FACULDADE DE TECNOLOGIA DE AMERICANA – MINISTRO RALPH BIASI

CURSO SUPERIOR DE TECNOLOGIA EM SEGURANÇA DA INFORMAÇÃO.

LUIZ HENRIQUE CAVALCANTI MEIRA

MARCELO LUVEZUTTO JUNIOR

ANÁLISE SOBRE SEGURANÇA DA INFORMAÇÃO EM CARROS INTELIGENTES – USO DO BLOCKCHAIN PARA GERENCIAMENTO DAS CONEXÕES E DADOS EM VANETS

AMERICANA, SP

2022

FACULDADE DE TECNOLOGIA DE AMERICANA – MINISTRO RALPH BIASI

CURSO SUPERIOR DE TECNOLOGIA EM SEGURANÇA DA INFORMAÇÃO.

LUIZ HENRIQUE CAVALCANTI MEIRA

MARCELO LUVEZUTTO JUNIOR

ANÁLISE SOBRE SEGURANÇA DA INFORMAÇÃO EM CARROS INTELIGENTES – USO DO BLOCKCHAIN PARA GERENCIAMENTO DAS CONEXÕES E DADOS EM VANETS

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação, sob a orientação do Prof. Especialista Marcus Vinicius Lahr Giraldi.

Área de concentração: Segurança da informação.

AMERICANA

2022

LUIZ HENRIQUE CAVALCANTI MEIRA

MARCELO LUVEZUTTO JUNIOR

ANÁLISE SOBRE SEGURANÇA DA INFORMAÇÃO EM CARROS INTELIGENTES – USO DO BLOCKCHAIN PARA TRATAMENTO DAS CONEXÕES EM VANETS

Trabalho de graduação apresentado como exigência parcial para a obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – FATEC/Americana.

Área de concentração: Segurança da Informação.

Americana, 22 de junho de 2022.

Banca Examinadora:

_____

Marcus Vinícius Lahr Giraldi (Presidente)

Especialista

Fatec Americana

_____

Edson Roberto Gaseta (Membro)

Mestre

Fatec Americana

_____

Elton Rafael Maurício da Silva Pereira (Membro)

Mestre

Fatec Americana

Agradecimentos

Em primeiro lugar, gostaríamos de agradecer a Deus, pois sem ele não estaríamos aqui. Em seguida agradecemos nossos familiares, que nos apoiaram durante o período de produção deste trabalho. E ao nosso orientador, Marcus Lahr por toda prestimosidade e apoio.

RESUMO

Neste trabalho traremos como pauta principal a segurança dos automóveis inteligentes e como lidar com a quantidade de dados, confiabilidade deles, as conexões e desconexões em massa em uma rede VANET e como limitar o acesso a tal, analisaremos também desde os primórdios dos veículos até os dias atuais e quais foram as necessidades humanas para desenvolver tal tecnologia, que permitisse que, o ato de dirigir não fosse mais uma atividade manual e passe a ser uma rotina automatizada, fazendo com que veiculos passe a ser computadores e dispositivos em uma rede, e como utilizar o Blockchain para que isso seja possível e seguro.

Abordaremos como esse sistema funciona, desde a sua utilização como câmeras, sensores e painéis de comando, até sistemas externos como a construção da rede utilizada chamada de VANETS, que mostra a comunicação desde, veículos com veículos (V2V) até veículos com rodovia (V2R) e o quão veloz essa conexão deve ser, mostraremos também o sistema de validação dessas comunicações, que atualmente utiliza o blockchain para validar as ações de determinado veículo em determinada situação afim de comunicar os demais com a consistência e veracidade da informação obtida naquele momento, traremos também qual o melhor sistema de validação em blockchain o que melhor funcionaria, e o que mais se adequa ao tema proposto neste trabalho.

Palavras-chave: Blockchain; conexões; carros.

ABSTRACT

In this work, we will bring the security of smart cars as the main agenda and how to deal with the amount of data, their reliability, the connections and disconnections in mass in a VANET network and how to limit access to such, we will also analyze from the beginnings of vehicles to the nowadays and what were the human needs to develop such technology, which would allow the act of driving to be no longer a manual activity and become an automated routine, making vehicles become computers and devices on a network, and how to use Blockchain to make this possible and safe.

We will discuss how this system works, from its use as cameras, sensors and control panels, to external systems such as the construction of the used network called VANETS, which shows communication from vehicles with vehicles (V2V) to vehicles with highway (V2R).) and how fast this connection must be, we will also show the validation system for these communications, which currently uses the blockchain to validate the actions of a given vehicle in a given situation in order to communicate the others with the consistency and veracity of the information obtained at that time, we will also bring the best blockchain validation system, which would work best, and what best suits the theme proposed in this work.

Keywords: Blockchain; Network; Cars.

Sumário

Lista de figuras

1 Introdução

A indústria automotiva sempre foi um campo fértil no que diz respeito a inovação em tecnologias que permitam níveis cada vez mais altos de interação entre homem e máquina, tais inovações garantem mais conforto e comodidade aos usuários. Porém toda inovação traz riscos que, nem sempre são observados pelos usuários de um determinado produto ou serviço, um destes riscos é a falta ou falhas na segurança digital dos sistemas que compõem um veículo que possua algum tipo de conexão com a Internet ou outros dispositivos.

Atualmente vemos a ascensão dos veículos inteligentes, podendo ser veículos que tenham desde um simples sistema de entretenimento e multimídia, até mesmo veículos totalmente autônomos, que possam inclusive, dispensar os motoristas. Claro que estes ainda estão longe da realidade de muitos, mas independente disto, até onde as pessoas estão cientes da capacidade de segurança de um dispositivo inteligente, neste caso um veículo. Isso reforça a necessidade de que as empresas produtoras de tecnologia e de veículos tem em projetar e manter sistemas cada vez mais seguros e resilientes em relação a ataques virtuais.

É comum para a maioria das pessoas pensar que invasões a veículos seriam algo que ocorreriam apenas em filmes, porém a verdade é que já houve ataques deste tipo. Em 2015, houve um recall de 1,4 milhões de veículos da Jeep, [1]através do sistema de entretenimento, foi possível controlar o sistema de ar-condicionado e limpadores de para-brisa dos veículos. Em 2020, em testes permitidos pela Tesla, teve o sistema de seus veículos invadido, possibilitando a exibição de mensagens na tela do veículo. Por tanto isso não é mais coisa de filme.

Neste trabalho, analisaremos um dos recursos mais utilizados em redes que envolvam carros inteligentes, a comunicação entre os nós dessa rede e como gerenciar quem faz parte dela ou não.

Fonte: https://veja.abril.com.br/tecnologia/chrysler-faz-recall-de-14-milhao-de-carros-vulneraveis-a-hackers/

2 Segurança da informação e seus conceitos básicos

A segurança da informação pode ser definida basicamente como a junção de diversas atividades que tenham como objetivo suprir a necessidade da manutenção dos três principais pilares da segurança de informações, confidencialidade, integridade e disponibilidade.

“Segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio[...]” (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, P9, 2005).

A aplicação de medidas que tenham como objetivo a proteção não apenas dos dados dos usuários que porventura possam estar presentes em um veículo autônomo ou com algum dispositivo inteligente é sem dúvidas uma das questões mais importantes a serem pensadas pelas fabricantes.

“As ameaças à segurança de software nos carros conectados incluem engenharia reversa, adulteração de software, cópia e ataques automatizados que podem ser realizados através da rede ou desde o computador do hacker.” (FUTURE, 2017).

Entendemos como ameaça, “a causa potencial de um incidente indesejado, que pode causar danos à um sistema ou organização” (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2005).

Uma vulnerabilidade é “uma fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças” (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2005).

Para ambos os conceitos apresentados acima é importante considerarmos que, eles podem ser provenientes de ações humanas ou simplesmente de falhas no sistema em si, consideramos a ação humana pois a negligência com acessos, senhas e demais fatores que estejam relacionados a contas que, possivelmente venham estar vinculadas ao veículo como um todo ou a serviços que estejam conectados ao mesmo, podem criar vulnerabilidades e consequentemente, elevar os riscos.

“Um risco de segurança é um evento possível e potencialmente danoso a uma organização, isto é, que possui chance de ocorrência futura que não é nula e que apresenta impacto negativo significante.” (FERNANDES, P13, 2011).

Em relação ao assunto abordado neste trabalho, os impactos podem afetar não somente os usuários ou passageiros de um veículo inteligente, mas também outras pessoas que possam estar a seu redor.

Dado em tecnologia da informação é um conjunto de códigos, números, símbolos, entre outros, é o “alicerce” da informação, podemos defini-lo como uma pedra que precisa ser esculpida até virar uma informação, isoladamente não se pode dizer que transmitam uma mensagem clara, são uma serie de fatos discretos que não apresentam um significado importante e não leva a nenhuma compreensão isoladamente.

O dicionário de Biblioteconomia e Arquivologia conceitua Dado como:

> Menor representação convencional e fundamental de uma informação (fato, noção, objeto, nome próprio, número, estatística etc.) sob forma analógica ou digital passível de ser submetida a processamento manual ou automático. Em sentido mais amplo, toda a informação quantificável (números, letras, gráficos, imagens, sons ou outra combinação desses tipos); Sinais ou códigos usados para alimentação, processamento, e produção de um resultado. Dados bibliográficos: conjunto de elementos (autor, título, local de edição e outros dados empregados na descrição bibliográfica) que representam um documento específico. (CUNHA. 2008, P112).

Diferentemente dos dados a informação tem uma estrutura, uma cadeia organizada de dados, onde todos tem direito de acesso podendo ter aplicabilidades de leis e deveres, tem como finalidade reduzir incertezas, se aprofundar no conhecimento e sabedoria de um determinado assunto, ou pode esclarecer o funcionamento de um processo, entretanto não é conhecimento de modo geral.

> A informação obtida por um indivíduo, para se transformar em conhecimento, dialoga com a sua cultura, seus valores e princípios, seu modo de ser e sua maneira de ver e compreender o mundo. O conhecimento, nesse caso, é subjetivo (inerente ao sujeito), mas ao mesmo tempo social, pois o ser humano interage com o mundo que o circunda, modificando-o e sendo por ele modificado. Nem toda informação existente em um documento vai se transformar em conhecimento, pois quem aprende precisa ter os elementos fundamentais para a decodificação da informação, ou seja, fazer a correlação dessa informação com as estruturas mentais e conhecimentos correlatos mínimos que possibilitarão o entendimento

> e, se for o caso, a geração de novos conhecimentos. (LIMA & ALVARES. 2012 p. 25).

No meio computacional pode se usar a informação de diferentes modos: produzir, reproduzir, transmitir, armazenar, utilizar, acessar e proteger.

> Uma distinção fundamental entre dado e informação é que o primeiro é puramente sintático e a segunda contém necessariamente semântica (implícita na palavra "significado" usada em sua caracterização). [..] É interessante notar que é impossível introduzir e processar semântica em um computador, porque a máquina mesma é puramente sintática (assim como a totalidade da matemática). (SETZER,2001. p 2).

A confidencialidade tem como principal característica a privacidade das informações, garante que os dados de uma determinada empresa, instituição, processo ou pessoa não seja divulgada sem determinada autorização.

Para Galvão (2015), confidencialidade representa a garantia que a informação estará acessível somente para a pessoa autorizada. Se uma pessoa sem autorização tem conhecimento, ocorre uma violação de privacidade.

A Integridade garante que nenhuma interferência externa na hora de transmitir os dados entre emissor e receptor irá ser comprometer ou danifica, as principais características são precisão, consistência e confiabilidade das informações.

Logo, Palma (2016) diz que, a integridade é um pilar essencial para os processos de negócio, onde informações corrompidas geram grandes problemas, ou também, necessidade de correção e retrabalho quando tratadas em tempo.

A disponibilidade está associada a acessibilidade dos dados, tornando-os disponíveis a qualquer momento por um usuário autorizado.

De acordo com Galvão (2015), disponibilidade é a garantia de que, quando as pessoas autorizadas solicitarem alguma informação, estas estejam disponíveis.

3 História do Automóvel

> Com a crise do cavalo, pela influência do processo de industrialização do séc. XVIII, e com as demandas do transporte a dispararem a nível dos preços, a alimentação do cavalo começou a competir com a alimentação humana, fazendo com que o custo da sua manutenção aumentasse. (Freyssenet, 2011).

Várias experiências e invenções nos séculos XVII e XVIII foram realizadas como oportunidade econômica, numa resposta à crise do sistema de transporte a cavalo, promovendo a atividade comercial no sector dos transportes. Foi através de investidores particulares, que começaram a comprar motores de vários fornecedores disponíveis na época, que se consolidou o desenvolvimento tecnológico do automóvel(...). Deste modo, podemos constatar que entre o séc. XVII e o séc. XVIII a evolução tecnológica do automóvel se deve basicamente ao desenvolvimento da ciência, predominantemente através da física e da química, com o intuito de uma aplicação para assuntos técnicos e econômicos (...) portanto, a crise da indústria cavalar configurando uma mudança ambiental na mobilidade que irá produzir consequências ao nível dos transportes, gerando a criação de variáveis para uma resolução da sua eficácia na Revolução Industrial.(JESUS, Pedro; CORREIA, Ericê. 2016. P 92).

No início do século 19 é que os automóveis começaram a ter aplicação prática e comercial, como carruagens a vapor. Nessa época, esse novo meio de transporte, já rodava em Paris, Inglaterra e Escócia(...). Por outro lado, em meados do século 19, as carruagens a vapor já não eram novidade, mas eram pesadas, caras e perigosas. Perdiam a preferência para as tradicionais de tração animal, nos transportes urbanos(...). Os primeiros carros com motores de combustão interna surgiram nos anos 1860. Foram experiências realizadas por Étienne Lenoir, na França, e Siegfried Marcus, na Áustria. Mas somente por volta de 1890 começaram a ganhar o mercado, com modelos de Karl Benz e Gottlieb Daimler, na Alemanha. Nos anos seguintes a Panhard & Levassor, da França, destacou-se na produção desse tipo de veículo(...). Em junho de 1903, Henry Ford fundou a Ford Motor Company. O primeiro carro dessa nova empresa chamava-se Model A, tinha dois cilindros e potência de 8 cv, destinava-se ao uso diário de negócios ou recreativo. Em 1904, produziu também o Model B, de quatro cilindros, um automóvel de passeio(...). Nos anos seguintes, a indústria

automobilística tomou grande impulso com os novos processos de produção em série. As cidades passaram a construir largas avenidas para os carros e bondes. Nos anos 1920, os carros deixaram de ser curiosidade e faziam parte da paisagem urbana. (BACELAR).

Vemos que a revolução automobilística se deu por conta da crise no auge da Revolução Industrial, onde fomentou ainda mais a mudança nos meios de transportes na época, a evolução foi muito rápida desde veículos a vapor até o primeiro movido a combustão, notamos também que não só com os veículos, mas com as ruas e paisagens começaram a mudar para se adaptar aos veículos que estavam em desenvolvimento, assim como o ambiente, cidades, e toda uma infraestrutura se prepara para atender aos requisitos que os automóveis irão solicitar conforme novas tecnologias vão sendo integradas a eles.

3.1 Os automóveis inteligentes

Os carros autônomos ou inteligentes não são uma coisa tão nova assim, a muito tempo atrás já se pensa em projetos desse tipo, seja com a motivação de salvar ou melhorar a vida do condutor e passageiros. O primeiro projeto de veículos que podem ser definidos desta forma, data de 1968, a empresa alemã Continental, fabricante de pneus, automatizou uma Mercedes para acompanhamento de testes e desenvolvimento de seus produtos, o veículo era equipado com alguns sensores que seguiam um cabo de aço na pista e câmeras que enviavam as informações a um centro de controle para análise das situações que estavam ocorrendo, o modelo ainda não contava com seguidores de faixas, detecção de objetos e outras tecnologias existentes hoje nestes veículos, mas já experimentava a incorporação de sensores que apontavam qual comportamento deveria ser tomado pelo mesmo.

A Figura 1 ilustra a conexão de sensores e sistemas de diversos tipos e objetivos em um sistema maior, que é o carro autônomo:

Figura 1 - Carro inteligente

Fonte: BBVA, 2019.

A preocupação no desenvolvimento destes veículos sempre existiu, mas uma coisa que somente a pouco tempo tem sido levada em consideração e em seu correto grau de importância é a questão da segurança digital. Segundo Zanni, existem estudos que apontam a estimativa de viagens seguras acima dos 200 km/h em carros deste tipo, sem dúvidas um ataque que permita o controle de um veículo nessas condições, uma vez que seja mal-intencionado, pode resultar em além de danos físicos, provocar também na perda de vidas, então devemos sim considerar que, a segurança de dispositivos pode influenciar sim na segurança das pessoas fora do mundo digital.

Segundo Zanni, dois programadores no ano de 2013, conseguiram através de um software e um notebook conectados a um Ford Scape e um Toyota Prius, controlar aceleração, freios e em baixas velocidades controlar o volante dos carros ocasionando pequenos socos no volante. Na Figura 2, são demonstradas as atividades que puderam ser desenvolvidas ao controle do Ford Scape e Toyota Prius:

Figura 2 - Invasão a carros inteligentes

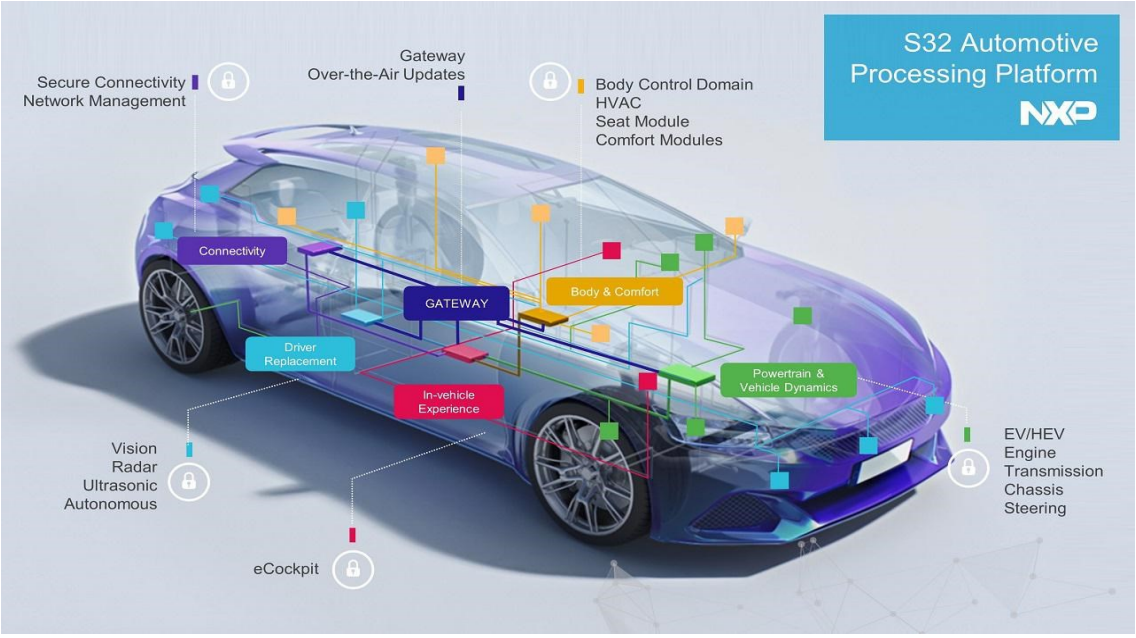
Fonte: Galileu, 2014

Segundo Gomes, os automóveis de hoje precisam tanto de processadores e componentes semicondutores como de pneus para poderem funcionar devidamente.

Segundo Gomes, desde a gestão do motor aos sistemas de entretenimento, sem esquecer os assistentes à condução, o funcionamento do automóvel passa obrigatoriamente por esses pequenos “cérebros” eletrônicos.

Abaixo a Figura 3, apresenta os diversos sistemas presentes em um veículo que são controlados por sistemas informatizados:

Figura 3 - Sistemas informatizados em um veículo



Fonte: Razão Automóvel, 2021

É comum pensarmos que ataques a veículos inteligentes ou autônomos envolverão sempre a manipulação física do veículo, podemos pensar em roubos em massa ou a ilegibilidade das informações provenientes dos sensores presentes nestes veículos ou simplesmente ataques visando apenas causar acidentes. De fato, estas e mais operações são possíveis, como já vistos em exemplos citados acima, mas ainda existem outros riscos, que não perceberíamos ao volante imediatamente.

Em veículos que necessariamente demandam conexão com a rede, seja para orientação dele mesmo em trânsito, ou para qualquer outra tarefa que seja desempenhada. Todos os componentes são integrados a muitos sistemas que aumentam as habilidades de navegação por meio de geolocalização, armazenamento e processamento de dados. No entanto, eles ainda apresentam riscos elevados de exposição a ameaças, portanto, essas preocupações criam um forte apelo aos pesquisadores, para compilar e analisar ataques que já visam carros autônomos.

É necessário que, toda a aplicação voltada a propósitos como controle de veículos e conexão com serviços externos, seja considerada como critica.

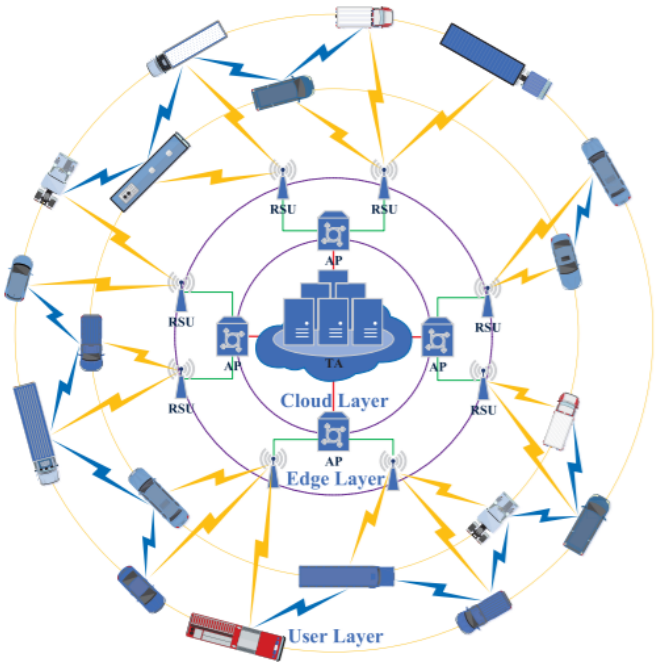
4 Funcionamento de uma Rede VANET

Uma VANET (Veicular Ad Hoc Network) é uma rede móvel distribuída onde dispositivos móveis trocam informações em tempo real.

> As redes ad hoc veiculares (VANETs) são definidas como redes sem fio distribuídas e auto-organizadas construídas por entidades veiculares heterogêneas, como veículo e Road-Side Units (RSUs). Geralmente, o VANET permite a comunicação dinâmica em tempo real com troca de dados duradoura entre os dispositivos participantes, o que pode facilitar drasticamente o aprimoramento da segurança no trânsito e a experiência de direção. (Tan, Haowen e Chung, Liyong .2020. V8. P 2482).

Uma VANET possui 3 itens básicos para sua estruturação, são eles: *Trusted Authority* (TA), *Road-Side Units* (RSUs) e os veiculos. A Figura 4, mostra de forma pratica a composição desta rede.

Figura 4 - Os elementos de uma VANET



Fonte: Secure Authentication and Key Management With Blockchain in VANETs, 2020.

4.1.1 *Trusted Authority* (TA).

Segundo Tan e Chung (2020), a TA atua como o provedor de serviços de nível superior e servidor de chaves central confiável responsável por todo o

sistema VANET. Portanto, as principais operações do sistema, como atribuição de parâmetros do sistema, registro de usuários, organização de grupos de veículos, juntamente com o gerenciamento de usuários e a verificação necessária para veículos correlacionados, são realizadas pela TA.

Os dados veiculares massivos de todas as VANETs legítimas são agregados e analisados pelo TA, por essa grande quantidade de informação ser tão massiva é utilizado de muita capacidade de armazenamento e processamento, com a chegada do avanço da rede 5G e armazenamento em nuvem, o fluxo de dados para este tipo de ação vem se tornando mais viável, fazendo com que a computação (processamento) e armazenamento sejam garantidos.

Tan e Chung (2020) também nos dizem que, além disso, os servidores em nuvem distribuídos podem gerenciar a interação entre várias VANETs simultaneamente, o que acelera a formação da iniciativa da Internet mundial do veículo (IoV).

4.1.2 *Road-Side Units* (RSUs).

> São definidas como as instalações distribuídas estabelecidas ao longo as estradas em intervalos fixos[...], a fim de fornecer serviços aos veículos visados, os alcances efetivos das RSUs fixas devem cobrir todas as seções da estrada. Cada RSU é responsável pela comunicação direta com os veículos em sua vizinhança. (Tan, Haowen e Chung, Liyong .2020. V8. P 2483).

De acordo com Tan e Chung (2020), o acesso as VANETs para os veículos só pode ser feito por meio das RSUs próximas a eles, e os veículos sendo a principal entidade das VANETs atuam tanto como usuários do terminal quanto como principal fonte de informação veicular.

> Dados de veículos heterogêneos massivos e características da estrada em tempo real, como congestionamento de tráfego e relatórios de acidentes, são adquiridos de forma colaborativa pelos veículos [...]. Os dados agregados são posteriormente carregados no servidor central VANET para posterior análise e gerenciamento. (Tan, Haowen e Chung, Liyong .2020. V8. P 2483).

Para que toda essa comunicação aconteça, segundo Tan e Chung (2020), todos os veículos estão equipados com uma unidade de bordo, On-Board Unit

(OBU), de forma que esses são implementados os módulos de comunicação sem fio (transceptores e transponders), a OBU é responsável por lidar com toda transmissão e recepção dos dados em alta mobilidade.

4.1.3 Veículos.

Por fim temos o último elemento da estruturação de uma Vanet, que são os próprios veículos. Segundo Tan e Chung (2020), o que valida a interação entre veículos é a comunicação V2V (*vehicle-to-vehicle),* e toda estrutura de redes veiculares sem fio auto-organizadas, envolvendo vários veículos de determinada vizinhança, podem ser construídas dessa maneira, oferecendo oportunidades para troca e agregação de dados em tempo real.

> Em cenários práticos de VANET, a troca de dados vitais de conexões V2V e V2R é realizada em ambiente sem fio aberto. As informações veiculares transmitidas podem ser interceptadas ou forjadas por entidades maliciosas, resultando em graves vulnerabilidades a várias ameaças de segurança e riscos de privacidade. As informações de chave importantes e os segredos do usuário podem ser revelados ilegalmente. Todo o sistema VANET pode ser comprometido desta forma. Nessa circunstância, é necessário implantar mecanismos eficazes de preservação da segurança e proteção da privacidade nas VANETs. (Tan, Haowen e Chung, Liyong .2020. V8. P 2483).

5 As desconexões e conexões em massa em uma VANET

Segundo Baza et. al. (2020), um dos principais objetivos de uma VANET é melhorar as condições de tráfego e segurança dos usuários de forma eficiente garantindo que a comunicação e condições necessárias para seu correto funcionamento estejam disponíveis sempre.

As redes pelas quais os veículos se comunicam podem ser consideradas a base e a principal ligação entre o funcionamento de todos os sistemas que estão presentes nos veículos conectados a estas redes. Nelas, cada veículo é um nó de comunicação, recebendo e enviando mensagens a todo momento a outros veículos que estejam próximos ou que estejam conectados a um mesmo grupo, uma vez que esta comunicação é repleta de condições especiais, é necessário que exista um controle rígido das operações e segurança das informações trafegadas na mesma, dado que este tipo de rede é considerado um serviço crítico.

Fernandes et. al. (2021), afirma que 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 segurança é um fator diretamente ligado a veracidade das informações que são fornecidas pelos nós presentes na rede. Uma informação incorreta pode ocasionar uma tomada de decisão errada pelo algoritmo e sistemas que controlam os veículos e consequentemente, causar acidentes. Por conta disso, a segurança nestes veículos se baseia nos mesmos princípios da segurança da informação, até porque, estamos falando diretamente da segurança e integridade dos dados e das informações presentes nas VANETs.

Fernandes et. al. (2021), afirma que 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.

Feng et. al. (2017), define que para isso, é fundamental que os nós da rede tenham confiança nas informações trocadas com seus vizinhos, pois decisões tomadas com base em informações erradas ou manipuladas podem levar a diminuição da segurança no trânsito.

6 Blockchain

Para lidar com estas questões, estas redes podem contar com um recurso já muito utilizado em transações virtuais, como criptomoedas por exemplo.

> 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. (Fernandes, Claudio Piccolo. et. al. 2021. P265).

Lamounier, afirma que, a tecnologia Blockchain revolucionou o mundo à sua maneira. Isso tornou o mundo mais seguro e garantiu que quase todos os setores se beneficiassem dele.

Mas, inicialmente é necessário que entendamos o que ele é e como ele funciona.

> 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. (Fernandes, Claudio Piccolo. et. al. 2021. P260).

O Blockchain pode ser entendido como uma espécie de livro, onde são registradas todas as transações em andamento, de forma que seja possível fazer o rastreamento de todos os ativos, neste caso entendemos os ativos como os dados e informações em processamento e em transmissão e os veículos ou dispositivos presentes nestes, responsáveis pela comunicação nas VANETs. Estes livros ou registros são compartilhados e imutáveis, como todos os registros são de conhecimento de todos os nós e todos podem ser negociados, os riscos se tornam iguais para todos os nós, resolvendo o problema da confiança entre eles.

Estes registros não ficam com um único detentor dos dados, eles são distribuídos entre os nós da rede, ou seja, não existe um centro de processamento. Isso aumenta a velocidade do tráfego das informações.

Como dito acima, algumas características das VANETs são: alta mobilidade, topologia dinâmica e desconexões frequentes, por conta disso é necessário que os dados trafeguem rapidamente entre os nós, para que a rede possa informar aos nós quem faz parte dela e quem não faz, a quem os pacotes devem ser entregues e quando. O fato de todos os nós deterem estas informações torna o processo corrente em tempos aceitáveis. Imagine a falha na comunicação em uma estrada de alta velocidade. Os danos seriam catastróficos.

O blockchain é transparente, auditável. A imutabilidade dos blocos consiste no fato das transações serem realizadas em blocos, e caso um bloco seja alterado, todas as transações resultantes deste bloco são invalidadas. Os blocos mesmo após seu processamento seguem armazenados e conhecidos por todos os nós do grupo. Contudo, é necessário saber que existem basicamente quatro tipos de configurações de blockchain, para que então se possa escolher um modelo que lide da maneira mais adequada em relação ao problema proposto, o gerenciamento das conexões e tráfego de informações. São eles:

- Blockchain Público;
- Blockchain Privado;
- Blockchain de consórcio ou federado;
- Blockchain autorizado.

A Figura 5 ilustra as particularidades de cada modelo de blockchain.

Figura 5 - Comparação dos tipos de Blockchains

Tipos de Blockchain			
Particularidade	**Publica**	**Privada**	**Consórcio**
Sem necessidade de permissão?	Sim	Não	Não
Quem pode ler?	Qualquer um	Apenas usuários convidados	Depende
quem pode escrever?	Qualquer um	Participantes aprovados	Participantes aprovados
Proprietário	Ninguém	Uma única entidade	Multiplas entidades
Participantes conhecidos?	Não	Sim	Sim
Velocidade das transações	Lenta	Rápida	Rápida

Fonte: Adaptação, BINANCE ACADEMY, 2020.

6.1.1 Blockchain Público

O blockchain público é bem conhecido no mundo das criptomoedas, é um modelo com funcionamento aberto, ou seja, não existem restrições de entrada quanto aos nós que desejam participar da rede. Tem seu funcionamento de forma descentralizada, e todos os membros têm participações igualitárias neste modelo.

Ele não é a melhor aplicação para o tema deste trabalho, visto que como não existe uma entidade verificando as negociações na rede, o processo de aceite ou rejeição é mais lento. Entretanto, é o mais transparente, uma vez que todos os nós presentes na rede são responsáveis pela fiscalização uns dos outros.

6.1.2 Blockchain Privado

O Blockchain privado, é justamente o contrário do modelo público, este é centralizado em relação ao acesso e visualização das informações que são trafegadas na rede pelos nós, ou seja, apenas um nó autorizado pode ter acesso aos dados e informações. Outro ponto que reforça a segurança nesse modelo é a capacidade do sistema gerenciar informações para que apenas nós participantes de uma negociação especifica tenham acesso aos dados específicos desta negociação. Como existe uma centralização em relação a autorização a velocidade de negociação neste modelo é maior.

Segundo Hoinaski, é uma ótima forma de fazer o controle de entrada e de governança, mas ainda assim manter a estrutura da tecnologia blockchain. E, claro, aumentar a agilidade das transações.

6.1.3 Blockchain de consórcio ou federado

O blockchain de consórcio ou federado, surgiu da demanda de criação de um modelo que une as características dos modelos citados acima, ele é descentralizado e transparente, no entanto existem entidades que controlam o acesso dos nós aos grupos e transações.

6.1.4 Blockchain autorizado

O blockchain autorizado segue basicamente o mesmo conceito do modelo federado, entretanto, neste, existe apenas uma autoridade responsável pela autorização dos nós, e para a entrada deles na rede é necessário que respeitem alguns critérios específicos, este é geralmente utilizado em transações B2B.

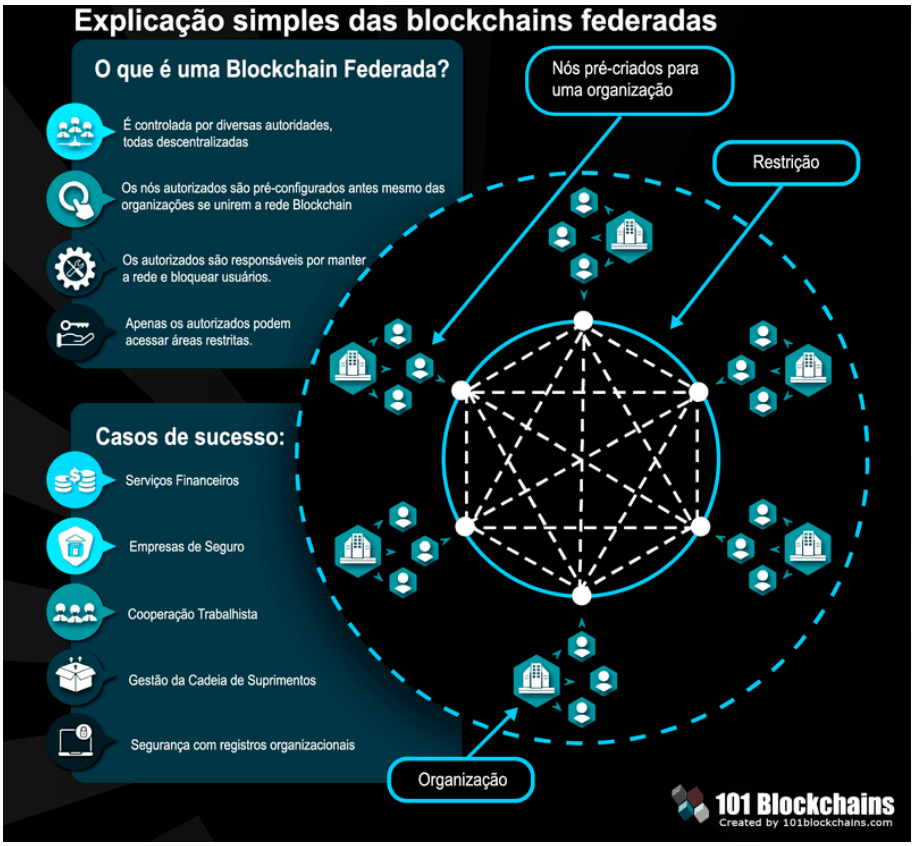
7 O modelo mais adequado a este propósito – Blockchain Federado

Também chamado de blockchain de consórcio, este é o modelo que mais se aplica ao gerenciamento de informações e conexões em uma rede VANET.

Hoinaski, evidencia que, neste meio existem diversas entidades responsáveis pelo controle de acesso e privacidade das transações, no caso existe então, um grupo responsável por determinar quais grupos terão acesso a quais informações e quando, essas definições são aplicadas através dos mecanismos de consenso.

Abaixo, na Figura 6 , Hoinaski apresenta em um infográfico uma explicação mais simples deste modelo.

Figura 6 - Explicação da blockchain federada



Fonte: Blog Ibid, 2021.

> A blockchain do consórcio é o meio termo entre as cadeias públicas e privadas, combinando elementos de ambas. A principal diferença de qualquer um dos sistemas pode ser observada no nível de consenso. Em vez de um sistema aberto em que qualquer um pode validar blocos ou um sistema fechado em que apenas uma única entidade nomeia validadores de blocos, uma cadeia de consórcios funciona com um grupo de participantes igualmente poderosos trabalhando como validadores. (BINANCE ACADEMY, 2020).

Entendendo este ponto, as regras para participação em um grupo devem ser definidas e implementadas no algoritmo de consenso que por sua vez é o responsável por fazer a aprovação dos nós entrantes na rede e caso um nó seja rejeitado ele não teria autorização para participar da rede e obviamente não compartilharia dos dados trafegados na mesma.

> Deve haver uma forma coordenada em que todas as transações sejam validadas e os nós participantes cheguem a um acordo em relação ao estado da rede. Daí surgem os chamados mecanismos de consenso, que são as regras e os procedimentos pelos quais os nós de uma rede distribuída concordam em validar transações. Importante notar que acréscimos no livro-razão só são feitos se as regras ditadas pelo mecanismo de consenso forem seguidas por todos. Especificamente em uma rede blockchain, o consenso é obtido por meio da convergência dos nós em direção a uma versão única e imutável do livro-razão. O mecanismo de consenso é responsável por permitir que os atores ou nós da rede concordem entre si com o conteúdo a ser armazenado na blockchain, levando em consideração o fato de que alguns atores podem ser maliciosos ou estar indisponíveis. (TCU. 2020, P14).

É importante entender que o blockchain é uma tecnologia que, embora garanta a transação segura de dados, no entanto, não existe uma receita pronta para a implantação. O mesmo ocorre com o algoritmo de consenso, no modelo de aplicação proposto nesse trabalho, cada órgão de trânsito deverá estar diretamente ligado aos órgãos provedores de tecnologia de seu país ou região para que sejam definidas as regras e feita a implantação.

> As cadeias de consórcio atenuam alguns dos riscos de contraparte de uma cadeia privada (removendo o controle centralizado) e um número menor de nós geralmente permite que elas tenham um desempenho muito mais eficaz que uma cadeia pública. Os consórcios provavelmente atrairão organizações que desejam otimizar a comunicação entre si. (BINANCE ACADEMY, 2020).

O resultado da aceitação de um nó é a geração de um bloco contido em um contrato digital.

> Contratos inteligentes, ou smart contracts, são código-fonte em linguagem de programação (scripts), que podem ser definidos e auto executados em uma infraestrutura de blockchain ou DLT. A definição e execução de um contrato inteligente nesses ambientes se dá sem a necessidade de intermediários. (TCU. 2020, P15).

Ainda segundo Szabo, um contrato inteligente pode ser caracterizado pelo atingimento de quatro objetivos principais: observabilidade, verificabilidade, privacidade e obrigatoriedade. Além de prover algumas outras vantagens.

> A utilização de contratos inteligentes provê as seguintes vantagens:
>
> a. transparência: contratos inteligentes podem ser escritos e verificados a qualquer momento por todas as partes envolvidas, que podem verificar o código-fonte do contrato;
>
> b. menor prazo para execução: a eliminação dos passos manuais torna a execução do contrato mais rápida e eficiente;
>
> c. precisão: como o contrato é descrito por um algoritmo computacional, sua execução é precisa, salvo se houver erro de programação;
>
> d. segurança: a infraestrutura de DLT garante a segurança em contratos inteligentes, que são assinados por chaves criptográficas e não podem ser violados por terceiros sem permissão de acesso;
>
> e. rastreabilidade: os dados de cada execução das “funções” do contrato ficam armazenados na DLT, permitindo que a execução do contrato seja auditável a qualquer tempo;
>
> f. menor custo: por sua natureza digital e em razão da eliminação de intermediários, os contratos inteligentes reduzem os custos de execução;
>
> g. confiança: as características citadas acima levam à maior confiança entre as partes envolvidas no contrato. (TCU. 2020, P16).

Além de todos os pontos supracitados a tecnologia Blockchain, independentemente do tipo utiliza criptografia para a proteção dos dados.

> Soluções baseadas em blockchain utilizam intensivamente técnicas tradicionais de criptografia para garantir a integridade das informações armazenadas. Como exemplo, pode-se citar a utilização de algoritmos criptográficos de chaves públicas, funções de hash e assinaturas digitais. (TCU. 2020, P17).

8 Conclusão

De fato, a indústria automotiva anda de braços dados com a tecnologia da informação nos dias de hoje, a necessidade das pessoas em estarem conectadas é cada vez maior e evidentemente os veículos que são utilizados seguem este mesmo caminho, e consequentemente a segurança das informações deve ser assegurada.

Com base nos estudos feitos para a construção deste trabalho, entendemos que, o assunto das conexões em uma rede VANET, e o tratamento dos dados e dos acessos a eles pode de fato ser feito através do uso do blockchain, no entanto, é necessário entender que essa é uma tecnologia ampla e relativamente complexa, se levarmos em consideração que a aplicação no tratamento e gerenciamento das conexões deve respeitar as características tecnológicas e porque não dizer sociais de uma região, visto que, regras de transito e tipos de vias por exemplo tem impacto no algoritmo a ser configurado, teremos diversos algoritmos sendo executados e gerenciando tudo isso de formas possivelmente diferentes e como dito acima, com características diferentes.

Entendemos que atualmente, pelo menos no Brasil, lugar no qual vivemos, ainda não teríamos condições de implantar tal tecnologia, incialmente por conta de custos operacionais, idade da frota, pois neste caso temos que considerar que, cada automóvel que utilize esta tecnologia é um nó ou ainda melhor dito, é um dispositivo conectado, que gera, recebe e envia dados para todos os outros.

O Blockchain é uma tecnologia disruptiva, que trabalha de forma diferente da grande maioria dos sistemas, podemos ou não ter uma centralização dos dados e a autorização dos nós participantes, pode ou não ser feita de formas diferentes, no caso deste trabalho, acreditamos que o modelo mais adequado é de fato o modelo de consórcio, se observarmos a Figura 6 - Explicação da blockchain federada, observamos que tal modelo pode ter um grupo autorizador, inicialmente, ou seja, somente grupos adjacentes a este poderiam homologar nós candidatos a participação de outros grupos, podemos ainda dizer que, um grupo principal, pode ser o órgão regulador de transito e os grupos subjacentes

poderiam ser as montadoras, é possível inclusive fazer a seguinte analogia: atualmente cada veículo possui uma numeração de chassis, que diz respeito a montadora, país de fabricação, modelo do veículo e quando foi fabricado e este número é único, neste mesmo sentido, poderíamos sugerir que, veiculos capazes de se comunicar em rede, passariam a ter endereços MAC, visto que é um número de identificação de hardware que identifica exclusivamente cada dispositivo em uma rede.

A aplicação de tal tecnologia, como citado neste trabalho é dependente de outras conexões e tecnologias disponíveis em cada lugar. Podemos citar tecnologias como GPS, 4G ou 5G e diversas outras. E, com base em tudo que foi apresentado no capítulo 8 deste trabalho, entendemos que a blockchain tem sim, capacidade de suprir as necessidades impostas pelas redes VANET, pois tem condições de lidar com conexões e desconexões frequentes, trafego de informações de forma confiável e auditável por todos e autorização ou desautorização de nós que desejam ter acesso aos dados que estão sendo trafegados na rede, além de respeitar os 3 pilares da segurança da informação: confidencialidade, integridade e disponibilidade.

9 Referencias

Así serán los automóviles del futuro: las tecnologías que marcan el camino. **BBVA**, 2019. Disponível em: < https://www.bbva.com/es/sostenibilidad/asi-seran-automoviles-futuro-tecnologias-marcan-camino/> Acesso em: 01 de setembro de 2021.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR 17799: Tecnologia da informação — Técnicas de segurança — Código de prática para a gestão da segurança da informação**. Rio de Janeiro. 2005.

BACELAR, Jonildo. **Guia geográfico, História do Automóvel**, disponível em: https://www.guiageografico.com/temas/historia-automovel.htm acesso em: 24 de outubro. 2021.

Baza, M., Nabil, M., Mahmoud, M. M. E. A., Bewermeier, N., Fidan, K., Alasmary, W.,and Abdallah, M. (2020**). Detecting sybil attacks using proofs of work and location in vanets**. IEEE Transactions on Dependable and Secure Computing.

Blockchains Privadas, Públicas e de Consórcios - Qual a Diferença?. **BINANCE ACADEMY**, 2020. Disponível em: < https://academy.binance.com/pt/articles/private-public-and-consortium-blockchains-whats-the-difference#consortium-blockchains> Acesso em: 01 de setembro de 2021.

Chrysler faz recall de 1,4 milhão de carros vulneráveis a hackers . **VEJA**, 2015. Disponível em: < https://veja.abril.com.br/tecnologia/chrysler-faz-recall-de-14-milhao-de-carros-vulneraveis-a-hackers/> Acesso em: 01 de setembro de 2021.

CUNHA, Murilo Basto da. **Dicionário de Biblioteconomia e Arquivologia**. Brasília: Briquet de Lemos Livros, 2008. 451p.

DEMARTINE, Felipe. Ataques a carros inteligentes são “questão de tempo”, diz especialista. **Canaltech**, 2021. Disponível em: <

https://canaltech.com.br/carros/ataques-a-carros-inteligentes-sao-questao-de-tempo-diz-especialista-180833/>. Acesso em: 01 de setembro de 2021.

Fabricantes de automóveis aumentarão investimentos para proteger veículos de ataques de hackers. **Future**, 2021. Disponível em: < https://www.future.com.br/fabricantes-de-automoveis-aumentarao-investimentos-para-proteger-veiculos-de-ataques-de-hackers/> Acesso em: 01 de setembro de 2021.

Feng, X., Li, C.-y., Chen, D.-x., and Tang, J. (2017). **A method for defensing**

Fernandes, Claudio Piccolo. et. al. **Blockchain e Sistemas de Reputação em Redes Veiculares: Uma Revisão Sistemática**. XII Computer on the Beach, 2021.

Fernandes, José Henrique Cabral, 2011. **Introdução à gestão de riscos de segurança da informação**, Artigo, p. 13, São Paulo, CEGSIC 2009-2011, 2011.

FREYSSENET, Michel. Lo más dudoso no es lo más improbable: el coche eléctrico: la nueva revolución del automóvil. In: **JORNADA INTERNACIONAL 'MOVILIDAD SOSTENIBLE Y VEHÍCULO ELÉCTRICO, EL MOTOR DE LA INNOVACIÓN LOCAL'**. Anais...Valladolid, Espana: Fundación San Pablo Castilla y León. 2011.

FROTA, M. N., FROTA, M. H. A. **Acesso à informação: estratégia para a competitividade**. Brasília: CNPQ/IBICT, FBB, 1994. 188p.

GALVÃO, Michele da Costa. **Fundamentos em Segurança da Informação**. São Paulo: Person Education do Brasil, 2015.

GOMES, Fernando. Falta de processadores está a estagnar produção automóvel. Razão Automóvel, 2021, disponível em: < https://www.razaoautomovel.com/2021/02/falta-de-processadores-esta-a-estagnar-producao-automovel#:~:text=Os%20autom%C3%B3veis%20de%20hoje%20precisam,es

ses%20pequenos%20%E2%80%9Cc%C3%A9rebros%E2%80%9D%20eletr%C3%B3nicos.> acesso em: 24 de outubro. 2021

H. Tan and I. Chung, "Secure Authentication and Key Management With Blockchain in VANETs," in *IEEE Access*, vol. 8, pp. 2482-2498, 2020, doi: 10.1109/ACCESS.2019.2962387.

HOINASKI, Fábio. TIPOS DE BLOCKCHAIN: QUAL O MELHOR PARA A CADEIA DE SUPRIMENTOS? **Blog Ibid**, 2021. Disponível em: < https://www.ibid.com.br/blog/tipos-de-blockchain-qual-o-melhor-para-a-cadeia-de-suprimentos/?msclkid=410f47d4ae0511ecb779f33c7a3ad765> Acesso em: 23 de março de 2021.

JESUS, Pedro R. R. C.; CORREIA, Ericê B. **Uma visão histórica da evolução tecnológica do automóvel.** Recife: v. 25, n. 2, 91-101, jul./dez. 2016

LAMOUNIER, Lucas. Blockchain Hibrida: O Melhor De Dois Mundos. **101Blockchains,** 2019. Disponível em < https://101blockchains.com/pt/blockchain-hibrida-explicado/> Acesso em: 01 de setembro de 2021.

LIMA, José Leonardo Oliveira; ALVARES, Lillian. Organização e representação da informação e do conhecimento. In: ALVARES, Lillian et al. (Org.). **Organização da informação e do conhecimento: conceitos, subsídios interdisciplinares e aplicações**. São Paulo: B4, 2012. p. 21-48.

O desafio da segurança digital nos carros autônomos. **Estadão**, 2020. Disponível em: < https://summitmobilidade.estadao.com.br/carros-autonomos/o-desafio-da-seguranca-digital-nos-carros-autonomos/>. Acesso em: 01 de setembro de 2021.

O que é a tecnologia Blockchain. **IBM**, 2022. Disponível em: < https://www.ibm.com/br-pt/topics/what-is-blockchain>. Acesso em: 06 de março de 2022.

RIBEIRO, Felipe. Foxconn diz que fabricará carros elétricos nos EUA a partir de 2023. **Canaltech**, 2021. Disponível em:

<https://canaltech.com.br/carros/foxconn-diz-que-fabricara-carros-eletricos-nos-eua-a-partir-de-2023-192564/ >. Acesso em: 01 de setembro de 2021.

Segurança digital de veículos, **TEN Sistemas de Redes,** 2018. Disponível em < https://ten.com.br/seguranca-digital-de-veiculos/> Acesso em: 27 de fevereiro de 2022.

Setzer, Valdemar W,2001. **Dado, Informação, Conhecimento e Competência**, Artigo, p. 14, São Paulo, Depto. de Ciência da Computação, 2014.

TRIBUNAL DE CONTAS DA UNIÃO. **SUMARIO EXECUTIVO – LEVANTAMENTO TA TECNOLOGIA BLOCKCHAIN**. BRASILIA. 2020.

Veículos autônomos têm pelo menos 50 pontos de ciberataque, **itforum,** 2018. Disponível em <https://itforum.com.br/noticias/veiculos-autonomos-tem-pelo-menos-50-pontos-de-ciberataque/> Acesso em: 01 de setembro de 2021.

Veículos autônomos: São o futuro?. **HS Consultoria**, 2020. Disponível em: < https://www.hshabilitacaosuspensa.com.br/blog/veiculos-autonomos-sao-o-futuro/> Acesso em: 01 de setembro de 2021.

ZANINI, Marco. Carros Inteligentes. **Galileu,** 2014. Disponível em <https://revistagalileu.globo.com/Revista/noticia/2014/01/carros-inteligentes.html> Acesso em: 01 de setembro de 2021.