CENTRE FOR JOINT WARFARE STUDIES

SYNODOS PAPER | VOL - XII NO-16 / JUL 2018

BLOCKCHAIN: MILITARY APPLICATIONS

Col Harpreet Singh is a 1991 batch EME officer. An alumnus of NDA and CDM, he has commanded an EME Battalion in CI Ops. His important staff appointments are AA & QMG of a Mountain Brigade and Director at Directorate General Military Training. He is presently a senior fellow at Centre for Joint Warfare Studies.

"Every ten minutes, all the transactions conducted are verified, cleared, and stored in a block which is linked to the preceding block, thereby creating a chain. Each block must refer to the preceding block to be valid. The structure permanently time-stamps and stores exchanges of value, preventing anyone from altering the ledger... so the blockchain is a distributed ledger representing a network consensus of every transaction that has ever occurred. Like the World Wide Web of information, it's the World Wide Ledger of value... This new digital ledger can be programmed to record virtually everything of value and importance to humankind: birth and death certificates, marriage licenses, deeds and titles of ownership, educational degrees, financial accounts, medical procedures, insurance claims, votes, provenance of food, or anything else that can be expressed in code."

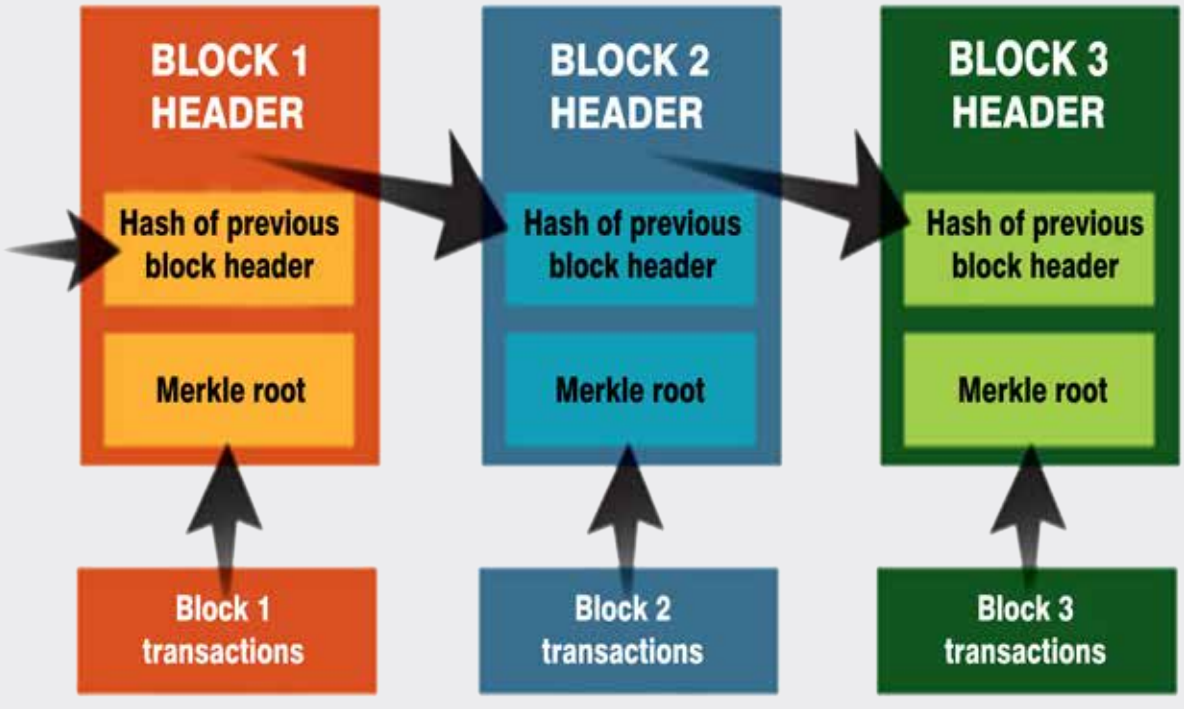
- Ian Khan, TEDx Speaker, Author, Technology Futurist

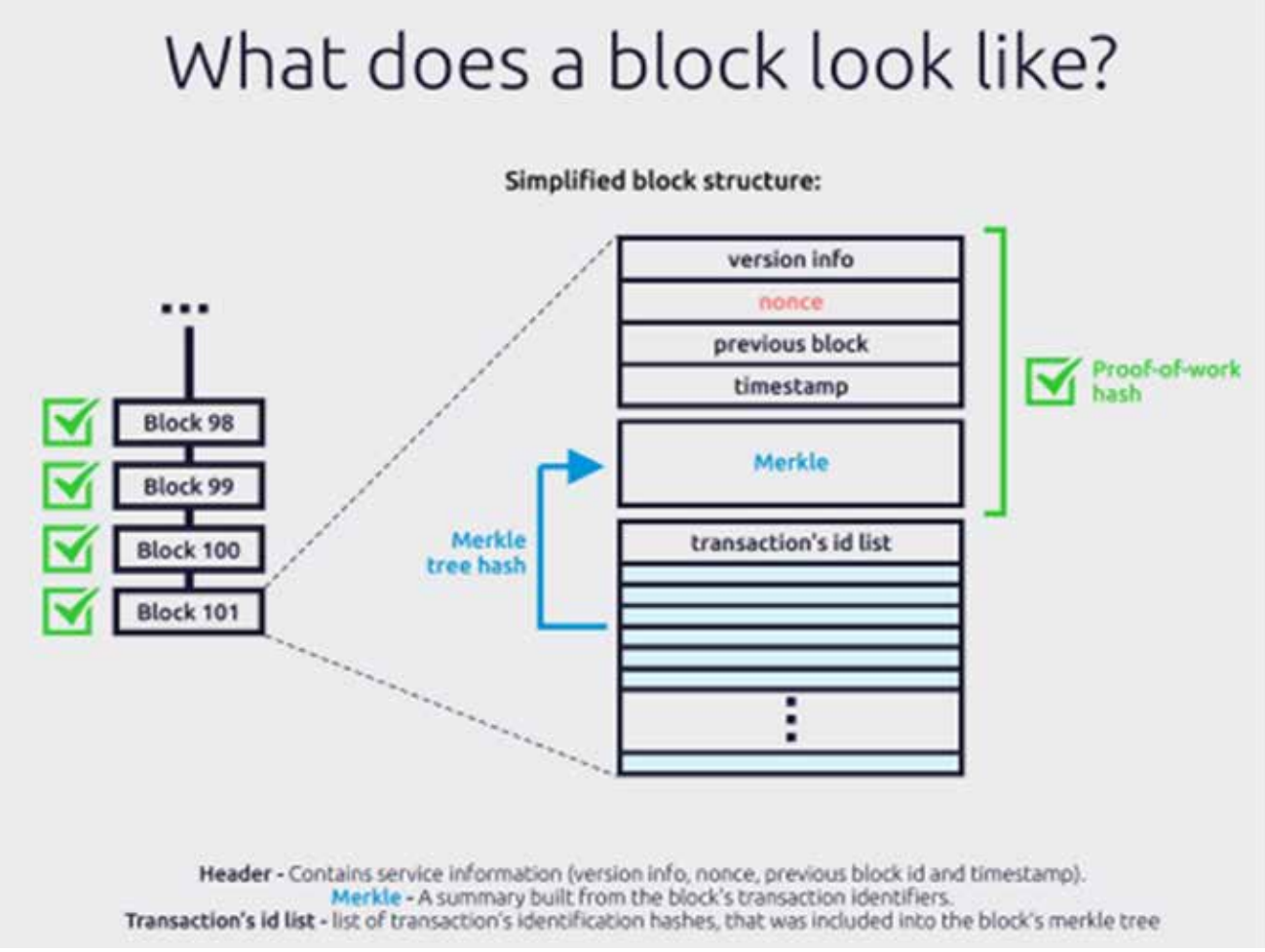
A blockchain is a continuously growing list of records, called *blocks*, which are linked and secured using cryptography. Each block typically contains a cryptographic hash of the previous block, a time stamp and transaction data. By design, a blockchain is inherently

resistant to modification of the data. It is an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way. For use as a distributed ledger, a blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol for inter-node communication and validating new blocks. Once recorded, the data in any given block cannot be altered retroactively without the alteration of all subsequent blocks, which requires collusion of the network majority. People who record and verify data are called miners who are given a monetary reward for their work.

The blockchain is an undeniably ingenious invention – only about a decade old, the brainchild of a person or group of people known by the pseudonym, Satoshi Nakamoto. But since then, it has evolved into something greater. By allowing digital information to be distributed but not copied, blockchain technology created the backbone of a new type of internet. Originally devised for the digital currency, Bitcoin, the tech community is now finding other potential uses for the technology. While many have seen the banking industry as an early adopter of this technology and the heftiest of spenders, there is an expectation that billions of dollars will flow into the blockchain market over the next few years from other sources as well, with banks acting as the entry point in creating a degree of legitimacy.

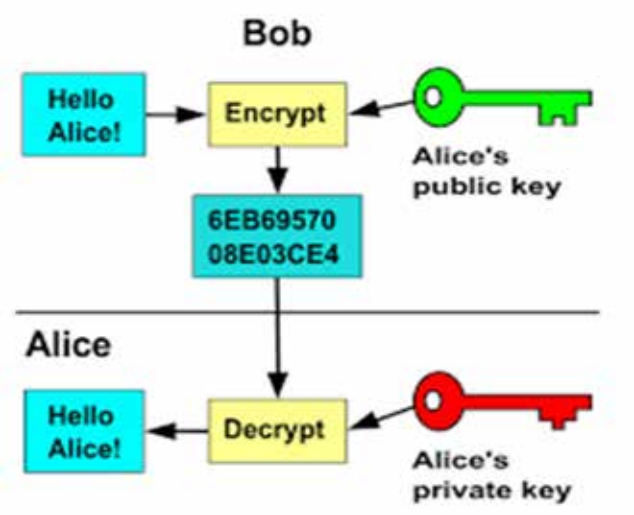
With blockchain technology, each page in a ledger of transactions form a block. That block has an impact on the next block or page through cryptographic hashing. In other words, when a block is completed, it creates a unique secure code, which ties the next page or block, creating a chain of blocks, or blockchain.



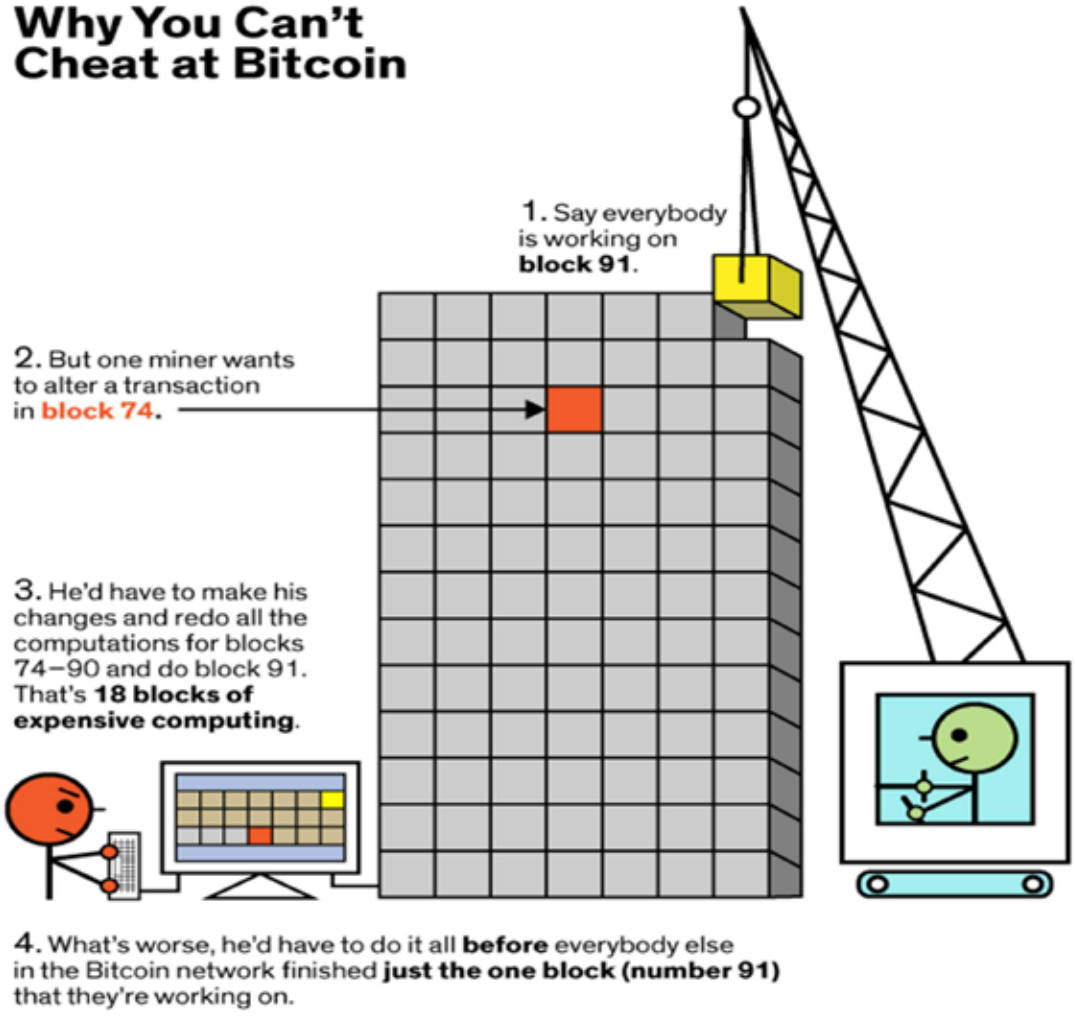


Salient Features of Blockchain

- Blockchain is a distributed and stored database.
- It is a publicly available shared ledger of records, which anyone can browse and verify.
- Blockchain does not belong to anyone and belongs to all at the same time.
- The network behaves like an incorruptible accountant who executes all types of transactions.
- A trusted third-party, for example, a bank, is not required to oversee transactions. Computers take over the contract processing, check the conditions and can automatically execute individual clauses.
- The complete process is constantly controlled by miners whose software verify all transactions, block for block, and substantiate their authenticity.
- Participation in a blockchain is easy and cheap. A cryptographic pair of blockchain software is required. This pair of keys is made up of a private and a public key. The public key is visible to all other members but the private key remains a secret. Every transaction which a user triggers, is signed using a private key. The process is illustrated as follows:-



- Once a block is verified, the result is etched in the digital stone. For reasons of efficiency, several transactions are always bundled into one block in the database. The new block not only includes the transaction but also the Hash-value of the parent blocks and it is also digitally signed.
- Rather than follow banks, which store databases on their own servers, the blocks of a blockchain are scattered across thousands of computers and there is no master copy.
- Blockchains tend to have a giant database. Currently, every full node for Bitcoin must download almost 100 GB Blockchain, while transactions require up to ten minutes.
- Blockchain is difficult to hack because there is no single go-to location. Database is not under any central, sole authority. You need support of 51% of miners to change the hashes of all previous blocks within 10 minutes to change any data – a near impossible feat.



HOW THE BLOCKCHAIN WORKS

The bitcoin illustration

Anna buys a book online

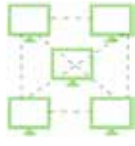
Her on line retailer accepts bitcoin and Anna already holds a bitcoin wallet.

The retailer send Anna his bitcoin address (a chain of 26 to 35 characters)

Anyone can verify the transaction with the public key

Anna sends her payment to the address of her retailer. She signs the transaction with the private key of her own address created for given transaction and adds her own public key to the transaction.

To ensure **privacy,** addresses are usually different for each transaction. An address is linked to a private key and a public key.



This is where the miners come into play

Transactions are recorded in **blocks.** The ledger is a chain of blocks. **Blockchain is the realization of a public ledger.**

The blockchains, shared in real time on the miners computers, stores the record of all confirmed bitcoin transactions.

As a new block is created every 10 minutes, modifying a recorded block would require modifying all the following blocks, which is nearly impossible

A block contains the hashes of the previous and current blocks, and a 'nonce' (a random number). All blocks are linked to one another. It can be viewed as a wax seal.

To store a transaction in the blockchain, miners computers create cryptographic **hashes** (strings of letters and numbers).

A hash must look a certain way (starting with a number of zeros). **Miners must generate many hashes before landing a successful one.**

The successful miner is **rewarded** in bitcoins.

Anna's transaction is now complete and verified.

Blockchain and Armed Forces

The defence industry involves a lot of resource management. It's also because the entire industry is resource intensive. In fact, a lot of countries around the world spend more on their defence sector than on basic amenities like education and health for their citizens. Because there is so much capital involved, the industry needs to adhere to strict resource management principles so that taxpayers' money is utilized in the best possible way. However, there have been several instances where lots of funds are wasted because of ill-management. Other than managing projects, communication in defence industry also requires a robust and protected platform. Countries are also habituated to being secretive about their defence projects before the masses, in general. Blockchain technology in defence may be of help here, to minimize the leakage of resources, to make the work flow more efficient, and also to provide a platform for defence communication.

The paradox is that the transparency given by blockchain may be an aspect that defence forces across the world may not be too comfortable with, as secrecy is an essential part of military operations. However the case for using a blockchain boils down to a concept in computer security known as information integrity. That is essentially the ability to track when a system or piece of data has been viewed or modified. The principal is that "Instead of trying to make the walls of a castle as tall as possible to prevent an intruder from getting in, it's more important to know if anyone has been inside the castle, and what they're doing there."

Blockchain technology is worthy of examination because it offers three significant advantages over traditional cyber defence strategies. First, rather than trying to defend boundaries from compromise, blockchains assume compromise by both adversaries and trusted insiders. They are designed to defend data in a contested cyber environment. Second, blockchain networks harness the aggregate power of the network to actively resist the efforts of malicious actors. That is, blockchains take advantage of the asymmetry of many against few. Finally, the security that blockchains provide is not dependent on secrets or trust. There are no passwords to be exposed, cryptographic keys to be protected, or administrators to be trusted. Blockchains solve a challenging problem in data science of reliably exchanging information over an unreliable network on which some of the participants cannot be trusted. The blockchain security model inherently assumes that these dishonest participants will attempt to create friction by not only generating false data, but also by attempting to manipulate valid data passed from honest participants. By using a variety of messaging and consensus techniques, blockchains ensure data integrity by both rejecting invalid data and preventing valid data from being secretly modified or deleted.

Blockchains provide an inherent security function on which additional security functions can be added, depending on the application. As result of these advantages, blockchains are capable of operating successfully and securely on the open internet, without a trusted central authority, and while fully exposed to hostile actors. Given their ability to protect the integrity of data in spite of adversary actions, blockchains offer significant military utility.

Also there are layers of protocols which can be added to give various degrees of security. Access control thus can be ensured. These are explained below:-

- **Public Blockchains.** A public blockchain has absolutely no access restrictions. Anyone with an internet connection can send transactions to it as well as become a validator (i.e., participate in the execution of a consensus protocol). Usually, such networks offer economic incentives for those who secure them and utilize some type of a Proof of Stake or Proof of Work algorithm. Some of the largest, most known public blockchains are Bitcoin and Ethereum.

- **Consortium Blockchains.** A consortium blockchain is often said to be semi-decentralized. It too, is permissioned but instead of a single organization controlling it, a number of companies might each operate a node on such a network. The administrators of a consortium chain restrict users' reading rights as they see fit and only allow a limited set of trusted nodes to execute a consensus protocol.

- **Private Blockchains.** A private blockchain is permissioned. One cannot join it unless invited by the network administrators. Participant and validator access is restricted. This type of blockchains can be considered a middle-ground for companies that are interested in the blockchain technology in general but are not comfortable with a level of control offered by public networks. Typically, they seek to incorporate blockchain into their accounting and record-keeping procedures without sacrificing autonomy and running the risk of exposing sensitive data to the public internet. Private blockchain allows administrators to control the participants on the network, the portions of the blockchain that can be viewed, who can write to the blockchain, and even who composes the consensus group. These may be suitable for defence forces.

Advantages of Blockchain use by Military

Besides the arguments given above there are several benefits the technology offers to the armed forces:-

- Blockchain's compelling element for military commanders is its distributed node system, with participants being allowed layers of activity inside a cryptographically sealed network.

- No centralized version of this information exists for a hacker to corrupt. This potentially gives unlimited redundancy - If one node is destroyed, you don't lose everything.

- Eliminates counterfeit components, delays, costs, human error & audit requirements.

- Enhances transparency, reliability, traceability and security.

- Blockchain adds any number of participants and touch points to a supply chain without compromising its efficiency.

- Blockchain technology is like the internet in that it has a built-in robustness. The internet itself has proven to be durable for almost 30 years. It's a track record that bodes well for blockchain technology as it continues to be developed.

- The blockchain network lives in a state of consensus, one that automatically checks in with itself every ten minutes. A kind of self-auditing ecosystem of a digital value, the network reconciles every transaction that happens in

ten-minute intervals. Two important properties result from this i.e. transparency and non-corruptibility

- We all rely on the "user name/ password" system to protect our identity and assets online. Blockchain security methods use encryption technology. The basis for this are the so-called public and private "keys", as discussed earlier. This is a more secure system.

- Currently faulty, counterfeit, or incorrect products are ordered or received. This results in time delays, increased costs & risks to security. Units/depots can enforce new supply chain standards and increase mission assurance using blockchain technology.

- Blockchain solution provides an immutable audit trail proving hardware, software and documentation authenticity and compliance across supply chains.

- Tech like CryptoSealand FPGA fingerprinting can give materials in the supply chain a unique identity to prove authenticity. This Proof of Value has the potential to completely revolutionise the supply chain system. This combination of technologies allows us to securely and transparently track all kinds of transactions, between OEMs, suppliers, manufacturers and customers/units.

- Every time an item in the supply chain is exchanged, the transaction is permanently documented and easily recovered. The history and unique identity of a product is therefore monitored from raw materials and parts, to the sale of the finished goods. This combination of technologies allows us to securely and transparently track all kinds of transactions, between OEMs, suppliers, manufacturers and customers/units.

- For intelligence operations, the ability to discretely pay intelligence professionals and informants is critical. Blockchain allows participants to apply for one or more accounts, regardless of "national and geographical restrictions," with no direct correlation between different accounts.

Blockchain use in World Militaries

World militaries have started looking at increasing efficiency and transparency through blockchain. Some of these are discussed below:-

US. Cybersecurity infrastructure is taking a leap forward with the support of DARPA, the research unit of the U.S. Department of Defence (that helped create the internet, among other things).The agency has funded a handful of start-ups to develop blockchain uses for secure communications, logistics, management of weapons systems, file storage, etc. DARPA recently awarded a $1.8 million contract to a computer security firm called Galois. The firm's assignment is to formally verify- a particular type of blockchain technology supplied by a company called Guardtime. Formal verification is one way to build nearly unhackable code and it's a big part of DARPA's approach to security .

The DoD had raised a critical need for a secure messaging and transaction platform accessible via web browser. DARPA has therefore sought proposals to "Create a secure messaging and transaction platform that separates the message creation, from the transfer (transport) and reception of the message using a decentralized messaging backbone to allow anyone, anywhere the

ability to send a secure message or conduct other transactions across multiple channels traceable in a decentralized data base.

The principal that US follows is that blockchain technology could create important intelligence around whether a hacker has modified something in a database, or if they are intruding and surveying a particular military system. As it is difficult to keep out every single hostile player, data integrity - the ability to track if information has been viewed or modified - may be more important. Blockchain offers a way for these agencies to quickly know who has infiltrated the system and what they did within it. As a result of its distributed nature and instantaneous recording, the blockchain is vastly more resistant to tampering than centralized systems. This could alert military and intelligence authorities if a hacker is surveying a particular military system or has made modifications, without allowing the actor to cover their tracks. Blockchain technology use by US military still has hurdles in reaching the magic that it promises, with performance kinks still being ironed out. However, the approach poses obvious advantages for traditional security software, which leaves a lag in the time it takes to detect a hacker. Most invaders spend 150 days on a network before they are discovered hence DARPA's hedging ushers in an enormous step forward in cybersecurity infrastructure.

NATO. The NATO Communications and Information Agency is currently evaluating proposals in areas of application of blockchain technology relating to military logistics, procurement and finance, Internet of Things, and other applications of interest to military. The proposals were submitted as part of the 2016 Innovation Challenge aimed at accelerating transformational, state-of-the-art technology solutions in support of NATO C4ISR and cyber capability requirements.

China. There is a limited amount of authoritative material on the subject in China. The main blockchain applications which have been outlined are intelligence operations, weapons life cycle, personnel management and military logistics. This foundational approach may very well frame future Chinese security-related blockchain endeavours and perceptions.

Applications in National Defence for India

Blockchain technology has obvious utility in our national defence applications. There are many specific, near to medium term uses where blockchains offer utility in both operational and support roles:-

- **Cyber Defence & Data Integrity**. Cyber defence is the most near-term, low-cost, high-payoff application of blockchain technology. As discussed earlier, cyber security relies on secrets and trust to maintain security, but neither can be assured. Blockchains operate independent of secrets and trust. The growing complexity of modern systems, including weapon systems, make vulnerabilities both more likely and less detectable. Instead of searching for vulnerabilities, equivalent to searching for a needle in a haystack, you can monitor every stalk of hay and every digital asset that constitutes the system you want to protect. Malware attacks against systems are integrity attacks against their configurations. Using blockchain, the configurations of every component in the system can be imaged, hashed, secured in the database, and continually monitored. Any unscheduled change to any configuration, no matter how small, can be detected almost instantly.

- **Supply Chain Management**.
  There is growing anxiety about supply chain management for defence systems, which increasingly use commercial-off-the-shelf components, mostly from China, for embedded software systems. The concern is that these components may contain deliberate vulnerabilities that could be exploited by an adversary at the time of his choosing. Thus, this issue is one of provenance, or the ability to establish the origin and traceable ownership of an asset. Blockchains offer a solution for most equipment, say an aircraft, that could establish the provenance of every circuit board, processor, and software component from "cradle to cockpit." The card design firm could use blockchains to log every design iteration of a circuit. Manufacturers could log every model and serial number of every card it produced. Finally, distributors could log the sale of batches of circuits to system integrators, who could log the allocation of circuits to specific aircraft assemblies, and so on. In this context, blockchains create a permanent records for the transfer of assets between owners, thereby establishing provenance.

- **Resilient Communications**.
  Blockchain technology can provide resilient communications in a highly contested environment. In a high-end conflict, we should be prepared for the adversary to contest the electromagnetic spectrum, particularly against critical communication systems such as satellites, undersea cables, and tactical data links. Additionally, adversaries will attempt to manipulate the data to complete the kill chain. Countering this threat will require the capability to securely generate, protect, and share data that is impervious to these adversary actions. Blockchain networks are uniquely able to provide these capabilities. The Bitcoin network demonstrates these capabilities. Bitcoin is relatively immune to suppression due to the mutually reinforcing nature of its security protocols, which include its messaging system, the adaptability of its protocol to various communication mediums, the distributed blockchain database, and the consensus mechanism. Bitcoin uses a peer-to-peer messaging model that propagates every message to every active node across the world within seconds. Every node on the Bitcoin network contributes to this service, including smart phones. If a node's terrestrial, wireless, or satellite internet service is disrupted, a bitcoin message can be sent through alternate channels, such as high-frequency radio, fax or even transcribed into a bar code and hand-carried. However it is received, the servicing node will verify the message, then retransmit it to every connected peer. Some of those peers are the 7,000 full nodes that are independently aggregating messages into new blocks. Because there is no "master"centralized node to disrupt, the network will continue to operate even if large portions become disconnected. Finally, the consensus mechanism ensures that invalid messages and blocks, generated by dishonest actors, are ignored. Together, these protocols ensure that verified message traffic is reliably transmitted, despite malicious attacks against communication paths, individual nodes, or the blockchain itself.

- **Securing and Verifying Remote Assets.** Managing remote assets is a significant responsibility for defence and security organisations. Logging the movement or use of military assets, through various stages in an engagement process, will be more secure when done using blockchain.

- **Managing Defence Projects.** Blockchain can help defence project managers track the progress of different aspects of the project. A single blockchain will help track changes made to all the various components of an assignment. This will help managers analyse the situation better and calculate precise delivery schedules. Government can also overlook the process so that there is a sense of transparency in trade between private contractors and defence stakeholders.

- **Speculative Blockchain Use.**

    - For espionage purposes to pay agents as the process would be effectively untraceable.

    - Blockchain security protocols, if properly implemented by intelligence and security agencies would essentially make state secrets impenetrable.

    - Prevent an information war within India as the authentication protocols provided by blockchain would make it nearly impossible to create and spread “fake news.”

Challenges

Given that there is virtually no movement on adopting blockchain by our armed forces, the process to move towards will definitely be challenging. Some crucial issues are:-

- Mindset is a problem. We need to get used to the fact that, under blockchain technology, electronic transactions are safe, secure and complete.

- Protocols and the question that who will be the ‘miners’ needs to be answered. Legal framework to be modelled to include blockchain technology.

- Migration of systems from existing centralized databases and systems could be tedious and expensive.

- Illegal use of Blockchain tech and hacking distributed networks may be a feasibility at a future date especially when quantum computing matures.

- In-house technical expertise needs to be developed as blockchain implementation will require training of key personnel.

The Way Forward

- Civilian blockchain systems being developed – mainly by banks – are highly secure because the participants and types of activity are controlled by cryptography keys. A magnitude of 10 times the civilian strength would be the starting point for defence applications.

- Further research on areas such as interoperability, network infrastructure and analysis on its regulatory framework should be encouraged.

- Develop organic government expertise in blockchain technology. There is currently limited awareness or

knowledge of blockchain technology within the Armed Forces. To combat this, we should establish a line of research within DRDO to explore the potential blockchain technology. Research is needed to ensure that blockchains are sufficiently scalable, adaptable, and secure to support the broad array of missions in the land, sea, air, space, and cyber domains. For this research we should not only harness the innovative spirit of our brightest junior officers, but also to grow a cadre of scientists and engineers familiar with blockchain technology.

- The Armed Forces should seek partnering opportunities with industry to cooperatively and collaborative develop blockchain based technologies for mutual benefit. The Armed Forces and industry share many common challenges, including the scourge of cybercrime and industrial espionage. Blockchain technology offers a new model of security and trust that could significantly mitigate a growing cyber threat.

- To start with, a pilot project should be given to, say a technical Cat A Training Institute of Army to study the feasibility of implementing some aspects blockchain technology.

Conclusion

Blockchain is a promising technology. The fact that modern militaries are focusing on applications of blockchain technology implies that the day is not far when its applications will percolate down to operational/tractical level operations. However there needs to be concrete plan to migrate to blockchain otherwise we will be playing 'catch up' with our adversaries.