electronics

MDPI

Article

When Data Fly: An Open Data Trading System in Vehicular Ad Hoc Networks

Markus Lücking [1,*], Felix Kretzer [1], Niclas Kannengießer [2,3], Michael Beigl [4], Ali Sunyaev [2,3] and Wilhelm Stork [1]

1 Institute for Information Processing Technologies, Karlsruhe Institute of Technology, 76131 Karlsruhe, Germany; felix.kretzer@alumni.kit.edu (F.K.); wilhelm.stork@kit.edu (W.S.)
2 Institute of Applied Informatics and Formal Description Methods, Karlsruhe Institute of Technology, 76131 Karlsruhe, Germany; niclas.kannengiesser@kit.edu (N.K.); sunyaev@kit.edu (A.S.)
3 Competence Center for Applied Security Technology (KASTEL), 76131 Karlsruhe, Germany
4 Chair for Pervasive Computing Systems, Karlsruhe Institute of Technology, 76131 Karlsruhe, Germany; michael.beigl@kit.edu
* Correspondence: markus.luecking@partner.kit.edu; Tel.: +49-157-316-74676

Abstract: Communication between vehicles and their environment (i.e., vehicle-to-everything or V2X communication) in vehicular ad hoc networks (VANETs) has become of particular importance for smart cities. However, economic challenges, such as the cost incurred by data sharing (e.g., due to power consumption), hinder the integration of data sharing in open systems into smart city applications, such as dynamic environmental zones. Moving from open data sharing to open data trading can address the economic challenges and incentivize vehicle drivers to share their data. In this context, integrating distributed ledger technology (DLT) into open systems for data trading is promising for reducing the transaction cost of payments in data trading, avoiding dependencies on third parties, and guaranteeing openness. However, because the integration of DLT conflicts with the short available communication time between fast moving objects in VANETs, it remains unclear how open data trading in VANETs using DLT should be designed to be viable. In this work, we present a system design for data trading in VANETs using DLT. We measure the required communication time for data trading between a vehicle and a roadside unit in a real scenario and estimate the associated cost. Our results show that the proposed system design is technically feasible and economically viable.

Keywords: data trading; vehicular ad hoc networks (VANETs); blockchain; distributed ledger technology (DLT); token economy; vehicle-to-everything (V2X)

Citation: Lücking, M.; Kretzer, F.; Kannengießer, N.; Beigl, M.; Sunyaev, A.; Stork, W. When Data Fly: An Open Data Trading System in Vehicular Ad Hoc Networks. *Electronics* **2021**, *10*, 654. https://doi.org/10.3390/electronics10060654

Academic Editor: Mariusz Nowostawski

Received: 18 January 2021
Accepted: 2 March 2021
Published: 11 March 2021

1. Introduction

Driven by the increasing automation and optimization of road traffic, the communication between vehicles and their surroundings (i.e., vehicle-to-everything or V2X communication) has become of special interest for designing smart cities. Integrating open V2X data sharing into traffic (software) applications (e.g., driver assistance) lays the foundation for future smart cities [1] that, for example, dynamically manage traffic flow under consideration of real-time traffic and air pollution data. To gather real-time data, vehicles can share on-board data (e.g., location information [2] or exhaust values [3]) with a roadside unit (RSU) when passing it. As an alternative or in addition to operating sensor networks, a smart city's road traffic department can use the shared data to monitor traffic and to set up ad hoc environmental zones in urban regions where the pollution level exceeds a defined threshold [4]. In the following text, we will use the term X-Node when referring to RSUs and vehicles.

Despite the potentials for sharing data in open systems for smart cities (e.g., setting up ad hoc environmental zones based on vehicle emissions), unique *economic* and *technical*

challenges hinder the operation of viable open data sharing systems for X-Nodes. *Economic challenges* relate to the design of an incentive mechanism that should sufficiently motivate X-Node controllers (e.g., RSU owners or vehicle drivers) to share data related to their X-Node. To address this challenge, existing research recommends integrating a payment service into a data sharing system and switching from free data sharing to data trading in VANETs [5,6]. Payments for data should, at a minimum, cover X-Node operating costs for sharing data (e.g., electric power consumption and hardware costs) [7] and should further incentivize the participation of X-Node controllers in data trading (e.g., to compensate confidentiality concerns). Several studies estimate a reasonable price for data sets to be traded between X-Nodes at a few micro-cents [8,9]. The low value of data sets to be exchanged between X-Nodes is mostly below the transaction fees charged by most traditional payment services. For example, the minimum transaction fees using VISA payments often vary between 0.1€ and 0.21€ [10]. The high transaction fees render data trading in open systems via V2X communication uneconomical and, thus, hinder the use of open data trading [11,12].

To prevent dependence on third parties that can, for example, charge fees for data trading, and to allow any X-Node controller to participate in data trading, the data trading system should be designed to be decentralized and open. However, decentralization and openness in data trading cause economic challenges beyond financial sustainability. To achieve adoption of the data trading system, X-Node controllers must place trust in the appropriate and automated execution of data trades between X-Nodes. Therefore, X-Node controllers must trust the mechanisms (e.g., authentication mechanisms) by which their X-Node assesses the reliability of other X-Nodes with respect to their claims about data for sale. Despite valuable contributions regarding the design of services offering mechanisms that can increase the trust of individuals in digital systems (e.g., authentication services [13] or reputation services [14]), it remains unclear how such services can be integrated into open data trading systems that are constrained by unique technical challenges.

Technical challenges question the feasibility of open data trading systems using VANETs. In VANETs, X-Nodes communicate directly with X-Nodes in their immediate vicinity using wireless ad hoc networks, such as vehicular ad hoc networks (VANETs). When driving, the distances between X-Nodes change, X-Nodes dynamically join new VANETs with X-Nodes in their current vicinity and leave VANETs with X-Nodes that leave their direct communication range. Therefore, the direct communication time between X-Nodes is limited. For example, two cars approaching each other at 50 km h^{-1} with a maximum communication range of 500 m only have 35 s for data trading in the VANET [15]. The limited communication time represents a special challenge for the integration of services (e.g., authentication, payment, or reputation services) required to address the economic challenges. It remains unclear how such services can be integrated into data trading systems while preserving the openness of the data trading system and still offering sufficient time for actual data transmission within the limited communication time.

To address the economic challenges, extant research (e.g., [9,16]) investigated the use of distributed ledger technology (DLT). DLT enables the operation of highly available, tamper-resistant distributed databases (i.e., distributed ledgers) that are operated by distributed storage and computing devices (i.e., DLT nodes) [17]. DLT was used, for example, to support payments at low charge (e.g., [18,19]), to achieve independence from trusted third parties (e.g., [20,21]), and to achieve a high degree of openness of the data trading system (e.g., [22]). Despite the beneficial characteristics of DLT for data trading systems (e.g., low or even no transaction fees for payments and a high degree of openness), existing studies (e.g., [23,24]) show that several DLT characteristics are at odds with the characteristics of direct wireless ad hoc communication. For example, the time required until a transaction can be considered confirmed on distributed ledgers often exceeds the time available for the direct communication between X-Nodes in VANETs [23]. It remains unclear to what extent DLT can be used to address the economic challenges in open data trading considering the limited time for direct communication in VANETs. To support

open data trading between X-Nodes in VANETs and clarify the potential of DLT to address prevalent economic and technical challenges, we ask the following research question:

RQ: How can an open data trading system be designed for smart cities?

To answer our research question, we developed a prototypical open data trading system based on VANETs and DLT. The data trading system comprises three main subsystems that involve a distributed ledger: an *authentication system*, a *payment system*, and a *reputation management system*. X-Nodes directly communicate with each other in VANETs to advertise and transmit data. We implemented and evaluated the designed data trading system in a real-world scenario regarding the cost of data trading and the consumed communication time to trade data between X-Nodes (see https://github.com/MarkusLue/When_data_fly accessed on 10 March 2021).

Our work contributes to research and practice as we show that low-value data trading is economically feasible under real-world conditions when using DLT and VANETs based on the IEEE 802.11p protocol. Our viability assessment reveals key factors (e.g., communication overhead) for the optimization of open data trading systems using DLT and VANETs. By identifying a lower boundary for data prices that enables economically sustainable data trading in VANETs, we support the development of business models related to open data trading of low-value data. Moreover, this work provides valuable insights regarding the trade-off between the available communication time for data trading and the use of additional services (i.e., payment or reputation management services) to incentivize X-Node controllers to share data in open systems for data trading.

This work is structured as follows. First, we introduce the foundations of VANETs and DLT. Second, we describe the design of the proposed open data trading system, its prototypical implementation, and discuss the security of the designed system. Third, we describe the experimental design to measure the required communication time for data trades between X-Nodes and to derive the required data trading cost. Fourth, we compare the proposed data trading system with existing research and highlight how we advance prior research. Fifth, we discuss our principal findings, explain the limitations of our work, and provide starting points for future research directions.

2. Background

2.1. Vehicular Ad Hoc Networks

VANETs are a type of wireless ad hoc network and are designed to connect mobile (e.g., vehicles) and stationary X-Nodes (e.g., RSUs). VANETs can cope with dynamic changes in their network topology (e.g., caused by changes in the position of mobile X-Nodes) and allow for the communication between X-Nodes in direct (single hop) and indirect (multiple hops) ways [25]. Each X-Node is connected to other X-Nodes in their communication range, which allows for loosely coupled mesh networks. To enable the communication between X-Nodes in VANETs independent of proprietary communication systems (e.g., base stations) [26], the wireless access in vehicular environment (WAVE) protocol stack has been developed [27]. The WAVE protocol stack comprises protocols and standards for the dedicated short-range communication (DSRC) that is optimized for use in automotive communication [25]. For DSRC protocols, the frequency range between 5.850 GHz to 5.925 GHz was reserved [28]. As one of the protocols defined in DSRC, the IEEE 802.11p protocol became one of the standards or the standard for V2X communication in many traffic applications [29] and is used by various automotive manufacturers (e.g., Toyota and Volkswagen [30]).

2.2. Distributed Ledger Technology

DLT enables the operation of highly available, append-only distributed databases (i.e., distributed ledgers) that are maintained by distributed storage and computing devices (i.e., DLT nodes) in an untrustworthy environment [17]. An untrustworthy environment is characterized by the arbitrary occurrence of crashes or fraudulent behavior of DLT nodes (e.g., issuing incorrect information). The participation in a distributed ledger can be

restricted to only defined DLT nodes (private distributed ledgers) or unrestricted (public distributed ledger). From the set of participating DLT nodes, either all (permissionless distributed ledger) or only defined (permissioned distributed ledger) DLT nodes are authorized to commit new transactions to the ledger [17]. To achieve consistency among all DLT nodes, distributed ledgers use a consensus mechanism (e.g., the Nakamoto consensus).

IOTA is an open-source DLT protocol using a nonlinear directed acyclic graph to store data in the *IOTA Tangle* [31]. The IOTA Tangle is designed for applications in the Internet of things [32], offers high transaction throughput, and charges no transaction fees. In the IOTA network, a transaction contains an address. IOTA addresses are generated from a randomly chosen seed that can be used like a password to access, spend, and receive tokens. The seed can be used to create private keys and transaction addresses. Using private keys, transaction issuers can prove to IOTA nodes that they own a certain address or the corresponding IOTA tokens and transfer them from one address to another.

DLT nodes in the IOTA network, *IOTA nodes*, append new transactions to their local ledger without immediate synchronization with other nodes [31]. Before an IOTA node appends a new transaction, it validates the transaction considering two criteria: First, the transaction issuer must have validated two transactions that were already stored on the ledger; second, the transaction issuer must find a valid nonce before issuing transactions. To find a valid nonce, the transaction issuer concatenates the transaction with randomly chosen nonces and calculates the hash value for the concatenation using the Curl-P81 hash function. For a nonce to be valid, the number of zeros with which the resulting hash value ends must match the number of zeros defined by the IOTA protocol [33]. Otherwise, the transaction issuer must repeat this procedure with another nonce until a valid nonce is found. The process of finding a valid nonce is considered proof-of-work (PoW). We regard the process of creating and testing a nonce as *PoW operation*.

2.3. Open Data Trading with Distributed Ledger Technology

To move data sharing to data trading and increase the trust of X-Node controllers in data trading in open systems with unknown trading parties, open systems for data trading should offer a *decentralized identity management*, *reputation management*, and *payments* [18]. Among several applications of DLT (e.g., managing pollution data collection [34]), these three services can be provided in a decentralized manner using DLT.

Decentralized identity management concerns the creation, modification, and assignment of digital identity representations of subjects (e.g., devices or humans; referred to as DID subjects) with no need for a central certificate authority [35]. Thereby, decentralized identity management addresses the drawbacks of traditional centralized public key infrastructures (PKIs), in which a central certification authority is a single point of failure that can issue forged certificates or even cause a denial of service of the overall system in the event of a server failure.

Decentralized identity management systems use decentralized document identifiers (DIDs) pointing to a DID document that includes personal information of (e.g., the name or role) or services offered by a DID subject [36]. DID documents associated with DID subjects are managed by DID controllers (e.g., human users) [37]. To authenticate themselves as the legitimate owner of a DID subject, DID controllers include authentication data (e.g., public keys) in the DID document.

The DID document is only managed by the DID controller and could include invalid information (e.g., the DID subject's identity may be invalid). To suggest the validity of DID documents, users that interacted with a DID subject can issue verifiable claims that consist of a claim and an attestation. The claim is a statement about the validity of information included in the DID document. The attestation includes meta data (e.g., the name of the claim issuer, validity period, and signature scheme) and the digital signature of the attestator to verify the claim [38]. On the basis of the aggregation of all verifiable claims, the validity of a DID document and the authenticity of an identity can be assumed.

Reputation management is concerned with suggesting the reliability of an identity regarding the provision of a service based on previous experiences with the service [39]. In open data trading, reputation management can prevent the spread of malicious data and stimulate collaboration among X-Nodes by collecting, distributing, and aggregating feedback about X-Node quality of service [40]. The concept of verifiable claims applied in decentralized identity management systems also applies to reputation models based on ratings (e.g., five-star ratings). For instance, after two X-Nodes trade data, both can rate each other by attaching verifiable claims to the corresponding DID. These verifiable claims assist other X-Nodes in deciding for or against data trading with a certain X-Node [41].

Payments via a distributed ledger concern the transfer of ownership of tokens that digitally represent assets (e.g., fiat money) with no need for a central authority [42]. Because of the usually low transaction throughput in distributed ledgers, payment channels were developed [43]. Payment channels can reduce the number of required interactions with a distributed ledger by aggregating multiple transactions into a set (e.g., a bundle in IOTA). Instead of individually sending transactions to the DLT network, only the set of transactions is sent and attached to the distributed ledger.

When using payment channels, payment channel participants face the *Buyer and Seller's dilemma* [44] because the transmission of data sets and corresponding payments cannot occur simultaneously (i.e., the service is paid before or after usage). The buyer can use the seller's data but leaves without paying for it, or the seller accepts the buyer's payment without sending the data. To solve the Buyer and Seller's dilemma, payment channels require the seller (e.g., data provider) and the buyer (e.g., data consumer) to deposit a sufficiently high collateral in the form of tokens on a shared, multi-signature address on the distributed ledger. The collateral must be at least as high as the price of the data and must be deposited by both X-Nodes. If the collateral were less than the price, the buyer would have no monetary incentive to finalize the data trade. The multi-signature address allows the channel participants (i.e., the service seller and buyer) to only transfer tokens from the multi-signature address after all channel participants have signed the respective bundle of transactions. For each transaction in which the service buyer sends tokens to the seller, the seller creates a separate transaction to transfer the same number of tokens from its tokens previously deposited on the multi-signature address to their own address. Moving tokens from a shared deposit motivates the channel participants to appropriately provide a requested service, while assuring adequate payments (e.g., payments per meter driven with a rental car [45]). Next, the channel participants exchange an arbitrary number of transaction bundles over a payment channel external to the distributed ledger. The bundle is digitally signed by all channel participants and must be valid to transfer tokens from the shared multi-signature address. After each payment, all channel participants update their version of the valid bundle. Each channel participant can close the payment channel at any time by sending the bundle of valid transactions to the distributed ledger. Channel participants have an interest in sending only bundles of valid transactions that do not leave unspent tokens on their shared multi-signature address, because tokens that remain on the shared multi-signature address are not automatically transferred back to the addresses of the individual channel participants [46].

3. Design and Implementation of the Open Data Trading System

3.1. System Model

3.1.1. System Components

The data trading system that we propose and analyze in this work comprises X-Nodes (i.e., RSUs and vehicles) and a distributed ledger (see Figure 1). X-Nodes can take two principal nodes: *data provider* or *data consumer*. X-Nodes acting as a data provider offer data (e.g., their current fuel consumption [47] or CO_2 emissions [48]) for data trades to other X-Nodes. If an X-Node accepts an offer by a data provider, that X-Node takes the role of a data consumer. X-Nodes communicate with each other for data trading in VANETs via DSRC.

For data trading, X-Nodes use three services that are available on a distributed ledger: *authentication service*, *reputation management service*, and *payment service*. The authentication service enables X-Nodes to verify the identity of their data trading partner (i.e., data provider or data consumer). The reputation management system allows X-Nodes to assume the reliability of a potential data trading partner based on prior ratings and to rate data trading partners. The payment service allows X-Nodes to make micropayments for received data.

To use these services, X-Nodes interact with the distributed ledger via long-range communication. For long-range communication, stationary X-Nodes (e.g., RSUs) use a stationary wireless network (e.g., WiFi) and mobile X-Nodes use a mobile one (e.g., cellular network). Stationary wireless networks offer high data rates and low network usage cost. Nevertheless, stationary wireless networks can only be used at fixed positions and have a limited communication range, which is why they do not guarantee permanent connectivity to mobile X-Nodes. Mobile wireless networks aim at the provision of full network coverage and permanent connectivity of devices with the internet. Yet, compared to stationary wireless networks, their data rate is lower, their network usage costs are higher, and their network capacity can be exceeded, resulting in a longer data transmission time [49].

As a distributed ledger, we chose the IOTA Tangle (see Section 2.2) to offer high scalability and transaction throughput, to support micropayments at no charge (i.e., no transactions fees), and to achieve openness of the data trading system so that every X-Node can arbitrarily join and leave the IOTA network. In addition, the IOTA protocol supports reducing operational cost for data trading by allowing for lightweight PoW operations compared to other public-permissionless distributed ledgers.

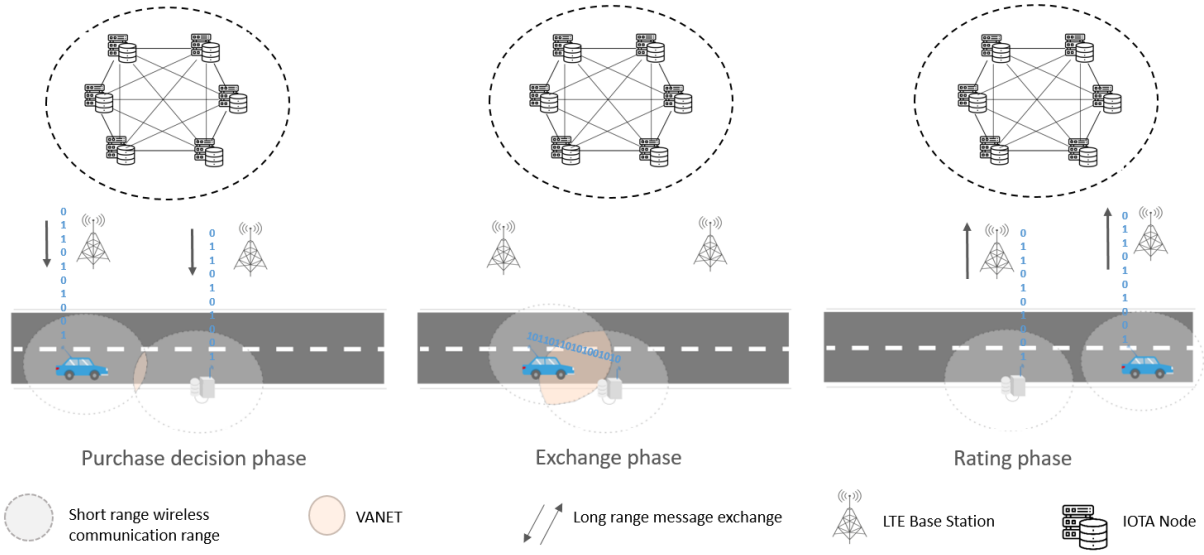

Figure 1. Schematic overview of the data trading system. For better readability, we have omitted the communication with the distributed ledger for the creation of the multi-signature address in the exchange phase.

3.1.2. Data Trading Sessions

Data trading sessions refer to the actions involved in allowing X-Nodes to trade data. After the initial *advertisement phase*, each data trading session comprises a sequence of three phases: the *purchase decision phase*, *exchange phase*, and *rating phase*. In the *purchase decision phase*, X-Nodes first authenticate the identity of the X-Node with which they consider a data trade. If the authentication is successful, the X-Nodes decide whether to exchange data and become data trading partners based on the reputation of the other X-Nodes. If both X-Nodes decide to trade data, the X-Nodes start the *exchange phase* by opening a payment channel. After the traded data and payment exchange, an X-Node closes the payment

channel, and both X-Nodes can submit a rating of the other X-Node to the reputation management system on the distributed ledger in the *rating phase*.

Advertisement phase. To start a data trading session, X-Nodes inform other X-Nodes about the data they offer for data trading in the *advertisement phase*. For this purpose, the data provider creates a data trading offer, digitally signs the offer, puts the offer and the digital signature into an advertisement message, and periodically broadcasts (single hop) the advertisement message to X-Nodes in their VANET. The offer contains information about the identity of the data provider (i.e., its public key and DID document), the offered data set (e.g., vehicle type or emission standard), and the price of the offered data set. Any X-Node passing through the data provider's transmission range can set up a VANET with the data provider to receive its advertisement message (see Figure 1) and check whether the offer meets its individual criteria (e.g., type of data, price, or reputation score). If an offer suits the data consumer's criteria, the data consumer can start a data trading session.

Purchase decision phase. To authenticate the data provider's identity, the data consumer uses the data provider's public key received in the advertisement message. Using the public key, the data consumer fetches verifiable claims associated with the data provider's identity address from the IOTA Tangle (see Section 2.3). An identity address represents a DID and is generated by hashing the concatenation of the X-Node's public key and identity claim (e.g, vehicle type) included in the X-Node's DID document. To reduce the time and cost for downloading verifiable claims from the IOTA Tangle, data consumers only download verifiable claims issued by known X-Nodes. An X-Node is considered known if it attached verifiable claims to the data consumer's and data provider's identity address [50].

Newly created X-Node identities start with the lowest assumed reliability because no verifiable claims are attached to these identity addresses. To counter this cold start issue, X-Node controllers can bootstrap the reliability of their X-Node's identity information by using verifiable claims issued by trusted third parties or public institutions (e.g., vehicle manufacturers or a department of motor vehicles).

In addition to verifiable claims related to the identity of the data provider, the data consumer retrieves verifiable claims related to the data provider's previous data trades from the IOTA Tangle to assess its reputation (see Section 3.1.2). Verifiable claims are stored on the IOTA reputation addresses of an X-Node. Similar to the identity addresses, a reputation address represents a DID document that is generated by hashing the concatenation of the X-Node's public key and reputation-related DID document. X-Nodes can issue verifiable claims to their data trading partners' reputation addresses to rate data trades.

If the data provider's identity can be authenticated and its reputation satisfies the requirements of the data consumer (e.g., ratings from known X-Nodes exceed a threshold), the data consumer generates an advertisement reply message including the data consumer's public key and a counteroffer (e.g., for price negotiation) or a confirmation of the trading conditions. The data consumer encrypts and signs the advertisement reply message using the data provider's public key and broadcasts the advertisement reply message in the VANET, including its submission timestamps and random data to prevent replay attacks. After the data provider receives the reply message, the data provider authenticates the data consumer and assesses its reputation following the described procedure.

Exchange phase In the *exchange phase*, the proposed data trading system uses payment channels (see Section 2.3) comprising three sub-phases: the *open payment channel*, *data trade*, and the *close payment channel*. The *open payment channel* sub-phase starts for both X-Nodes with the calculation and exchange of an advanced encryption standard (AES) key fragment to create a shared secret (i.e., session key). The session key is built by adding both AES key fragments to a single AES session key. The AES key fragments are encrypted using the trading partner's public key to prevent other X-Nodes from reading the session key and then broadcasted to the VANET. Using the session key, the X-Nodes encrypt all subsequent network messages in the VANET related to the data trade. We chose symmetric encryption

for most of the messages because of its better performance compared to asymmetric encryption [51]. Next, the data provider and consumer open a payment channel.

In the *data trade* sub-phase, the data consumer and data provider exchange payments and the actual data sets (see Section 3.2). For each payment, the data consumer creates a new bundle, puts transactions in the bundle to pay for the first data set, and digitally signs the bundle. Subsequently, the data consumer puts the bundle and its signature into a payment message, encrypts the message using the session key, and broadcasts the message in the VANET. The data provider decrypts the payment message, verifies the correctness of the bundle hash using the transaction data included in the bundle, signs the bundle, and locally stores the bundle. Next, the data provider puts the signature of the bundle hash (that is now valid for transferring tokens from the multi-signature address) and the just-paid data set into a new payment message, encrypts the payment message, and broadcasts the payment message in the VANET. The X-Nodes repeat this procedure until the data transfer is completed or the X-Nodes are no longer connected to each other.

In the *close payment channel* sub-phase, the X-Nodes finish the data trade. First, both X-Nodes verify that their collateral has been successfully transferred to their shared multi-signature address (i.e., have been confirmed by the IOTA network). After the X-Nodes receive the confirmation, the two X-Nodes can independently send their valid bundles to the IOTA Tangle at any time to close the payment channel and enforce the payments. This way, the data provider can still receive payments for transferred data sets in case the connection between data consumer and data provider breaks down and not all data sets can be exchanged. Unlike the previous two sub-phases, the *close payment channel* phase does not require DSRC between the X-Nodes.

Rating phase. After the *exchange phase*, the data consumer and provider can rate their data trading partner by attesting reputation-related verifiable claims stored on the IOTA Tangle, for example, to express that the traded data complies with the data offer from the advertisement message. For the rating, an X-Node sends an IOTA transaction that includes a verifiable claim to the reputation address of its corresponding trading partner. Each verifiable claim contains a numeric rating score between zero and five to disagree (zero) or agree (five) with the statements in the respective data trading partner's DID document. The reputation of an X-Node results from the aggregation of rating scores included in verifiable claims attested by known X-Nodes.

3.2. Prototypical Implementation

We implemented the data trading system using one mobile (i.e., a car) and one stationary (i.e., RSU) X-Node. The car is equipped with an on-board unit to extract vehicle parameters (e.g., speed, fuel consumption [47], or CO_2 emissions [48]) and a GPS module. All X-Nodes are equipped with computing units (i.e., a Raspberry Pi 4B) and communication modules for wireless DSRC and long-range communication. For long-range communication, we attached an LTE/UMTS module to the car and connected the RSU to a conventional WiFi router (Speedport Smart 3). Using the open-source experimentation and prototyping platform OpenC2X [52], we configured two WiFi routers (TP-Link WDR 3600 [53]) for the X-Nodes communication via DSRC standards. We equipped each X-Node with one router for the communication in VANETs over IEEE 802.11p [54]. Compared to other short-range wireless communication protocols (e.g., Bluetooth or ZigBee), the IEEE 802.11p protocol transmits data faster [55], does not rely on fixed access points (i.e., cellular base stations) [56], and uses a frequency spectrum (ITS-G5) at no charge, reducing the transmission cost (e.g., no additional service provider cost) [57]. OpenC2X does not support the full intelligent transportation system (ITS) protocol stack. For instance, the basic transport protocol (BTP) facilities found in ETSI EN 302 636-5-1 [58] for sending messages between X-Nodes is not supported by OpenC2X. Thus, we customized cooperative awareness messages (CAMs) to transmit data (single hop) between X-Nodes in VANETs [59]. We used the CAM header and payload of the standard CAM structure to transmit customized messages (e.g., payment messages). Unfortunately, the maximum

payload (1.300 B [60]) of a single CAM is too small to transmit a single IOTA transaction (1.590 B [61]). Therefore, we split all messages (e.g., the payment message) that contain IOTA transactions into several message fragments before their transmission. We attached a multi-part attribute to each transmitted message fragment to express the total number of CAMs required to transmit the full message and the individual number of the message fragment. This way, the CAM receiver can check if all message fragments have been successfully received to assemble the message.

For the communication with the IOTA Tangle, we used the IOTA node software *Hornet v0.5.6*, client library in Java *v1.0.0-beta7*, and IOTA Comnet with MWM 14 to have the same difficulty for the nonce calculation as the current IOTA Mainnet. PoW operations (see Section 2.2) are usually time-consuming on general purpose CPUs, which is crucial in open data trading because of the limited communication time. Field programmable gate array (FPGA) boards can decrease the required time of PoW operations by a factor of 300 compared to that of the single core processors of a Raspberry Pi 3B [62] by parallelizing PoW operations. Consistent with prior work [62], we used a Zynq Z-7020 FPGA board [63] to expedite the finding of a valid nonce at a minimal magnitude weight of 14 to 400 ms on average. In our prototypical implementation, the car operated the FPGA board and the RSU outsourced its PoW operations in the *open payment channel* sub-phase to the car. In the *close payment channel* sub-phase, only the car sent the final IOTA transactions to the IOTA network.

For the authentication and reputation system, we used two separate IOTA addresses (i.e., identity and reputation addresses) as DIDs. Information about the X-Node's identity and previous data trades are stored unencrypted and publicly accessible on the identity address and reputation address (see Section 3.1). To confirm an X-Node's identity or reputation, X-Nodes send verifiable claims to the corresponding address (i.e., the identity or reputation address) of its data trading partner (see Section 3.1.2). As verifiable claims, we use IOTA transactions with a JSON object, including the public key of the attesting X-Node, its digital signature, and its actual identity confirmation or rating score regarding the data trade. Additionally, each verifiable claim is tagged with the hashed and condensed public key of the attestator to support other X-Nodes in faster filtering verifiable claims from known X-Nodes by only downloading verifiable claims associated with public keys of known X-Nodes.

3.3. Security of the Data Trading System

3.3.1. Network Security

To discuss the security of the proposed data trading system from the network perspective, we apply the Dolev-Yao adversary model [64]. The Dolev-Yao adversary model comprises an insecure communication channel between two parties (e.g., X-Nodes) and an adversary as an active saboteur. In the Dolev-Yao model, the adversary has six principal capabilities for handling messages [65]: *eavesdropping*, *forging*, *replaying*, *delaying and rushing*, *reordering*, and *deleting*. In the following section, we adopt the descriptions for the capabilities of the adversary provided by Walker [65].

Eavesdropping: *An adversary can listen to any message transmitted in the network.*

In VANETs, messages are broadcast, and all X-Nodes receive all messages. Among these messages, only the advertisement messages are readable for all X-Nodes in the VANET. All other messages are encrypted using the corresponding X-Node's public key or the generated AES key. An adversary can read these messages only by breaking the applied cryptographic mechanism. The effort and cost (e.g., in computational resources) of breaking the cryptographic mechanism will exceed the actual data value. Therefore, an adversary is unlikely to use data from broadcasted messages without paying for them.

Using hypertext transfer protocol secure (HTTPS), the data trading system hinders an adversary in reading the data of messages sent over long-range communication. Nonetheless, while an adversary can conduct traffic analyses (e.g., to infer the type of request to the IOTA node), an adversary cannot read the data. In the proposed data trading system,

the requests from an X-Node to the IOTA node in the rating phase enable the IOTA node to deduct the public key used by the X-Node. If the same IOTA node is used by a single X-Node for all requests (e.g., moving IOTA tokens in the exchange phase), an adversary controlling the IOTA node can connect the public key with payment information.

Forging: *An adversary can create and inject new messages into a data stream and change messages during a transmission.*

All messages, except advertisement messages that are transmitted between X-Nodes via DSRC, are either digitally signed and encrypted using RSA (1024-bit key length, private key generated with PKCS#8, public key generated with X.509) or only encrypted using AES (128-bit key length in operating mode ECB and with PKCS5 padding). If an adversary forges a message without knowing the keys to encrypt or sign the message, the message decryption will fail, or the digital signature of the adverse message will not be valid. Hence, X-Nodes can detect forged messages by verifying the message's digital signature or encryption. Forged messages will be ignored by the X-Node.

For long-range communication, an adversary cannot forge messages because of the use of HTTPS and the digital signature scheme inherent to the IOTA protocol, except via the IOTA node if it is compromised. If the IOTA node itself is compromised, an adversary can decide to not implement the X-Nodes' requests and return forged messages. In the purchase decision phase, forged replies by an IOTA node can be exposed by the X-Nodes (e.g., through compromised signatures). In other phases (e.g., the exchange phase), forged replies will only be exposed by the X-Nodes if the X-Nodes compare the replies of additional IOTA nodes with the forged replies. A simple approach is a quorum, in which multiple IOTA nodes are queried, and the replies given by most IOTA nodes are used by the X-Nodes for the next steps. An adversary will face high costs in operating a sufficient number of IOTA nodes that forge replies and gain a majority in a quorum. The costs of operating that many IOTA nodes will exceed the gains generated by the data trade. Consequently, it is unlikely that an adversary will forge messages by controlling a sufficient number of IOTA nodes.

Replaying: *An adversary can resend valid messages (e.g., advertisement messages or payment messages) that have been sent earlier.*

An adversary can record a data trading session of an X-Node and replay the X-Node's messages with valid signatures. To make replayed messages detectable for X-Nodes, our protocol uses sequence numbers. Additionally, the messages that are asymmetrically encrypted contain a timestamp combined with a random text. Thus, X-Nodes can identify replayed messages and ignore them.

In long-range communication, replayed messages to and from an IOTA node do not affect the data trade between X-Nodes. Replaying an X-Node's request to IOTA nodes will cause repeated responses of publicly visible data. In the exchange phase, replayed transactions will be invalid. In our system design, all transaction bundles either completely drain the funds of an input address or partially drain the input address and send the tokens remaining on the multi-signature address back to the input address (e.g., in cases where preliminary bundles are generated and collateral should remain on the multi-signature address). Therefore, replayed IOTA transactions will be invalid because the necessary number of tokens is no longer available on the input address. An adversary could top up the input address with its own tokens but would thereby only waste those tokens. Replaying ratings causes redundant verifiable claims to be assigned to an X-Node's reputation address. Redundant verifiable claims have identical transaction hash values and can be detected by the X-Nodes. Every X-Node that calculates the reputation of an X-Node can ignore redundant verifiable claims. Thus, replay attacks are either detected and ignored by X-Nodes or considered invalid by the IOTA protocol, which is why our system is not vulnerable to replay attacks.

Delaying and rushing: *An adversary can delay or accelerate the delivery of messages.*

Because of the direct communication between X-Nodes in VANETs, the data provider and data consumer can only delay or rush their own messages. Delaying messages

reduces the available communication time for subsequent message transmissions and, thus, decreases the number of tradable data sets and the number of tokens earned by the data provider. Moreover, delaying messages increases the risk of not receiving the full data set within the limited communication time for the data consumer. Consequently, X-Nodes have no incentive to delay or rush messages in VANETs.

Delaying requests of X-Nodes to the IOTA network in the purchase decision phase shortens the available time for the communication in the VANET and, thus, hinders the successful data trade between X-Nodes. Rushing requests to the IOTA Tangle increases the available communication time for data trading in the VANET because it accelerates the data exchange with the IOTA network in the purchase decision phase. Other requests to the IOTA network (e.g., to send bundles) are not time critical, and delaying these message does not affect the security of the data trading system.

Reordering: *An adversary can change the delivery order of messages.*

An adversary cannot change the delivery order of messages in VANETs because X-Nodes directly communicate with each other.

For long-range communication, an adversary can aim to change the order of entire requests to the IOTA network or reorder data packages related to a single request to the IOTA node. In the first case, X-Nodes repeatedly send requests to the IOTA node if the request has not been successfully answered. In the second case, HTTPS, transport layer security (TLS), and transmission control protocol (TCP) mitigate the effect of reordered packages in long-range communication. TCP handles data packages that arrive at their destination out of order [66]. Consequently, an adversary cannot disrupt the long-distance connection between X-Nodes and the IOTA nodes.

Deleting: *An adversary can drop messages in a data stream.*

An adversary dropping messages in VANETs has no effect on the data trading system because the data consumer and data provider communicate directly.

For long-range communication between X-Nodes and the IOTA node, an adversary can aim to drop messages in the communication between the X-Nodes and the IOTA network (e.g., by compromising the local routing or the internet service provider) or block requests from X-Nodes by compromised IOTA nodes. In both cases, X-Nodes repeat their request to the IOTA network when not receiving a response within a defined time span. Thereby, the available communication time for data trading decreases, which reduces the number of traded data sets between X-Nodes.

3.3.2. Concept Security

In this section, we discuss the security of the open data trading system focusing on the application concept. We assume that an adversary cannot influence the used networks (see Section 3.3.1) but can only use the regular functionality offered by the data trading system (e.g., identity creation and rating) and view publicly accessible data stored on the IOTA Tangle. We do not refer to cyber-physical attacks (e.g., construction of physical barriers or radio jamming to hinder messages in VANETs).

For the concept security analysis, we assume that X-Nodes behave honestly regarding the creation and issuance of verifiable claims for ratings. For example, an X-Node does not give its data trading partner a negative rating if the data trading was satisfactory.

Aborting: *An adversary stops transmitting data or making payments even before the data trade is completed.*

In the exchange phase, adverse data providers or consumers can abort the transmission of data or payments. In case not all data were traded, tokens of the data consumer and provider remain on the shared multi-signature address (see Section 2.3). Using payment channels, all exchanged data fragments are directly payed. Because of the risk of losing tokens locked on the shared multi-signature address, data providers and consumers are unlikely to abort data trades voluntarily.

Bad or good mouthing: *An adversary repeatedly rates another X-Node to lower or increase its reputation.*

To give an X-Node negative (bad mouth) or positive ratings (good mouth), an adversary must know the targeted X-Node's public key. The adversary can only extract public keys of X-Nodes from verifiable claims or advertisement messages. Verifiable claims are publicly accessible on the IOTA Tangle and the public keys of the issuers of verifiable claims can be deducted. Nonetheless, public keys can be hardly associated with a specific X-Node because of the large number of keys. In the reputation assessment, X-Nodes only consider verifiable claims issued by known X-Nodes. Thus, an adversary must first establish a relationship (e.g., successful data trade) with numerous other X-Nodes so that these X-Nodes consider the fraudulent verifiable claim. Moreover, only the last sent verifiable claim of each known X-Node is considered for the calculation of an X-Node's reputation. Therefore, an adversary cannot disproportionally influence an X-Node's rating when issuing multiple verifiable claims from the same IOTA account.

Behavior inferring: *An adversary can survey publicly available data to infer X-Node controller behavior.*

To infer X-Node controller behaviors in the data trading system, an adversary can use two types of publicly accessible data stored on the IOTA Tangle: payment-related data and reputation-related data. Payment-related data (i.e., the IOTA transactions that transfer tokens) disclose information regarding the time and date when an IOTA transaction was issued. By analyzing IOTA transactions associated with the shared multi-signature address, an adversary can draw conclusions on data trades between X-Nodes. An adversary cannot link payment information with X-Node identities or ratings because public keys of X-Nodes are not revealed by payments.

By analyzing verifiable claims, an adversary can retrieve the public keys of X-Nodes. Each IOTA transaction that includes a verifiable claim contains the public key of the X-Node that issued the verifiable claim, the rating score, and a digital signature. An adversary cannot extract the public key of the X-Node from its reputation address because reputation addresses are generated by hashing public keys and reputation claims. Therefore, adversaries cannot infer mutual ratings of X-Nodes and corresponding past data trades between X-Nodes.

Fake claim issuing: *An adversary initiates the issuance of verifiable claims from multiple identities to manipulate an X-Node's reputation.*

In the presented data trading system, only ratings from known X-Nodes are considered to determine X-Node reputations and identities (see Section 3.1.2). Newly created identities start with the lowest reliability in the IOTA network because they are unknown to other X-Node controllers. Thus, an adversary cannot succeed in manipulating an X-Node's reputation using verifiable claims from newly created identities because those claims will not be considered by other X-Node controllers.

Reselling: *An attacker resells data after buying it.*

The presented data trading system does not protect data from being resold.

4. Viability Assessment of the Open Data Trading System

For the viability assessment, we focused on the available communication time and cost caused by the energy consumption and communication cost (e.g., for communication over 3G). For the assessment, we used the prototypical implementation of the data trading system in a real-world scenario to measure the communication time required for data trading and to estimate the incurred cost (e.g., for using the cellular wireless network and for electric power consumption). In the scenario (see Figure 2), there were two X-Nodes: an RSU as the data consumer and a car as the data provider. We installed the RSU near a road at a fixed position. The car was travelling at a constant speed of 30 $\mathrm{km\,h^{-1}}$.

Both X-Nodes broadcasted advertisement messages at an interval of 0.1 s in their VANETs. In the purchase decision phase, both X-Nodes downloaded 10 identity-related verifiable claims from the identity address and 37 reputation-related verifiable claims from the reputation address of their data trading partner. The X-Nodes traded three data sets, each 300 B in size. In the exchange phase, the vehicle computed all PoW operations required

for IOTA transactions. In the rating phase, both X-Nodes performed PoW operations to issue transactions to the IOTA Tangle.

(**a**) (**b**) (**c**)

Figure 2. The scenario setup for the viability assessment including the car (**a**), the road driven with the car during the viability assessment (**b**), and the RSU mounted along the road (**c**).

We performed 42 repetitions of full data trading sessions and achieved confidence interval widths of approximately 1 s for both X-Nodes (confidence intervals at the 95% confidence level: 13.72 s to 14.78 s for the car and 14.24 s to 15.28 s for the RSU) regarding the available DSRC time. A slight increase in the sample size of 42 measurements would not have had a significant effect on the confidence interval widths of the communication time.

4.1. Communication Time

We started measuring the communication time when one X-Node received the advertisement message from another X-Node. We stopped the measurement after both X-Nodes submitted their ratings to the IOTA network. During the viability assessment, we logged the communication times for all data trading phases (i.e., the purchase decision phase, exchange phase and its sub-phases) and the rating phase; see Figure 3).

In the *purchase decision phase*, the measurements of the communication times started after both X-Nodes received the advertisement message and ended after both X-Nodes authenticated their respective data trading partner's identity and locally calculated its reputation. The required median time to download and authenticate verifiable claims associated with the identity and reputation addresses was 1.6 s for the car and 2.8 s for the RSU (see Figure 3). The median time differences are related to different message success rates that are caused by the degradation of the DSRC distance between X-Nodes (see Table 1). Our measurements show that message transmission losses in DSRC increase with the distance between X-Nodes (see Table 1). We determined the maximum DSRC distance of 140 m by measuring at what distance the moving car could repeatedly communicate with the RSU. The degradation of DSRC at long distances is not equal for both X-Nodes. The RSU successfully received more messages than the car (see Table 1). Different message success rates can relate to signal attenuation. For instance, different alignments of the used antennas for the DSRC between X-Nodes can lead to different radiation patterns and varying message success rates [67]. In addition, the presence of other signal obstructing vehicles that come in between X-Nodes affect the measured message success rate [68,69].

We individually measured all three sub-phases (i.e., open payment channel, data trade, and close payment channel) in the exchange phase. We started the measurements for the *open payment channel* sub-phase directly after the *purchase decision phase* and stopped them after the car submitted its bundle to the IOTA network. We calculated a median time for the *open payment channel* sub-phase of 6.9 s for the car and 6.2 s for the RSU (see Figure 3). The mean times differ primarily because only the car used an FPGA board to accelerate the PoW operations. The RSU did not perform PoW operations in this phase. The median time in the *open payment channel* sub-phase (see Figure 3) is the highest of all (sub-)phases. The *open payment channel* sub-phase is time-consuming, primarily because of the PoW

operations and a high number of CAMs exchanged to outsource PoW operations from the RSU to the vehicle.

Table 1. Average success rate of DSRC messages exchanged between X-Nodes for different data trading phases. No DSRC messages are exchanged between X-Nodes during the rating phase.

Direction	Advertisement	Purchase Decision	Exchange			Rating
			Open Payment Channel	Data Trade	Close Payment Channel	
Sent by car to RSU	10.0%	76.4%	93.9%	95.7%	97.3%	-
Sent by RSU to car	2.1%	37.5%	52.8%	80.1%	89.7%	-

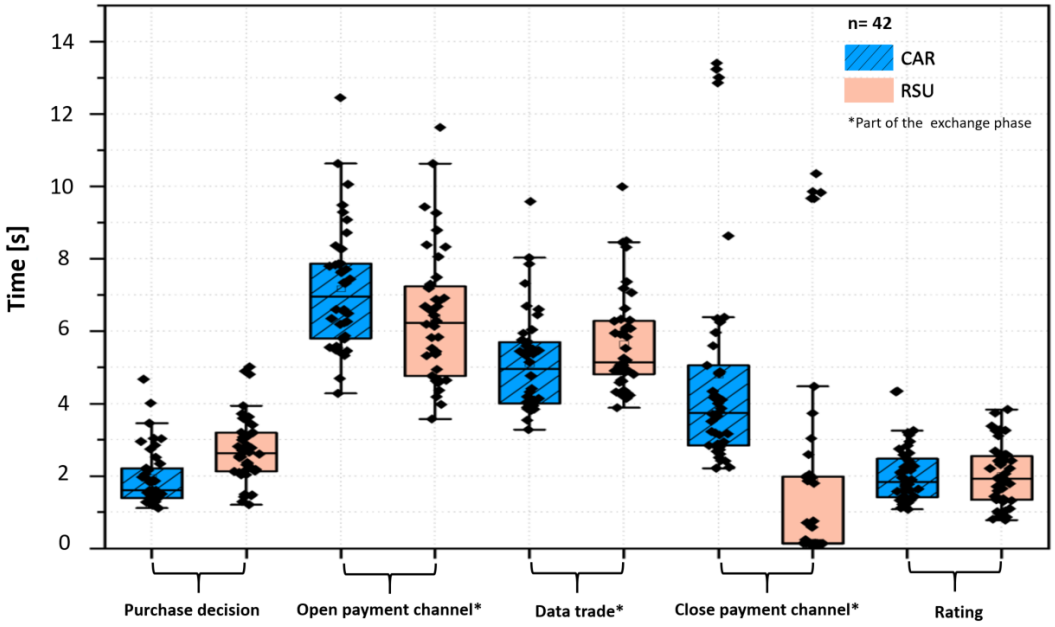

Figure 3. Communication times for all data trading phases, measured in 42 data trading sessions between a moving and stationary X-Node.

For the *data trade* sub-phase, we started the measurements after the *open payment channel* sub-phase and ended after all data sets were traded. The median time to trade three data sets between the X-Nodes was 4.9 s for the car to 5.1 s for the RSU. The time for the *data trade* sub-phase strongly depends on the number of payment messages that are exchanged to transfer and pay data. Because of the small payload size of CAM, which limits the transmittable amount of data per message (see Section 3.2), nine CAMs had to be exchanged between X-Nodes to trade a single data set. If a single CAM is not successfully delivered (e.g., because of signal interference), the corresponding payment message is incomplete. To resend missing CAMs, additional communication time is needed.

For the *close payment channel* sub-phase, we started the measurements after the final bundle was exchanged between the X-Nodes and ended after the submission of the bundle to the IOTA network. Completing this sub-phase required a median time of 3.7 s for the car and 0.1 s for the RSU. This time difference exists because only the car closes the payment channel.

We started the measurements for the *rating phase* after the *close payment channel* sub-phase was completed. We measured a median communication time to perform PoW operations and to submit ratings to the IOTA Tangle of 1.8 s for the car and 1.9 s for the RSU. For the rating, both X-Nodes execute IOTA transactions using their Raspberry Pi,

which is why the measured median times between X-Nodes do not differ significantly from each other. Accelerated PoW operations are not used during this phase, because data trade ratings can be submitted at any time to the IOTA network independent of time constraints by X-Nodes.

Considering the measured DSRC distance of 140 m (see Figure 2) and the car's speed of 30 km h^{-1}, the available DSRC time in a VANET is approximately 16.5 s. Our viability assessment shows that the data trading sub-phases (i.e., *purchase decision*, *open payment channel*, and *data transfer* phases) require a total median communication time of 14.6 s for both X-Nodes. The subsequent *close payment channel phase* and *rating phase* require a median time of 5.8 s for the car and 2.1 s for the RSU. Because both phases do not rely on DSRC, all data sets were successfully traded in all 42 data trading sessions. Assuming a point-symmetric DSRC distance between both X-Nodes and a total DSRC range of 280 m, X-Nodes have a DSRC time of 28.8 s to exchange messages in a VANET, allowing X-Nodes to trade more than three data sets.

4.2. Data Trading Cost

The data trading costs are related to communication and electric power consumption. The DSRC via the IEEE 802.11p protocol charges no service fees. Communication costs are only caused by long-range communication (see Section 3.1) between X-Nodes and the IOTA Tangle. During the viability assessment, we measured the data traffic (i.e., data up- and download) between X-Nodes and the IOTA Tangle for all data trading phases to determine the total communication cost of a single data trading session.

In the *purchase decision phase* (see Section 3.1.2), both X-Nodes downloaded 47 verifiable claims stored on two IOTA addresses. The costs for downloading data from the IOTA Tangle relate to the number of verifiable claims X-Nodes require to authenticate their data trading partner's identity and reputation. The more verifiable claims that are required, the higher the communication costs will be. In the *open payment channel* and the *close payment channel* sub-phase, the data upload is primarily caused by the submission of bundles to the IOTA network, whereas the data download is caused by querying data (e.g., selected tips) about submitted bundles and the successful token deposition from the IOTA Tangle.

In each data trading session, each X-Node, on average downloaded 37.3 kB of data from and uploaded 62.5 kB of data to the IOTA Tangle (see Table 2). The total cost for using mobile wireless networks for the data transfer is approximately 0.00055€ for each data trading session. The costs are based on the business-to-customer prices for cellular broadband in the European Union in 2019 of 0.00277 € MB^{-1} for a median data volume of 5 GB [70]. The communication costs are independent of the amount of traded data between X-Nodes and pertain to the interactions of the X-Nodes with the IOTA Tangle.

Table 2. Average data traffic between a single X-Node and the IOTA Tangle during a data trading session.

Data Trading Phases	Description of the Main Task in Each Phase	Download [kB]	Upload [kB]
Purchase decision	Request and download of verifiable claims	10.90	5.73
Open payment channel *	Create multi-signature address	11.43	24.43
Data trade *	Ad hoc data exchange	0.00	0.00
Close payment channel *	Resolve multi-signature address	11.42	19.04
Rating	Attesting the trading partner's reputation claim	3.50	13.32
Total data traffic per X-Node		37.3	62.5

* Part of the exchange phase.

In addition to communication cost, we estimate the cost related to the electric power consumption of the used hardware modules (see Table 3). Considering the recent electricity price in Germany of 0.3 € kW^{-1} h^{-1} [71] for both X-Nodes, the median communication time of 20.2 s for each data trading session by the car and the maximum power consumption

of 18.4 W of all hardware modules used by the car, we determined electric power consumption related costs of 0.000031€ for the car. The costs related to the power consumption of cars with a combustion engine might vary from the current electricity price of stationary X-Nodes because energy can be generated by the cars. In our viability assessment, the RSU did not use a PoW accelerator and, thus, consumed less power than the car. The RSU's maximum power consumption was 15.3 W, causing a cost of 0.000023€ for electric power consumption for each data trading session. The median communication time for each data trading session for the RSU was 18.0 s. The time difference with the vehicle is mostly caused by the RSU not performing PoW operations for the final IOTA transaction bundle in the *close payment channel* sub-phase.

Considering costs related to communication and electric power consumption, the car has a data trading cost of 0.000581€. The data trading cost related to low-value data (e.g., vehicular data) trades should be below 2% of the total data price [9]. On the basis of this ratio of data trading cost to data price, the car should offer three data sets for trading at a total price of at least 0.029€ to maintain the 2% cost-revenue ratio with costs of 0.000581€. Thus, our system fulfills the demand from previous studies [72,73] of a low data trading cost to support the trade of low-value data (i.e., a value of a few micro-cents) between X-Nodes.

Table 3. Electric power consumption of different hardware modules used by the car in Watts [W].

Hardware Module	Minimum [W]	Average [W]	Maximum [W]
Computing unit	3.9	4.9	5.2
Short-range communication module	3.5	4.3	4.9
FPGA-based PoW accelerator	3.1	3.1	3.1
Long-range communication module	5.2	5.2	5.2
Sum	15.7	17.5	18.4

5. Comparison with Related Work

Prior studies on data trading in dynamic environments, such as road traffic, highlighted the importance of trust of X-Node controllers in data trading and investigated the feasibility of implementing payments for data trading (e.g., [5,9]). To increase trust in data trading, existing research presents different authentication systems (e.g., [74]) and reputation management systems (e.g., [75]).

Existing research (e.g., [74,76–78]) on decentralized identity management investigated the use of DLT for the mutual authentication of X-Nodes and controlling their identifying information. Previous work (e.g., [74,76]) on the authentication of X-Nodes used permissioned distributed ledgers and smart contracts (i.e., agreements that are formalized in program code and deployed to the distributed ledger). Other studies (e.g., [77,78]) present concepts related to self-sovereign identities, where users can manage data related to their identities on a distributed ledger. Our work differs from prior studies as X-Nodes store identifying information on a public-permissionless distributed ledger. The authentication system implemented in this work is completely open and decentralized. To decrease data trading costs (e.g., gas consumption in Ethereum) and the required communication time (e.g., contract execution time) [9], our authentication system does not use smart contracts, unlike other systems [79,80].

Previous works on reputation management systems suggest two approaches for the assessment of ratings of X-Nodes: first, the inclusion of only nearby vehicles (e.g., [75]); second, the integration of a central authority (e.g., [81]). The first approach (e.g., [75]) limits the number of verifiable claims to be included in the reputation assessment to only those of nearby X-Nodes. The inclusion of only nearby X-Nodes in the reputation assessment can decrease the reliability of reputation assessments. The second approach engages a central authority (e.g., governmental transportation authority) to manage identifying information. A central authority represents a single point of failure (e.g., favoring a fake reputation

by a compromised central authority), makes the reputation management system more prone to censorship, and creates dependencies of X-Nodes on a third party. To overcome the drawbacks of existing approaches, we propose a flexible reputation management system that can increase the reliability of reputation assessments by avoiding a central authority. Moreover, the presented reputation management system is compatible with several reputation models (e.g., direct experiences or witness information models [82]).

Gathering information about X-Node identities or reputations is computationally expensive [83]. In our work, X-Nodes authenticate each other using verifiable claims issued by known X-Nodes. This way, the proposed system minimizes the computational workload for the mutual authentication of X-Nodes. Our work advances existing knowledge by showing the feasibility of the proposed system for X-Node authentication in VANETs.

Simulations of data trading systems using VANETs and DLT (e.g., [23,24]) show that the confirmation latency of blockchains (see Section 2.2) hinders traffic applications from benefitting from data trading systems. For example, the median time (e.g., a few minutes) for a transaction with miner fees to be included in a mined block and added to the permissionless distributed ledger is too high for many VANET application scenarios (e.g., platooning), where data needs to be exchanged within seconds [23]. To overcome the limited transaction throughput of blockchains, several works rely on payment channels instead of directly interacting with the distributed ledger for each transaction (e.g., [72,73]). A comparative study [72] on transaction fees in payment channels shows that transaction fees vary from 0.1€ in Ethereum's Raiden network to 0.32€ in Bitcoin's Lightning network with a respective transaction confirmation latency of 76 s and 1.200 s. Accordingly, the payment channels used in these studies [72,73] are too expensive for trading low-value data. Our work revealed that transaction costs for micropayments using the IOTA Tangle are mainly caused by computational resource consumption (e.g., the energy required for PoW operations) instead of transaction fees. Our work shows that open data trading using a DLT-based payment service is economically feasible and the viability assessment complements existing knowledge by quantifying a lower boundary for the prices of data sold in open trading systems.

Our work advances simulation-based findings on data trading in VANETs by providing empirical insights into the system behavior under real-world conditions. Our viability assessment revealed that open data trading between X-Nodes is feasible and cost affordable. We found that the communication costs are mainly related to the use of payment channels and, thus, are independent of the traded data.

Despite valuable contributions for individual subsystems of an open system for data trading, only a few studies allow for conclusions regarding the combined use of DLT and VANETs for data trading between X-Nodes (e.g., [5,84]). Existing research mainly approached the challenge of limited communication time in VANETs using simulations (e.g., [85]). Simulations build on simplified models for real-world scenarios and may not reflect the actual system behavior [86]. For example, VANET models for simulations simplify complex signal interferences and, thus, do not represent real-world conditions [69].

6. Conclusions

In this work, we present an open data trading system based on VANETs and DLT for dynamic environments, such as road traffic. The data trading system comprises services for the authentication of X-Nodes and data payments, and it supports the suggestion of the reliability of data trades in advance through a reputation management system. We implemented the open data trading system to assess its viability, quantify the constraints caused by the limited communication time in VANETs, and estimate the cost for open data trades. Our results show that open data trading is technically feasible and indicate a lower boundary for data prices.

The exchange of payment messages consumes a large portion of the communication time between X-Nodes in VANETs. Future research should focus on the development of more lightweight payment channels to address the issue of constrained payload size per

message (i.e., CAMs) in VANETs. For example, different data compression techniques should be investigated to find a Pareto optimum between the reduction of data transmission time because of the reduced message payload size and the required processing time to (de-)compress transmitted messages. In addition, future work should focus on how to predict the available data transmission time to determine in advance the number of individual data sets that can be traded between mobile X-Nodes during a single data trading session. We suggest using a link prediction algorithm [5] at the beginning of each trading session to predict the required data transmission time for DSRC considering the X-Node's route information, speed, traffic density, and DSRC signal strength.

Our calculation of the cost of data trading considers costs for consumed electricity and the internet connection. We did not perform a total cost of ownership, so the price of data trading in production operation of open data trading systems may be higher than calculated here. Future research should investigate the total cost of ownership to further specify the cost per data trade. In addition, more research needs to be conducted to investigate what type of data is perceived as sufficiently valuable for purchase at a price that is higher than the cost of data trading and how to optimize price formulation, for instance, using auction-based game theoretical approaches [87].

In the proposed data trading system, each data trade encompasses two phases (i.e., a purchase decision phase and exchange phase) that take a certain fraction of the available direct communication time in the VANET. In the viability assessment, we neglected computational overhead caused by negotiations between X-Nodes regarding the price of a data set prior to its transmission. We only considered the data trading system using a basic reputation model, which can be improved as explained in existing research (e.g., [82]). Nonetheless, the price negotiation and the reputation model affect the available time for the *exchange phase*, in which payment transactions and data are transferred between X-Nodes. To extend the available time for the *exchange phase* to favor data transmission (e.g., to transmit more data sets), the available time for the purchase decision phase could be shortened (e.g., by reducing the number of downloaded verifiable claims). Shortening the time for the purchase decision phase is likely to decrease the reliability of X-Node identities and reputations and vice versa. This trade-off between the degree of reliability of X-Node identity and reputation and the amount of transmittable data between X-Nodes represents a sociotechnical challenge that determines X-Node controllers' (e.g., car drivers) degrees of trust in the identity claimed and data offered by individual X-Nodes. The more reliable an X-Node appears (e.g., based on verifiable claims), the higher an X-Node controller's trust toward that X-Node will be but the less data that can be transmitted in the *exchange phase* and vice versa. This interdependence represents a trade-off between the utility of the data trading system (i.e., the amount of data that can be transferred between X-Nodes) and adoption (i.e., the trust X-Node controllers have toward other X-Nodes). The identification of an equilibrium in this trade-off between X-Node controller trust and the utility of a data trading system should be addressed in future research to unfold the potentials of open data trading.

Author Contributions: Conceptualization, M.L., F.K. and N.K.; Methodology, M.L., F.K. and N.K.; Validation, M.L., F.K. and N.K.; Investigation, M.L., F.K. and N.K.; Resources, M.L.; Writing–original draft preparation, M.L. and N.K.; Visualization, M.L.; Writing–review and editing, M.B., A.S., and W.S.; Supervision, M.B., A.S., and W.S.; All authors have read and agreed to the published version of the manuscript.

Funding: Open access funding provided by the Institute for Information Processing Technologies.

Acknowledgments: We thank M. Beyene and B. Sturm for their kind reviews, which helped us to improve this work. This work was performed in the scope of the project COOLedger (Helmholtz Association of German Research Centers: HRSF-0081, Russian Science Foundation: Project No. 19-41-06301). This work was supported by the Competence Center for Applied Security Technology (KASTEL).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Fong, B.; Situ, L.; Fong, A. Smart Technologies and Vehicle-to-X (V2X) Infrastructures for Smart Mobility Cities: Foundations, Principles, and Applications. In *Smart Cities: Foundations, Principles, and Applications*; John Wiley & Sons: Hoboken, NJ, USA, 2017; pp. 181–208. [CrossRef]
2. Bhavani, M.M.; Valarmathi, A. Smart city routing using GIS & VANET system. *J. Ambient. Intell. Humaniz. Comput.* **2020**. [CrossRef]
3. Zahmatkesh, H.; Saber, M.; Malekpour, M. A New Method for Urban Travel Rout Planning Based on Air Pollution Sensor Data. *Curr. World Environ.* **2015**, *10*, 699–704. [CrossRef]
4. Celikkaya, N.; Papapanagiotou, E.; Busch, F. *TUM Living Lab Connected Mobility State of the Art Report Eco-Sensitive Traffic Eco-Sensitive Traffic Management*; Technical University of Munich: Munich, Germany, 2016.
5. Ramachandran, G.S.; Ji, X.; Navaney, P.; Zheng, L.; Martinez, M.; Krishnamachari, B. MOTIVE: Micropayments for trusted vehicular services. *arXiv* **2019**, arXiv:1904.01630.
6. Park, Y.; Sur, C.; Kim, H.; Rhee, K.H. A Reliable Incentive Scheme Using Bitcoin on Cooperative Vehicular Ad Hoc Networks. *IT Converg. Pract. (INPRA)* **2017**, *5*, 34–41.
7. Zhang, X.; Bai, X.; Liu, Q. A Research of Vehicle Ad Hoc Network Incentive Mechanism. In Proceedings of the IEEE 8th International Conference on Electronics Information and Emergency Communication, Beijing, China, 15–17 June 2018; pp. 175–179. [CrossRef]
8. Ensor, A.; Schefer-Wenzl, S.; Miladinovic, I. Blockchains for IoT Payments: A Survey. In Proceedings of the IEEE Globecom Workshops, Abu Dhabi, United Arab Emirates, 9–13 December 2018; pp. 1–6. [CrossRef]
9. Missier, P.; Bajoudah, S.; Capossele, A.; Gaglione, A.; Nati, M. Mind My Value: A decentralized infrastructure for fair and trusted IoT data trading. *ACM Int. Conf. Proc. Ser.* **2017**. [CrossRef]
10. Visa Inc. Visa U.S.A. Interchange Reimbursement Fees. Available online: https://usa.visa.com/dam/VCOM/download/merchants/visa-usa-interchange-reimbursement-fees.pdf (accessed on 9 January 2021).
11. Rezaeibagha, F.; Mu, Y. Efficient micropayment of cryptocurrency from blockchains. *Comput. J.* **2019**, *62*, 507–517. [CrossRef]
12. Ali, S.T.; Clarke, D.; McCorry, P. The nuts and bolts of micropayments: A survey. *arXiv* **2017**, arXiv:1710.02964v1.
13. Manvi, S.S.; Tangade, S. A survey on authentication schemes in VANETs for secured communication. *Veh. Commun.* **2017**, *9*, 19–30. [CrossRef]
14. Li, Q.; Malip, A.; Martin, K.M.; Ng, S.; Zhang, J. A Reputation-Based Announcement Scheme for VANETs. *IEEE Trans. Veh. Technol.* **2012**, *61*, 4095–4108. [CrossRef]
15. Demmel, S.; Lambert, A.; Gruyer, D.; Rakotonirainy, A.; Monacelli, E. Empirical IEEE 802.11p performance evaluation on test tracks. In Proceedings of the 2012 IEEE Intelligent Vehicles Symposium, Madrid, Spain, 3–7 June 2012; pp. 837–842. [CrossRef]
16. Shrestha, R.; Bajracharya, R.; Shrestha, A.P.; Nam, S.Y. A new type of blockchain for secure message exchange in VANET. *Digit. Commun. Netw.* **2019**, *6*, 177–186. [CrossRef]
17. Kannengießer, N.; Lins, S.; Dehling, T.; Sunyaev, A. Trade-offs between Distributed Ledger Technology Characteristics. *ACM Comput. Surv.* **2020**, *53*. [CrossRef]
18. Deng, X.; Gao, T. Electronic Payment Schemes Based on Blockchain in VANETs. *IEEE Access* **2020**, *8*, 38296–38303. [CrossRef]
19. Park, Y.; Sur, C.; Rhee, K.H. A Secure Incentive Scheme for Vehicular Delay Tolerant Networks Using Cryptocurrency. *Secur. Commun. Netw.* **2018**, *2018*, 5932183. [CrossRef]
20. Lwin, M.T.; Yim, J.; Ko, Y.B. Blockchain-based lightweight trust management in mobile ad hoc networks. *Sensors* **2020**, *20*, 698. [CrossRef]
21. Lu, Z.; Wang, Q.; Qu, G.; Liu, Z. BARS: A Blockchain-Based Anonymous Reputation System for Trust Management in VANETs. In Proceedings of the 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications and 12th IEEE International Conference on Big Data Science and Engineering, New York, NY, USA, 1–3 August 2018; pp. 98–103. [CrossRef]
22. IOTA Foundation. Data Marketplace. Available online: https://docs.iota.org/docs/blueprints/0.1/data-marketplace/overview (accessed on 9 January 2021).
23. Wagner, M.; McMillin, B. Cyber-physical transactions: A method for securing VANETs with Blockchains. In Proceedings of the IEEE 24th Pacific Rim International Symposium on Dependable Computing 2019, Kyoto, Japan, 1–3 December 2019; pp. 64–73. [CrossRef]
24. Kim, S. Impacts of Mobility on Performance of Blockchain in VANET. *IEEE Access* **2019**, *7*, 68646–68655. [CrossRef]
25. Mohammad, S.A.; Rasheed, A.; Qayyum, A. VANET Architectures and Protocol Stacks: A Survey. In *Communication Technologies for Vehicles*; Strang, T., Festag, A., Vinel, A., Mehmood, R., Rico Garcia, C., Röckl, M., Eds.; Springer: Berlin/Heidelberg, Germany, 2011; pp. 95–105.
26. Eze, E.C.; Zhang, S.J.; Liu, E.J.; Eze, J.C. Advances in vehicular ad hoc networks (VANETs): Challenges and road-map for future development. *Int. J. Autom. Comput.* **2016**, *13*, 1–18. [CrossRef]
27. Jiang, R.; Zhu, Y. Wireless Access in Vehicular Environment. In *Encyclopedia of Wireless Networks*; Shen, X.S., Lin, X., Zhang, K., Eds.; Springer International Publishing: Cham, Switzerland, 2019; pp. 1–5. [CrossRef]

28. Federal Communications Commission. Dedicated Short Range Communications (DSRC) Service. Available online: https://www.fcc.gov/wireless/bureau-divisions/mobility-division/dedicated-short-range-communications-dsrc-service (accessed on 9 January 2021).
29. Hameed Mir, Z.; Filali, F. LTE and IEEE 802.11p for vehicular networking: A performance evaluation. *Eurasip J. Wirel. Commun. Netw.* **2014**, *2014*, 1–15. [CrossRef]
30. Abuelsamid, S. Volkswagen Adds 'Vehicle-To-Everything' Communications to Revamped Golf with NXP Chips. Available online: https://www.forbes.com/sites/samabuelsamid/2019/10/28/volkswagen-includes-nxp-v2x-communications-in-8th-gen-golf/#5a213ae016bc (accessed on 23 December 2020).
31. Popov, S. IOTA whitepaper v1.4.3. *New Yorker* **2018**, *81*, 1–28.
32. Silvano, W.F.; Marcelino, R. Iota Tangle: A cryptocurrency to communicate Internet-of-Things data. *Future Gener. Comput. Syst.* **2020**, *112*, 307–319. [CrossRef]
33. IOTA Foundation. Proof of Work. Available online: https://docs.iota.org/docs/getting-started/0.1/transactions/proof-of-work (accessed on 11 November 2020).
34. Lücking, M.; Kannengießer, N.; Kilgus, M.; Riedel, T.; Beigl, M.; Sunyaev, A.; Stork, W. The Merits of a Decentralized Pollution-Monitoring System Based on Distributed Ledger Technology. *IEEE Access* **2020**, *8*, 189365–189381. [CrossRef]
35. World Wide Web Consortium (W3C). Decentralized Identifiers (DIDs) v1.0. Available online: https://w3c.github.io/did-core/#design-goals (accessed on 11 December 2020).
36. World Wide Web Consortium (W3C). Decentralized Identifiers (DIDs) v1.0—Core Architecture, Data Model, and Representations. Available online: https://w3c.github.io/did-core/ (accessed on 11 November 2020)
37. Mühle, A.; Grüner, A.; Gayvoronskaya, T.; Meinel, C. A survey on essential components of a self-sovereign identity. *Comput. Sci. Rev.* **2018**, *30*, 80–86. [CrossRef]
38. World Wide Web Consortium (W3C). Verifiable Claims Data Model and Representations. Available online: https://www.w3.org/TR/2017/WD-verifiable-claims-data-model-20170803/ (accessed on 11 December 2020).
39. Lee, Y.J.; Lee, K.M.; Lee, S.H. Blockchain-based reputation management for custom manufacturing service in the peer-to-peer networking environment. *Peer- Netw. Appl.* **2020**, *13*, 671–683. [CrossRef]
40. Kim, C.H.; Bae, I.H. A Misbehavior-Based Reputation Management System for VANETs. In *Embedded and Multimedia Computing Technology and Service*; Park, J.J.J.H., Jeong, Y.S., Park, S.O., Chen, H.C., Eds.; Springer: Dordrecht, The Netherlands, 2012; pp. 441–450.
41. Huynh, T.D.; Jennings, N.R.; Shadbolt, N.R. Certified reputation: How an agent can trust a stranger. *Proc. Int. Conf. Auton. Agents* **2006**, *2006*, 1217–1224. [CrossRef]
42. Dziembowski, S.; Eckey, L.; Faust, S.; Malinowski, D. Perun: Virtual payment hubs over cryptocurrencies. In Proceedings of the IEEE Symposium on Security and Privacy, San Francisco, CA, USA, 19–23 May 2019; pp. 106–123. [CrossRef]
43. McCorry, P.; Möser, M.; Shahandasti, S.F.; Hao, F. Towards Bitcoin Payment Networks. In Proceedings of the Australasian Conference on Information Security and Privacy, Melbourne, Australia, 4–6 July 2016; pp. 57–76. [CrossRef]
44. Asgaonkar, A.; Krishnamachari, B. Solving the Buyer and Seller's Dilemma: A Dual-Deposit Escrow Smart Contract for Provably Cheat-Proof Delivery and Payment for a Digital Good without a Trusted Mediator. In Proceedings of the IEEE 1st International Conference on Blockchain and Cryptocurrency, Seoul, Korea, 14–17 May 2019; pp. 262–267. [CrossRef]
45. Lamberti, R.; Fries, C.; Lücking, M.; Manke, R.; Kannengießer, N.; Sturm, B.; Komarov, M.M.; Stork, W.; Sunyaev, A. An Open Multimodal Mobility Platform Based on Distributed Ledger Technology. In *Internet of Things, Smart Spaces, and Next Generation Networks and Systems*; Springer International Publishing: Cham, Switzerland, 2019; pp. 41–52.
46. ABmushi. IOTA: Multisig Explained. Available online: https://medium.com/@abmushi/iota-multisig-explained-bca334d250a2 (accessed on 11 January 2021).
47. OBD-II PIDs. Available online: https://en.wikipedia.org/wiki/OBD-II_PIDs#Service_01 (accessed on 11 January 2021).
48. Jung, K.K.; Choi, W.S. Estimation of Vehicle's CO2 Emission using OBD-II Interface. *J. Korea Soc. Comput. Inf.* **2011**, *16*, 167–174. [CrossRef]
49. Khaled, Y.; Tsukada, M.; Santa, J.; Ernst, T. The role of communication technologies in vehicular applications. In *Advances in Vehicular Ad-Hoc Networks: Developments and Challenges*; IGI Globa: Pennsylvania, PA, USA, 2010; pp. 37–58. [CrossRef]
50. Theodorakopoulos, G.; Baras, J.S. On trust models and trust evaluation metrics for ad hoc networks. *IEEE J. Sel. Areas Commun.* **2006**, *24*, 318–328. [CrossRef]
51. Padmavathi, B.; Kumari, S.R. A Survey on Performance Analysis of DES, AES and RSA Algorithm along with LSB Substitution Technique. *Int. J. Sci. Res. (IJSR)* **2013**, *2*, 170–174.
52. Klingler, F. OpenC2X-Standalone. Available online: https://github.com/florianklingler/OpenC2X-standalone/blob/master/config/openc2x_dcc (accessed on 11 January 2021).
53. TP-Link. TP Link WDR 3600 Datasheet. Available online: https://www.tp-link.com/us/support/download/tl-wdr3600/ (accessed on 20 January 2021).
54. Klingler, F.; Pannu, G.S.; Sommer, C.; Bloessl, B.; Dressler, F. Poster: Field testing vehicular networks using OpenC2X. In Proceedings of the 15th Annual International Conference on Mobile Systems, Applications, and Services, Niagara Falls, NY, USA, 19–23 June 2017; p. 178. [CrossRef]

55. Matsumoto, A.; Yoshimura, K.; Aust, S.; Ito, T.; Kondo, Y. Performance evaluation of IEEE 802.11n devices for vehicular networks. In Proceedings of the IEEE 34th Conference on Local Computer Networks, Zurich, Switzerland, 20–23 October 2009; pp. 669–670. [CrossRef]
56. Festag, A. Standards for vehicular communication—From IEEE 802.11p to 5G. *Elektrotechnik Informationstechnik* **2015**, *132*, 409–416. [CrossRef]
57. ABI Research. V2X System Cost Analysis DSRC+LTE and C-V2X+LTE. Available online: https://unex.com.tw/public/uploads/shortcuts/ABI-DSRC-price-comparison.pdf (accessed on 17 January 2021).
58. Laux, S.; Pannu, G.S.; Schneider, S.; Tiemann, J.; Klingler, F.; Sommer, C.; Dressler, F. Demo: OpenC2X—An open source experimental and prototyping platform supporting ETSI ITS-G5. *IEEE Veh. Netw. Conf. VNC* **2016**, 16–17. [CrossRef]
59. Santa, J.; Pereñíguez, F.; Moragón, A.; Skarmeta, A.F. Experimental evaluation of CAM and DENM messaging services in vehicular communications. *Transp. Res. Part C Emerg. Technol.* **2014**, *46*, 98–120. [CrossRef]
60. Radiocommunication Study Groups. *Intelligent Transport Systems (ITS) Usage in ITU Member States*; Technical Report; International Telecommunication Union: Geneva, Switzerland, 2017.
61. Schiener, D. The Anatomy of a Transaction. Available online: https://domschiener.gitbooks.io/iota-guide/content/chapter1/transactions-and-bundles.html (accessed on 6 January 2021).
62. Pototschnig, T. PiDiver 1.3 Documentation. Available online: https://gitlab.com/microengineer18/pidiver1.3/-/wikis/home (accessed on 11 November 2020).
63. Xilinx. Zynq-7000 SoC. Available online: https://www.xilinx.com/products/silicon-devices/soc/zynq-7000.html (accessed on 5 December 2020).
64. Dolev, D.; Yao, A.C. On the Security of Public Key Protocols. *IEEE Trans. Inf. Theory* **1983**, *29*, 198–208. [CrossRef]
65. Walker, J. Chapter 7—Internet Security. In *Computer and Information Security Handbook*; Vacca, J.R., Ed.; Morgan Kaufmann: Boston, MA, USA, 2009; pp. 93–117. [CrossRef]
66. Bohacek, S.; Hespanha, J.P.; Lee, J.; Lim, C.; Obraczka, K. A new TCP for persistent packet reordering. *IEEE/ACM Trans. Netw.* **2006**, *14*, 369–382. [CrossRef]
67. Condo Neira, E. Antenna Evaluation for VehicularApplications in Multipath Environment. Ph.D. Thesis, Chalmers University of Technology, Gothenburg, Sweden, 2017.
68. Boban, M.; Vinhoza, T.T.V.; Ferreira, M.; Barros, J.; Tonguz, O.K. Impact of Vehicles as Obstacles in Vehicular Ad Hoc Networks. *IEEE J. Sel. Areas Commun.* **2011**, *29*, 15–28. [CrossRef]
69. Schmidt, R.K.; Köllmer, T.; Leinmüller, T.; Böddeker, B.; Schäfer, G. Degradation of Transmission Range in VANETs caused by Interference. *PIK Prax. Der Informationsverarbeitung Und Kommun.* **2010**, *32*. [CrossRef]
70. Mobile Broadband Prices in Europe. p. 87. Available online: https://op.europa.eu/en/publication-detail/-/publication/5a9b64f1-02c8-11eb-8919-01aa75ed71a1/language-en (accessed on 4 January 2021). [CrossRef]
71. Eurostat. Electricity Prices (Including Taxes) for Household Consumers, First Half 2020. Available online: https://ec.europa.eu/eurostat/statistics-explained/index.php/Electricity_price_statistics (accessed on 4 January 2021).
72. Khan, N.; State, R. Lightning Network: A Comparative Review of Transaction Fees and Data Analysis; In *Blockchain and Applications*; Springer International Publishing: Cham, Switzerland, 2019; pp. 11–18. [CrossRef]
73. Robert, J.; Kubler, S.; Ghatpande, S. Enhanced Lightning Network (off-chain)-based micropayment in IoT ecosystems. *Future Gener. Comput. Syst.* **2020**, *112*, 283–296. [CrossRef]
74. Tan, H.; Chung, I. Secure Authentication and Key Management with Blockchain in VANETs. *IEEE Access* **2020**, *8*, 2482–2498. [CrossRef]
75. Chen, L.; Lit, Q.; Martin, K.M.; Ng, S.L. A privacy-aware reputation-based announcement scheme for VANETs. In Proceedings of the IEEE 5th International Symposium on Wireless Vehicular Communications, WiVeC 2013, Dresden, Germany, 2–3 June 2013; Volume 61, pp. 4095–4108. [CrossRef]
76. Lu, Z.; Wang, Q.; Qu, G.; Zhang, H.; Liu, Z. A Blockchain-Based Privacy-Preserving Authentication Scheme for VANETs. *IEEE Trans. Very Large Scale Integr. Syst.* **2019**, *27*, 2792–2801. [CrossRef]
77. Xu, J.; Xue, K.; Tian, H.; Hong, J.; Wei, D.S.; Hong, P. An Identity Management and Authentication Scheme Based on Redactable Blockchain for Mobile Networks. *IEEE Trans. Veh. Technol.* **2020**, *69*, 6688–6698. [CrossRef]
78. Lux, Z.A.; Thatmann, D.; Zickau, S.; Beierle, F. Distributed-Ledger-based Authentication with Decentralized Identifiers and Verifiable Credentials. In Proceedings of the 2nd Conference on Blockchain Research and Applications for Innovative Networks and Services, BRAINS, Paris, France, 28–30 September 2020; pp. 71–78. [CrossRef]
79. Kchaou, A.; Ayed, S.; Abassi, R.; Fatmi, S.G.E. Smart Contract-Based Access Control for the Vehicular Networks. In Proceedings of the 2020 International Conference on Software, Telecommunications and Computer Networks (SoftCOM), Hvar, Croatia, 17–19 September 2020; pp. 1–6. [CrossRef]
80. Ma, Z.; Zhang, J.; Guo, Y.; Liu, Y.; Liu, X.; He, W. An Efficient Decentralized Key Management Mechanism for VANET With Blockchain. *IEEE Trans. Veh. Technol.* **2020**, *69*, 5836–5849. [CrossRef]
81. Mühlbauer, R.; Kleinschmidt, J.H. Bring your own reputation: A feasible trust system for vehicular ad hoc networks. *J. Sens. Actuator Netw.* **2018**, *7*. [CrossRef]
82. Sabater, J.; Sierra, C. Review on computational trust and reputation models. *Artif. Intell. Rev.* **2005**, *24*, 33–60. [CrossRef]

83. Huang, Z.; Ruj, S.; Cavenaghi, M.A.; Stojmenovic, M.; Nayak, A. A social network approach to trust management in VANETs. Peer Netw. Appl. **2014**, *7*, 229–242. [CrossRef]
84. Sadiq, A.; Javaid, N.; Samuel, O.; Khalid, A.; Haider, N.; Imran, M. Efficient Data Trading and Storage in Internet of Vehicles using Consortium Blockchain. In Proceedings of the 2020 International Wireless Communications and Mobile Computing, Limassol, Cyprus, 15–19 June 2020; pp. 2143–2148. [CrossRef]
85. Breu, J.; Brakemeier, A.; Menth, M. Analysis of cooperative awareness message rates in VANETs. In Proceedings of the 13th International Conference on ITS Telecommunications, Tampere, Finland, 5–7 November 2013; pp. 8–13. [CrossRef]
86. Ahmed, H.; Pierre, S.; Quintero, A. A flexible testbed architecture for VANET. *Veh. Commun.* **2017**, *9*, 115–126. [CrossRef]
87. Hassija, V.; Chamola, V.; Gupta, V.; Chalapathi, G.S. A Framework for Secure Vehicular Network using Advanced Blockchain. In Proceedings of the 2020 International Wireless Communications and Mobile Computing, Limassol, Cyprus, 15–19 June 2020; pp. 1260–1265. [CrossRef]