Blockchain para Segurança em Redes Veiculares Uma Mini Revisão da Literatura

Everton V. Cardoso
Programa de Pós-graduação em Telecomunicações
Instituto Nacional de Telecomunicações
Santa Rita do Sapucaí, Brazil
everton.vilhena@mtel.inatel.br

Eylen J. M. Ontiveros
Programa de Pós-graduação em Telecomunicações
Instituto Nacional de Telecomunicações
Santa Rita do Sapucaí, Brazil
eylen.ontiveros@mtel.inatel.br

***Abstract*—Advances in transportation are making wireless communication increasingly important. This communication can be between vehicles (V2V) or between vehicles and infrastructure (V2I). Several projects rely on these technologies to optimize the transportation of the future, improving the comfort and services offered to users. However, the presence of terminals in vehicles or infrastructure centers creates possible points of fragility, establishing potential points of vulnerability in transportation systems that can be used for malicious and malicious actions, compromising their functionality. In the context of connected vehicles, data security between vehicles and infrastructure is directly related to privacy and personal security. The possibility of data degradation, modification, or addition can lead to inappropriate or even dangerous responses from vehicles and networks. Given the need to ensure data security, blockchain has emerged as a promising solution for connected vehicles. It is a transparent and secure technology that stores, validates, and transmits information without the need for a central authority. Blockchain is being analyzed to ensure secure communication between vehicles, transportation infrastructure, and centralized or distributed information platforms. However, it is not yet fully effective against new forms of attack that go beyond the physical barrier of wireless communication;**

***Abstract*—Os avanços no transporte estão tornando a comunicação sem fio cada vez mais essencial. Essa comunicação pode ocorrer entre veículos (V2V) ou entre veículos e infraestrutura (V2I). Diversos projetos dependem dessas tecnologias para otimizar o transporte do futuro, aprimorando o conforto e os serviços oferecidos aos usuários. No entanto, a presença de terminais em veículos ou em centros de infraestrutura criam possíveis pontos de fragilidade, estabelecendo potenciais pontos de vulnerabilidade nos sistemas de transporte, que podem ser utilizados para ações mal-intencionadas e maliciosas, comprometendo sua funcionalidade. No contexto dos veículos conectados, a segurança dos dados entre veículos e infraestrutura está diretamente relacionada à privacidade e à segurança pessoal. A possibilidade de degradação, modificação ou adição de dados pode resultar em respostas inadequadas ou até perigosas por parte dos veículos e das redes. Diante da necessidade de garantir a segurança dos dados, o blockchain surge como uma solução promissora para os veículos conectados. Trata-se de uma tecnologia transparente e segura que armazena, valida e transmite informações sem a necessidade de um órgão central de controle. O blockchain está sendo analisado para assegurar comunicações seguras entre veículos, infraestrutura de transporte e plataformas de informação centralizadas ou distribuídas. Contudo, ainda não é totalmente eficaz contra novas formas de ataques que ultrapassam a barreira física da comunicação sem fio.; (vou traduzir depois)**

INTRODUÇÃO

Contexto

O número de veículos em circulação no mundo tem crescido de forma exponencial, atualmente, há cerca de 2 bilhões de veículos motorizados em uso, dos quais cerca de 1,3 bilhões são de carros, impulsionado pela urbanização, crescimento populacional e aumento do poder aquisitivo em mercados emergentes (OICA, 2023; Statista, 2023). Esse crescimento, embora signifique avanços econômicos e sociais, traz desafios significativos, como congestionamentos, aumento de acidentes de trânsito, emissão de gases e a necessidade de sistemas de transporte mais eficientes. Com base nisso, sistemas tecnológicos inovadores têm se tornado imprescindíveis para enfrentar tais problemas, sendo os Sistemas de Transporte Inteligentes (ITS) e as Redes Veiculares (VANETs) ferramentas fundamentais.

Veículos modernos combinam hardware e software avançados, incluindo o uso de GPS, comunicação sem fio, entretenimento, recursos visuais e alarmes automáticos, exigindo alto processamento de dados e conectividade avançada. Esse crescente volume de dados e e a demanda pela integração entre veículos e infraestruturas, impulsionam o avanço das redes veiculares.

A rápida evolução das redes veiculares, especialmente as redes veiculares ad hoc (VANETs), tem transformado significativamente o panorama dos sistemas de transporte inteligentes (ITS). Essas redes possibilitam a comunicação veículo-a-veículo (V2V), veículo-infraestrutura (V2I) e veículo-para-tudo (V2X), permitindo a troca de informações em tempo real. Essa conectividade aprimorada desempenha um papel crucial na gestão de tráfego, segurança rodoviária e melhoria da experiência do usuário. No entanto, a crescente interconexão e dependência de sistemas digitais também expõem as redes veiculares a uma ampla gama de ameaças à segurança e privacidade, como acesso não autorizado, manipulação de dados e ataques de negação de serviço distribuído (DDoS) (Hussain et al., 2021; Zhang et al., 2022).

Nesse contexto, o uso blockchain tem crescido, como uma solução promissora para abordar esses desafios, graças às suas propriedades inerentes de descentralização, transparência

e imutabilidade. Originalmente desenvolvida para sustentar criptomoedas, como o Bitcoin, a tecnologia blockchain tem demonstrado potencial em diversos domínios, incluindo saúde, gerenciamento da cadeia de suprimentos e Internet das Coisas (IoT), devido à sua capacidade de garantir transações seguras e resistentes a adulterações (Nakamoto, 2008; Zheng et al., 2018). No cenário das redes veiculares, o blockchain surge como uma ferramenta viável para reforçar a segurança, possibilitando a gestão segura de identidades, protegendo a integridade dos dados e promovendo a colaboração confiável entre nós da rede (Shrestha et al., 2020).

A integração do blockchain às redes veiculares, apesar de promissora, apresenta desafios únicos. Destacando-se, o alto custo computacional associado aos mecanismos de consenso, problemas de escalabilidade em redes de grande porte e os compromissos necessários entre privacidade e transparência (Dorri et al., 2017). Para enfrentar essas limitações, estudos recentes propuseram inovações, como protocolos de consenso leves e modelos híbridos de blockchain, adaptados às particularidades das redes veiculares (Wang et al., 2022; Liu et al., 2023). Entretanto, apesar do progresso, a compreensão abrangente do estado atual de pesquisa e das implementações práticas, ainda é essencial para avanços significativos nessa área.

Este artigo oferece uma revisão sistemática sobre as aplicações do blockchain na segurança de redes veiculares. Ele sintetiza os avanços recentes, categoriza as soluções existentes com base em suas áreas de foco e identifica direções futuras de pesquisa e desafios tecnológicos.

Motivação

A tecnologia 5G integrada promete revolucionar a experiência dos usuários nos transportes, especialmente em veículos automotivos, permitindo operações mais eficientes e seguras. Espera-se que a indústria automotiva enfrente grandes transformações, exigindo soluções inovadoras, robustas, estáveis e confiáveis.

Um dos principais benefícios do 5G é a baixa latência, que será essencial para o desenvolvimento inicial de serviços como gestão de tráfego, segurança viária e, eventualmente, condução autônoma. Essa rede permitirá diferentes tipos de comunicação: veículos entre veículos (V2V), veículos entre veículos e infraestrutura rodoviária (V2I), até entre veículos e pedestres ou outros usuários vulneráveis da estrada (V2P).

Essa conectividade é viabilizada pela tecnologia de rádio 5G, que oferece duas interfaces de comunicação principais: a interface Uu ou LTE-Uu, utilizada para comunicações V2N, e a interface PC5, que suporta comunicações diretas V2V, V2P e V2I. Com essas capacidades, os veículos poderão "enxergar" além de sua linha de visão, perceber melhor o ambiente ao redor, antecipar riscos e contribuir para um fluxo de tráfego mais fluído.

As oportunidades oferecidas pelo 5G-V2X devem levar, em breve, ao surgimento de novos serviços que aproveitem plenamente as capacidades desta tecnologia. Entre os avanços esperados estão: latência ultrabaixa, alta confiabilidade de comunicação, ampla largura de banda e suporte a um grande número de veículos autônomos e conectados (ACVs). Além disso, o 5G oferece conectividade confiável mesmo em condições de alta mobilidade.

Essa evolução só será viável com a adoção massiva do 5G em sua versão autônoma (SA), viabilizada por tecnologias como o network slicing (fatiamento de rede) e Redes Definidas por Software (SDN). Essas ferramentas permitirão uma gestão eficiente e personalizada das redes, possibilitando a integração total de veículos conectados no ecossistema de transporte inteligente.

Justificativa

Diante deste cenário, a presente pesquisa justifica-se pela necessidade de explorar soluções que adaptem e aprimorem a tecnologia blockchain para o contexto das redes veiculares. A proposta busca abordar as limitações atuais, desenvolvendo mecanismos de segurança mais eficientes e escaláveis, capazes de atender às exigências de baixa latência e alta mobilidade inerentes ao ambiente veicular. Além de garantir maior confiabilidade e proteção contra ameaças cibernéticas, os resultados esperados podem contribuir significativamente para o avanço das tecnologias de transporte inteligente e conectividade segura.

Objetivo

Analisar trabalhos com propostas de sistema seguro para comunicação em redes veiculares, utilizando blockchain para autenticação e integridade de dados em comunicações V2V (veículo a veículo) e V2I (veículo a infraestrutura), enfrentando os desafios de latência e escalabilidade.

FUNDAMENTAÇÃO TEÓRICA / BACKGROUND

Redes Veiculares (VANETs)

As redes veiculares ad hoc (VANETs - Vehicular Ad-Hoc Networks) representam uma subclasse das redes móveis ad hoc (MANETs), projetadas para suportar a comunicação dinâmica e em tempo real entre veículos e entre veículos e a infraestrutura. Essas redes desempenham um papel central nos sistemas de transporte inteligentes (ITS - Intelligent Transportation Systems), permitindo a troca de informações críticas, como alertas de segurança, condições de tráfego e suporte à navegação em tempo real. (Hussain et al., 2021).

A arquitetura das VANETs é composta por três camadas principais:

1) **Comunicação veículo-a-veículo (V2V)**:Interações diretas entre veículos permitem o compartilhamento de dados sobre emergências, condições de estrada e ações de outros veículos. Essa tecnologia é essencial para

evitar colisões e melhorar a segurança (Sichitiu e Kihl, 2008).

2) **Comunicação veículo-infraestrutura (V2I)**: Conexões entre veículos e unidades de infraestrutura, como semáforos inteligentes e unidades de beira de estrada (RSUs - Road-Side Units), que facilitam a coleta de dados para monitoramento de tráfego e suporte à navegação.
3) **Comunicação veículo-para-tudo (V2X)**: Engloba interações com dispositivos IoT, pedestres e outros sistemas, promovendo uma visão holística do ecossistema urbano e ampliando o alcance das VANETs para um ambiente integrado e interconectado (Zhang et al., 2022).

As VANETs são compostas por nós móveis, ou seja, veículos equipados com dispositivos de comunicação, e por pontos fixos de infraestrutura, como unidades de beira de estrada (RSUs - Road-Side Units). Esses nós operam em um ambiente altamente dinâmico, caracterizado pela alta mobilidade dos veículos e pela rápida mudança na topologia da rede (Kumar et al., 2020).

Essas redes são suportadas por tecnologias de comunicação de curto alcance dedicadas, como o Dedicated Short-Range Communication (DSRC) e o 5G-V2X, que oferecem baixa latência e alta confiabilidade. O DSRC utiliza a banda de 5,9 GHz para suportar comunicações críticas, enquanto o 5G-V2X fornece capacidades aprimoradas para lidar com cenários de alta densidade e alta mobilidade (Campolo et al., 2017).

No entanto, as VANETs enfrentam desafios significativos relacionados à segurança e privacidade. Entre os principais problemas estão os ataques de falsificação de identidade (Sybil attacks), onde um nó malicioso simula múltiplas identidades para manipular a rede; ataques de eavesdropping, nos quais dados sensíveis são interceptados; e ataques de negação de serviço (DoS), que podem paralisar a rede (Ali et al., 2020). Além disso, o ambiente distribuído e a falta de uma autoridade central complicam ainda mais a implementação de mecanismos de segurança robustos.

Internet of Vehicles

A Internet of Vehicles (IoV) representa uma evolução das VANETs, integrando veículos a um ecossistema mais amplo de comunicação baseado na Internet. A IoV conecta veículos não apenas entre si (V2V) e com a infraestrutura (V2I), mas também com dispositivos inteligentes, sensores e sistemas externos, como serviços na nuvem e cidades inteligentes, formando uma rede interconectada para troca e processamento de informações em tempo real (Gerla et al., 2014).

Essa arquitetura possibilita uma ampla gama de aplicações, como monitoramento avançado de tráfego, navegação colaborativa, manutenção preditiva de veículos e serviços personalizados baseados em dados (Yang et al., 2019).

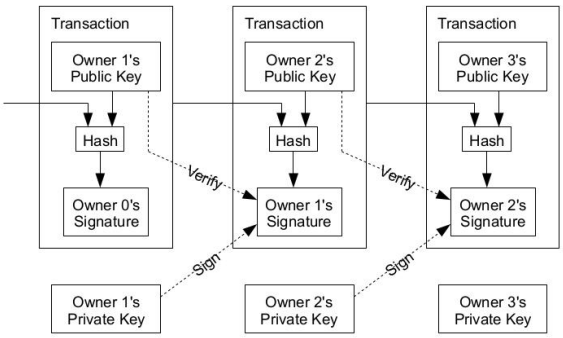
Uma característica central da IoV é a sua dependência de tecnologias emergentes, como inteligência artificial (IA), computação em nuvem e computação de borda, para processar grandes volumes de dados de maneira eficiente e em tempo real (Kumar et al., 2020). Além disso, a IoV requer protocolos de comunicação robustos para lidar com a diversidade de dispositivos e garantir a interoperabilidade entre diferentes sistemas.

Apesar de seu grande potencial, a IoV enfrenta desafios relacionados à segurança e privacidade, pois a vasta interconectividade aumenta os vetores de ataque, expondo informações sensíveis, como localização e comportamento do motorista (Zhou et al., 2020). Por isso, o blockchain tem sido explorado como uma solução viável para fortalecer a confiabilidade e a integridade dos dados na IoV, permitindo que os veículos e dispositivos interajam de maneira segura e confiável (Shrestha et al., 2020).

Blockchain Technology

A blockchain, inicialmente proposto por Nakamoto (2008) como o mecanismo subjacente ao Bitcoin, é uma tecnologia de registro distribuído (Distributed Ledger Technology - DLT) que permite o armazenamento de informações de forma descentralizada, imutável e transparente. Conforme Figura 1, é composto por uma sequência de blocos, cada um contendo um conjunto de transações. Esses blocos são vinculados de forma criptográfica, de modo que qualquer tentativa de modificação em um bloco invalida a cadeia subsequente. Cada bloco é validado por meio de um mecanismo de consenso, como Proof of Work (PoW) ou Proof of Stake (PoS), que garante a integridade e a confiança no sistema (Zheng et al., 2018).

Figure 1. Arquitetura de compartilhamento de dados que preserva a privacidade e é controlada pelo usuário.



Fonte: Extraído de Nakamoto (2008)

: Entre as características fundamentais do blockchain estão:

- **Descentralização**: Não há necessidade de uma autoridade central, pois o consenso é alcançado por meio de mecanismos específicos, como Proof of Work (PoW), Proof of Stake (PoS) ou variantes híbridas (Dorri et al., 2017).
- **Imutabilidade**: Todas as transações são registradas e podem ser auditadas por qualquer participante da rede, promovendo confiança.
- **Transparência e Rastreamento**: Originalmente desenvolvida para sustentar a criptomoeda Bitcoin, a tecnologia blockchain rapidamente encontrou aplicações em áreas

como saúde, cadeia de suprimentos, Internet das Coisas (IoT) e redes veiculares (Wang et al., 2022).

No contexto das redes veiculares, o blockchain tem sido explorado como uma solução para desafios de segurança e privacidade. A tecnologia pode, por exemplo, fornecer um sistema de identidade digital descentralizado, onde cada veículo possui uma identidade única e verificável, reduzindo o risco de ataques (Sybil attacks). Além disso, o blockchain pode garantir a integridade dos dados trocados entre os veículos, evitando a manipulação de mensagens críticas, como alertas de segurança (Shrestha et al., 2020).

Blockchain e Redes Veiculares

A aplicação do blockchain em redes veiculares apresenta um alinhamento natural com os requisitos de segurança e confiabilidade dessas redes. Em uma VANET, o blockchain pode atuar como um registro descentralizado para armazenar e verificar transações de dados, eliminando a necessidade de uma autoridade central de confiança. Isso é particularmente importante em cenários onde a colaboração entre veículos de diferentes fabricantes ou sistemas é necessária (Dorri et al., 2017).

Além disso, o uso de mecanismos de consenso adaptados ao ambiente veicular, como Proof of Authority (PoA) ou Proof of Reputation (PoR), pode mitigar os desafios de escalabilidade e eficiência energética associados aos métodos tradicionais de blockchain. Esses mecanismos são projetados para atender às características específicas das VANETs, como alta mobilidade e baixa latência, sem comprometer a segurança ou a confiabilidade do sistema (Wang et al., 2022; Liu et al., 2023).

Apesar do potencial significativo, a integração do blockchain com redes veiculares enfrenta desafios técnicos e operacionais. Entre os principais desafios estão o alto custo computacional dos algoritmos de consenso, as limitações de largura de banda e a necessidade de padronização para garantir a interoperabilidade entre diferentes sistemas (Zhang et al., 2022). A superação desses obstáculos é fundamental para que as vantagens do blockchain sejam plenamente exploradas nesse domínio.

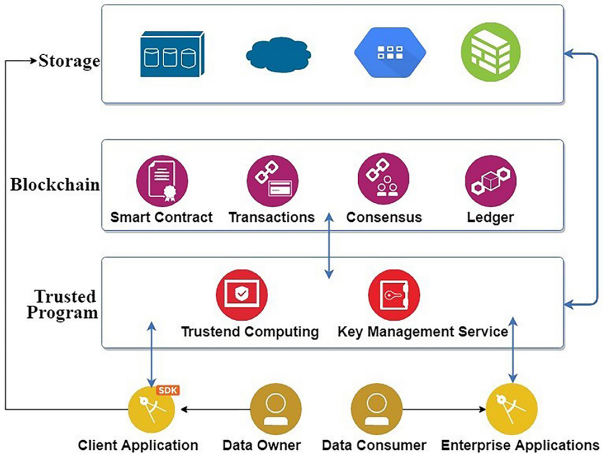
Trabalhos Relacionados

A pesquisa sobre a aplicação do blockchain para segurança em redes veiculares (VANETs) e na Internet of Vehicles (IoV) tem crescido exponencialmente nos últimos anos, refletindo o potencial da tecnologia em resolver problemas críticos relacionados à segurança, privacidade e eficiência. Nesta seção, os principais avanços são analisados detalhadamente, organizados em categorias que abrangem autenticação, integridade de dados, consenso, contratos inteligentes e escalabilidade. Cada subseção apresenta uma análise crítica das soluções propostas, destacando suas contribuições, limitações e direções futuras.

Autenticação e Gerenciamento de Identidade

A autenticação é um aspecto essencial em redes veiculares para garantir que somente veículos e dispositivos autorizados possam se comunicar, protegendo a rede contra ataques de falsificação de identidade (*Sybil attacks*). Shrestha et al. (2020) introduziram um sistema baseado em blockchain que utiliza identidades digitais descentralizadas para autenticação. O modelo elimina a necessidade de uma autoridade central confiável, utilizando contratos inteligentes para verificar as credenciais de veículos. Além disso, o sistema é projetado para oferecer atualizações dinâmicas de identidade, reduzindo os riscos associados ao uso prolongado de chaves criptográficas fixas. No entanto, o trabalho destaca que o aumento da densidade da rede pode comprometer o desempenho devido ao aumento da complexidade computacional.

Figure 2. Arquitetura de compartilhamento de dados que preserva a privacidade e é controlada pelo usuário.



Fonte: Extraído de Shrestha et al. (2020)

: Huang et al. (2019) propôs uma abordagem híbrida que combina blockchain com redes de confiança (*trust networks*). Nesse sistema, cada veículo acumula uma reputação baseada em seu histórico de interações, e a autenticidade das mensagens é validada utilizando essa reputação. Embora eficaz contra ataques Sybil, o sistema enfrenta dificuldades em lidar com redes altamente dinâmicas, onde os veículos frequentemente entram e saem da rede, tornando o cálculo da reputação mais complexo.

Integridade de Dados e Privacidade

A integridade dos dados é fundamental para evitar manipulações em mensagens trocadas entre veículos e a infraestrutura. Liu et al. (2023) apresentaram uma arquitetura híbrida de blockchain que combina blockchains públicos e privados para atender simultaneamente aos requisitos de transparência e privacidade. O modelo utiliza computação de borda para processar transações localmente, minimizando a latência e reduzindo o congestionamento da rede principal. Além disso, dados sensíveis, como informações de localização, são armazenados em blockchains privados, enquanto informações menos sensíveis permanecem públicas. Contudo, o aumento do custo computacional para gerenciar múltiplos blockchains ainda representa uma limitação para ambientes de grande escala.

Xu et al. (2020) exploraram o uso de provas de conhecimento zero (*Zero-Knowledge Proofs*) em redes veiculares para proteger informações sensíveis enquanto garantem a verificação de integridade. Essa abordagem é particularmente relevante em cenários onde a privacidade é essencial, como em veículos autônomos. Embora a solução ofereça um alto nível de segurança, sua complexidade e dependência de recursos computacionais significativos podem limitar sua aplicação em dispositivos com capacidade restrita.

Mecanismos de Consenso

Os mecanismos de consenso são a espinha dorsal do blockchain, garantindo a integridade e a confiabilidade das transações. Wang et al. (2022) introduziram o *Proof of Reputation* (PoR) como um mecanismo de consenso adaptado para redes veiculares. Nesse modelo, a reputação dos veículos é usada como um critério para validar transações, reduzindo a necessidade de cálculos intensivos, como ocorre no *Proof of Work* (PoW). Essa abordagem é eficiente em termos energéticos e adequada para cenários de alta mobilidade, mas levanta preocupações quanto à manipulação da reputação por nós maliciosos.

Por outro lado, Dorri et al. (2017) propuseram um esquema baseado em *Proof of Authority* (PoA), onde um subconjunto de nós confiáveis é responsável pela validação das transações. Essa abordagem reduz significativamente o custo computacional, tornando-a ideal para veículos com recursos limitados. No entanto, a centralização implícita na escolha dos validadores pode introduzir pontos de vulnerabilidade e limitar a resiliência do sistema.

Contratos Inteligentes em Redes Veiculares

Contratos inteligentes são amplamente utilizados para automatizar processos em redes veiculares, aumentando a eficiência operacional. Zhang et al. (2022) propuseram o uso de contratos inteligentes para coordenar *platoons* de veículos, onde grupos de veículos viajam juntos para reduzir o consumo de combustível e aumentar a segurança. Os contratos inteligentes permitem que os veículos negociem parâmetros como velocidade e distância entre os membros do *platoon* de forma autônoma. Embora os resultados sejam promissores, a execução de contratos inteligentes em plataformas públicas, como Ethereum, apresenta desafios de latência, especialmente em cenários de tráfego intenso.

Chen et al. (2021) exploraram contratos inteligentes no contexto de redes elétricas inteligentes, permitindo que veículos elétricos negociem automaticamente o carregamento e descarregamento de energia. O sistema assegura que as transações sejam transparentes e rastreáveis, mas sua dependência de infraestrutura de comunicação avançada, como 5G, limita sua aplicação em regiões com conectividade limitada.

Escalabilidade e Eficiência

A escalabilidade é um dos maiores desafios para a adoção do blockchain em redes veiculares. Kumar et al. (2020) revisaram abordagens inovadoras para melhorar a eficiência, incluindo *sharding*, onde a rede é dividida em subgrupos menores para processar transações paralelamente, e compressão de blocos, que reduz os requisitos de armazenamento. Embora essas técnicas ofereçam melhorias significativas, a interoperabilidade entre diferentes blockchains e subgrupos ainda é um problema técnico considerável.

Tecnologias emergentes, como redes definidas por software (SDN) e computação em nuvem, têm sido integradas a redes veiculares para melhorar a escalabilidade e a eficiência. Essas abordagens prometem reduzir a sobrecarga computacional em dispositivos móveis, mas levantam novas preocupações relacionadas à latência e à segurança das conexões com servidores externos.

A literatura existente evidencia que o blockchain é uma ferramenta poderosa para resolver desafios relacionados à segurança, privacidade e eficiência em redes veiculares e na IoV. No entanto, lacunas permanecem em termos de escalabilidade, interoperabilidade e custos computacionais. Além disso, a maioria dos estudos existentes foca em experimentos simulados, destacando a necessidade de validação prática em ambientes reais.

Aplicações do Blockchain em Redes Veiculares

O uso do blockchain em redes veiculares abrange uma ampla gama de cenários de aplicação, que abordam problemas como autenticação, integridade de dados, privacidade até eficiência operacional e proteção contra ataques cibernéticos. A Figura 3 apresenta uma visão geral das aplicações descritas na literatura, enquanto a Figura 4 organiza esses cenários de forma temática, destacando os principais casos de uso.

Gestão de Identidade e Autenticação

A autenticação é um pilar essencial para garantir a segurança nas redes veiculares. Em ambientes altamente dinâmicos, ataques como falsificação de identidade (*Sybil attacks*) podem comprometer a integridade da rede.

O blockchain fornece uma solução descentralizada ao criar identidades digitais únicas e imutáveis para veículos e dispositivos conectados. Por exemplo:

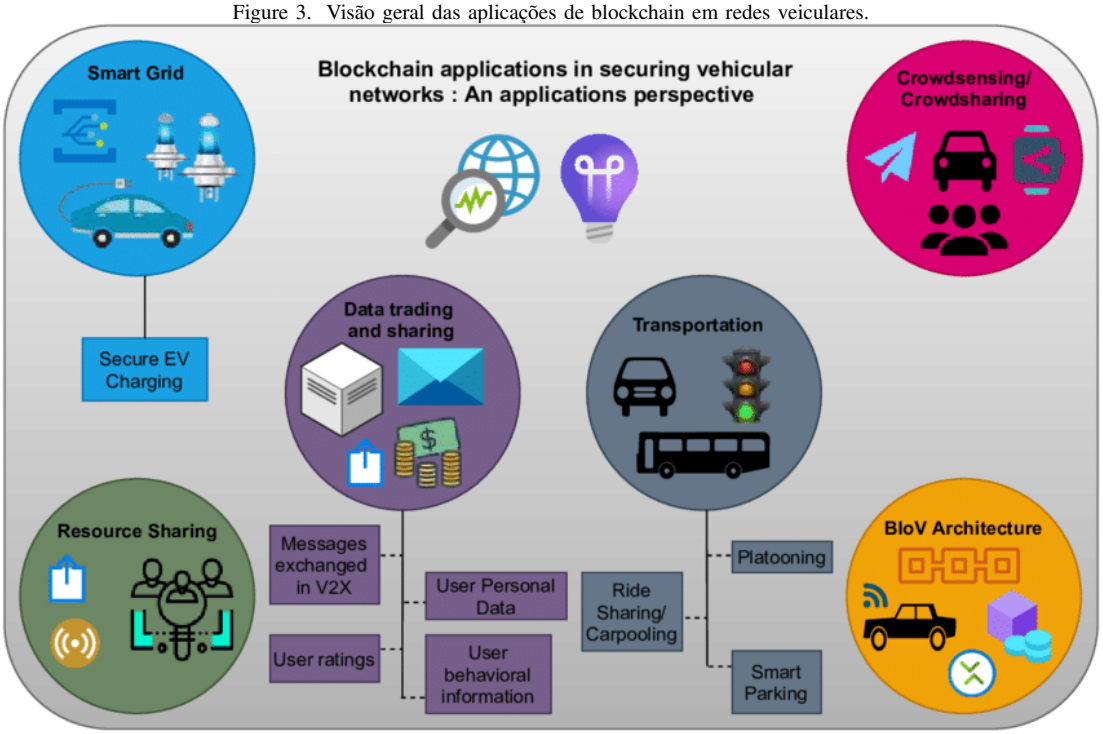
- **Autenticação descentralizada em tempo real:** Contratos inteligentes podem verificar automaticamente a identidade dos veículos ao ingressarem em uma rede. Essa abordagem elimina a necessidade de uma autoridade central e reduz os riscos de pontos únicos de falha.
- **Histórico imutável:** Cada interação autenticada é registrada no blockchain, criando um histórico auditável que pode ser usado para análise posterior.

Apesar de suas vantagens, o custo computacional e a escalabilidade permanecem como desafios, especialmente em redes de alta densidade. Pesquisas futuras devem explorar soluções híbridas que combinem computação em borda com blockchains leves para mitigar esses problemas.

Mecanismo	Descrição	Vantagens e Desvantagens
Proof of Reputation (PoR)	Utiliza a reputação dos veículos como critério para validação de transações. Introduzido por Wang et al. (2022).	5**Vantagens:** Alta eficiência energética e adequado para cenários de alta mobilidade. **Desvantagens:** Suscetível à manipulação de reputação por nós maliciosos.
Proof of Authority (PoA)	Baseia-se em um subconjunto de nós confiáveis para validar transações. Proposto por Dorri et al. (2017).	**Vantagens:** Baixo custo computacional, ideal para veículos com recursos limitados. **Desvantagens:** Centralização implícita pode introduzir vulnerabilidades e reduzir resiliência.

Table I: Comparação de Mecanismos de Consenso para Redes Veiculares

Figure 3. Visão geral das aplicações de blockchain em redes veiculares.



Fonte: Extraido de (Tejasvi Alladi et al., 2022)

Integridade e Privacidade dos Dados

O blockchain é amplamente utilizado para proteger a integridade e a privacidade dos dados em redes veiculares. Alguns exemplos incluem:

- **Proteção de mensagens críticas:** Alertas de colisão ou condições adversas de tráfego podem ser autenticados e protegidos contra adulterações por meio de blockchains públicos.
- **Privacidade aprimorada:** Provas de conhecimento zero (*Zero-Knowledge Proofs*) permitem validar transações sem expor informações sensíveis, como localização ou comportamento do motorista.

Abordagens híbridas, que combinam blockchains públicos e privados, têm se mostrado eficazes para atender a diferentes níveis de confidencialidade, mas o aumento do custo computacional ainda representa um desafio.

Coordenação de Veículos Autônomos

A coordenação segura de veículos autônomos é um campo emergente onde o blockchain tem grande potencial. Exemplos incluem:

- **Formação de comboios (*Platoons*):** Contratos inteligentes negociam parâmetros como velocidade, rota e distância entre veículos autônomos, garantindo eficiência e segurança.
- **Monitoramento e auditoria:** O blockchain registra todas as transações e interações entre veículos, criando um

histórico confiável que pode ser utilizado para análises de desempenho e resolução de disputas.

Apesar dos avanços, desafios relacionados à latência e ao tempo de execução de contratos inteligentes em blockchains públicos, como Ethereum, precisam ser resolvidos para permitir operações em tempo real.

Redes Elétricas Inteligentes e Comércio de Energia

Com a popularização dos veículos elétricos (VEs), o blockchain tem sido aplicado para gerenciar transações de energia em redes elétricas inteligentes. Casos de uso incluem:

- **Negociação de carregamento:** Contratos inteligentes permitem que veículos negociem automaticamente tarifas de carregamento e descarregamento de energia com estações de carregamento.
- **Comércio descentralizado de energia:** VEs podem vender excedentes de energia armazenada para outros veículos ou para a rede elétrica, utilizando tokens baseados em blockchain.

Embora promissoras, essas soluções dependem de infraestrutura avançada, como estações de carregamento compatíveis e conectividade de alta velocidade, como o 5G.

Proteção Contra Ataques e Resiliência

A resiliência contra ataques cibernéticos é uma aplicação essencial do blockchain em redes veiculares. Exemplos práticos incluem:

- **Mitigação de ataques Sybil:** Identidades verificáveis armazenadas no blockchain impedem que nós maliciosos criem múltiplas identidades falsas.
- **Defesa contra ataques de negação de serviço (DoS):** Protocolos distribuídos eliminam pontos únicos de falha, reduzindo a vulnerabilidade a ataques de DoS.

Mecanismos de consenso mais leves, como *Proof of Authority* (PoA) e *Proof of Reputation* (PoR), estão sendo explorados para melhorar a eficiência e escalabilidade nesses cenários.

Organização dos Cenários de aplicação

A Figura 4 detalha os cenários de aplicação do blockchain de forma temática, categorizando-os por funcionalidade e impacto na segurança:

- **Transações seguras:** Uso de contratos inteligentes para automatizar negociações entre veículos, como o comércio de dados e serviços.
- **Gerenciamento de tráfego:** Blockchain utilizado para monitoramento e otimização de tráfego em tempo real, reduzindo congestionamentos.
- **Sistemas de compartilhamento de recursos:** Aplicações para caronas compartilhadas e otimização de rotas.
- **Suporte à mobilidade elétrica:** Blockchain aplicado para gerenciar carregamento, pagamento e uso sustentável de energia em veículos elétricos.

Discussão

A análise dos trabalhos reforça que o blockchain desempenha um papel central na transformação de redes veiculares, abordando desafios históricos de segurança e eficiência. Embora as soluções apresentadas sejam promissoras, questões como escalabilidade, interoperabilidade e custo computacional permanecem como barreiras para uma adoção em larga escala.

A escalabilidade é um dos maiores desafios para o uso do blockchain em redes veiculares devido à grande quantidade de transações que precisam ser processadas em tempo real é à alta densidade de veículos. Os mecanismos de consenso como *Proof of Work* (PoW) apresentam alta latência e consumo de energia, tornando-os inadequados para cenários de alta mobilidade. No entanto, existem várias alternativas e direções futuras como o uso de mecanismos de consenso mais leves como *Proof of Authority* (PoA) e *Proof of Reputation* (PoR), pode reduzir a carga computacional e melhorar a eficiência energética. Por outro lado, aplicação de técnicas como *sharding*, que divide a rede blockchain em subgrupos menores para processar transações em paralelo, pode melhorar significativamente a escalabilidade.

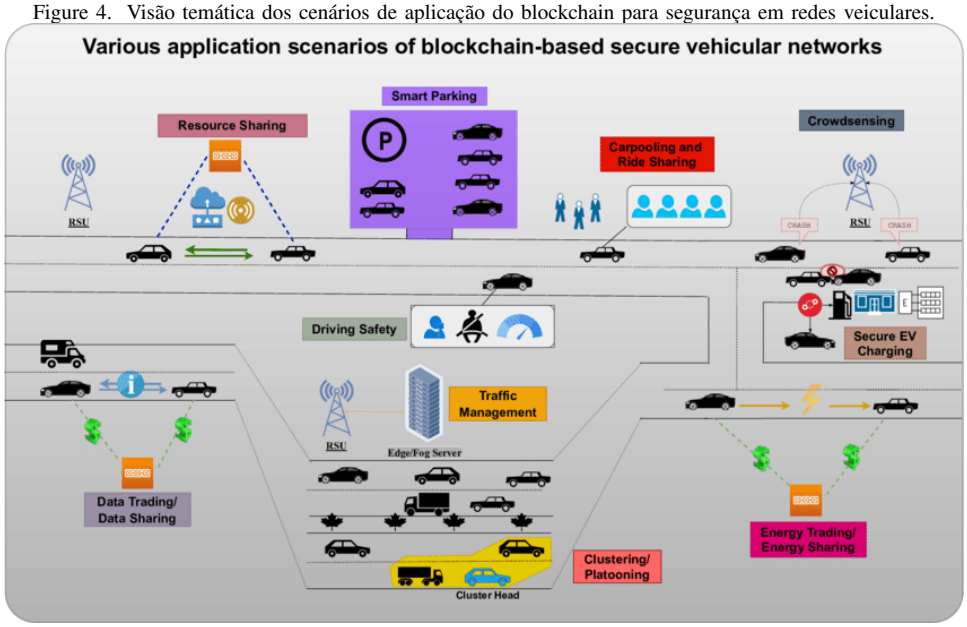
A latência é uma preocupação crítica em redes veiculares, onde as decisões precisam ser tomadas em frações de segundo para garantir a segurança dos usuários. Contratos inteligentes e validações no blockchain frequentemente introduzem atrasos que podem comprometer o tempo de resposta. No entanto, a integração do blockchain com tecnologias de computação em borda (*edge computing*) pode reduzir a latência, permitindo que transações sejam processadas localmente antes de serem registradas na cadeia principal.

A interoperabilidade entre diferentes sistemas veiculares é um desafio crítico, dado que veículos de diferentes fabricantes e regiões podem utilizar soluções blockchain distintas. A falta de padronização dificulta a colaboração e a troca de informações entre redes. Por esse motivo padrões globais para o uso de blockchain em redes veiculares devem ser estabelecidos, promovendo a colaboração entre indústrias e governos.

A implementação e manutenção de blockchains em larga escala ainda são caras, especialmente quando envolvem tecnologias como contratos inteligentes e blockchains híbridos. Uma direção futura a ser tomada poderia ser o desenvolvimento de soluções mais acessíveis, como blockchains leves e otimizados para dispositivos com baixa capacidade computacional. Alem incentivar colaborações público-privadas para compartilhar os custos iniciais de infraestrutura.

Como apresentamos no artigo a seguir, grande parte das pesquisas atuais é baseada em simulações e experimentos controlados, o que pode refletir com precisão as condições reais de operação. No futuro, espera-se que seja possível realizar estudos de caso em ambientes reais, como testes em cidades inteligentes e rodovias equipadas com infraestruturas de comunicação avançadas. Isso exigirá desenvolver parcerias entre fabricantes de veículos, governos e empresas de tecnolo-

Figure 4. Visão temática dos cenários de aplicação do blockchain para segurança em redes veiculares.



Fonte: Extraido de (Tejasvi Alladi et al., 2022)

gia para implementar projetos piloto em larga escala. A colaboração interdisciplinar e os avanços tecnológicos continuarão a ser os principais facilitadores para que o blockchain atenda às demandas crescentes das redes veiculares e da Internet of Vehicles (IoV).

Conclusão

A incorporação de segurança nos automóveis conectados exige uma abordagem abrangente e proativa. Essa estratégia deve ser planejada antes de qualquer incidente, garantindo múltiplas camadas de proteção e considerando todas as possíveis superfícies de ataque. É prudente assumir que, em algum momento, um carro conectado pode ser alvo de um ataque cibernético. Hackers que tentam comprometer dispositivos embarcados por meio de ataques remotos exploram vulnerabilidades, buscando portas abertas que possam revelar fragilidades no sistema.

A redução da superfície de ataque passa pelo bloqueio de todas as portas e protocolos que não estejam em uso. Além disso, registrar pacotes que violam as regras de filtragem configuradas ajuda a identificar comportamentos suspeitos. É crucial lembrar que a maioria dos ataques cibernéticos só é descoberta quando já causou danos. Portanto, a detecção precoce é fundamental para mitigar os riscos.

Quando dois dispositivos se comunicam dentro de uma rede automotiva, essa interação deve ser protegida contra acessos não autorizados. Isso requer a autenticação rigorosa e intrínseca de programas ou dispositivos, assegurando que todas as conexões de entrada sejam verificadas de forma confiável e que o sistema seja resistente a possíveis ataques.

Com a evolução dos carros conectados, torna-se cada vez mais recomendável implementar a segurança cibernética de maneira remota, utilizando sistemas de gerenciamento de segurança empresarial. Essa abordagem centralizada permite a definição e o gerenciamento de políticas de segurança, monitoramento contínuo dos dispositivos, análise de dados em tempo real e gerenciamento de eventos. Além disso, oferece ferramentas para analisar logs e aprimorar a detecção e a resposta a incidentes, promovendo maior segurança e resiliência em um ambiente digital em constante transformação.

References

[1] Hussain, R., et al. (2021). Security and Privacy in Vehicular Networks: Challenges and Solutions. *IEEE Communications Surveys & Tutorials, 23*(2), 1234-1265.

[2] Zhang, L., et al. (2022). Emerging Threats and Countermeasures in Vehicular Ad-Hoc Networks. *IEEE Transactions on Intelligent Transportation Systems, 24*(3), 765-789.

[3] Zhang, L., Wei, L., Zhao, Y., & Yang, J. (2022). Smart Contracts for Vehicular Platoons Using Blockchain Technology. *IEEE Transactions on Intelligent Transportation Systems, 23*(3), 2125–2136. https://doi.org/10.1109/TITS.2021.3074342.

[4] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from https://bitcoin.org/bitcoin.pdf.

[5] Zheng, Z., et al. (2018). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. *IEEE Access, 6*, 11738-11751.

[6] Dorri, A., et al. (2017). Blockchain for IoT Security and Privacy: The Case Study of Smart Home. *Proceedings of the IEEE International Conference on Pervasive Computing and Communication Workshops*, 618-623.

[7] Wang, Y., Zhang, Z., & Li, H. (2022). Proof of Reputation Consensus Mechanism for Blockchain-Based Vehicular Networks. *IEEE Transactions on Vehicular Technology, 71*(5), 4112–4123. https://doi.org/10.1109/TVT.2022.3145768.

[8] Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2006). A survey on sensor networks. *IEEE Communications Magazine, 40*(8), 102-114.

[9] Campolo, C., et al. (2017). 5G Network Architecture for Connected and Autonomous Vehicles. *IEEE Access, 5*, 24236-24244.

[10] Gerla, M., et al. (2014). Internet of Vehicles: From Intelligent Grid to Autonomous Cars and Vehicular Clouds. *Proceedings of the IEEE World Forum on Internet of Things (WF-IoT)*, 241-246.

[11] Yang, F., et al. (2019). An Overview of Internet of Vehicles. *IEEE Access, 7*, 183116-183131.

[12] Kumar, R., et al. (2020). Vehicular Ad Hoc Networks: Challenges and Future Directions. *Journal of Communications and Networks, 22*(3), 197-205.

[13] Kumar, R., Singh, J., & Kohli, M. (2020). A Comprehensive Survey on Scalability and Security Challenges in Blockchain Technology. *Journal of Communications and Networks, 22*(3), 197–210. https://doi.org/10.23919/JCN.2020.000013.

[14] Zhou, B., et al. (2020). Challenges and Opportunities in Secure Internet of Vehicles. *IEEE Network, 34*(1), 151-157.

[15] Shrestha, R., Bajracharya, R., & Nam, S. Y. (2020). A Blockchain-Based Approach for Secure and Trustworthy Data Sharing in Vehicular Networks. *IEEE Internet of Things Journal, 7*(6), 5724–5735. https://doi.org/10.1109/JIOT.2020.2978450.

[16] Huang, X., Yang, L., Zheng, Z., & Zhang, Y. (2019). Blockchain-Based Trust Management in Vehicular Networks. *IEEE Transactions on Internet of Things, 6*(2), 2324–2335. https://doi.org/10.1109/TIOT.2018.2878343.

[17] Liu, J., Zhang, X., Chen, T., & Wang, Y. (2023). Hybrid Blockchain for Privacy-Preserving Vehicular Communication Systems. *IEEE Journal on Selected Areas in Communications, 41*(2), 456–468. https://doi.org/10.1109/JSAC.2023.3231112.

[18] Xu, C., Gao, L., Wei, X., & Zhang, K. (2020). Zero-Knowledge Proof Based Privacy-Preserving Blockchain for Vehicular Networks. *IEEE Transactions on Industrial Informatics, 16*(7), 4827–4835. https://doi.org/10.1109/TII.2020.2969831.

[19] Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017). Blockchain for IoT Security and Privacy: The Case Study of Smart Home. *Proceedings of IEEE PerCom Workshops*, 618–623. https://doi.org/10.1109/PERCOMW.2017.7917634.

[20] Chen, T., Wang, H., Li, Z., & Yang, F. (2021). Energy Trading for Electric Vehicles Using Blockchain-Based Smart Contracts. *IEEE Transactions on Smart Grid, 12*(4), 3568–3577. https://doi.org/10.1109/TSG.2021.3054768.