CENTRE FOR LAND WARFARE STUDIES

ISSUE BRIEF

No. 141 June 2018

Utilisation of Blockchain Technology for Armed Forces

Col **Deepak Kumar Gupta** is Director (Archiving & Digitisation), DGPP, IHQ of MoD (Army), New Delhi

The first generation of the digital revolution brought us the Internet of information. The second generation – powered by blockchain technology – is bringing us the Internet of value: a new platform to reshape the world of business and transform the old order of human affairs for the better…[1]

– Don Tapscott, Author

Introduction

A blockchain is a digital, immutable, distributed ledger that chronologically records transactions in near real time. The prerequisite for each subsequent transaction to be added to the ledger is the respective consensus of the network participants (called nodes), thereby creating a continuous mechanism of control regarding manipulation, errors, and data quality. Simply put, blockchain is a protocol for exchanging value over Internet without an intermediary. Blockchain is mostly known as the backbone technology behind the bitcoin (digital currency).

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 timestamp and transaction data. By design, a blockchain is inherently resistant to modification of the data. It is an open, distributed ledger that can record

Key Points

1. A blockchain is a digital, immutable, distributed ledger that chronologically records transactions in near real time.
2. A blockchain is a continuously growing list of records called blocks, which are linked and secured using cryptography.
3. The blockchain is a new information technology that inverts the cybersecurity paradigm completely.
4. Blockchain functions in enhancing cybersecurity by various means such as encrypted authentication, digital signatures and keyless signature encryption, distributed ledgers based on consensus, smart contracts and fault-tolerant transaction processing.
5. In the coming years, the defence research community across the globe is expected to look for new applications for the military, based on the blockchain technology with predominant candidate areas such as cyber defence, secure messaging, resilient communications and the networking of the defence Internet of Things.

The Centre for Land Warfare Studies (CLAWS), New Delhi, is an autonomous think-tank dealing with national security and conceptual aspects of land warfare, including conventional and sub-conventional conflict and terrorism. CLAWS conducts research that is futuristic in outlook and policy-oriented in approach.

Website: www.claws.in Contact us: landwarfare@gmail.com

Utilisation of Blockchain ...

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 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[2].

The whole process starts with someone making a request for a transaction. The transaction is broadcasted to a peer-to-peer network consisting of several nodes (computers). The network validates the transaction and user's status using a known algorithm. Once verified, the transaction is combined with other transactions to make a new block of data for the ledger. The new block is then added to the existing blockchain, in a way permanent and unalterable. In simple terms, technology is about storing blocks of information that are identical across its network.

The typical blockchain network has the following properties[3]:

- The blockchain network cannot be controlled by any single entity and has no single point of failure, thereby building inherent robustness.
- The blockchain network lives in a state of consensus, one that automatically checks in with itself periodically (say ten minutes).
- By design, the blockchain is a decentralised technology. Anything that happens on it is a function of the network as a whole.
- Transparency is embedded within the network as a whole, by definition, it is public.
- Data cannot be corrupted, as altering any unit of information on the blockchain would mean using a huge amount of computing power to override the entire network.

Data and Cybersecurity

Blockchain is a new information technology that inverts the cybersecurity paradigm. Blockchain networks are trustless so they assume that compromise of the network can be done by both insiders and outsiders. Also, blockchains are transparently secure which means they do not rely on failure-prone secrets, but rather on a cryptographic data structure that makes tampering both exceptionally difficult and immediately obvious. Finally, blockchain networks are fault tolerant as they align the efforts of honest nodes to reject those that are dishonest.

The blockchain addresses the fundamental flaws of security by taking away the human factor from the equation, which is usually the weakest link. By leveraging a distributed ledger and taking away the risk of a single point of failure, blockchain technology provides end-to-end privacy and encryption while still ensuring convenience for users[4]. Few security applications that are currently tried by the industry are given in the succeeding paragraphs.

Keyless Signature Infrastructure (KSI)

To connect to any network, public keys are used for authentication and encryption under the prevalent public key infrastructure (PKI). The keys are awarded through digital certificates managed on an authorised central server. By attacking the central repository where certificates are stored, hackers can easily fake user identities and break encrypted exchange of data. But with the help of a blockchain-based technology known as KSI, the public keys can be securely managed, which eliminates the risk of breach. KSI relies on the use of hash function cryptography as compared to the traditional asymmetric key cryptography used in PKI, and provides real-time signature validation to ensure comprehensive enterprise security.

User Access Management

In a blockchain system, an identity of a user can be tied to a tamper-proof hash, making it almost impossible for someone to copy the identity. By matching the identity of an individual tied to the blockchain hash, the entire identity management system can be reconstructed in case of a mishap. Hacking into servers and attaining user passwords is a big cause of enterprise data breach. Blockchain technology is being used to create networks which do not require entering the user password. A unique Secure Sockets Layer certificate is issued to all devices in the network which is recorded on the blockchain, removing the need for an authentication server and password database. This makes it difficult for the hackers to attack those networks.

Ensuring Privacy and Security of Data

There is an inherent danger of social engineering, hacks and other security vulnerabilities in data transactions. The use of a blockchain-decentralised network, which cannot be censored or controlled by any single source, can effectively plug security vulnerabilities. In addition, metadata used for communication of these transactions is

scattered throughout the distributed ledger, and cannot be gathered at one central point, reducing the risk of surveillance through such digital fingerprints.

Tamper-Free Network

Every new block of information being added to a chain is encrypted with a part of the previous chain, making the historical record of data unchangeable. It is designed in a way that if a hacker tries to alter anything on the blockchain, it will cause a change in the entire data signature, which can be easily identified and isolated to alert the network administrators. For a hacker to successfully attack the blockchain network, it would require him to simultaneously alter the constantly updating nodes, making it almost immune to tampering.

Trusted Environment

Blockchain allows users to deal with others whom they ordinarily cannot trust, without the need of a neutral third party or regulator. Using advanced cryptography, a blockchain is unreadable to the members it is shared with. It is based on hash functions that are constantly updated, making it more secure than simple encryption. The distributed nature of blockchain removes the presence of blind trust in third parties.

Secure Web

Blockchain technology is also being used to serve as an alternate form of web protocol in place of the present HTTP, which is known as InterPlanetary File System (IPFS). It is a decentralised peer-to-peer form of network which uses the blockchain protocol and hash cryptography to make a more secure form of internet. IPFS employs nodes to distribute files stored in the network, thus eliminating the central point of failure by ensuring no single node is storing all of the data.

Recent Development across the Globe

The United States of America

The US President, Mr. Donald Trump, has signed a $700 billion military spending bill that includes a mandate for a blockchain cybersecurity research study. The bill, which was signed into law by the President on December 12, 2017, authorises the Department of Defense to look into the 'potential offensive and defensive' cyber applications of distributed database and blockchain technologies. The study forms part of the Modernizing Government Technology Act, which looks to improve the US governments' information technology and cybersecurity systems. The study will look into the following three distinct areas[5]:

- The current efforts by 'foreign powers, extremist organisations and criminal networks' to make use of blockchain technology;
- The planned, or current, use of the technology by both the federal government and 'critical infrastructure networks';
- The vulnerabilities that exist in critical infrastructure networks that could be exploited by cyberattacks.

The engineers of the Defense Advanced Research Projects Agency (DARPA) are currently experimenting with blockchain to create a messaging service that is secure and impenetrable to foreign attacks. This service will be tested internally first and on successful trials, the same may find its way onto the battlefield soon. DARPA is seeking to create a code that will prevent hackers from breaking into secure databases using this technology. DARPA is not the only government agency that has taken notice of blockchain technology and its possible use in the public services but in fact, various subsidiaries and units of the US government have been focusing on the technology in optimising the existing processes, including the US Navy and various federal agencies.

A 2016 military doctrine from the United States Air Force (USAF) outlines the future importance of blockchain technology in cyber defence systems. It has been clearly enumerated in the doctrine that the ability of the USAF to prevail in the highly contested environment of 2040 will be dictated by its ability to defend cyber-enabled systems, and the data within them, from compromise and manipulation. The contemporary cyber defence is faltering and incremental improvements seem unlikely to overcome an exponentially growing cyberthreat. Thus, an entirely new model for cyber defence strategy is needed.[6]

China

China's Ministry of Information Technology and Industry has put blockchain standardisation high up on its list of priorities for 2018. The ministry's Information and Software Bureau has outlined seven major areas of focus in its 2018 agenda, four of which will cover standardisation initiatives that relate to the blockchain technology. Top of the list, based on the announcement, is the formation of a dedicated committee that will seek to develop and roll out a standardised framework for blockchain use in the country.[7]

The committee will recommend standards in Blockchain reference architectures, data format specification, interoperability and smart contracts. The blockchain innovation plan involves linking domestic and international resources as well as investing in Chinese Blockchain projects, attracting foreign investment and leading international blockchain forums.[8]

Data collected from the international patent organisation shows that over half of the 406 patents filed in the field of blockchain technology in 2017 were from China. The country filed 225 blockchain patents, followed by the United States (91) and Australia (13). Chinese patent applications for blockchain technology tripled last year and Chinese companies are six of the top nine filers for blockchain patents from 2012 to 2017, led by Beijing Technology Development Board.[9]

The United Kingdom

Great Britain's upper chamber of parliament, the House of Lords, has recommended the exploration of the possible various applications of blockchain or distributed ledger technology (DLT) across government services. The House added that the government should study the possibility of using the technology in sectors such as national security and public safety, healthcare, cybersecurity as well as customs and immigration. It also claimed that the adoption of blockchain in the public sector could change the relationship between the government and its citizens through the technology's decentralised trust mechanisms.[10]

Defence Science and Technology Laboratory, a UK Ministry of Defence agency, is currently working on using blockchain technology to improve the trustworthiness of a network of sensors (security cameras) and to track the status and level of the individuals' security clearance. The UK's justice ministry is looking at proving tamper-proof evidence by registering them on a blockchain platform. Foreign and Commonwealth Office has improved the way work permits are issued and records stored using said technology. The Police Foundation, a UK think tank focusing on policing and crime, is pushing British police to explore the blockchain technology.[11]

Australia

In March 2018, Standards Australia published a roadmap for Blockchain Standards, emphasising that the industry should first develop blockchain and DLT terminology standards as a means to clarify definitions in the sector and to set the pace for further related standards. Whilst the technology is still an emerging one, Standards Australia highlighted that its applications can be foreseen across a wide spectrum of sectors, namely, financial services, consumer products and services, health, minerals and precious stones, real estate, Internet of Things (IoT) and business.[12]

India

State governments of Andhra Pradesh and Telangana, as well as a few commercial banks are using this technology to protect their database records and fight against cybercrime. A lot of Indian players have tested usage of Blockchain in the areas of trade finance, cross-border payments, bill discounting, supply chain financing, loyalty and digital identity areas. Some of the Indian banks, business conglomerates and one stock exchange are among the pioneers for exploring blockchain in India. Reserve Bank of India (RBI) has been closely monitoring developments related to blockchain technology. In July 2016, Institute for Development and Research in Banking Technology (IDRBT), the technology research arm of RBI, took the initiative of exploring the applicability of blockchain to the Indian Banking and Financial Industry by conducting a workshop involving all the stakeholders, such as the academicians, bankers, regulators and technology partners.[13]

Utilisation of Blockchain Technology for Armed Forces

Blockchain functions in enhancing cybersecurity through various means such as encrypted authentication, digital signatures and keyless signature encryption, distributed ledgers based on consensus, smart contracts and fault-tolerant transaction processing.

The technology is promising as compared to the traditional methods of security. The blockchain technology is recommended to be used for the following:

Joint Operations

Secure data network can be developed for all three services using blockchain technology as issues of trusted environment, tamper-proof network and security of data can be addressed. Integrated messaging service (akin to Army Wide Area Network), web services (akin to Intranet or Air Force Network) and secure peer-to-peer data transfer including intelligence, surveillance, target acquisition, and reconnaissance data can be achieved by deploying integrated data network based on blockchain technology.

Secure Voice over Data Network

It is highly possible to provide secure voice communications over a blockchain network. Web Real-Time Communication Protocol or Session Initiation Protocol (used for Voice over Internet Protocol services) over blockchain network are being utilised by private players to provide secure audio/video voice services (e.g. EncryptoTel)[14]. The same can be utilised for providing secure voice services to armed forces and will be especially useful in joint operations.

Hybrid Cloud

Blockchain technology can be utilised for integration of Intranet and Internet because of trusted network architecture, digital signatures and keyless signature encryption. This integration will result in reduced hardware requirements, increased information accessibility and extend the reach of data network.

Internet of Things

Privacy and security issues are serious concerns for IoT. As the smart devices integrated in IoT are dependent on data and information, the danger is this data could be manipulated or falsified. A number of defence applications are being built around IoT, it is being pondered upon by research community that blockchain, by becoming the backbone to IoT interactions, will create a secure, independent and decentralised platform suitable for developing IoT applications for defence.

Conclusion

In the coming years, the defence research community across the globe is expected to search for new applications for the military based on blockchain technology with predominant candidate areas such as cyber defence, secure messaging, resilient communications and the networking of the defence IoT.

Cyberthreats are a critical and consistent issue in the defence sector. Military organisations constantly battle threats from hacking to data manipulation. The cyber landscape has exposed the inherent vulnerabilities in legacy information management systems. In response, defence research communities are now investing in blockchain systems. This disruptive technology represents the next generational leap in information security and assurance. With a decentralised system facilitated by a blockchain, defence and security organisations can ensure their highly sensitive data is secure and that information integrity is always protected.

Notes

1. https://www.intelligenthq.com/finance/12-bitcoin-and-blockchain-thoughts-and-quotes-you-need-to-read/
2. https://en.wikipedia.org/wiki/Blockchain
3. https://blockgeeks.com/guides/what-is-blockchain-technology/
4. https://www.forbes.com/sites/omribarzilay/2017/08/21/3-ways-blockchain-is-revolutionizing-cybersecurity/#5db0abc12334
5. https://www.blockchaintechnology-news.com/2017/12/13/defence-blockchain-study-authorised-trump/
6. https://www.zerohedge.com/news/2017-12-19/us-military-rushes-study-blockchain-hybrid-wars-loom
7. https://www.coindesk.com/blockchain-standardization-tops-chinese-it-ministrys-2018-agenda/
8. https://cointelegraph.com/news/china-it-ministry-to-create-committee-for-blockchain-standards-domest
9. https://cointelegraph.com/news/china-filed-the-most-blockchain-patents-in-2017
10. https://cointelegraph.com/news/house-of-lords-recommends-exploration-of-blockchain-technology-to-the-british-government
11. http://www.firstpost.com/tech/news-analysis/police-and-military-security-agencies-are-beginning-to-see-blockchain-as-a-potential-solution-to-securing-data-4239465.html
12. org.au/.../News/.../Roadmap_for_Blockchain_Standards_report.pdf
13. http://www.cio.in/feature/blockchain-can-it-strengthen-cybersecurity-indian-enterprises
14. https://blog.wavesplatform.com/encryptotel-launches-groundbreaking-secure-voip-on-waves-82cf84b715c4

... Technology for Armed Forces

References

1. https://www.eda.europa.eu/webzine/issue14/cover-story/blockchain-technology-in-defence
2. https://en.wikipedia.org/wiki/Blockchain
3. https://blockgeeks.com/guides/what-is-blockchain-technology/
4. https://www.forbes.com/sites/omribarzilay/2017/08/21/3-ways-blockchain-is-revolutionizing-cybersecurity/#5db0abc12334
5. https://www.blockchaintechnology-news.com/2017/12/13/defence-blockchain-study-authorised-trump/
6. https://www.zerohedge.com/news/2017-12-19/us-military-rushes-study-blockchain-hybrid-wars-loom
7 https://www.coindesk.com/blockchain-standardization-tops-chinese-it-ministrys-2018-agenda/
8. https://cointelegraph.com/news/china-it-ministry-to-create-committee-for-blockchain-standards-domest
9. https://cointelegraph.com/news/china-filed-the-most-blockchain-patents-in-2017
10. https://cointelegraph.com/news/house-of-lords-recommends-exploration-of-blockchain-technology-to-the-british-government
11. http://www.firstpost.com/tech/news-analysis/police-and-military-security-agencies-are-beginning-to-see-blockchain-as-a-potential-solution-to-securing-data-4239465.html
12. Standards.org.au/.../News/.../Roadmap_for_Blockchain_Standards_report.pdf
13. http://www.cio.in/feature/blockchain-can-it-strengthen-cybersecurity-indian-enterprises
14. https://blog.wavesplatform.com/encryptotel-launches-groundbreaking-secure-voip-on-waves-82cf84b715c4
15. http://www.atimes.com/article/blockchain-secure-internet-things/
16. https://byzgen.com/technology/blockchain-in-defence-and-security/

CENTRE FOR LAND WARFARE STUDIES (CLAWS)
RPSO Complex, Parade Road, Delhi Cantt, New Delhi 110010
Tel.: +91-11-25691308, Fax: +91-11-25692347, Email: landwarfare@gmail.com
Website: www.claws.in
CLAWS Army No. 33098