Proceedings of the International Conference on Intelligent Sustainable Systems (ICISS 2017)
IEEE Xplore Compliant - Part Number:CFP17M19-ART, ISBN:978-1-5386-1959-9

Employability of Blockchain Technology in Defence Applications

Amool Sudhan[1#], Manisha J Nene[2$]
[1,2] Department of Computer Science and Engineering
Defence Institute of Advanced Technology (DU)
Pune, India
[#]amool_mcse16@diat.ac.in, [$]mjnene@diat.ac.in

Abstract— **Military operations enabled using networks involves generation, transmission, collection and analysis of mission critical data to enable better decision making capabilities to commanders at all levels to achieve the objectives. This data is generated by variety of heterogeneous elements like humans and equipment in the battlefield. It is of utmost importance to ensure high level of integrity, confidentiality and availability of this data in such an environment and to ensure its sustainability in hostile environments. This paper presents scope and detailed analysis of the idea of utilizing Blockchain technology as a viable solution for ensuring integrity and provenance of data to suit military operations using networks and maintaining sustainability of these networks. The core concepts of Blockchain are presented in a comprehensive manner along with its variations. Military operations enabled using networks are modeled using Network Enabled Military Operations (NEMO) model. The viable framework and architecture for incorporating Blockchain technology to suit security requirements has been analyzed using three case studies relevant in today's scenario.**

Keywords—Battlefield Management System (BMS); Blockchain; Consensus Mechanism; Cryptography; Cyber Security; Digital Signature; Distributed Ledger Technology; Defence Application; Immutability; Logistics; Network Centered Operations; Peer-to-Peer network (P2P); Smart Contracts; Supply chain management.

I. INTRODUCTION

Military operations encompass all actions undertaken by state/ non-state actors in the domain of land, air, sea and space to achieve a well-defined objective [1]. To facilitate any successful military operation, various heterogeneous players coordinate their actions based on information derived from different sources in the complex environment. These sources include humans, weapon systems, sensor grid data from aircrafts, warships, radars, military satellites etc. These sources are either part of the backbone network or adhoc networks that enable networked military operations [2]. Examples include Battle field Management Systems.

The information derived from this data is collected and disseminated across the players to assist them in making better decisions that facilitate success in operations [3]. Majority of such existing technologies are based on centralised control, ensuring data security and measured transparency. Centralised control is also prone to single point of failure. Hence, alternate means needs to be identified to make these systems more secure and sustainable.

Blockchain based data provenance [4] in the form of distributed ledger technology can enhance the data availability and ensure data integrity by offering transparent and tamper-proof records. The immense popularity and success of *Bitcoin*, the first decentralised and most widely accepted cryptocurrency till date, built using blockchain technology has proven that blockchain possesses the capability to become a disruptive technology.

Substantial research is being carried out in the areas of blockchain and its applications. However, scope of incorporating blockchain technology in defence sector has not been studied in detail prior to this study [5].

The paper is organized as follows. The proposed NEMO model is described in Section II. Section III explains Blockchain technology and its features used in NEMO models. Section IV highlights the salient features of Blockchain technology. Section V discusses the advantages on using blockchain in NEMO using three Case Studies. Section VI concludes the paper and proposes scope for future works.

II. NETWORK ENABLED MILITARY OPERATIONS (NEMO)

The primary players of any networked military or defence environment are Hosts and Inter Networking devices. They form the backbone for any military operation in a networked environment and are responsible for generation and communication of information [6]. This information sharing in real time enables transparency and clarity in viewing and understanding the environment. This can help commanders at all levels to take better decisions.

This paper proposes NEMO models, existing data flow communication models and new framework inclusive of blockchain to assure high level of integrity and accountability in data and control flow.

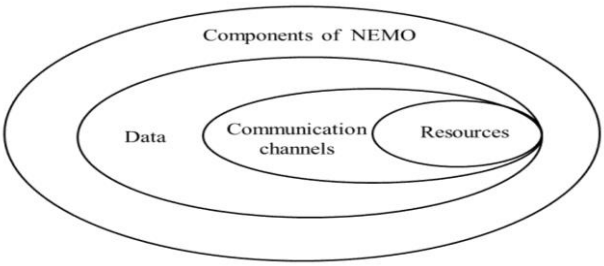

Fig. 1. NEMO Components

TABLE 1. ELEMENTS, THREATS AND DESIRED FEATURES

Charact-eristics	Components Of NEMO		
	Resources	Communication	Data
Elements	Hosts: • Users Equipment: • Sensor grid • Satellites • Weapon systems • Surveillance devices	• OFC • Cable • Terminals • Routers • Radio • Microwave	• Voice • Data • Images • Consolidated database
Threats Faced	• Physical attacks • Sabotage • EMP	• Electronic warfare threats • Jamming • Masking • Deception • Eves dropping • Corruption of channel	• Eves dropping • Corruption • Manipulation • Data Breach • Denial of Service
Desired Features/ Requirements	• Reliability • Robustness	• Secrecy • Secure data communication	• Immutability • Availability • Resilient against data corruption

The framework of Network Enabled Military Operations (NEMO) can be defined as a robust network established between players in a complex military environment that facilitates the availability, confidentiality and integrity of data transmitted between these players [7]. The data shared among these elements is crucial for enhanced situation awareness and mission effectiveness in military operations.

The main components of NEMO as shown in Figure 1. includes:

- Resources involved in generation of data and analyzing received data.
- Communication channels.
- Data transmitted.

Details of elements that constitute NEMO, threats faced and desirable properties to withstand these threats are listed in Table 1. Use of blockchain technology can address the threats faced by NEMO and fulfill the requirements in data and communication sectors.

III. BLOCKCHAIN IN NEMO

Blockchain technology can be viewed as the fifth paradigm of computing technology following the mainframe, the personal computer, the Internet and finally the mobile and social network revolution [8].

A blockchain is an algorithmic data structure that allows the creation of a resilient tamper-proof digital ledger of transactions between various users/ nodes. This technology uses public-key cryptography to sign and secure transactions among users/ nodes. The transactions are then stored on a distributed ledger. The ledger consists of cryptographically linked blocks of transactions, which form a blockchain. It is immutable to alter or remove blocks of data once they are recorded on the blockchain ledger.

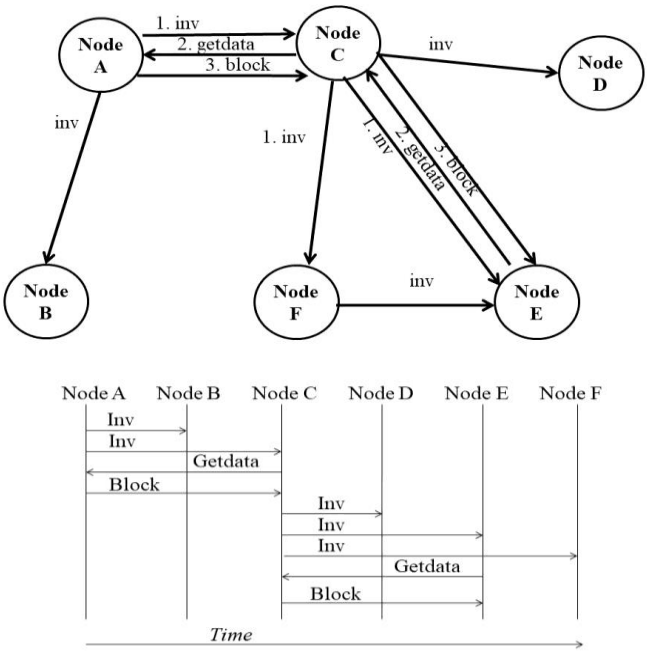

Fig. 2. Message propagation among nodes in a Peer-to-Peer network and Time Sequence using Gossip protocol.

A. *Blockchain Enablers*

Bitcoin was the first digital cryptographic currency system that introduced the concept of blockchain and used it as its underlying technology [9]. The technologies that enable blockchain are described in context with Bitcoin.

1) Peer to Peer Network (P2P): Transmission of data/ blocks through an ad hoc peer-to-peer network (P2P) requires specialized nodes/ users. Each node/ user in this decentralized communication model possess varied capabilities like validation and addition of data into the blockchain and are responsible for running the whole P2P network. Gossip Protocol [10] is implemented to flood the data in the network.

Figure 2 depicts the propagation of a message through the network and time sequence for the same. Nodes send INV messages containing hash of new blocks/ transactions created/ received. Peers can request this data by responding with a GETDATA message following which the data is forwarded only to the node requesting it. This prevents infinite propagation of the message in the network. Ability of nodes to join/leave the network randomly and lack of centralized control makes the network *fault-tolerant.* The network can easily accommodate growing number of nodes and adapt to frequent change in network configuration making it highly *scalable.*

2) Cryptography: In order to preserve the integrity of the blockchain, each block in the chain confirms the integrity of the previous one, all the way back to the first one, the *genesis block*. This is achieved by using cryptographic techniques.
Data authentication is ensured by using Public key cryptography. ECDSA (Elliptic Curve Digital Signature Algorithm) [11] is widely used for generation of public and private keys. Any message or data transmitted from a node/ sensor is signed with the private key of the sender and contains the public key of the receiver before it is broadcast to the network. Sender's signature on the message verifies for everyone that the message is authentic. The complete history of transactions is stored by every node, so that anyone can verify the source of messages.

3) Consensus mechanism: Integrity and concurrency control of data transmissions in a decentralized network can be achieved using various methods. Consensus is a process that enables "a set of *distributed processes* [to] achieve agreement on a value or an action despite a number of faulty processes" [12]. This is formally known as the Byzantine General's Problem [13].

In a blockchain network, consensus is used to prevent dishonest actors from writing potentially invalid information to the database. The specific consensus mechanism used for any given blockchain depends on a number of assumptions, including the amount of trust between parties and the alignment of their interests, as well as factors concerning the shape and synchronization of the network.

Various types of consensus mechanism are Proof of Work (PoW), Proof Of Stake (PoS), Proof of Importance (PoI), Practical Byzantine fault tolerance (PBFT) etc.

Proof of Stake (PoS): Nodes capable of creating and adding new blocks are chosen in a deterministic (pseudo-random) way, where the computational requirements for the same are low compared to PoW mechanism [14].

Proof of Importance (PoI): Nodes are clustered based on *transaction indicators*. The credibility and importance of a node is decided by the number of validated transactions it has carried out [15].

4) Proof-of-Work (PoW): PoW employs a cryptographic hash function to solve a computationally intensive puzzle. A cryptographic hash function essentially takes input data of unequal length and transforms it into a relatively compact, fixed output string (in the case of SHA-256 [16] the output hash is 32 bytes). Any slightest change to the input data produces an exponential change in the output hash generated. This is known as *avalanche effect* and it provides strong unpredictability characteristics to hash functions. The hash serves the dual purpose of identification as well as integrity verification.

The hashing difficulty factor is achieved by requiring the hash output has a number of leading zeros. For example, let the target value in Hex is *000000FF*. Solving the proof of work puzzle involves finding a nonce which when appended to the message produces a hash value less than *00000010*, i.e. it starts with 6 zeros. Figure 3 describes the Proof-of-Work scheme in Bitcoin [17].

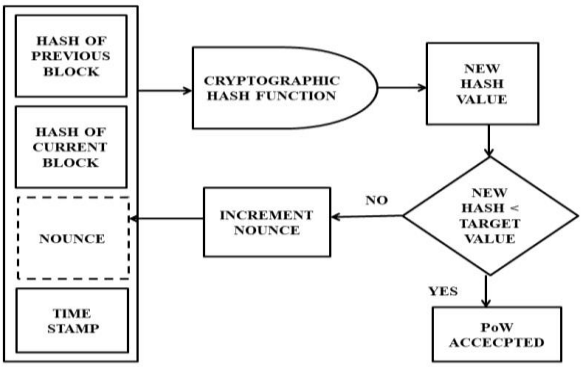

Fig. 3. Proof-of-Work scheme in blockchain

5) Classification of Nodes: Nodes form the backbone of the P2P network. The nodes differ in their hardware configuration and tasks carried out depending on the varied requirements. The nodes can be classified as Full, Partial and Simple.

Full node maintains a copy of the full blockchain. It has the capability to make and add transactions to the block chain as well as validate transactions send by other nodes.

Partial node is a scaled down version of a full node. It has limited rights and can create, transmit and verify new transactions and blocks but only stores useful metadata of blockchain database

Simple node has limited resources. It may create, transmit and verify new transactions but cannot contain the blockchain in totality. It is similar to the Simple Payment Verification (SPV) nodes in a Bitcoin network.

B. Block Construction

A transaction is the process of transferring certain information. A block is a collection of records/ transactions associated to a time-stamp. A simple chain of three blocks is presented in Figure 4. Multiple transactions can be stored in one block, connected using a Merkle tree [18]. The blocks are identified by the hash of all the transactions it contains, time it was created and the hash identifier of its previous block in the Blockchain. Blocks are chained with each other by means of the hash identifier of the previous block in the chain. Starting from a certain block, it is possible to identify complete information stores in all the previous blocks, upto the very first block of the chain, the *'Genesis' block*.This ensures *tamper resistant* property of blockchains. Any attempt to modify/delete any of the previous transactions in a block will result in the modification of hash value of the block as well as the blocks after it in the blockchain. This change can be easily detected by other nodes holding legitimate copy of the blockchain. Consequently, the blockchain becomes increasingly difficult to compromise as the network size increases.

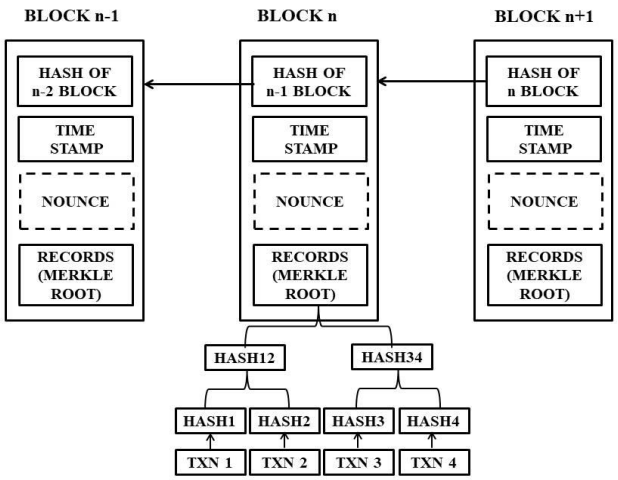

Fig. 4. Block chain example with 3 blocks

Hence a blockchain system is seen as a *distributed ledger system* that verifies and stores transactions, ensuring its integrity, transparency, authenticity and availability. A blockchain can be seen as a distributed database system using blocks as *unitary memory units*, which are copied and stored in multiple nodes/users in the network.

C. Blockchain Variants

Depending on the consensus mechanism invoked and hosts/ players involved, Blockchain can be broadly classified into three variants:- Public, Private and Consortium/ Hybrid. Table 2 illustrates major differences between a public blockchain and a private/ consortium Blockchain [19].

Permissioned/ private systems retains the strong security of blockchain, but has advantages of being a private, need to know basis, smaller, faster technology. It functions on the basis of a participant whitelist. Speed, costs, censorship are just some of the important aspects balanced between permissioned systems and public ones.

IV. SALIENT FEATURES OF BLOCKCHAIN

The salient features of blockchain technology which can be utilised in NEMO environment are:

1) Availability of complete data: The blockchain consensus mechanism enforces each node to store a complete copy of transaction records. Hence this ensures data availability at all times. Unlike centralised data storage models, this feature offers robustness against single point-of-failure issues.

2) Integrity: Data integrity refers to the accuracy and consistency of stored data. All transactions in a blockchain are verified and processed by all nodes, using public key cryptography [11], and creating hash of the transactions thereby ensuring the integrity of the data.

3) Fault tolerance: All nodes possess a similar copy of the ledger. This ensures that the transactions are updated in real time by the healthy nodes. Any node that is off road can get an updated copy of the blockchain ledger once it rejoins the network. This enables fault tolerance at a superior level in the network.

TABLE 2. COMPARISON: PUBLIC AND PRIVATE/ CONSORTIUM BLOCKCHAIN

Parameters	Public	Private/ Federated/ Consortium
Access	Open Read/ Write	Permissioned Read/ Write
Consensus mechanism	PoW, PoS, PoB,, PoI, PBFT	Custom, multi party
Speed	Slow	Fast
Identity of participants	Anonymous/pseudoanonimous	Pre approved participants
Participant risk	Can be malicious	Trusted and pre-approved
Efficiency (wrt Cost, computing requirements)	Less	High
Finality	No finality	Enables finality
USP	Disruptive technology	Highly efficient, economic and precise
Examples	Bitcoin, Ethereum	R3, B3i , EWF, MONAX

4) Decentralisation of trust: Lack of central control and trust between entities eliminates the risk of compromise of healthy nodes. Consensus mechanism like PoW, PoS, PoI etc are required to add new transactions to a block. This results in complete elimination of requirement of a central controlling authority.

5) Empowered users: Users possess complete control of all information and transactions of data stored in the nodes.

6) High quality data: Data is a blockchain has complete record of all transactions with high level of accuracy.

7) Durability and reliability: Blockchain does not have a central point of failure and is better able to withstand malicious attacks.

8) Longevity of data: Data is stored in the blockchain from the initial transaction (genesis block) to the latest block and is available with everyone. Even if this information is lost from a majority of the nodes, it can still be retrieved from the balance of the nodes.

9) Transparency: Any change in the blockchain is publicly viewable by all nodes/ users thereby ensuring transparency.

10) Immutability: All transactions once committed to the blockchain cannot be altered or deleted.

11) Clarity: All transactions are added to a single public ledger, thereby reducing clutter and complications of multiple ledgers.

However, certain limitations observed have been listed as under:

1) Increased energy consumption: The consensus mechanisms currently used are processor intensive, resulting in need for powerful hardware resulting in increased energy consumption. This may adversely affect its utilization in

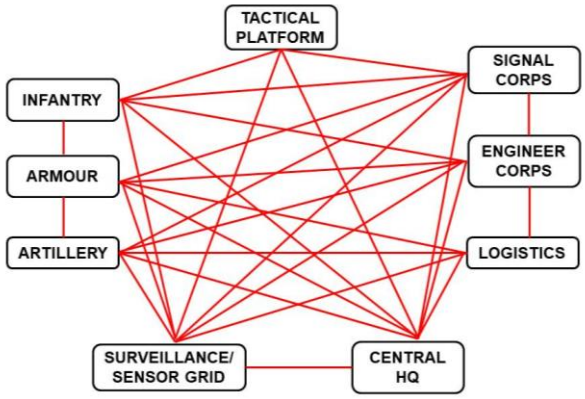

Fig. 5. NEMO Case study 1: Extended Network of BMS Elements

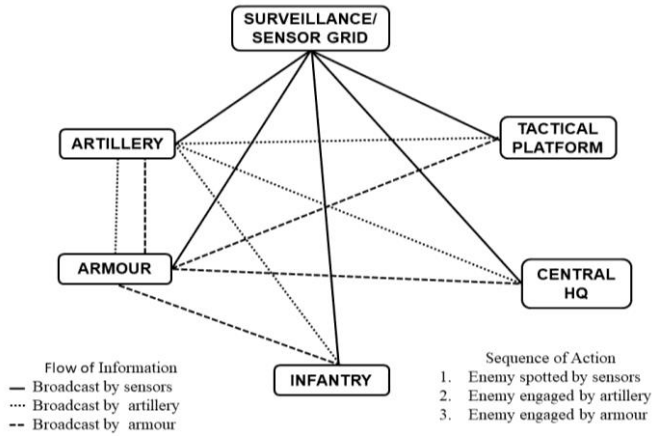

Fig. 6. Data flow and sharing of information in a battlefield scenario

military environment where availability of such resources cannot be guaranteed at all times.

2) Control, security, and privacy: Public blockchain offers transparency and access to the blockchain information to all users which may not be required in certain applications like military where secrecy is of paramount importance. This calls for the development of private blockchain technology.

3) Bloating: Blockchain continuously keep growing storing all previous transactions. This necessarily leads to increased storage requirements since the ledger is kept by nodes. Scalability is therefore an important disadvantage.

4) Pseudo identity issue: Public, permission less systems (such as Bitcoin) permits any node to become part of the network and provide access to the blocks. This increases the possibility of a Sybil attack [20].

5) Legal and Regulatory issues: Smart contracts and programmable logic capabilities can improve the time spend on negotiating and formalizing the contracts. But the credibility under existing laws are not clearly defined.

V. POTENTIAL EMPLOYABILITY OF BLOCKCHAIN IN NEMO

Blockchain technology can be effectively utilized in a wide array of battlefield scenarios/ military applications like:

- Secure messaging service between troops in battle field/ forward zones and command and control centres operating from headquarters/ tactical centers.
- Keeping track of details of manufacture, storage, carrying out proof and segregation of ammunition lots.
- Supply chain management for spares of vehicles, clothing and other important equipment.
- Maintaining a record of patients in the hospitals along with their case history which can be accessed by personnel with permission, etc.

We put forward certain case studies where blockchain in NEMO context can be used effectively:

A. NEMO Case Study 1: Data communication in Battlefield Management System(BMS)

Aim: To ensure immutable, secure and verifiable communication of data transmitted between various elements of the Battlefield Management System (BMS) [21] operated by the field Army.

NEMO Requirements: Data generated, transmitted and analysed in a BMS is highly confidential and needs to be protected from various threat vectors like eves dropping, man-in-the middle attacks, data corruption etc.

Blockchain features utilised: Blockchain technology can ensure robust, tamperproof data communication in hostile environments by ensuring data provenance, use of encryption , hashing methods and consensus mechanism between users.

NEMO with Blockchain: Advancements in technology has enabled the enemy to carry out a variety of attacks with considerable ease and anonymity. Blockchain technology will ensure that all transmissions are encrypted and broadcasted. This ensures availability of data to all nodes in the network. These transmissions are subsequently included in the database using consensus mechanism among nodes/ users and will be immutable. This prevents possibility of corruption or alteration of data. Figure 5 shows a basic layout of a distributed network of elements of BMS for ground warfare Internet/intranet and direct satellite link using low bandwidth /radio communication mediums can be used as backbone network to connect the various elements/ end nodes. The blockchain data will be stored at predefined elements/ users depending on factors like storage and computing capabilities available etc. The information in blockchain can be accessed on a need to know basis by these elements. Also, decentralised nature helps to improve the sustainability of the network.

Figure 6. describes communication of data for a simulated battlefield scenario. Surveillance devices detect enemy presence and broadcasts details like location and strength to all elements in BMS in encrypted manner. The headquarters and fighting elements analyses this data. Primarily, artillery units

which can engage the target within least time is pressed into action. The details of the artillery support provided is broadcasted. Affected units prepare for the next stage of attack. Armour and combact vehicles can now engage the target followed by infantry. All data introduced into the environment is uniquely signed by users ensuring accountability and avoiding deniability. All data is included in blockchain and is immutable and tamperproof. Data ownership and access will be transparent to users only after due verification. This ensures that the same database is available with every member in the network but access to it will be regulated, there by achieving redundancy and secrecy. This results in enhanced situation awareness among all elements. Since each block is interlinked with the hash of the previous block, alteration of data in the chain can be immediately detected. Equal importance and responsibility for all nodes in the network will ensure that network is functioning even when majority of the nodes are down.

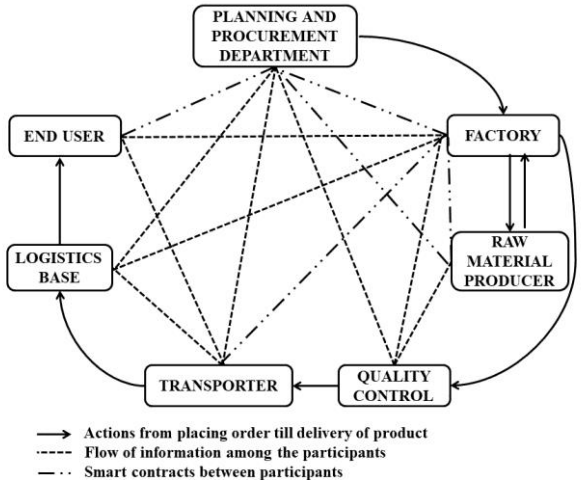

Fig. 7. NEMO Case study 2: Integration of Logistics support Elements

B. NEMO Case Study 2: Logistics Support for the Armed Forces.

Aim: To ensure security, compliance and transparency in logistic support for Armed Forces, specifically Army and to increase the efficiency of the supply chain channel between end user and manufacturer.

NEMO Requirement: To primarily establish provenance and level of trust in transactions between manufacturers and end users. Need for better asset visibility and tracking of assets in a heterogeneous multi-level environment.

Blockchain features utilised: Blockchain ensures provenance by creating a distributed, tamperproof record of transactions among various manufacturers, retailers, suppliers and end users. Every supplier/ receiver element in the chain can maintain a copy of the complete database. Users are identified by their digital signatures. Smart contracts are executed between the players for transparency and validation. The transactions can be independently verified and processed by every node/ user.

NEMO with Blockchain: Logistics in warfare includes various factors like providing war like stores, ammunition, and other essential stores to troops involved in combat operations. Logistics also incorporates the role of various organizations that equip, support and cater to the needs of the Armed Forces, the transportation system involving railways and load carriers for transporting the forces to be deployed and plans in place to restock / resupply the depleted resources once they are deployed.

Figure 7. depicts the process from placing of an order for a product till its delivery to the end user. Each user will have a complete copy of blockchain but the access can be made restricted. This 'need to know' method will provide access to order details, progress of manufacturing at factories, location of shipments and goods etc concerning a specific node/ element. Smart contracts between factories, raw material providers and procurement agencies can drastically reduce the time taken compared to present scenario. Amendments in contracts, changes in order quantities etc. can be implemented with minimum time and legal delays. Optimizing a supply chain on the blockchain makes new things possible, such as the real-time synchronization of decisions with supply chain partners [22],[23].

Supply chain management using blockchain has the following advantages*:*

- Reduce or eliminate errors and fraud.
- Improve inventory management.
- Reduce delays caused by paperwork.
- Identify anomalies and faster resolutions.
- Minimize transportation costs.
- Information is publically available and immutable.

Considerable share of technologies used by the armed forces presently are procured from vendors outside the nation. These vendors and manufacturers often resort to *commercial-off-the-shelf (COTS)* components for cost reduction and reducing R&D overhead. However the level of trust between these entities is disputable. Probability of a malicious software getting embedded in such COTS technology is relatively very high. This has led to the issue of provenance management, or the ability to establish the origin and traceable ownership of an asset [4]. This is very critical to ensure reliability and trustworthiness of the systems in today's environment where adversaries are capable of implanting logic bombs, worms and other malicious entities in the COTS components.

C. NEMO Case Study 3: Smart Contracts in Ammunition Management

Aim: To optimize handling of ammunition and its components by the implementation of smart contracts.

NEMO Requirement: Efficient ammunition management by the utilization of smart contracts.

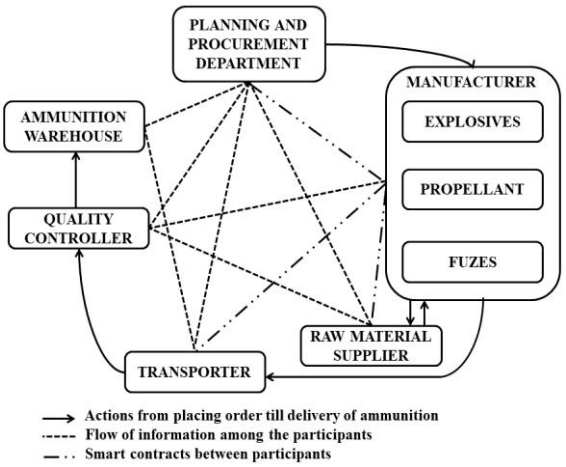

Fig.8. NEMO Case study 3: Smart contracts in Ammunition Management

Blockchain features utilised: Distributed Ledger technology can provide real time access to information like details of manufacture, transportation status and stock holding of ammunition at various locations to the end users, logistic echelons and manufacturers. Smart contracts will increase the efficiency of supply chain management by proactive implementation of activities like recycling, segregation and repair of affected ammunition.

NEMO with Blockchain: Ammunition management is a complex task involving manufacture, transportation, storage, turn over, maintenance, repair and demolition activities. Ammunition is made up of a variety of components like explosives, fuzes, propellants with varied shelf life. Smart contracts can be incorporated in the system which will ensure timely efficient management of manufacture, transportation, storage and maintenance of ammunition [21],[23].

Figure 8. depicts the process of placing of an order for ammunition till its delivery at the warehouse. Blockchain can help in tracking the details of manufacturing, design and configuration of *lots* manufactured. It can ensure monitoring of critical ammunition components and can auto execute purchase orders when stocks levels fall below the reserved level. The purchase orders are digitally signed and held by all players. Any anomaly found in specific batches can be intimated to all through broadcast. Technical activities like proof, repair and turnover of ammunition will become extremely simple and transparent. Location data and time stamping of data assists in increased transparency. Thus, a supply chain with continuous, real-time access to a chain of events can optimize iteratively.

VI. CONCLUSION

Military networks works on shared information, shared knowledge and shared understanding from a variety of heterogeneous elements to achieve information superiority. This results in increased situational awareness and better decision making capabilities. Inter equipment communication between internetworked devices are prone to several vulnerabilities [3],[6]. Manipulation of this data by the adversary or even accidental corruption of mission-critical data can result in catastrophic effect down the decision chain.

This paper introduces NEMO model to represent the parameters and resources involved in military operations in a networked environment. Ensuring accountability, privacy and validity of data in a diverse, distributed environment like NEMO has various challenges Use of blockchain technology in NEMO promises security, availability and integrity of data communicated. Various possibilities/ areas in NEMO framework where blockchain can be used to achieve provenance, reliability, usability and authenticity of data generated and communicated has been described.

Out of the various scenarios cited in Section V, three case studies are analyzed for the feasibility of incorporating blockchain technology into the existing NEMO framework. These case studies highlight properties of blockchain like immutability, fault tolerant nature, trustlessness, data provenance and transparency.

Blockchain is a relatively new technology and is undergoing rapid advancements. The unique nature of blockchain ensures confidentiality, integrity and availability of data, stored and accessed in a decentralized manner. Features like Smart contracts and programmable logic helps in bringing intelligence to systems. Future study demands assuming and organizing resources specific to any of the case studies discussed in Section V. and developing a prototype model for implementation.

REFERENCES

[1] Yanga, Ang, “Understanding Network Centric Warfare.” (2004).
[2] Dekker, Anthony H, “Centralisation and Decentralisation in Network Centric Warfare.” (2003).
[3] Yao, Yong and Zhi Li, “Research of information dissemination model based on Network Centric Warfare”, 2010 IEEE International Conference on Information Theory and Information Security (2010): 962-965.
[4] Xueping Liang, Sachin Shetty, Deepak Tosh, Charles Kamhoua, Kevin Kwiat, Laurent Njilla, “ProvChain: A Blockchain-Based Data Provenance Architecture in Cloud Environment with Enhanced Privacy and Availability” 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID), 2017
[5] Neil B. Barnas, “Blockchain in National Defense - Defense Technical Information Center”
URL: http://www.dtic.mil/doctrine/education/jpme_papers/barnas_n.pdf
[6] S. Roy and M. J. Nene, "Analysis and recommendations for network and communication security for mission critical infrastructure," 2016 3rd International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, 2016, pp. 1-8.
doi: 10.1109/ICACCS.2016.7586382
[7] S. Roy and M. J. Nene, "A security framework for military application on infrastructure based wireless sensor network," 2015 IEEE International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN), Kolkata, 2015, pp. 369-376.
doi: 10.1109/ICRCICN.2015.7434266
[8] “Blockchain: Blueprint for a New Economy” Book by Melanie Swan, O’Reilly Media, Inc. Sebastopol, CA, USA, 2015.
[9] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” Oct. 2008.

[10] K. Jenkins, K. Hopkinson and K. Birman, "A gossip protocol for subgroup multicast", International Conference on Distributed Computing Systems Workshop, 2001
[11] Don Johnson, Alfred Menezes and Scott Vanstone, "The Elliptic Curve Digital Signature Algorithm (ECDSA)", International Journal of Information Security, (2001) 1: 36.
URL: https://doi.org/10.1007/s102070100002
[12] T. Swanson, "Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems," 2015.
[13] Miguel Correia et al., "Byzantine Consensus in Asynchronous Message-Passing Systems: A Survey.," International Journal of Critical Computer-Based Systems 2, no. 2 (2011): 141–61.
[14] Iddo Bentov, Charles Lee, Alex Mizrahi, Meni Rosenfeld, "Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake" SIGMETRICS Perform. Eval. Rev. 42, 3 (December 2014), 34-37. DOI=http://dx.doi.org/10.1145/2695533.2695545
[15] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, E. W. Felten, "SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies", IEEE Symposium on Security and Privacy. IEEE Computer Society, pp. 104-121, 2015
[16] Descriptions of SHA-256, SHA-384, and SHA-512
URL: www.iwar.org.uk/comsec/resources/cipher/sha256-384-512.pdf
[17] The Proof-of-Work Concept | Satoshi Nakamoto Institute
URL: https://nakamotoinstitute.org/mempool/the-proof-of-work-concept
[18] R. C. Merkle, "A digital signature based on a conventional encryption function", Conference on the Theory and Application of Cryptographic Techniques. Springer, 1987, pp. 369–378
[19] Nikola Bozic. Guy Pujolle and Stefano Secci, "A Tutorial on Blockchain and Applications to Secure Network Control-Planes", SCNS IEEE 2016.
[20] J. R. Douceur, "The sybil attack," in International Workshop on Peerto-Peer Systems. Springer, 2002, pp. 251–260.
[21] Battlefield Management System for Indian Army- Where are we? By Lt Gen Prakash Katoch, Issue Net Edition | Date : 31 Jan , 2017
URL:http://www.indiandefencereview.com/news/battlefield-management-system-for-indian-army-where-are-we/
[22] H. Watanabe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu and J. Kishigami, "Blockchain contract: Securing a blockchain applied to smart c ontracts," 2016 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, 2016, pp. 467-468.
[23] H. Watanabe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu and J. Kishigami, "Blockchain contract: Securing a blockchain applied to smart contracts," 2016 IEEE International Conference on Consumer Electronics(ICCE), Las Vegas, NV, 2016, pp. 467-468.