Blockchain e Sistemas de Reputação em Redes Veiculares: Uma Revisão Sistemática

Claudio Piccolo Fernandes*
Universidade Federal de Santa Catarina - UFSC
Florianópolis, SC, Brasil
claudio.piccolo@estacio.br

Carlos Barros Montez
Universidade Federal de Santa Catarina - UFSC
Florianópolis, SC, Brasil
carlos.montez@ufsc.br

Daniel Domingos Adriano
Universidade do Vale do Itajaí - UNIVALI
São José, SC, Brasil
daniel.dadriano@gmail.com

Michelle Silva Wangham
Universidade do Vale do Itajaí - UNIVALI
São José, SC, Brasil
wangham@univali.br

RESUMO

Vehicular networks form an important pillar of current Intelligent Transportation Systems. Due to its specific characteristics, these networks have been using reputation systems and or trust models to ensure security and trustworthiness. In addition, blockchain is a valuable technology that enables the development of these systems, addressing privacy, anonymity, and access control issues. This work aims to describe the results of the systematic literature review on blockchain-based reputation systems. We compared some selected works and highlighted the adopted techniques and the main challenges.

KEYWORDS

blockchain, vehicular networks, reputation system

1 INTRODUÇÃO

Sistemas de Transportes Inteligentes (*Intelligent Transport Systems* - ITS) é um conceito genérico que designa tipos de aplicação que são integrados com tecnologias de comunicações, controle e processamento de informações do sistema de transporte [31]. Os ITS costumam ser formados por um conjunto de aplicações que fazem uso das tecnologias de informação e comunicação no campo de transporte, com o objetivo de obter benefícios econômicos, sociais e energéticos. Este tipo de sistema pode ser aplicado a qualquer meio de transporte e considera qualquer um dos agentes envolvidos: veículo, infraestrutura e usuário.

As redes veiculares ou VANETs (*Vehicular Ad hoc Network*), juntamente com os avanços tecnológicos incorporados aos veículos automotivos, formam a espinha dorsal dos ITS do futuro. Nestas redes, os veículos são considerados nós de comunicação que trocam mensagens entre veículos próximos e equipamentos fixos localizados às margens de estradas, ruas e avenidas [2]. As redes veiculares têm como objetivo prover conforto e melhorar as condições de tráfego urbano e rodoviário de forma segura e eficiente, garantindo a comunicação entre os diversos nós inseridos na rede, oferecendo as condições necessárias para que aplicações, com diferentes requisitos, sejam desenvolvidas [30]. Essas redes possuem desafios a serem superados devido a algumas características, como: **alta mobilidade**, **topologia dinâmica** e **desconexões frequentes**. Essas características decorrem dos nós da rede que podem se mover em diferentes velocidades e de forma imprevisível.

A arquitetura das redes veiculares define como os veículos se organizam e se comunicam. Os principais elementos que compõem a arquitetura são [20]: as **unidades de bordo** (*On-Board Unit - OBU*) embarcadas nos veículos, com capacidade de processamento, armazenamento e comunicação; e as **unidades de acostamento** (*Road Side Unit - RSU*) que atuam como pontos de acesso à Internet e **nós de retransmissão**. A comunicação nas redes veiculares pode ser de **veículo para veículo** (*Vehicle-to-Vehicle - V2V*), sem qualquer tipo de suporte de uma infraestrutura externa; **veículo para infraestrutura** (*Vehicle-to-Infrastructure - V2I*), permitindo evitar a falta de conectividade; e **de forma híbrida**, que possibilita comunicação (V2V e V2I) de longa distância [8].

A segurança em redes veiculares é um fator crítico [11], pois decisões tomadas com base em informações erradas ou manipuladas podem levar a diminuição da segurança no trânsito. Aplicações de segurança no trânsito, como disseminação de alertas, necessitam da cooperação e honestidade dos nós. Os clientes dessas redes precisam confiar na fonte de informação. Contudo, a disponibilidade de informações para prover a necessária confiança pode contradizer os requisitos de privacidade. Os requisitos de segurança mais importantes em redes veiculares dizem respeito à autenticação dos nós, à integridade, à confidencialidade dos dados, à privacidade e ao controle de acesso [24]. Para inibir a ação de nós maliciosos, destacam-se métodos que utilizam sistemas de reputação que privilegiam os nós com comportamentos corretos. Nesta abordagem, grupos de confiança baseados em comportamentos passados são criados e cooperam entre si com o intuito de combater nós maliciosos [10]. Nesse contexto, detectar nós maliciosos e minimizar seus ataques e as consequências de seus comportamentos tornaram-se problemas complexos. A tecnologia emergente de *blockchain* pode ser uma forma eficiente de lidar com esses desafios, devido às suas características de descentralização, anonimato e confiança.

O objetivo deste trabalho é, por meio de uma revisão sistemática da literatura (RSL), analisar os trabalhos que descrevem sistemas de reputação baseados na tecnologia de *blockchain*, para redes veiculares. Através dessa RSL, executada em Outubro de 2020, foi possível identificar, avaliar e interpretar os estudos primários mais relevantes disponíveis nesta área de pesquisa. Como resultado da análise, identificou-se as principais características, tendências e questões

*Both authors contributed equally to this research.

em aberto que apontam os desafios para o desenvolvimento e uso destes sistemas de reputação baseados em *blockchain*.

Este artigo está organizado da seguinte forma. Na Seção 2 são apresentados os conceitos chaves de *blockchain* e seu uso em VANETs. A Seção 3 apresenta o método usado na revisão sistemática da literatura e os resultados do protocolo de busca. A descrição dos trabalhos selecionados na RSL e uma análise comparativa destes são apresentados nas Seções 5 e 6, respectivamente. Por fim, a Seção 7 apresenta a conclusão e indicações de trabalhos futuros.

2 BLOCKCHAIN E SUA INTEGRAÇÃO EM REDES VEICULARES

Blockchain pode ser considerada uma tecnologia emergente que oferece suporte distribuído confiável e seguro para realização de transações entre participantes que não têm necessariamente confiança entre si e que estão dispersos em larga escala em uma rede *peer-to-peer* (P2P). É um paradigma computacional que surgiu com o protocolo *bitcoin* em 2008 [28]. Conforme [13], *blockchains* ou *distributed ledgers* são sistemas disruptivos, pois criam digitalmente uma entidade de confiança descentralizada, replicada e compartilhada entre os membros de uma rede, eliminando a necessidade de uma terceira parte de confiança.

Diferentemente da tradicional estrutura de rede centralizada, na *blockchain*, não há nós centrais fixos. Todos os membros da rede têm posições relativamente iguais e armazenam a mesma cópia, materializada na forma de um livro-razão (*ledger*) distribuído. A *Distributed ledger technology (DLT)* permite conter um registro robusto e auditável de todas as transações. Devido à alta segurança e confiabilidade, esta tem sido utilizada em muitos cenários de aplicação e é considerada como uma das principais técnicas para garantir a segurança dos dados e a privacidade [5]. Além da descentralização, os demais elementos chaves da tecnologia *blockchain* são [13, 21]:

- **Transparência:** todos os registros dos dados na *blockchain* são transparentes para cada nó, estando disponíveis para todos os usuários, podendo desta forma, serem verificados e auditados.
- **Disponibilidade e Integridade:** os conjuntos de dados e transações são replicados, de forma segura, em diferentes nós da rede.
- **Código Aberto:** a maioria dos sistemas são abertos, podendo seus registros serem verificados publicamente.
- **Imutabilidade e Irrefutabilidade:** uma *blockchain* consiste em uma cadeia de blocos consecutivamente conectados. Qualquer modificação no bloco anterior invalida todos os blocos consequentemente gerados; ou seja, uma vez registrados não podem ser refutados.
- **Privacidade e Anonimato:** O conceito de privacidade em *blockchain* consiste em manter o anonimato e a desvinculação de transações. As transações são feitas através de chaves públicas, as quais representam os nós, e a chave privada utilizada para assinar as transações na rede.

As tecnologias *blockchain* são categorizadas em três tipos [5]: **(i) pública, aberta ou não permissionadas**, na qual as transações são públicas, ou seja, todos os nós podem realizar transações e consultar o histórico de transações na rede; **(ii) de consórcio, federada ou permissionadas**, a qual é formada por grupos de corporações ou instituições que operam a rede de *blockchain*, dividem o investimento e estabelecem uma lista de pessoas que têm acesso ao sistema; e **(iii) privada**, que é uma *blockchain* permissionada especial operada por uma entidade.

Os sistemas *blockchain* não precisam de uma autoridade terceira confiável. Em vez disso, um conjunto de nós é responsável por verificar as transações na rede. Essa validação de confiabilidade, a consistência dos dados e transações, pode ser obtida por algoritmos de consenso. Há na literatura diversas metodologias de consenso que realizam o processo de validação da *blockchain* [5].

Mesclar a tecnologia de *blockchain* às redes veiculares é um desafio, e essa integração tem despertado um crescente interesse de pesquisadores e desenvolvedores [16]. A *blockchain* pode oferecer soluções práticas para muitos problemas das redes veiculares [15], especialmente aqueles relacionados à confiança para o compartilhamento e a disseminação de dados entre veículos. A ideia é de que os dados transmitidos pelos veículos conectados à *blockchain* sejam criptografados e assinados pelo verdadeiro remetente que contém uma chave pública exclusiva, garantindo a segurança dos dados transmitidos, bem como a sua confiança.

O funcionamento das redes veiculares e a disseminação eficiente dos dados são baseados na ideia de cooperação de veículos [25] e, estabelecer confiança entre seus nós, é essencial para garantir a segurança nas rodovias. Decisões tomadas com base em informações erradas ou manipuladas podem levar à diminuição da segurança no trânsito, pois mensagens alteradas podem provocar acidentes graves. Portanto, diferentes serviços de segurança devem ser considerados para, por exemplo, evitar que veículos possam ser rastreados. Além disso, informações a respeito de condutores devem permanecer inacessíveis para os nós não autorizados. Assim, a integração da tecnologia *blockchain* com as redes veiculares pode facilitar o estabelecimento de um sistema de transporte inteligente seguro, confiável e descentralizado.

3 REVISÃO SISTEMÁTICA DA LITERATURA

Uma revisão sistemática da literatura (RSL) é uma metodologia para a realização de uma revisão bibliográfica por meio de etapas bem definidas e estruturadas que proporciona confiabilidade e base teórica [7]. De acordo com [19], são necessários quatro passos para conduzir uma RSL: (a) identificação dos recursos (questão de pesquisa, palavras chaves e fontes); (b) seleção dos estudos; (c) extração dos dados; e (d) análise dos dados. O estabelecimento das questões de pesquisa é a parte mais importante de uma revisão sistemática. O processo de revisão visa encontrar e analisar os estudos primários que são capazes de responder às questões de pesquisa formuladas. Para identificar e selecionar estes estudos, um protocolo de busca precisa ser executado.

Segundo [26] a RSL, é um processo que permite coletar evidências relevantes sobre o tema em questão que se enquadram nos critérios de elegibilidade pré-especificados e ter uma resposta para as questões de pesquisa formuladas.

3.1 Trabalhos de RSL ou Surveys Relacionados

Com o objetivo de identificar trabalhos que descrevem revisões sistemáticas, que exploram a tecnologia *blockchain* no contexto

das redes veiculares, outro protocolo de busca foi executado. Os estudos secundários mais relevantes estão elencados na Tabela 1. Conforme pode ser constatado, as revisões sistemáticas encontradas não focam no uso sistemas de reputação integrando a tecnologia *blockchain* e redes veiculares. Foram também encontrados *surveys* [9, 25, 29, 34, 36], porém, estes não apresentam de fato uma investigação detalhada de sistemas de reputação utilizando a tecnologia *blockchain* em VANETs. Assim, estas observações evidenciam o diferencial e a relevância deste presente trabalho.

Tabela 1: Trabalhos de RSL Relacionados

Trab.	Foco	Proposta da Revisão Sistemática
[1]	Internet de veículos	Tipos de ataques, soluções implementadas para solucionar as ameaças e avaliação de desempenho.
[23]	VANETs	Análise da segurança de veículos autônomos com a utilização da tecnologia *blockchain*.
[14]	Veículos autônomos	Classificação, ameaça, tipos de ataques em veículos autônomos e os desafios do uso da *blockchain* para superar estes problemas.
[4]	Cidades inteligentes	O uso da *blockchain* para prover segurança em comunidades inteligentes (saúde, transporte, etc).
[3]	Sistemas de transporte	As principais aplicações baseadas em *blockchain* aplicadas ao setor de transporte para compartilhamento cooperativo e seguro de dados

3.2 Metodologia - Execução da RSL

A RSL foi realizada no mês de outubro de 2020 com o objetivo de responder à questão de pesquisa: **Quais modelos de confiança e/ou sistemas de reputação utilizam a tecnologia de *blockchain* em redes veiculares**? Definiram-se ainda as seguintes questões secundárias: (1) Quais problemas as soluções visam resolver?; (2) Qual a categoria e local da *blockchain*; e (3) Quais problemas não foram tratados. Definiram-se que apenas estes estudos na língua inglesa seriam considerados de acordo com a *string* de busca: *("vanet"OR "vehicular ad hoc network") AND ("blockchain") AND ("trust"OR "trustworthiness"OR "reputation").*

O protocolo de busca foi executado, considerando as cinco fontes mais relevantes da área, sendo estas (organizadas em ordem alfabética): *ACM Digital Library*[1], *IEEE Xplore*[2], *ScienceDirect*[3], *Scopus*[4] *e Springer Link*[5].

Os critérios predefinidos de inclusão e exclusão da literatura para a realização deste trabalho de revisão sistemática são apresentados na Tabela 2. Dos artigos analisados, aqueles como publicações repetidas, *surveys* e trabalhos nos quais títulos e resumos apresentem informações conflitantes, ou seja, o título remete a um assunto e o resumo a outro foram excluídos.

A Figura 1 apresenta o fluxograma das atividades executadas na RSL. Para obter a primeira lista de possíveis trabalhos, executou-se a *string* de busca nas fontes citadas, considerando título e resumo e, em caso de dúvidas na seleção, foi lida sua introdução. Visando

[1]http://dl.acm.org/
[2]http://ieeexplore.ieee.org/
[3]http://sciencedirect.com/
[4]http://scopus.com/
[5]http://link.springer.com/

Tabela 2: RSL - Critérios de inclusão e exclusão

Critério	Decisão
Quando as palavras-chave predefinidas na string de busca existem no título ou resumo do artigo	Inclusão
O artigo foi escrito no idioma inglês	Inclusão
Estudos que apresentam evidências de sistemas de reputação utilizando tecnologia de Blockchain	Inclusão
Artigos duplicados na pesquisa	Exclusão
Artigos que não são acessíveis ou surveys	Exclusão
Artigos nos quais títulos e resumos apresentem informações conflitantes	Exclusão

um refinamento da seleção dos estudos, todos os artigos, previamente selecionados, foram lidos na íntegra para confirmar que estes realmente respondem à questão de pesquisa.

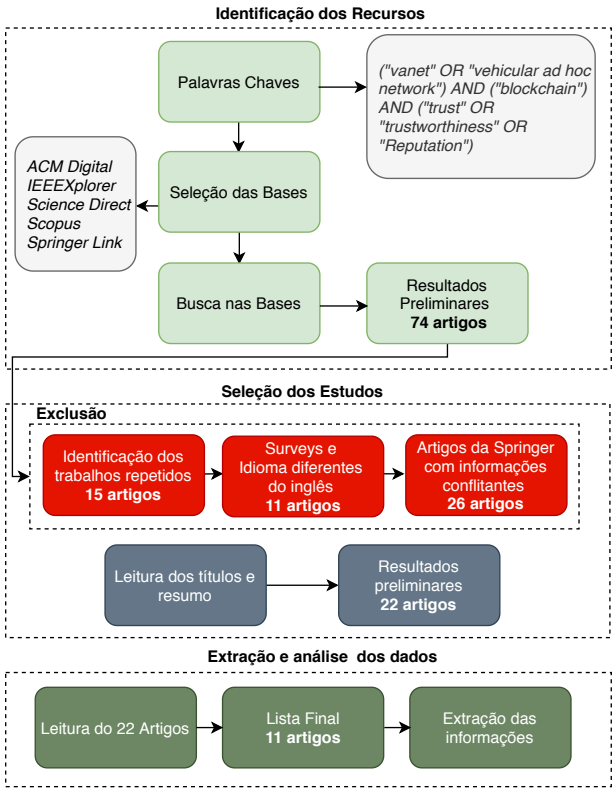


Figura 1: Fluxograma da Revisão Sistemática

A Tabela 3 apresenta o total de publicações retornadas de cada base. No estágio inicial, um total de 74 (setenta e quatro) trabalhos foram encontrados. Dos trabalhos encontrados, 52 foram removidos por serem repetidos, ou *surveys*, ou estarem em idioma diferente do inglês, ou devido a uma limitação da ferramenta de busca da *Springer Link* que realiza a consulta no texto completo, resultando em um número elevado de trabalhos que não são adequados ao contexto buscado. Assim, o número de trabalhos foi reduzido para 22 artigos os quais foram realizados a leitura completa. No final,

restaram 11 publicações que preencheram todos os critérios de inclusão usados neste trabalho de Revisão Sistemática.

Tabela 3: Resultados da execução do protocolo de busca

	ACM Digital	IEEE	Science Direct	Scopus	Springer	Total
Resultado da string	3	13	2	30	26	**74**
Trabalhos repetidos	0	4	1	10	0	**15**
Trabalhos analisados	3	9	2	8	0	**22**
Trabalhos selecionados	1	6	2	2	0	**11**

Devido à diferença que há entre as ferramentas de busca de cada base selecionada, a *string* de busca foi adequada para cada execução. Nas bases da *ACM, IEEE e Science Direct*, esta foi pesquisada no título e resumo. Na *Scopus*, a busca foi realizada por título, resumo e palavras chaves, enquanto na *Springer Link*, foi efetuada a busca no texto completo.

4 DESCRIÇÃO TRABALHOS SELECIONADOS

Esta Seção apresenta os trabalhos correlatos selecionados na RSL os quais utilizam modelos de confiança e/ou sistemas de reputação em redes veiculares com a utilização da tecnologia de *blockchain*. A Tabela 4 apresenta os trabalhos com a sua respectiva avaliação utilizando o sistema Qualis-Periódicos de classificação.

Tabela 4: Trabalhos Selecionados

Trab.	Ano	Journal / Conferência	Qualis[6]	Rank Scimagojr[7]
[6]	2020	Journal	A2	Q1
[12]	2019	Journal	A1	Q1
[16]	2019	Journal	A1	Q1
[17]	2018	Journal	A1	Q1
[18]	2018	Conferência	A2	-
[22]	2018	Journal	A1	Q1
[27]	2019	Journal	A3	Q4
[33]	2020	Journal	-	Q1
[35]	2019	Journal	-	Q4
[37]	2019	Journal	A1	Q1
[38]	2017	Conferência	A2	-

Os autores em [38] apresentam um sistema descentralizado de reputação que utiliza *blockchain* para garantir a credibilidade das mensagens em redes veiculares. Com base nas classificações, os veículos podem calcular o valor da reputação do remetente da mensagem, usando seu conhecimento local e, em seguida, avaliar a credibilidade da mensagem. O valor da reputação é calculado usando as classificações de mensagens anteriores transmitidas por um determinado veículo. Um nó central temporário (minerador) fornece as classificações e essas são validadas pela maioria dos veículos, para então serem armazenadas na *blockchain*. Os mineradores são selecionados entre os veículos e seu papel é criar um bloco com todas as classificações e enviá-lo aos demais nós da rede. Essa eleição é realizada por meio de um mecanismo de consenso, sendo que o veículo com maior capacidade de detecção e precisão de seus sensores, certificada pela autoridade confiável, será eleito o minerador da rede. Em seguida, os veículos vizinhos, formam um consenso para essas classificações dos veículos e, se aceito, o bloco é adicionado na *blockchain*. Experimentos foram realizados na plataforma *MatLab* a fim de validar o sistema proposto. O desempenho da proposta baseada em *blockchain* foi comparado a um sistema no qual as classificações são verificadas pelos veículos sem a utilização de um consenso. Os resultados apresentados demonstram que a utilização da tecnologia *blockchain* para detectar veículos maliciosos e verificar a credibilidade das mensagens é melhor, quando comparada com a experiência individual de cada veículo. No entanto, o custo adicional do sistema com a utilização da *blockchain* (tempo para alcançar o consenso), bem como os métodos de preservação da privacidade, não são apresentados.

O sistema de reputação baseado em *blockchain*, denominado BARS *(blockchain-based anonymous reputation system)* [22], visa impedir a distribuição de mensagens falsas e, ao mesmo tempo, preservar a privacidade da identidade dos veículos. Mediante um modelo de confiança, os autores pretendem melhorar a confiabilidade das mensagens, com base nas interações históricas diretas e nas opiniões indiretas, para formar a reputação do remetente. Um algoritmo de gerenciamento de reputação é utilizado para avaliar a confiabilidade de cada veículo de acordo com a autenticidade das mensagens transmitidas, bem como as opiniões de outros veículos. As mensagens são registradas na *blockchain* com o objetivo de ser uma prova permanente para a LEA *(law enforcement authority)* avaliar o escore de reputação de cada veículo. Também foi empregado um mecanismo de autenticação. Este mecanismo faz uso de uma autoridade de certificação (CA) a qual é utilizada para a emissão e revogação de certificados desvinculando desta maneira a chave pública e a identidade real de um veículo. Todas as ações da CA são registradas na *blockchain* de forma transparente, sem revelar informações confidenciais sobre veículos, de modo que a chave pública possa ser usada como um pseudônimo autenticado. Como mecanismo de consenso foi utilizado a prova de trabalho. Assume-se que o processo de mineração dos dados é realizado pelos próprios veículos. Para avalidação do BARS, foram realizadas simulações com diferentes densidades de veículos com o objetivo de avaliar a segurança, o algoritmo de reputação e a avaliação do desempenho. No entanto, uma de suas limitações é o alto poder computacional ocasionado pelo mecanismo de consenso PoW.

Em [18], um sistema de gerenciamento de confiança distribuída para redes veiculares, denominado DTCMV *(distributed trust management scheme)* visa avaliar a mensagem disseminada com base no comportamento do veículo. O sistema DTCMV avalia o comportamento dos veículos, enquanto a credibilidade das mensagens é avaliada pelo sistema TCMV *(Trust Clustering Mechanism for VANET)*. O comportamento dos veículos leva em consideração os parâmetros de direção, velocidade e aceleração dos veículos que se encontram próximos do evento relatado. Já a credibilidade das mensagens é definida pelo CH *(cluster head)* com o uso da reputação dos veículos, sendo as RSUs responsáveis pela formação dos *clusters* e também os mineradores da rede da *blockchain*. Cada RSU é responsável por uma determinada área geográfica e por controlar os veículos pertencentes a essa área. Cada *clusters* de veículos possui um CH, eleito pela RSU. O critério para a eleição é a escolha do veículo que obteve mais interação com a RSU. Este CH é responsável,

[6]Qualis-Periódicos de classificação - Ano 2019
[7]https://www.scimagojr.com/

além da comunicação com as RSU, pela comunicação com os membros do *cluster* e com os outros CH na rede. Após a RSU analisar o comportamento do veículo por um período pré-definido e receber a credibilidade da mensagem do CH, ela toma uma decisão utilizando lógica *fuzzy* para verificar se o evento é correto ou incorreto. Em seguida, ocorre a atualização do escore da reputação do veículo e este é enviado aos CHs que os armazenam localmente. Então é criado um novo bloco e, tão logo seja validado, é armazenado na *blockchain*. Não houve implementação e simulação do sistema proposto para avaliar o seu desempenho. O trabalho não especifica qual o padrão adotado para a comunicação V2V V2I. A preservação da privacidade dos dados no sistema proposto não foi explorada.

Em [17], os autores apresentam um sistema de reputação para compartilhamento de dados em VANETs, cujo objetivo é a escolha de uma fonte de dados mais confiável, visando melhorar a credibilidade dos dados. O sistema faz uso da computação em névoa e emprega tecnologias de *blockchain* de consórcio e contratos inteligentes para garantir a eficiência. As RSUs são os nós pré-selecionados para formarem a *blockchain* de consórcio, sendo estas as responsáveis e autorizadas por realizar o processo de consenso. São utilizados dois contratos inteligentes implantados em uma *blockchain* veicular. O DSSC é o contrato inteligente de armazenamento de dados e o ISSC é o contrato inteligente de compartilhamento de informações para o armazenamento e compartilhamento seguro dos dados entre os veículos. Os veículos que trafegam na rodovia geram e enviam seus dados para a RSU mais próxima (via DSSC). Estes dados são armazenados em uma *blockchain* na RSU. Enquanto isso, para o compartilhamento dos dados, os veículos primeiro pesquisam os dados por meio do ISSC com o objetivo de descobrirem as informações de seu interesse. Em seguida, estes comunicam-se com os provedores de dados para solicitar autorização de acesso. Os veículos escolhem o melhor provedor de dados de acordo com os valores de reputação. Para obter uma reputação local mais precisa e confiável, o sistema faz uso de uma técnica de múltiplos pesos, que considera algumas métricas com base no histórico de interações entre os veículos. A reputação é formada, usando a opinião local de cada veículo. Em seguida, as diferentes opiniões de diferentes recomendadores (veículos vizinhos) são integradas em uma única opinião (opinião final). Por fim, para escolher uma fonte da dados mais confiável, o veículo compara os valores finais de reputação dos provedores de dados. Simulações foram realizadas com cem táxis na cidade de São Francisco, por um período de trinta dias. Os resultados evidenciaram que o sistema proposto atinge eficiência e segurança para o compartilhamento dos dados, uma vez que veículos com comportamentos anormais tiveram seu valor de reputação reduzidos. No entanto, o processo de autenticação e segurança no compartilhamento de dados não teve um bom desempenho na avaliação em tempo real.

Em [16], um sistema de votação baseado em reputação visa garantir a seleção segura de mineradores na rede com o uso da tecnologia *blockchain*. O sistema proposto avalia a reputação dos candidatos a mineradores, utilizando interações históricas e opiniões recomendadas de outros veículos. Uma RSU para ser candidata a mineradora, envia sua identidade para a CA que verifica sua autenticidade, calculando a reputação média de acordo com as opiniões armazenadas dos veículos. Somente se a reputação média dessa RSU for maior que um limite de confiança, esta RSU poderá se tornar um candidato a minerador. Os candidatos a mineradores com os mais altos níveis de reputação são selecionados para fazerem parte de um grupo, sendo divididos em mineradores ativos e mineradores em espera (*standby*). Os mineradores ativos são responsáveis pela geração dos blocos na rede *blockchain*, enquanto os mineradores em espera são responsáveis por verificar e auditar os blocos para evitar conluio interno entre mineradores ativos. Para calcular a reputação das RSUs, os veículos fazem uso de interações históricas (direta) juntamente com opiniões recomendadas de outros veículos (armazenadas na *blockchain* veicular), obtendo desta maneira a opinião final. Todas as opiniões de reputação dos veículos são registradas na *blockchain* para o cálculo da reputação. Para a atualização da reputação, após cada rodada do processo de consenso, os veículos fazem *download* das opiniões existentes sobre as RSUs na *blockchain*, denominadas opiniões recomendadas. Se os dados estiverem corretos, os veículos atualizam suas opiniões sobre a reputação desses mineradores e carregam as novas opiniões assinadas digitalmente por meio de RSUs próximas. Para fins de consenso, é utilizado o mecanismo DPoS. Simulações foram realizadas em um cenário real com 536 táxis com o objetivo de avaliar a segurança na seleção de mineradores baseado em reputação. Os resultados demonstraram a eficiência na taxa de detecção de candidatos maliciosos a mineradores, uma vez que, devido ao cálculo de reputação preciso, as reputações destes veículos maliciosos foram diminuindo a partir das opiniões dos outros veículos e interações históricas locais. Os autores não evidenciam neste trabalho qual a forma de incentivo utilizado para os mineradores participarem do processo de consenso.

Em [27], o uso de uma mini *blockchain*, formada apenas por uma cadeia de cabeçalhos de blocos é proposta com o objetivo de detectar veículos maliciosos na rede veicular. No sistema proposto, veículos com comportamentos maliciosos não são capazes de obter a confiança de outros veículos e fazer parte da rede veicular. Para atingir esses requisitos, os veículos vizinhos verificam a autenticidade do veículo e analisam também se os dados recebidos são autênticos. Cada veículo possui uma *blockchain* local. Ao se comunicar com outro veículo, ambos precisam chegar a um consenso sobre a *blockchain*, que é a cadeia de blocos mais longa das duas versões. Somente quando uma troca bem-sucedida ocorre, a *blockchain* é alterada e, portanto, seu comprimento se torna mais longo. Um veículo malicioso não poderá obter uma cópia da *blockchain* existente pois, devido à falta de trocas bem-sucedidas, o tamanho de sua cadeia de blocos na *blockchain* local será menor que o limiar aceitável na rede. Para validar o sistema proposto, o autor considera apenas um único veículo malicioso tentando ingressar na rede para obter uma cópia da *blockchain* de veículos vizinhos. Entretanto, detalhes de simulações não são descritos no trabalho e problemas de ataques de conluio não são tratados.

Em [35] os autores propõem um mecanismo para tornar as redes veiculares mais segura, as informações mais confiáveis e também identificar nós maliciosos, adaptando os conceitos da tecnologia de *blockchain* para as necessidades das redes veiculares. O mecanismo faz uso de duas *blockchains*: uma armazenada no próprio veículo que é usada para armazenar informações relacionadas a eventos que ocorrem (ex. acidentes) em uma determinada região e outra na nuvem que armazena os dados de maneira global (país). Cada veículo é equipado com uma unidade de *blockchain* personalizada (BCU). As informações sobre eventos de alerta são propagadas para os veículos vizinhos que as armazenam na sua BCU e, posteriormente,

enviam para a RSU mais próxima. A RSU recebe as mensagens sobre um determinado alerta dos veículos e aguarda uma janela de tempo (30 minutos). Depois que a janela de tempo encerra, a RSU analisa todas as transações recebidas sobre o mesmo evento. Se os dados enviados pelo veículos combinam entre si, a RSU assume que o evento realmente aconteceu e incrementa o nível de confiança dos veículos (reputação) e os armazena na *blockchain* na nuvem. Os veículos recebem a *blockchain* atualizada sempre que ingressarem na rede veicular ou quando mudam de região.A avaliação do mecanismo proposto não é descrita. A sincronização das *blockchains* e a divisão e integração das regiões também não são abordadas.

Os autores [12] descrevem um modelo baseado em confiança para suprimir atividades maliciosas na rede veicular. Os autores integram a tecnologia de *blockchain* com redes definidas por *software* (SDN) e computação em névoa para garantir um bom desempenho do modelo de confiança proposto. Para reduzir os custos computacionais e atrasos, uma *blockchain* de consórcio foi usada no compartilhamento de dados na rede veicular e, as RSUs são responsáveis pela mineração dos dados com o uso do mecanismo de consenso PBFT. A fim de verificar a confiabilidade dos alertas recebidos, a opinião de outros veículos é levada em consideração. Os veículos são agrupados em *clusters*, os quais possuem um líder, que recebe a opinião dos outros veículos sobre a confirmação ou não do alerta e, em seguida, o valida. Então, o líder envia o alerta para a RSU para que o consenso seja realizado e ocorra a atualização do modelo de confiança na *blockchain*. Para avaliar o desempenho do sistema, simulações foram realizadas utilizando MATLAB e NS-3, em uma rodovia de 8 km, bidirecional e com quatro faixas. Foram analisadas apenas as taxas de entrega de pacotes e o atraso de sua transmissão. Os autores não descrevem como a escolha do líder no *cluster* é realizada.

Em [33], os autores descrevem uma proposta para comunicação V2V segura, integrando um sistema de confiança que usa *blockchain*, com o objetivo de reduzir os problemas de disseminação de mensagens em redes veiculares. O sistema faz uso de uma *blockchain* pública para determinar a confiabilidade dos nós juntamente com a confiabilidade da mensagem. Diferentemente das *blockchains* tradicionais, nas quais os blocos são transmitidos globalmente, o sistema proposto utiliza o conceito de *blockchain* dentro de uma área geográfica específica, denominada de região de interesse (RoI). Esta área é dividida em países e, segundo os autores, esta divisão ameniza os problemas de escalabilidade na rede. O sistema considera dois tipos de mensagens a serem disseminadas: mensagens de sinalização, para informar localização dos vizinhos, na qual um certificado de localização é gerado como prova digital e mensagens de eventos, para sinalizar eventos críticos na estrada. Apenas as mensagens de eventos são armazenadas na *blockchain*. O veículo, ao entrar na RoI (cobertura da RSU), faz o *download* e atualização da *blockchain*, a qual armazena todo o histórico do nível de confiança dos veículos, juntamente com o histórico das mensagens de eventos. Os veículos verificam cada mensagem de evento na *blockchain* com base no nível de confiança do remetente, local do evento, direção, velocidade, registro de data/hora, etc. Em seguida, caso seu nível de confiança seja maior que um limiar definido pelo sistema, o veículo armazena localmente a mensagem de evento e, em seguida, a transmite na rede. Caso contrário, a mensagem será descartada. Veículos com altos níveis de confiança na rede são aqueles que podem participar do processo de mineração, ou seja, são responsáveis pela criação dos blocos. Os autores apenas discutem a escalabilidade da *blockchain* nas redes veiculares e a sobrecarga de armazenamento, mas não descrevem nenhum avaliação experimental.

Os autores em [6] apresentam uma proposta que explora as garantias e segurança da *blockchain* e a forma escalável e flexível da computação em névoa, para resolver os principais problemas de gerenciamento de confiança distribuído. Os autores não consideram as questões específicas das redes veiculares, mas sim uma abordagem mais genérica. No modelo, os veículos ou dispositivos IoT não possuem uma *blockchain*. Essas ficam armazenadas em nós de borda, como as RSUs, e contêm os valores de confiança, com base em suas interações, dos membros da rede. O grau de confiança dos nós não são disseminados periodicamente na rede. Os próprios nós solicitam aos nós de borda quando necessário. Caso o grau de confiança solicitado não exista ou seja antigo na *blockchain*, um consenso é realizado entre os participantes e essa é atualizada com base nos resultados obtidos. Os autores realizaram análises de desempenho e tolerância a falhas para demostrar a capacidade de resposta e robustez da proposta. Os resultados não demonstram claramente a viabilidade do tempo de resposta demandado para a realização do consenso na *blockchain*. Outro ponto em aberto diz respeito à privacidade dos nós, que não é tratada no trabalho, apenas sugere-se que pseudônimos podem ser usados.

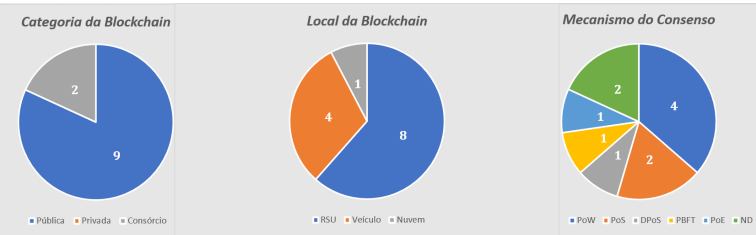
O sistema de [37] propõe uma estrutura de validação de eventos de tráfego (BTEV) baseada em *blockchain* que introduz, ao contrário dos mecanismos de consenso tradicionais, um novo mecanismo de consenso denominado prova de evento (PoE), o qual visa garantir a confiabilidade dos eventos e confirmar a validade de suas ocorrências. Inicialmente, as RSUs coletam informações sobre um (possível) evento na estrada e iniciam um processo de consenso entre os veículos sobre a autenticidade deste evento. Se houver um consenso entre os veículos, a mensagem é então considerada confiável e os veículos na área de cobertura da RSU serão notificados sobre o alerta e as informações do evento serão armazenadas na *blockchain* local (RSU). A RSU também notifica as outras RSUs na mesma zona e, uma vez que todas as RSUs concordem com a correção do evento, após revisar as evidências anexadas na mensagem, o evento então será adicionado a *blockchain* global a qual inclui todos os eventos na área e são compartilhadas publicamente, podendo ser acessado pelos veículos para verificação de eventos.Para demonstrar os benefícios deste sistema, os autores compararam o mecanismo PoE com algoritmos de consenso existentes (PoA, PoW) e também mediram a sua segurança do em termos de taxa de sucesso de eventos falsos no simulador de rede NS-3. No entanto, devido a utilização de uma *blockchain* global, no qual um grande número de eventos são submetidos a *blockchain* diariamente, pois pode estar cobrindo todos os eventos em uma área geográfica muito grande, o seu tamanho poderá ser enorme exigindo um alto custo computacional.

5 ANÁLISE TRABALHOS

A Tabela 5 apresenta uma síntese comparativa dos trabalhos selecionados na RSL, voltados ao uso da tecnologia de *blockchain* em redes veiculares.

Tabela 5: Análise dos trabalhos selecionados

Autor	Proposta	Principal Característica	Categoria Blockchain	Local Blockchain	Mecanismo de Consenso	Problemas em Aberto
[38]	Verificar credibilidade da mensagem; e Veículos maliciosos.	Avalia a credibilidade dos dados e dos nós	Pública	Veículo	PoS	Custo Computacional Privacidade veículos
[22]	Disseminação de mensagens falsas; e Privacidade dos nós.	Uso de pseudônimos para garantir a privacidade	Pública	RSU	PoW	Implementação da *blockchain*
[18]	Segurança da comunicação entre os veículos	Gerenciamento de Confiança distribuída	Pública	RSU	PoW	Preservação da privacidade dos dados.
[17]	Compartilhamento de dados e privacidade.	Uso de contratos inteligentes	Consórcio	RSU	PoS	Desempenho em tempo real
[16]	Seleção segura de mineradores na rede.	Uso de sistema de votação	Pública	RSU	DPoS	Forma de incentivo aos mineradores
[27]	Detectar e isolar nós maliciosos na rede.	Uso de um mini *blockchain*	Pública	Veículo	ND	Simulação.
[35]	Detectar e isolar nós maliciosos na rede.	Duas *blockchains*: veículo e nuvem	Pública	Veículo Nuvem	PoW	Ataques de conluio Simulação. Sincronismo das *blockchains*
[12]	Detectar e isolar nós maliciosos na rede.	Integração de 3 tecnologias SDN, FOG e *Blockchain*	Consórcio	RSU	PBFT	Eleição do líder Métricas desempenho
[33]	Verificar credibilidade das mensagens e nós.	*Blockchain* dentro de uma área geográfica específica	Pública	Veículo RSU	PoW	Detalhes da simulação. Latência
[6]	Gerenciamento de confiança distribuído.	Abordagem genérica IoT e VANETs	Pública	RSU	ND	Tempo de resposta. Privacidade
[37]	Validação de eventos.	Novo mecanismo de consenso proposto	Pública	RSU	PoE	Alto custo computacional da *blockchain* Global



A maioria dos artigos analisados tem suas soluções validadas em ambientes reais ou de simulação. As exceções são os trabalhos de [32] e [18] que apenas descrevem suas propostas. Predominam trabalhos cujo o problema alvo é evitar ou minimizar possíveis ataques de nós maliciosos em redes veiculares que para a sua construção fazem uso da credibilidade da mensagem ou do nó.

Algumas questões ficaram em aberto nos trabalhos. O problema voltado à preservação da privacidade não é tratado nos trabalhos de [6, 18, 38]. Também em [38], a latência e o custo computacional do processo de consenso na *blockchain*, não foram bem discutidos. Em [22], não foi descrito como ocorreu a implementação da *blockchain*. Uma questão não evidenciada em [16] é a forma de incentivo utilizada para que os mineradores tenham interesse em participarem do processo de consenso. As simulações não demonstram claramente seus resultados em [27] deixando em aberto a real validação do sistema. Já em [35], não há uma discussão acerca da sincronização das *blockchains*. Não sendo essas descritas, assim como a forma da divisão e integração das regiões para compor a *blockchain*. [12] não evidenciam como é realizada a escolha do líder no *cluster* e as métricas de desempenho são pouco exploradas. Em [33], simulações não foram realizadas para comprovar a eficácia da confiabilidade das mensagens e a latência pelo armazenamento dessas na *blockchain*. Nos estudos de [6], os resultados não demonstram claramente a viabilidade do tempo de resposta demandado para a realização do consenso na *blockchain*.

Nos trabalhos analisados, com exceção de [17] e [12], as transações são efetuadas em *blockchain* públicas sendo visíveis a todos na rede veicular e totalmente descentralizada. Todos os trabalhos analisados focam na forma de tratamento do problema de nós maliciosos que propagam mensagens falsas na rede. Apenas [16] difere, uma vez que trata de RSUs maliciosas que podem modificar ou descartar dados durante o processo de mineração. Outro ponto importante a destacar é como as soluções apresentadas lidam com a alta complexidade computacional dos algoritmos de consenso. Em sua maioria, os trabalhos [38], [22], [17], [35], [12] e [6] embora com simulações, não deixam claro se o uso de recursos empregados é satisfatório para se alcançar o processo de consenso na rede veicular.

6 CONCLUSÃO

O uso da tecnologia *blockchain* em redes veiculares vem ganhando muita atenção nos últimos anos. Seus principais cenários de uso estão em sistemas de gerenciamento de confiança, visando trocas de mensagens seguras e na sua aplicabilidade para resolver problemas de privacidade, anonimato e controle de acesso. Os trabalhos

relacionados que descrevem revisões sistemáticas no que tange as redes veiculares não apresentam de fato uma solução de sistemas de confiança/reputação utilizando *blockchain*, o que evidencia a importância do estudo sistemático realizado neste artigo.

Baseado em um protocolo de revisão sistemática, realizou-se uma pesquisa com o objetivo de identificar e analisar estudos recentes os quais utilizam a tecnologia *blockchain* em modelos de confiança e sistemas de reputação para redes veiculares. Como resultado, foi possível identificar os diferentes problemas analisados para o tratamento de nós maliciosos na rede. As características adotadas para minimizar as consequências dos ataques e seus comportamentos maliciosos são os que diferem os escopos dos trabalhos.

Após a análise dos problemas em aberto dos onze trabalhos selecionados, conclui-se que desafios ainda permanecem, como questões relacionadas à preservação da privacidade e à minimização do uso de recursos quando da utilização da *blockchain* e dos protocolos de consenso. Como trabalhos futuros, sugere-se a execução de simulações que permitam avaliar o comprometimento do desempenho da utilização da tecnologia *blockchain* nos trabalhos estudados. Outra sugestão é a concepção de controles mais elaborados para o gerenciamento de confiança/reputação que complementem as lacunas identificadas nos trabalhos selecionados.

REFERÊNCIAS

[1] Manar Abu Talib, Sohail Abbas, Qassim Nasir, and Mohamad Fouzi Mowakeh. 2018. Systematic literature review on Internet-of-Vehicles communication security. *International Journal of Distributed Sensor Networks* 14, 12 (2018), 1550147718815054.

[2] Saif Al-Sultan, Moath M Al-Doori, Ali H Al-Bayatti, and Hussien Zedan. 2014. A comprehensive survey on vehicular ad hoc network. *Journal of network and computer applications* 37 (2014), 380–392.

[3] Vittorio Astarita, Vincenzo Pasquale Giofrè, Giovanni Mirabelli, and Vittorio Solina. 2020. A review of blockchain-based systems in transportation. *Information* 11, 1 (2020), 21.

[4] Bharat Bhushan, Aditya Khamparia, K Martin Sagayam, Sudhir Kumar Sharma, Mohd Abdul Ahad, and Narayan C Debnath. 2020. Blockchain for Smart Cities: A review of Architectures, Integration Trends and Future Research Directions. *Sustainable Cities and Society* (2020), 102360.

[5] Christian Cachin and Marko Vukolić. 2017. Blockchain consensus protocols in the wild. *arXiv preprint arXiv:1707.01873* (2017).

[6] Marcello Cinque, Christian Esposito, Stefano Russo, and Oscar Tamburis. 2020. Blockchain-empowered decentralised trust management for the Internet of Vehicles security. *Computers & Electrical Engineering* 86 (2020), 106722.

[7] Heather L Colquhoun, Danielle Levac, Kelly K O'Brien, Sharon Straus, Andrea C Tricco, Laure Perrier, Monika Kastner, and David Moher. 2014. Scoping reviews: time for clarity in definition, methods, and reporting. *Journal of clinical epidemiology* 67, 12 (2014), 1291–1294.

[8] Felipe Cunha, Leandro Villas, Azzedine Boukerche, Guilherme Maia, Aline Viana, Raquel AF Mini, and Antonio AF Loureiro. 2016. Data communication in VANETs: Protocols, applications and challenges. *Ad Hoc Networks* 44 (2016), 90–103.

[9] Hong-Ning Dai, Zibin Zheng, and Yan Zhang. 2019. Blockchain for Internet of Things: A survey. *IEEE Internet of Things Journal* 6, 5 (2019), 8076–8094.

[10] Richard Dennis and Gareth Owenson. 2016. Rep on the roll: a peer to peer reputation system based on a rolling blockchain. *International Journal for Digital Society* 7, 1 (2016), 1123–1134.

[11] Xia Feng, Chun-yan Li, De-xin Chen, and Jin Tang. 2017. A method for defensing against multi-source Sybil attacks in VANET. *Peer-to-Peer Networking and Applications* 10, 2 (2017), 305–314.

[12] Jianbin Gao, Kwame Opuni-Boachie Obour Agyekum, Emmanuel Boateng Sifah, Kingsley Nketia Acheampong, Qi Xia, Xiaojiang Du, Mohsen Guizani, and Hu Xia. 2019. A blockchain-SDN-enabled Internet of vehicles environment for fog computing and 5G networks. *IEEE Internet of Things Journal* 7, 5 (2019), 4278–4291.

[13] Fabíola Greve Greve, Leobino Sampaio Sampaio, Jauberth Abijaude Abijaude, Antonio Coutinho Coutinho, Ítalo Valcy Valcy, and Sílvio Queiroz Queiroz. 2018. Blockchain e a Revolução do Consenso sob Demanda. *Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC)-Minicursos* (2018).

[14] Rajesh Gupta, Sudeep Tanwar, Neeraj Kumar, and Sudhanshu Tyagi. 2020. Blockchain-based security attack resilience schemes for autonomous vehicles in industry 4.0: A systematic review. *Computers & Electrical Engineering* 86 (2020), 106717.

[15] Razi Iqbal, Talal Ashraf Butt, Muhammad Afzaal, and Khaled Salah. 2019. Trust management in social Internet of vehicles: Factors, challenges, blockchain, and fog solutions. *International Journal of Distributed Sensor Networks* 15, 1 (2019), 1550147719825820.

[16] Jiawen Kang, Zehui Xiong, Dusit Niyato, Dongdong Ye, Dong In Kim, and Jun Zhao. 2019. Towards Secure Blockchain-enabled Internet of Vehicles: Optimizing Consensus Management Using Reputation and Contract Theory. *IEEE Transactions on Vehicular Technology* (2019).

[17] Jiawen Kang, Rong Yu, Xumin Huang, Maoqiang Wu, Sabita Maharjan, Shengli Xie, and Yan Zhang. 2018. Blockchain for secure and efficient data sharing in vehicular edge computing and networks. *IEEE Internet of Things Journal* (2018).

[18] Amira Kchaou, Ryma Abassi, and Sihem Guemara. 2018. Toward a distributed trust management scheme for vanet. In *Proceedings of the 13th International Conference on Availability, Reliability and Security*. ACM, 53.

[19] Staffs Keele et al. 2007. *Guidelines for performing systematic literature reviews in software engineering*. Technical Report. Technical report, Ver. 2.3 EBSE Technical Report. EBSE.

[20] Eun-Kyu Lee, Mario Gerla, Giovanni Pau, Uichin Lee, and Jae-Han Lim. 2016. Internet of Vehicles: From intelligent grid to autonomous cars and vehicular fogs. *International Journal of Distributed Sensor Networks* 12, 9 (2016), 1550147716665500.

[21] Iuon-Chang Lin and Tzu-Chun Liao. 2017. A survey of blockchain security issues and challenges. *IJ Network Security* 19, 5 (2017), 653–659.

[22] Zhaojun Lu, Wenchao Liu, Qian Wang, Gang Qu, and Zhenglin Liu. 2018. A privacy-preserving trust model based on blockchain for vanets. *IEEE Access* 6 (2018), 45655–45664.

[23] Subhrajit Majumder, Akshay Mathur, and Ahmad Y Javaid. 2019. A Study on Recent Applications of Blockchain Technology in Vehicular Adhoc Network (VANET). In *National Cyber Summit*. Springer, 293–308.

[24] P Manickam, K Shankar, Eswaran Perumal, M Ilayaraja, and K Sathesh Kumar. 2019. Secure data transmission through reliable vehicles in VANET using optimal lightweight cryptography. In *Cybersecurity and secure information systems*. Springer, 193–204.

[25] Leo Mendiboure, Mohamed Aymen Chalouf, and Francine Krief. 2020. Survey on blockchain-based applications in internet of vehicles. *Computers & Electrical Engineering* 84 (2020), 106646.

[26] Wondimagegn Mengist, Teshome Soromessa, and Gudina Legese. 2020. Method for conducting systematic literature review and meta-analysis for environmental science research. *MethodsX* 7 (2020), 100777.

[27] Ahmad Mostafa. 2019. VANET Blockchain: A General Framework for Detecting Malicious Vehicles. *J. Commun* 14, 5 (2019), 356–362.

[28] Satoshi Nakamoto. 2009. *Bitcoin: A peer-to-peer electronic cash system*. Technical Report. Manubot.

[29] Hirofumi Onishi. 2018. A survey: Engineering challenges to implement vanet security. In *2018 IEEE International Conference on Vehicular Electronics and Safety (ICVES)*. IEEE, 1–6.

[30] Benedikt Ostermaier, Florian Dotzer, and Markus Strassberger. 2007. Enhancing the security of local dangerwarnings in vanets-a simulative analysis of voting schemes. In *The Second International Conference on Availability, Reliability and Security (ARES'07)*. IEEE, 422–431.

[31] Asier Perallos, Unai Hernandez-Jayo, Enrique Onieva, and Ignacio Julio García Zuazola. 2015. *Intelligent Transport Systems: Technologies and Applications*. John Wiley & Sons.

[32] Rakesh Shrestha, Rojeena Bajracharya, and Seung Yeob Nam. 2018. Blockchain-based Message Dissemination in VANET. In *2018 IEEE 3rd International Conference on Computing, Communication and Security (ICCCS)*. IEEE, 161–166.

[33] Rakesh Shrestha, Rojeena Bajracharya, Anish P Shrestha, and Seung Yeob Nam. 2020. A new type of blockchain for secure message exchange in VANET. *Digital Communications and Networks* 6, 2 (2020), 177–186.

[34] Fatima Tariq, Maria Anwar, Abdul Rehman Janjua, Muhammad Haseeb Khan, Asad Ullah Khan, and Nadeem Javaid. 2020. Blockchain in WSNs, VANets, IoTs and Healthcare: A Survey. In *Workshops of the International Conference on Advanced Information Networking and Applications*. Springer, 267–279.

[35] Ravi Tomar et al. 2019. Maintaining Trust in VANETs Using Blockchain. *Ada User Journal* 40, 4 (2019).

[36] Chao Wang, Xiaoman Cheng, Jitong Li, Yunhua He, and Ke Xiao. 2020. A Survey: Applications of Blockchains in the Internet of Vehicles. In *International Conference on Wireless Algorithms, Systems, and Applications*. Springer, 457–468.

[37] Yao-Tsung Yang, Li-Der Chou, Chia-Wei Tseng, Fan-Hsun Tseng, and Chien-Chang Liu. 2019. Blockchain-based traffic event validation and trust verification for VANETs. *IEEE Access* 7 (2019), 30868–30877.

[38] Zhe Yang, Kan Zheng, Kan Yang, and Victor CM Leung. 2017. A blockchain-based reputation system for data credibility assessment in vehicular networks. In *2017 IEEE 28th annual international symposium on personal, indoor, and mobile radio communications (PIMRC)*. IEEE, 1–5.