# Blackchain: Scalability for Resource-Constrained Accountable Vehicle-to-X Communication

Rens W. van der Heijden
Institute of Distributed Systems
Ulm University
Ulm, Germany
rens.vanderheijden@uni-ulm.de

Felix Engelmann
Institute of Distributed Systems
Ulm University
Ulm, Germany
felix.engelmann@uni-ulm.de

David Mödinger
Institute of Distributed Systems
Ulm University
Ulm, Germany
david.moedinger@uni-ulm.de

Franziska Schönig
Ulm University
Ulm, Germany
franziska.schoenig@uni-ulm.de

Frank Kargl
Institute of Distributed Systems
Ulm University
Ulm, Germany
frank.kargl@uni-ulm.de

## Abstract

In this paper, we propose a new Blockchain-based message and revocation accountability system called Blackchain. Combining a distributed ledger existing mechanisms for security in V2X communication systems, we design a distributed event data recorder (EDR) that satisfies traditional accountability requirements by providing a compressed global state. Unlike previous approaches, our distributed ledger solution provides an accountable revocation mechanism without requiring trust in a single misbehavior authority, instead allowing a collaborative and transparent decision making process through Blackchain. This makes Blackchain an attractive alternative to existing solutions for revocation in a Security Credential Management System (SCMS), which suffer from the traditional disadvantages of PKIs, notably incuding centralized trust. Our proposal becomes scalable through the use of hierarchical consensus: individual vehicles dynamically create clusters, which then provide their consensus decisions as input for road-side units (RSUs), which in turn publish their results to misbehavior authorities. This authority, which is traditionally a single entity in the SCMS, responsible for the integrity of the entire V2X network, is now a set of authorities that transparantly perform a revocation, whose result is then published in a global Blackchain state. This state can be used to prevent the issuance of certificates to previously malicious users, and also prevents the authority from misbehaving through the transparency implied by a global system state.


*SERIAL'17, December 2017, Las Vegas, USA*

ACM ISBN 123-4567-24-567/08/06…$15.00
https://doi.org/10.475/123_4

***CCS Concepts*** • **Networks → Network security**; *Peer-to-peer protocols*; • **Security and privacy →** *Network security*;

***Keywords*** Distributed Ledger, VANET, Accountability

**ACM Reference Format:**
Rens W. van der Heijden, Felix Engelmann, David Mödinger, Franziska Schönig, and Frank Kargl. 2017. Blackchain: Scalability for Resource-Constrained Accountable Vehicle-to-X Communication. In *Proceedings of ACM SERIAL Workshop, Las Vegas, USA, December 2017 (SERIAL'17),* 5 pages.
https://doi.org/10.475/123_4

## 1 Introduction

An event data recorder (EDR), the car equivalent of a flight recorder, can be used for a multitude of applications, e.g., forensic accident reconstruction [4, 8] and misbehavior detection [10]. EDRs are difficult to implement for V2X as they require complex append-only semantics, and they should provide at least tamper-evidence. These circumstances, missing data de-duplication and a lack of research lead to expensive components, which encumbers adoption in real-world scenarios.

To tackle these problems, this paper examines the use of distributed ledgers (DL) for this application. Distributed ledgers are distributed data storages, which provide an append-only semantic to the participants. This allows us to employ known techniques of data de-duplication and tamper-proofing the data.n at Middleware. Students attending workshops/tutorials or who are not presenting papers are encouraged to apply. Student presenters with funding available fro The most well known implementation of a distributed ledger, Bitcoin [7], provides the consensus, and therefore tamper-proofing, by restricting the rate of data write through a proof-of-work mechanism. However, a naive adoption of this ledger is not suitable for our scenario, because it does not scale to the message frequency encountered by an in-vehicle EDR.

Therefore we propose a public permissioned based on a hierarchical byzantine fault tolerant consensus. On the lowest layer, cars form clusters and agree on a state change which is propagated to a road side unit (RSU). As there are too many RSUs deployed to reach a global consensus efficiently, smaller RSU groups form and aggregate a partial state. The fixed set of transaction issuers allow for a weighted consensus and efficient, distributed mining process.

In recent years, with concrete implementation plans for V2X communication systems, researchers have started to look more closely at the design of a real-world public key infrastructure (PKI) and the multitude of requirements in such a system. Most recent designs, such as that proposed by Whyte et al. [11], include a misbehavior authority, in addition to a standard certificate revocation component as in regular PKIs. This authority is responsible for accepting misbehavior reports, processing them according to some fixed algorithm, and revoking any vehicles that show malicious behavior. In the real world, it is likely that not just one, but several of such SCMSs will be deployed by competing entities (either vehicle manufacturers or countries [8]. To make this process more transparent, and to reduce the trust necessary in any one SCMS, we propose the use of a distributed ledger for accountability. This will not only include accountability of vehicles towards the system, but also the accountability of the MAs amongst each other, and towards the users of the system (i.e., the vehicle owners). There is a lot of work on how to locally revoke malicious vehicles [1, 5], but transferring this consensus to a global system is an as-yet unsolved challenge, despite various proposals in the literature. In particular, it is challenging to make the consensus verifiable without additional trust requirements from the users.

In the remainder of this paper, we introduce the conceptual foundations of our proposal. Specifically, we describe a detailed system model, including privacy and attacker models, in Section 2. Section 3 then describes our Blackchain proposal and some possible attacks on our base system. We finally discuss the implications of these ideas for distributed ledgers and misbehavior detection research in Section 4.

## 2 System and Attacker Model

Vehicular ad-hoc networks (VANETs) consist of vehicles and road-side units (RSUs), equipped with wireless communication modules. Unlike traditional wireless networks, VANETs are primarily based on broadcast communication: vehicles periodically broadcast beacons, containing application-relevant information such as position, speed, heading, and some metadata. Applications of VANETs vary from crash avoidance to finding fastest routes and fuel and road efficiency applications, which can potentially be combined with self-driving vehicles to further increase performance. Communication typically uses the IEEE 802.11 standard, with a range between 300 and 1000 meters; many authors propose more advanced communication patterns on top of this. RSUs are typically assumed to be available in some locations only (e.g., attached to traffic lights), but provide an intermittent link to the Internet for all vehicles. Some research suggests that the current work in 5G cellular communication may provide more permanent Internet connectivity, although this may be costly for users; a heterogeneous network using both technologies is a current hot topic in this community [9]. For this paper, we focus on the case of clustering, where vehicles communicate with others in communication range directly, but a cluster head (CH) is responsible for communication with other clusters. For an overview of clustering techniques, we refer interested readers to a recent survey by Cooper et al. [3].

In VANETs, security plays an important role, due to the lives dependent on the communication. Unlike existing IT infrastructures, the main focus of security lies on integrity and availability, rather than confidentiality; it is generally assumed that the message contents are not encrypted, since any vehicle needs access to this content for any VANET application to provide any real benefit. Message integrity is generally protected through signed messages, where each vehicle possesses a number of authentic public keys from a vehicular public key infrastructure (VPKI). One of the proposed standards to organize such a VPKI, proposed by Whyte et al. [11], is the security credential management system (SCMS), which proposes a number of authorities to protect the privacy of the users. Issuing pseudonyms involves the following authorities: the enrollment certificate authority (ECA), responsible for long-term identities of vehicles, the registration authority (RA), who essentially checks whether a vehicle may still receive pseudonyms, and the pseudonym certificate authority (PCA), which issues pseudonyms. When vehicles report misbehavior, this report mainly concerns specific vehicles (and ideally includes evidence, see e.g. [2]). As evidence suspicious messages can be used, for example. A sample misbehavior report can be found in Figure 1. The trust statement mirrors the solution of the local misbehavior detection system. Besides information of the suspects a report could store the detected misbehavior, the pseudonym identifier of the reporter and the associated cluster identifier. This information is processed by the misbehavior authority (MA), which can decide on the validity of these reports and subsequently revoke pseudonyms and long term identities in cooperation with the PCA and one or more linkage authority (LA). This protocol also informs the RA not to issue any more certificates for the reported vehicle.

It is important that the MA only revokes reliable vehicles, which requires that the MA is able to validate the reports of vehicles (i.e., objectively check the evidence) and detect when an attack against the revocation system itself is ongoing. Attacks on the revocation system include those that exist for traditional reputation systems (e.g., bad-mouthing attacks, where an attacker creates false accusations), often

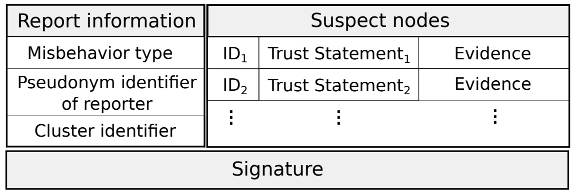


**Figure 1.** Sample structure of a misbehaviour Report

combined with Sybil attacks (where an attacker uses multiple pseudonyms to artificially increase the evidence for their claim). In our proposed system model, we allow the attacker to use at most two pseudonyms at any time, in order to limit the Sybil attack capabilities within a cluster. This can be achieved in real-world system by limiting the validity of certificates appropriately (as discussed in EU proposals [6]), increasing the overhead, but providing tighter control with limited privacy loss.

## 3 Blackchain

We propose Blackchain (*Black*box Block*chain*), with which we aim to provide cluster-based VANETs with an integrated accountability system that exploits clusters to create a distributed ledger for exchanged messages. Since these messages relate to real-world observations and processes, there are objective ways to establish which of these messages are correct (i.e., corresponding to the real world), and which contain false data. Detecting malicious actors this way is referred to as *misbehavior detection*: for a survey of different mechanisms that can be used for this purpose, we refer interested readers to our recent survey on this topic [10]. This objective truth can also be used to detect attackers at a central location, such as the MA discussed in the previous section. In this paper, we propose that the Blackchain can be used to perform this centralized misbehavior detection and revocation without requiring trust in any individual trusted third party (TTP). The concept is shown in Figure 2: different countries will likely run their own SCMS, and a protocol is needed to perform cross-border revocation. Our proposal not only enables this functionality, but also makes each SCMS accountable towards the participating vehicles.

Each vehicle accumulates information about it's own state and, through received messages, about other vehicles in the vicinity. Unlike the classical approach to store these state changes in an EDR, with the overhead of a trusted platform to ensure the append-only property, we persist these changes in a DL. A direct approach to this would be to require each vehicle to participate in the Blackchain directly as a network node, but without participating in the mining process. Having observations from different nearby neighbours in the Blackchain, malicious behaviour can easily be detected through misbehavior detection. By propagating the resulting blocks to the MAs, who also participate in the Blackchain network, a consensus decision can then be made to revoke the corresponding vehicle, which can be stored in the Blackchain along with the associated evidence, persisting all the relevant information automatically. This results in a public, permissioned blockchain, where all MAs mine blocks by reaching consensus about misbehavior detection decisions. Although the decision making process is restricted to MAs, the public nature of the Blackchain allows all participants to verify the correctness of these decisions. Most importantly, the append-only property is guaranteed globally instead of trusting the individual blackboxes in each vehicle.

Unfortunately this approach is not viable in the presence of millions of vehicles and update frequencies of 10 Hz for each vehicle. Therefore, we reduce the amount of state updates and increase the number of verifying nodes. The first is achieved by clustering vehicles together which all agree on a reduced common state (using a local revocation protocol, such as OREN [1]). The cluster state reduces the size and frequency of updates from vehicles but still allows other parties to verify the correct behaviour of the cluster participants. The second adaptation is to use the RSUs, which also observe messages, to participate in the network as verification nodes. All RSUs have known identities, which can be used to run a byzantine fault tolerance (BFT) consensus. A BFT consensus over all RSUs will still result in a poor performance, due to the latencies and the sheer number of RSUs that may be deployed in the future. We thus again apply clustering to reduce the amount of nodes and increase performance. This can be done by grouping RSUs by area or manufacturer, e.g., all RSUs in one city, to form a cluster and agree on a common state, and thus a set of maliciously behaving clients.

## 4 Conclusion

In this paper, we have provided some conceptual foundations for Blackchain, a distributed ledger that provides accountability for misbehavior authorities and vehicles alike. The purpose of Blackchain is to reduce the trust requirements on users of a vehicular communication system, improving the

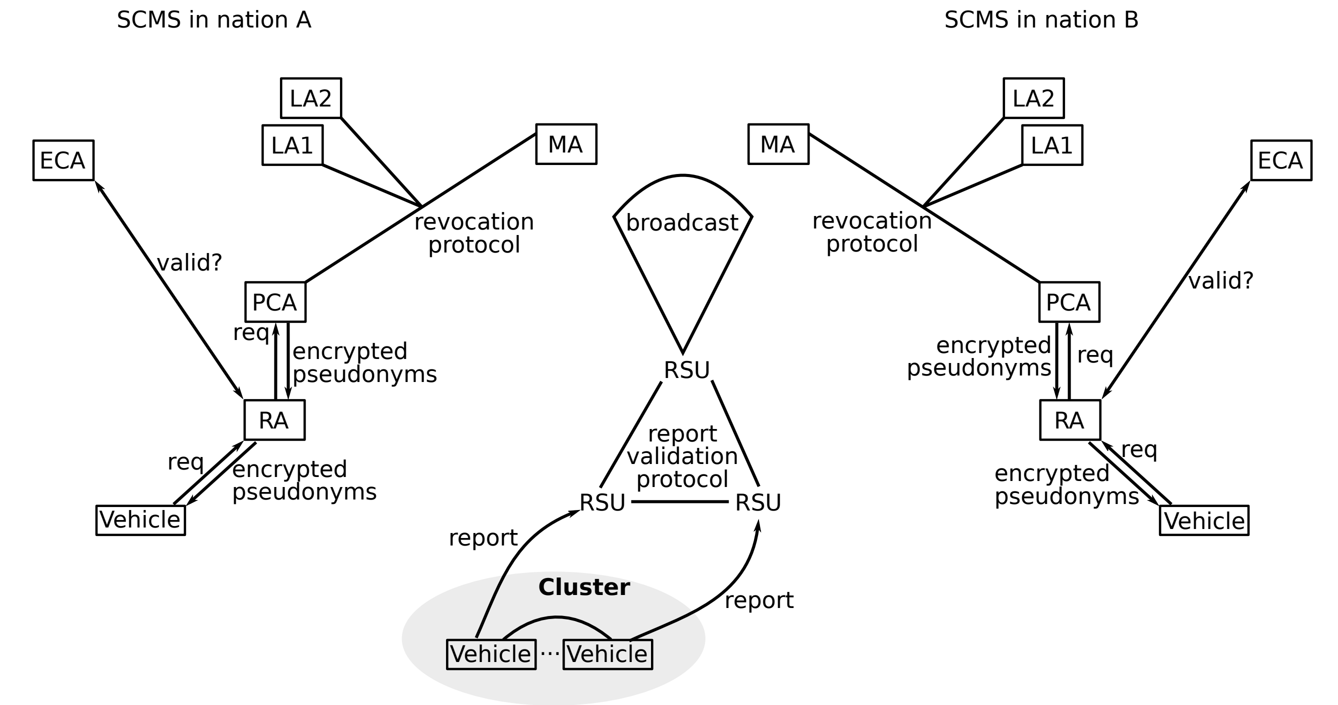


**Figure 2.** Blackchain's underlying system architecture.

performance of global revocation algorithms by employing hierarchical consensus, and creating accountability for misbehavior authorities. However, these foundations are only the first step in this area of research: there are many open questions that still need to be solved to make this system practically feasible. From the vehicular perspective, the most important factor is whether clusters are stable enough to provide the necessary consensus algorithms. From a distributed ledger perspective, the most exciting question is what guarantees hierarchical consensus can provide compared to a full consensus where all RSUs and MAs (and even potentially all vehicles) participate. Although Blackchain itself may not be feasible to implement, we think our proposal gives interesting directions of research for both fields, which are valuable beyond the actual implementation of Blackchain.

## Acknowledgments

This work was partially funded by the Baden-Württemberg Stiftung. In addition, we would like to thank Benjamin Erb for the initial discussion that lead to the creation of this paper.

## References

[1] Igor Bilogrevic, Mohammad Hossein Manshaei, Maxim Raya, and Jean-Pierre Hubaux. 2011. OREN: Optimal revocations in ephemeral networks. *Computer Networks* 55, 5 (April 2011), 1168–1180. https://doi.org/10.1016/j.comnet.2010.11.010

[2] Norbert Bißmeyer, Joël Njeukam, Jonathan Petit, and Kpatcha M. Bayarou. 2012. Central misbehavior evaluation for VANETs based on mobility data plausibility. In *Proceedings of the ninth ACM international workshop on Vehicular inter-networking, systems, and applications (VANET)*. ACM Press, New York, NY, USA, 73–82. https://doi.org/10.1145/2307888.2307902

[3] C. Cooper, D. Franklin, M. Ros, F. Safaei, and M. Abolhasan. 2017. A Comparative Survey of VANET Clustering Techniques. *IEEE Communications Surveys Tutorials* 19, 1 (Firstquarter 2017), 657–681. https://doi.org/10.1109/COMST.2016.2611524

[4] Yuliya Kopylova, Csilla Farkas, and Wenyuan Xu. 2011. *Accurate Accident Reconstruction in VANET*. Springer Berlin Heidelberg, Berlin, Heidelberg, 271–279. https://doi.org/10.1007/978-3-642-22348-8_23

[5] Bisheng Liu, Jerry T. Chiang, and Yih-Chun Hu. 2010. Limits on Revocation in VANETs. In *Pre-Proceedings of the 8th International Conference on Applied Cryptography and Network Security (ACNS 2010 industry track)*.

[6] Z. Ma, F. Kargl, and M. Weber. 2008. Pseudonym-On-Demand: A New Pseudonym Refill Strategy for Vehicular Communications. In *2008 IEEE 68th Vehicular Technology Conference*. 1–5. https://doi.org/10.1109/VETECF.2008.455

[7] Satoshi Nakamoto. 2009. Bitcoin: A Peer-to-Peer Electronic Cash System. (2009). https://bitcoin.org/bitcoin.pdf.

[8] M. Raya, P. Papadimitratos, and J. p. Hubaux. 2006. SECURING VEHICULAR COMMUNICATIONS. *IEEE Wireless Communications* 13, 5 (October 2006), 8–15. https://doi.org/10.1109/WC-M.2006.250352

[9] L. C. Tung, J. Mena, M. Gerla, and C. Sommer. 2013. A cluster based architecture for intersection collision avoidance using heterogeneous networks. In *2013 12th Annual Mediterranean Ad Hoc Networking Workshop (MED-HOC-NET)*. 82–88. https://doi.org/10.1109/MedHocNet.2013.6767414

[10] Rens W van der Heijden, Stefan Dietzel, Tim Leinmüller, and Frank Kargl. 2016. Survey on Misbehavior Detection in Cooperative Intelligent Transportation Systems. *arXiv preprint arXiv:1610.06810* (2016).

[11] W. Whyte, A. Weimerskirch, V. Kumar, and T. Hehn. 2013. A security credential management system for V2V communications. In *2013 IEEE*

*Vehicular Networking Conference*. 1–8. https://doi.org/10.1109/VNC.2013.6737583