations of the IOTA Framework.
3) Quantify the ease of developing decentralized applications using IOTA framework.
4) Propose an approach to deploying Web 3.0[1] applications for autonomous vehicles.
5) 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 warnings 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] Web 3.0 refers to the next phase of the evolution of the Web/internet and is built on the core concepts of openness, decentralization and greater user utility.

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 to forecast and share potentially dangerous road conditions among nodes in 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 co-ordinator. 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[2]), each vehicle is

[2] 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].

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 1). 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.

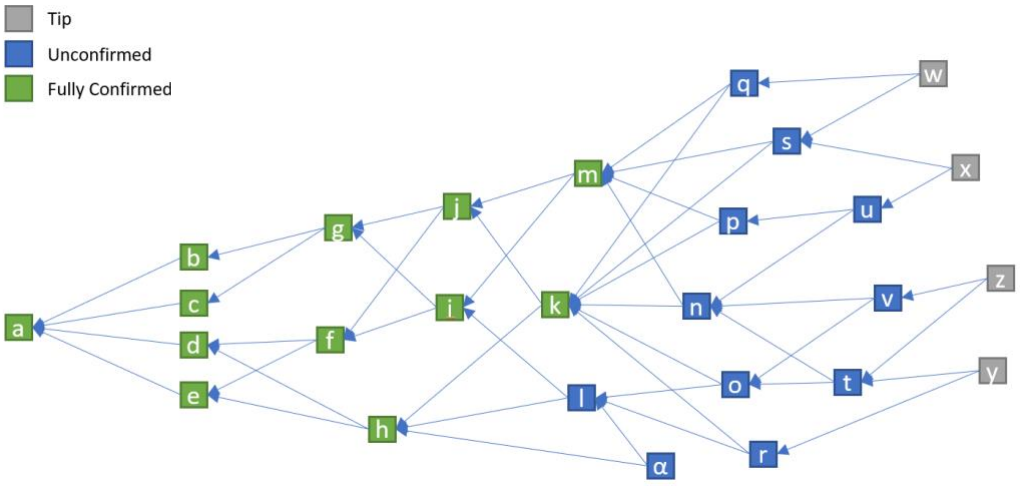

Figure 1: The Tangle Data Structure [29]

The main idea of the tangle is as follows; to create a new transaction on the Tangle (represented as vertices in Figure 1), users must work to approve two other transactions on the Tangle (represented as edges in Figure 1). 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) [30], 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 [30]. 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 2, 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 2, 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].

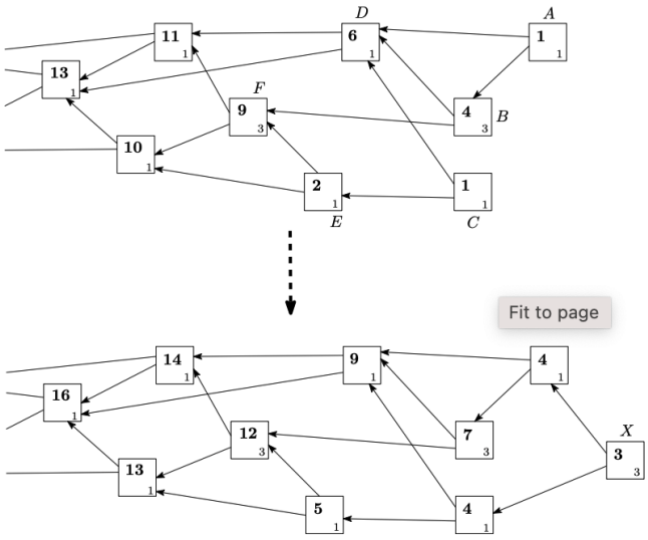

Figure 2: Tangle Transaction Cumulative Weights [28]

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 [31]. Nodes in the IOTA network run the core software and have three main functions:

1) To validate transactions and add them to the 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) [32]. 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.

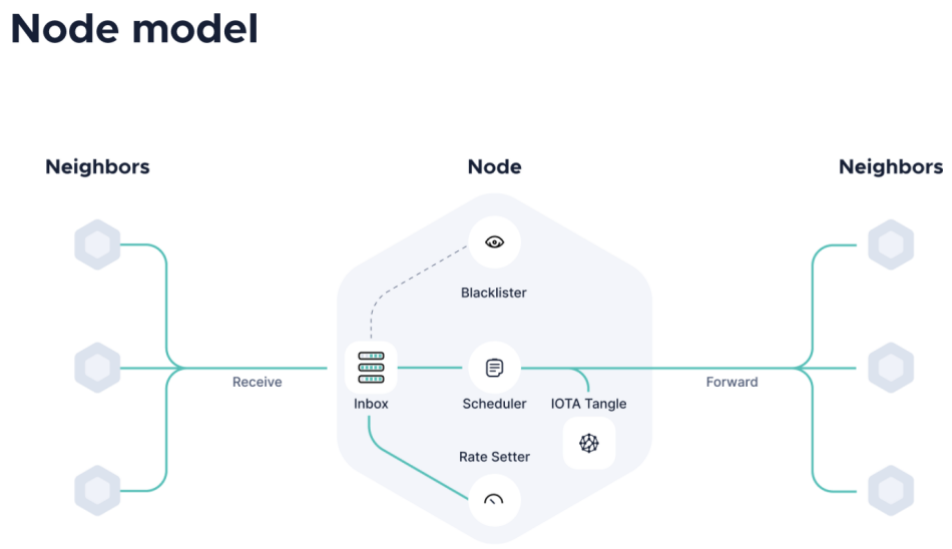

Figure 3: An IOTA Node [32]

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.* [33] 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.* [34] 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 [35]. 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 can be bought using other cryptocurrencies or *fiat* currency[3]. 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 ensures that 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 [32].

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 [36]. It allows devices to communicate securely and 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 multipe bindings including C and NodeJs [37].

To date, there has been no major studies on IOTA Streams, due to the product being in its nascence. Streams will be the communication tool used to develop the use case scenario. Other studies have been conducted using the legacy version of IOTA Streams

[3] 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.

called Masked Authenticated Messaging (MAM). Lamtzidis *et al.* [38] 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.

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 [39]. 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 [40, 41]. 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 [42] 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 [43] 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 [44]. 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” [45]. 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 five 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 for a road condition monitoring and alerting system, and IOTA Identity to manage device identification, each product using the underlying tangle technology. These new IOTA features will be integrated into a simulation application to examine the applicability of these new features.

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 [46]. 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 4 shows a breakdown of the main OBU components for a DSRC-based system.

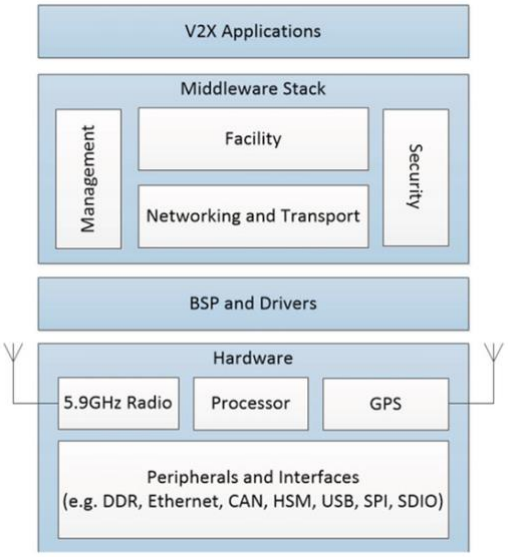

Figure 4: A DSRC-Based OBU [46]

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 [47]. 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 [48]. 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 [49]. For reference, Figure 5 gives a conceptual overview of the two system architectures.

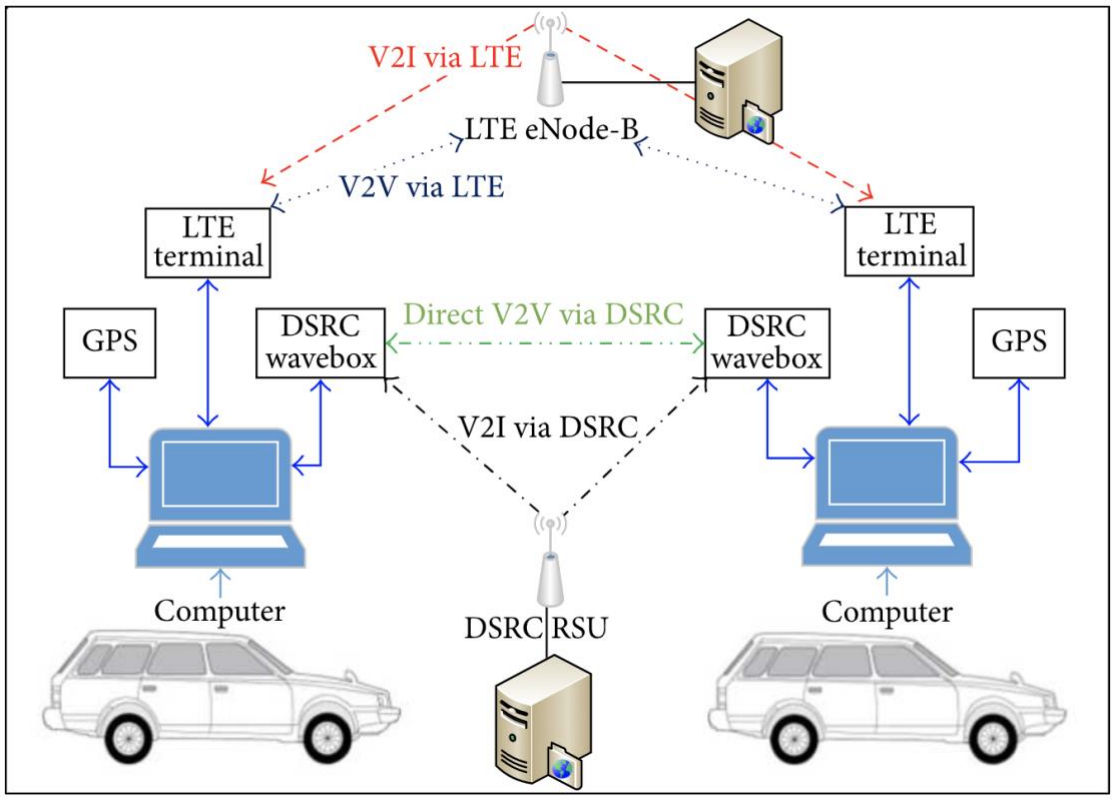

Figure 5: DSRC Versus Cellular Concept [50]

More recently, the Third Generation Partnership Project (3GPP) 4G Release 14 allowed for direct device-to-device communication [51]. 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 [50, 52] 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.

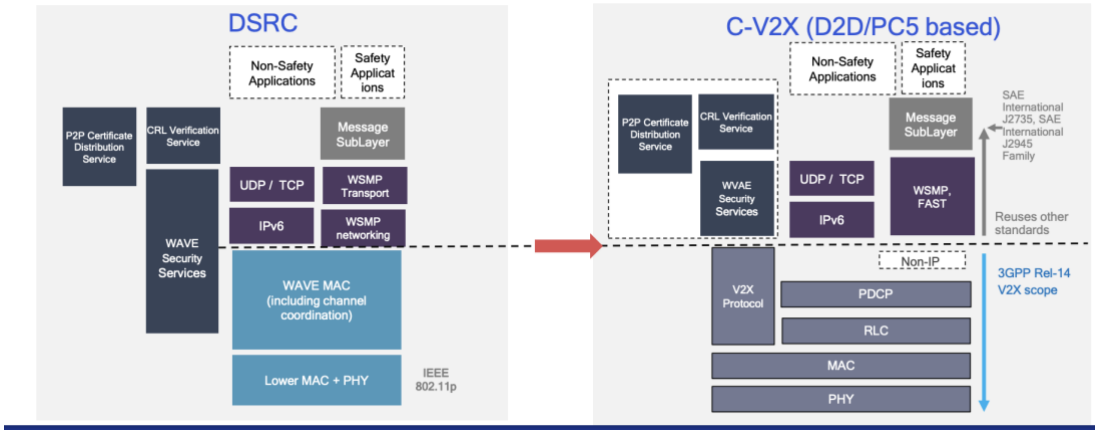

Figure 6: DSRC Versus C-V2X Architecture Comparison [53]

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) [54] 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 [54]. 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 [46] 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 [54].

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

Tesei *et al.* [40] 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.* [41]. 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 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 or all of these issues.

2.4 Rational for 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 [55]. 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 [56].

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.* [57] 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.* [58] 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.* [59] 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.

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 Bittcoin 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.

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] 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).

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

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

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

[33] 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.
[34] 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.
[35] 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.
[36] T. I. Foundation. "Final Alpha Release for IOTA Streams." https://blog.iota.org/final-alpha-release-for-iota-streams-5a4cfeca506c/ (accessed December 3, 2021).
[37] I. Foundation. "IOTA Streams." https://github.com/iotaledger/streams/tree/develop/bindings (accessed.
[38] 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.
[39] I. Foundation. "Identity.rs." https://github.com/iotaledger/identity.rs/ (accessed Dec 4th, 2021).
[40] 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.
[41] 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.
[42] 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.
[43] 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.
[44] 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).
[45] Elaad. "IOTA Charging Station." https://www.elaad.nl/projects/iota-charging-station/ (accessed.
[46] R. Miucic, *Connected Vehicles: Intelligent Transport Systems*. Detroit: Springer, 2019.
[47] 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.

[48] 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).
[49] 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.
[50] 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.
[51] 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.
[52] 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.
[53] Qualcomm, "ITS Stack," 2020. [Online]. Available: https://www.qualcomm.com/media/documents/files/c-v2x-its-stack.pdf
[54] (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
[55] W. H. Organization. "Road traffic injuries." https://www.who.int/news-room/fact-sheets/detail/road-traffic-injuries (accessed December 3, 2021).
[56] T. Zebra. "Winter Driving Statistics in 2021." https://github.com/iotaledger/streams/tree/develop/bindings (accessed.
[57] 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.
[58] 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.
[59] 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.