Persistência de dados de Redes Veiculares Ad Hoc em Blockchain

André Luis Francisco Junior
Departamento de Ciência da Computação - DCC
Universidade do Estado de Santa Catarina - UDESC
Joinville, Santa Catarina - Brasil
andre.lfj@edu.udesc.br

Adriano Fiorese
Departamento de Ciência da Computação - DCC
Universidade do Estado de Santa Catarina - UDESC
Joinville, Santa Catarina, Brasil
https://orcid.org/0000-0003-1140-0002
adriano.fiorese@udesc.br

***Abstract*—The credibility and reliability of information is under constant threat. The case of information relating to traffic dynamics involving different vehicles and drivers on different pathways, it is no exception. This is the case for generated information related to vehicles, traffic events and other data in vehicular ad hoc networks (VANETs - Vehicular Ad-Hoc Networks). One of the ways to provide this reliability is by ensuring that the persistence of this data is secure enough to prevent changes. This work aims to present a solution for securing storage of this information using a blockchain, since it presents as one of its main characteristics the ability to ensure the immutability of stored data. A developed score will also be presented representing how the driver behaves in the VANET network, which will use the data stored in the blockchain to be calculated.**

***Resumo*—A credibilidade e confiança das informações é alvo de constante ameaça. Para o caso de informações relativas à dinâmica de trânsito envolvendo diferentes veículos e condutores, em diferentes vias, isso não é exceção. É o caso para informações geradas relacionadas aos veículos, eventos de trânsito e outros dados nas redes veiculares *ad hoc* (VANETs - *Vehicular Ad-Hoc Networks*). Uma das formas de disponibilizar esta confiabilidade é garantindo que a persistência desses dados seja segura o suficiente para impedir alterações. Este trabalho tem como objetivo apresentar uma solução para o armazenamento seguro dessas informações utilizando uma *blockchain*, pois estas apresentam como uma de suas principais características a capacidade de garantir a imutabilidade dos dados armazenados. Também será apresentado um índice que representa como o motorista se comporta na rede VANET, que utilizará os dados armazenados na *blockchain* para ser calculado.**

***Palavras-chave*—VANET; Blockchain; credibilidade.**

I. Introdução

As informações geradas por uma rede veicular *ad hoc* (VANET - *Vehicular Ad-Hoc Network*) precisam ser armazenadas de forma segura, confiável e imutável. Uma das características que justificam tais necessidades é a certificação temporal da ocorrência dos eventos que se apresentam dinamicamente em tais redes e que condicionam, eventualmente, decisões de funcionamento da rede. Outra razão importante para justificar a utilização de um armazenamento seguro como o de uma *blockchain* é a necessidade do histórico do comportamento do veículo ou motorista analisado.

Uma VANET consiste em uma rede veicular para troca de informações entre veículos (V2V) ou entre veículos e infraestrutura (V2I), tendo como foco principal transmitir rapidamente informações sobre acidentes, engarrafamentos ou qualquer situação que coloque vidas em risco [1]. A rede VANET gera informações que podem ser utilizadas por diversos atores para melhorias das condições de tráfego, alerta de acidentes, monitoramento de veículos e rodovias, dentre outros. Tais aplicações demandam comunicação eficiente e confiabilidade de armazenamento. Tendo em vista a necessidade de confiabilidade, uma rede *blockchain* pode ser formada e utilizada para armazenar os dados gerados pela VANET, aproveitando-se da imutabilidade e registro de tempo dos blocos, em uma rede *blockchain* para assegurar que nenhuma informação sensível é alterada ou perdida.

Blockchain é uma tecnologia que consiste em disponibilizar um mecanismo para armazenar informações de forma descentralizada [2] e imutável [3]. Em termos de descentralização, uma *blockchain* é composta de uma rede de usuários comprometidos com os propósitos particulares daquela rede, como por exemplo, assegurar a confiabilidade de transações financeiras. Além disso, uma rede *blockchain* também é composta por utilizadores dos protocolos daquela *blockchain*, como por exemplo, os nós processadores (computadores) das informações e executores das comunicações necessárias para o propósito da rede. Nesse sentido, forma-se uma rede que envolve e processa diversos dos mecanismos necessários a formação e manutenção da *blockchain* conhecida como rede *blockchain*, sendo que muitas vezes ambos os termos são usados intercambiavelmente.

Uma *blockchain*, como o nome sugere, é uma cadeia de blocos estruturados de informação, da forma que o bloco atual

tem uma ligação com o bloco anterior, e assim sucessivamente até se chegar ao primeiro bloco, chamado de bloco gênesis. Todos os blocos tem um registro de tempo marcando o exato momento em que ele foi inserido na *blockchain* e nenhuma informação já inserida pode ser alterada. Além disso, todos os usuários da rede recebem e mantém uma cópia de toda a *blockchain*. Tais características dificultam a alteração da informação já armazenada, por algum ente interno ou externo da rede *blockchain*, proporcionando imutabilidade da informação armazenada como uma de suas principais características, tornando-a assim um sistema seguro.

Nesse sentido, este trabalho apresenta uma possível solução para o armazenamento seguro de informações obtidas e geradas por uma rede VANET, utilizando uma rede *blockchain* privada. O trabalho também apresenta uma utilização para as informações armazenadas na rede *blockchain*, sendo esse o Fator de Credibilidade Veicular. O trabalho está organizado da seguinte maneira. A Seção 2, apresenta o referencial teórico, que visa embasar conceitos discutidos no trabalho. A Seção 3, apresenta uma revisão de trabalhos relacionados. A Seção 4, apresenta uma proposta para a solução do problema de armazenamento de dados de redes VANETS em *blockchain* e a utilização do Fator de Credibilidade Veicular. Finalmente, a Seção 5 apresenta as considerações finais sobre o presente trabalho.

II. Referencial Teórico

Blockchain é um banco de dados distribuído e descentralizado que armazena todas as informações em blocos. Um bloco é constituído por uma quantidade de transações, o seu identificador e o identificador do bloco anterior. Quando um bloco está pronto, cada nó (chamado de *peer*, que é um computador conectado a rede), tenta validar e publicar o bloco. Além disso, todos os nós da rede possuem uma cópia de toda a *blockchain*. Para decidir qual nó vai publicar o bloco, um algoritmo de consenso é utilizado. Esse algoritmo consegue decidir qual bloco deve ser publicado mesmo que alguns nós falhem ou sejam maliciosos. Os nós que participam do algoritmo de consenso são chamados de mineradores. Alguns exemplos de algoritmos de consenso são:

- Proof of Work (PoW): é o algoritmo mais conhecido. É utilizado pela criptomoeda Bitcoin. Este algoritmo consiste em resolver um quebra-cabeças que é resolvido através de uma função matemática chamada Hash. Cada bloco consiste do Hash do bloco anterior, histórico de transações, um nonce (number only used once [4]) e o hash do bloco atual [5]. Este algoritmo é seguro pois para um atacante conseguir inserir um bloco falso na rede, ele precisa ter mais de 50% do poder computacional da rede, tornando o ataque muito difícil e custoso.
- Proof of Stake (PoS): é o segundo algoritmo mais conhecido. A criptomoeda Ethereum adotou esse mecanismo de consenso em 15 de Setembro de 2022. [6]. A ideia do Proof of Stake é de resolver alguns problemas do Proof of Work, como a eficiência energética [5]. O algoritmo PoW utiliza poder computacional para resolver o quebra-cabeça, o tornando um algoritmo que consome um elevado nível de energia. No algoritmo PoS, o criador do próximo bloco é escolhido baseado em vários fatores, o principal deles é a quantidade de participação (a quantidade de moedas em *blockchain*s baseadas em criptomoedas). Assim como no PoW, o Proof of Stake também é bastante seguro contra ataques, neste caso, o atacante precisa ter em sua carteira mais do que 50% de todas as moedas disponíveis na rede.
- Practcical Byzantine Fault Tolerance (PBFT): foi desenvolvido pensando em resolver o *Byzantine General problem*. Nesse algoritmo, o consenso é alcançado quando pelo menos 2/3 dos nós concordam que a informação é verdadeira. Assim, um atacante precisa de mais de 2/3 dos nós da rede, tornando ainda mais difícil o ataque.
- Raft: também é da família de algoritmos pensados em ser resistentes a falhas. Raft [7] foi desenvolvido baseado na premissa que o tempo todo, mais de 50% dos nós funcionam corretamente [8]. Esse algoritmo é implementado em redes privadas, impossibilitando um ataque externo.

Além disso, uma *blockchain* pode ser pública, consorciada ou privada. *Blockchains* públicas são as mais conhecidas, como Bitcoin. Nelas, qualquer indivíduo consegue acessar as informações e transações armazenadas nos blocos como também participar do método de consenso, necessitando assim de uma maior segurança, visto que um atacante pode participar na mineração ou votação dos blocos sem nenhuma restrição. Em uma rede consorciada, qualquer indivíduo pode acessar as informações da rede, mas apenas os nós que possuem permissão podem participar do processo de consenso. Em uma *blockchain* privada, diferente das redes consorciada e pública, apenas os nós que possuem permissão conseguem acessar as informações e participar do método de consenso, dando maior flexibilidade em relação a segurança, visto que todos os nós participantes da rede são conhecidos e hipoteticamente confiáveis.

A ferramenta de código aberto chamada Hyperledger Fabric [9], desenvolvida e mantida pela Linux Foundation é uma plataforma muito útil para a criação e configuração de *blockchains* privadas permissionadas. Essa ferramenta utiliza do conceito de *chaincode*, também conhecido como *smart contract*. Um *chaincode* é responsável por processar as requisições das transações e determinar se essas transações são válidas executando a lógica de negócio. A lógica de negócio pode ser uma simples atualização de informações ou uma quantidade

de funções complexas fazendo operações com as informações inseridas na *blockchain* [10]. O Hyperledger Fabric também utiliza dos conceitos de *peers*, organizações e canais. *Peers* são a peça fundamental da *blockchain*, são eles que armazenam e computam tudo o que é armazenado na rede [11], é nos *peers* que o *chaincode* é instalado. Organizações são conjuntos de *peers*, no entando, *peers* de uma mesma organização não precisam estar necessariamente próximos um ao outro. Os canais são a forma em que os *peers* utilizam para comunicar-se entre si ou com outras aplicações [11].

Segundo [12], o conceito de VANETs é derivado das redes Mobile Ad-hoc Networks (MANETs) e são projetadas para nós que estão em movimento constante, suportados por *Road Side Units* (RSUs). Nesse caso, os veículos são os nós da rede em constante movimento. Além de possuírem características próprias para aplicações de mobilidade, particularmente importantes para sistemas de transporte, logística, etc., tais nós (veículos) contam também com agentes humanos, isto é, seus motoristas, que sofrem e também influenciam nas decisões de mobilidade. Além disso, como em qualquer rede com aplicação prática, a comunicação entre os nós habilita a execução de tarefas úteis e é uma das mais importantes características a serem exploradas.

Sendo assim, as VANETs contam com uma grande quantidade de aplicações. Alguns exemplos incluem a segurança e comodidade dos motoristas, auxílio na manutenção das rodovias e obtenção de dados do trânsito e motoristas nas rodovias. A comunicação de uma rede VANET pode ocorrer na forma de veículo-para-veículo (V2V), veículo-para-infraestrutura (V2I), veículo-para-rede (V2N) e veículo-para-pedestre (V2P) [13]. Outros autores citam também uma arquitetura hibrida, sendo ela veículo-para-veículo-para-infraestrutura (V2V2I) [14]. A fim de simplificar, neste trabalho são consideradas as formas V2V e V2I.

Por serem sistemas embarcados com pouco processamento e armazenamento, as redes VANETs precisam ser apoiadas por uma infraestrutura. Essa infraestrutura é a que recebe as informações dos veículos quando eles se aproximam. Na proposta atual, cada RSU será um *peer* da rede, participando do algoritmo de consenso e adicionando novos blocos à rede. À medida que novos blocos sejam adicionados à rede, cada *peer* da rede (RSU) irá armazenar essas informações em sua cópia da *blockchain*. Desta forma, todos os *peers* da rede possuem uma cópia de toda a *blockchain*.

III. Trabalhos relacionados

Existem muitos trabalhos sobre o tema *blockchain* que auxiliam no entendimento de como a rede funciona, assim como também há trabalhos sobre VANETs. É possível também encontrar alguns trabalhos que envolvem as duas áreas. Nessa seção vamos discutir sobre esses trabalhos e como eles estão relacionados com o tema.

O trabalho de [12] é um survey que apresenta tecnologias relacionadas, como VANETs, Internet of Vehicles (IoV) e *blockchain*. O survey apresenta também alguns algoritmos de consenso, métodos de ataque à uma rede comum e uma rede *blockchain* e como se defender deles. Também mostra frameworks que podem ser utilizados para auxiliar no desenvolvimento de uma rede *blockchain*.

A questão do registro e autenticação dos participantes de uma rede VANET é tratada em [15]. O trabalho propõe um mecanismo de autenticação e registro seguros auxiliado por identificadores descentralizados em uma *blockchain* de dupla camada, chamado (*Blockchain Distributed Registration and Authentication* (BDRA), para redes VANETs. de acordo com os autores a utilização do mecanismo reduz o tempo de comunicação para re-registro das informações em 30%. Outro trabalho que trata da autenticação de nós utilizando *blockchain* para a proteção contra atividades maliciosas e falsa informação na rede VANET é [16].

O artigo de [17] tenta resolver os problemas de mensagens falsas de aviso como acidente, frenagem ou trânsito (livre ou engarrafado) feito por um atacante a fim de distrair o motorista ou mudar a sua forma de dirigir para benefício próprio. O artigo propõe o framework ALICIA *(AppLied Intelligence in bloCkchaIn vAnet)* que utiliza uma rede neural para excluir nós maliciosos do processo de consenso. Utiliza o algoritmo de consenso PBFT e a ferramenta *Hyperledger Fabric* para desenvolver a *blockchain*.

O survey de [5] apresenta vários algoritmos de consenso e faz comparações entre eles. Os algoritmos apresentados são Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), Proof of Elapsed Time, Practical Byzantine Fault Tolerance (PBFT), Delegated Byzantine Fault Tolerance, Proof of Weight (PoWeight), Proof of Burn (PoB), Proof of Capacity, Proof of Importance, Proof of Activity e Directed Acyclic Graphs.

Outro survey que apresenta algoritmos de consenso e diferenças entre eles, especialmente relacionados a protocolos públicos, privados e consorciados para autenticação em redes VANETS e ambientes IoV, baseados em *blockchain*, é o de [18].

O survey de [19] revisa os algoritmos de consenso mais conhecidos e apresenta as diferenças entre eles. Apresenta o Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), Practical Byzantine Fault Tolerance (PBFT) e Raft.

O trabalho de [20] visa disponibilizar um framework para comunicação segura no ambiente IoV utilizando *blockchain*. Nesse sentido, o trabalho propõe o algoritmo *High Performance*

Blockchain Consensus (HPBC) que atua na troca das chaves de criptografia que tornam a comunicação segura.

O artigo de [21] propõe utilizar uma rede *blockchain* para resolver os problemas de nós maliciosos em redes VANETs. Neste trabalho é proposto um framework em que nós maliciosos da rede não vão conseguir aumentar o seu nível de confiança em relação aos outros nós, sendo assim excluídos da rede. Também cita a utilização de uma mini *blockchain* para resolver os problemas de armazenamento que uma *blockchain* pode causar.

IV. Proposta

Neste trabalho é proposto o desenvolvimento e utilização de uma rede *blockchain* privada utilizando o algoritmo de consenso Raft para armazenar as informações dos veículos presentes em uma rede VANET. A Figura 1 exemplifica uma parte da cadeia de blocos (*blockchain*) desenvolvida.

Fig. 1. Exemplo de uma parte da *blockchain* desenvolvida.

Na proposta atual, todos os veículos que em algum momento fizerem parte da VANET têm suas informações, como montadora, modelo, ano, cor, etc..., armazenadas em blocos na rede *blockchain*, como pode ser observado na Figura 1. Essas informações são armazenadas e atualizadas como transações na *blockchain*, se tornando imutáveis e seguras. Assim, a *blockchain* desenvolvida conta com um limite de 10 transações por bloco e um tempo máximo de espera de 2 segundos, ou seja, um novo bloco é publicado na rede assim que ele atinge 10 transações ou possui pelo menos uma transação à mais de 2 segundos. Isso faz com que a rede seja rápida apresentando baixo tempo de espera entre a publicação (compartilhamento) dos blocos.

O algoritmo de consenso Raft foi escolhido para este trabalho pois foi desenvolvido para redes privadas e por ser de fácil compreensão. Nesse contexto, o algoritmo Raft é mais fácil de implementar comparado com outros algoritmos conhecidos, como PBFT, PoW ou PoS. Além disso, há prova formal de que Raft seguro, assim como os outros algoritmos de consenso mais conhecidos [7].

A *blockchain* foi elaborada utilizando o Hyperledger Fabric para criar uma rede privada sob a ferramenta Minifabric [22]. O Hyperledger Fabric é um *framework* que visa auxiliar na criação de redes *blockchain* privadas. Suas principais características são criar uma rede *blockchain* com bom desempenho e segurança. O Hyperledger Fabric disponibiliza a capacidade de automação de tarefas relacionadas com o processamento das transações que ocorrem na rede *blockchain*. Tal capacidade é fornecida por meio dos *chaincodes*. Um *chaincode* é responsável por processar as requisições das transações e determinar se essas transações são válidas excetuando a lógica de negócio [10]. A lógica de negócio pode ser uma simples atualização de informações ou uma quantidade de funções complexas fazendo operações com as informações inseridas na *blockchain*. O *chaincode* pode ser escrito em Go, Javascript ou Java. Nesse trabalho utilizamos a linguagem Go. Já a ferramenta Minifabric é utilizada para auxiliar nas operações de criação da rede, criação de canal, juntar os peers ao canal, instalar o *chaincode* nos *peers* e invocar o *chaincode*. A Figura 2 ilustra logicamente a ligação entre os nós da rede *blockchain*.

Após a *blockchain* criada e o *chaincode* devidamente configurado, as novas transações podem ser incluídas contendo as informações do(s) veículo(s). Para fins de teste e validação da *blockchain*, dados hipotéticos demonstrados na Figura 1 foram criados e inseridos na rede. Para a compreensão do processo, alguns conceitos utilizados pelo Hyperledger Fabric para a criação e operação de uma rede *blockchain* são necessários. Dentre eles o conceito de organização. Uma organização é uma forma de organizar os *peers* responsáveis de processamento das transações incluindo a execução do mecanismo de consenso junto ao *framework* Hypeledger Fabric. Nesse sentido, esse conceito visa definir as entidades que contribuem com nós na formação da rede *blockchain*. Assim, dois *peers* de uma mesma organização não precisam necessariamente estar no mesmo espaço físico, podendo estar distantes um do outro. Outro conceito é o de *Ledger*. Nesse caso, *ledger* é o nome dado para a cópia da cadeia de blocos que cada *peer* possui.

Assim, neste trabalho, a rede conta com duas organizações, cada uma com dois *peers* e cada *peer* com uma cópia do *ledger*, nesse caso todos os *peers* utilizam o mesmo *chaincode*, e se encontram dentro de uma RSU, como demonstrado na Figura 2.

O cenário de utilização da proposta desse trabalho é

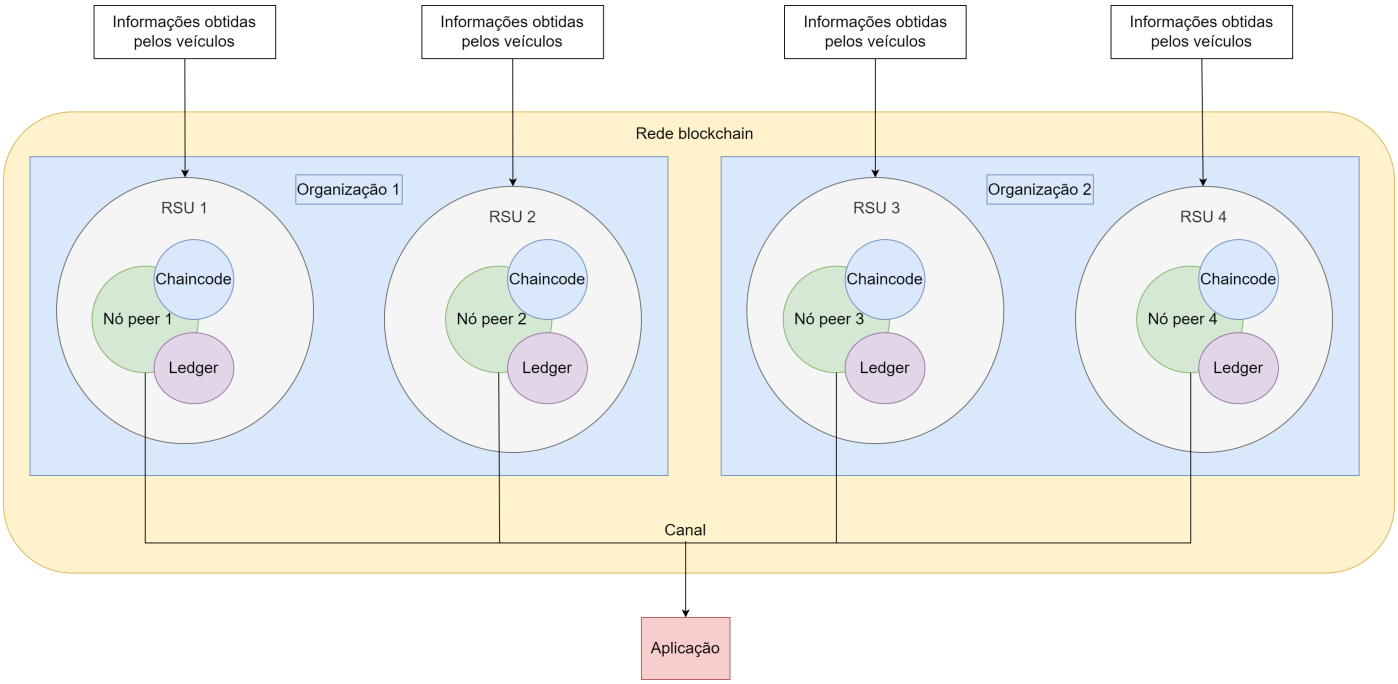

Fig. 2. Diagrama de uma parte da *blockchain*.

aplicável a quaisquer entidades que tenham interesse na operacionalização da persistência de dados de redes VANETS inicialmente, ou de Internet of Vehicles (IoV). Nesse domínio podemos citar desde as próprias concessionárias de gestão de rodovias que podem tirar vantagem da infraestrutura que administram para, por meio da gestão dos dados armazenados na *blockchain*, otimizarem seus processos internos auxiliando na melhoria do tráfego, bem como autoridades governamentais responsáveis pelo trânsito.

Um exemplo que trata do aproveitamento dessas informações é o cálculo de uma pontuação para cada veículo, baseado no comportamento dentro da VANET. Nesse sentido, esse trabalho também propõe tal avaliação, que será chamada de Fator de Credibilidade Veicular (FCV), e pode ser utilizada em aplicações no domínio da mobilidade veicular, urbana e em geral, com o propósito de auxiliar na tomada de decisões. Nesse sentido, o FCV utiliza-se das informações armazenadas na *blockchain* para ser calculado. Em princípio, por definição, o FCV indica a forma como o motorista do veículo analisado se comporta nas estradas. O fator leva em conta se o motorista respeita as velocidades máximas das vias, se trafega em horários de pico, tempo dirigido nos últimos 30 dias, bem como a quilometragem percorrida nesses últimos 30 dias, seu tempo de habilitação, seu histórico de multas, o ano do veículo e por fim, a idade do motorista relacionada com a potência do veículo. Tais informações são então fornecidas pelos veículos durante o tráfego rodoviário urbano e geral e armazenadas na rede *blockchain* que serve de origem dos dados para o cálculo. O valor do FCV pode ser calculado de acordo com a Equação 1.

$$\begin{aligned} v =&((V_M * 10) + (H_P * 3) + (T_D * 1) + (KM_M * 2) \\ &+ (T_C * 5) + (M * 10) + (A_V * 2) + (I * 4)) \end{aligned} \quad (1)$$

$$FCV = \frac{v}{37}$$

O resultado do FCV é um valor parametrizado entre 0 e 1 que indica o quão bom é o desempenho do motorista observado em uma seção de participação na VANET. Assim, quanto mais perto de 1, melhor. Uma seção corresponde ao tempo em que é iniciado um trajeto (partida do veículo) até o final do trajeto (desligamento do veículo). Esse período é contabilizado para obtenção das variáveis que que são utilizadas na Equação 1. Os valores são dados também em intervalos entre 0 e 1, onde 0 é ruim e 1 é ótimo. Matematicamente, o FCV é uma média ponderada das variáveis que o compõe.

Assim, a variável V_M é dada pelo valor que o motorista do veículo analisado recebe conforme a velocidade média observada, a depender da velocidade média e da via em que ele trafegou. Por exemplo, se o motorista dirige em uma velocidade

TABELA I
EXEMPLO DE CÁLCULO DO FCV

Pesos	10	3	1	2	5	10	2	4	
#	V_M	H_P	T_D	MK_M	T_C	M	A_V	I	FCV
Carro1	0,75	0,5	0,5	0,5	1	1	0,75	1	0,837
Carro1	1	0,75	0,5	0,5	1	1	0,75	1	0,925
Carro2	1	0,5	1	0,75	0,5	0,75	1	0,75	0,783
Carro2	1	0,75	1	0,75	0,75	1	1	0,75	0,905
Carro3	0,5	0,75	0,75	0,75	0,5	0,5	0,5	0,5	0,540
Carro3	1	0,75	0,75	0,75	0,5	1	0,5	0,5	0,810

fora do limite das vias, o valor é baixo, caso contrário, o valor será ótimo.

A variável H_P é dada por um valor baseado em quanto tempo do trajeto o motorista trafegou em horários de pico. Portanto, se trafegou por muito tempo em horário de pico seu valor será menor.

A variável T_D representa o valor recebido pelo motorista relacionado ao tempo dirigido. Se dirigiu por muito tempo seu valor é levemente reduzida.

A variável KM_M representa quantos quilômetros o motorista trafegou no último mês, seu valor é levemente reduzido conforme a quantidade de quilômetros aumenta.

A variável T_C representa o tempo em que o motorista está habilitado para dirigir, é uma variável externa e não está armazenada na *blockchain*. Caso o motorista tenha obtido a sua carteira a pouco tempo, o valor da variável T_C será baixo.

A variável M representa o histórico de multas do motorista, também é uma variável externa. Seu valor é reduzido drasticamente se possui muitas multas nos últimos 12 meses.

Por sua vez, a variável A_V representa o ano do veículo, reduz quanto mais antigo for o veículo. A variável I representa o valor da idade do motorista relacionada com a potência do veículo que ele dirige, por exemplo, um motorista de 20 anos dirigindo um veículo com 250 cv de potência terá um valor menor em comparação com um motorista de 40 anos dirigindo um veículo de 125 cv.

A Tabela I apresenta um exemplo da obtenção do valor do FCV. O exemplo apresenta três veículos, cada qual em dois cenários ou seções de obtenção de dados. Assim, cada duas linhas da tabela apresentam um veículo em duas situações. A segunda dessas linhas apresenta o cenário em que ocorre melhora em algum aspecto da utilização da VANET e refletindo assim em alguma variável do FCV e consequentemente melhorando-o. Particularmente, de acordo com o exemplo, é possível observar que o valor do FCV aumenta significativamente se o motorista passa a respeitar as leis de trânsito mais importantes, como limites de velocidade e menor quantidade de multas no último ano.

V. CONCLUSÃO

O trabalho apresentou e desenvolveu um modelo de persistência segura de informações dos veículos da VANET utilizando uma rede *blockchain* consorciada. A tecnologia *blockchain* foi escolhida por ser uma forma descentralizada e segura para armazenamento desse tipo de informação, oferecendo assim a segurança necessária para aplicações que necessitem de dados de mobilidade urbana, por exemplo.

O trabalho também apresentou uma utilização para as informações geradas pela rede VANET, e disponibilizadas pela rede *blockchain* proposta. Nesse sentido, modelou-se e apresentou-se o fator de credibilidade veicular, que utilizando-se das informações armazenadas na *blockchain* para ser calculado representa, de forma segura, o comportamento dos envolvidos na dinâmica da mobilidade veicular urbana e rodoviária. Para tanto, pesos para cada variável envolvida foram atribuídos de forma a modelar a importância das mesmas no referido cálculo.

Para trabalhos futuros, pode-se popular a *blockchain* desenvolvida para medir o seu desempenho. Assim, efetuar a comparação da proposta de armazenamento de informações de uma VANET atual para a de um banco de dados tradicional, visando a identificação de *overheads* de desempenho e utilização.

Também para trabalhos futuros, pode-se medir o desempenho da rede desenvolvida comparando-a com outra rede *blockchain*, com outro algoritmo de consenso. Neste sentido, comparar a rede atual com ela mesma, mas com um maior número de computadores e *peers* para comparar o desempenho e escalabilidade também são listados como atividades a serem desenvolvidas.

REFERÊNCIAS

[1] R. Shrestha, R. Bajracharya, A. P. Shrestha, and S. Y. Nam, "A new type of blockchain for secure message exchange in vanet," *Digital Communications and Networks*, vol. 6, no. 2, pp. 177–186, 2020.
[2] N. Z. Benisi, M. Aminian, and B. Javadi, "Blockchain-based decentralized storage networks: A survey," *Journal of Network and Computer Applications*, vol. 162, p. 102656, 2020.
[3] F. Hofmann, S. Wurster, E. Ron, and M. Böhmecke-Schwafert, "The immutability concept of blockchains and benefits of early standardization," in *2017 ITU Kaleidoscope: Challenges for a Data-Driven Society (ITU K)*. IEEE, 2017, pp. 1–8.
[4] J. Frankenfield, "Nonce," 2022. [Online]. Available: https://www.investopedia.com/terms/n/nonce.asp
[5] S. M. H. Bamakan, A. Motavali, and A. Babaei Bondarti, "A survey of blockchain consensus algorithms performance evaluation criteria," *Expert Systems with Applications*, vol. 154, p. 113385, 2020.
[6] The merge. [Online]. Available: https://ethereum.org/en/upgrades/merge/
[7] D. Ongaro and J. Ousterhout, "In search of an understandable consensus algorithm," in *2014 USENIX Annual Technical Conference (Usenix ATC 14)*, 2014, pp. 305–319.
[8] G.-T. Nguyen and K. Kim, "A survey about consensus algorithms used in blockchain," *Journal of Information processing systems*, vol. 14, no. 1, pp. 101–128, 2018.

[9] C. Cachin *et al.*, "Architecture of the hyperledger blockchain fabric," in *Workshop on distributed cryptocurrencies and consensus ledgers*, vol. 310, no. 4. Chicago, IL, 2016, pp. 1–4.
[10] H. A. W. Group, "Hyperledger architecture, smart contracts." vol. 2, 2018.
[11] H. Fabric. Peers — hyperledger-fabricdocs main documentation. [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/release-2.2/peers/peers.html#
[12] T. Alladi, V. Chamola, N. Sahu, V. Venkatesh, A. Goyal, and M. Guizani, "A comprehensive survey on the applications of blockchain for securing vehicular networks," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 2, pp. 1212–1239, 2022.
[13] S.-h. Sun, J.-l. Hu, Y. Peng, X.-m. Pan, L. Zhao, and J.-y. Fang, "Support for vehicle-to-everything services based on lte," *IEEE Wireless Communications*, vol. 23, no. 3, pp. 4–8, 2016.
[14] F. Cunha, L. Villas, A. Boukerche, G. Maia, A. Viana, R. A. Mini, and A. A. Loureiro, "Data communication in vanets: Protocols, applications and challenges," *Ad Hoc Networks*, vol. 44, pp. 90–103, 2016.
[15] X. Li, T. Jing, R. Li, H. Li, X. Wang, and D. Shen, "BDRA: Blockchain and Decentralized Identifiers Assisted Secure Registration and Authentication for VANETs," *IEEE Internet of Things Journal*, pp. 1–1, 2022, conference Name: IEEE Internet of Things Journal.
[16] A. Arora and S. K. Yadav, "Block Chain Based Security Mechanism for Internet of Vehicles (IoV)," in *Proceedings of 3rd International Conference on Internet of Things and Connected Technologies (ICIoTCT)*, Apr. 2018.
[17] S. R. Maskey, S. Badsha, S. Sengupta, and I. Khalil, "Alicia: Applied intelligence in blockchain based vanet: Accident validation as a case study," *Information Processing & Management*, vol. 58, no. 3, p. 102508, 2021.
[18] S. Abbas, M. A. Talib, A. Ahmed, F. Khan, S. Ahmad, and D.-H. Kim, "Blockchain-Based Authentication in Internet of Vehicles: A Survey," *Sensors (Basel, Switzerland)*, vol. 21, no. 23, p. 7927, Nov. 2021.
[19] D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei, and C. Qijun, "A review on consensus algorithm of blockchain," in *2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, 2017, pp. 2567–2572.
[20] K. Mershad and B. Said, "A blockchain model for secure communications in internet of vehicles," in *2020 IEEE/ACS 17th International Conference on Computer Systems and Applications (AICCSA)*, 2020, pp. 1–6.
[21] A. Mostafa, "Vanet blockchain: A general framework for detecting malicious vehicles." *J. Commun.*, vol. 14, no. 5, pp. 356–362, 2019.
[22] T. LI, R. Jones, A. Ramil Aguel, D. Liu, M. Potter, A. J Le Hors, and V. Killu, "Minifabric," original-date: 2020-01-03. [Online]. Available: https://github.com/hyperledger-labs/minifabric/blob/a61c275f88295a7ca2f5fe7f07fd65be2f645ae6/docs/README.md