Journal of The Korea Society of Computer and Information
Vol. 23 No. 12, pp. 49-55, December 2018
www.ksci.re.kr
https://doi.org/10.9708/jksci.2018.23.12.049

Blockchain Technology and Utilization Schemes in Tactical Communication Network

In-Deok Yoo*, Woo-Sin Lee*, Hack-Joon Kim*, So-Yeon Jin*, Se-Hyeon Jo*

Abstract

In this paper, we propose schemes of blockchain utilization in tactical communication environment. The military tactical communication environment has similar characteristics with blockchain network such as distributed architecture, decentralization, and the need for data integrity. A communication node constituting a tactical communication network is constituted by a system capable of configuring and connecting a network for each node. When a communication node, having such capabilities, is configured as a node of blockchain network, various functions could be performed. In this paper, we propose utilization schemes of authentication, integrity, record management, and privilege control based blockchain technology. Functions for authentication, integrity verification, and record management need to ensure the stored data and could track history. The requirement of function's characteristics are matched to blockchain which is storing data sequentially and difficult to hack data, so that it could perform functionally and sufficiently well. Functions for authority control should be able to assign different privileges according to the state of the requestor. Smart contract will function when certain conditions are satisfied and it will be able to perform its functions by using it.

In this paper, we will look over functions and utilization schemes of blockchain technology which could reliably share and synchronize data in a tactical communication environment composed of distributed network environment.

▸Keyword: Blockchain, Blockchain technology, Tactical communication, Tactical communication network, NCW(Network Centric Warfare)

I. Introduction

우리나라 군 전술 환경은 IP 기반의 전술통신망을 갖춰나가면서 네트워크 중심전(NCW, Network Centric Warfare) 환경을 구축해나가고 있는 상태이며[1], 정찰 정보, 전술 정보, 명령 등 전술통신망과 국방망을 통해 유통되는 정보의 종류와 유통량이 많아지고 있다. 이런 다양한 종류의 정보 데이터는 기지국 역할을 하는 여러 통신 노드를 거쳐 상급부대 또는 지휘본부로 전달되고, 전술 명령 또한 지휘본부에서 작전 부대까지 여러 통신 노드를 거쳐 전달이 된다. 하지만 산악 지형에 분산 형태로 구성되고 이동성이 높은 통신 노드들 특성 상 무선 통신 환경이 수시로 변경되기 때문에 전술 통신 환경에서 데이터를 지속적으로 공유하고 동기화하기에는 많은 어려움이 존재한다. 블록체인은 이와 같은 분산 네트워크 환경에서 데이터를 신뢰성 있게 공유하고 동기화 할 수 있는 기술이라고 할 수 있다.

2008년 사토시 나카모토의 논문 'Bitcoin : A Peer-to-Peer Electronic Cash System'에서 처음 제안된 블록체인 개념[2]은 금융 분야를 넘어 다양한 산업 분야에서 연구 및 적용되고 있다. 블록체인 기술은 탈중앙화 환경에서 노드로 불리우는 블록체인 네트워크 참여자들이 동일한 데이터를 공유할 수 있는 기술로 네

• First Author: In-Deok Yoo, Corresponding Author: In-Deok Yoo
*In-Deok Yoo (indeok.yoo@hanwha.com), Communication SW Team, Hanwha Systems
*Woo-Sin Lee (woosin.lee@hanwha.com), Communication SW Team, Hanwha Systems
*Hack-Joon Kim (hjn.kim@hanwha.com), Communication SW Team, Hanwha Systems
*So-Yeon Jin (soyeon.jin@hanwha.com), Communication SW Team, Hanwha Systems
*Se-Hyeon Jo (shn.jo@hanwha.com), Communication SW Team, Hanwha Systems
• Received: 2018. 10. 26, Revised: 2018. 11. 15, Accepted: 2018. 11. 21.

트워크상에 원격으로 존재하는 노드 간 공유 데이터를 동기화하고 투명하게 관리 할 수 있는 장점을 가지고 있다. 이러한 블록체인 기술의 장점을 필두로 공유 데이터가 위변조 되지 않았다는 높은 신뢰를 필요로 하는 금융, 물류, 거래, 인증 등의 분야에서 연구 개발이 활발히 진행되고 있으며[3-7], 국방 분야에서도 전술 명령과 같은 고신뢰를 요구하는 정보를 배포하고 공유하는 만큼 블록체인 기술 활용에 대한 관심이 커지고 있는 상태이다.

드론, 로봇, 자율 주행 차량 등 무인화 체계가 많아지고 미래 전술 환경에서 중심이 될 무인화 체계 제어 및 통제를 위한 정보 보안의 중요성은 현재보다 더욱 커질 것이다. 해킹으로 인해 임무 데이터가 위변조 될 경우 임무 실패, 자산 유실 뿐만 아니라 아군의 안전까지 위협 받을 수 있고, 동료 무인체계로 전파될 경우 해당 부대의 손실을 발생 시킬 수도 있다. 군인의 경우 판단을 통해 잘못된 명령을 식별하고 거부할 수 있겠지만 무인체계인 경우 해킹에 의해 위변조 된 정보라고 할지라도 진위여부를 판단 할 뿐 도덕적인 판단은 할 수가 없기 때문이다.

블록체인 기술은 앞서 언급한 바와 같이 정보의 신뢰성 보장이 필요하고 데이터 동기화를 유지하며 변경 기록의 확인이 필요한 환경에 적용하기 적합하며, 이는 곧 무인화 체계로 변화하는 전술 환경에서 정보의 신뢰성을 보장 할 수 있는 방안으로 적합하다고 볼 수 있다.

본 논문에서는 금융, 물류 등의 산업 분야와는 큰 차이를 갖는 전술 환경에서 활용 가능한 기능 및 방안에 대해 제시하고자 한다. 2장에서 블록체인을 구성하는 주요 기술들에 대해 정리하고 3장에서 활용 방안을 살펴본 후 마지막으로 결론을 짓고자 한다.

II. Preliminaries

1. Blockchain

블록체인은 거래가 가능한 암호화폐로 유명세를 얻으며 화폐 기능이 부각되었다. 하지만 기본 기능은 거래 이력 정보를 블록이라 불리우는 하나의 데이터셋 형태로 구성하고, 주기적으로 생성되는 블록을 주변 노드에 전파하면서 합의 과정을 통해 유효성이 검증된 블록을 체인 형태로 연결하여 모든 노드가 동일한 정보를 저장하는 것이다. 각 블록은 생성 과정에서 이전 블록의 hash 값을 포함하여 자신의 hash 값을 생성하고 그림 1과 같이 순차적으로 연결되기 때문에 저장된 데이터의 위변조가 어려운 특징을 갖는다. 비트코인, 이더리움과 같은 블록체인의 각 블록은 중앙집중화된 데이터베이스에 저장된 정보와 달리 데이터에 대한 접근 제한이 없기 때문에 누구나 세부 내역을 확인할 수 있고, 이 때문에 투명성의 특징을 갖는다. 하지만 투명성을 갖는 블록체인의 특징은 정보 보안이 중요한 국방 또는 기업체에서 블록체인을 사용하기에 어렵도록 하는 주 요인이다. 이런 이유로 허가 받은 네트워크 참여자만 노드에 접근이 가능한 허가형 방식의 블록체인이 생겨났다. 대표적으로 IBM의 하이퍼렛저 패브릭과 R3의 Corda가 있다. 비허가형과 허가형 블록체인은 표 1과 같은 차이를 갖는다.

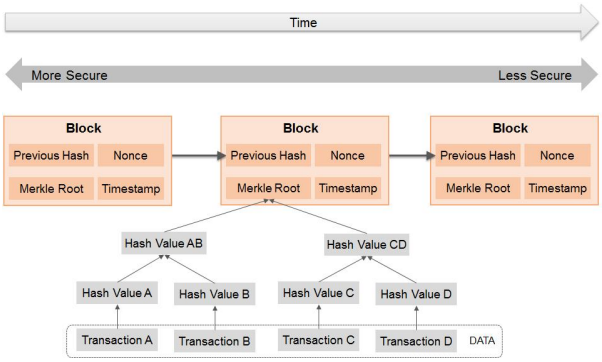

Fig. 1. Blockchain structure

Table 1. Comparison of Permissionless and Permissioned blockchain

	Permissionless (Public)	Permissioned (Private)
Block Access	Every user	Permitted user
Validate and approve transactions	Every user	Permitted user
Transaction request	Every user	Permitted user
Consensus algorithm	PoW or PoS	PBFT Algorithm
Structure	Decentralized, Distributed	half-centralized, Distributed
Platforms	Bitcoin, Ethereum	HyperLedger Fabric, Corda

블록체인은 사용 목적과 구성에 따라 비허가형, 허가형으로 구분이 가능하지만 블록체인을 구성하는 주요 기술은 동일하다고 할 수 있다. 본 논문에서는 비트코인 블록체인을 바탕으로 블록체인을 구성하는 주요 기술을 살펴보고자 한다.

1.1 DLT(Distributed Ledger Technology)

분산 원장(Distributed Ledger), 공유 원장(Shared Ledger)로도 불리는 분산 원장 기술(DLT, Distributed Ledger Technology)은 합의 알고리즘을 통해 원격에 존재하는 노드들 간 디지털 데이터를 공유하고 동기화를 수행하는 기술이다[8].

비트코인 블록체인에서는 디지털 데이터에 해당하는 블록에 암호화폐 거래 이력을 기록하고 신규로 생성되는 블록들을 인접 노드에 배포함과 동시에 자신의 체인에 순차적으로 연결한다. 신규 블록은 생성 과정에서 체인의 마지막에 연결된 블록의 hash 값을 포함하고, 해당 값을 포함한 상태에서 자신의 hash 값을 생성한다. 신규 블록을 수신한 인접 노드에서는 이전 블록과의 hash 값 비교를 포함하여 블록 검증을 수행하고, 유효성이 입증된 블록은 체인에 연결하여 단일 블록체인을 구성하게 된다.

만약 잘못 생성된 블록 또는 해킹으로 인해 값이 변경된 블록이 배포된 경우에는 이전 블록과의 hash 값 비교를 통해서

잘못된 블록임을 판단하고 연결을 거부하게 된다. 이와 같이 블록체인을 구성하는 과정에서 신규 블록 생성부터 배포, 검증 및 체인 구성까지를 합의 과정이라고 할 수 있다.

1.1.1 Merkle Tree

비트코인 블록체인에 연결된 블록들은 그림 1과 같이 거래 이력 정보를 데이터로 관리하고 있다. 블록에 저장되어 있는 모든 거래 이력 데이터는 블록 헤더의 Merkle Root 필드를 통해서 관리가 되는데, Merkle Root 는 거래 이력 정보들의 최종 hash 값을 나타낸다. Merkle Root를 생성하는 과정을 살펴보면 각각의 거래 이력 정보 별로 hash 과정을 거쳐 hash 값을 생성하고, 생성된 hash 값들을 다시 hash 하는 방식을 반복 수행하여 최종 hash 값인 Merkle Root 값을 도출하게 된다. 이 과정에서 생성되는 hash 값들은 그림 2와 같이 tree 구조 형태로 연결이 되는데, 이는 거래 내역 정보들을 효율적으로 관리할 수 있게 한다. Tree 구조로 연결된 거래 이력 정보가 변경될 경우 상위 레이어에 연결되어 있는 hash 값이 전부 변경되어 블록 헤더에 저장되어 있는 Merkle Root와 다른 값을 갖게 되므로 블록에 포함된 거래 이력의 수와 상관없이 빠르게 데이터의 변경 유무를 확인 할 수 있고, 위변조된 데이터 탐색도 빠르게 처리 할 수 있다. Merkle Tree는 블록체인 상의 각 블록에 저장된 데이터를 효율적으로 관리하고 데이터의 무결성을 보장 할 수 있는 자료구조이다.

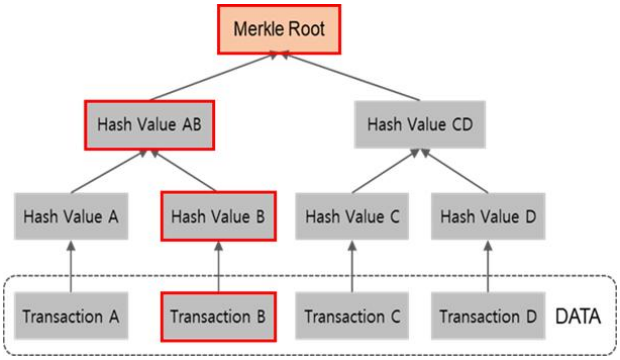

Fig. 2. Merkle tree structure

1.1.2 Hash

Hash 함수는 입력으로 주어진 데이터를 고정된 길이의 데이터로 바꾸어 출력하는 함수이다. 동일한 입력 데이터에 대해서는 동일한 출력 값을 보장하지만 입력 데이터가 1Byte라도 달라지면 전혀 다른 값을 출력하는 특징이 있다. 예를 들면 1byte 데이터와 100byte의 데이터를 입력해도 출력 값은 32 Byte로 동일한 것이다.

Fig. 3. Hash function

Hash 함수는 그림 3과 같이 역산이 불가능한 대표적인 단방향 함수이며 빠른 연산 속도를 바탕으로 Hash table을 사용하는 검색 등에 많이 사용된다. 비트코인 블록체인에서는 SHA-256 Hash 함수를 사용한다.

1.2 P2P Network

P2P 네트워크는 네트워크 참여자들이 클라이언트, 서버 역할을 동시에 수행하며 구성하는 네트워크 구조로 P2P 네트워크와 오버레이로 구성된다. P2P 네트워크는 네트워크 참여자 간 데이터 통신을 수행하는 기능으로 Hybrid P2P, Pure P2P로 구분 할 수 있다. Hybrid P2P는 각 노드의 정보를 보유한 인덱스 서버로부터 목적지 노드 정보를 얻어서 해당 노드와 직접 데이터 통신을 수행하는 방식으로 설계와 관리는 편리하지만 확장성이 떨어지는 특징이 있다. Pure P2P는 인덱스 서버와 같은 데이터 정보를 갖는 특정 서버가 없고 노드 간 메시지 전송을 통해 데이터 검색을 수행한다. 서버가 없는 만큼 확장성이 좋으나 시스템 설계 및 관리가 어렵고 Hybrid P2P와 달리 노드 검색을 위한 알고리즘이 필요한 특징이 있다. 오버레이는 노드 탐색을 위해 응용 프로그램 수준의 네트워크를 구축하는 것으로 비구조화/구조화 오버레이로 구성된다. 구조화 오버레이는 노드 별로 탐색 메시지를 전달할 노드가 사전에 정의되어 있는 반면 비구조화 오버레이는 인접 노드로 탐색 메시지를 배포하여 노드 탐색을 수행한다.

1.3 PKI(Public Key Infrastructure)

메시지 송신자와 수신자가 서로 다른 키를 이용하여 송수신 데이터 암호화 및 디지털 서명이 가능한 비대칭 알고리즘으로 공개키/비공개키의 한 쌍의 키로 구성된다. 수신자 측에서 키 생성을 한 경우 송신자의 요청 시 공개키를 전달하고, 송신자로부터 공개키로 암호화한 데이터를 수신하게 되면 보관하고 있는 비공개키로 복호화하여 원본 데이터를 복원 할 수 있다. 송신자 또한 수신자가 비공개키로 암호화한 데이터를 전송하면 공개키를 이용하여 복호화 할 수 있다. 그림 4는 이와 같은 암복호화 매커니즘을 간단히 표현하고 있다.

Fig. 4. Encryption and decryption mechanism

공개키/비공개키를 이용하면 데이터 암호화 뿐만 아니라 전자 서명을 통한 유효성 검증이 가능하다. 송신자가 비공개키를 이용하여 디지털 서명을 포함하는 데이터를 송신할 경우 수신자는 데이터에 포함된 송신자의 공개키를 이용하여 데이터 복호화 뿐만 아니라 디지털 서명 확인을 통한 유효성 검증이 가능하기 때문에 데이터의 신뢰성 확보가 가능하다.

1.4 Consensus algorithm

블록체인 네트워크에 참여하는 노드는 원격에 분산되어 존재하게 된다. 각 노드 간 데이터를 공유하면서도 동기화를 유지하기 위해서는 일종의 규칙이 필요한데 합의 알고리즘이 그에 해당한다. 특정 노드에서 배포하는 신규 블록을 수신한 주변 노드들은 hash 값과 merkle root 값 확인을 비롯한 블록의 유효성 검증을 수행하고 기존 블록에 연결하여 체인을 구성한다. 만약 인접한 두 곳의 노드에서 동시에 신규 블록을 배포할 경우 블록을 수신하는 노드들마다 먼저 수신하는 블록이 다를 것이다. 대표적인 합의 알고리즘인 PoW(Proof of Work)는 이와 같은 상황에서 분기를 허용하여 일시적으로 두 갈래로 나뉘는 체인의 형상을 하게 된다. 이어서 수신되는 블록들을 연결하여 최종적으로는 노드의 길이가 긴 체인을 유효한 체인으로 유지함으로써 모든 노드들이 동일한 블록으로 구성된 단일 체인을 유지하게 된다. 지분을 기반으로 합의를 수행하는 PoS(Proof of Stake)도 PoW와 동일하게 분기를 허용한다. 이와 달리 허가형 블록체인 플랫폼에서 사용되는 PBFT(Practical Byzantine Fault Tolerance) 계열의 합의 알고리즘은 분기가 발생하지 않는 매커니즘으로 동작하며 PoW와 달리 리더로 지정해놓은 특정 노드에서 합의 매커니즘을 시작하게 된다. PoW, PoS, PBFT 알고리즘 별 특징을 살펴보면 표 2와 같다.

Table 2. Comparison of consensus algorithms

Algorithm	Details
PoW	• Competitive agreement by computing power • Using SHA-256 hash function • Hashing values to find specific patterned value • Offers incentives - incentive for block creation - transaction fee
PoS	• Using stake ratio rather than computing power • Determined by the participant's stake and the date on which the stake was created • Assuming that participants with large stakes will not engage in malicious behavior • Offers incentives like PoW
PBFT	• Using in permissioned blockchain • No incentive is required • Permitted users are allowed in network • Primary node starts consensus algorithm

1.5 Smart contract

스마트 컨트랙트는 특정 조건을 만족 할 경우 작성해놓은 코드가 자동적으로 실행되는 이벤트를 기반으로 수행되는 프로그램이라고 할 수 있다. 스마트 컨트랙트의 개념은 닉사보(Nick Szabo)가 1994년 처음 제시한 것으로 블록체인 상에서는 이더리움을 시작으로 활성화 되었다[9].

블록체인 상에서 스마트 컨트랙트는 디지털 계약서로 많이 사용이 되고 있다. 블록체인과 스마트 컨트랙트 기반의 스마트 계약 내에서 조건이 만족 할 경우 거래가 자동으로 성립되고 이를 통해 중간 거래자에 의한 비용 증가, 사기의 위험성, 계약서 위조와 같은 위험을 낮출 수 있다.

전술 통신 환경에서는 특정 정보나 기능을 요청하는 사용자의 정보를 확인하여 수락 또는 거절하는 방식의 권한 제어 용도로 사용 할 수 있을 것이다.

2. Study trend

미국은 군에서도 전술 측면 뿐 아니라 시스템 개선 등을 위한 기술로 블록체인에 대한 연구를 다양하게 진행하고 있다. 미국방부에서는 작전 부대와 본부 간 통신의 신뢰도를 높이고 보안이 향상된 메시징 서비스 구축을 위한 방안으로 DARPA와 ITAMCO사가 2017년 블록체인 기반의 메시징 서비스 구축 방안 연구 및 개발을 시작했다. 3단계로 시작된 프로젝트는 2018년 9월까지 계획된 1단계에서 메시징 앱 기반의 사이버보안 아키텍처를 개발하고, 2단계에서 프로토타입의 어플리케이션을 개발, 마지막 3단계에서 플랫폼을 완성하여 사용 가능한 버전을 출시하는 것을 목표로 하고 있다[10].

미국 방위산업체인 록히드마틴의 경우 개발 프로세스의 모든 단계를 추적하고 해킹으로 인한 개발 SW의 변경을 예방하기 위한 방안으로 블록체인 기반의 트래킹 시스템을 구축 중이다[11]. 블록체인에 프로세스 단계 별 이력을 기록할 경우 순차적으로 기록되는 블록체인 특성 상 이력 추적이 가능하고 해킹으로 인한 위변조의 위험을 줄일 수 있기 때문이다.

미국 해군 사령부에서는 항공기 부품 추적을 위한 시스템 구성에 블록체인 기술 활용 방안을 검토 중인 상태이다. 블록체인 플랫폼으로는 SIMBA를 계획 중으로 알려졌다. SIMBA는 ITAMCO와 DARPA가 함께 개발한 블록체인 서비스 플랫폼으로 허가형 방식인 프라이빗 블록체인이며 성능과 컴퓨팅 파워 측면에서 효율성이 좋은 합의 메커니즘을 적용 할 것으로 알려진 상태이다[12].

러시아도 군사 기술 진흥원(The nation's military technology accelerator)에서 블록체인 기술이 사이버 공격을 식별하고 핵심 인프라를 보호하는데 사용될 수 있는지 검토 및 연구를 위한 특수과학 실험실(Special scientific lab)을 출범준비 중이며, 우리나라는 국방부에서 국방과학연구소를 통해 블록체인 기술 도입 방안을 검토 중인 상태이다[13-14].

III. The Proposed Scheme

국방 분야에서는 블록체인 기술에 대해 다양한 연구를 진행하고 있는 미국의 경우도 아직은 활용 방안 연구와 기초 개발 중일 정도로 블록체인 기술의 적용률은 매우 낮은 상태이다. 전술 환경은 민간 산업 분야와 비교하여 기술 적용 시 고려해야 할 사항이 많고 블록체인 플랫폼을 운영 할 인프라와 네트워크 참여자도 제한적이며 제약이 많다.

군 전술통신 환경은 이와 같은 많은 제약이 존재하지만 블록체인 네트워크와 분산 구조, 탈중앙화, 데이터 무결성의 필요 등 여러 측면에서 유사한 특징을 가지고 있기 때문에 활용 방안에 대해서 연구하게 되었다.

군 전술통신 환경을 구성하는 통신 노드는 노드 별로 네트워크를 구성하고 연결 할 수 있는 시스템이 구성되어 있는데, 이런 기능을 갖춘 통신 노드를 블록체인 네트워크의 노드로 구성할 경우 다양한 방법으로 블록체인 기술 활용이 가능 할 것이다.

본 논문에서는 그림 5와 같이 통신 노드를 블록체인 노드로 구성하는 상황을 가정하여 군 전술 환경에 적용 할 수 있는 방안에 대해 제시하고자 한다.

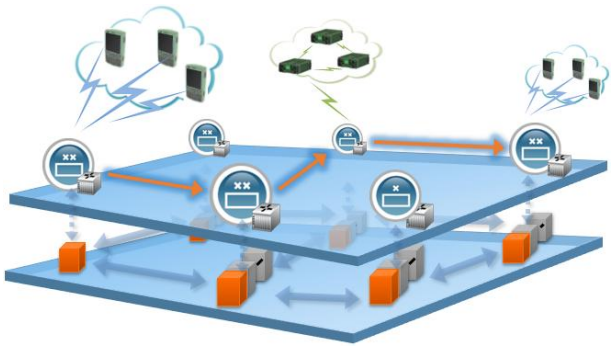

Fig. 5. Blockchain on tactical communication system

1. Authentication

IP 기반의 전술통신 환경에서 네트워크를 구성하는 노드의 연결성은 네트워크 구축과 통신 품질 확보에 있어서 매우 중요하다. 이런 이유로 노드 연결의 보안 강화를 위한 네트워크 가입 및 연동 방안에 대한 연구의 필요성이 제기되었고 학술적으로 다양하게 진행되고 있는 상태이다[15-17].

현재의 노드 간 연결과 노드와 단말 간 연결은 노드 별로 저장 중인 정보를 토대로 상호 인증을 수행하는 방식이며 민간 분야와 다르게 인증서 등 각 노드를 인증 할 수 있는 인증 데이터는 부재한 상태이다.

블록체인 플랫폼에서는 PKI 기반의 전자 서명을 통해 노드 간 초기 가입 및 연동 절차에서 인증 정보로 사용하고 인증을 위한 노드 정보 암복호화에도 활용 할 수 있을 것이다. 이 기능은 노드와 단말 간의 인증에도 동일하게 적용이 가능하며, 추가적으로 단말 인증을 위한 암호화된 정보를 노드 간 공유하여 단말의 통신 노드 간 이동성을 보장 할 수 있고 해킹을 통한 기존 단말의 정보 변경 및 네트워크 내 악의적 단말의 추가도 차단 할 수 있을 것이다.

2. Integrity

앞서 언급한바와 같이 무인체계가 증가 할 것으로 보이는 미래 전장 환경에서는 임무 정보 보안의 중요성은 더욱 커질 것이다. 임무 정보는 무인체계를 동작 시키는 정보인데 정상적인 방법으로 전달된다면 배포 과정에서 해킹으로 인해 데이터가 위변조 되어도 변경 유무 파악이 어렵고 무인체계 특성 상 위험을 초래 할 수 있기 때문이다. 임무 정보는 권한을 소유한 제한된 인원에 의해서만 관리 및 배포가 되어야 하며 해당 임무를 수신하는 무인체계로서는 권한을 소유한 인원이 배포한 임무인지 확인 절차가 필요 할 것이다. 이는 전자 서명을 통한 소유권 증명과 데이터 유효성 검증을 통한 무결성 보장이 가능하다면 데이터 위변조에 대한 위험성은 크게 줄일 수 있을 것이다.

3. Record management

전술 명령은 현재의 지휘통제 체계에서 매우 중요한 정보이고, 그 중요성은 더욱 커질 것이다. 하지만 정보의 중요성에 비해 배포 경로, 배포자, 배포시점 등 정보 전달 과정의 확인은 어려움이 많은 상태이다. 블록체인을 적용하면 명령 배포시점에 관련 정보를 블록 형태로 저장하고 체인에 연결하여 기록 관리가 가능 할 것이다. 이는 곧 명령 체계의 정확성을 높이고 부인방지도 가능 할 것으로 판단된다.

4. Authority control

보안이 중요한 군 특성 상 직급과 임무에 따라 단말을 이용한 네트워크상의 정보 접근과 특정 기능의 사용 권한을 제한해야 할 필요성이 존재한다. 스마트 컨트랙트의 특정 조건이 만족할 경우 계약 내용이 동작하는 특성을 이용하여 권한 제어가 가능하다. 정보 접근자의 인증 정보를 스마트 컨트랙트의 조건과 비교하여 만족 할 경우 정보 접근에 필요한 키 정보를 제공하고 조건을 만족하지 못할 경우 접근 거부를 할 수 있을 것이다. 이 방식은 정보의 접근뿐만 아니라 노드 간 연결 시에도 사용 가능 할 것이다. 통신 노드의 해킹 또는 탈취와 같은 이유로 전술 통신 네트워크에 연결 제한이 필요한 경우, 해당 노드 정보를 블록체인에 기록하고 노드 연결 과정에서 블록체인을 확인하여 노드의 권한을 제한하고 연결을 차단하는 것이 가능 할 것이다.

IV. Conclusions

블록체인 기술은 인공지능, IoT 등과 함께 산업 파급력이 클 것으로 예상되는 기술로 꼽히고 있다. 하지만 금융권을 제외하고는 아직까지 활용 분야가 제한적이고 기술 보급이 더딘 실정이다.

금융 및 일반 산업 분야에서 기술 발전이 진행된 블록체인 기술이 널리 확산되지 않은 상태에서 전술 통신 환경을 비롯한 국방 분야에 적용하기 위해서는 활용 방안 검토와 연구 개발이 많이 필요할 것으로 보여진다. 3장에서 제시한 활용 분야도 실제 전술 통신망에 적용하기 위해서는 추가적으로 많은 연구 및 개발이 필요한 상태이다. 전술 통신 환경의 특징을 반영한 합의 알고리즘에 대한 연구, 인증 및 데이터 암복호화를 위한 암호키 관리에 대한 연구, 그리고 지속적으로 증가할 블록체인 상의 데이터 관리에 대한 연구도 필요 할 것이다.

미국을 시작으로 국방 분야에서 블록체인 기술을 활용하기 위하여 활용 방안과 기술 적용성에 관한 연구가 증가하고 있고, 우리나라도 국방부에서 블록체인 기술 도입 방안 검토를 진행 중인 만큼 앞으로 블록체인 기술의 도입 증가와 발전이 기대된다.

REFERENCES

[1] H. D. Kim and T. B. Choi, "Trends of tactical data link technologies standardization," The Journal of The Korean Institute of Communication Sciences, Vol. 24, No. 10, pp. 7-14, Oct. 2007.

[2] Bitcoin : A Peer-to-Peer Electronic Cash System, *https://bitcoin.org/bitcoin.pdf*

[3] Ki Jin Jang, "The A Study on Innovative Financial Services of Business Models Using BlockChain Technology," The e-Business Studies, Vol. 18, No. 6, pp. 113-130, Dec. 2017.

[4] SamsungSDS, Application of Blockchain technology to shipping logistics, *http://www.zdnet.co.kr/news/ news_view.asp?artice_id=20180223184928*

[5] Youn-a Min and Yeong-Tae Baek, "A Study on the Application of Block Chain Ethereum Technology to Activate Digital Contents Trading as Sharing economy-data encryption and modify merkle tree," Journal of the Korea Society of Computer and Information, Vol. 23, No. 10, pp. 73-80, Sep. 2018.

[6] Byeong-ju Park, Tae-jin Lee and Jin Kwak, "Blockchain-Based IoT Device Authentication Scheme," Journal of the Korea Institute of Information Security & Cryptology, Vol. 27, No. 2, pp. 343~351, Apr. 2017.

[7] Seungjin Han, "A Secure Decentralized Storage Scheme of Private Information in Blockchain Environments," Journal of the Korea Society of Computer and Information, Vol. 23, No. 1, pp. 111-116, Jan. 2018.

[8] DLT, https://en.wikipedia.org/wiki/Distributed_ledger

[9] Smart contract, *https://en.wikipedia.org/wiki/ Smart_contract*

[10] Secure Messaging, *https://www.prnewswire.com/news-releases/itamco-to-develop-blockchain-based-secure-messaging-app-for-us-military-300464063.html*

[11] Lockheed Martin Contracts Guardtime Federal For Innovative Cyber Technology, *https://news.lockheedmartin.com/2017-04-27-Lockheed-Martin-Contracts-Guardtime-Federal-for-Innovative-Cyber-Technology*

[12] U.S Navy, applying blockchain technology, *https://www.coindeskkorea.com/usnavypartstracking/*

[13] Russia's Minbistry of National Defense prepares to launch 'Blockchain Institute', *https://www.coindeskkorea.com/%EB%9F%AC%EC%8B%9C%EC%95%84-%EA%B5%AD%EB%B0%A9%EB%B6%80-%EB%B8%94%EB%A1%9D%EC%B2%B4%EC%9D%B8-%EC%97%B0%EA%B5%AC%EC%86%8C-%EC%B6%9C%EB%B2%94-%EC%A4%80%EB%B9%84/*

[14] Korea's Ministry of National Defense, interoduction of blockchain, *http://www.thebchain.co.kr/news/ articleView.html?idxno=1729*

[15] Yu-Jin Son, Byoung-Gu Bae, Taeshik Shon, Young-Bae Ko, Kwang Jae Lim and Mi-Young Yun, "Mutual Authentication Method between Wireless Mesh Enabled MSAPs in the Next-generation TICN," The Journal of Korean Institute of Communications and Information Sciences, Vol. 37, No. 5, pp. 385-394, May. 2012.

[16] Kwangho Ahn, Juhyung Lee, Joonyoung Cho and Hyukjun Oh, "A Node Management Scheme in Tactical Data Link Network," The Journal of The Korean Institute of Communication Sciences, Vol. 36, No. 5, pp. 385-390, Apr. 2011.

[17] Byoung-Gu Bae, Sun-Joong Yoon and Young-Bae Ko, "A Hybrid Authentication Scheme for Wireless MSAP Mesh Networks in the Next-Generation TMCS," The Journal of The Korean Institute of Communication Sciences, Vol. 37, No. 11, pp. 1011-1019, Nov. 2012.

Authors

In-Deok Yoo received the B.S. degree in Computer Science and Engineering from Kangwon National University, Korea, in 2010. He is currently an engineer at Hanwha Systems and is interested in blockchain, deep learning and data links.

Woo-Sin Lee received the B.S., M.S. and Ph.D. degrees in Computer Engineering from Kwangwoon University, Korea, in 2001, 2003 and 2007, respectively. Dr. Lee is currently a chief engineer in Hanwha Systems. He is interested in data links, tactical networks.

Hack-Joon Kim received the B.S. degree in Computer Engineering from Hongik University, Korea, in 2004. He is currently a senior engineer in Hanwha systems and also a M.S. graduate student in Defense Fusion Engineering, Yonsei University, Korea. He is interested in Common/Tactical data links, UAS and machine learning.

So-Yeon Jin received the B.S. degree in Computer Engineering from Chonbuk National University, Korea, in 2003. So Yeon Jin is currently a senior engineer in Hanwha systems. She is interested in data links, machine learning, military communications, unmanned systems.

Se-Hyeon Jo received the B.S. degree in Computer Science and Engineering from Hanyang University, Korea, in 2010. In 2010, he joined Hanwha Systems Co., Republic of Korea, and he is currently an engineer. He is interested in data links and deep learning.