Military Applications of Blockchain and the Canadian Armed Forces
Date: Sept. 15, 2018

Disclaimer: this briefing note contains summaries of open sources and does not represent the views of the Canadian Association for Security and Intelligence Studies.

KEY EVENTS

Military services and associated research and development agencies with experience in cybersecurity are actively exploring how to utilize / employ blockchain technology within various combat and support roles. Several key events indicate military applications are being pursued. The United States signed into law the 2018 National Defense Authorization Act, a $700 billion defense policy bill that mandates for a "briefing on cyber applications of blockchain technology." The Russian Defense Ministry is building a research lab to test blockchain applications under the direction of the Russian Federation's 8th Directorate of the General Staff of the Armed forces in the coastal town of Anapa on the Black Sea.

NATURE OF DISCUSSION

This briefing note will consider the following issues:

1. A broad background of blockchain such as who invented it, why it was invented and how does it work.
2. Strengths and weaknesses of blockchain.
3. Current civilian applications of blockchain.

After the brief introduction, a detailed presentation of military application of blockchain technology is presented. Broadly grouped military blockchains are considered to applicable to theatre-level operations (offensive and defensive), strategic level (offensive and defensive).

The final discussion will be about North Korea as a blockchain threat, and Colombia as the emerging blockchain research and development hub affecting North America.

BACKGROUND

Blockchain was developed in 2008 by Satoshi Nakamoto (a pseudonym) to support the peer-to-peer electronic cash systems called Bitcoin. The identity of Nakamoto remains unknown till this day. It is estimated that whoever invented Bitcoin is sitting on approximately $7 billion USD.

The strengths of the blockchain is summarized as follows. Blockchain is a permanent and tamper-proof record of transactional data, within a peer-to-peer (P2P) network. With these traits, the blockchain cannot be attacked at a single point of failure, and continually updates and validates itself simultaneously, after which a hash value is generated and used to validate each subsequent block. If the validation fails, no new blocks can be added. In order for blockchain to be valid, a majority of the P2P nodes must agree on the block hash value.

The vulnerability of blockchain is summarized as follows. Blockchain's cryptotext format is standardized which means certain letters, characters, or numbers are always in the sample places – which means the attacker can begin predict the block's encryption. The underlying SHA-256 Cryptographic Hash Algorithm (designed by NSA) provides a value consisting of an almost unique 256-bit (32-byte) signature for the text. Hackers' can attack the SHA-256 is implemented correctly, and the cryptotext can not be hacked, the hacker attacks the website hosting the transactions using stolen computer administrator login credentials.

Blockchain usage in civilian applications include converting illiquid assets such as penny stocks, microcap stocks and nanocap stocks; ownership interests in private companies; collectibles like art and antiques; partnership shares in hedge funds and alternative investments; certain types of options, futures and forward contracts; and some types of bonds and debt instruments into tradable goods as well as increasing supply chain management transparency which enable multiple parties to product development see the provenance of the product, smart metering and selling of solar power generation, and increased portability of healthcare patient records.

The remaining section explores military application of blockchain technology is presented. Broadly grouped military blockchains are applicable to theatre-level (offensive and defensive) and strategic-level (offensive and defensive) operations. Specific examples are: supply chain and procurement support for deployment of troops and equipment, security of operations at the tactical level, promoting transparency of the weapons and munitions manufacturing process, information assurance and confidence of battlefield generated data, and preventing cyber and physical attacks.

Given the security functions of blockchain and diversity of applications, the US Air Force is currently developing military doctrine which outlines the future importance of blockchains in cyber defense systems. The doctrine specifically acknowledges that contemporary cyber defense is faltering, and incremental improvements seem unlikely to overcome an exponentially growing cyber threat. Thus, an entirely new model for cyber defense strategy is needed. This new model will be blockchain based. Specific military examples are drone flight decision and engagement decision, Aegis military platform deployed on battleships, protecting DOD critical communication systems such as satellites, undersea cables, and tactical datalinks; and finally, monitoring of contaminated nuclear or chemical waste at a military base.

Final points to consider, North Korea and Colombia.

North Korea. The dominant contributions of blockchain are linked to Europe, Russia, United States, and Canada. However, North Korea and Colombia must also be considered. North Korea is estimated to earn between $15 million and $200 million by creating and selling cryptocurrencies and then turning it into hard cash to fund its nuclear and ballistic missile program. Another example of North Korea's cybercrime capability is the successful 2015 theft of $81 million from the Central Bank of Bangladesh. North Korea continues to attract bitcoin and blockchain interest with the announcement that it will be hosting the Korean International Blockchain Conference (October 1st to 3rd, 2018) which will attract world experts who will be providing consulting services to North Korean business leaders on the final day of the conference.

Colombia. President Ivan Duque intends to turn Colombia into a technological leader in the region. His strategy consists of tax exemptions for technology and information companies as well as dedicated government-appointed technology advisor. Evidence which supports this strategy is the start-up of the Colombia Blockchain Association was announced, where 6 companies (IntiColombia, RSK, Buda Colombia, Cajero.co, Panda Group and Bitcoin Colombia) related to the sector have come together to implement the technology in the country. This dedicated sector approach is unique to Colombia and suggests Latin America may be moving towards technology innovation. Colombia continues to deal with organized crime threats to banking executives, government officials, and corruption. The presence of the high tech innovation strategy may be lucrative financial incentives which will attract organized crime involvement.

KEY POINTS OF DISCUSSION AND WEST COAST PERSPECTIVES

Canada's Department of Defence's Defence Research and Development Canada (DRDC) published in June 2018 analysis of blockchain contribution to the military domain and concluded "it is far from clear that it (blockchain) is the correct solution" for the problems noted above and should still be considered carefully. Considering this cautious conclusion, the following opportunities should be considered as means of exploring the challenges of blockchain within existing military context.

Relevant to Canada Opportunities:

- **Leveraging Opportunity:** NATO is presenting at UBC Blockchain in November 2018, what are the fuller implications for technology adoption and adaption by CAF/DND within a NATO context?
- **Blockchain Innovation in Canada:** What are the opportunity to leverage US Air Force research on blockchain?
- **Immediate implications:** Should the DND / CAF approach WASHINGTON GROUP (North Vancouver) contractor for Canadian Coast Guard – requesting research to include blockchain capabilities for DND/CAF within an existing operational environment?