Tezos-based Vehicular Ad Hoc Blockchains

-

Vision Paper - Version 0.6
September 11, 2018

Benjamin Leiding and William V. Vorobev

Chorus Mobility
Email: hello@chorus.mobi

Abstract. The next generation of tightly interconnected vehicles offers a variety of new technologies as well as business opportunities where vehicles form so-called vehicular ad hoc networks (VANETs). Sophisticated systems of interconnected cars in the context of VANETs often assume a full coverage of 5G networks to unfold their full potential. However, nowadays network infrastructure is neither 5G-ready nor does it provide reliable and full coverage of all areas that might be relevant for VANET-based networks. Hence, the conventional mode of operations of all nodes being connected to one blockchain at all times is not feasible. In addition, traditional blockchains require every node to process each transaction and smart contract command which is highly inefficient. Therefore, we present a solution based on so-called mobile ad hoc blockchains that enable groups of nodes involved in any kind of collaboration to effectively form temporary networks and coordinate themselves.
Another critical requirement of VANETs and interconnected vehicles is security. The safety of network participants does not only depend on the vehicle's hardware, but also on the correctness of the software that controls the interaction and transaction within the network. Formal verification is a common way to address the issue proving the correctness of software. The self-amending blockchain Tezos supports Turing-complete smart contracts and also offers built-in formal verification of their programming languages, thereby fostering the security of our solution.
This whitepaper fills the gap by introducing Tezos-based vehicular ad hoc blockchains based on mobile ad hoc blockchains that allow groups of nodes to be temporarily disconnected from the overall network but still being able to enact and transact on a local network level for the duration of their interaction. We present the advantages of the system, outline the requirements and goals, as well as the architecture of the system.

Keywords: VANET, Formal Verification, Tezos, Mobile Ad Hoc Blockchains, Blockchain, Smart Contracts, Interoperability, Vehicle Networks, V2X

1 Introduction

Despite steadily growing public transport networks and systems, especially in most first world countries, cars are still the default standard for urban trans-

portation. In the U.S., "about 86 percent of all workers commuted to work by private vehicle, either driving alone or carpooling" [36], even though in recent years the numbers remained relatively stable after decades of consistent increase. Similar applies to other industrial countries [37][19] though the overall percentage of vehicle commuters in Europe is lower than in the U.S. [13]. While it was normal for the last few decades to own a vehicle and commute on a day-by-day basis, the future will be radically different due to the progressing evolution of self-driving cars and autonomous vehicles. The car-sharing economy that developed in recent years in combination with autonomous cars results in a so called *passenger economy* [27]. Users no longer own cars, instead they just hop on an autonomous car, pick a destination and get transported without any human interaction. An Intel report estimates the size of this economy to be around US$ seven trillion in 2050 [27].

A key technology for this next generation of tightly interconnected vehicles are so-called vehicular ad-hoc networks (VANETs) [46]. Vehicles form VANETs and thereby enable vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), vehicle-to-human (V2H), or in general vehicle-to-everything (V2X) communication and interaction. In our previous work [32][33], we presented a blockchain-based system that enables a manufacturer agnostic platform solution allowing VANET participants to enact and transact any kind of services and goods. Sophisticated networks of interconnected cars require full coverage of 5G networks to unfold their full potential [3][10][39]. However, nowadays network infrastructure is neither 5G-ready nor does it provide reliable and full coverage of all areas that might be relevant for VANET-based platforms. Hence, the conventional mode of operations of all nodes being connected to one blockchain at all times is not feasible. In addition, traditional blockchains such as Bitcoin [41] and Ethereum [49] also require every node to process each transaction and smart contract commands which are highly inefficient. Therefore, we present a solution based on so-called mobile ad hoc blockchains that enable groups of nodes involved in any kind of collaboration to effectively form temporary networks and coordinate themselves [4]. They only connect to nodes they need to be connected to, depending on the context, for the duration of their interaction.

Another critical requirement of VANETs and interconnected vehicles is security. The safety of network participants does not only depend on the vehicle's hardware, but also on the correctness of the software that controls the interaction and transaction within the network. Formal verification is a common way to address the issue proving the correctness of software with respect to a certain formal specification or property using formal methods of mathematics [48]. The self-amending blockchain platform Tezos [26] does not only support Turing complete smart contracts, it also offers built-in formal verification of their smart contract programming languages, thereby fostering the security of our solution.

This work fills the gap by introducing our Tezos-based vehicular ad hoc blockchain solution, thereby answering the question of how to enable vehicular ad hoc blockchains that allow groups of nodes to be temporarily disconnected from the overall network but still being able to enact and transact on a local network

level for the duration of their interaction? In order to answer this question with a separation of concerns, we pose the following sub-questions: What is the corresponding architecture of the Tezos-based vehicular ad hoc blockchain? What are the detailed network and communication processes? What kind of use cases and application scenarios exist?

The remainder of this paper is structured as follows: Section 2 introduces supplementary literature and related work. Section 3 outlines the system architecture our solution and expands on the network communication processes. Next, Section 4 introduces example use cases and application scenarios. Finally, Section 5 concludes this work and provides an outlook on future work.

2 Technical Background and Supplementary Literature

The following section provides background information, introduces underlying concepts and describes related works regarding previous ideas that focus on blockchain-based VANET platforms. First, Section 2.1 introduces the general concepts of blockchain technology, terms and frameworks. Afterwards, Section 2.2 and Section 2.3 focus on the fundamentals of vehicular ad-hoc networks as well as formal verification. Finally, Section 2.4 introduces related work.

2.1 Blockchain Technology

As the name suggests, a blockchain consists of a chronologically ordered chain of blocks. Every block consists of a certain number of validated transactions and each of those block links to its predecessor by a hash reference. As a result, changing the content of one block also changes all succeeding blocks and hence breaks the chain. All blocks are stored on and verified by all participating nodes. While the initial Bitcoin blockchain only supported a very limited set of scripting instructions, the next generation of blockchain platforms, e.g., Ethereum [49], Qtum [14], or Tezos [26], provide Turing-complete programming languages on the protocol-layer level in order to enable smart contract capabilities. Smart contracts are "orchestration- and choreography protocols that facilitate, verify and enact with computing means a negotiated agreement between consenting parties" [14]. Hence, the entities participating in the enactment of a smart contract establish binding agreements and deploy applications using such smart contracts in order to provide blockchain-based applications. Those application are as versatile as smart contracts itself and enable services including the finance sector [42][45], academic and business authentication and identity solutions [7][12][29][35], reputation systems [8] as well as platforms for Internet-of-Things (IoT) applications [11][43].

The blockchain concept is particularly interesting for the V2X economy for three reasons. First, it removes the need for trusted third parties and instead enables trust-less transaction enactment. Second, transactions that were agreed up on cannot be changed later on since the underlying blockchain is tamperproof. Third, no human interaction is required for any kind of transaction between vehicles or machines in general.

2.2 Vehicular Ad-Hoc Networks - VANETs

Communication between vehicles, road infrastructure and Internet-based services is a key enabler for the upcoming generation of vehicles. So called vehicular ad-hoc networks provide an abstract concept that models the different components that are required for V2V, V2I, or V2X communication. Figure 1 illustrates the main components of VANETs: Vehicles, on-board-units (OBUs), application-units (AUs) and road-side-units (RSUs). RSUs are placed along the road side or in dedicated locations such as at crossroads. Typically, RSUs provide short range communication based on IEEE 802.11p radio technology but can also be equipped with other network devices in order to provide communication within the infrastructural network [1]. OBUs are mounted onto a vehicle and used for data exchange. To do so, short range wireless- or radio communication is used to exchange these information [6]. Closely linked to the OBU is the AU, they might even reside in the same physical unit or as a mobile until that is regularly removed from the vehicle (e.g smartphones). The AU provides an execution environment for applications that utilize the OBU's communication capabilities [1][6].

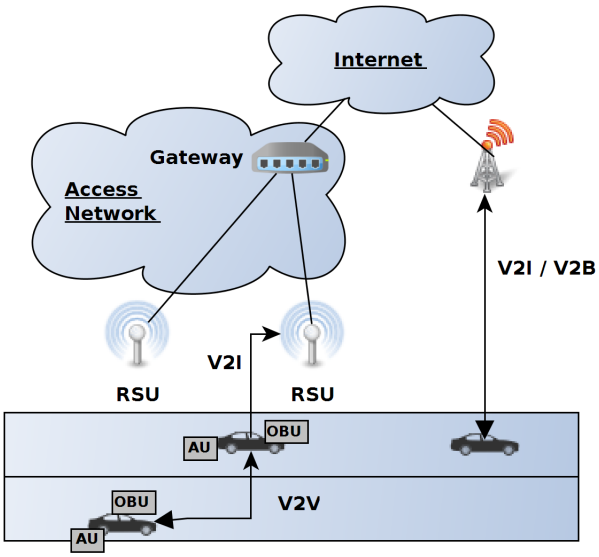

Fig. 1. General VANET architecture (Based on [6] and [30])

Communication in VANETs occurs either inside a vehicle between AUs and OBU, wirelessly between different vehicles (V2V), vehicles and infrastructure (V2I) or vehicles and the infrastructure via broadband (V2B) [17]. For authentication purposes, each network participant is equipped with a unique pub-

lic/private key pair that resides in a tamper-proof-device (TPD). In blockchain terms, the TPD is similar to an external hardware wallet.

2.3 Formal Verification

Another critical requirement of VANETs and interconnected vehicles is security. The safety of network participants does not only depend on the vehicle's hardware, but also on the correctness of the software that controls the interaction and transaction within the network. Formal verification is a common way to address the issue proving the correctness of software according to a specification using formal methods of mathematics. "A formal method is a mathematically-based technique used in computer science to describe properties of hardware and/or software systems. It provides a framework within which large complex systems may be specified, developed, and verified in a systematic rather than ad-hoc manner. A method is formal if it has a sound mathematical basis, typically given by a formal specification language" [48]. The concept of formal verification is not new at all and over many decades, several approaches and concepts for formal methods have been introduced, e.g., Statecharts [21], abstract state machines (ASMs) [20], Petri nets [44], as well as timed automata [2] and communicating sequential processes [22].

The self-amending blockchain platform Tezos[1] [26] does not only support Turing complete smart contracts, it also offers built-in formal verification of their smart contract programming languages. The idea is to leverage the built-in formal verification mechanism to ensure a correct behavior (in terms of programming logic) of the involved smart contracts, thereby enhancing the security of applications within VANETs. Especially due to the progressing digitalization and inter-connection of vehicles, the dependencies of large and complex software to operate those vehicles and networks grows tremendously and hence becomes more vulnerable to unintended security issues caused by badly written code.

2.4 Related Work

In our previous work [32][33], we introduced a blockchain-based value transaction layer protocol for vehicular ad hoc networks that is supposed to fuel vehicle economy. However, that work focused on providing a protocol layer and an abstract platform architecture whereas this work extends our previous efforts and suggests a specific Tezos-based implementation.

MONET[2] [4] introduced the idea mobile ad hoc blockchains in combination with the Babble consensus algorithm. The downside of Babble is that it is based on Hashgraph [5] which is patented in the U.S. and requires a license which limits widespread adoption of their solution. In addition, MONET relies on Ethereum and its smart contracting languages which do not offer built-in formal verification as Tezos does. Moreover, by relying on Ethereum the MONET platform inherits

[1] `https://tezos.com/`
[2] `https://monet.network/`

most of the current Ethereum issues as well. Finally, the authors do mention a public/private key based identity solution that is necessary for their permissioned blockchain. However, how to prevent sybil node attacks and ensure a mapping between identity and its owner is still unclear.

Cosmos[3] [25] proposed a network architecture of independent and parallel blockchains that rely on the Tendermint consensus protocol - a partially synchronous BFT consensus protocol derived from the DLS consensus algorithm [16]. They also introduce the concept of an inter-blockchain communication (IBC) protocol that allows for interaction among the parallel blockchains.

3 System Design and Architecture

As previously mentioned in Section 2.4 the concept of mobile ad hoc blockchains is not new and has been recently applied to mobile ad hoc networks (MANETs) in the form of the MONET project [4]. The following sections outline the process of adapting the general concept of mobile ad hoc blockchains to VANETs. VANETs are a sub-category of MANETs with two main differences between these two types of networks. First, not all entities in VANETs are mobile and only sparsely connected to the Internet, e.g., RSU and infrastructure components. They are stationary and hence it easy to establish permanent Internet access, making them the perfect relay stations. Second, in VANETs the communication nodes are moving on predefined roads in contrast to nodes in MANETs that are not bound to any restrictions. Note that this definition excludes flying vehicles such as drones from VANETs in the context of this work.

Section 3.1 and Section 3.2 present the high-level architecture of the VANET blockchain, followed by Section 3.3 that discusses the topics of identities within our system. Next, Section 3.4 outlines the consensus strategies for vehicular ad hoc blockchains while Section 3.5 discuss inter-blockchain communication.

3.1 System Architecture

The system architecture illustrated in Figure 2 extends the commonly used VANET concept of Figure 1 that we introduced earlier. RSUs, vehicles equipped with OBUs and AUs as well as the infrastructure backend remain the same. However, mobile nodes, i.e., vehicles, form vehicular ad hoc blockchains - similar to the concept of mobile ad hoc blockchains. Only vehicles within a certain range of each other form such networks. To do so, they agree up on an initial list of participants, while new nodes may join later or current nodes leave - depending on the context.

[3] `https://cosmos.network/`

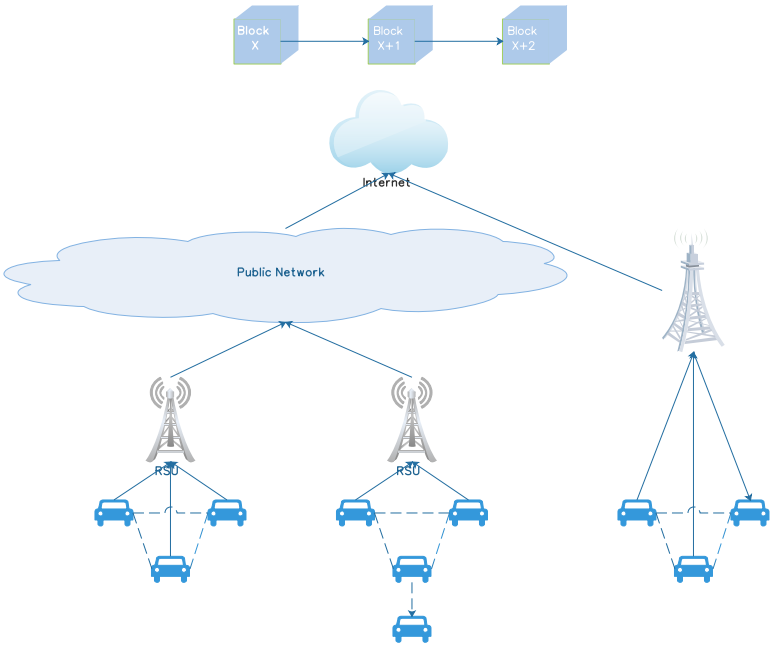

Fig. 2. Overview vehicular ad hoc blockchains.

Nodes that form a vehicular ad hoc blockchain agree up on transactions on their own (see Section 3.4 for more details on consensus) and periodically forward state and status information to RSUs or other infrastructure entities. Those permanent and fixed components have a direct connection to the Internet as well as the VANET backend which enables them to relay received information from the specific independent vehicular ad hoc blockchains to the main blockchain (depicted at the top of Figure 2). Vehicular ad hoc blockchains are either directly connected to RSUs or to some other kind of infrastructure that providers access to the Internet. Vehicles that do not have access to a RSU or alternative options can use a mesh-based approach where they connected to an ad hoc network that relays their information to the destination (middle of Figure 2). Due to the missing full network coverage along the existing road infrastructure, there might be periods where a complete set of nodes is only interconnected among each others, but not to the main network. Our system tolerates such temporary disconnects assuming that a mesh-based Internet connection can be established within a few hops or the disconnect is only limited to certain time. Longer disconnects might result in security and transaction issues, e.g., double spending, etc. and should hence be avoided. In the longterm, this problem will solve itself

once full 5G coverage is available along road sides which is anyways essential for VANETs to unfold their full potential.

3.2 Tezos Hubs and Ad Hoc Blockchains

Besides the temporary vehicular ad hoc blockchains, we also envision – similarly to [4], [25] and [33] – a set of Tezos hubs that act as master blockchain for our network. This could be the Tezos main network or an alternative independently operated Tezos chain - as long as they ensure permanent availability and Internet connection. All network participants are able to create their own hub or deploy any other solution to support their applications. The Tezos hubs are operated by validators and rely on Proof-of-Stake to reach consensus. The intention of the hub structure is to enable permanent availability of network supporting services that enable inter-blockchain communication (see Section 3.5), identity services (see Section 3.3), or backend services for applications of the vehicular ad hoc blockchains.

3.3 Identities

Tamper-proof-devices (TPDs) are a standard component of VANETs. They usually contain a public/private key pair (similar to wallet addresses) that uniquely identifies a vehicle and serves for authentication and signing as well as verification purposes. Usually, TPDs are pre-equipped by the car manufacturer and built into the vehicle's hardware. In the context of blockchains, an identity is further required in most consensus algorithms to uniquely identify participants. Moreover, a mapping between public/private keys (that constitute an identity) and vehicles is also necessary to prevent sybil node attacks. As stated by [7], "this type of attack is a common issue in large-scale peer-to-peer (P2P) systems, where hostile or faulty computing elements threaten the security of the whole network. Single faulty entities may be able to present multiple identities, thereby controlling a substantial fraction of the system, consequently undermining its functionality and security [15]".

Unfortunately, the majority of current cars does not have such a TPD that constitutes an identity. Hence, an alternative solution is required. We are currently evaluating different approaches. First, equipping vehicles on our own with small hardware devices that can easily be attached to vehicles and contain a TPD that ensures an identity binding. Second, utilizing smartphones as identity providers. Third, using blockchain-based validation and authentication protocols such as Authcoin [28][29][31].

3.4 Blockchain Consensus in VANETs

In the context of blockchains, consensus algorithms are used to agree on a set of transactions that constitutes the next block that is added to the chain. Proof-of-Work [41] and Proof-of-Stake [24] are most commonly used for example by

Bitcoin and Ethereum. For both major consensus algorithms, different flavors exists as well as a large variety of alternative protocols. However, almost all current state of the art algorithms suffer some kind of disadvantage, e.g., scalability issues, security issues, efficiency issues, and so on [18][23]. Figure 3 illustrates a collection of consensus algorithms and their scalability as well as performance properties. Those problems become even more complex in the context of mobile-

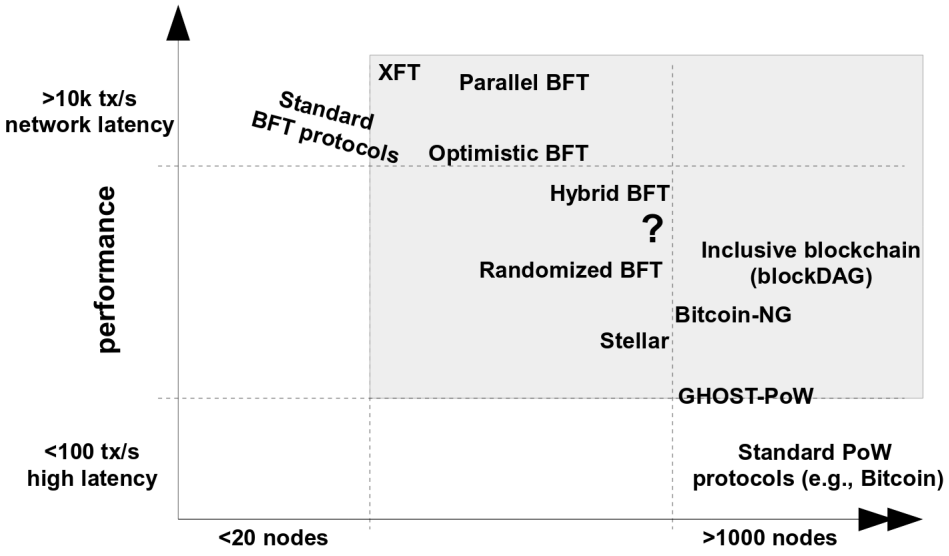

Fig. 3. Performance/Scalability comparison of a selection of consensus algorithms (Source: [47]).

and vehicular ad hoc blockchains due to the large number disjunct chains that exist in parallel as well as the the fact that entities are sometimes only connected in a mesh network without connection to the Internet which makes consensus on a global level even more difficult. In this context, timing assumptions become important. Consensus protocols might be fully synchronous which means that all messages are delivered within a pre-defined time x whereas asynchronous consensus protocols only ensure that all messages are eventually delivered [**?**]. Between those two extrema different sub-categories such as eventually synchronous, partial synchronous and weakly synchronous consensus algorithms exist [**?**][**?**][**?**]. In vehicular ad hoc blockchains a fully asynchronous consensus protocol is desirable due to the sparse connectivity of nodes and missing connection guarantees among nodes.

There are different protocols that aim to offer solutions in this regard. The Babble consensus algorithm [40] relies on a leaderless, asynchronous, Byzantine fault tolerant (BFT) algorithm that is based on Hashgraph [5].However, Hash-

graph is patent protect in the U.S. and therefore limited in us. Alternative protocols such as [38], [**?**] and [**?**] exist besides Hashgraph with certain limitations. We are currently researching different solutions that enable a leaderless, asynchronous with BFT guarantees that also scales well. Alternatively, VANETs also allow for a hierarchical blockchain solution where RSUs act as *always-on* relay blockchain nodes that accept and process transactions from groups of vehicular ad hoc blockchains, e..g, in a Cosmos-like style [25]. The RSUs then process the incoming transactions and project them into a blockchain hub block structure as outlined in Section 3.2.

3.5 Inter-Blockchain Communication

Based on the hub and ad hoc chain structure outlined earlier in Section 3.2 it is necessary to enable communication among different chains, .e.g, chain A should be able to certify that transaction x happened on chain B, even after ad hoc chain B already dissolved due to all of their members leaving. The concept of inter-blockchain communication (IBC) helps to solve this problem [4][9][25]. Essentially, the idea is that in order to proof the existence of transaction x on chain B, chain B posts a Merkle proof on chain A. In order to enable chain A to verify the Merkle proof, it must be able to keep up with the chain B's block headers - hence, interacting chains are required to be aware of one another via a bidirectional stream of proof-of-existence transactions [25]. Moreover, nodes are not required to keep a full copy of each blockchain that they interact with. Instead, light clients can be implemented in form of smart contracts and deployed on the corresponding ad hoc blockchain.

However, it is important to keep in mind that while it is possible to proof that a certain transaction took place, it is not possible to prove that a user is aware of all transactions that occurred up to the present moment. Hence, to prove completeness of transactions to the present moment an entity has to create a transaction and have it included. Afterwards, a proof that confirms that the most recent transaction was confirmed with the proper sequence number is created and distributed.

4 Use Cases and Application Scenarios

Previous sections described the general concepts of blockchains, VANETs and formal verification in the context of Tezos as well as the system architecture and communication processes of vehicular ad hoc blockchains. Next, this section introduces a selection of potential use cases and application scenarios.

As part of our previous work [32], Chorus Mobility developed a prototype application for car insurance companies that incentivizes good driving behavior of their clients. Good driving behavior comprises several factors such as: Keeping the distance to the car in front, no aggressive acceleration, no excessive speeding, no hard breaking if not necessary, or not using the phone while driving. Not only do these good driving behavior guidelines increase the overall safety of the driver

as well as all other road users, they also help to mitigate traffic congestions in urban areas. The prototype that we already developed is currently ported to Tezos.

Similarly, [30] proposed to implement all traffic rules and regulations in a digital form that all vehicles have to adhere to. "Based on exchanged traffic data, automated identification of cars, video-monitoring (e.g. at crossroads) and other traffic related data, it is possible to identify misbehaving cars and punish them accordingly. This might include speeding, ignoring traffic lights, causing an accident, etc." [30].

Another idea that is based on[30] and was further refined in [34] as well as our previous work [32][33] is the idea of road space negotiation and traffic marshaling to reduce traffic congestions. The idea is that vehicles that are either interested in using priority lanes [34] pay an extra fee to do so, or in more general, vehicles conduct road-space negotiation auctions among each other that results either in a change of positions or not [30][32][33]. Vehicles that have to move fast can pay other road space users to prioritize them so that they can reach their destination in time. Other vehicles that do not have any strict time constraints can earn some small extra money.

Finally, due to the Turing-completness of Tezos' smart contract languages, the variety of potential applications within our system is quite vast. Moreover, due to our mesh-based structure that allows for temporary disconnects of vehicular ad hoc blockchains, we further widen the field of applications.

5 Conclusion and Future Work

This work presents Chorus Mobility's Tezos-based ad hoc blockchain solution that enables vehicular ad hoc blockchains that allow groups of nodes to be temporarily disconnected from the overall network but still being able to enact and transact on a local network level for the duration of their interaction. This works extends our previous papers [32][33] where introduced a blockchain-based value transaction layer protocol for vehicular ad hoc networks that is supposed to fuel vehicle economy. However, this work extends our previous efforts and suggests a specific Tezos-based implementation that utilizes Tezos' built-in formal verification of programming languages to provide secure service provision within VANETs.

Subsequently, we outline the system architecture and detail critical components of the infrastructure, e.g., identities. Furthermore, we discuss interoperability and inter-blockchain communication that is vital for our solution. A further core element of vehicular ad hoc blockchains is an asynchronous Byzantine fault tolerant consensus algorithm. Finally, we provide three example use cases and application scenarios that rely on and benefit from the combination of formally verified smart contract languages and vehicular ad hoc blockchains.

Future work focuses on the longterm vision and the development of the platform as well as the APIs and SDKs. Besides that, we will also continue to focus

on further research aspects of the upcoming V2X economy that will facilitate future developments of Chorus Mobility.

Finally, we refer the interested reader to our previously published papers [32][33] that contain more detailed information on certain system aspects as well as the longterm vision of Chorus Mobility that we did not discuss in details as part of this vision paper.

References

1. Al-Sultan, Saif and Al-Doori, Moath M and Al-Bayatti, Ali H and Zedan, Hussien: A Comprehensive Survey on Vehicular Ad Hoc Network. Journal of Network and Computer Applications 37, 380–392 (2014)
2. Alur, R., Dill, D.L.: A Theory of Timed Automata. Theoretical computer science 126(2), 183–235 (1994)
3. Anwer, M.S., Guy, C.: A survey of vanet technologies. Journal of Emerging Trends in Computing and Information Sciences 5(9), 661–671 (2014)
4. Arrivets, M.: MONET: Mobile Ad Hoc Blockchains - Whitepaper. URL: `https://drive.google.com/file/d/1PcI69i_oJpWdsIsOciLliYEsFv9hHCVr/view` (2018), (Accessed September 04, 2018)
5. Baird, L.: The Swirlds Hashgraph Consensus Algorithm: Fair, Fast, Byzantine Fault Tolerance - Whitepaper. URL: `https://www.swirlds.com/downloads/SWIRLDS-TR-2016-01.pdf` (2016), (Accessed September 06, 2018)
6. Baldessari, R., Bödekker, B., Deegener, M., Festag, A., Franz, W., Kellum, C.C., Kosch, T., Kovacs, A., Lenardi, M., Menig, C., et al.: Car-2-Car Communication Consortium - Manifesto (2007)
7. Bochem, A., Leiding, B., Hogrefe, D.: Unchained Identities: Putting a Price on Sybil Nodes in Mobile Ad hoc Networks. In: Security and Privacy in Communication Networks (SecureComm 2018). Singapore (August 2018)
8. Calcaterra, C., Kaal, W.A., Vlad, A.: Semada Technical Whitepaper - Blockchain Infrastructure for Measuring Domain Specific Reputation in Autonomous Decentralized and Anonymous Systems. URL: `https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3125822` (2018), (Accessed April 18, 2018)
9. Chen, Z.d., Zhuo, Y., Duan, Z.b., Kai, H.: Inter-blockchain communication. DEStech Transactions on Computer Science and Engineering (cst) (2017)
10. Chiti, F., Fantacci, R., Giuli, D., Paganelli, F., Rigazzi, G.: Communications protocol design for 5g vehicular networks. In: 5G Mobile Communications, pp. 625–649. Springer (2017)
11. Christidis, K., Devetsikiotis, M.: Blockchains and Smart Contracts for the Internet of Things. IEEE Access 4, 2292–2303 (2016)
12. Civic Technologies, Inc.: CIVIC - Whitepaper. URL: `https://tokensale.civic.com/CivicTokenSaleWhitePaper.pdf` (2017), (Accessed May 01, 2018)
13. Cortright, J.: Sprawl Tax: How the US Stacks Up Internationally . URL: `http://cityobservatory.org/sprawl-tax-how-the-us-stacks-up-internationally/` (2016), (Accessed April 26, 2018)
14. Dai, P., Mahi, N., Earls, J., Norta, A.: Smart-Contract Value-Transfer Protocols on a Distributed Mobile Application Platform. URL: `https://qtum.org/uploads/files/a2772efe4dc8ed1100319c6480195fb1.pdf` (2017), (Accessed May 01, 2018)
15. Douceur, J.R.: The Sybil Attack. In: International Workshop on Peer-to-Peer Systems. pp. 251–260. Springer (2002)

16. Dwork, C., Lynch, N., Stockmeyer, L.: Consensus in the presence of partial synchrony. Journal of the ACM (JACM) 35(2), 288–323 (1988)
17. Faezipour, M., Nourani, M., Saeed, A., Addepalli, S.: Progress and Challenges in Intelligent Vehicle Area Networks. Communications of the ACM 55(2), 90–100 (2012)
18. Gervais, A., Karame, G.O., Wüst, K., Glykantzis, V., Ritzdorf, H., Capkun, S.: On the security and performance of proof of work blockchains. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. pp. 3–16. ACM (2016)
19. Goodyear, R., Ralphs, M.: Car, bus, bike or train: What were the main means of travel to work (2009)
20. Gurevich, Y., et al.: Evolving Algebras 1993: Lipari Guide. Specification and validation methods pp. 9–36 (1995)
21. Harel, D.: Statecharts: A Visual Formalism for Complex Systems. Science of computer programming 8(3), 231–274 (1987)
22. Hoare, C.A.R.: Communicating Sequential Processes. In: The origin of concurrent programming, pp. 413–443. Springer (1978)
23. Houy, N.: It will cost you nothing to'kill'a proof-of-stake crypto-currency (2014), (Accessed September 11, 2018)
24. King, S., Nadal, S.: PPcoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake. URL: `https://peercoin.net/assets/paper/peercoin-paper.pdf` (2012), (Accessed September 11, 2018)
25. Kwon, J., Buchman, E.: Cosmos: A Network of Distributed Ledgers - Whitepaper. URL: `https://cosmos.network/docs/resources/whitepaper.html` (2018), (Accessed September 06, 2018)
26. L. M. Goodman: Tezos - A Self-Amending Crypto-Ledger (White paper). URL: `https://www.tezos.com/static/papers/white_paper.pdf` (2014), (Accessed September 04, 2018)
27. Lanctot, R.: Accelerating the Future: The Economic Impact of the Emerging Passenger Economy. URL: `https://newsroom.intel.com/newsroom/wp-content/uploads/sites/11/2017/05/passenger-economy.pdf` (2017), (Accessed April 27, 2018)
28. Leiding, B.: Securing the Authcoin Protocol Using Security Risk-oriented Patterns
29. Leiding, B., Cap, C.H., Mundt, T., Rashidibajgan, S.: Authcoin: Validation and Authentication in Decentralized Networks. In: The 10th Mediterranean Conference on Information Systems - MCIS 2016. Cyprus, CY (September 2016)
30. Leiding, B., Memarmoshrefi, P., Hogrefe, D.: Self-Managed and Blockchain-Based Vehicular Ad-Hoc Networks. In: Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct. pp. 137–140. ACM (2016)
31. Leiding, B., Norta, A.: Mapping requirements specifications into a formalized blockchain-enabled authentication protocol for secured personal identity assurance. In: International Conference on Future Data and Security Engineering. pp. 181–196. Springer (2017)
32. Leiding, B., Vorobev, W.V.: Enabling the Vehicle Economy Using a Blockchain-Based Value Transaction Layer Protocol for Vehicular Ad-Hoc Networks. URL: `https://uploads-ssl.webflow.com/5a4ea18a81f55a00010bdf45/5b69e53263e2a6076124ecbe_Chorus-Mobility-WP--v1.0.1.pdf` (2018), (Accessed September 06, 2018)

33. Leiding, B., Vorobev, W.V.: Enabling the Vehicle Economy Using a Blockchain-Based Value Transaction Layer Protocol for Vehicular Ad-Hoc Networks. In: The 12th Mediterranean Conference on Information Systems - MCIS 2018. Corfu, Greece (September 2018)
34. MacNeille, P.R., Wisniewski, J., DeCia, N.: Vehicle-to-Vehicle Cooperation to Marshal Traffic (Mar 27 2018), uS Patent 9,928,746
35. McCorry, P., Shahandashti, S.F., Clarke, D., Hao, F.: Authenticated key exchange over bitcoin. In: International Conference on Research in Security Standardisation. pp. 3–20. Springer (2015)
36. McKenzie, B.: Who Drives to Work? Commuting by Automobile in the United States: 2013. American Community Survey Reports (2015)
37. Mieke Berends-Ballast et al.: Transport and Mobility 2016. URL: `https://www.cbs.nl/en-gb/publication/2016/25/transport-and-mobility-2016` (2016), (Accessed April 26, 2018)
38. Miller, A., Xia, Y., Croman, K., Shi, E., Song, D.: The honey badger of bft protocols. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. pp. 31–42. ACM (2016)
39. Mitra, R.N., Agrawal, D.P.: 5g mobile technology: A survey. ICT Express 1(3), 132–137 (2015)
40. Mosaic Networks: Babble Consensus - Documentation. URL: `https://babbleio.readthedocs.io/en/latest/consensus.html` (2017), (Accessed September 08, 2018)
41. Nakamoto, S.: Bitcoin: A Peer-to-Peer Electronic Cash System. URL: `https://bitcoin.org/bitcoin.pdf` (2008), (Accessed May 01, 2018)
42. Nguyen, Q.K.: Blockchain - A Financial Technology for Future Sustainable Development. In: Green Technology and Sustainable Development (GTSD), International Conference on. pp. 51–54. IEEE (2016)
43. Ouaddah, A., Elkalam, A.A., Ouahman, A.A.: Towards a Novel Privacy-Preserving Access Control Model Based on Blockchain Technology in IoT. In: Europe and MENA Cooperation Advances in Information and Communication Technologies, pp. 523–533. Springer (2017)
44. Petri, C.A.: Kommunikation mit Automaten. Ph.D. thesis, Technical University of Darmstadt (1962)
45. SALT Technology, Ltd.: SALT - Blockchain-Backed Loans - Whitepaper. URL: `https://membership.saltlending.com/files/abstract.pdf` (2017), (Accessed April 25, 2018)
46. Toh, C.K.: Ad hoc mobile wireless networks: protocols and systems. Pearson Education (2001)
47. Vukolić, M.: The quest for scalable blockchain fabric: Proof-of-work vs. bft replication. In: International Workshop on Open Problems in Network Security. pp. 112–125. Springer (2015)
48. Wing, J.M.: A Specifier's Introduction to Formal Methods. Computer 23(9), 8–22 (1990)
49. Wood, G.: Ethereum: A Secure Decrentralized Generalised Transaction Ledger. URL: `http://gavwood.com/paper.pdf` (2014), (Accessed May 01, 2018)