



WHITE PAPER



SAFEGUARDING NUCLEAR AND CONVENTIONAL WARHEADS USING BLOCKCHAIN

FARHAN HAMEED KHAN



About the Author

Farhan Hameed Khan is a researcher at the Global Foundation for Cyber Studies and Research. He is a technology innovator, blockchain architect, and a specialist in product development. He has more than 15 years of experience working in the global IT industry and holding a legacy of producing numerous cybersecurity products for the US, Pakistani, and Middle Eastern markets. His work includes Blockchain based solutions, security awareness, phishing platforms, digital verification, multi-factor, biometrics, data protection, surveillance, and encryption technologies. He has a history of collaborating with scientific communities around the world in R&D and innovation. In addition to this, his development contributions are also available on the open-source platforms, especially in the blockchain technology. He is a certified blockchain architect/strategist and has created variations of decentralized multiparty blockchain-based solutions using technologies like Ethereum, Corda, and Hyperledger Fabric. Other than his technology work, he is a great story writer and author of a children's philosophy book "Irteqa-e-Shaheen" which has been published in Urdu language for the children across the World.

About GFCyber

Global Foundation for Cyber Studies and Research is an independent, non-profit and non-partisan policy research think tank. For more information, please visit <http://www.gfcyber.org>

All rights reserved, no part of this publication may be reproduced or transmitted in any form or by any means electronic or mechanical including photocopying, recording or any information storage or retrieval system, without the prior written permission of the copyright holder. Academic and research institutions are granted permissions to make copies of the works strictly for research and educational purposes, using the citation style mentioned at the bottom of this page, without any explicit permission from GFCyber. Please direct all your enquiries to info@gfcyber.org

GFCyber does not express any opinion of its own, all opinions expressed in the publications are a sole intellectual representation and responsibility of the author(s).

Cover Design: Muhammad Babar Khan

Styling Credit: Amanullah Quadri

Webmaster: Fajri Kurniawan

Citation Style

Farhan H.K., "Safeguarding Nuclear and Conventional Warheads using Blockchain", Global Foundation for Cyber Studies and Research, Washington D.C. USA, April 2020.



Safeguarding Nuclear and Conventional Warheads Using Blockchain

Abstract

The advancement in technology is rapidly threatening the digital infrastructure and industries with the cyberattacks. These threats are not limited to commercial sectors, but sensitive institutions like the military, nuclear plants, responsive logistics, and government command systems are also under the radar of cyber threats. The impact of these threats is unimaginable if a non-state actor compromises these sensitive warheads for different purposes; therefore, such risks are not limited to a country, but it covers an entire region or the world as a whole. The blockchain technology is being discussed mostly in the financial perspective; however, in this paper, we present how this technology can create a new wall against such attacks on military and nuclear installations.

Introduction

Bitcoin established the blockchain technology's capability to safeguard digital trust using provenance and immutability. When we talk about the blockchain, we mostly discuss how the distributed ledger is using sophisticated encryption and producing a chain of records; however, the real heart to mention about this technology is its democratic consensus system. Over the past few years, the networks in any institution were looked at as a centralized system, regardless if they were technically distributed for backup or any safeguarding purposes, but the whole idea behind these networks is to control centrally.

In the military, centralized governance and control systems are very much in practice at this moment, which is one of the reasons why these systems could play a significant role in catastrophe if an enemy actor disrupts the communication or warhead data.


There are many incidents reported about militaries that they have faced genuine cyber-attacks while performing their warheads tests. By leveraging the blockchain technology in sensitive eco-systems can minimize such attacks. Additionally, it can provide a new model where military officials have to think about how democratically they can manage their sensitive data since the next war will not be fought on land but on the digital frontier.



Security Threats in Different Nuclear Warheads

It is difficult to believe that the warheads which a nation uses can possess cyber threats to themselves, but the fact of matter is these difficulties are not new. They were always there since the dawn of new inventions in the field of warfare. Below are some of the significant points that outline the vulnerabilities in warfare systems, including the command and control systems of the nuclear arms:

- Those countries who possess nuclear warheads have distinct command and control authority to activate or deactivate their atomic warheads. Generally, a group of individuals constitute the commanding authority for any preemptive or reactive actions; however, in desperate times, the action is required in minimal time [1]. Therefore, for such authority, it is essential to identify if a threat is real, and it requires some preemptive or non-preemptive actions. However, a cyberattack could infiltrate the communication data by showing fake incoming physical attacks between these commanding participants; this could lead a reason to start a fake war against another country or launch of a warhead.
- The supply chain of nuclear materials also poses a threat to every nation using it either for defense or energy. Therefore, it is incumbent to track and secure nuclear materials within their borders. The ability to track the uranium and its usage can avoid nuclear terrorism, and restricted monitoring of these radioactive materials in real-time is an essential security measure [2].
- Many countries are still using legacy systems for their warheads, and due to this reason, a centralized command and control system is still in practice. These command and control systems receive data from different types of sensors for an incoming physical attack, who direct them to counter or defend such an offensive strike using a defensive weapon system. However, due to the centralized nature, such systems are vulnerable to a centralized cyberattack regardless if it is coming from an external non-state actor or an inside black-sheep.
- Battle plan on the battlefield has an integral role in achieving successful missions. However, if a plan required continuous communication between battle participants, then insecure transmission could jeopardize the whole mission. The centralized management of digital communications is vulnerable to cyberattacks that spoof commands or provide fake data on the progress of the fight plan. The impact could be dangerous and reverse the whole strategy against the existing battle plan.
- The nuclear and non-nuclear warhead hardware is mostly dependent on computers, motherboards, and microchips. However, it has been reported that there are cases when a microchip allegedly allowed the external attacks to create a backdoor into the network. This spy chip could cause machines to alter their programming and turn them into a spy radar. These undetectable chip tamperings are also a big issue for the military installations, where most of their work requires hardware-based digital infrastructures.
- Intelligent systems that are dependent on swarm processing with self-organized capabilities also possess threats. When warheads like drones or robots need to do close coordination, for instance, if one of the swarm devices gets hacked, then there is a possibility exists to alter the “global knowledge” between other swarms. This inter-swarm communication between each swarm device means each



of them is open for a cyberattack from the outside. To persist, the accurate global knowledge between these devices is a tough job, especially in the warzones.

- Nuclear device activation control panels are also something that should need a democratic control system. By distributing the power of activation between different human participants can decrease insider threats. However, in the digital era, when things are moving with more powerful artificial intelligence and battle moves built on computer algorithms, they still need a voting system inbuilt with their nuclear device control system.
- Uncontrollable AI decisions is also a significant area of research, wherein the warheads in the future will require minimum interaction with the human controller. There are reports of drone algorithms that can estimate the distance to the target and attempt to strike the targets even outside their targeted scope.

Blockchain - The Missing Brick in Digital Trust Between Isolated Parties


It is the concatenation of multiple technologies that contributes to the “digital trust between participants.” Technologies like distributed-ledger, chain-of-records data structure, RSA-encryption, peer-to-peer network, and democratic-consensus-protocols are the source of this novel invention.

For instance, combining distributed-ledger and chain-of-records helps in distributing duplicate data between participants with the immutability feature on the network. Additionally, using RSA-encryption to verify the data or hide its knowledge, and to add anything on the network requires approval from decentralized peer-to-peer decision-making democratic-consensus-protocols.

The abovementioned five technologies, with the add-on of smart-contracts or chain codes, give the power of programmatically enabled rules and regulations on the network as per each participant requirement. We look at the term as server-side and client-side, and see the possibility of an attack on a centralized server. However, in the case of blockchain, it is impossible to compromise anything centrally. For example, DDOS (Distributed Denial of Service) attacks cannot work because of the network nature where each node is distributed with its self-aware existence in peer to peer fashion.

Even if an attacker compromises one of the nodes in the network, he still cannot penetrate the entire network or change any data at all. Because to compromise the network, an attacker needs to control specific nodes based on the threshold ratio for any approval required, known as 'hashing power.' For instance, to compromise a Bitcoin or Ethereum network requires an attacker to hack more than 51% of individual network nodes. Well, this one is for the open public blockchain network; however, for the private/ federated blockchain network or consortium-based blockchain network, different ratios are used. There are different consensus protocols where an attacker might need to control the entire or 100% network to infiltrate any data.

Furthermore, the essence of distributed nodes is also a significant hurdle to attack an entire network, where each node not necessarily deployed under one entity or its datacenters. If an attacker compromises a consensus protocol within a node or multiple nodes, still he has to capture the entire network nodes' consensus protocol, therefore, altering consensus code within one machine is entirely useless and the waste of time.



Similarly, an insider or perpetrator within one participant's premises can penetrate the vulnerable network nodes. But still, the blockchain's democratic distribution of nodes disallows the attacker to compromise the entire eco-system between multi-participants, where each party contains the whole history of the real data. This pure data can only be added back to any new network node regardless if it was attacked before or came for the first time.

Blockchain technology ensures data protection against any perpetrators. In case of an attack, the democratic threshold of the votes from all the nodes decide whether the data be allowed or rejected on the encrypted network. Therefore, leveraging blockchain technology in safeguarding the warfare assets is a key to defend against cyber threats.

Public, Private or Federated Sensitive Data

Each blockchain type comes with its own merits and demerits, and this is where most of the organizations get confused in choosing the right blockchain network. When we talk about the military or sensitive installations, we see these institutions require a private or federated blockchain network. However, the possibility of encrypted hashes or data can also be placed on the public blockchain network, which will be completely irreversible and anonymous.

It is a vital role for any sensitive entity to identify their dynamic and non-dynamic data as highly classified private data or classified permission data or classified sharable data or authentic shareable public data.

- The highly classified private-permissioned data denotes such data that does not require a department or an entity to share with anyone, but with minimal numbers of identified users. For example, data communication between the state's president or prime minister with the army chief of staff needs a highly secured private encrypted channel. This data cannot be shared within a department, but only official personals can be allowed to read.
- The classified permissioned data denotes the permission-based accessibility to that data for some users, regardless if they belong to the same department or within a single department. To access this data, they would need proper access or privilege to see or use. One of the examples is the sharing of sensitive files between departments within an army installation. This data cannot go outside of its premises.
- The classified shareable data usually managed between known participants who do not belong to the same premises, but exist externally. This kind of data is used in the communication between devices/persons from different multiple sensitive platforms e.g., drones with command and control.
- Another classified data could be the sharable data, which can be utilized by the public. For instance, in desperate times and chaos, fake news can be countered using this technique and data to keep citizens inform about any attack or emergency. This data is very important because information warfare is also used as a weapon to jeopardize the battle plan using public sentiments.

In order to select an appropriate blockchain network, it is highly important to identify battle participants and classifies the war data. This selection can be made using a proper blockchain strategy for each warhead within or outside sensitive installations.



Choosing Correct Blockchain Network for the Warheads

The first network invented using blockchain technology is a public blockchain; however, the technology was experimented later using the private and consortium-based or permissioned networks.

The Public blockchain network is a network that cannot be controlled by anyone. However, the capability of smart contracts can give strength to secure access with quantified encrypted data using programmatic rules. This development requires the developer to write a highly secure code using the secure patterns and maintains the user privileges and permission in the smart contract. Furthermore, the data itself will be visible entirely to anyone; however, irreversible hashes or encrypted data can be a useful technique requiring a backup or out of premise storage. Why one should use a public blockchain network is also depends on the scenario where one does not need to rely on the data within premises at all. However, they want to rely on something that can be used as a trusted layer between participants who do not want to reveal if they have any physical network at all.

Federated blockchain network is similar to a consortium network; the sole purpose of this network is to remove the single influence between multiple participants and make it a clear democratic way to store or share data. In this scenario, the data will remain under private entities, and no data will go outside from their boundaries. A situation where government and military need to work together to launch an activity requires this kind of a network, simply because it will remove the centralized attack or centralized insider job to harm the country or biased non-democratic actions.

The private blockchain network is something that might have a zero value in the commercial market. However, this is the best approach where the data supposed to live within the boundary of a single entity while permission supposed to be given to sub-departments so they can even verify sharable data between each other.

This network is an excellent choice when internal departments verify communication or data from each other using proper protocols. Its features could create a more democratic and authentic environment to see any approval or disapproval. In an exigent situation, even if one department cannot completely trust the other, an electronic trust layer between departments will minimize cyber-attacks or data leaks.

There is another network of the blockchain which could be labeled as a hybrid network with the capability of sharing data from federated or private to the public using interoperability protocols. This type of scenario has a public engagement or two-way communication without the involvement of any sensitive network. The interoperability from federated or private to the public can create this kind of access for specific situations.

Below is the table that differentiates between network types:

Table 1.0. Types of Blockchain Networks

Internals	Public Blockchain	Private Blockchain	Federated Blockchain	Hybrid
Public Access	Yes	No	No	Depends
Network Control	0%	100%	Democratically decided	Partial / 50% or depends
Customize Regulation	Yes, using smart contract	Yes (smart contract, credential provider, certificate authority, customize network)	Yes (smart contract, credential provider, certificate authority, customize network)	Yes (private smart contract, credential provider, certificate authority, customize network) and , using public smart contract
Access level	Public can view / add	Only known can view or add within premises	Only known can view or add within or outside premises (Optional : Public can view under permission)	Only known can view or add within privately or under federation. Interoperability used for public view.

Combining Blockchain with Nuclear Warheads Eco-System

As discussed earlier, the possibilities of cyberattacks on nuclear warheads thoroughly, and most of the area showed this vulnerability could be engaged to turmoil the battle plan strategy and disrupt the defense system. The following are the areas where blockchain technology can help or guide the military installations to avoid any future cyberattacks or inside attacks.

Command and Control Communication

The command and control authority to make the decision requires a short time span, primarily to address the incoming physical threat. However, the cyber threat could trick or infiltrate the decision between state personal's communications.

A blockchain federated permissioned network under the recognized or known participants would need a democratic decision strategy, where individual votes must be casted by each participant. For instance, military and government, if required to take action like addressing the physical threat against their nation, then both entities distributed federated permission nodes can initiate the demand of a defensive or offensive strike. These nodes will require certain prominent members' input to vote for approval from each participated entity; this could make the control democratically distributed between institutions.

Using blockchain in such communication helps in avoiding a fake war initiation, removal of biased centralized actions in launching nuclear warheads, and challenging to alter anyone's decision in the control center.

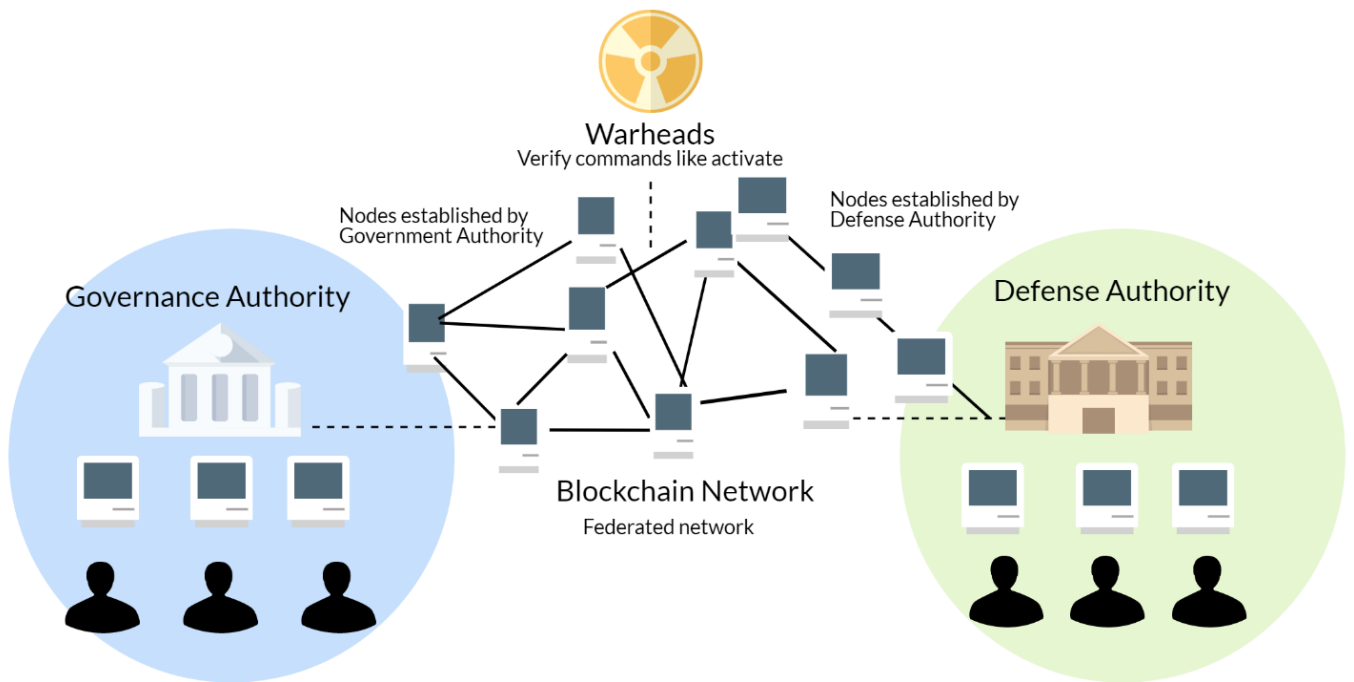


Figure 1. Communication Network between Government and Defense Authority

Radioactive material usage and supply chain's real-time tracking

Nations that possess nuclear technology use radioactive materials for their defensive warheads or experimental requirement. These materials, like Uranium, would need restricted security controls, including track records of each supplied item and material [2]. However, changing the data within database or computer files even in a restricted environment is possible; this data-change attempt can come from anywhere, even from unauthorized external sources such as a malicious individual or state actors.

Using blockchain technology under permission privileges can ensure the integrity of the data, especially by adding machine-based input, thereby minimizing the need human and consequently reducing the possibility of contamination of the data. The clean data then could be sent to the blockchain and make it immutable with zero integrity. The close integration of the tracking and monitoring systems with the blockchain will ensure the integrity and authenticity of the real time data. For such integration, smart circuits and sensors can help in collecting the real time movement of any radioactive material under or outside the premise; all such sensor and smart circuits can play their role of smart nodes.

Additionally, the same strategy can be followed to safeguard the supply chain or logistics of atomic warheads by removing the presence of a human element in monitoring and tracking records. Secondly, by making each real time local record immutable and shareable between the auditing teams on the blockchain network. Therefore, even if someone would able to change a digital record on the local monitoring system cannot alter its proof on the encrypted network.

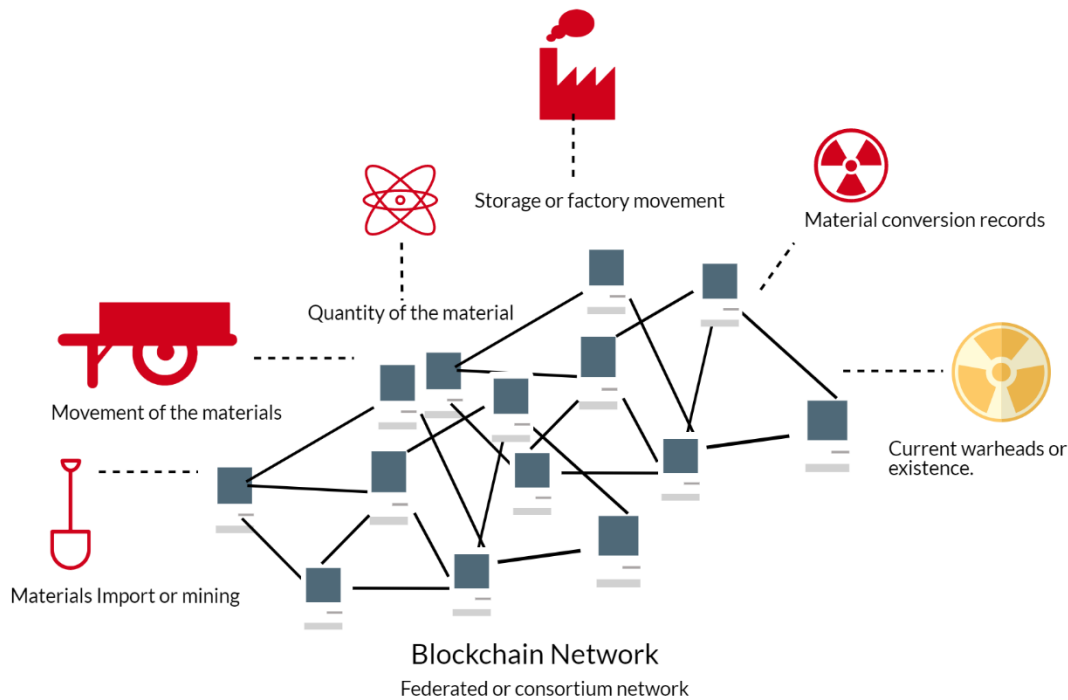


Figure 2. Network between Sensitive Supply Chain Stakeholders

Uninterrupted and authentic communication between the authority and war-assets

The centralized communication between a nuclear asset and the commanding station is also a vulnerable area. Usually, these assets get a command digitally from a central authority of the defensive system which does not guarantee that the command to launch a missile strike is really coming uninterrupted from the administration, what if encryption keys were compromised or lost.

These questions and scenarios reveal a big gap of trust in the communication between authority and its warheads; therefore, existing strategy to trust entirely on the control panel and its assets is not only dangerous, but could create a catastrophe in desperate times.

To counter these issues, a private blockchain network between asset control panels, commanding authority, and physical assets can minimize many security risks. For instance, command authority receives incoming threats data from their satellites, radar, and other monitoring-sensors. Once these incoming data reaches the command authority, they approve and send the action to launch the missile asset [3]. These centralized communications are vulnerable; however, adding a blockchain peer to peer distributed network in between them will work according to the battle plan.

Any server or servers are vulnerable in the client-server network, but if those servers exist in a distributed manner loosely coupled and each server or node verifies the data individually, then an attacker needs to hack the entire nodes or servers. If the ratio of the power threshold is 90%, then an attacker needs to hack a 90% network to infiltrate the commands between command control and the launching pad. This technique minimizes such attacks and improves security in the protection of sensitive communication.

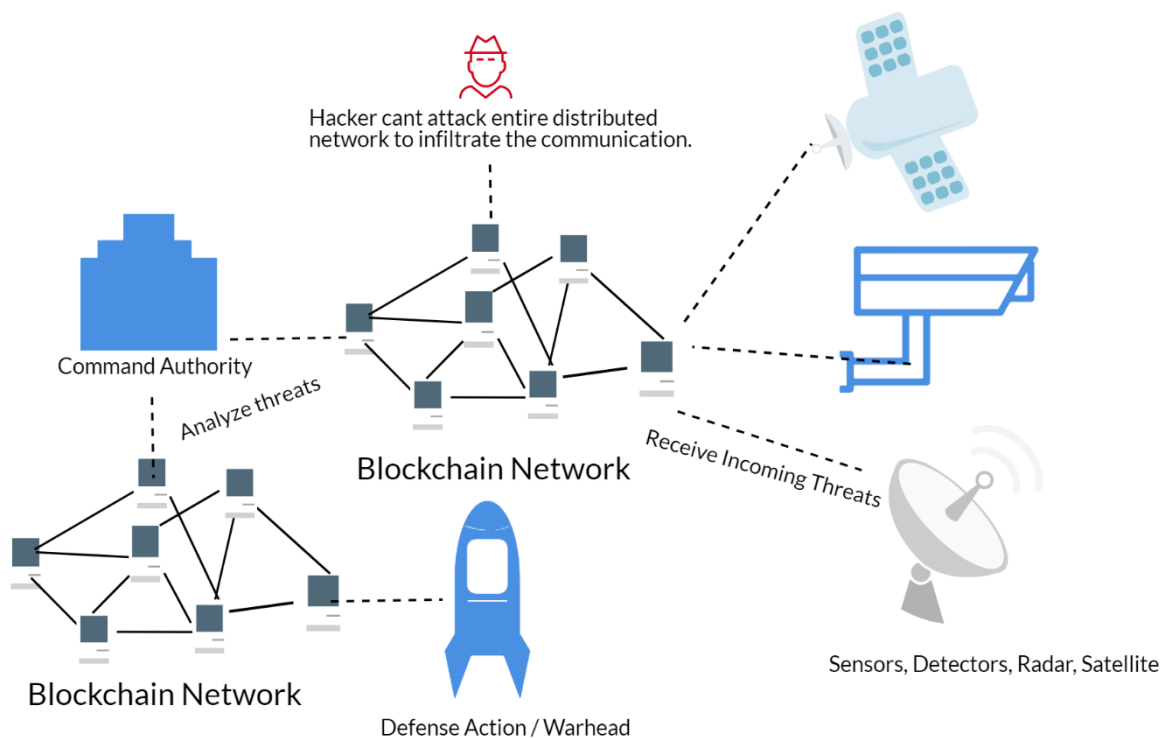


Figure 3. Uninterrupted Network in Exigent Scenario

Microchip, motherboard and digital hardware authenticity

The term “big hack” came when it was revealed that the hardware vulnerabilities are a bigger threat than the software ones inside many sensitive systems in the military. Wherein, an attacker can secretly extract the data and send it to the perpetrator, this hack is happened due to the manufacturing companies who were collaborating with other manufacturers to develop microchips for devices and systems. A tiny chip, which is equal to a single rice grain, was used to infiltrate the data between sensitive installations [4].

The blockchain technology can help here in improving the trust and assurance by adding the concept of “secure digital twin” for circuit or chip manufacturing. The secure digital twin provides complex fingerprinting data, which is made out of uniquely built chips, sensors, circuits, etc., this fingerprint can help the auditors to identify and review the provenance and immutability of the hardware.

This proof can be stored on the encrypted network of the blockchain by the trusted manufacturers. This network can be arranged between the buyer, manufacturers, and contractors where a buyer can compare the digital twin and see if the hardware digital twin matches with the record on the blockchain. Otherwise, the hardware would be considered tampered or corrupted. This preemptive approach will help a military establishment to obtain only secure equipment, which will minimize the cyber risks attached to it.

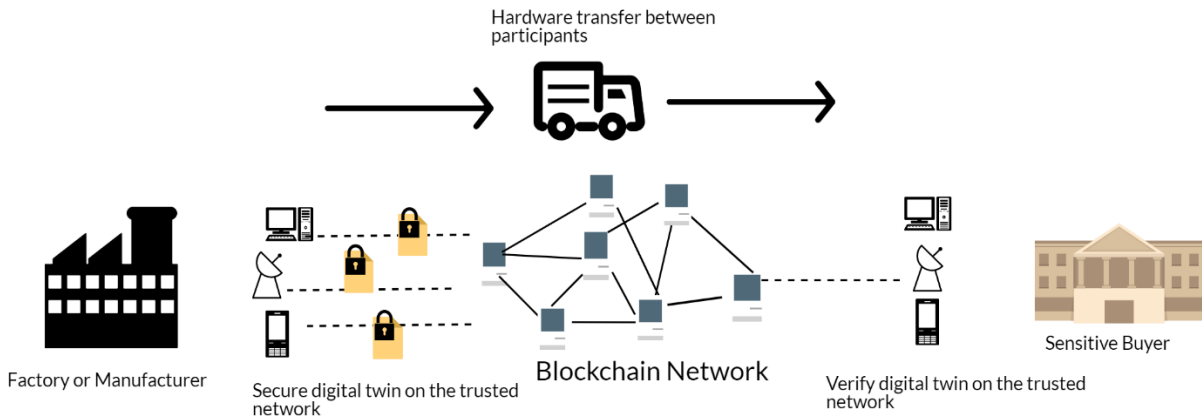


Figure 4. Digital Twin on the Network between Multi-participants

Automated swarm systems and authenticity

Swarm intelligence is in a great demand and comes with different warheads like weapon-sensors, robots, and drones. This system works through inter-communication and sharing artificial intelligence experiences of the environment and threats [3]. Their objective is to function in tandem with other swarm systems and overcome an opponent's defense and destroy the target. The swarm inter-communication is completely non-centralized communication; however, due to their autonomous system in comparison to other systems, the communication is vulnerable to the hacking. It can affect the coordinated attacks or defense because all swarm shares global knowledge regarding their experiences and next move.

In swarm inter-communication, a blockchain network can play a vital role in protecting the global knowledge between systems. Each swarm device, robot, or drone will act as a node of the blockchain network [3]; therefore, a bad node can be easily identified based on the consensus of validation. Consequently, approved and verified data between swarm can be easily managed and controlled using the distributed ledger technology between each node or swarm.

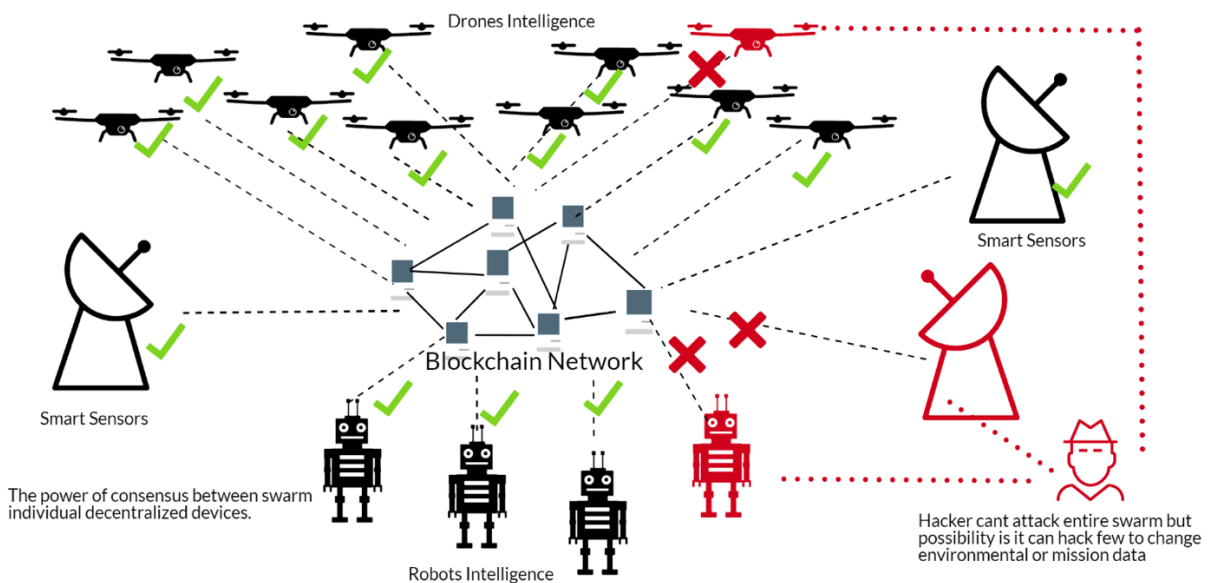


Figure 5. Consensus between Swarm Devices to Verify Reports



Democratic controls on nuclear warheads

Nuclear weapons are dangerous if any biased mindset or biased agenda controls them. Each country who possess these arms not only needs to protect them but also share the power of activation between different participants. In the digital age, where everything is transforming from manual to automation still requires manual intervention with democratic essence. Therefore, digital identities on the decentralized, encrypted network is an important aspect to protect identity theft and democratic control.

The authority to launch these warheads requires a private blockchain network, where consensus or vote must be cast by every authority-sharing individual electronically using their relevant identities. These measures are necessary for obtaining democratic approvals for strikes using warheads, and it will protect such dangerous weapons from being misused.

Furthermore, it protects from cyberattacks to launch an offensive strike to wage war between countries, to sabotage their nuclear arsenals, or to corrupt the system. This activation protocol requires engineers to introduce encrypted decentralized digital identity network along with the integration of warhead control systems.

Global Acceptance of the Blockchain Technology in Military and Defense Institutions

Currently, many countries are targeting blockchain and AI technology in the governance of sensitive institutions to protect their systems or to use it as communication networks.

USA / DARPA

The Defense Advanced Research Projects Agency (DARPA) is experimenting with blockchain to create a more efficient, robust, and secure platform via blockchain-based protocols that will allow personnel from anywhere to transmit secure messages [5]. This application has several uses such as, facilitating communication between units and headquarters, transmitting information between intelligence teams and the Pentagon [5]. DARPA also has been trying to develop an 'unhackable' code using blockchain as it offers intelligence on hackers who try to break into secure databases.

China


Chinese military could implement a blockchain rewards system to manage personnel data and to incentivize its workforce [6]. The blockchain system would likely not involve financial incentives, but would be used as an innovation strategy for the military's management.

Russia

Russian creation of a military research lab inside the country dedicated to studying how blockchain can be used to detect and possibly counter cyber-attacks [7].

South Korea

South Korea's defense department announced a blockchain pilot program to prevent external tampering with its military supply chain. The history of the entire process from bidding, evaluation, and results for



defense improvement projects will be recorded on the blockchain, enabling more transparent management of the company selection process [6].

NATO

“Yes, potentially. Digital technologies have been transforming warfare since the 1990’s so emerging technologies such as blockchain have the potential to define the war industry over the coming decades. Data and data sharing will be critical for warfare in the future, particularly with the development of artificial intelligence. [6]”.

- NATO Secretary General Anders Fogh Rasmussen

Future View with Artificial Intelligence, Blockchain, and Nuclear Warheads

There are several research reports available, which predict that post 15 years, all the wars strategies will be controlled by artificial intelligence for most of the developed countries. These intelligence systems will not require human intervention, or it is safe to say that it will minimize human interaction to the least [8]. Additionally, it has been predicted that probably the next Chief of Army Staff post 20 years would be an AI. If the above statements and reports are even slightly correct, then there is no reason not to worry about the future because such future possesses threats and risks from the very own same technologies which we have built to protect us.


In order to understand this threat, it is essential to magnify such technology as Public blockchain networks, which are the immutable technology uncontrollable by humans. The concept of decentralized autonomous organization is a concept that is existent on the public blockchain, where human resources can be removed entirely or slightly, and the organization’s protocol rules and jobs would be written in the smart contract. In other words, the code will be the law for the organization, and hence it does not need to be directed by extensive involvement of the human.

Now the exciting part is when you combine the DAO concept with artificial intelligence, which ultimately opens the door of unanswered questions to the unexplored world. By extending the same idea with nuclear weapons like drones, jets, and submarines, you can see the unknown danger because of the same technology, but this time, prevention is not from the human but the machines.

The whole idea treated as science fiction and creates questions like what if an artificial intelligence writes itself on the public blockchain to live its code forever? Furthermore, what if it sales on e-commerce stores its services so it can power up more hashing power on the network, and what if this intelligent system provoke a nuclear war? Since it knows it will live forever on the distributed ledger technology, but maybe the three laws of AI do not work anymore due to the consciousness of the AI.

- An AI must not injure a human
- An AI must obey the order given by human
- An AI must protect its own existence

All these questions are like a science fiction story, but we are not very far away from where an intelligent system could write a better programming code as compared to the human programmers. Therefore, it’s not very hard to imagine that AI can write its code in the future to live forever on the distributed network. The idea is hazardous and seems like a movie terminator where a Skynet tries to capture the entire world or matrix where artificial intelligence had the conscious of controlling a human as a battery.



Aside from such imagination, after the inclusion of Quantum computing, a more powerful blockchain system and artificial intelligence will rise, and this is where a human community needs to safeguard their very own warheads not only from humans but from virtual beings as well.

Conclusion

In this paper, we discussed how blockchain could be leveraged in protecting nuclear warheads from cyberattacks and minimize the national security risks using several scenarios. We also learned about a few nations that are considering blockchain technology to protect their arsenal and to see the possibility of using it as a trust machine between sensitive installations. The right choice of blockchain network under different warzone circumstances is the key to strategize a preemptive approach from cyber risks in protecting sensitive arms. The blockchain technology is an amazing technology that can give great possibilities, including protecting nuclear weapons. It can fill the gap of trust between participants and make sure that none can alter the message, which was put on the network. However, great power comes with great responsibility, and this is what every federation needs to understand. Therefore, every nation has a great responsibility to address this sensitive issue and minimize digital risks, which could create a havoc against themselves in desperate times. Additionally, it is important to understand that every technology has its strengths and weaknesses regardless if the subject is of Quantum, Blockchain or AI.

References

- [1] Beyza Unal and Patricia Lewis | International Security Department | January 2018 | Cybersecurity of Nuclear Weapons Systems Threats, Vulnerabilities and Consequences | <https://www.chathamhouse.org/sites/default/files/publications/research/2018-01-11-cybersecurity-nuclear-weapons-unal-lewis-final.pdf>
- [2] Preventing Proliferation: Tracking Uranium on the Blockchain | April 2018 | MEGHNA BAL https://www.orfonline.org/wp-content/uploads/2018/04/ORF_Issue_Brief_235_Blockchain-Uranium.pdf
- [3] Why Military Blockchain is Critical in the Age of Cyber Warfare | Dr. Victoria Adams | Mar 5, 2019 | <https://media.consensys.net/why-military-blockchain-is-critical-in-the-age-of-cyber-warfare-93bea0be7619>
- [4] The big hack how China used a tiny chip to infiltrate USA top companies | Bloomberg - Jordan Robertson and Micheal Riley | 2018-10-04 <https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies>
- [5] DOD-DIGITAL-MODERNIZATION-STRATEGY | Jul-12-2019 | Department of defense United states of America <https://media.defense.gov/2019/Jul/12/2002156622/-1/-1/1/DOD-DIGITAL-MODERNIZATION-STRATEGY-2019.PDF>
- [6] Coin telegraph - Weaponizing blockchain vast potential but projects are kept secret | Andrew Singer | Nov 09 2019 <https://cointelegraph.com/news/weaponizing-blockchain-vast-potential-but-projects-are-kept-secret>
- [7] RUSSIAN NEWS AGENCY | 22 AUG 2017 | <https://tass.com/defense/961423>
- [8] Pakistan politico Militarization of Artificial Intelligence | October 17, 2019 | Shaza Arif <http://pakistanpolitico.com/militarization-of-artificial-intelligence/>



Global Foundation for Cyber Studies and Research (GFCYBER) is an independent, nonprofit and non-partisan think tank, which conducts studies and research and provides consultation on cyberspace challenges and issues from the intersecting dimensions of policy and technology for the betterment of a globally-connected world. The foundation works on the philosophy that together we can secure the cyberspace!

Contact Us:

5614 Connecticut Avenue, N.W., No. 209,
Washington, D.C. 20015, USA.

 www.gfcyber.org

 info@gfcyber.org

 [@gfcyber](https://twitter.com/gfcyber)