ISSN 2515-8260 Volume 10, Issue 05, 2023

Prospects, Use Cases, and Pitfalls of Blockchain as a Cyber Defense

Nagaraju I [1], Dileep P [2], Kamal M V [3], Revathy P [4]

[1,2,3] Associate Professor, Department of Computer Science and Engineering

[4] Assistant Professor, Department of Computer Science and Engineering

[1,2,3] Malla Reddy College of Engineering and Technology,Kompally,Hyderabad,India.

[4] Narsimha Reddy Engineering College,Kompally,Hyderabad,India.

Abstract- Using Blockchain to Protect Against Cyberattacks: Promising Practices and Future Directions Cybercriminals' prey isn't limited to the corporate world. The fact that nation-states have been successfully attacked online shows that cyber threats may endanger vital national interests. As a result, countries have launched what is called "cyber defence" at the national level to deal with cyber threats. The importance of the cyber defence industry to national security necessitates the use of cutting-edge security systems. Blockchain, in contrast to traditional systems, offers robust security qualities devoid of a centralised control body; as a result, it is receiving a lot of attention for its potential use in the cyber defence field. In this article, we discuss the benefits and drawbacks of using blockchain technology in cyber security, academic and government endeavours. We compiled a survey of material published between 2016 and 2021, including official documents, interviews, news articles, technical reports, and research papers. So, by methodically researching and analysing blockchain's potential for cyber protection, our work helps narrow the gap. According to our findings, blockchain is being aggressively promoted not just by academic institutions but also by government-led schemes, suggesting that it will have a significant impact on cybersecurity. Future research directions for blockchain technology, assessment, and survey are discussed in the last section of this work.

Keywords— Blockchain, cyber security, cyber defense, military, survey.

I. INTRODUCTION

The goal of cyber defence is to protect a nation against cyberattacks. Throughout the last several decades, we have maintained a rate of fast digital transition. Maybe the growing number of cyberattacks is the price we have to pay for the efficiency gains brought about by the switch to digital systems. Too often, security was overlooked in the development and implementation of IT systems. Moreover, new varieties of security flaws are discovered often. Given that the state, not a single service or corporation, is now the major target of cyber attacks, this is an important problem that has to be addressed. Infrastructure on a national scale, including power plants, hospitals, and even military networks, is constantly being integrated. One source [1] claimed unequivocally that nuclear submarines may be hacked. The inability to rapidly upgrade or redesign the systems of some national infrastructures compounds the problem. For cyber defence, nation states need robust security technology. In light of these considerations, an amendment to the U.S. Defense Authorization Act for 2021 was recently enacted [2][4] that recognises blockchain technology as an emerging technology with use in the military industry. This demonstrates that blockchain's high security standards are catching the attention of the cyber security community. Bitcoin, the world's first cryptocurrency, was first implemented using blockchain technology [5]. Since several ledgers record the same information and verify it in a decentralised fashion, blockchain is also known as a distributed ledger technology. Unless an attacker controls more than 50% of the system's resources, this architecture will prohibit any tampering with the data. A Turing-complete smart contract [6] implemented in a blockchain environment can provide a safe computing environment. As a result, blockchain can support a wide range of decentralised programmes. Cryptocurrencies and other blockchain initiatives have shown to offer high levels of security. As a result, cyber defence authorities in at least a few nations are actively advocating for a variety of blockchain initiatives. Data security, a distributed military network, a trustworthy supply chain for weapons systems, swarms of drones, and member authorization are just some of the many uses for these applications.

II. RELATEDWORKS

Numerous research projects have looked at blockchain's potential impact on cyber security. The theme, key contributions, and limitations of the associated research are shown in Table 1. Applications of blockchain technology in cyber security were comprehensively evaluated by Taylor et al. [7]. Zhu et al. [8] looked at blockchain's potential cyber security applications. The research conducted by Lilly and Lilly [9] examined actual military blockchain initiatives in the United States, China, and Russia. Bunsal et al. [10] looked at how blockchain may be used for specific purposes in cyber security. Defense and aerospace are closely connected fields, thus

ISSN 2515-8260 Volume 10, Issue 05, 2023

Ahmad et al. [11] looked at blockchain applications there. Their research offers an in-depth look at the framework of blockchain programmes.

To the best of our knowledge, however, no articles have even come close to attempting a study of blockchain applications that may be encompassed under the umbrella of cyber security. The scope of cyber defence extends beyond the military to include the protection of the country as a whole. Research into blockchain's potential for use in cyber defence is necessary in light of the gravity of modern cyber threats to our nation's safety. Our work draws on existing literature on blockchain's potential impact in the field of cyber security.

TABLE 1. Comparison with previous research.

Research	Topic	Main Contribution	Limitation
Taylor et al. [7]	Blockchain for cyber security	Systematic literature review on blockchain for cyber security	Limitations of the role of blockchain are not discussed.
Zhu et al. [8]	Blockchain for defense	Introduction to various blockchain applications combined with the latest technologies	Existing cases or studies are not thoroughly investigated.
Lilly and Lilly [9]	The weaponization of blockchain in the US, China, and Russia	Specific case studies of the three countries and a strategical analysis on them	Since it is case-oriented, related research is not sufficiently handled.
Bansal et al. [10]	Blockchain for cybersecurity	Conceptual investigation on the use of blockchain for various applications of cybersecurity	It focuses on detailed topics such as private messages, DDoS, and DNS.
Ahmed et al. [11]	Blockchain for aerospace and defense	State-of-the-art survey on blockchain aerospace and defense and detailed examples	The research domain is focused on border protection, battlefield, swarm, and supply chain management.
Our research	Blockchain for cyber defense	The first blockchain survey with the approach of cyber defense, and plenty of the latest research and application cases	Due to linguistic limitations, national projects are not surveyed in a balanced manner.

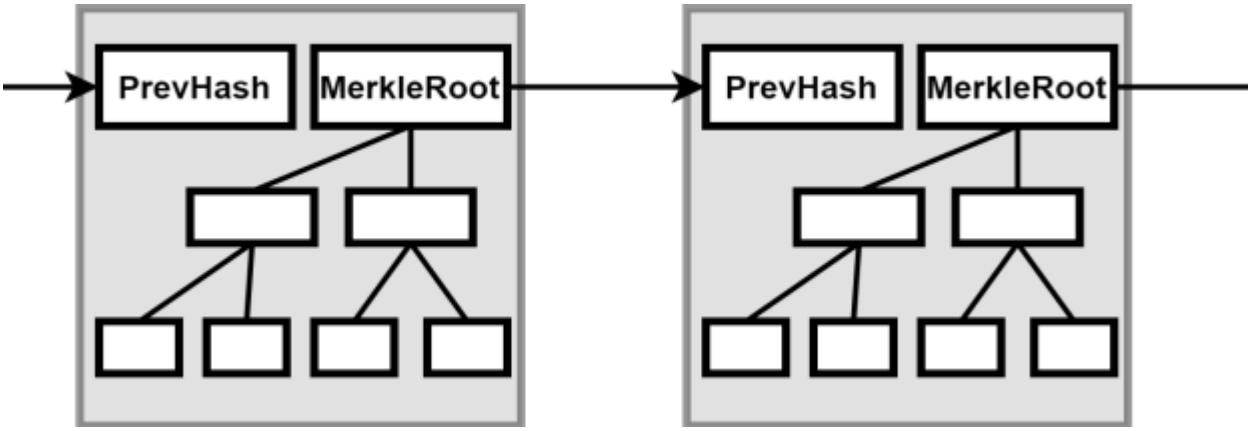

FIGURE 1. Bitcoin data structure.

In this article, we'll give you a quick rundown of what blockchain is and how it works. With the introduction of the first successful cryptocurrency, Bitcoin, in 2009, the concept of a blockchain has found widespread use. Bitcoin's ability to function as e-cash in trustless contexts is made possible by the blockchain, the cryptocurrency's fundamental data structure. The amount sent, the addresses involved, and the signature of the recipient are all recorded in a Bitcoin transaction. As seen in Fig. 1, a block may hold several transactions, hence the term

ISSN 2515-8260 Volume 10, Issue 05, 2023

"blockchain" accurately characterises Bitcoin's underlying data structure. Every block, with the exception of the first "genesis" block, contains the hash of the prior block in the chain. To prevent modification, each block stores the Merkle root hash of the transactions, and the chain of connected blocks verifies each block's authenticity. In other words, if the transaction information in this block is changed, the value of all the blocks before it must also be changed. Bitcoin's decentralised network decides how blocks are generated using its own Proof-of-Work-based consensus method (PoW). Yet, there are other ways to organise a blockchain than the way Bitcoin does it. Ethereum, Zcash, Ripple, and IOTA are just several altcoins that have slightly modified or notably different architectures from Bitcoin.

Fig. 2 (a) depicts the longest chain rule of Bitcoin. Proof-of-Work (PoW) is used to produce blocks and demonstrates that an adequate quantity of computational resources have been used. Each block has a single outgoing connection, however if there's a fork, then two or more blocks might potentially refer to the same prior block. As a result, Bitcoin considers the longest chain as the most reliable. PoW ensures that the greatest resources are being used to create the longest chain. Although while Bitcoin's underlying data format is similar to that employed by Blockchain, the two are not identical. The proof-of-work algorithm in Ethereum [6] uses a multiply linked list. As Ethereum may produce a new block every 15 seconds, it is simple to have many blocks that refer to the same block. Ethereum's solution to this problem is the Greedy Heaviest-Observed Sub-Tree (GHOST) protocol, which recognises the heaviest chain as the valid chain rather than the longest chain. In Fig. 2 (b), the grey chain is shown to become the heaviest and, therefore, the genuine chain, whereas the black and longest chain is shown to be invalid. Because many blocks are left out of the longest chain, the miners of uncle blocks get rewarded.

The tangle is used by IOTA [12] and is analogous to a directed graph. Only when two other transactions in the tangle reference it is that transaction considered valid. Although if a node chooses which transactions to validate and refer at random, there are still many centralization concerns with this design. Deterministic block creation is used in blockchains based on the Practical Byzantine Fault Tolerance (PBFT) protocol. To the best of their ability to agree, they produce a single block of uniform height. That's why you'll still find just one continuous chain of them. Given the need of pre-identification of blockchain nodes, a PBFT-style blockchain is often deployed only inside private networks. Since blockchain networks are decentralised, they need a Sybil control mechanism to ensure that no malevolent users may take over the process of creating new blocks. Proof-of-Work (PoW) was used by Bitcoin to establish the network's decentralised Sybil control mechanism. Simply said, sufficient computing effort on the side of the players is needed for PoW to work. Dwork introduced the Proof-of-Work (PoW) idea in order to stop spam emails [13]. When a Bitcoin block has a hash value that is difficult enough to nd, the block is considered confirmed. This difficulty is set by the Bitcoin network. While Bitcoin's Sybil control mechanism is Proof-of-Work (PoW), other cryptocurrencies and blockchain solutions use decentralised Sybil control mechanisms such as Proof-of-Stake (PoS), Proof-of-Burn (PoB), Delegate Proof-of-Stake (DPoS), and Proof-of-Future (PBFT), so we do not consider PoW to be an essential property of a blockchain.

There are four distinct kinds of blockchains based on how they are used. Table 2 lists the several types of blockchains now in use, including public (permissionless), public permissioned, consortium, and private. Bitcoin's blockchain is open to everybody and is thus public and permissionless. That is to say, on the public blockchain, anybody may propose a block, and everybody can verify information. As the blockchains underlying the vast majority of cryptocurrencies are open to the public, anyone may propose a new block, perform a transaction, or verify its contents. A private blockchain is only available inside a closed network to which only authorised users belong, such as an organisation. A private blockchain is, by definition, not as distributed as the public blockchain. Since a consortium blockchain is created or controlled by a group of organisations, the number of its users is restricted. Therefore, it shares features with both public and private blockchains.

Finally, one of the most significant developments in blockchain technology is the smart contract, which was first implemented by Ethereum. Ethereum offers a Turing-complete smart contract ecosystem that can implement any computable code, including recursion, with user-friendly languages like Solidity, making it superior to simplified scripts for e-cash transactions. Decentralized networks use multiparty computing in the form of smart contracts, with all participating nodes implementing and verifying the calculations in a distributed ledger. If all participating nodes arrive at the same outcome after executing the code of a smart contract, that result is recorded in the distributed ledger. Smart contracts provide dependable computation in a wide range of software.

Moreover, blockchains may be broken down into two distinct types: permissioned blockchains and permissionless blockchains, with the former requiring participant identification and the latter not. A public blockchain, as we've already established, is often a permissionless blockchain. For decentralised administration, however, we can build a public permissioned blockchain with a permissioned writership system, and everyone will be able to view and verify blockchain data. This blockchain combines the best features of both public and consortium blockchains.

ISSN 2515-8260 Volume 10, Issue 05, 2023

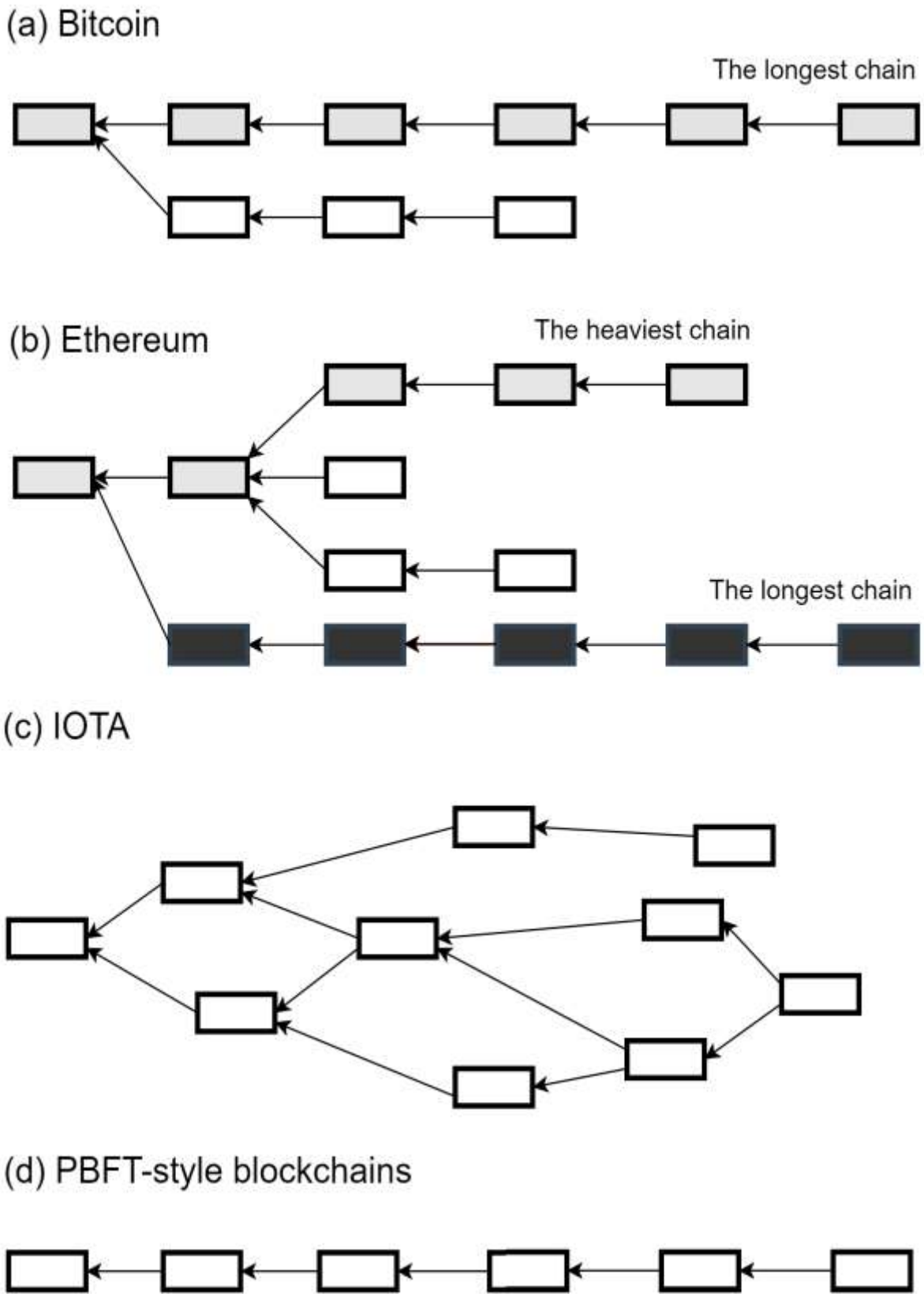

FIGURE 2. Hash chain structures.

ISSN 2515-8260 Volume 10, Issue 05, 2023

III. BENEFITS OF USING A BLOCKCHAIN FOR CYBER DEFENSE

Recent cyberattacks on governments throughout the globe have made cyber defence an established practise. Cyber assaults on nations are become a major problem. Governments have become aware of an ongoing "cyber war" as a result of assaults such as those in 2007 against Estonia, 2008 against Georgia, 2009 against South Korea, 2010 against Iran's nuclear plant, and other conflicts between the United States and China. There are, of course, external dangers from other nations, but there are also significant internal concerns. A single insider threat may bring down a vital infrastructure system. It's hard to plan for things like betrayal or accidental blunders made by humans. Since a sophisticated supply chain structure may include an adversary, supply networks are intricate and involve many parties. Invisible software or hardware backdoors, for instance, might infiltrate networks.

Cyberspace interventions, especially via social media, into political processes have also been highlighted on several occasions. Cyber defence is the process of protecting a country's digital infrastructure against attacks, both small and big. Blockchain's distributed and shared ledger structure increases data visibility, which in turn may increase security. The fast development of technology has resulted in a proliferation of data providers and consumers as the military undergoes a process of modernization and digitization. The necessary aptitude for efficient processing might be hampered by an abundance of data. This may create difficulties in responding to dangers. 52% of cyber security professionals, according to a recent poll in Balbix's corporate security report [15], do not have continuous visibility on their risk area, making this a significant challenge when dealing with attacks. Everything that happens to a piece of data, from its inception to its final storage, is recorded and visible on a blockchain. As a result, everyone can see who is responsible for creating and processing data. Such transparency allows for the early detection of risks and the rapid development of solutions to remove them. Businesses, it has been argued, might also financially benefit from this transparency. PricewaterhouseCoopers (PwC) [16] has conducted an analysis of how implementing blockchain technology into the supply chain of the aviation sector will result in a about 4% prot due to data efficiency. Blockchain's information sharing improves resource allocation in industry, according to a recent research, which is economically beneficial. Yet, blockchain's use in the military industry may be more constrained than in other sectors. Confidential information, for instance, might be difficult to disseminate across the group. By doing the necessary data processing in an off-chain environment and just adding the relevant information in the blockchain, this use case is suitable for blockchain technology.

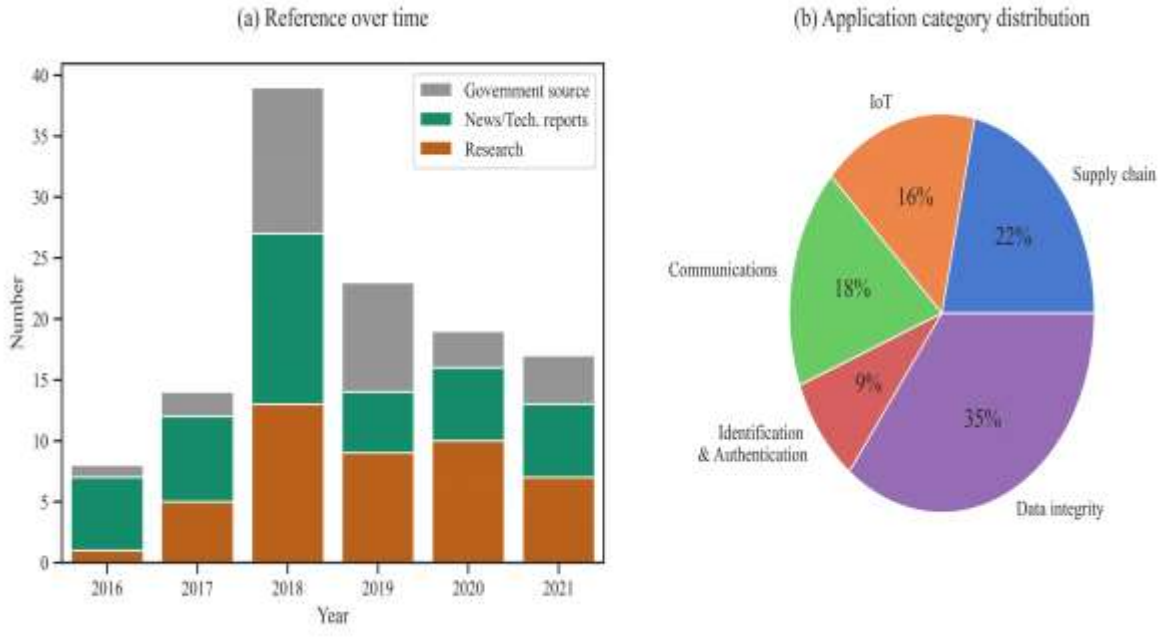

Fig.3 The two charts illustrate our system of survey. Fig. (a) shows references over year and sources. Fig. (b) is what we classified references according to the application domains.

Fig. 3 (a) shows the sources we used by year by classifying them by type. Starting in 2017, when the cryptocurrency boom occurred, we found plenty of references on related projects this year. Fig. 3 (b) illustrates what types of projects. We stress that it is challenging to investigate the details of such projects since military projects are often partially disclosed or undisclosed. Furthermore, we found that various basic studies are currently being conducted.

ISSN 2515-8260 Volume 10, Issue 05, 2023

For example, the Russian military research lab [53] and the Small Business Innovation Research (SBIR) program on provenance using blockchain on disconnected networks [42] are such cases.

IV. ANALYSIS OF BLOCKCHAIN R&D TRENDS IN CYBER DEFENSE

Here, we take a close look at the current state of blockchain technology and where it seems to be headed in terms of both academic study and official regulation. We begin by openly describing our survey's structure. Next, we provide our findings after doing research and analysis on blockchain applications, beginning with supply chain and ending with identification and authentication services, Internet of Things, communications, and data integrity. We surveyed many people on how blockchain technology may be used for cyber security. To begin, RQ2 states that we want to "detect trends in blockchain applications by identifying initiatives that are genuinely encouraged by the government" as well as "find relevant studies." Second, the objectives inform the primary categorization of the survey's reference sources. Both are useful, but one is more academic in nature and the other more project-based. Further categorization of project references included official government papers, online sites, company technical reports, and press articles. There were unavoidable allusions to programmes with implications for national security or the military, details of which are sometimes best kept secret. We also avoided duplicating efforts when official records revealed a connection between an ongoing activity and an event in the press. Finally, Google and Google Scholar were the key research tools we used. Using the keywords and citations from the most important sources, we were able to find more relevant references.

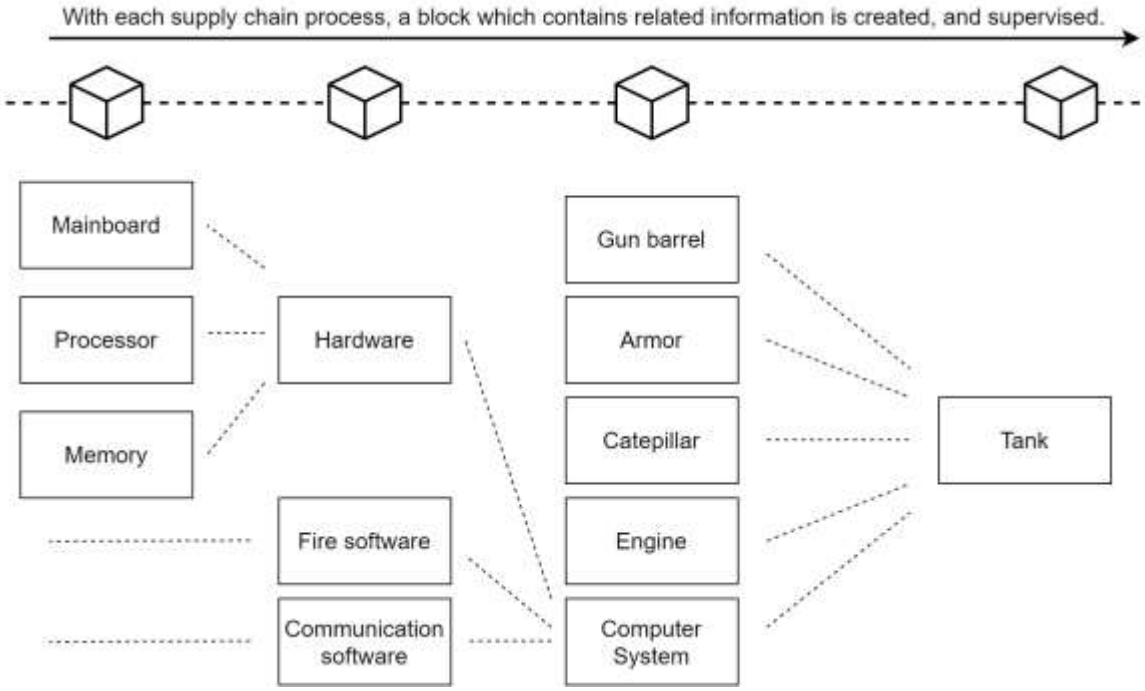

Fig.4 Blockchain-based supply chain example.

To manufacture a tank, there are a lot of components are needed. From a certain level of component, a block is created with the related information. Therefore, we can supervise the supply process of every single tank. Especially, tracking and monitoring of each part prevent the inclusion of fake parts in the tank. Blockchain has the potential to safeguard the SCM data from unauthorised changes. Since they rely on very reliable data, SCM procedures are extremely difficult to tamper with. Using blockchain technology across the board in SCM is intended to mitigate this risk by facilitating the efficient procurement of the appropriate defensive equipment.

Fig. 5 depicts an example blockchain-based supply chain for a tank manufacturer. Major parts include cannons, shields, an engine, and electronics. There are minor parts that make up the larger ones. A block is generated with all the pertinent information about a component during production, allowing suppliers and authorities to keep tabs on it in a completely transparent manner. With the blockchain's immutable data, we think we can stop the sale of fake parts. In SCM, a digital twin is one of the cutting-edge technologies being highlighted. In a multi-party, complicated digital twin process, the blockchain has been shown in several tests to offer safe data management capabilities [60], [61]. Digital twins are cyber representations of physical assets used in industrial management for the purposes of understanding, simulating, predicting, analysing, and optimising such assets. A manufacturer may track and analyse

ISSN 2515-8260 Volume 10, Issue 05, 2023

a product in the digital and informational systems by creating a digital twin of the actual physical product. Digital duplicates of manufactured goods are kept up to date with the same production history as their physical counterparts. During this procedure, data is stored digitally as permanent recordings. Particularly, Putz et al. [61] utilised Ethereum to offer a fully functional open source prototype for a digital twin, implying that a blockchain may be directly deployed to the digital twin.

This is why various different types of SCM and cyber protection R&D initiatives were executed. Hsieh and Ravich [63] looked at the potential of blockchain technology in the logistics industry. From an economic point of view, they explored how a blockchain may prevent assaults on supply chains in cyberwarfare. Rahayu et al. [33] looked at the logistics of implementing blockchain in military supply chains. Nevertheless, the study did not provide any numbers or detailed descriptions of its results. The United States Department of Defense (DoD) has begun work on a blockchain-based supply chain risk management system that takes use of the immutability of Physically Unclonable Functions (PUFs) to save costs while increasing security [39]. The physical microstructure during production is what determines the PUF, making it similar to a digital ngerprint of the hardware. A unique identifier is embedded into the hardware, allowing for efficient supply chain tracking of individual components like chips. The US Navy and the Indiana Technology and Manufacturing Companies (ITAMCO) have begun working together to improve the logistics tracking of aircraft components [22]. Article [26] proved the effectiveness of a blockchain technology pilot project in the aerospace and defence (A&D) supply chains, and businesses are continually discovering new applications for the technology.

V. FUTURE SCOPE AND CONCLUSION

Our research here centred on using blockchain for cyber security. Cyberattacks are inevitable due to the proliferation of digital technology in military and civilian infrastructure. One of the up-and-coming technologies for military security is blockchain technology. Because of its decentralised design, a blockchain can guarantee the accuracy of all data processing. It's a huge boon in protecting systems against cyber attacks. We defined cyber protection and discussed current and future directions in blockchain R&D. We then looked at previous studies and blockchain techniques to identify possible problems that might arise from using blockchain technology. As a result, this study elucidates the benefits, uses, and difficulties of blockchain technology in the context of cyber security.

REFERENCES

[1] E. MacAskill. (2017). *U.K.'s Trident Nuclear Submarines Vulnera-ble to Catastrophic Hack*. Accessed: Oct. 19, 2021. [Online]. Available: https://www.theguardian.com/U.K.-news/2017/jun/01/uks-tridentnuclear-submarines-vulnerable-to-catastrophic-hack-cyber-attack

[2] *National Defense Authorization Act for Fiscal Year 2020*, United States Congr., Washington, DC, USA, 2020. [Online]. Available: https://www.congress.gov/116/cprt/HPRT40810/CPRT- 116HPRT40810.pdf

[3] *Amendment to Rules Committee Print 116_57 Offered by Mr. Soto of Florida*, United States Congr., Washington, DC, USA, 2020. [Online]. Available: https://amendments-rules.house.gov/amendments/SOTO_052_xml713201215551555.pdf

[4] *Amendment to Rules Committee Print 116_57 Offered by Mr. Soto of Florida*, United States Congr., Washington, DC, USA, 2020. [Online]. Available: https://amendments-rules.house.gov/amendments/SOTO_051_xml71320121507157.pdf

[5] Nakamoto. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash Sys- tem*. Accessed: Oct. 19, 2021. [Online]. Available: https://bitcoin.org/ bitcoin.pdf

[6] V. Buterin. *A Next-Generation Smart Contract and Decentralized Application Platform*. Accessed: Oct. 19, 2021. [Online]. Available: https://github.com/ethereum/wiki/wiki/White-Paper

[7] P. J. Taylor, T. Dargahi, A. Dehghantanha, R. M. Parizi, and K.-K.-R. Choo, ``A systematic literature review of blockchain cyber security,'' *Digit. Commun. Netw.*, vol. 6, no. 2, pp. 147_156, May 2020.

[8] Y. Zhu, X. Zhang, Z. Y. Ju, and C. C. Wang, ``A study of blockchain technology development and military application prospects,'' *J. Phys., Conf. Ser.*, vol. 1507, no. 5, Apr. 2020, Art. no. 052018.

[9] B. Lilly and S. Lilly, ``Weaponising blockchain,'' *RUSI J.*, vol. 166, no. 3, pp. 46_56, 2021, doi: 10.1080/03071847.2021.1886871.

[10] P. Bansal, R. Panchal, S. Bassi, and A. Kumar, ``Blockchain for cybersecurity: A comprehensive survey,'' in *Proc. IEEE 9th Int. Conf. Commun. Syst. Netw. Technol. (CSNT)*, Apr. 2020, pp. 260_265.

[11] R. W. Ahmad, H. Hasan, I. Yaqoob, K. Salah, R. Jayaraman, and M. Omar, ``Blockchain for aerospace and defense: Opportunities and open research challenges,'' *Comput. Ind. Eng.*, vol. 151, Jan. 2021, Art. no. 106982.

ISSN 2515-8260 Volume 10, Issue 05, 2023

[12] S. Popov. (2018). *The Tangle (Version 1.4.3)*. Accessed: Oct. 19, 2021. [Online]. Available: http://www.descryptions.com/Iota.pdf
[13] C. Dwork and M. Naor, ``Pricing via processing or combatting junk mail," in *Proc. Annu. Int. Cryptol. Conf.* Berlin, Germany: Springer, 1992, pp. 139_147.
[14] R. von Solms and J. van Niekerk, ``From information security to cyber security," *Comput. Secur.*, vol. 38, pp. 97_102, Oct. 2013.
[15] Balbix. (2020). *2020 State of Enterprise Security Posture Report*. Accessed: Oct. 19, 2021. [Online]. Available: https://www.balbix.com/ app/uploads/2020-State-of-Enterprise-Security-Posture-Report.pdf
[16] PwC. (2020). *Blockchain in Aerospace*. Accessed: Oct. 19, 2021. [Online]. Available: https://www.pwc.com/gx/en/industries/aerospacedefence/ publications/blockchain-in-aerospace.html
[17] L. Martin. (2020). *F-35 Lightning II Program Status and Fast Facts*. Accessed: Oct. 19, 2021. [Online]. Available: https://www.f35.com/ content/dam/lockheed-Martin/aero/f35/documents/FG21-00000_001%20F35FastFacts6_2021.pdf
[18] J. R. Douceur, ``The sybil attack," in *Proc. Int. Workshop Peer-Peer Syst.* Berlin, Germany: Springer, 2002, pp. 251_260.
[19] Galois, Portland, OR, USA. (2016). *Galois and Guardtime Federal Awarded $1.8 Million DARPA Contract to Formally Verify Blockchain- Based Integrity Monitoring System*. Accessed: Oct. 19, 2021. [Online]. Available: https://galois.com/news/galois-guardtime-formal-veri_cation/
[20] S. Ranger. The U.S. Military wants its own encrypted messaging app built on blockchain, ZDNet. Accessed: Oct. 19, 2021. [Online]. Available: https://www.zdnet.com/article/the-us-military-wants-its-ownencrypted-messaging-app-that-uses-blockchain/
[21] *Department of Defense Fiscal Year (FY) 2019 Budget Estimates*, United States Congr., Washington, DC, USA, 2018. [Online]. Available: https://comptroller.defense.gov/portals/45/documents/defbudget/fy2019/fy19_green_book.pdf
[22] J. Neidig. Naval aviation enterprise exploring blockchain with Indianabased company ITAMCO. Cision. Accessed: Oct. 19, 2021. [Online]. Available: https://www.prnewswire.com/news-releases/naval-aviationenterprise- exploring-blockchain-with-indiana-based-company-itamco-300716633.html
[23] DHS S&T Press Of_ce, Homeland Security,Washington, DC, USA. *DHS Awards Austin-Based Factom, Inc. $192k for Blockchain Tech*. Accessed: Oct. 19, 2021. [Online]. available: https://www:dhs:gov/scienceandtechnology/ news/2018/06/15/news-release-dhsawards-austin-basedfactom-inc-192k
[24] Crossword Security, London, U.K. (2016). *Crossword Wins Contract With MOD's Defence Science and Technology Laboratory to Create Blockchain Enabled Smart Documents*. Accessed: Oct. 19, 2021. [Online]. Available: https://www.crosswordcybersecurity. com/2016/05/25/2016-5-crossword-wins-contract-with-mods-defencescience- and-technology-laboratory-to-create-blockchain-enabled-smartdocuments/
[25] J. Wagstaff and B. Kaye. (2017). For security agencies, blockchain Goes from suspect to potential solution. Reuters. Accessed: Oct. 19, 2021. [Online]. Available: https://www.reuters.com/article/us-tech-blockchainsecurity/ for-security-agencies-blockchain-goes-from-suspect-topotential- solution-idUSKBN1DX01A
[26] G. Cowan. Companies look to blockchain to secure supply chains. AIN. Accessed: Oct. 19, 2021. [Online]. Available: https://www.ainonline.com/aviation-news/aerospace/2018-07- 12/companies-look-blockchain-secure-supply-chains
[27] J. Kang. (2018). The department of defense will prepare blockchain application plans till november. Digital Today. Accessed: Oct. 19, 2021. [Online]. Available: https://www.digitaltoday. co.kr/news/articleView.html?idxno=301229
[28] S. Han. (2018). Blockchain introduction to military secret management? Experts say negative. Coindesk Korea. Accessed: Oct. 19, 2021. [Online]. Available: https://www.coindeskkorea. com/news/articleView.html?idxno=30682
[29] E. Janus. (2019). French military police _nds use case for tezos blockchain. Bitcoinist. Accessed: Oct. 19, 2021. [Online]. Available: https://bitcoinist.com/french-military-police-_nds-use-case-for-tezosblockchain/
[30] R. Martinez. South Korean military gets a blockchain-based upgrade. Bitcoinist. Accessed: Oct. 19, 2021. [Online]. Available: https://bitcoinist.com/south-korean-military-gets-a-blockchain-basedupgrade/
[31] Y. Khatri. South Korea's military acquisitions agency plans blockchain pilot. Coindesk. Accessed: Oct. 19, 2021. [Online]. Available: https://www.coindesk.com/south-koreas-military-acquisitions-agencyplans-blockchain-adoption/

ISSN 2515-8260 Volume 10, Issue 05, 2023

[32] T. J. Willink, ``On blockchain technology and its potential application in tactical networks," DRDC_Ottawa Res. Centre, Ottawa, ON, Canada, Tech. Rep. DRDC-RDDC-2018-R033, Apr. 2018.
[33] S. B. Rahayu, N. D. Kamarudin, and A. M. Azahari, ``Military blockchain for supply chain management," *J. Educ. Social Sci.*, vol. 13, no. 1, pp. 9_14, 2019.
[34] C. Chedrawi and P. Howayeck, ``The role of blockchain technology in military strategy formulation, a resource-based view on capabilities," in *Proc. Cogn. Anal. Manage. Conf. At*. Beirut, Lebanon: American Univ. Beirut Lebanon, 2018.
[35] Y. Wang, L. Cong, Y. Fang, J. Deng, and Y. Chen, ``Research on missile data security based on blockchain," *J. Phys., Conf. Ser.*, vol. 1237, no. 2, Jun. 2019, Art. no. 022139, doi: 10.1088/1742-6596/1237/2/022139.
[36] K. H. Lee and H. S. Park, ``Study on trends and strategies for defense blockchain and ICT technologies," *Electron. Telecommun. Trends*, vol. 35, no. 1, pp. 12_24, 2020.
[37] U.S. Small Business Administration, Washington, DC, USA. (2017). *Navy Approved Multi-Factor Authentication for Personal Mobile Devices*. Accessed: Oct. 19, 2021. [Online]. Available: https://www.sbir.gov/sbirsearch/detail/1254599
[38] U.S. Small Business Administration, Washington, DC, USA. (2018). *Automated Processing, Exploitation and Dissemination*. Accessed: Oct. 19, 2021. [Online]. Available: https://www.sbir.gov/node/1413791