Journal of the Korea Academia-Industrial cooperation Society
Vol. 22, No. 7 pp. 306-312, 2021

https://doi.org/10.5762/KAIS.2021.22.7.306
ISSN 1975-4701 / eISSN 2288-4688

# 블록체인 기술을 활용한 정비장비 보안기능 향상 방안

**변종민**
**한화시스템 시험장비팀**

# Improvement of Maintenance Equipment Security by Using BlackChain

Jong-Min Byeon
ATE Team, Hanwha Systems

**요 약** 현재 세계는 4차 산업혁명을 겪고 있으며, 일부 기술들은 이미 상용화가 되어 우리 삶에 녹아들어 있는 상황이다. 4차 산업의 핵심 기술로는 AI, 무인자율주행, 전기자동차 그리고 블록체인 등이 있다. 여기서 앞서 설명한 기술은 앞선 보안성이 바탕이 되어야 하기에, 보안의 중요성은 나날이 높아지고 있다. 본 논문에서는 4차 산업혁명 기술 중 하나인 블록체인 기술을 정비장비에 적용하여 정비장비의 보안기능을 향상할 수 있는 방안에 대해 다룬다. 블록체인을 구성하는 블록 구조, SHA256 알고리즘, 개인키, 공개키의 특성을 정비장비에 접목시켜 정비장비의 보안기능을 향상할 수 있으며, 나아가 육군, 해군, 공군에서 사용되는 전투 시스템에도 적용 가능 여부를 논의한다. 그리고 해당 기술을 사용함으로서 발생할 수 있는 문제에 대한 대처 방안을 논의한다. 본 논문은 비트코인의 블록 구조를 기반으로 설명하였으며, 앞으로 블록체인 기술이 방위산업에 적용되면 어떠한 효과를 가질 수 있는지에 대해서 기술한다.

**Abstract** Currently, the world is undergoing the 4th industrial revolution, and some technologies have already been commercialized. The core technologies of the 4th industrial revolution include AI, autonomous driving, electric vehicles, and BlockChain. Because these technologies described above need to be based on high security, the importance of security is increasing steadily. This paper reports a plan to improve the security function of maintenance equipment by applying BlockChain technology, part of the 4th industrial revolution, to maintenance equipment. The security function of the maintenance equipment can be improved by incorporating the characteristics of the block structure, SHA256 algorithm, private key, and public key constituting the BlockChain into the maintenance equipment. Furthermore, this paper discussed whether it can be applied to combat systems used in the army, navy, and air force. This is followed by a discussion of ways to cope with problems that may arise from using this technology. This paper is explained based on the Bitcoin block structure and describes what effect BlockChain technology can have if it is applied to the defense industry in the future.

**Keywords :** Block Chain, 4th Industry, Bitcoin, Test Equipment, Network Security

*Corresponding Author : Jong-Min Byeon(Hanwha Systems)
email: jm1502.byeon@hanwha.com
Received April 5, 2021 Revised April 29, 2021
Accepted July 2, 2021 Published July 31, 2021

# 1. 서론

4차 산업혁명의 핵심 기술로는 빅데이터, AI, 자율주행 등 여러 기술이 있다. 그 중, 블록체인은 화폐로만 사용되었으나, 현재 민수분야에서 금융, 물류, 에너지, 헬스케어, 데이터 인증 등 다양한 분야에서 사용되고 있다[1]. 방위산업 분야에선 블록체인을 국방 사물인터넷 분야(IoT) 플랫폼 적용에 대한 논의가 이루어지고 있으며[2], 블록체인에 기반한 네트워크 인증 기법에 관한 연구가 이뤄짐을 확인할 수 있다[3]. 본 논문에서는 블록체인 기술을 정비장비에 적용하는 방안에 대해 제시하고, 해당 기술 적용을 함으로써 발생할 수 있는 문제점에 대한 해결책을 제시한다.

본 논문은 서론에서 언급한 블록체인 기술을 2.1절에서 설명한다. 블록의 구조, 유효성을 검증하는데 사용되는 SHA256 알고리즘, 기술 적용 사례 등에 대해 설명한다. 2.2절에선 앞서 설명했던 내용을 정비장비에 적용하는 방안에 대해 설명하며, 추가로 기대효과에 대해 기술한다.

# 2. 본론

## 2.1 블록체인

### 2.1.1 블록체인 기술 정의

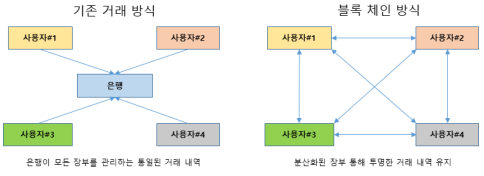


Fig. 1. Explanation of block chain

블록체인은 데이터 분산 처리 기술로서, 네트워크에 참여하는 모든 사용자가 모든 거래 내역 등의 데이터를 분산, 저장하는 기술을 말한다. 블록들을 체인 형태로 묶인 형태이기에 블록체인이라고 한다. 이런 블록들은 형성된 후 시간에 흐름에 따라 순차적으로 연결된 체인 구조를 가지게 된다. 모든 사용자가 거래내역(트랜잭션)을 보유하고 있어 거래 내역을 확인할 때는 모든 사용자가 보유한 장부를 대조하고 확인을 한다. 이런 기술을 갖고 있는 블록체인은 분산되고, 독립적이며, 공통 장비 관리 기술이라고 할 수 있다.

### 2.1.2 블록 구조

블록체인 기술을 구성하는 각각의 블록 구성요소는 다음 Fig. 2와 같다.

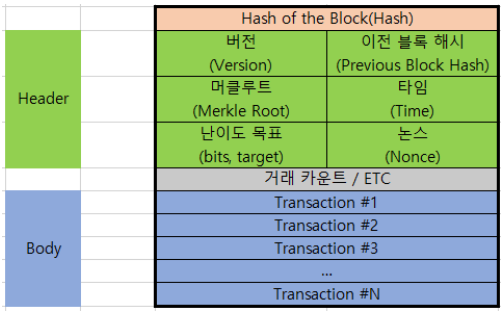


Fig. 2. Structure of block

맨 위의 블록에 블록 해시가 붙고 밑으로 Header와 Body가 붙어 하나의 블록을 이룬다. Header 부분에는 버전, 이전 블록 해시, 머클루트, 타임, 난이도, 목표, Nonce로 되어 있으며, Body 부분은 거래내역(트랜잭션)으로 되어 있다[4].

Fig. 3. Linkage structure with former block hash

각 요소에 대한 설명은 다음과 같다.

가. 블록 해시 : 블록의 식별자 역할을 하며, 버전과 이전 블록 해시, 머클루트, 타임, 난이도, 목표, Nonce를 연결한 후 SHA256 알고리즘으로 변환한 결과

나. 버전 : 현재 이 블록 헤더를 만든 비트코인 프로그램의 버전 정보

다. 이전 블록 해시 : 이전 블록의 주소 값을 가리키는 요소

라. 머클루트 : 블록의 Body 부분에 저장된 트랜잭션들의 해시 트리. 머클루트 값을 통해 거래내역(Transaction) 및 블록의 무결성을 검증할 수 있다.

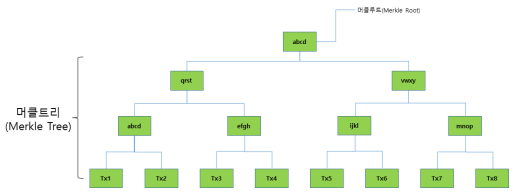


Fig. 4. Relationship with merkle root and merkle tree

마. 타임 : 해당 블록의 생성 시간

바. 난이도(target) : 난이도 해시 목표 값. 해당 값에 따라 채굴 난이도가 변경된다. 난이도가 높을 경우, 트랜잭션 속도가 느려지며, 새로운 블록 생성 시간이 느려진다. 반면, 난이도가 낮을 경우, 트랜잭션 속도가 빨라지며, 새로운 블록 생성시간이 빨라진다.

사. Nonce : 블록을 만드는 과정에서 해시 값을 구할 때 사용. 채굴자가 블록을 생성시에 Nonce값과 Nonce값을 제외한 값을 조합하여 SHA256 알고리즘을 통해 블록을 생성할 수 있게 된다. 0부터 시작하며 순차적으로 하나씩 값을 올려가며 채굴. “https://blockchain.info/ko” 사이트를 참고하면 특정 블록의 정보를 알 수 있다.

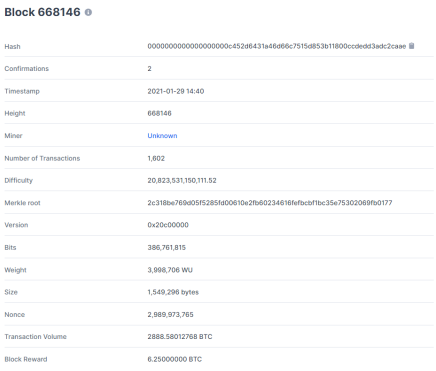


Fig. 5. Block information

Fig. 5. 블록 정보를 참고하면 668146번째의 블록의 해시 값을 시작으로 머클루트, Nonce, 버전, Block Reward 등의 해당 블록 정보를 알 수 있다.

### 2.1.3 SHA256 알고리즘

SHA256은 해시 함수의 일종이며, 출력된 값으로 입력된 값을 알 수가 없다. 간단한 함수로 y = x + 1 과 같은 식이 있다고 하자. 이 함수의 경우, y를 알면 x를 알 수 있고, x를 알면 y 값을 알 수 있다. 하지만 해시 함수의 경우 x값을 입력하여 y값을 알 수 있지만, y값을 안다고 해서 x값을 알 수가 없다. 덧붙여 SHA256 알고리즘은 문자나 숫자가 하나만 바뀌어도 완전히 다른 값이 나오므로 결과 값을 바탕으로 입력 값 유추가 불가능하다.

“http://convertstring.com/ko/Hash/SHA256” 사이트에서 “SHA256 알고리즘” 문자열을 입력 후 해당 값을 해시 값으로 변환하면 다음의 결과가 나옴을 알 수 있다.


Fig. 6. Input “SHA256 알고리즘”


Fig. 7. Changed value by hash algorithm

여기에서 .(dot) 하나만 마지막으로 추가를 하면 다음의 결과가 나옴을 알 수가 있다.

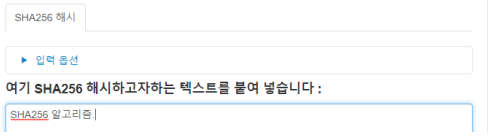


Fig. 8. Add “.”(dot)


Fig. 9. Changed value by hash algorithm

Fig. 7과 9를 비교해보면 문자 하나의 추가로 인해 완전히 다른 해시 값을 생성한다는 것을 알 수가 있다. 추가로 문자를 하나만 변경해도 유추할 수 없는 결과 값이 만들어짐을 알 수 있다.

### 2.1.4 노드

블록체인의 노드는 풀 노드와 라이트 노드로 구분된다. 풀 노드는 모든 블록의 정보를 수집하고, 저장하는 역할을 수행하며, 새로운 블록을 추가하기 위해 전달받은 블록에 대한 검증을 수행한다. 라이트 노드는 모든 블록 정보의 원본을 갖고 있지는 않지만 헤더 정보만 갖고 있다. 모든 블록 정보를 갖고 있지 않기에, 개별 거래에 대

한 트랜잭션을 확인하기 위해 풀 노드에 블록 정보를 요청하여 이 거래가 검증된 거래인지를 확인한다.

#### 2.1.5 적용 사례

블록체인 기술의 적용 사례로는 금융 산업의 송금 시스템 - Ripple, 데이터 인증 분야 - NFT(Non Fungible Token), 소셜 네트워크 - Steemit 등이 있다. 그 외에도 공공 서비스, 물류, 유통 분야 등에서도 관련 기술이 적용되어있다. 관련 내용은 아래의 Table 1을 참고한다.

Table 1. Applicaiton Example

| Industry | Finance | Data | SNS |
|---|---|---|---|
| Case | Ripple | NFT | Steemit |
| Purpose | Remittance | Verification | Reward |

### 2.2 정비장비 적용 방안

#### 2.2.1 현황 및 문제점

정비장비는 전투체계에 들어가는 구성품을 장치단, 보드단으로 점검을 수행하는 장비이며, 점검을 통해 고장난 품목을 수리 또는 교환하여 군 운용성을 향상시킨다. 형태로는 데스크 형태와 노트북 형태가 있다. 현재 PXIe 타입[5]의 계측기의 발전으로 인해 데스크 형태에서 노트북 방식에 경량화된 PXIe 타입의 계측기가 추가되어 개발되는 추세이다. 육군사업의 경우 차륜형 대공포, 해군사업의 경우 FFX-III 사업에 적용되어 개발되고 있으며, 앞으로는 데스크 형태보단 경량화된 휴대형 정비장비로 개발 및 양산 되는 추세이다.

Fig. 10. PXIe type

Fig. 11. Desk type – FFX-II FTE

Fig. 12. Light notebook type – KDX-I PIP STE

이러한 현재 운용 환경은 해커의 목표물이 되어 문제를 일으킬 위험이 있다. 그 이유로는 단순히 계정과 비밀번호, 사내 보안프로그램만 해킹하면 되기에 바이러스 감염에 취약한 구조다. 바이러스에 감염된다면, 정비장비 운용에 문제를 불러올 것이며, 나아가 해당 장비로 정비 대상품을 점검한다면, 바이러스가 정비 대상품에 침투하여 점검대상품의 오작동 및 기밀 자료 유출을 초래할 수 있다.

#### 2.2.2 블록체인 구조를 적용한 개선

제안하는 운용 환경 구성은 아래의 3가지 가정을 기반으로 한다.

(1) 폐쇄적인 네트워크의 구성
(2) 초기 네트워크는 신뢰할 수 있고 블록 저장
(3) 프라이빗 블록체인 적용[6]

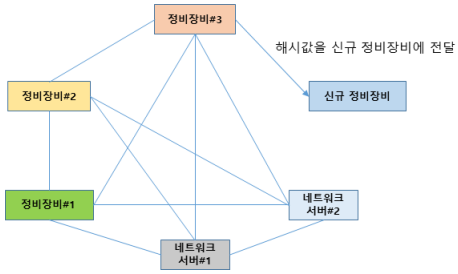


Fig. 13. Delivery the last block hash value to new maintenance equipment

가. Fig. 13를 참고하면, 새로운 장비가 추가되었을 시, 신규 장비가 온라인(인트라넷)상에 연결되어 가장 최근에 추가되었던 블록의 이전 해시 값 받음.
나. 전 해시 값을 신규 장비가 받은 후, 이전 해시 값과 운용자 정보, H/W 성능 변수들을 조합하여 새로운 해시 값을 생성한 후 생성된 해시 값을 바탕으로 새로운 블록을 생성.
다. 새로운 블록이 모든 노드에 전파되며, 신규 블록에 대한 신뢰성 검증 작업을 실시.

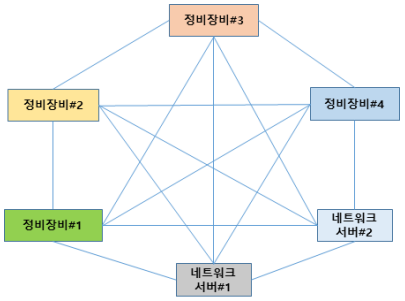


Fig. 14. Block chain bond

라. 신뢰성 검증 작업이 완료되면, 모든 블록의 거래 기록에 해당 신규 장비에 대한 정보(운용자 정보, H/W 성능)가 기록된다.

마. 노드들이 그물 형태를 이루며, 외부의 공격으로부터 안전한 시스템을 갖게 된다.

비트코인 기준으로 모든 블록에 대한 정보는 대략 150GB의 용량을 갖는다. 전투체계 시스템의 경우 항시 동작하는 환경을 고려한다면, 네트워크 서버는 풀 노드로 동작하고, 정비장비는 라이트 노드로 동작한다면 안정적인 동작 환경 구성이 가능함을 예상할 수 있다.

### 2.2.3 SHA256 알고리즘 활용

만약 누군가가 의도적으로 블록체인 시스템을 해킹해서 내부의 정보들을 알아내려 한다고 가정해보자. 먼저 해커가 블록체인 시스템의 네트워트에 연결되어 노드의 일부가 되어야 한다. 해당 노드는 이전 블록의 해시 값을 이용하여 이전 블록의 정보를 알아내려 하지만, 해당 해시 값은 SHA256 알고리즘으로 인해 암호화되어 있으므로 역으로 본래의 정보를 찾아내기란 불가능하다. 설령 해당 정보를 찾아냈다고 하더라고 상당한 노력과 시간이 걸릴 것이며, 해당 블록 하나만 찾는다고 해도 모든 블록이 체인 형태를 이루고 있기에 전체 시스템을 해킹하기엔 불가능에 가깝다.

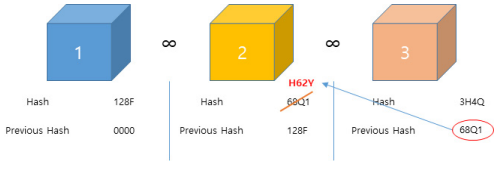


Fig. 15. Discordance of hash value

추가로 해당 블록을 해킹하여 블록의 데이터를 조작한다고 해도 블록체인 기술은 분산원장을 갖기 때문에 데이터의 위변조가 불가함을 알 수 있다.

### 2.2.4 개인키, 공개키 활용

사용자 계정을 개인키, 공개키를 알고리즘을 사용한다면 해킹으로부터 안전하다. 공개키로 암호화된 사용자 계정은 개인키로만 복호화가 될 수 있으며, 개인키로 암호화된 계정은 공개키로만 복호화 할 수 있다. 암호화 및 복호화 원리는 Fig. 16을 참고한다.

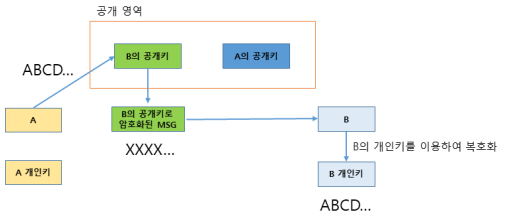


Fig. 16. Encoding and decoding by using public and private key

공개영역의 A, B의 공개키는 누구나 알 수 있는 키다. 먼저 A는 누구나 알 수 있는 B의 공개키를 이용하여 “ABCD...”라는 계정을 암호화한다. SHA256 알고리즘으로 변환된 메시지(“XXXX...”)는 B에게 전달된다. B는 자신만 알고 있는 B의 개인키를 사용하여 A가 보낸 계정을 확인한다. 그 반대의 경우엔 B가 A의 공개키를 이용하여 계정을 암호화한 후 A에게 보낸다. A는 전과 동일하게 A 자신만 알고 있는 A의 개인키를 이용하여 수신한 계정을 복호화한다. 해당 알고리즘으로 공개키, 개인키를 이용한 계정 암호화, 복호화를 통해 계정의 기밀성이 보장되며, 해당 알고리즘을 사용한다면 인증된 계정을 통해 장비를 사용할 수 있다.

## 2.3 적용 비용 산정

블록체인 시스템을 유지하기 위한 데스크탑 PC 채굴기 1대당 운용비용을 예측해보자. 500W 의 소모전력을 가진다고 가정하고 한달동안 풀 노드로 동작하는 채굴기를 사용한다고 가정한다. 총 사용 전력은 해당 장비의 소비전력과 총 사용 시간의 곱이 되므로, 다음의 (1)식과 같다.

$$\textit{사용전력[kW]} = \textit{소비전력[kW]} * \textit{사용 시간} \quad (1)$$

위의 (1)식에 해당하는 값들을 대입하면 대략 360 kW가 소모됨을 알 수 있고, 해당 가격을 주택용 저압으

로 가정하여 계산한다면 대략 56,000원이 나옴을 알 수 있다. 산업용 전기요금으로 계산한다면 채굴기 1대당 운용 비용은 이보다 더 낮게 나올 것으로 예상된다. 풀 노드의 한 달간 채굴 요금을 감안하여 일부장비는 라이트 노드로 운용할 시, 이보다 요금이 적게 나올 수 있음을 예측할 수 있다. 만약 기술 구축 및 운용 비용이 현재 보안 시스템 구축 비용(대략 투자비용 30억원, 라이선스 및 유지보수 비용 5년간 20억원)보다 크더라도, 보안성 및 신뢰성을 고려한다면, 충분히 블록체인 기술을 적용하는 것이 미래를 위한 더 나은 대처 방안이 될 것이다.

### 2.4 발생 가능한 문제

예상 문제로는 2가지가 있다. 첫 번째는 신규 장비의 추가로 인해 풀 노드의 경우 데이터 저장 공간에는 한계가 올 것이고, 이는 정상적인 노드로의 동작 장애를 유발할 것이다. 이 문제를 해결하기 위해 엣지/클라우드 구조, 선별된 누드만 합의를 수행함으로써 확장성을 높이는 방안, 각 노드의 역할에 따라 글로벌 체인을 관리하는 방안을 사용하면 첫 번째 문제는 해결이 가능하다[7].

두 번째 문제점은 네트워크의 부하 문제가 있다. 장비 추가로 인한 인증 과정에서의 네트워크 부하를 줄이기 위해 Byzantine Fault Tolerance(BFT) 합의 과정에 Software Defined Networking(SDN)을 도입하여 네트워크 부하 문제를 완화하는 방법[8]을 사용하여 두 번째 문제를 해결한다.

### 2.5 기대 효과

오프라인상에서 동작하는 경우 해커의 단일 타켓이 되기 쉬운 반면, 인트라넷에서 블록체인 기술의 장점인 보안성을 이용하여 체인 형태를 이룬다면, 해커의 타켓이 되기 어렵다. 바이러스 감염 예방으로 인해 장비 운용에 차질이 없게 되므로 운용성 개선 효과를 누릴 수 있다. 덧붙여 기존 인트라넷을 위해 사용되던 서버를 채굴기로 이용한다면, 보안 시스템 구축 비용 또한 절감할 수 있다. 기존 정비장비와 3가지 측면에서 개선될 사항은 아래의 Table 2를 참고한다.

Table 2. Expectancy Effects Compared with Current System

| | Security | Operation | Cost |
|---|---|---|---|
| BlockChain System | Improvement | Improvement | Decrease |

## 3. 결론

본 논문에서 블록체인 기술의 개념을 설명하였고, 관련 기술을 정비장비에 적용 시, 어떤 이점이 있을지 확인하였다. 2.1절은 블록체인 기술의 세부 요소 및 동작 원리에 대해 알아보았고, 2.2절은 블록체인 기술을 정비장비에 적용했을 경우에 어떤 부분이 개선될지 알아보았다.

본 논문에서 제안한 기술을 정비장비에 적용하게 된다면, SHA256 알고리즘, 개인키, 공개키의 활용으로 인한 강력한 보안성 향상과 거래내역(트랜잭션)의 분산화로 인한 장비 관리 비용에서 이점을 가질 것으로 판단된다. 반면, 네트워크에 전투 체계와 정비장비, 기타 장비가 연결되어야 하기에, 해당 부분에 대한 보안 규제[9,10]가 걸림돌이 될 것으로 생각된다. 앞서 설명했던 적용 사례를 참고하여 민수 분야에서 블록체인 기술이 충분히 검증된 이후, 관련 기술을 군수 제품에 점차 접목시킨다면, 보안성이 향상된 운용환경을 가질 수 있을 것이다. 더불어, 전투력 향상 및 제품 유지 보수 방면에서 많은 도움이 될 것으로 판단된다.

## References


[1] Shin-Ok Lee, Young-Hoon Park, “Application of Blockchain Technology in Industry: A Survey”, *Journal of The Institute of Electronics and Information Engineers*, Vol. 56, NO.12, pp. 1277~1285, Dec. 2019. DOI: https://doi.org/10.5573/ieie.2019.56.12.83

[2] Dong-Yeon Kim, Young-Hwa Sung, Su-Jae Park, Sung-Ho Kim, “Application of Blockchain to Military IoT Platforms”, *Korea Institute of Military Science and Technology*, Vol. 27, pp. 1540~1541, June. 2019.

[3] Jun-Ho Park, “A Network Authentication Scheme based on Blockchain Technique”, *Korea Institute of Military Science and Technology*, Vol. 25, pp. 1863~1864, June. 2018.

[4] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic. pp. 4~5, 2008.

[5] Hyeokjin - Kwon, “Implementation of PXIe platform based portable Automatic Test Equipment to improve reliability”, *Journal of The Korea Society of Computer and Information*, Vol. 22, NO. 7, pp. 9~16, July. 2017. DOI: https://doi.org/10.9708/jksci.2017.22.07.009

[6] Hun-Hee Lee, Jeong-Hoon Lee, Ki-Young Lee, “A Study on IoT Security Method Based on Blockchain”, *Journal of The Institute of Electronics and Information Engineers*, pp. 822~824, Nov. 2018.

[7] Min-Seo Yu, Dan-A Yang, In-Shil Doh, “Scalability

Improvement of Blockchain System", *Journal of The Institute of Electronics and Information Engineers*, pp. 2209~2212, Aug. 2020.

[8] Yong-Seok Kwon, "A study on scalability of the Blockchain in the Mobile Communication and Computing", *Journal of The Institute of Electronics and Information Engineers*, Republic of Korea, pp. 1485~1486, June. 2019.

[9] Don Tapscott, Alex Tapscott - Block Chain Revolution, USA, pp. 516~520, Jan. 2017.

[10] JungSub - Han, Bitcoin Imperialism, Republic of Korea, pp. 144~169, June. 2019.

변 종 민(Jong-Min Byeon) [정회원]

- 2015년 2월 : 한국해양대학교 전자통신공학과 (공학학사)
- 2015년 1월 ~ 현재 : 한화시스템 선임연구원

〈관심분야〉
무기체계, 자동화시험장비