# Blockchains and smart contracts for the Network-Centric Warfare

Silvio Roberto Assunção de Oliveira Filho, Fernando Rodrigues de Sá
Instituto Tecnológico de Aeronáutica (ITA), São José dos Campos/SP – Brasil

***Abstract* – In the age of information, Network-Centric Warfare (NCW), a theory of war, is a concept of operations based on the sharing of information on the Battlefield**. **Blockchain, a recently proposed data structure and decentralized network has a variety of applications in warfare theory. Blockchain technology can improve the availability and integrity of data with its concept of work, a chain of blocks, that stores information which cannot be changed or erased. Bitcoin was the first and it is the most known blockchain and cryptocurrency, proposed by Sakamoto, in 2008, and has proven that it possesses the capability to become a disruptive technology. In a private network, blockchain has strong security and in a public, it has an accessibility as a detached feature. Speed, costs and censorship are just some of the important aspects between licensed and public systems. We present the main features of this new technology and its defense applications in NCW, as well as its limitations. We present possibilities of blockchain application based on his features found in literature and suggest application, thus surmising that blockchain has a variety of possibilities in logistics, communication and in the military industries.**

***keywords* – blockchain, distributed processing, network-centric warfare.**

## I. INTRODUCTION

In the information age, a network-centric warfare (NCW) is a concept of operations based on the sharing of information between people, systems and sensors in the Battlefield. First used, by the USA, in the invasion of Granada in 1983 and in the Persian Gulf War in 1990 and widely accepted in the lightning-fast invasion of Iraq. NCW provided forces with data sharing and situational Awareness capability with significant advantages during this war [1]. Improving the transmission of information increases the speed of command and transforms the superiority of information into military advantage in Military Operations.

In the field of combined operations, with multiple nations forces, communications become even more critical when various agent such as human, sensor and equipment produce and share a huge battle field data, blockchain is a possible structure to support the network necessary capacities as, integrity, confidentiality and availability, became extended with authentication of the data creator, fast dissemination for every player, and finally maintaining a sustainability of network.

Blockchain, a proposed data structure and decentralized network [2] has a variety of applications in this warfare. As proposed in reference [3] Blockchain technology can improve the availability and integrity of data with its concept of work, explained in detail in section II of this paper.

Bitcoin was the first, and it is the most known cryptocurrency and blockchain proposed by Sakamoto [2] has proven that it possesses the capability to become a disruptive technology [3]. But, it is much more than only a cryptocurrency confident structure. While "blockchain" was virtually pseudonymous of Bitcoin for these years, it should be made clear that they are two separate technologies.

> *Bitcoin is just the first popular use of blockchain, just as email was the first application of the internet. The blockchain can be used for any form of asset registry, inventory and exchange, including every area of finance, economics, and money; hard assets (physical property); and intangible assets (votes, ideas, reputation, intention, health data, and information).* [4]

Blockchain is an algorithmic data structure that allows creating a resilient tamper-proof digital ledger of transactions between various users or nodes. This technology uses cryptographic to sign and secure the data writing and a concept of ledger, a financial transaction of registry, to store all data along the time frame and as a financial ledger, where all cash transactions are stored in sequential and permanent books by time-stamp.

A huge variety of research is being carried out in the areas of application [3], this paper intends to focus in military application and describe possibilities of application proposed in [3] and go further with more implementations cases.

The paper is organized as follows. Blockchain features is described in section II. Section III is shown and discussed the possibilities of use in military application [3]. Section IV describes final observations.

## II. BLOCKCHAIN TECHNOLOGY FEATURES

The structure of blocks, where data, the transactions in the case of Bitcoin, are linked maintaining the integrity and the immutability of the whole structure.

In blockchain the data storage structure is one block, each block is connected to the former, from the first block known as "genesis" [2]. Each subsequent block stores information about the previous block and the new data to be stored. Thus, if any data is changed, the entire structure must be modified, making the manipulation of only one block perceptible and not accepted by the net.

The blockchain has several integrated technologies, described below.

### *A. Technologies onboard*

1) Peer to Peer Network (P2P): there is no central node or hierarchical structure in the network. The Gossip Protocol [5] is used to flood the data on the network. Decentralization

Silvio R Assunção de oliveira Filho, silviora@ita.br; Fernando Rodrigues de Sá, desa@ita.br.

allows nodes to join or leave the network making it fault-tolerant. It adapts to frequent changes in number of nodes and accommodate growth by becoming highly scalable [3].

2) Cryptography: using cryptographic techniques such as hash, each node maintains information from the previous, up to the first, the "genesis". The crypto concept of public and private keys signs the transmission of data and verifies the authenticity of all messages. Because all messages are stored in the data structure, each transaction is maintained and can be verified by any entity with access to the blockchain.

3) Consensus mechanism: there are many methods to reach consensus to see if it is a trusted block to be inserted into the chain. This is a process that allows "a set of distributed processes to reach agreement on a value or an action, despite several defective processes [4]. This was formally known as the Byzantine General's Problem [6].

In a decentralized network, consensus is used to prevent malicious users from writing invalid information. The most common is the Proof of Work (PoW), which uses a puzzle to be solved before inserting new information. Other consensuses are: Stake Proof (PoS), Proof of Importance (PoI), Practical Tolerance to Byzantine Faults (PBFT), etc. [3].

### B. Block Construction

In Bitcoin blockchain, each block has the previous hash address, a time stamp, a nonce that is the puzzle answer and a tree of information, transactions in this case, as shown in figure 1 [2]. As seen, data could be anything digital, since registries, as music or financial transactions, even application codes.

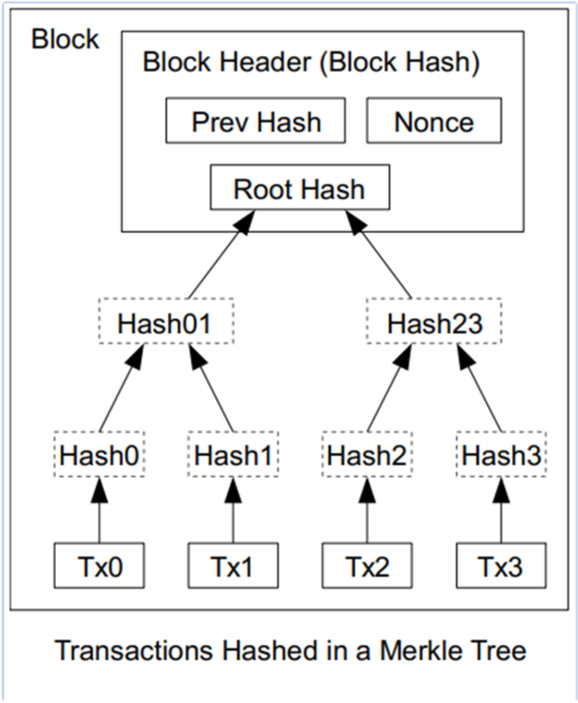

Fig 1. Block Structure [2].

### C. Smart Contract - Turing-Complete Virtual Machine

Nakamoto implemented two important blockchain concepts in Bitcoin, the decentralized ledger and the value transfer protocol without the need for intermediaries. The third designed by Nakamoto is the ability of the network to execute algorithms, which was firstly presented on the Ethereum network, the second most known cryptocurrency, created by Vitalik Buterin in 2013.

> *Nakamoto envisioned not just sending money from point A to point B, but having programmable money and a full feature set to enable it. One blockchain infrastructure project aiming to deliver a Turing-complete scripting language and Turing-complete platform is Ethereum. [4]*

In Ethereum platform, it is possible build and publish scripts, such as distributed applications that run over the network when accessed by any node on the net.

A common example is a contract to send goods from seller A to buyer B, using the smart contract as an intermediary. The buyer sends the value to the application at an Ethereum address wallet and the "script" only releases the value to the seller upon receipt and approval of the receipt of the goods by the buyer. In case of any disagreement, both dealers are responsible for resolving it, until a scheduled date, when the values will be automatically deleted by the script.

Making the application even more "smart", the contract itself can monitor the sending and receiving of merchandise, releasing partial values or triggering functions in steps.

In NCW, the smart contract could execute commands using the network autonomously, such as updating the target's location or canceling a mission because there are restrictions, identified in real time, since they were previously implemented in the smart contract algorithm.

In the third example of the reference [3], smart contracts are used in Ammunition Management, these scripts being incorporated into the munition system, can send alerts or usage restrictions autonomously, and run the most secure real-time transport and storage of ammunition. Even further, it may even deny the loading, which may be carried out autonomously by some robot, on an unmanned aircraft. In a fully automated process.

### D. Blockchain Consortium

Blockchain can be created publicly, such as crypto-networks, private, so-called "permissioned network", or even hybrid, depending on the hosts or players involved.

This accessibility should be defined in the design of the blockchain, depending on the level of security and use of the information. Such data may contain public information, such as property of assets or values, or restricted access, such as personal information or government data.

Public networks allow anyone to have access with anonymity. Everyone can log in, out or access data in these cases.

Blockchains with permission, in addition to the hosts being on private nodes, players' access can be restricted on a white list, with the advantage of this network being safer, faster and smaller.

Hyperledger Project Framework is a Linux Foundation permissioned project [7] launched in 2015, as an open-source permissioned blockchain.

Hybrid blockchains provide different data access: read-only, read and write, and allow combinations of anonymous or identified users.

TABLE I PUBLIC X PERMISSIONED COMPARISON. ADAPTED FROM [8]

| ***Feature*** | ***Bitcoin*** | ***Hyperledger Framework*** |
|---|---|---|
| Cryptocurrency based | Yes | No |
| Permissioned | No | Yes |
| Anonymous | Yes | No |
| Privacy | Yes | Yes |
| Immutable ledger | Yes | Yes |
| Distributed | Yes | Yes |
| Smart Contracts | No | Yes |
| Consensus protocol | Proof of work | Several Options |
| Transaction rate | Very low | High |

### *E. Blockchain NCW*

Below are the features of blockchain that is most suitable for NCW.

1) Restrict Access in NCW

In a permissioned implementation, blockchain has strong security. Speed, costs and censorship are just some of the important aspects between licensed and public systems [3]. Players in this case must be identified and allowed access to read or make changes in database.

2) Robust and availability

Each node maintains a complete copy of the records, offering availability and robustness against point-of-failure, being fault tolerant.

3) Decentralized Data Storage and Resilience

The blockchain allows the node to enter or leave the network, keeping the network resilient in the event of loss of one or more nodes [3]. This characteristic imposes a vulnerability, because as all nodes have the entire database, it is a weakness to be considered in the case of unauthorized access to the network, or the hijacking of a node. There is a need for management and the use of techniques such as data encryption or partitioning.

4) Longevity, immutability and Audit

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.

All Data is stored in blockchain, since the beginning of operations. Even if this information is lost from a majority of the nodes, it can still be retrieved, and it is immutable.

It is a good feature in case of post-operation audit.

5) Propagation, Clarity and transparency

Any data is publicly viewed, for network players, in a single ledger, keeping simple all data record.

### *F. Blockchain limitations for NCW*

Blockchain is in early development, so there are different kinds of potential limitations. These restrictions are related to technical issues, ongoing industry thefts and scandals, public perception and government regulation [4].

1) Limitation of Data Processing

Bitcoin blockchain has a limitation of 7 transactions per second, which is extremely low in comparison with VISA that can process peaks of 10.000 transactions per second [4].

This limitation should be considered in NCW blockchain implementation, but there is a variety of studies to minimize this problem. For example, the Litecoin which is at least slightly faster than Bitcoin.

2) Scalability

The Bitcoin community calls the size problem “bloat”. The blockchain is 25 GB and grew by 14 GB in the last year [4].

It is a problem when for decentralization reasons every node must run the full node. Large data is solved using different technics [9].

Thinking about all transactions in Bitcoin since 2008, 25 GB is not so big when you consider Big Data. In NCW, permissioned blockchain can easily be stored in small drives, as in Internet of Things onboard nodes.

3) Privacy and security

In public network, all data is accessible, in case of Bitcoin or Copyright, they intend to be public. But in case of personal information, or even in propriety ownership, it should be a permissioned blockchain. As in NCW, depending on data.

Public access and transparency are not intended to be shared, but as described above, blockchain can be encrypted, which will increase the data processing necessity.

A 51-percent attack should be considering in NCW, problem which is degraded in blockchain growth. Another kind of consensus, when not using PoW, example Proof of Stake (PoS), requires less computational power and improve security for small chains. [4]

4) Legal and Regulatory

Smart contracts and programmable logic resources can improve the time spent negotiating and formalizing contracts. But credibility under existing laws and responsibilities are not clearly defined. [3]

## III. CASES OF STUDIES

Reference [3] describes blockchain’s application in three first defense possibility:

### *A. Data Communication in Battlefield Management System*

Blockchain technology can ensure robust data communication in hostile environments, ensuring the provenance of data, the use of encryption and consensus mechanism among users.

This can avoid the possibility of corruption or alteration of data. In addition, the decentralized nature helps to improve the sustainability of the network [3].

Blockchain technology is essentially an information technology.

### B. Logistics Support for the Armed Forces

Blockchain guarantees the provenance by creating a distributed and tamper-proof transaction record between multiple manufacturers, retailers, vendors and end users. Each provider or receiver element in the chain can maintain a copy of the complete database. Users are identified by their digital signatures. Smart contracts are run between players for transparency and validation. Transactions can be verified and processed independently by each user. [3]

Optimizing a supply chain in the blockchain enables new things, such as real-time synchronization of decisions with supply chain partners [9]

### C. Smart Contracts in Ammunition Management

Distributed Ledger technology can provide real-time access to information such as manufacturing details, transportation status and ammunition stock at multiple locations for end users and manufacturers. Smart contracts will increase the efficiency of supply chain management through the proactive implementation of activities such as recycling, segregation and repair of affected ammunition [3].

In addition, in the case of fully autonomous management chains, Intelligent Contracts and IoT can be fully integrated to control the expiration of ammunition items and restrict shipment, which is also done autonomously by robots.

### D. Possible future Directions in NCW

Register of DNA and information of combatants in blockchain can be used to identify bodies or nationality of wounded, as well as in a humanitarian attitude, be shared among the members of the conflicts. As well it can be used to store patient's health information in Red Cross hospital with shared databank.

## IV. Final Observations

Blockchain technology can be quite complementary in a space of possibilities for the future world, which includes centralized and decentralized models. Like any new technology, the blockchain is an idea that initially disrupts and, over time, could promote the development of a larger ecosystem, which would include both the old and the innovative new paths.

Furthermore, we listed features of blockchain that is applied in Bitcoin, and even more specific in NCW applications.

Possibilities of uses are difficult to predict but by the innovation of this technology, several fields of research are open.

We are developing this technology in Aeronautic Institute of Technology (ITA) and intend to create a prototype soon.

## References

[1] A. Yang, "Understanding network centric warfare," *ASOR BULLETIN*, vol. 23, nº 4, pp. 2-6, 2004.

[2] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.

[3] A. Sudhan and M. J. Nene, "Employability of Blockchain Technology in defence applications," in *2017 International Conference on Intelligent Sustainable Systems (ICISS) IEEE*, 2017.

[4] M. Swan, Blockchain: Blueprint for a new economy, O'Reilly Media, Inc., 2015.

[5] K. Jenkins, K. Hopkinson e K. Birman, "A gossip protocol for subgroup multicast," em *Distributed Computing Systems Workshop, 2001 International Conference on. IEEE*, 2001.

[6] M. Correia, G. S. Veronese, N. F. Neves e P. Verissimo, "Byzantine Consensus in Asynchronous Message-Passing Systems: a Survey," em *International Journal of Critical Computer-Based Systems*, 2011.

[7] C. CACHIN, "Architecture of the hyperledger blockchain fabric," em *Workshop on Distributed Cryptocurrencies and Consensus Ledgers*, 2016.

[8] F. A. CARS, "Blockchains and Content-Centric Networking," *ieee vehicular technology magazine*, 2018.

[9] H. Watanabe, "Blockchain contract: Securing a blockchain applied to smart contracts," em *2016 IEEE International Conference on. IEEE*, 2016.