



ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS

CAP COM CARLOS HENRIQUE DIAS DE OLIVEIRA

**TECNOLOGIA BLOCKCHAIN: POSSÍVEIS IMPACTOS NA UTILIZAÇÃO EM
SISTEMAS DE INFRAESTRUTURAS CRÍTICAS PELO EXÉRCITO
BRASILEIRO**

**Rio de Janeiro
2019**



ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS

CAP COM CARLOS HENRIQUE DIAS DE OLIVEIRA

TECNOLOGIA BLOCKCHAIN: POSSÍVEIS IMPACTOS NA UTILIZAÇÃO EM SISTEMAS DE INFRAESTRUTURAS CRÍTICAS PELO EXÉRCITO BRASILEIRO

Trabalho acadêmico apresentado à Escola de Aperfeiçoamento de Oficiais, como requisito para a especialização em Ciências Militares com ênfase em Educação e Cultura Militar.

**Rio de Janeiro
2019**

1. INTRODUÇÃO

O surgimento da tecnologia *blockchain* ou “o protocolo da confiança”, remonta ao ano de 2008 e está atrelado ao nascimento da criptomoeda *Bitcoin*. Esta moeda digital utiliza a tecnologia *blockchain* para assegurar a validade das suas transações e ser à prova de violação. Essas garantias conferem para esta inovação, o princípio da confiabilidade nas operações, permitindo com isso que duas pessoas que, não se conhecem, possam realizar transações de forma segura dentro do mundo digital, sem necessidade de um intermediador. Apesar do *blockchain* ter mais de dez anos de existência, foi nos últimos anos que essa técnica ganhou seu devido destaque, passando a ser considerada por muitos como a “quinta evolução” da computação (LAURENCE, 2019).

Basicamente, ela funciona como um livro-razão das transações computacionais, garantindo confiabilidade e transparência, validando essa operação, que fica armazenada na rede tornando-se muito difícil modificar seu registro. As áreas que essa tecnologia poderá atuar são amplas e variadas como: cartórios, mercado de propriedade intelectual, em uma cadeia de logística, no compartilhamento de dados no âmbito da Administração Pública Federal Brasileira, na segurança dos dados e em sistemas de infraestruturas críticas.

As infraestruturas críticas são definidas como instalações, serviços, bens, sistemas, que se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político e na segurança nacional ou internacional. São as grandes infraestruturas do país que, se atacadas, colocam em risco a segurança nacional.

1.1 PROBLEMA

Na Era da Informação os ataques em infraestruturas críticas são cibernéticos. A informação, é um ativo importantíssimo que deve ser bem protegido. Por isso, esta pesquisa é focada em sistemas de infraestruturas críticas da informação. Danos a essas infraestruturas podem causar situações graves, como por exemplo: sérios prejuízos a imagem da força e do Brasil; vazamentos de dados que envolvam a segurança nacional e nos casos mais graves, morte de pessoas.

Os sistemas de infraestruturas críticas da informação vêm aumentando sua quantidade com o avanço da tecnologia, tornando-se cada vez mais necessários e vitais. Por exemplo, um ataque ao sistema de infraestrutura energética nacional, pode causar um apagão e gerar graves danos ao País. Aprimoramentos no sistema podem

melhorar a confiabilidade e como consequência, aumentar a segurança desses recursos.

O tema apresentado foca principalmente no levantamento das vantagens e vulnerabilidades da tecnologia *blockchain*, para a utilização em sistemas de infraestruturas críticas da informação. Se as desvantagens, inviabilizam a utilização da mesma para sistemas de infraestruturas críticas pelo Exército Brasileiro. E devido a importância dessa tecnologia, levantar se os militares conhecem esse tema. Foram levantados dados/informações com o propósito de responder ao seguinte problema de pesquisa:

Em que medida e quais soluções tecnológicas do *Blockchain* podem favorecer na implementação de sistemas de infraestruturas críticas da informação?

1.2 OBJETIVOS

O presente trabalho tem como objetivo geral analisar as possíveis utilizações por militares do Exército Brasileiro das soluções tecnológicas do *Blockchain* na implementação de sistemas de infraestruturas críticas da informação do Brasil.

Nessa linha busca-se alcançar os seguintes objetivos específicos:

- a) identificar se os militares conhecem o que é o sistema de infraestruturas críticas da informação;
- b) identificar, a partir da opinião dos militares, seu conhecimento sobre a tecnologia *Blockchain* e de onde provem esse conhecimento; e
- c) conhecer e identificar, a partir da opinião dos militares, as vantagens e vulnerabilidades da tecnologia *Blockchain*.

1.3 JUSTIFICATIVAS E CONTRIBUIÇÕES

O que impulsionou a realização desse trabalho foi entender essa nova tecnologia. Apresentando conceitos e definições sobre esse tema e possíveis impactos no emprego desse método pelo Exército Brasileiro, com base nas concepções da tecnologia *blockchain* sendo empregadas em sistemas de infraestrutura críticas.

Devido a importância de sistemas de infraestruturas críticas e as possibilidades da tecnologia *blockchain*, essa pesquisa se justifica através da compreensão da

tecnologia *blockchain* em contribuição com a utilização pelo Exército Brasileiro em sistemas do Brasil. O conhecimento das vantagens pode melhorar a validação de operações e verificar os possíveis impactos de suas vulnerabilidades no emprego dessa tecnologia.

Este trabalho contribui para melhorar o processo de defesa desses sistemas fundamentais do Brasil. A melhora no processo, agrega princípios primordiais como: disponibilidade, integridade, confidencialidade e autenticidade.

Dessa forma essa pesquisa busca verificar a viabilidade do uso dessa tecnologia pelo Exército e seus possíveis impactos. Não se trata de um estudo que visa abordar todas as características e nuances e encerrar o assunto, pois se trata de uma técnica nova e ainda em crescimento. Deste modo, devido à dificuldade para encontrar materiais que versam sobre o assunto, busca-se levantar alguns impactos que poderiam ser causados, caso adotado esse método de validação em sistemas de infraestrutura críticos.

2 METODOLOGIA

Este projeto de pesquisa delimitou-se em colher informações sobre como a compreensão da vulnerabilidade da tecnologia *Blockchain* impacta na implementação de sistemas de infraestruturas críticas do Exército Brasileiro. Tem como referência artigos e pesquisas que versam sobre o *Blockchain*, sistemas de infraestrutura crítica e decreto da Política Nacional de Segurança de Infraestruturas Críticas - PNSIC. Com relação ao método, a pesquisa se estruturou na forma de quantitativo.

Na forma de abordagem do problema, utilizaram-se os conceitos da pesquisa quantitativa, para auxiliar a busca do objetivo geral questões foram utilizadas, quantificando as respostas obtidas através de questionários. Para Neves e Domingues (2007, p.54), “Elas são o ponto de partida para encontrar um caminho que leve ao melhor conhecimento acerca do problema, e são fundamentais para chegar a uma solução”.

Nesse estudo, será realizada uma pesquisa básica, visto que, avaliará novos fenômenos e seus fundamentos não estudados até o presente momento. Devido ao pouco conhecimento disponível acerca dos assuntos tratados nesse artigo, foi empregada a modalidade exploratória, necessitando uma pesquisa inicial e questionário para buscar o objetivo geral.

2.1 REVISÃO DE LITERATURA

Na busca de solucionar o problema de pesquisa, a revisão de literatura delimitou-se no período de 2009 a 2019. Essa delimitação se baseia no surgimento da tecnologia *Blockchain* até a data da produção deste artigo. Essa delimitação ganha importância devido principalmente a rápida evolução e surgimento de novas tendências, principalmente na área de tecnologia. Por ser um período recente ainda há poucos estudos sobre o tema que se encontra em constante evolução.

As palavras-chave utilizadas foram *blockchain*, SICI, segurança.

2.2 COLETA DE DADOS

Para o aprofundamento teórico sobre o assunto, foi utilizado o seguinte meio para a coleta de dados: questionário.

A amplitude do universo foi estimada a partir do efetivo de graduados e oficiais do Exército Brasileiro, retirado do site Defesa.gov (2019), ficando com uma população

de 85.824 militares da ativa. Com um nível de confiança aplicado de 90% e erro amostral de 10%, a amostra ficou em 44 militares da ativa.

2.2.1 Questionário

O questionário foi respondido por 46 militares voluntários, nele buscou-se identificar pessoal com conhecimento na área de TI, como por exemplo possuidores do Curso de Guerra Cibernética ou com formação na área, separando dos militares que não possuem conhecimento específico na área de computação, no período de 01 de julho de 2019 a 31 de julho de 2019.

No ANEXO B é possível verificar o desenho final das perguntas ecaminhadas aos militares do Exército Brasileiro. Ela foi estruturada em três partes mandatórias e a última parte opcional.

3. RESULTADOS E DISCUSSÃO

Decorrente do que foi visto, o protocolo de validação descentralizado gerará grandes mudanças. Trata-se, inegavelmente, de uma nova tecnologia que irá melhorar processos. Seria um erro, porém, implementá-la sem uma averiguação profunda e sem o levantamento de suas vulnerabilidades. Podemos verificar um exemplo de utilização dessa tecnologia, como no sistema de energia elétrica (TELLES, 2018). Assim, reveste-se de particular importância estudos sobre o tema. Sob essa ótica, ganha particular relevância o levantamento das vulnerabilidades e possíveis impactos na Infraestrutura Críticas do Exército Brasileiro.

Em seus livros alguns autores citados, enfatizam novas possibilidades de emprego e as vantagens de ser uma tecnologia descentralizada. Fica claro que casos concretos de aplicação, ainda são diminutos, pois se trata de uma tecnologia ainda em crescimento. Até a criptomoeda Bitcoin que foi a primeira a usar essa tecnologia está em evolução e ainda faltam estudos do impacto que essa moeda pode causar. Como bem nos assegura uma matéria publicada na revista On Line Editora (2007, p. 96) " Apesar de despertar o interesse e a curiosidade de muita gente, ainda é impossível imaginar quais serão de fato as grandes revoluções provocadas por sistemas que se utilizam do *blockchain*".

Para MOUGAYAR (2018) aborda a falta de aplicações maduras ainda:

Demora para aplicações novas emergirem quando uma nova tecnologia de base vem à tona. Em um caso extremo, quase qualquer aplicação de software poderia ser reescrita com um pouco de *blockchain* e descentralização, mas não significa que seja uma boa ideia. Talvez 2016 seja para o *blockchain* o que 1995 foi para o último estágio de proliferação de aplicações web. (MOUGAYAR, 2018, p. 72)

Parece óbvio que o autor, conforme explicado acima, relata uma grande possibilidade de utilização em todos os softwares, no caso extremo de uma previsão. Nesses casos, o benefício seria o melhoramento de processos, que nesse artigo são os sistemas de infraestrutura críticos. Porém, ele também enfatiza que isso pode não ser uma boa ideia. O autor deixa claro, que essa observação feita se baseia na ideia de verificar as vulnerabilidades que podem vir junto ao *blockchain*. Afinal, trata-se de algo novo, que trás consigo, benefícios e desafios a serem superados.

Para se entender melhor como essa tecnologia funciona deve-se primeiro entender que ela trabalha com um sistema distribuído, Lamounier (2019) define:

[...] é um banco de dados descentralizado, ou seja, distribuído em vários computadores ou nós. Nesta tecnologia, cada nó manterá o registro e, se ocorrer alguma alteração de dados, o registro será atualizado para todos. A atualização ocorre independentemente em cada nó.. Todos os nós têm status

igual em termos de autoridade. Ou seja, não há autoridade central ou servidor gerenciando o banco de dados, o que torna a tecnologia transparente. Cada nó pode atualizar o livro-registro e outros nós verificarão sua validade. O processo de verificação é muito fácil, na verdade. Os nós tentarão verificar a transação com o algoritmo de consenso ou votação. No entanto, o direito de voto ou a participação de todos os nós dependerá das regras específicas de cada registro. Assim, às vezes todos os nós podem participar, em outros momentos, apenas os nós selecionados participarão. Depois que todos os nós emitirem o sinal, a transação obterá um lugar no registro e todos os nós poderão receber o status atualizado. (LAMOUNIER, 2019, p. 1).

Uma característica desta tecnologia é ela possuir estabilidade e imutabilidade. Este benefício é alcançado quando um processo é concluído, é gerado um *hash*, que pela definição de Filho (2012) “é uma espécie de algoritmo, que torna quase impossível dois conteúdos diferentes terem o mesmo *hash*, e por isso, é um método seguro para se ver se o conteúdo foi alterado”. Esse *hash* é armazenado dentro dos blocos, tornando esse dado imutável. Zerbini(2019) aborda está característica:

Uma *blockchain* pode ser vista como um grande banco de dados descentralizado, transparente e, sua principal diferença, é a imutabilidade dos dados escritas nela. Toda a imutabilidade da *blockchain* é alcançada devido a função de *hash*. O link dos *hashes* torna a cadeia inquebrável — caso alguma mudança seja feita em algum bloco, afetaria todos os blocos subsequentes, e por isso a mudança pode ser facilmente rejeitada ou observada. (ZERBINI, 2019, p. 1).

Essa tecnologia também adiciona a transparência e a confiança, Mougayar(2018) em seu livro aborda esse tema:

[...] uma aspiração-chave dos *blockchains* é se tornar o tom para serviços baseados em confiança. Isso significa que poderemos verificar a veracidade e a autenticidade dos fatos, dados, processos, eventos, ou qualquer outra coisa, com a mesma facilidade com que procuramos por informações, serviços ou produtos no Google hoje em dia. A busca por transparência e verdade é uma característica complementar da confiança. A transparência faz a pergunta: podemos ver? A confiança faz a pergunta: podemos verificar? (MOUGAYAR, 2018, p. 35).

O *Blockchain* também é conhecido por ser um sistema "Trustless", que é:

[...]as transações não dependem apenas das duas partes envolvidas, mas também de um intermediário - como um banco, empresa de cartão de crédito ou provedor de pagamento. Ao usar a tecnologia *Blockchain*, todo esse arranjo não é mais necessário porque a rede distribuída de nodes verifica as transações por meio de um processo conhecido como mineração. Por essa razão, a *Blockchain* é usualmente conhecida como um sistema "Trustless". (BINANCE, 2019, p. 1).

Depois de termos abordado as principais vantagens, serão levantados alguns desafios que o *Blockchain* apresenta. Um dos principais é o conhecido como Ataque 51%, que é:

O algoritmo de consenso Proof of Work (PoW) que protege a *Blockchain* do Bitcoin provou ser muito eficiente ao longo do tempo. No entanto, existem alguns ataques em potencial que podem ser realizados contra redes *Blockchain*, dentre eles está o Ataque de 51%. Tal ataque pode acontecer se uma organização conseguir controlar mais que 50% do poder computacional da rede, permitindo que eles interfiram no funcionamento da rede excluindo ou modificando intencionalmente a ordenação das transações. Apesar de ser teoricamente possível, nunca houve um Ataque de 51% bem-sucedido na rede *Blockchain* do Bitcoin. À medida que ela cresce, a segurança aumenta e é muito improvável que os mineradores invistam grandes quantias de dinheiro e recursos para atacar o Bitcoin, já que são mais bem recompensadas por trabalhar honestamente. Além disso, um Ataque de 51% bem-sucedido só seria capaz de modificar as transações mais recentes por um curto período de tempo, porque os blocos são vinculados através de provas criptográficas (mudar blocos mais antigos exigiria níveis intangíveis de poder computacional). (BINANCE, 2019, p. 1).

Outra dificuldade que essa tecnologia pode apresentar é a modificação da informação gravada, apesar da imutabilidade se mostrar em muitos casos como uma vantagem, em caso de um erro, essa inalterabilidade pode gerar certos problemas na hora da correção, como verificamos:

Outra desvantagem dos sistemas *Blockchain* é que, uma vez que os dados foram adicionados à rede, é muito difícil modificá-los. Embora a estabilidade seja uma das vantagens da *Blockchain*, nem sempre é uma boa característica. Alterar dados ou o código de uma rede *Blockchain* é normalmente muito complicado e geralmente requer um Hard Fork (Bifurcação), onde uma cadeia de blocos é abandonada e outra é criada. (BINANCE, 2019, p. 1)

Um dos desafios a ser superado é o da perda da chave privada. Como o sistema funciona com criptografia, a perda dessa chave, que funciona como uma senha, poderia causar a perda dos dados armazenados, como enfatiza Lyra (2019):

Um endereço em um *blockchain* é semelhante a um e-mail, no qual se pode enviar e receber de outras pessoas as unidades de troca daquele bloco. O endereço da rede *blockchain* é criptografado e, ao se criar um endereço, simultaneamente é criada uma chave privada ou senha (ibid). É a única forma de acesso para destravar os tokens e enviar para um determinado endereço, Se houver perda dessa chave, não há como mover os tokens desse endereço (ibid). (LYRA, 2019, p. 13).

Um fator relevante é a grande necessidade de poder computacional para se achar um hash de bloco válido e isso pode gerar com o passar do tempo, sistemas ineficientes:

As *Blockchains* que usam o algoritmo de consenso PoW são altamente ineficientes. Como a mineração é extremamente competitiva e há apenas um vencedor a cada dez minutos, o trabalho de todos os outros mineradores é desperdiçado. Como eles estão sempre tentando aumentar seu poder computacional, para ter uma chance maior de encontrar um hash de bloco válido, os recursos usados pela rede aumentaram significativamente nos últimos anos e atualmente consomem mais energia do que muitos países, como a Dinamarca, a Irlanda e a Nigéria. (BINANCE, 2019, p. 1)

Outro fator é o armazenamento que esse tipo de sistema pode demandar:

Os livros das *Blockchains* podem crescer muito ao longo do tempo. A *Blockchain* do Bitcoin atualmente requer cerca de 200 GB de armazenamento. A velocidade no crescimento das *Blockchains* parece estar superando o visto na capacidade dos discos rígidos (HDs) e a rede corre o risco de perder nodes se o livro ficar muito grande, impedindo que usuários baixem e armazenem o mesmo. (BINANCE, 2019, p. 1)

Essa tecnologia apresenta algumas vantagens exclusivas, porém apresenta alguns desafios a serem superados. Porém o *Blockchain* veio para ficar e nos próximos anos iremos ver governos e empresas utilizando essa tecnologia (BINANCE, 2019).

Este estudo tem como propósito compreender os desafios da tecnologia *Blockchain* na implementação em infraestruturas críticas da informação. Bem como identificar se os militares do Exército Brasileiro conhecem ou não essa nova tendência. A suposição feita a partir do problema foi que, tendo a tecnologia *Blockchain* a possibilidade de revolucionar sistemas em poucos anos, identificar quais são os seus benéficos e desafios. Verificar a aplicabilidade em prol dos sistemas sob responsabilidade do Exército. Para Laurence (2019), o autor deixa claro que esse tipo de base de dados é considerado a "quinta evolução" da computação. A autora deixa claro as grandes possibilidades que essa tecnologia pode agregar. Seguindo essa premissa, vê-se a necessidade de que os militares conheçam este método para poder melhorar seus sistemas.

A amostra dos que responderam o questionário, foi de 46 militares da ativa do Exército Brasileiro. A maior porcentagem foi de 60,9 %, que são capitães e possuem uma média de 15 anos de serviço, seguido de 17,4% de sargentos, 13% de tenentes 4,3% tanto de majores como de subtenentes conforme quadro abaixo:

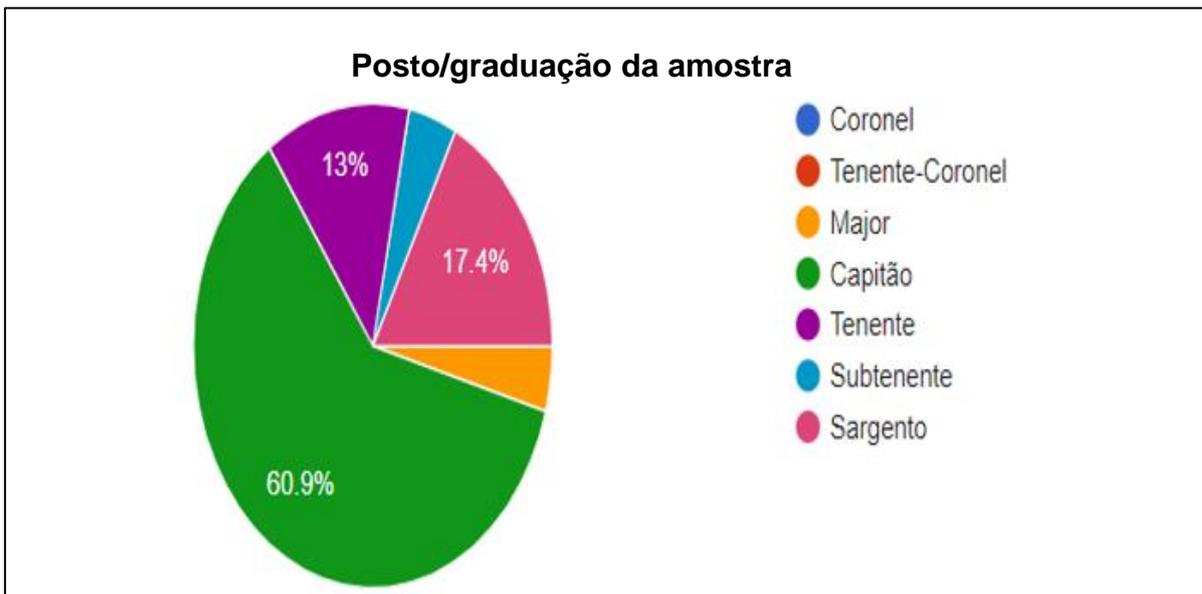


GRÁFICO 1 - Posto/graduação da amostra

Fonte: O autor

Dessa amostra pode-se observar que 10,9 % dos militares questionados são especialistas em TI (com formação na área), totalizando assim 5 militares. Dentre eles, 4 possuem o curso de Guerra Cibernética. Usuários com conhecimento avançado totalizou 15,2 %, mediado com 32,6 %, usuário básico com 39,1 % e que não possuem nenhum conhecimento em 2,2 % conforme gráfico 2 e 3 abaixo:

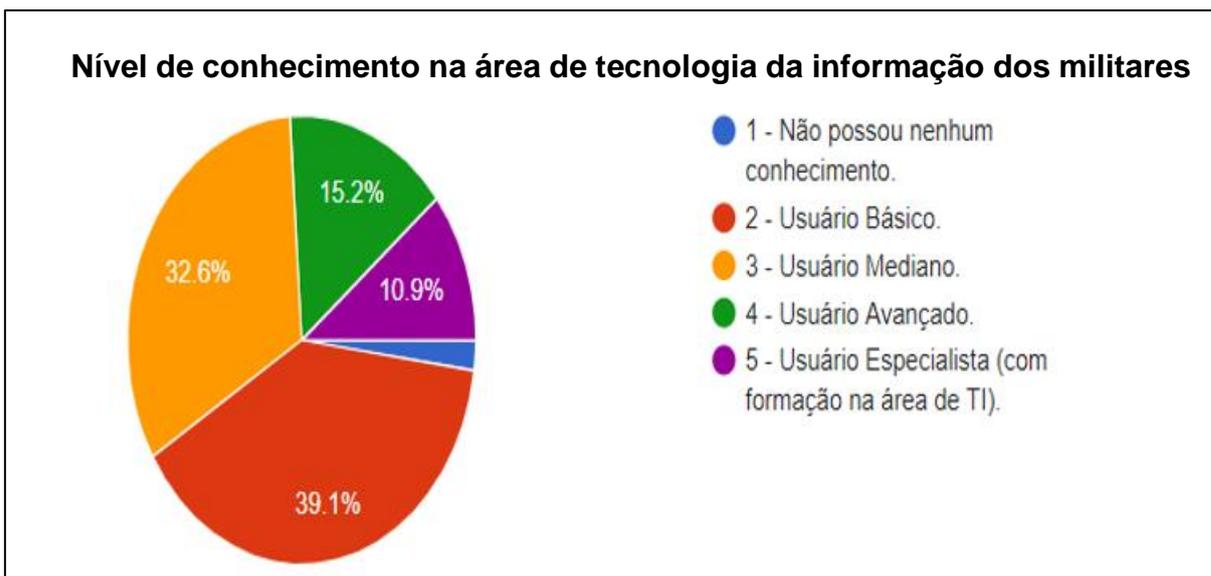


GRÁFICO 2 - Nível de conhecimento na área de tecnologia da informação dos militares

Fonte: O autor

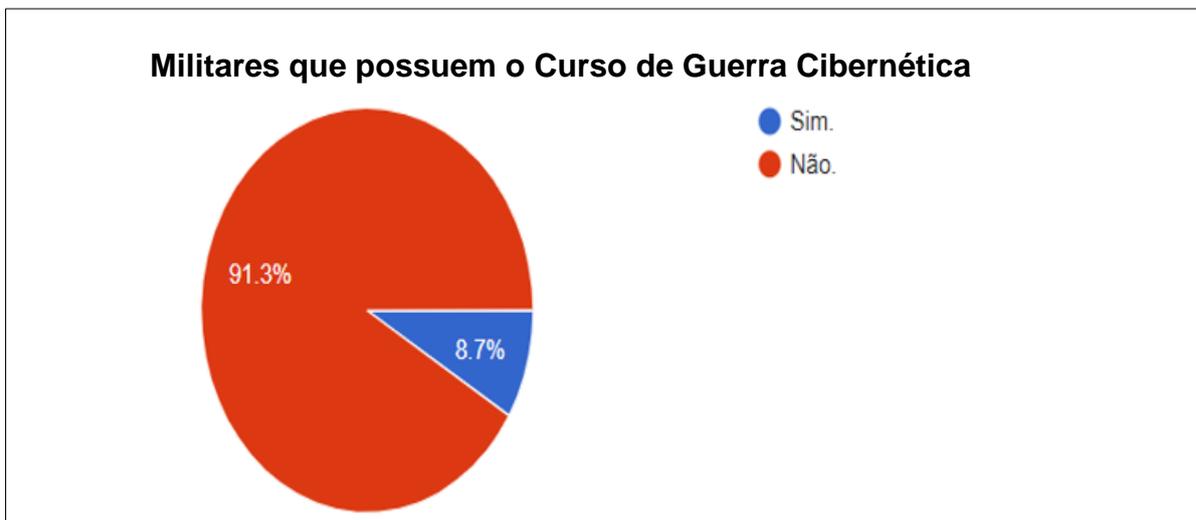


GRÁFICO 3 - Militares que possuem o Curso de Guerra Cibernética

Fonte: O autor

Pode-se observar que as maiores dificuldades na implementação da tecnologia *Blockchain* em sistemas de infraestrutura crítica é o desconhecimento sobre o assunto. Dos 46 militares que responderam a pesquisa, 12 militares se declaram com conhecimento avançado e especialista, totalizando 26,1%, dentre os quais somente 10,9%, isto é, 5 militares, que souberam responder o que é um SICI e conseguiram defini-la. Fica evidente o desconhecimento do que é um SICI tanto dos militares da área de TI, bem como de usuários com níveis de conhecimento mediano e básico. Esse percentual totaliza 89,1% dos que não conseguem definir o que é um SICI, mesmo sendo uma responsabilidade do Exército a segurança desses sistemas. Sendo pouco conhecido o que se trata um SICI, dificulta-se a elaboração de medidas de segurança e inovações que poderiam vir a agregar o sistema.

Militares que possuem conhecimento sobre Sistemas de Infraestruturas Críticas da Informação (SICI)

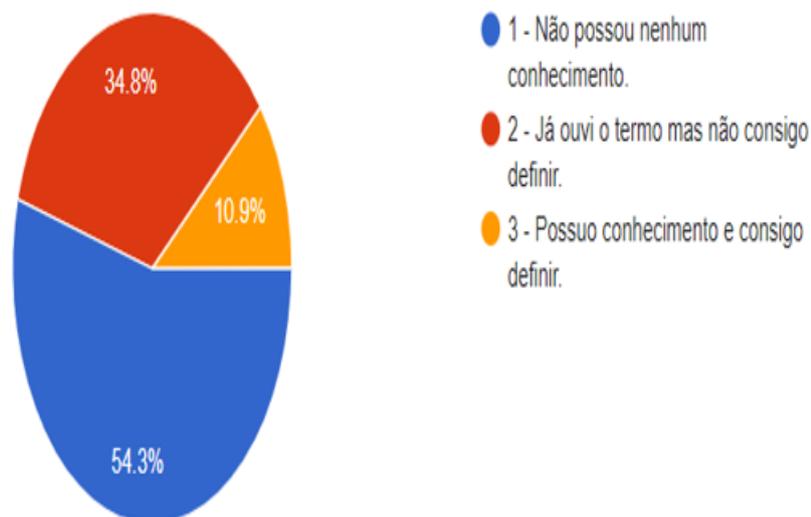


GRÁFICO 4 - Militares que possuem conhecimento sobre Sistemas de Infraestruturas Críticas da Informação (SICI)

Fonte: O autor

Vale destacar, por exemplo, o grande percentual de militares que não possuem nenhum conhecimento sobre o tema, mesmo com uma amostra de militares da ativa e em sua maioria com mais 15 anos de serviço, tendo o G Ciber a função de cooperar na proteção cibernética das infraestruturas críticas brasileiras (COTER, 2017).

Na identificação do conhecimento dos militares sobre as Blokchain, notamos também um alto grau de desconhecimento sobre o tema. Cerca de 41,3% não possuem nenhum conhecimento, outros 23,9 % já ouviram o termo, mas não conseguem definir e apenas 15,2 % possuem conhecimento e conseguem definir o que é Blokchain. O próximo quadro, mostra o pouco conhecimento sobre o assunto, mesmo sendo uma tecnologia atrelada ao Bitcoin e amplamente difundida.

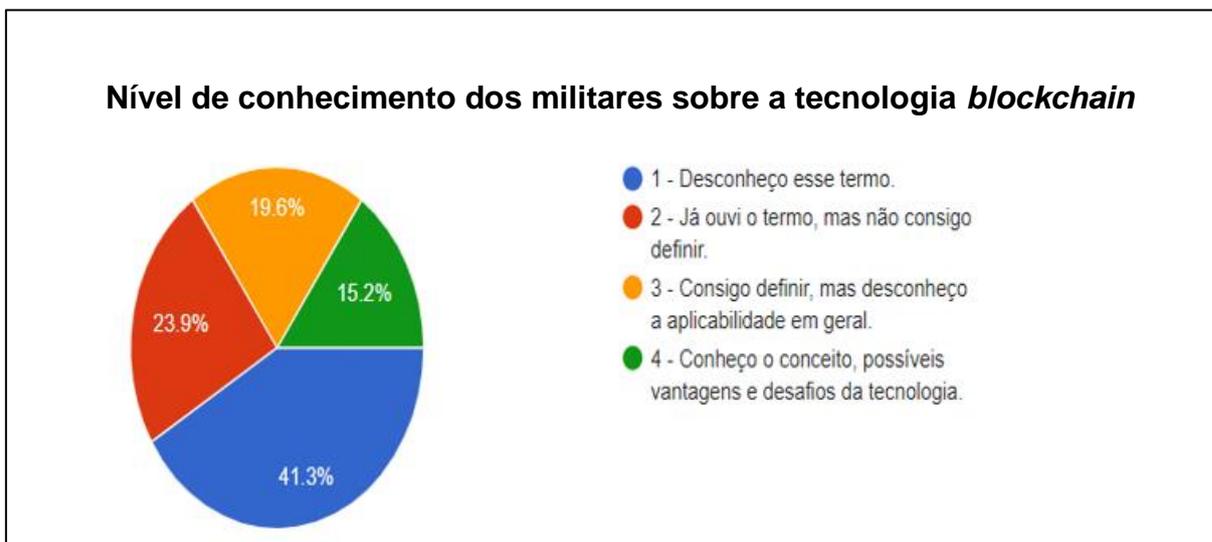


GRÁFICO 5 - Nível de conhecimento dos militares sobre a tecnologia blockchain

Fonte: O autor

Vale destacar, por exemplo, que mesmo especialistas na área de TI desconhecem sobre essa tecnologia, sendo em sua maioria militares com experiência. Conforme explicado, Tapscott e Tapscott (2018) falam que o *Blockchain* irá dar acesso a capacidades únicas que revolucionarão os sistemas da informação de hoje e por isso os autores deixam claro a importância de estar atento a essa futura revolução.

Dos que conseguem conhecer e identificar a tecnologia *Blockchain* em proveito do SICI, ficou no patamar de 15,2 %, isto é, 7 militares da amostra. Verificando-se que a fonte desse conhecimento, 71,4% obtiveram através da internet, 14,3% através de cursos e outros 14,3% por mídia, como podemos verificar no gráfico abaixo:

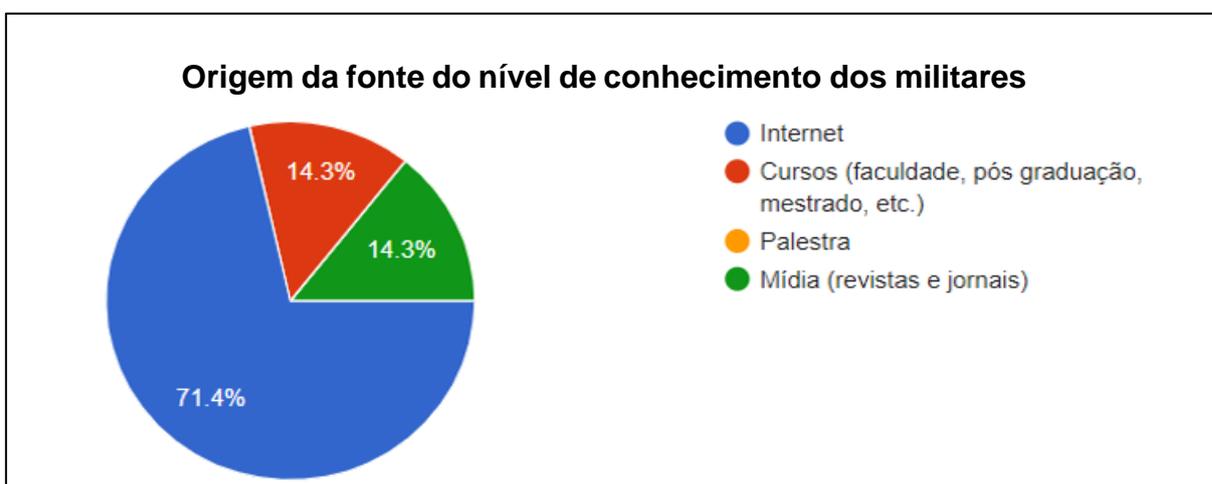


GRÁFICO 6 - Origem da fonte do nível de conhecimento dos militares

Fonte: O autor

Já com o nível de acordo ou desacordo com as seguintes afirmações em referência a tecnologia de *Blockchain*, 100 % concordam totalmente ou parcialmente que a tecnologia é amplamente escalável e futuramente vai conseguir adoção massiva. 85,71% concordam totalmente ou parcialmente que esta tecnologia pode introduzir vantagens a curto prazo, sobrando os 15,29% restantes discordando parcialmente. Já para 71,42% concordam totalmente ou parcialmente que tecnologia *Blockchain* é mais segura que os sistemas baseados em tecnologias atuais, conforme podemos verificar no gráfico abaixo:

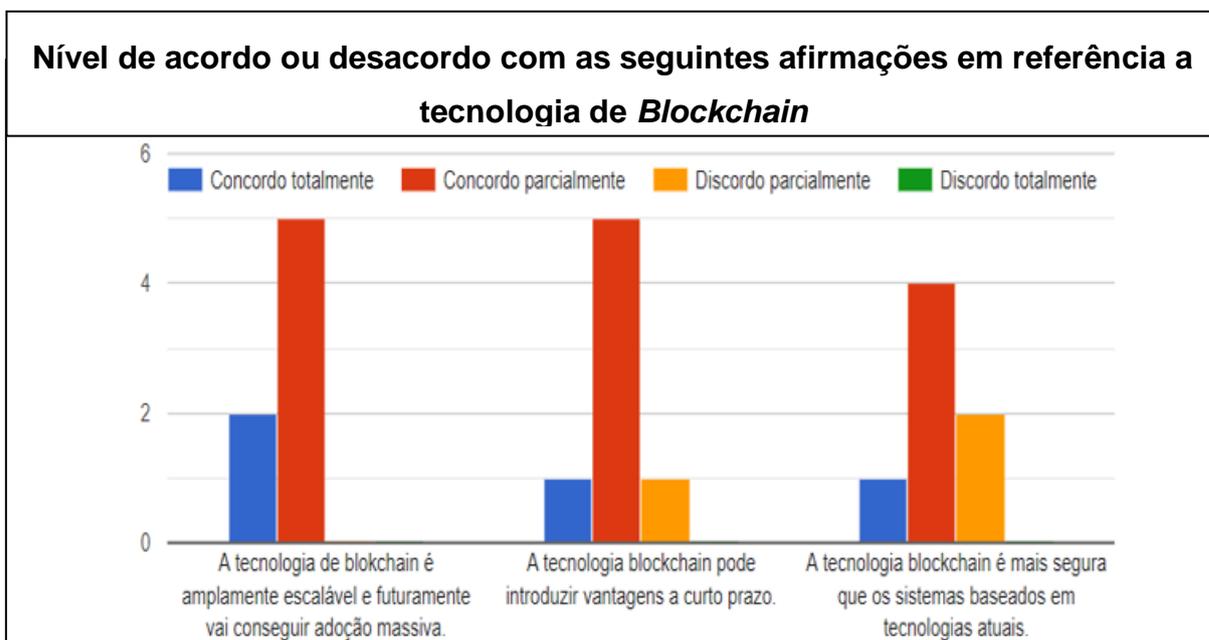


GRÁFICO 7 - Nível de acordo ou desacordo com as seguintes afirmações em referência a tecnologia de *Blockchain*
 Fonte: O autor

Podemos verificar que nenhum dos questionados com conhecimento discordam que a tecnologia poderá agregar valor em um futuro.

Com relação as possíveis vantagens do uso da tecnologia, os dois principais apontados foram o benefício de o sistema poder ser distribuído e o de agregar confiança aos sistemas de infraestrutura críticas, sendo apontado por 71,4% dos especialistas. A estabilidade, imutabilidade e a desintermediação foram apontadas por 42,9%. A transparência e proveniência foi marcado por 28,6%. Como mostrado no gráfico abaixo:

Possíveis vantagens do uso tecnologia blockchain

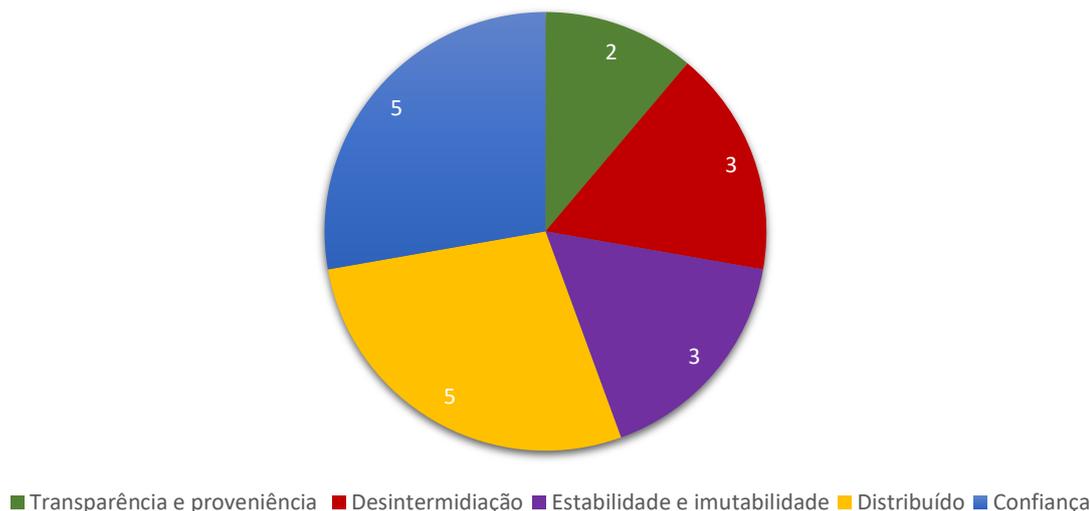


GRÁFICO 8 - Possíveis vantagens do uso tecnologia blockchain

Fonte: O autor

Na visão dos especialistas, os possíveis desafios da tecnologia *Blockchain* em SICI são como principais a modificação de informações de acordo com 57,1% dos aptos a responder. Seguidos pelo ataque de 51% e as chaves privadas, apontando 42,9% das respostas. Ineficiência e armazenamento receberam 2 votos cada uma, contabilizaram 28,6% cada uma. Recebeu apenas um voto o pouco conhecimento e exemplos existentes do uso do Blockchain em SICI e implementação, ficando com uma porcentagem de 14,3%. As respostas, não tenho certeza e nenhum desafio a ser superado, não receberam nenhum voto.

Possíveis desafios da tecnologia blockchain em SICI

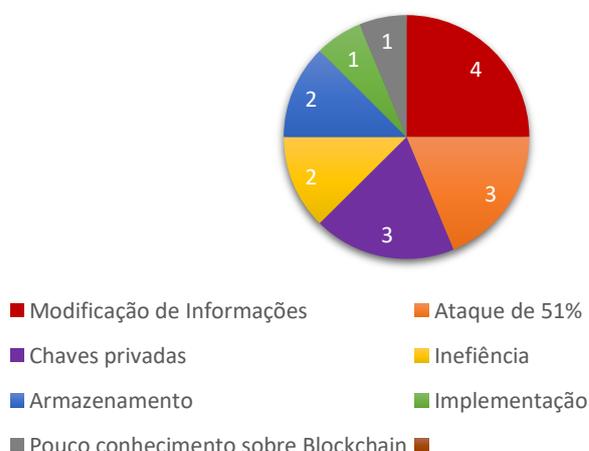


GRÁFICO 9 - Possíveis desafios da tecnologia blockchain em SICI

Fonte: O autor

Os resultados das pesquisas aplicadas focadas em obter dados sobre o nível de conhecimento sobre a tecnologia *Blockchain*, suas vantagens e desafios mostram

inicialmente, o pouco conhecimento sobre o que se trata esta tecnologia. Isto pode gerar dificuldades para se utilizar e implementar esse sistema, visto que ele se encontra ainda pouco difundido no meio militar, sendo de conhecimento apenas de 15% dos militares e conhecimento sobre SICI ainda menor, com apenas 10% dos militares com conhecimento sobre esse tema.

Pela avaliação dos especialistas militares, por exemplo, a tecnologia apresenta como principais vantagens de confiante e apresentar o sistema distribuído. Sendo a resposta escolhida por 71,4% dos que responderam o questionário. Com relação aos desafios a modificação de informação apareceu como principal, apontado por 57,1 % das respostas, também o ataque 51% e as chaves provadas tiveram destaque, com 42,9 %.

A pesquisa mostra que mesmo que a tecnologia possa melhorar sistemas em um futuro, apresentará dificuldades por ser pouca difundida no meio militar. Diante disso, é possível afirmar que se houver desejo de se utilizar essa tendência, o principal desafio que vem pela frente será capacitar e instruir os militares sobre essa tecnologia.

4. CONCLUSÃO

O desenvolvimento do presente estudo possibilitou uma verificação se os militares estão atentos ao surgimento de novas tecnologias, no caso dessa pesquisa focada na tecnologia *Blockchain*, uma reflexão acerca dos seus benefícios e desafios encontradas ao tentar se implementar em Sistemas de Infraestrutura Críticas da Informação.

De um modo geral, poucos militares entendem essa tecnologia e conseguem verificar as vantagens e desafios a serem superados. Essa pouca quantidade pode gerar dificuldades na hora de utilizar essa ferramenta ou pode ocorrer um atraso na utilização da mesma em sistemas, gerando uma lacuna de vulnerabilidades. A maioria dos militares que entendem dessa nova tendência, apontaram vantagens, que poderiam ser adicionadas com a utilização desse modelo em Sistemas de Infraestrutura Críticas da Informação, adicionando maior confiabilidade ao sistema, visto que, poderia agregar confiança na realização de processos de validação e verificação.

Outro fator bastante apontado foi ser um sistema distribuído, que por utilizar uma rede distribuída de *nodes* (nós), agrega ao sistema de dados, por ser altamente resistente a falhas técnicas e ataques maliciosos. Outras duas vantagens mais apontadas foram a estabilidade e imutabilidade, que adicionariam uma grande dificuldade de alteração dos blocos confirmados para que sejam revertidos posteriormente, cooperando para agregar maior confiança; outro foi a desintermediação que requer menos supervisão e retira de uma autoridade central ou de uma terceira parte, no momento da transação para validar o processo.

Já com relação aos principais desafios, a dificuldade de se modificar uma informação de processo validado pode se mostrar como uma dificuldade do sistema, visto que, em caso de erro, poderia gerar transtornos na hora da correção. Outro desafio apontado, é o “Ataque 51%”, que poderia validar um processo, se houvesse 51% dos *nodes* responsáveis pela validação, podendo, com isso, burlar o sistema de validação, realizando transações e as validando incorretas, sem que a rede distribuída pudesse identificar esse processo incorreto. Um SICI trabalhando de uma maneira isolada, com menos nós distribuídos, poderia mais facilmente sofrer um ataque desse estilo. O terceiro desafio mais apontado foi as chaves privadas, sendo as informações criptografadas, em caso de perda da chave privada, poderia se gerar uma indisponibilidade de acesso aos dados gravados, causando sérios problemas.

Dada à importância do tema, torna-se necessário o desenvolvimento de pesquisas com testes, implementações dessa tecnologia, que se mostra promissora, podendo gerar grandes benefícios.

Por fim, podemos chegar à conclusão de que apesar da tecnologia *Blockchain* estar presente há 10 anos e estar atrelada ao Bitcoin que é amplamente conhecido, ela ainda é conhecida somente por uma minoria de militares. Logo, é indiscutível que podeira gerar uma dificuldade ou um atraso na utilização dessa tendência. Nesse sentido, é necessário buscar uma maior divulgação e uma especialização de militares para que possam implementar iniciativas com essa tecnologia.

REFERÊNCIAS

- BINANCE, A. Academy Binace. **Academy Binace**, 2019. Disponível em: <<https://www.binance.vision/pt/blockchain/positives-and-negatives-of-blockchain>>. Acesso em: 5 julho 2019.
- COTER. **Manual de Campanha EB70-MC-10.232**. 1º. ed. Brasília: [s.n.], 2017.
- DEFESA, M. D. Portal do Ministério da Defesa. **defesa.gov.br**, 2019. Disponível em: <<https://www.defesa.gov.br/forcas-armadas/111-lei-de-acesso-a-informacao/perguntas-frequentes/remuneracao-dos-militares-das-forcas-armadas-no-brasil-e-no-exterior/8637-efetivos>>. Acesso em: 01 junho 2019.
- DRESCHER, D. **Blockchain básico: Uma introdução não técnica em 25 passos**. 1. ed. São Paulo: Novatec Editora, v. I, 2018.
- EDITORA, O. L. Bitcoin - O Dinheiro Do Futuro? **Guia Mundo**, São Paulo, v. I, n. 02, p. 97, Fevereiro 2007. ISSN ISBN: 978-85-432-1886-1.
- FILHO, J. E. M. **Descobrimo o Linux - 3ª Edição: Entenda o sistema operacional GNU/Linux**. 3º. ed. São Paulo: Novatec Editora, 2012.
- LAMOUNIER, L. 101blockchains. **101blockchains**, 2019. Disponível em: <<https://101blockchains.com/pt/blockchain-vs-registro-distribuido/>>. Acesso em: 06 Julho 2019.
- LAURENCE, T. **Blockchain para leigos**. 1º. ed. Rio de Janeiro: Alta Books, v. I, 2019.
- LYRA, J. G. **Blockchain e Organizações Descentralizadas**. 1º. ed. São Paulo: Brasport, v. I, 2019.
- MOUGAYAR, W. **Blockchain para negócios: Promessa, prática e aplicação da nova tecnologia da internet**. 1. ed. Rio de Janeiro: Alta Books Editora, v. I, 2018.
- TAPSCOTT, ; TAPSCOTT,. **Blockchain revolution**. 2º. ed. São Paulo: SESI SENAI Editora, 2018.
- TELLES, A. **O futuro é smart: Como as novas tecnologias estão redesenhando os negócios e o mundo em que vivemos**. 1. ed. Curitiba: PUCPress, v. I, 2018.
- ZERBINI,. **https://medium.com/**, 2019. Disponível em: <<https://medium.com/@zerbinidamata/entendo-a-imutabilidade-da-blockchain-8432cd4248a5>>. Acesso em: 15 Junho 2019.