title

-

Research Paper - Version 0.0
August 26, 2018

Benjamin Leiding and William V. Vorobev

Chorus Mobility
Email: hello@chorus.mobi

Abstract.

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

1 Introduction

The next generation of tightly interconnected vehicles offers a variety of new technologies as well as business opportunities. Vehicles form so-called vehicular ad-hoc networks (VANETs) in order to 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 research paper, we presented a blockchain-based system that enables a manufacturer agnostic platform solution that allows VANET participants to enact and transact any kind of services and goods. Usually, sophisticated systems of interconnected cars in the context of VANETs 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 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. 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. The

self-amending blockchain platform Tezos 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 whitepaper fills the gap by introducing Vehicular Ad Hoc Tezos 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.

This whitepaper addresses the detected gap by introducing the Chorus Mobility solution, thereby answering the question of how to implement a blockchain-based transaction layer that enables a V2X platform for goods and services? In order to answer this question with a separation of concerns, we pose the following sub-questions: What is the long term vision of Chorus Mobility? What are the critical requirements and the corresponding architecture of the Chorus V2X platform? What are the system-engagement processes for the stakeholders?

The remainder of this paper is structured as follows: Section 2 introduces supplementary literature and related work. Section 3 outlines the vision of Chorus Mobility. Afterwards, Section 4 analyses the requirements of the system and outlines the resulting system architecture that we derive from the requirements. Afterwards, Section 5 expands on the system-engagement processes for the stakeholders, followed by Section **??** that introduces our prototype. Section 7 provides an discussion and an analysis of related projects. Finally, Section 6 concludes this work and provides an outlook on future work.

2 Technical Background and Supplementary Literature

The following section provides background information and describes related works regarding previous ideas and concepts that focus on a 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 [20], Qtum [7], or Tezos [10], 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" [7]. 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 [16][18], academic and business authentication and identity solutions [3][6][12][15][19], reputation systems [4] as well as platforms for Internet-of-Things (IoT) applications [5][17].

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 [2]. 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][2].
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) [8]. For authentication purposes, each network participant is equipped with a unique public/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

basic introduction with motivation, advantages and disadvantages A380 example?

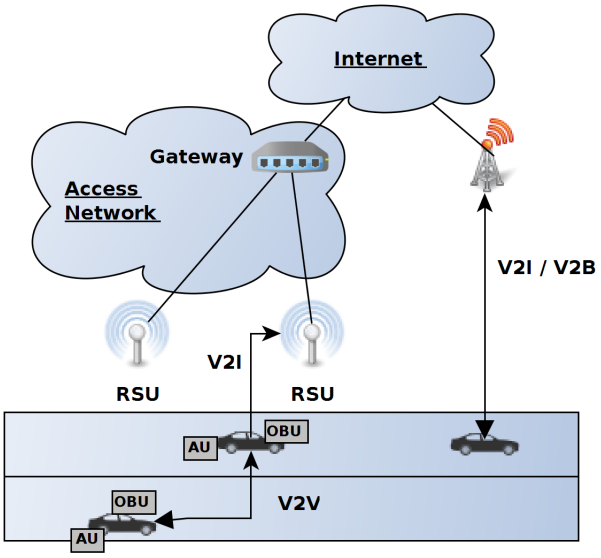

Fig. 1. General VANET architecture (Based on [2] and [13])

connect formal verification and blockchain tezos cardano others?

2.4 Related Work

3 System Design and Architecture

3.1 System Architecture

3.2 Identities

involve Authcoin [11][12][14]

3.3 Blockchain Consensus in VANETs

4 Network and Communication

4.1 Inter-Blockchain Communication

4.2 Network Communication

+5g

4.3 Hubs

5 Use Cases and Application Scenarios

6 Conclusion and Future Work

This whitepaper presents

7 Notes

– somehow get FOAM [9] into this?

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. 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)
3. 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)
4. 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)
5. Christidis, K., Devetsikiotis, M.: Blockchains and Smart Contracts for the Internet of Things. IEEE Access 4, 2292–2303 (2016)
6. Civic Technologies, Inc.: CIVIC - Whitepaper. URL: `https://tokensale.civic.com/CivicTokenSaleWhitePaper.pdf` (2017), (Accessed May 01, 2018)
7. 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)
8. 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)
9. Foamspace Corp: FOAM - Whitepaper. URL: `https://www.foam.space/publicAssets/FOAM_Whitepaper_May2018.pdf` (2018), (Accessed May 08, 2018)
10. L. M. Goodman: Tezos - A Self-Amending Crypto-Ledger (White paper). URL: `https://www.tezos.com/static/papers/white_paper.pdf` (2014), (Accessed April 27, 2018)
11. Leiding, B.: Securing the Authcoin Protocol Using Security Risk-oriented Patterns
12. 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)
13. 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)
14. 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)
15. 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)

16. 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)
17. 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)
18. SALT Technology, Ltd.: SALT - Blockchain-Backed Loans - Whitepaper. URL: `https://membership.saltlending.com/files/abstract.pdf` (2017), (Accessed April 25, 2018)
19. SelfKey Foundation: SelfKey - Whitepaper. URL: `https://selfkey.org/whitepaper/` (2017), (Accessed April 27, 2018)
20. Wood, G.: Ethereum: A Secure Decrentralized Generalised Transaction Ledger. URL: `http://gavwood.com/paper.pdf` (2014), (Accessed May 01, 2018)