Blockchain-inspired Event Recording System for Autonomous Vehicles

Hao Guo   Ehsan Meamari   Chien-Chung Shen

Department of Computer and Information Sciences

University of Delaware, U.S.A.

{haoguo,ehsan,cshen}@udel.edu

Abstract—Autonomous vehicles are capable of sensing their environment and navigating without any human inputs. However, when autonomous vehicles are involved in accidents between themselves or with human subjects, liability must be indubitably decided based on accident forensics. This paper proposes a blockchain-inspired event recording system for autonomous vehicles. Due to the inefficiency and limited usage of certain blockchain features designed for the traditional cryptocurrency applications, we design a new "proof of event" mechanism to achieve indisputable accident forensics by ensuring that event information is trustable and verifiable. Specifically, we propose a dynamic federation consensus scheme to verify and confirm the new block of event data in an efficient way without any central authority. The security capability of the proposed scheme is also analyzed against different threat and attack models.

I. INTRODUCTION

An autonomous vehicle (also known as driverless vehicle or self-driving vehicle) is capable of sensing its environment and navigating without any human input [1]. To facilitate self-driving, autonomous vehicles adopt a variety of sensory technologies, such as lidar, camera, and ultrasound, to detect their surroundings, and use a control system to interpret sensory information to identify appropriate navigation paths, as well as avoid obstacles and follow relevant traffic signs. Based on a recent survey, roughly two-thirds of Americans expect cars to be totally autonomous in the next half century [2].

However, *with autonomy, comes accountability*. When autonomous vehicles are involved in accidents (collisions between themselves, or collisions with conventional vehicles, pedestrians or other objects), how could such events be recorded for forensic purposes to determine liability? In addition, how could such recorded events be verified, trusted, and not tampered? Such issues become critical when there exist incentives for different parties involved to tamper with the recorded events to avoid punitive penalties. This paper proposes a blockchain-inspired event recording scheme to help autonomous vehicles achieve a tamper-proof and verifiable event recording and forensics system.

A blockchain consists of a series of blocks, each of which is composed of sets of timestamped transactions and a hash of its previous blocks [3]. The original blockchain was designed for Bitcoin, a digital cryptocurrency, to solve the double-spending problem by using the *Proof of Work* (PoW) mechanism [4]. In PoW, miners compete with one another to become the first to solve a hash puzzle so as to obtain the right to generate the next block and to receive incentives. However, PoW usually takes 10 minutes to solve a puzzle and generate a new block. Due to the computational difficulty of the current PoW, miners tend to form bigger mining pools to conduct PoW [5], which diminishes one original feature of being decentralized.

In our proposed event recording system, accidents are recorded as timestamped transactions which are to be saved into a new block in real-time. Although autonomous vehicles may be equipped with reasonable computing capacity, conducting PoW to save the event of an accident in real-time will not be feasible due to the complexity of solving a hash puzzle.

To address this critical issue, we propose the mechanism of *Proof of Event with Dynamic Federation Consensus* to record accident events in a new block. When an accident occurs, vehicles directly involved in the accident broadcast 'event generation' requests (via IEEE 802.11p [DSRC], for instance), which only those vehicles within the (DSRC) communication range will receive and respond. Then, both the vehicles directly involved in the accident and those vehicles receiving the request will generate and broadcast the event into a 'vehicular network' which is defined based on the existing cellular network infrastructure. Within the vehicular network, a random federation group is formed to verify and save the event data into a new block by using a multi-signature scheme [6]. And finally the generated new block will be sent and saved in Department of Motor Vehicles (DMV) for the permanent records.

The mechanism of Proof of Event with Dynamic Federation Consensus records events for indisputable accident forensics and protects data integrity and trustworthiness by utilizing event data from multiple sources and the generated hash digest. The recorded events also provide traceable evidence. Specifically, the proposed Dynamic Federation Consensus scheme replaces the role of PoW in the original blockchain to confirm and save a new block in a fast and effective way without incurring extensive computation. As a federation is dynamically formed around each accident over a vehicular network, the consensus on the authenticity of the generated events can be recorded in a flexible and robust manner.

The remainder of the paper is organized as follows. Related work is described in Section II. In Section III, we present the cellular network-based vehicular network and describe the mechanism of Proof of Event with Dynamic Federation Consensus. In addition to normal cases, 'extreme' accident

scenarios are discussed in Section IV. In Section V, we analyze the security of the proposed scheme against potential attacks. Section VI concludes the paper.

II. RELATED WORK

A. Event Data Recorders

An event data recorder (EDR), a vehicle equivalent of a plane's flight recorder or "black box," is installed in vehicles to record information related to crashes or accidents [7]. Some EDRs continuously record data until a crash or accident stops them, and others are activated by crash-like events (such as a sudden decrease in velocity) and may continue to record until the accident is over, or until the recording time expires [7]. Due to its individual and independent installation, once an EDR is damaged or malfunctions, there is no chance to restore or verify the information stored.

Heijden et al. [8] proposed a distributed ledger that provides accountability for both misbehavior authorities and vehicles. The goal is to reduce the requirements of trust on users of vehicular communication systems and to create accountability for misbehavior authorities via hierarchical consensus and global revocation. In contrast, our work focuses on accident forensics for autonomous vehicles. By employing the mechanism of Proof of Event with Dynamic Federation Consensus, accident events are stored in a trustable, verifiable, and tamper-proof manner.

B. Blockchain-based Vehicular Systems

Yuan et al. [9] proposed a secured and decentralized blockchain-based autonomous intelligent transportation systems with better usage of infrastructures and resources. A case study is presented to describe a blockchain-based real-time ride-sharing system. By using Ethereums smart contract system. Leiding et al. [10] proposed a self-managed and decentralized system to deploy and run any type of application on vehicular ad-hoc networks without a central managing authority. By using a blockchain-based public key infrastructure, Rowan et al. [11] proposed a novel inter-vehicle session key establishment protocol to secure vehicle-to-vehicle communications through visible light and acoustic side-channels. However, none of the work took inspiration from blockchain to design an accident forensics system for autonomous vehicles.

C. Consensus Methods

As consensus is critical to the decentralized nature of blockchain, we review existing consensus schemes to highlight our unique contribution. In the current state-of-the-art, PoW [12], Proof of Stake (PoS) [13], and Proof of Authority (PoA) [14] and several other Proof of 'X' consensus models all rely on selecting one single peer to produce the new block. However, these consensus models gradually deviate from the original goals of decentralization and democratization. For instance, one single peer is selected by nonce lottery via mining as with PoW, by random selection among the largest stake holders as with PoS [15], and by random selection among nodes via

one centralized authority as with PoA. Therefore, large mining pools centralize authorities of Bitcoin, PoS concentrates power in the hands of few peers based on their balance, and PoA leaves the decision of which entities can generate new blocks in the network to one central authority [15]. Thus, all of these models have been falling short of their initial goals. In contrast, the mechanism of Proof of Event with Dynamic Federation Consensus proposed in this paper addresses the dynamic and autonomous nature of self-driving vehicles so that the accident forensic information could be validated by a federation than one single individual.

III. ARCHITECTURE OF RECORDING SYSTEM

A. Cellular Network-based Vehicular Network

We adopt a cellular network-based infrastructure to define a 'vehicular network' for each accident, where all the vehicles covered by the same base station (*i.e.*, within the same cell) of the vehicles directly involved in an accident form a 'vehicle network' as depicted in Fig. 1. We also assume that all the autonomous vehicles register with an authority, such as Department of Motor Vehicles (DMV), using license plate and VIN number.

Vehicles use the IEEE 802.11p standard of Dedicated Short-Range Communications (DSRC) [16] to send and receive 'event generation' requests. Meanwhile, vehicles are connected to a cellular network to broadcast and confirm event data within the corresponding vehicular network so as to create new blocks.
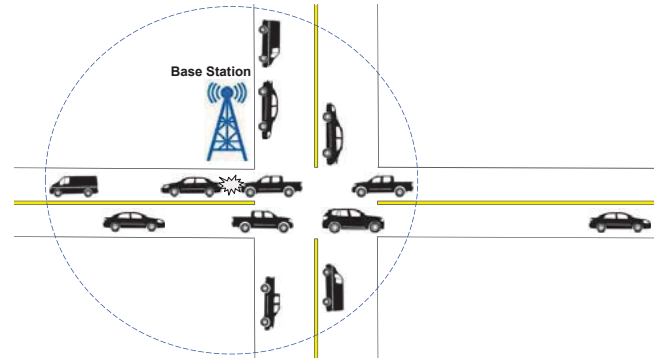

Fig. 1: Cellular network-based 'vehicular' network.

B. Proof of Event with Dynamic Federation Consensus

To facilitate forensic investigation after an accident, one issue is the correctness and trustworthiness of the recorded data, as vehicles involved, both directly and as bystanders, might have incentives to alter accident related information to avoid punitive penalties. Therefore, it is critical to record authenticated event data at the specific time and location of the accident. The recorded information about the accident could later be retrieved and cross-examined to determine liability. It can provide the consensus on whether an event is verifiable and trustworthy at the certain geographic location and time. We propose the following two steps to accomplish the goal:
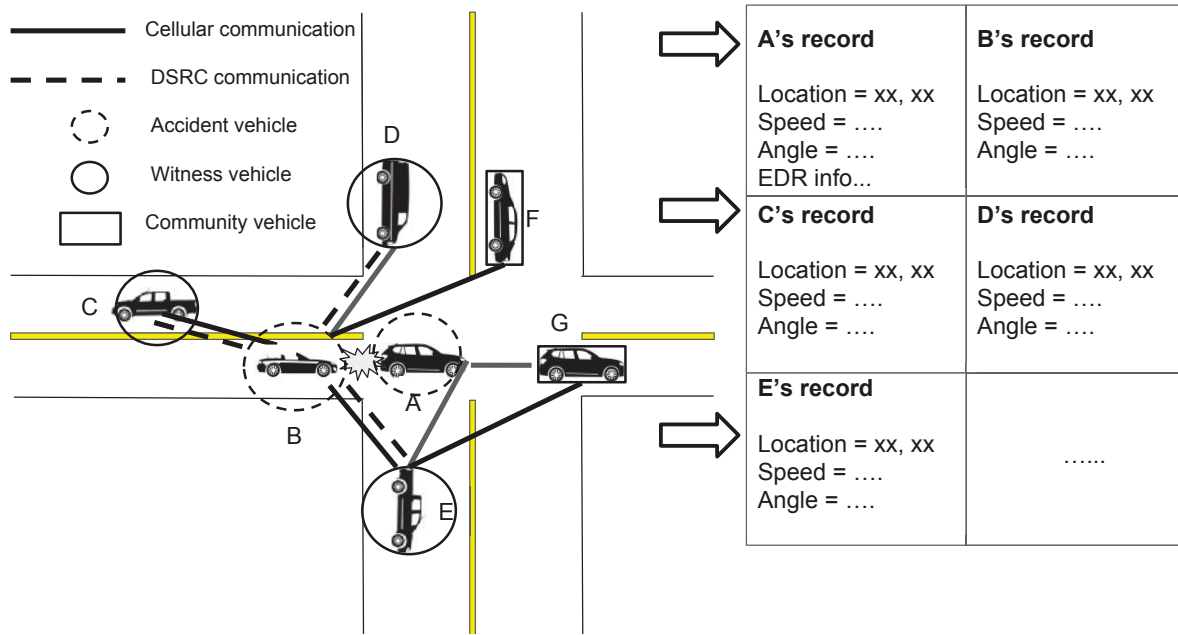
A's record	B's record
Location = xx, xx Speed = …. Angle = …. EDR info...	Location = xx, xx Speed = …. Angle = ….
C's record	**D's record**
Location = xx, xx Speed = …. Angle = ….	Location = xx, xx Speed = …. Angle = ….
E's record	
Location = xx, xx Speed = …. Angle = ….	…....

Fig. 2: After an accident, both accident and witness vehicles generate and broadcast event data.

first to gather trustable event data from both vehicles directly involved in the accident and neighboring vehicles, then to verify and save event data with the help of a dynamically formed federation of vehicles within the same vehicular network.

1) Gathering event data: Vehicles directly involved in an accident are termed "accident" vehicles, vehicles within the DSRC transmission range from the accident scene are termed "witness" vehicles, and vehicles within the same cell but outside the DSRC transmission range from the accident scene are termed "community" vehicles. To record the event of an accident, upon the occurrence of an accident, "accident" vehicles send 'event generation' requests to "witness" vehicles. Fig. 2 depicts a scenario, where vehicles A and B got into an accident. "Witness" vehicles C, D, and E within the DSRC transmission range from the accident scene receive the event generation requests and confirm with the "accident" vehicles via DSRC. Fig. 4 depicts these sequence of events over time.

Fig. 3: Hash digest of event data.

Then, both "accident" and "witness" vehicles generate their respective event data with their own locations, EDR records (which capture histories of sensor readings around the accident scene), timestamps and the corresponding hash digests (as computed in Fig. 3), and broadcast their event data via cellular communications within the vehicular network under the same cell. All the broadcast event data from both "accident" and "witness" vehicles will be verified and saved in a new block by a federation to be described next.

2) Verifying and creating new block of accident event: Upon the occurrence of an accident, "accident" vehicles also broadcast, via cellular communication, 'federation formation' requests to the "community" vehicles in the vehicular network to start the selection of a subset of "community" vehicles as "verifier" vehicles to form a federation. Such a selection process can be based on the notion of a *reputation score* which may be determined based on a vehicle's driving and reporting records. Also the "verifier" vehicle with the highest reputation score is designated as the *lead* verifier via a distributed leader election algorithm [17], who is responsible for generating a new block for the accident. After that, new block generated by *lead* verifier vehicle will be sent to DMV and kept for the permanent records.

As depicted in Fig. 4, after the "accident" and "witness" vehicles generate and broadcast event data into the vehicular network, "verifier" vehicles take the responsibility of validating the received event data against the received hash digests, and confirm with the lead "verifier" vehicle (I in Fig. 4). The lead "verifier" vehicle executes the n-of-m multi-signature scheme [6] to achieve federation consensus when n out of m "verifier" vehicles confirm, and generates a new block of accident event. The lead "verifier" vehicle may then broadcast
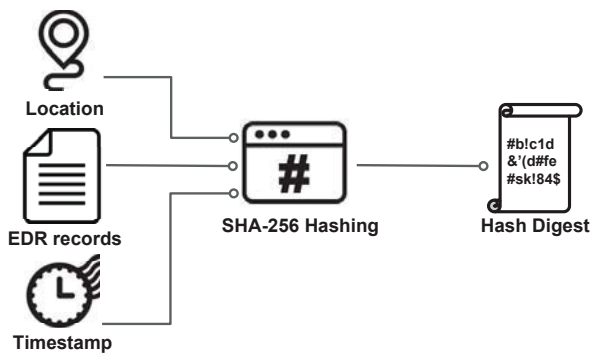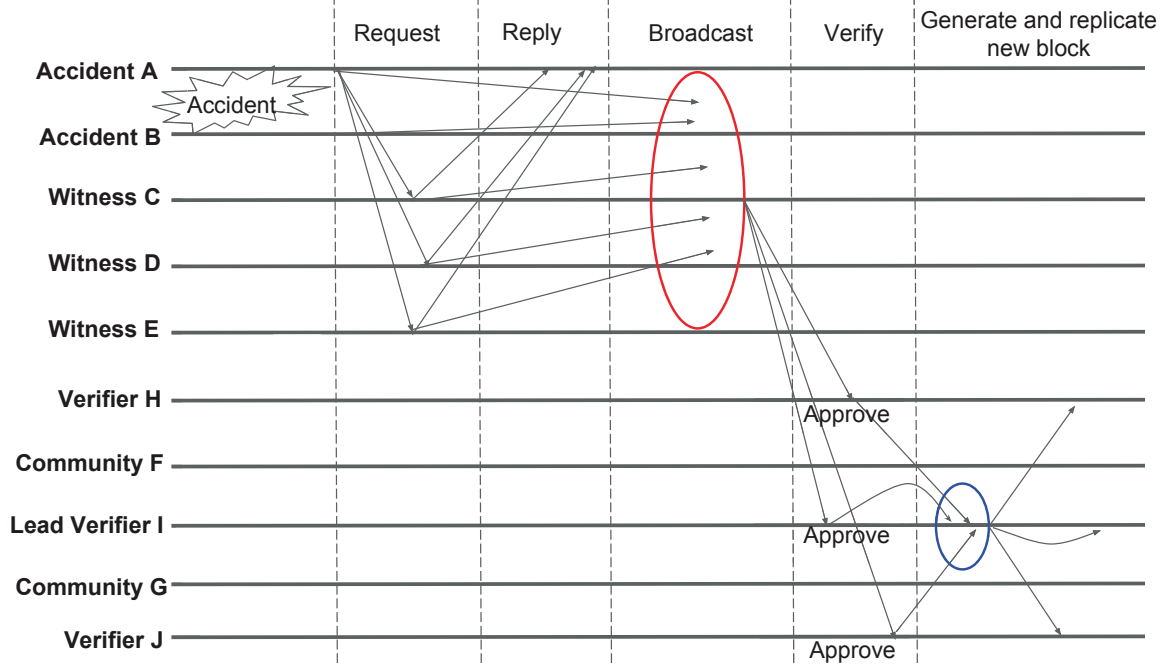
Fig. 4: Sequence diagram for accident, witness, community, and verifier vehicles.

the new block to all the "community" vehicles.

Compared to PoW, our solution does not incur any expensive computation associated with mining. Unlike PoA, which relies on the decision of one single authority, our solution demands confirmations from multiple authorities, if the n-of-m multi-signature [6] threshold is satisfied, verifier vehicles approve the event records and generate a new block. Every new block has its hash header and linked with the previous block's hash header. For instance, as depicted in Fig. 5, block i is verified by 3 out of 4 verifier vehicles from federation, while the block i+1 is 3 out of 5 case.
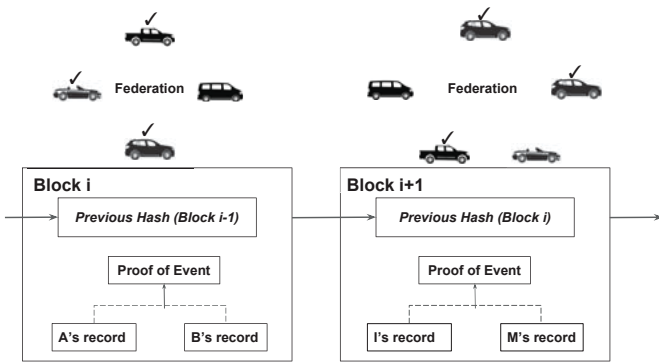

Fig. 5: Each block contains event data and hash value of previous block, and all confirmed by the verifier vehicles from the federation.

Note that "witness" vehicles (C, D, and E) function differently from "verifier" vehicles (H, I, and J). The job of the former is to generate event data, while that of the latter is to verify event data and generate a new block of accident event. "Witness" vehicles are close to the accident scene, whose EDR records may contain sensory readings related to the "accident" vehicles. In contrast, "verifier" vehicles are dynamically chosen which are located at random geographical locations within the same cell, even away from the accident scene, which makes them to be more neutral and independent. The decoupling of event data generations from their verification process mitigates the possibility of any malicious activities, such as tampering of event data and collusion among vehicles.

C. Incentives for participation and honesty

Bitcoin supplies new bitcoins to miners as an incentive for their efforts of PoW [4]. However, there is no obvious tangible award in the proposed Proof of Event. To motivate autonomous vehicles to participate as either "witness" or "verifier", different incentives (or rewards) must be defined. For instance, being a "witness" or "verifier" could raise a vehicle's credit score and to lower its insurance premium. Also, "accident" vehicles that engage reliably in Proof of Event and cooperate fully in accident forensics may receive a reduced liability.

D. Reviewing blocks for accident forensics

Later, people (police or judge) can review the accident event data stored in the blockchain from the DMV's record. If there is no discrepancy between event data generated by "accident" and "witness" vehicles, liability can be clearly determined. Otherwise, further investigation becomes necessary. For instance in Fig. 2, if "accident" vehicle B reported its own speed as 20 mph, while other "witness" vehicles (C, D, and E)

reported higher speeds for B, it is highly likely that "accident" vehicle B had a faulty speed sensor which caused it to speed and collided with vehicle A.

IV. EXTREME SCENARIOS

Our proposed mechanism works the best in accident scenarios where the density of the cell-based vehicular network covering the accident scene is above a certain threshold. In such cases, there are enough "witness" to generate event data vehicles and enough "verifier" vehicles to form a federation, reach a consensus, and create a new block. However, there exists the following three 'extreme' scenarios when such vehicular network is very sparse or no vehicle around the accident scene.

(1) Neither "witness" nor "verifier" vehicle exists for an accident. Since there is no "witness" or "verifier" vehicle, no new block could be generated. The EDRs of the "accident" vehicles will be the only evidence for forensic investigation.

(2) No "witness" vehicle exists for an accident. A new block will be created based on the event data generated only by the "accident" vehicles.

(3) No "verifier" vehicle exists for an accident. In this case, there exists (few) "witness" vehicles around the accident scene, but no "verifier" vehicle within the vehicular network. We argue that such scenarios will be extremely rare in practice.

V. SECURITY ANALYSIS

In this section, we analyze the robustness of the proposed event recording scheme with respect to potential attacks.

A. Spoofing event data

Existing EDRs installed on individual vehicles may be hacked and tampered to avoid liability. Our proposed Proof of Event scheme have both "accident" and "witness" vehicles generate event data which is to be validated by an independent group of "verifier" vehicles to avoid possibility of collusion. The recored event data in the block could be cross-examined later to determine cause and liability.

Further, the use of DSRC communications range limits which vehicles could serve as witness, which prevents vehicles away from the accident scene to generate any 'fake' event data.

B. Impersonation attack

As mentioned in Section III-A, legitimate autonomous vehicles are required to register with DMV. A malicious vehicle may impersonate a reputable vehicle so as to be selected as a "verifier" vehicle. Unless there are enough number of colluding vehicles selected within the same federation, the use of n-of-m multi-signature scheme to approve a new block is to lower the possibility of invalidate consensus.

C. Fake witness vehicle attack

As mentioned before, 'event generation' requests are broadcast via DSRC so that only the "witness" vehicles, which receive such request, can generate event data. However, a "witness" vehicle might resend the 'event generation' request to other vehicles which are beyond the range of DSRC communication, and 'invite' them to respond. Such act may launch the fake "witness" vehicle attack, where fake "witness" vehicles generate the fake event data in favor of "accident" vehicles. One possible solution to prevent such attacks is to set a small time window for "witness" vehicles to reply and broadcast event data.

VI. CONCLUSION

As autonomous systems are becoming essential parts of our life, proper systems must be put in place to "look after" them so as to determine liability from malfunctions, defects, or even malicious attacks. By drawing inspiration from blockchain, this paper presents a novel approach to providing a tamper-proof and verifiable event recording system for accident forensics of self-driving vehicles as they are the most influential autonomous systems in our society. In future, we plan to evaluate our proposed scheme using an experimental testbed.

REFERENCES

[1] S. K. Gehrig and F. J. Stein, "Dead reckoning and cartography using stereo vision for an autonomous car," in *Intelligent Robots and Systems, 1999. IROS'99. Proceedings. 1999 IEEE/RSJ International Conference on*, vol. 3. IEEE, 1999, pp. 1507–1512.

[2] Pew Research Center, http://www.pewinternet.org/2017/10/04/americans-attitudes-toward-driverless-vehicles/.

[3] J. Dilley, A. Poelstra, J. Wilkins, M. Piekarska, B. Gorlick, and M. Friedenbach, "Strong federations: An interoperable blockchain solution to centralized third party risks," *arXiv preprint arXiv:1612.05491*, 2016.

[4] F. Tschorsch and B. Scheuermann, "Bitcoin and beyond: A technical survey on decentralized digital currencies," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 2084–2123, 2016.

[5] I. Eyal, "The miner's dilemma," in *Security and Privacy (SP), 2015 IEEE Symposium on*. IEEE, 2015, pp. 89–103.

[6] https://en.bitcoin.it/wiki/Multisignature.

[7] "Event data recorder," 2017. [Online]. Available: https://en.wikipedia.org/wiki/Event_data_recorder

[8] R. W. van der Heijden, F. Engelmann, D. Mödinger, F. Schönig, and F. Kargl, "Blackchain: Scalability for resource-constrained accountable vehicle-to-x communication," *CoRR*, vol. abs/1710.08891, 2017.

[9] Y. Yuan and F.-Y. Wang, "Towards blockchain-based intelligent transportation systems," in *Intelligent Transportation Systems (ITSC), 2016 IEEE 19th International Conference on*. IEEE, 2016, pp. 2663–2668.

[10] B. Leiding, P. Memarmoshrefi, and D. Hogrefe, "Self-managed and blockchain-based vehicular ad-hoc networks," in *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct*. ACM, 2016, pp. 137–140.

[11] S. Rowan, M. Clear, M. Gerla, M. Huggard, and C. M. Goldrick, "Securing vehicle to vehicle communications using blockchain through visible light and acoustic side-channels," *arXiv preprint arXiv:1704.02553*, 2017.

[12] M. Jakobsson and A. Juels, "Proofs of work and bread pudding protocols," in *Proceedings of the IFIP TC6/TC11 Joint Working Conference on Secure Information Networks: Communications and Multimedia Security*, ser. CMS '99. Deventer, The Netherlands: Kluwer, B.V., 1999, pp. 258–272. [Online]. Available: http://dl.acm.org/citation.cfm?id=647800.757199

[13] P. Vasin, "Blackcoins proof-of-stake protocol v2," *URL: https://blackcoin. co/blackcoin-pos-protocol-v2-whitepaper. pdf*, 2014.

[14] S. De Angelis, L. Aniello, R. Baldoni, F. Lombardi, A. Margheri, and V. Sassone, "Pbft vs proof-of-authority: applying the cap theorem to permissioned blockchain," 2017.

[15] http://www.ubiquicoin.com/assets/proof.pdf.

[16] D. Jiang, V. Taliwal, A. Meier, W. Holfelder, and R. Herrtwich, "Design of 5.9 GHz DSRC-based vehicular safety communication," *IEEE Wireless Communications*, vol. 13, no. 5, 2006.

[17] H. Attiya and J. Welch, *Distributed computing: fundamentals, simulations, and advanced topics*. John Wiley & Sons, 2004.