박사학위청구논문

2022학년도

블록체인 활용 국방 정보체계 보안 강화 모델 연구

A Study of the Security Enhancement Model of Defense Information System Based on Blockchain

광운대학교 대학원

방위사업학과

박 용 탁

블록체인 활용 국방 정보체계 보안 강화 모델 연구

A Study of the Security Enhancement Model of Defense Information System Based on Blockchain

광운대학교 대학원

방위사업학과

박 용 탁

블록체인 활용 국방 정보체계 보안 강화 모델 연구

A Study of the Security Enhancement Model of Defense Information System Based on Blockchain

지도교수 김 도 영

이 논문을 공학 박사학위 청구논문으로 제출함.

2023년 6월 일

광운대학교 대학원

방위사업학과

박 용 탁

박용탁의 공학 박사학위논문을 인준함.

심사위원장 _____ (인)

심 사 위 원 _____ (인)

심 사 위 원 _____ (인)

심 사 위 원 _____ (인)

심 사 위 원 _____ (인)

광운대학교 대학원

2023년 6월 일

감사의 글

존경하는 김도영 교수님과 사랑하는 가족 그리고 제 연구에 도움을 주신 모든 분께 감사의 글을 올립니다.

2019년, 어찌 보면 공부하기에는 이미 늦은 35세의 나이에 박사과정을 시작해야겠다고 마음먹으며 깊은 고민에 빠졌던 기억이 납니다. 그렇게 학업에 정진하는 동안 4년이 흘러 저는 39세가 되었고, 감사하게도 더 늦지 않게 박사학위를 마치게 되었습니다. 지금 그때를 돌이켜 회상해보면 정말 시간이 빠르게 지난 것 같아 감회가 새롭습니다. 처음 박사과정을 시작할 때만 해도 내가 과연 이 과정을 끝낼 수 있을까 하는 의구심이 스스로 들 때도 있었고, 긴 시간 동안 일과 육아, 학업과 연구를 병행하며 많은 어려움이 있었지만, 지도 교수님과 사랑하는 가족의 끊임없는 지지와 격려 덕분에 이 모든 도전의 시간을 극복할 수 있었습니다.

특히, 본 연구를 진행하는 동안 주제 선정부터 테스트 모듈 개발, 실험 및 결과 검증까지 전 과정에 걸쳐 어려움에 봉착할 때마다 지도교수님의 학문적인 통찰력과 열정은 저에게 큰 영감을 주었으며, 연구 방향을 명확히 하고 발전시키는 일의 확고한 기준이 되었습니다. 또한, 교수님의 조언과 격려는 제가 좀 더 나은 연구를 하게 되는 바탕이 되었고 더 넓은 학문적 스펙트럼을 가지게 되는 기반이 되었습니다.

그리고 이 글을 통해, 사랑하는 가족들께도 깊은 감사의 말을 전하고 싶습니다. 제가 일과 학업을 병행하며 힘들어할 때 가족들은 항상 저를 응원하고 격려해주었습니다. 특히, 아내는 제가 몸과 마음이 지쳐 매우 예민해져 있을

때도 저에게 무한한 믿음을 주었고, 학업으로 인해 어쩔 수 없이 소홀해질 수 밖에 없었던 가정의 일과 육아를 홀로 짊어졌던 희생은 제가 이 모든 과정을 헤쳐 나아갈 수 있는 가장 큰 원동력이 되었습니다. 그리고 논문을 작성하는 동안 바쁘다는 핑계로 자주 함께해주지 못했던 우리 사랑하는 아들 박건하에게는 미안하다는 마음을 전달합니다. 아마, 이러한 가족들의 지지가 없었다면 오늘 제가 이 목표를 달성하기는 힘들지 않았을까 생각합니다.

이렇듯, 이 학위는 저의 노력뿐만 아니라 주변에서 저를 도와주신 모두가 함께 이룩한 결과이며, 지금 이 글 정도의 표현으로는 충분하지 않을 정도로 큰 의미를 지닙니다.

끝으로, 제 논문을 평가해주시고 더 나은 연구가 될 수 있도록 이끌어주신 정형원 교수님, 최진주 교수님, 백석철 박사님, 표상호 박사님 네 분 심사위원님께도 감사한 마음을 전달해 드립니다.

제가 이렇게 성장하며 학업을 마칠 수 있었던 공을 이 모든 분께 돌립니다. 감사합니다.

2023. 06.

박 용 탁 올림

국문 요약

블록체인 활용 국방 정보체계 보안 강화 모델 연구

4차 산업혁명은 인류의 삶을 디지털 사회에서 초연결 사회로 진화시켰고 클라우드(Cloud), 빅데이터(Big data), 사물 인터넷(IoT, Internet of Things), 인공지능(AI, Artificial Intelligence) 등으로 대표되는 신기술은 상호운용성을 바탕으로 급성장하여 국가의 기간 시스템을 구성하는 기반 기술로 활용되기에 이르렀다. 하지만, 주요 정보시스템 간 상호운용성 발달에는 그것을 노리는 공격 수법 또한 고도화되는 현상이 뒤따르게 되었고 최근까지도 국가와 조직에 막대한 손실을 일으키는 수준의 침해 사고가 지속해 발생하고 있다. 이에 따라, 각 분야의 보안 담당자들은 다양한 보완책을 세워 취약점에 대응하고 있지만 끊임없이 변화하는 수많은 유형의 공격 수법을 모두 방어한다는 것은 방어자 관점에서 막대한 자원의 소모를 감수해야만 하는, 한없이 불리한 싸움의 연속일 수밖에 없다.

이러한 현실은 대한민국 국방부도 마찬가지다. 국방 정보체계는 그동안 기밀성(Confidentiality), 가용성(Availability)에 막대한 투자를 하여 보안시스템을 구축하였고 그에 따른 성과를 이루었지만, 내부자 위협을 고려하지 않은 취약한 보안시스템으로 인해 최근까지도 국군 현역 장교가 합동지휘통제체계(KJCCS)의 자료 탈취를 시도하는 간첩행위 중 적발되는 등 관련사건이 끊임없이 발생하고 있다. 이러한 사례들은 아무리 보안이 튼튼하다 해도 보안 담당자, 관리자 등 내부자를 통한 사회공학적공격에는 기존 보안시스템은 무력

해진다는 것을 보여주고 있다.

따라서, 국방 정보보안시스템은 복잡한 미래 환경에 대응하기 위해 첨단기술을 활용한 변화가 꾸준히 요구되고 있으며, 이러한 시대적 요구사항을 관철하기 위한 여러 방안 중 허가형 블록체인(permissioned blockchain)의 비가역성과 신원인증 및 암호화 기술은 가장 합리적인 대안이 될 수 있다.

허가형 블록체인은 블록체인의 비가역적 특성은 그대로 유지하면서 공개키(Public Key Infrastructure)를 활용한 암호화와 멤버십 관리를 통한 참여자 접근 통제 기술로 인해 기존 시스템 대비 기밀성, 가용성, 무결성(Integrity)에서 모두 우수한 특성을 보인다. 또한, 타 블록체인과 같이 특정 보상을 통해 네트워크 참여를 유도하는 방식이 아닌 업무적으로 같은 목적을 가진 사용자들이 자발적으로 네트워크에 참여하는 구조로 엔터프라이즈 시스템 적용에 적합하다.

정보체계에 허가형 블록체인을 적용하기 위해서는 시스템의 특성을 고려해야 한다. 예를 들어, 복잡한 계산 및 통계 분석 업무에서는 기존 데이터베이스 시스템이 유리하며 데이터의 비가역성을 활용한 기준정보관리, 로깅, 물류, 전자계약 등의 업무에선 허가형 블록체인이 유리할 것이다.

본 연구에서는 앞서 제기된 문제점을 극복하는 방법으로 기존 정보체계 및 데이터베이스 시스템을 허가형 블록체인으로 대체하는 국방 블록체인 플랫폼 모델 연구를 통해 데이터 변조 및 탈취 등의 사이버 침해 사고를 원천적으로 대비하는 방안을 구체화하고 테스트 모듈 개발을 통한 실증으로 국방환경의 다양한 정보체계에 허가형 블록체인 플랫폼을 적용할 수 있음을 증명한다. 또한, 이를 시작으로 블록체인 기술의 국방적용에 관한 차기 연구가 지속되어 AI(Artificial Intelligence), 클라우드 기술과 융합(Convergence) 및 MongoDB,

Couchbase 등 성능, 보안, 가용성, 효율성 등에서 이미 많은 연구를 통해 검증된 DBMS(Database Management system) 기술의 블록체인 원장(World State DB) 적용을 통한 성능개선, 그리고 국방 블록체인 관련 법과 제도의 정비 등이 이루어진다면 허가형 블록체인 기술은 첨단화된 현재 국방 정보시스템 사이버안보 환경에서 가장 훌륭한 대안으로 자리매김할 수 있을 것으로 기대된다.

주제어: 허가형 블록체인, 국방 블록체인 플랫폼, 사이버안보

ABSTRACT

A Study of the Security Enhancement Model of Defense Information System Based on Blockchain

Yong Tak Park
Dept. of Defense Acquisition Program
The Graduate School
Kwangwoon University

The 4th industrial revolution has evolved human life from a digital society to a hyper-connected society, and has evolved into a Cloud, Big data, Internet of Things (IoT), and artificial intelligence (AI). The representative new technology has grown rapidly based on interoperability and has come to be used as a basic technology constituting the national core system. However, the development of interoperability between major information systems has also led to the advancement of attack methods aimed at it, and until recently, intrusion accidents that cause enormous losses to countries and organizations continue to occur. Accordingly, security personnel in each field are responding to vulnerabilities by establishing various supplementary measures, but defending all the ever-changing numerous types of attack methods is bound to be an

infinitely unfavorable series of fights that require enormous resource consumption from the defender's point of view.

The same is true of the Ministry of National Defense of the Republic of Korea. The defense information system has invested heavily in confidentiality and availability to establish a security system and has achieved results, but related incidents have been continuously occurring until recently, with active military officers attempting to steal data from the Korean Joint Command and Control System (KJCCS). These examples show that no matter how strong security is, the existing security system becomes powerless against social engineering attacks through insiders such as security officers and managers.

Therefore, the defense information security system is constantly required to change using advanced technology to cope with the complex future environment, and among the various measures to fulfill the requirements of the times, the irreversibility and identity authentication of the permissioned blockchain and encryption technology can be the most reasonable alternative.

The permissioned blockchain has superior confidentiality, availability, and integrity compared to existing systems due to encryption using Public Key Infrastructure and participant access control technology through membership management while maintaining the irreversible characteristics of the blockchain. In addition, it is suitable for the application of enterprise systems with a structure in which users with the same purpose voluntarily

participate in the network, rather than inducing network participation through specific rewards like other blockchains.

In order to apply a permissioned blockchain to an information system, the characteristics of the system must be considered. For example, the existing database system will be advantageous in complex calculation and statistical analysis tasks, and the permissioned blockchain will be advantageous in tasks such as reference information management, logging, logistics, and electronic contracts using data irreversibility.

This study demonstrates how to fundamentally prepare for cyber-infringement accidents such as data modulation and theft through research on a defense blockchain platform model that replaces existing information systems and database systems with permissioned blockchain. In addition, if the next research on the defense application of blockchain technology continues, the best performance of the DBMS (Database Management System) technology, such as AI (Artificial Intelligence), Cloud Technology, MongoDB, and Couchbase, will be approved.

Key words: Permissioned blockchain, defense blockchain platform, cyber security

차 례

그림 차례

표 차례

약어

<A>

<B>

<C>

<D>

<M>

<N>

<N>

<P>

<O>

<R>

<S>

<T>

<U>

<W>

제1장 서론

제1절 연구의 배경 및 필요성

1. 연구의 배경

4차 산업혁명은 인류의 삶을 디지털 사회에서 초연결 사회로 발전시켰고 클라우드, 빅데이터, 사물 인터넷, 인공지능 등으로 대표되는 신기술의 컨버전스 융합을 통해 수많은 시스템은 하나로 연결되어 국가의 핵심 시스템을 구성하는 기반 기술로 사용되기에 이르렀다. 하지만, 정보체계의 상호운용성이 높아질수록 그것을 노리는 공격 수법이 고도화되면서 조직에 막대한 손실을 입힐 수 있는 수준의 침해 사고가 지속해 발생하고 있다. 이에 따라, 각 분야에서 다양한 보완책을 세워 취약점에 대응하고 있지만 공격을 방어하는 처지에서는 침입자에 대응하여 막대한 자원 소모를 감수해야만 하는 끝없이 불리한 싸움의 연속일 수밖에 없다. 또한, 과거 해킹이 단순 정보 탈취에 그쳤다면, 현재에는 정보 위·변조를 통한 시스템 조작, 파괴의 가능성이 증가하는 등 새로운 형태의 위협도 증가하였다.

최근 민간에서는 위와 같은 사이버보안 취약점을 원천적으로 해결하는 방안으로 '분산 원장'으로 알려진 [1]블록체인 기술에 대한 논의가 한창이다. 최초의 블록체인 기술은 탈중앙화 전자화폐 '비트코인'을 구현하기 위해 사용되어 세계의 주목을 받았지만, 현재는 단순히 가상자산보다는 정보 위·변조 차단, 분

1) 블록체인: 안전하게 공유되는 분산된 데이터 원장

산화, 스마트 계약 구현 등 블록체인 기술을 활용한 다양한 엔터프라이즈 시스템에 관한 연구들도 주목받기 시작했다. 최근에는 민간과 해외 정부뿐만 아니라 우리 정부도 CBDC(Central Bank Digital Currency) 등 여러 방면에서 블록체인을 적용하려는 모의시험을 하고 있다. 따라서, 우리 군 역시 증가하는 사이버 위협으로부터 군 정보자산을 지키기 위해 블록체인이라는 첨단기술 기반으로 복잡한 미래 환경에 대응하기 위한 새로운 패러다임으로의 변화가 절실히 요구되고 있다.

2. 연구의 필요성

국방 정보체계는 국가 안보에 직결되는 주요 정보자산이며 이에 대한 보안 강화는 매우 중요한 숙제이다. 그러나 기존 국방 정보체계의 보안 방식은 암호화, 방화벽, 메가센터 구축 등 주로 기밀성과 가용성에만 치중하여 투자되었고 내부자 위협을 고려하지 않은 보안시스템으로 2022년 4월 28일 국군 현역 장교가 직접 합동지휘통제체계(KJCCS)의 자료 탈취에 가담하는 간첩행위를 하다 적발되는 등 관련사건이 끊임없이 발생하고 있다. 이러한 사례들은 기존 형태의 보안시스템이 아무리 튼튼하게 구축되어 있다고 해도 보안 담당자, 관리자 등 내부자를 통한 사회공학적공격에는 무력해진다는 것을 보여주고 있다. 따라서 중앙집중식의 기존 데이터베이스 시스템에서 탈피하여 이제는 블록체인을 활용한 분산 원장 기술로 데이터의 무결성(Integrity) 보장, 신뢰성(Reliability) 확보, 접근통제를 위한 새로운 보안 방식을 설계해야 한다.

하지만, 대한민국의 블록체인 군 적용에 관한 연구는 글로벌 군사 강국 대

비 상대적으로 소극적이다. 예를 들어, 미국은 2019년부터 DoD(Department of Defense) 차원의 '국방 디지털 현대화 전략'을 통해 사이버보안의 패러다임을 바꿀 수 있는 새로운 정보기술로 블록체인을 제시하였고 이미 블록체인을 활용하여 그들이 가지고 있는 주요 전략자산 및 네트워크의 보호를 위한 연구개발을 TOP-DOWN 형태로 진행 중이다. 그에 반해 대한민국은 2018년 국방과학연구소에서 작성한 '블록체인 기술의 군내 도입방안 연구'를 마지막으로 추가연구가 진행되고 있지 못하다. 그마저도, 지금까지의 사전 연구는 블록체인 기술 적용 필요성에 관한 논거, 블록체인 기술 도입을 위한 로드맵 제시 정도의 개념적 수준으로 연구되었고 실제 적용할 수 있는 모델 제안이나 프로토타입 개발 그리고 법제도 개선 등 보다 세부적이고 실증적인 연구는 없었다.

또한, 기술적인 관점에서도 기존의 연구들은 한계점이 분명하다. 기존의 연구들은 단순히 블록체인 1.0 개념에 머물러 차세대 블록체인의 핵심 가치인 스마트 컨트랙트, 접근통제, 책임추적, 부인방지 등 블록체인 2.0 이후 강조되는 기술에 관한 연구 및 활용은 미흡하였다. 그리고 어떠한 신기술을 도입하기 전에는 우리에게 그 기술이 왜 필요한가에 대한 원론적인 고민이 필요한데, 지금까지 대한민국 국방은 단순히 대외적 상황에 의해 신기술을 도입할 뿐 정작 해당 프로젝트에서 왜 블록체인이 필요하며 이 신기술이 어떤 문제를 해결하기 위한 대안이 될 수 있는가에 대한 심도 있는 고민이 없었다.

따라서, 본 연구를 기점으로 이제는 지금까지 언급된 선행연구와는 달라져야 한다. 실제 국방 정보체계 프로젝트에서 활용될 수 있도록 기술, 정책 등 여러 방면에서 상세한 실증연구가 필요하다. 이러한 연구가 지속되어야 블록체인 도입을 고려하는 국방 관련 차세대 프로젝트나 후속되는 국가 또는 국방부 차원의 대규모 차기 연구에 좋은 선례를 제공해줄 수 있을 것이다.

제2절 연구내용 및 범위

1. 연구내용

본 연구는 초연결 시대의 고도화된 국방정보체계를 비롯하여 급변하는 정보화 환경 전체를 관통하는 보안 이슈에 대한 시대적 요구사항을 관철하기 위해 허가형 블록체인(Permissioned Blockchain)을 국방 분야에 도입하여 국방정보체계의 보안성을 강화하는 데 그 목적이 있다. 또한, 국방 블록체인 플랫폼 모델을 제시하고 테스트 모듈을 개발하여 실효성과 보안 수준을 검증한다.

허가형 블록체인은 블록체인 참여자가 시스템을 사용하거나 노드(Node)로 참여할 때 네트워크의 허가가 필요한 시스템을 말하며, 블록체인의 비가역적 특성과 우수한 무결성은 그대로 유지하면서 공개키 기반구조(Public Key Infrastructure)를 활용한 비대칭 암호화 알고리즘 및 멤버십 서비스 관리 기능으로 참여자를 제한하여 퍼블릭 블록체인 대비 뛰어난 기밀성을 확보할 수 있고 암호화폐를 보상으로 네트워크 참여를 유도하는 방식이 아닌 같은 목적을 가진 노드들이 자발적으로 네트워크에 참여하는 구조로 국방정보체계 분야에 적용하기 적합한 구조의 블록체인 유형이라고 할 수 있다.

이러한 허가형 블록체인을 국방 분야에 적용하기 위해서는 대상 시스템의 특성을 고려해야 한다. 기본적으로 블록체인 기술이 모든 유형의 시스템 적합하지 않기 때문이다. 데이터의 일관성이 중요하고 복잡한 계산, 통계 분석 등의 업무는 기존 데이터베이스 시스템이 유리하며 분산 원장의 비가역성을 통한 무결성 유지 및 데이터의 신뢰성이 중요한 시스템에는 허가형 블록체인이 유리하다.

국방 블록체인 플랫폼은 데이터 변조, 탈취 등의 공격을 원천적으로 대비하는 방안이 될 것이며 이를 구체화하여 다양한 체계에 적용할 수 있는 방안을 마련한다면 국방 보안의 새로운 변화를 가져올 것이다. 또한 이를 시작으로 민간 대비 정체된 국방 분야 블록체인 관련 연구가 더욱 활발해질 것이다.

2. 연구범위

본 연구는 2절 1의 목적에 관한 연구 범위를 다음과 같이 정리한다.

첫째, 국방 분야 블록체인 기술 도입의 필요성 논거 및 방안 제시

현재 국방 분야 정보체계가 가진 문제점과 이에 따른 새로운 변화의 필요성에 대한 설명 그리고 해결방안을 제시한다.

둘째, 국방 블록체인 적용 대상 및 모델설계

제시된 방안을 통해 블록체인 기술을 군에 적용하기 위한 대상 분야 식별과 플랫폼 선정 그리고 국방 블록체인 모델을 설계한다. 여기서 플랫폼 선정은 아키텍처 설계 및 개발을 직접 할지 다양한 민간 플랫폼 중 하나를 도입할 것인지를 결정하여야 한다.

셋째, 블록체인 테스트 모듈 개발 및 효용성 검증

선정된 플랫폼과 설계한 국방 블록체인 모델을 통해 테스트 모듈을 구현하고 실제 국방정보체계 환경에 적용할 수 있을지 여부 및 효용성을 검증한다.

제3절 데이터베이스와 블록체인의 개요

1. 데이터베이스

가. 기존 데이터베이스의 기본적 정의

데이터베이스란 여러 사람에 의해 공유되어 사용될 목적으로 통합하여 관리되는 데이터의 집합을 말한다. 자료항목의 중복을 없애고 자료를 구조화하여 저장함으로써 자료 검색과 갱신의 효율을 높인다. (두산백과사전)

이처럼, 기존 데이터베이스 시스템은 데이터와 관리 권한이 모두 중앙화되어 있고 중앙서버에 모든 데이터를 보관한다. 또한, 관리자는 클라이언트의 정보 접근 여부를 통제할 수 있으며 클라이언트는 관리자가 부여한 권한 내에서 정보 접근이 가능하다.

나. 기존 데이터베이스의 진화

데이터베이스는 1970년대에 효율적 정보 처리를 위해 관계형 데이터베이스(RDBMS, Relational Database Management System)[2]가 개발된 이후 정형화되고 복잡한 데이터구조를 최대한 효율적으로 처리하기 위해 RDBMS 위주로

2) RDBMS(Relational Database Management System): 관계형 데이터베이스, 데이터의 관계를 기준으로 데이터베이스를 구축하고 관리하는 프로그램. 대표적으로 Oracle, MySQL, PostgreSQL, MariaDB, Microsoft SQL Server 등이 있다.

발전되었고 현세대 대부분의 대규모 정보체계는 오라클을 필두로 한 RDBMS를 기반으로 개발되었다.

이러한 기존 데이터베이스는 빠른 속도와 데이터에 대한 접근통제가 쉬워 민감한 정보를 다루기 편리하고 중앙집중형 데이터베이스에 암호 기술을 적용해 정보의 기밀성을 보장한다는 특징을 가지고 있다. 이처럼, 복잡한 데이터를 빠르고 안정적으로 처리해야 하는 분야에서는 기존 데이터베이스를 활용하는 것이 적절하다.

반면, 기존의 데이터베이스는 보안 측면에서 중앙서버에 모든 정보와 권한이 집중된다는 부분이 단점으로 지적된다. 중앙 관리자는 많은 권한이 있으므로 데이터베이스에 불법적인 행위를 할 수 있다. 그뿐만 아니라 데이터베이스가 해킹당할 시 전체 시스템이 마비되거나 중요 정보가 모두 유출될 가능성이 있다. 최근 발생하는 대부분 해킹 사건이 데이터베이스 정보 유출 사건이라는 점을 고려하면, 이는 큰 취약점이라고 할 수 있다.

2010년대 이후 글로벌 빅테크 기업의 정보기술 서비스와 빅데이터의 등장으로 현세대의 시스템들은 기본적으로 처리해야 하는 데이터 규모가 기하급수적으로 증가하였고 따라서 유지해야 할 보안 수준이 상향되면서 기존 RDBMS를 대체하기 위한 수단들이 꾸준히 연구되고 있다. 그 대표적인 기술이 NoSQL[3]과 블록체인이며 <표 1>은 기존 데이터베이스와 신기술들의 특징을 간단히 비교하였다. 또한, 시스템 설계자는 데이터베이스 선정에 앞서 기술적 유형에 따른 절대적 옳고 그름을 따지기보다는 해당 기술을 적용하려는 정보체계의 특성에 따라 시너지 효과를 낼 수 있는지를 검토하여야 한다.

---

3) NoSql(Not Only SQL): 대규모 데이터 처리 등을 목적으로 데이터베이스에 관계형 데이터구조뿐만 아니라 확장성, 유연성, 가용성 등 다른 특성을 부가적으로 지원하기 위해 개발된 데이터베이스. MongoDB, Couchbase, CouchDB 등이 이에 해당한다.

<표 1> 유형별 데이터베이스 특징 비교

항목	기존 데이터베이스	NoSQL	블록체인(퍼블릭)
유형	중앙 제어 시스템	분산형 데이터베이스	탈중앙화 제어 시스템
기밀성	권한을 가진 자 접근 가능	권한을 가진 자 접근 가능	네트워크의 모든 참여자 접근 가능
무결성	중앙 관리자의 권한 하에 기록된 데이터 변경 가능	데이터의 일관성 측면에서 무결성이 RDBMS보다 상대적으로 불리함	기록된 이력 데이터는 변경 불가, 변경된 상태는 비가역적
가용성	중앙서버 중단 시 전체 시스템 사용 불가	분산 서버 구조로 RDBMS 대비 가용성이 높음	중앙 관리자가 없는 분산 서버 구조로 가용성이 가장 높음
권한 통제	관리자로부터 권한을 부여받은 사용자만 CRUD[4] 가능	관리자로부터 권한을 부여받은 사용자만 CRUD 가능	합의 알고리즘을 통한 블록체인 네트워크 자체 검증 가능
내부 위협에 대한 내성	권한이 있는 사용자의 행동을 검증하는 과정이 없어 악의적인 행동에 대한 내성 없음	권한이 있는 사용자의 행동을 검증하는 과정이 없어 악의적인 행동에 대한 내성 없음	검증을 통해 네트워크에 참여하는 악의적인 노드에 대한 내성이 있음, 내부자 위협에 비교적 강함
안정성 / 속도	데이터의 일관성이 높으며 복잡한 구조의 데이터 처리에 장점 있음	RDBMS 대비 일관성 떨어지며 단순한 구조의 대용량 데이터 처리에 장점이 있음	기존 데이터베이스 대비 높은 투명성과 무결성을 보장하지만, 상대적으로 속도가 느림
확장성	scale-up	scale-out	scale-out
스키마	미리 정의된 스키마	자유로운 스키마	자유로운 스키마
데이터 모델	계층적 데이터 부적합	계층적 데이터 적합	계층적 데이터 적합
쿼리	복잡한 쿼리 사용 유리	복잡한 쿼리 사용 불리	복잡한 쿼리 사용 불리
적합한 업무	데이터가 복잡하고, 일관성이 중요한 업무 다양한 통계 분석 업무	구조가 단순하며 대용량 데이터 처리가 필요한 업무 실시간 동시처리가 중요한 업무	데이터의 비가역성 및 보안이 중요한 업무

4) CRUD(Create Read Update Delete): DBMS에서 이루어지는 쓰기/읽기/수정/삭제 업무

2. 블록체인

가. 블록체인 개념

블록체인은 분산 원장(Distributed Ledger)이라고 하는 일종의 분산 데이터베이스 시스템이며 네트워크에서 일정 시간 동안 발생 된 트랜잭션에 의해 확정된 거래내역을 하나의 블록에 기록한다. 그 블록에는 바로 직전 블록의 거래내역 해시값[5]과 현재 거래내역 해시값이 저장되어 있어 블록들이 서로 연결되어 있다고 표현하며, 마치 이 모습이 체인과 같다고 하여 블록체인이라 불린다. 또한, 해시 알고리즘의 특성으로 무결성이 보장되어, 공격자의 데이터 위·변조 시 블록의 합의 과정에서 문제가 되는 블록은 자연스럽게 제거된다.

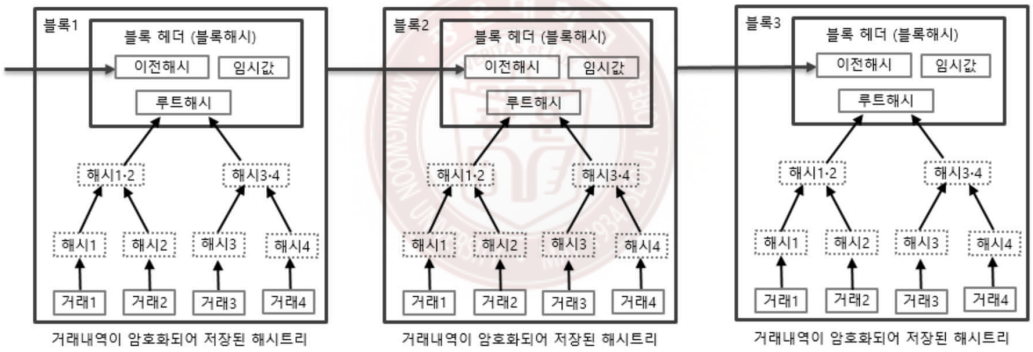
2008년에 발표된 Satoshi Nakamoto의 'Bitcoin: A Peer-to-Peer Electronic Cash System'에서 처음 소개된 블록체인 기술은 기존의 중앙집중식 거래 시스템을 탈중앙화할 수 있는 핵심 기술로 금융과 암호화폐 분야에 처음 도입되어 활발히 활용되고 있으며 최근에는 금융에만 한정되지 않고 새로운 비즈니스 플랫폼으로 확산하면서 다변화되는 추세다.

블록체인은 기존 데이터베이스 시스템과 다르게 참여자 스스로 정보를 감독하므로 중앙 관리자가 필요 없는 구조로 되어 있으며 이것을 탈중앙화되어 있다고 표현한다. 따라서, 블록체인 기반 시스템에서는 누구나 네트워크에 참여해 정보에 접근할 수 있고 트랜잭션에 대한 검증 절차를 거친다면 모든 노드가 블록체인에 정보를 추가할 수도 있다.

---

5) 해시(hash): 다양한 길이를 가진 데이터를 고정된 길이를 가진 데이터로 매핑(mapping)한 값으로 단방향 암호화 등에 주로 사용된다.

구조적 관점에서 살펴보면, 블록체인은 특정 기록이 담긴 블록으로 구성되어 있으며 일반적으로 이 블록은 자체 정보가 담긴 블록 헤더와 거래 기록이 담긴 블록 바디로 구성된다. 모든 블록 헤더에는 이전 블록을 참조하기 위한 해시값이 포함되며 대부분의 블록체인 플랫폼은 이 값을 이용해 신생 블록이 과거 블록을 참조한다. 예를 들어 비트코인은 SHA-256 해시 알고리즘의 결괏값이 블록 헤더에 있다. [그림 1]과 같이 블록 1의 해시값을 블록 2가 참조하고 블록 2의 해시값을 블록 3이 참조하는 구조이다. 이렇게 블록체인은 신생 블록부터 최초 생성 블록까지 전체가 하나의 Linked-List로 연결되어 있다.



[그림 1] 블록체인 구조

자료: http://wiki.hash.kr/index.php/블록체인

나. 블록체인의 진화

기존 데이터베이스 기술과 블록체인 기술은 각각 장단점이 있다. 블록체인 기술은 분산 시스템 내 악의적인 사용자가 존재하더라도 정보 무결성을 지킬

수 있다. 모든 사용자가 주체가 돼 정보를 관리하기 때문에 공격자가 특정 노드의 데이터베이스를 조작해도 전체 데이터베이스에는 영향이 없다. 이를 바탕으로 사용자들은 중개자 없는 시스템, 정보 무결성이 중요한 시스템, 체계 생존성이 중요한 시스템에 블록체인 기술을 활용할 수 있다. 한편, 블록체인 기술은 기술의 성숙도가 낮다. 기존 데이터베이스 기술은 30년 이상 연구돼 속도와 안전성이 검증되었으며 이미 수많은 시스템이 기존 데이터베이스 기반으로 구동되고 있어 예측 불가한 변수가 상대적으로 적다. 반면 초기 블록체인 기술은 상대적으로 안정성과 속도 측면에서 단점들이 발견되어 실제 업무에 사용하기 어려운 문제가 있다. 그리고 블록체인 기술의 안정성을 검증할 구체적인 방안이 정립되지 않아 체계의 취약점을 분석하는 데 어려움이 존재한다. 이외에도 블록체인 기술 자체는 정보의 기밀성을 보장하지 않아 민감한 정보에 대해서는 추가적인 조처를 해야만 한다는 한계가 있다.

다. 블록체인의 분류와 허가형 블록체인의 필요성

블록체인은 네트워크의 성격, 범위 등에 따라 여러 가지 형태로 분류되며 퍼블릭 블록체인, 프라이빗 블록체인, 컨소시엄 블록체인 등 각각 유형별로 사용 용도에 맞게 응용되어 사용된다.

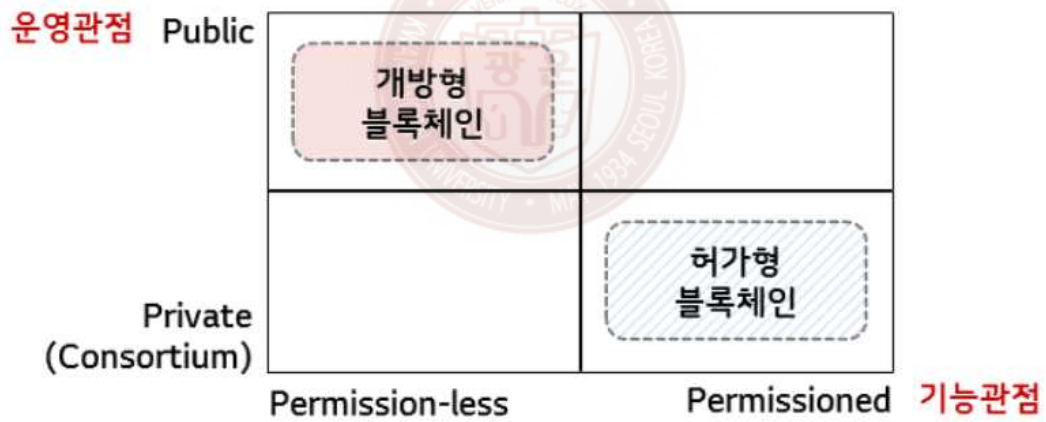
퍼블릭 블록체인은 비트코인, 이더리움과 같이 누구나 네트워크에 참여할 수 있는 블록체인이고 프라이빗 블록체인은 하나의 기관에서 독자적으로 관리하는 블록체인이며 컨소시엄 블록체인은 여러 기관이 컨소시엄을 이뤄 구성하는 블록체인으로 허가된 기관만 네트워크에 참여할 수 있다.

현재 기업 또는 기관들이 엔터프라이즈용 플랫폼으로 관심을 가지는 블록체인 기술은 퍼블릭이 아닌 프라이빗 혹은 컨소시엄 블록체인이다. 이유는 블록체인의 무결성을 활용하면서 접근 통제기법 적용으로 기밀성 확보와 참여자 관리가 가능하며 합의 알고리즘의 차이로 속도 또한 월등히 빠르기 때문이다. 상세 차이점은 <표 2>에서 블록체인 유형별 비교를 통해 확인할 수 있다.

<표 2> 블록체인 유형별 비교

요소	퍼블릭 블록체인	프라이빗 블록체인	컨소시엄 블록체인
관리주체	모든 참여자	중앙기관	컨소시엄에 소속된 참여자
거버넌스	한번 정해지면 변경이 어려움	중앙기관의 의사결정에 따라 유연하게 변경 가능	컨소시엄 참여자들의 합의에 따라 유연하게 변경 가능
거래 속도(TPS)	느림	빠름	비교적 빠름
데이터 접근 (트랜잭션 생성)	네트워크 참여자 누구나 가능	허가받은 사용자만 가능	허가받은 사용자만 가능
식별성	익명성	식별 가능	식별 가능
주요 합의 알고리즘	PoW(Proof-of-Work), PoS(Poof-of-Stake), DPoS(Delegated PoS)	오더링 서비스를 통한 합의(SOLO, Kafka, Raft)	포크(fork)를 허용하지 않는 BFT 계열의 합의 알고리즘
네트워크 참여 유도	토큰 보상	특수목적에 의한 자발적 참여	특수목적에 의한 자발적 참여
토큰 유무	있음	불필요	불필요
예시	비트코인, 이더리움, 이오스	하이퍼레저 패브릭, EEA	R3CEV, CASPER

또한, 본 연구의 목적인 블록체인 기술의 국방적용과 같이 실제 엔터프라이즈용 블록체인으로 어떤 유형이 가장 적합한지를 알아보기 위해서는 운영관점과 기능관점의 특징을 알아볼 필요가 있다. [그림 2]에 따르면 블록체인을 운영관점에서 바라볼 때 Public과 Private로 구분할 수 있고 기능관점에서 바라보면 Permissioned와 Permission-less로 구분할 수 있는데, 결국 블록체인을 엔터프라이즈용으로 사용하기 위해서는 Private과 Permissioned의 특성을 동시에 가져야 하며 그러한 유형의 블록체인을 허가형 블록체인이라고 말한다. 허가형 블록체인은 <표 2> 기준으로 설명하면 프라이빗 블록체인과 컨소시엄 블록체인을 합친 성격의 블록체인이라고 말할 수 있다.



[그림 2] 관점 기준의 블록체인 유형 분류

자료: LG CNS, “블록체인: 혁신인가? 혁명인가”, 스마트금융 컨퍼런스, 2017.

이러한 특성으로 현재 엔터프라이즈용 블록체인 시장에서 가장 주목받는 유형은 단연코 허가형 블록체인이라고 말할 수 있으며 국방 분야 또한 허가형 블록체인을 통해 정보체계 보안의 새로운 돌파구를 찾을 수 있을 것이다.

제2장 국방정보체계와 보안 연구

본 장에서는 국방 관련 정보체계 및 정보보안의 정의에 대해서 논의하고 블록체인을 활용한 국방 정보체계의 정보보안 관련 동향과 사례를 분석한다.

제1절 국방정보체계와 정보보안

1. 국방 정보체계의 정의

국방정보화업무훈령에서 국방정보체계는 국방 정보의 수집・가공・저장・검색・송신・수신 및 그 활용과 관련되는 기기 등 응용소프트웨어와 기반 운영환경의 조직화된 체계로 정의하고 있으며, 국방 정보시스템의 장비운영 및 관리를 위해 응용소프트웨어를 다음과 같이 분류한다.

① 전장관리정보체계: 지휘통제, 전투지휘, 군사정보체계
② 자원관리정보체계: 기획・재정, 인사・동원, 군수・시설, 전자행정, 군사정보지원, 상호운용성
③ 국방M&S체계: 연습・훈련용, 분석용, 획득용

또한, 정보시스템의 기반 운영환경은 주장비, 통신망, 단말기, 주변장치, 시설, 정보보호체계, 상호운용성 관리에 필요한 시스템, 그 밖의 시스템 소프트웨어를 말한다.

2. 국방 정보체계의 보안 및 사이버보안

국방정보화업무훈령에서 정보시스템의 보호관리 및 사이버보안에 관한 업무는 “「국방사이버안보훈령」 등(국방보안업무훈령 포함)에 따른다”라고 명시되어 있으며, 국방사이안보훈령은 정보 보호와 관련해서 아래와 같이 정의한다.

① 정보통신보안(정보보호): 정보통신수단에 의하여 처리, 저장, 소통되는 자료를 도청, 해킹 등 외부 위협으로부터 보호하거나 취약 요인을 제거하기 위한 각종 수단과 방법 등의 일체의 행위를 말한다.

② 정보통신보안시스템(보안시스템): 정보통신 수단으로 생산, 처리, 저장, 송·수신되는 정보를 유출, 변조, 훼손 등으로부터 보호하기 위한 암호장비, 보안자재, 암호논리 등을 말한다.

③ 국방사이버안보 업무: 국방 사이버 공간을 안전하고 정확하며 효과적으로 창출·유지·보호하고, 적대세력에 비해 사이버 공간에서의 우위를 확보하기 위한 제반 활동으로 사이버정책과 사이버보안 및 사이버 작전 업무로 구분한다.

④ 사이버보안 업무: 국방 사이버 공간에서 정보의 기밀성·무결성·가용성을 보장하기 위하여 취하는 물리적, 기술적, 관리적 활동으로, 국방 정보시스템과 내장형 소프트웨어(Embedded Software)를 가지고 있는 무기체계 및 전력 지원체계의 수명주기와 연계한 보안 활동, 국방 사이버 공간 취약점 분석·평가 및 조치, 각 군 및 기간의 사이버보안 관리 수준 평가, 그 밖의 일상적인 예방 활동을 포함한다.

3. 국방 정보체계의 보안 취약 분야와 블록체인 적용

국방정보화업무훈령의 분류상 국방 정보체계는 크게 전장관리정보체계, 자원관리정보체계, 국방M&S체계로 분류되어 그 아래 수많은 정보체계가 존재한다. 최근 정보화의 발전과 함께 분류상 존재하는 모든 체계가 고도화되면서 기능이 복잡해지고 체계 간 상호운용성이 증대되면서 정보보안에 관련된 취약점과 그에 따른 관리 포인트가 기하급수적으로 증가하였다. 따라서, 국방 정보체계의 분류상 언급된 모든 체계는 보안 이슈의 당사자이며 보안 강화의 대상이 된다. 하지만 그렇다고 해서 존재하는 모든 정보체계를 블록체인으로 대체한다는 것은 불가하다. 블록체인이 갖는 고유의 특성과 해당 시스템의 특징을 고려하여 블록체인 적용에 대한 적합성 여부와 결국 대상이 되는 정보체계에서 원하는 보안 수준을 달성하기 위한 가장 효율적인 대안이 블록체인인가에 대해서 고려해야 하기 때문이다.

이러한 제반 환경에서 블록체인 기술을 통해 국방정보체계의 보안을 강화하기 위한 방안으로, 가장 보안에 취약하며 블록체인 적용에 적합한 분야를 찾아보면 국방 연동체계를 고려할 수 있다. 국방 연동체계는 상호운용성의 필요성에 따라 상기 분류의 수많은 시스템을 하나로 연결하는 물리적/논리적 특성으로 인해 상대적으로 보안에 취약할 수밖에 없으며 그 특성은 단지 하나의 정보체계에 국한되는 문제가 아니라 연동 네트워크를 구성하는 전체 노드에 걸쳐 발생하는 문제이므로 상당히 치명적인 이슈라고 할 수 있다. 또한 국방연동체계는 시스템의 특성상 단순한 데이터의 관점에서 보안의 3대 요소인 기밀성, 가용성, 무결성뿐만 아니라 네트워크의 관점에서 책임 추적성, 부인방지, 인증, 접근통제 등의 요소까지 달성해야 하는 특성을 가지므로 그 어떤 분류

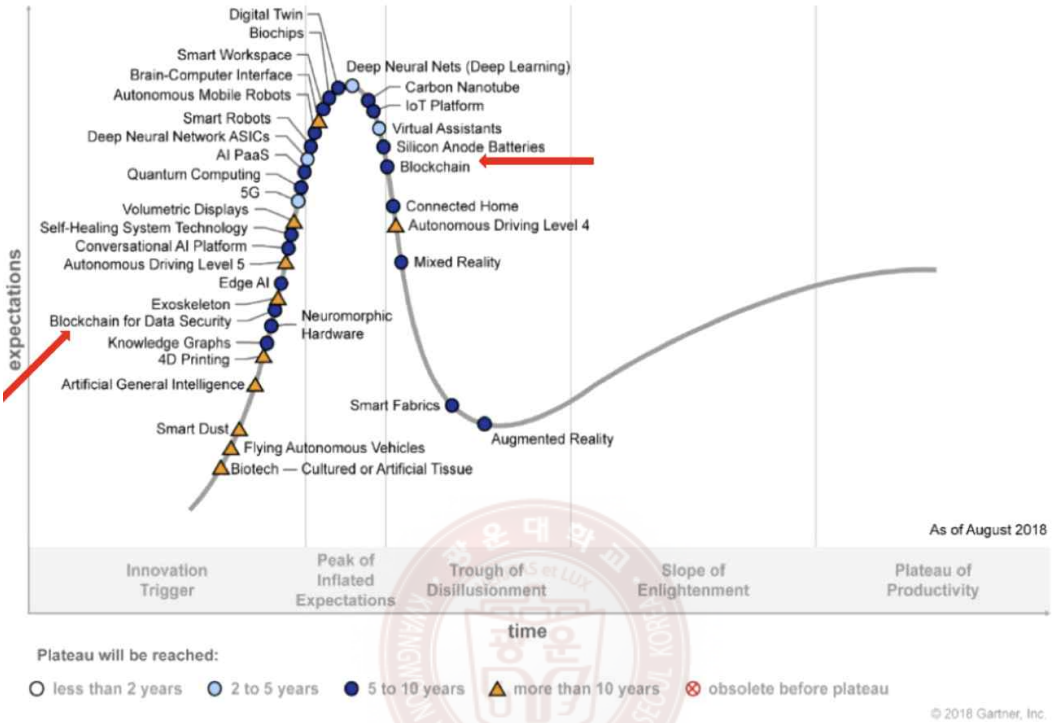
보다 블록체인의 특성에 부합한다고 판단되며 이에 대한 상세 내용은 '3장-2절-1-나. 블록체인 적용 가능 국방정보체계'를 통해 논의하도록 한다.

제2절 국방 블록체인 기술의 글로벌 동향

1. 글로벌 국가들의 국방 블록체인 기술에 대한 방향성

2018년 미국의 정보기술 연구 및 자문 회사 가트너는 [그림 3]과 같이 블록체인 기술에 대한 동향을 분석하였다. 최초의 블록체인 기술은 비트코인을 필두로 한 가상화폐의 등장과 함께 급성장했다가 현재는 퇴색해 가고 있는 기술로 분류되고 있다면, 블록체인 기반의 데이터 보안기술은 기대되는 최신기술로 떠오르고 있으며 해당 기술의 발전은 향후 다양한 분야에서 활용 가치가 급성장할 것으로 기대되고 있다. 다만, 블록체인 기술은 아직 그 역사가 짧고 기술의 완성도가 미성숙하여 국내외 또는 민간, 국방 할 것 없이, 앞으로 한참을 지속해서 연구를 더 해 나가야 하는 상황이라고 할 수 있다.

국방 분야에서 블록체인에 대한 활용 가치를 이해하려면 인사, 정보, 작전, 군수 등의 개념에 블록체인의 비가역성, 무결성, 암호화, 참여자 관리 등의 기술적 잠재력이 어떻게 내재화될 수 있는지 상세히 연구되어야 한다. 국방에서 블록체인 기술은 정보시스템의 보안 및 효율성 향상을 위한 데이터 플랫폼 역할을 할 수 있으며 전시 장병의 안전 및 평시 부대 관리 문제를 지원하고, 물자의 공급망을 추적하여 관리에 민감한 탄약, 의약품, 식품과 같은 품목의 실시간 추적 등 기존에 문제가 되었던 부분을 예방하고 개선할 수 있다.

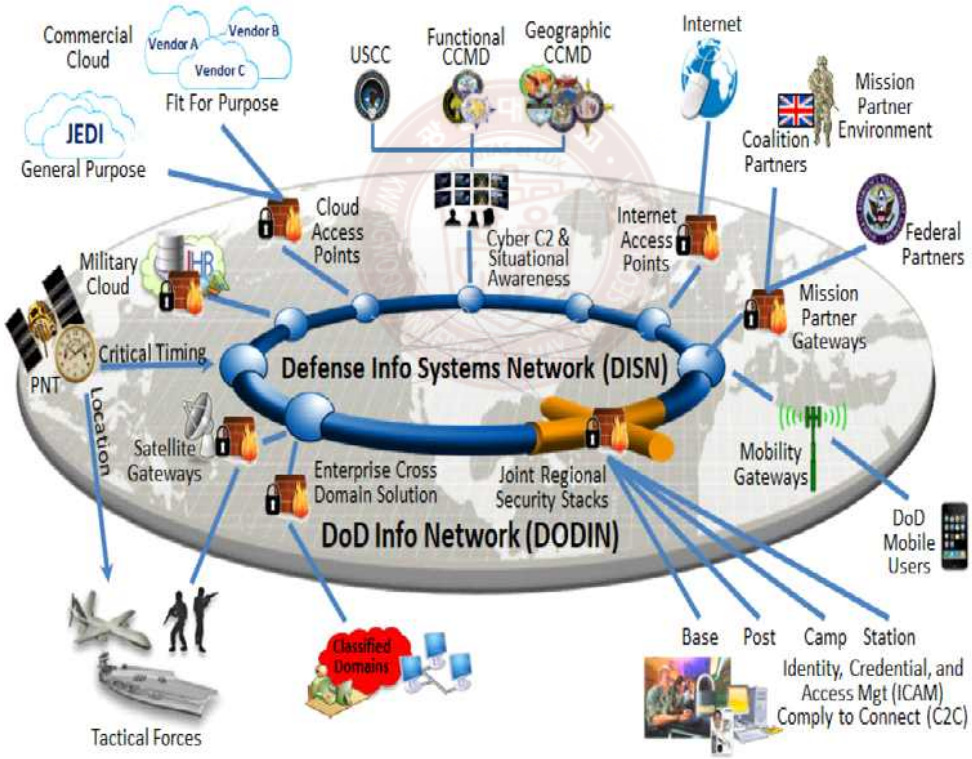


[그림 3] 최신기술 하이퍼-사이클 분석 결과

자료: Gartner, 2018.

2016년 세계경제포럼(WEF, World Economic Forum)의 클라우스 슈바프 의장에 의해 4차 산업혁명이라는 용어가 전 세계에 알려진 전후로 인공지능, 사물 인터넷, 빅데이터, 클라우드 컴퓨팅, 블록체인 등으로 대표되는 기존의 기술 질서를 붕괴시키는 차세대 신기술에 대한 글로벌 군사 강국들의 기술 패권 경쟁은 매우 치열해졌다. 기술 경쟁에서의 성패가 곧 국제사회에서 패권의 향방을 결정할 수 있기 때문이다. 이러한 현상은 국방 블록체인 분야의 개발 동향에서도 나타나고 있으며 개발 형태는 주로 국가 수준의 기술 개발 요구를 탑-다운 형태로 수행하는 방식을 취한다.

2019년 발표된 미국 '국방 디지털 현대화 전략'의 연합 정보환경 프레임워크(JIE, The Joint Information Environment)는 이런 점을 잘 보여준다. 해당 전략에서 미국은 [그림 4]와 같이 네트워크 및 통신 부문의 개선 전략 계획에 미 국방 고급 연구 프로젝트 기관(DARPA, The Defense Advanced Research Projects Agency)을 통한 블록체인 프로토콜 기반의 안전한 메시지 플랫폼 및 해킹 불가능한 코드를 개발하려고 노력 중이다.



[그림 4] 미국 DoD의 JIE 프레임워크 범위

자료 : DoD DIGITAL MODERNIZATION STRATEGY, U.S. DoD Office of Prepublication and Security Review, 2019.7.12.

미국 DoD의 최고정보책임자(CIO, Chief Information Officer)는 국방 디지털 현대화 전략에서 사이버보안, 인공지능, 클라우드, C3(명령/제어/통신) 기술을 우선순위로 선정하였다. 그리고 그중 사이버보안 패러다임을 뒤집는 새로운 정보기술로 블록체인을 제시하였고 그 세부 내용은 아래와 같다.

① 블록체인 네트워크는 내부 및 외부에서 네트워크를 훼손할 수 있다는 것을 가정한다.
② 블록체인은 투명하고 안전하다. 장애가 발생하기 쉬운 비밀에 의존하지 않고 암호화된 데이터구조에 의존하므로 변조가 어렵고 신뢰성을 가진다.
③ 블록체인 네트워크는 내결함성이 있다. 정상적인 노드들의 합의를 통해 비정상 노드를 거부한다.
④ 결과적으로, 블록체인 네트워크는 타협의 가능성을 줄일 뿐만 아니라 이를 달성하기 위해 상대에게 훨씬 더 큰 비용을 부과한다.

이처럼 미국은 정보기술의 경쟁우위 확보, 효율성 및 향상된 기능을 위한 최적화, 민첩한 국방 태세를 위한 사이버보안 발전, 디지털 인력 인재 양성을 목표로 국방 디지털 발전전략을 수립하고 신기술 개발전략, 목표, 비전을 구체화하였다. 또한, 신기술의 국방 분야 적용을 군사기술 경쟁 차원을 넘어서 기술 자체를 전략자원으로 인식하고 있으며 특히, 블록체인 기술을 국방 전반에 적용하여 사이버 공간의 데이터 보안 및 네트워크의 신뢰성을 담보하는 수단으로 활용한다. 사이버보안 강화, 의사결정 실패 방지, 효율성 및 투명성 제고 등을 위해 국방 블록체인을 실현하고자 하는 것이다. (Soto, Daren, “Potential Uses of Blockchain by the U.S. Department of Defense”, Value Technology foundation, pp. 8-9, 2020.)

2. 글로벌 국가들의 연구개발 현황

미국은 국방 블록체인 개발을 4가지 범주의 분야별 적용전략을 수립하여 추진하고 있으며 ① 에너지, 물, 수송망 등의 사이버보안 ② 긴급상황, 재난 상황에의 신속한 의사결정과 의사결정 실패 방지 ③ 조달 투명성 제고 ④ 국방 물류, 장비 부품 등 공급망 관리 분야 등으로 정리된다.

또한, 미국 DoD는 사이버안보, 무기체계 제조 및 개발, 데이터 무결성 유지를 통한 전장의 신뢰 보장, 정보 보호, 국방 군수 및 조달계약, NATO 및 동맹국 간의 운용 기반 확보 등 7가지 분야에서의 기술 개발을 진행하고 있으며, 2019년에는 7천억 달러 규모를 투입하여 디지털 보안 플랫폼을 개발하고 있다. 특히 주목할 분야는 미 육군의 우주 통신 데이터 사이버 침해 여부를 감시하는 프로그램이다. 그리고 더 나아가 NATO 회원국 간의 협력을 강화하기 위한 블록체인 솔루션도 개발하고 있다. (Alessia et al., “Blockchain in Defense: A Breakthrough?”, Finabel European Army Interoperability Center, pp. 16-17, 2020.) 이러한 미국 및 국외의 국방 블록체인 기술 적용 정책 및 연구에 대한 동향은 <표 3>에서 확인할 수 있다.

<표 3> 국방 블록체인 글로벌 동향

국가/기관/분야	내용
[미국방부-전체] 연합정보화환경 프레임워크 (사이버보안)	• “미국 국방 디지털 현대화 전략” 국방 정보 자원의 관리 전략 계획인 “PLAN FY19-23” 2019년 7월 정책 수립 공포(블록체인 활용 정책 포함) • 모든 국방 전술상에 연계된 유무인체들의 “연합정보화 환경 프레임워크” 정책으로 이들 요소의 생산단계부터 반영, 자율적 연합동작 능력 인프라 포트폴리오 추구 중
[미국방부-총괄]	• 미국 트럼프 대통령은 “블록체인을 사이버보안 등 군대 적용 연구비 승인 문서(Military Spending Bill)”에 사인(약 1.1 billion/년)

국가/기관/분야	내용
	• 블록체인의 7대 활용분야 선정 (1) 사이버공격 (2) 무기체계 제조 개발 (3) 전장 신뢰 보장 (4) 정보 보호 (5) 국방물류/계약 (6) 무기체 보호 (7) NATO 응용
[미국방부] 사이버 공격	• 사이버 공격 분야를 확대, 초연결되는 상황을 고려하여 파워 공급 네트워킹 컴퓨터, 유무선 이동무기체를 연결하는 모든 상황에 예상되는 사이버 공격에 대비한 강력한 보안 및 신뢰 수단인 블록체인 적용
[미국-NATO-DARPA] 무기체계 보호	• 모든 유무선 이동 무기체계를 보호하고 강화하는 분야 NATO의 경우는 'Navy's Aegis Combat System'에 블록체인을 이용하여 네트워킹 분산화 정책을 조속히 적용 예정 • 블록체인 기반의 무기체계 모니터링 시스템 개발을 위한 방위 산업체와 파트너쉽 체결
[미국방부-해군] 블록체인 전함	• '블록체인 전함'이라는 명명하에 분산 네트워크를 사용 • '이지스함'을 제어하고, 분산 노드들이 동일한 Data Set에서 작동하도록 하는 미래의 전함 제어를 준비
[NATO-국방] 연합 미션 네트워킹	• 국방분야 신뢰 관리에 정책과 표준으로 블록체인 적합성에 대한 정책 검증을 실시 중 • NATO는 FMN(Federated Mission Networking) 환경에서 데이터 및 네트워킹에 블록체인 도입 전략화 중 • 연합 군사작전에 블록체인 기반으로 분산 원장을 활용하는 신뢰 보안용 작전 명령 적용 표준화 협정(STANAG 4778) 비준 절차 중
[EU-EDA] 군 통신 데이터 무결성	• EDA(European Defence Agency)하에 블록체인 기술을 도입하여 Peer-to-Peer 통신과 데이터의 확신성 및 무결성을 위한 연구 정책 진행 중 • 2019년에는 국방용 IoT 네트워킹, 사이버 국방, 보안 메시징 등 블록체인 기반의 새로운 국방 응용 서비스 정책을 도입할 예정
[미국-DARPA] 메시지시스템	• 2016년에 미국 DARPA에서 "블록체인 메시지 시스템"을 연구하여 2017년에 ITAMCO사가 전송 및 수신 방식에서 메시지 생성을 분리하는 해킹 방지 메시징 및 트랜잭션 플랫폼 앱을 개발함
[미국방부] 전장 IoBT	• 전장사물인터넷(IOBT: Internet-of-Battlefield Things)을 센서, 무기, 이동형 무기체, 로봇 그리고 각종 웨어러블 디바이스(센싱, 통신, 액터 등)들이 군대와 협업하기 위한 블록체인 협동 강화 시스템 연구 개발 중 • 전체적으로, 위성 통신을 활용 지상 무기 이동체와 아주 밀접하게협업하는 블록체인 기반 전장 플랫폼
[미국방부]	• 적측가공(AM)은 3D 인쇄 군사 용어. 미군은 AM 방식을 사용하여 무기와

국가/기관/분야	내용
적측가공 (AM: Additive Manufacturing)	차량을 위한 프로토타입과 부품을 제작. 1년 전 미 해군은 단 4주 만에 전체 잠수정을 3D로 인쇄 • 미 해군은 블록체인이 AM 프로세스에 가져올 수 있는 잠재력 존재 인식 2017년 이래 AM 사업의 각 단계 내에서 블록체인을 통합하기 위해 노력 이러한 방식으로 분산 네트워크를 사용하면 디지털 스레드의 요구사항을 충족. 이론적으로 무제한의 안전한 데이터 저장소를 제공. 또한 네트워크의 노드를 사용하여 전체 AM 프로세스에서 데이터를 공유 • 블록체인은 또한 앞으로 다가올 AM을 일반적인 제조 공급 체인에 광범위하게 채택할 수 있는 원동력
[캐나다-국방과학연구소] 국방 전술 망	• 국방 전술 망에서 블록체인 활용 전략 연구를 수행 중 • 블록체인의 활용 차원에서 무결성, 자원 관리(네트워크 관리, 정책 관리, 전파 분배)를 기반으로 블록체인 기술 종합 적용 마스터 플랜을 연구 중 • “Tactical Clusters” 분야는 군인이 미래 착용하는 웨어러블 장치들을 군인 개별 군집 단위로 고려하여, 군집 정보 전술을 블록체인 레이어별(TRANSACTION, BLOCK, CONSENSUS, CHAIN)로 정립해가는 연구 전략 존재
[인도-국방연구소] 군사 운영	• 국방 운영시스템에 블록체인 적용으로 네트워크 생존성을 향상하기 위한 연구 중 • 인도 국방 전장 NEMO(Network Enabled Military Operations) 모델에 블록체인 적용, 전장의 3가지(자원, 통신채널, 데이터) 측면 고신뢰화 추구
SupplyBlockchain (미국회사)	• NATO MApN에 의해 협약된 군 의무훈련인 “Vigorous Warrior 19”에 블록체인 SW를 공급 • Vigorous Warrior 19는 NATO의 가장 큰 의무관련 훈련이며 39개국 2,500명 이상이 참여하고, 1,000여 개의 시나리오, 300개의 의무조치, 1,500개의 재난상황이 시뮬레이션됨 • 의약품의 추적, 글로벌적 위조 약품에 의한 피해 감소, 음식의 출처, 인도주의적 원조의 투명성 확보를 위해 사용됨
PENTOZ	• Blockchain Military Applications의 한 영역으로 AI-enabled Drones의 데이터를 블록체인으로 관리하여 비행내용과 수행행동을 기록 • 해군의 타격시스템(미사일, 레이다, 군함 등)은 하나의 복합적인 시스템 구성체이므로 위협에 대응 하기 위한 분산화된 블록체인 필요성 제기 • Additive Manufacturing(AM)은 3D 프린팅 용어이며 이와 관련한 데이터에 대한 안전한 보관에 블록체인 활용 필요

자료: 이경휴, 박혜숙, “국방 블록체인 기술 동향 및 국방 ICT 융합 전략 연구”, (ETRI)전자통신동향분석 35권 제1호, 2020.

제3절 한국의 국방 블록체인 선행연구

2018년 11월 대한민국은 국방부가 소요제기 및 사업통제를 하고 국방과학연구소(ADD, Agency for Defense Development)를 과제 수행 및 사업수행기관으로 하여 “블록체인 기술의 군내 도입방안 연구”라는 보고서를 발간하였다.

이 보고서는 블록체인 기술의 군내 도입방안을 도출하기 위해 블록체인 기술 이해, 블록체인 기술의 군 적용방안, 블록체인 기술 적용 시범사업 시스템 제안의 총 3가지 항목에 관한 연구를 진행하였다. 그 이후에도 국방 분야의 블록체인 활용방안에 관한 연구는 <표 4>와 같이 존재하였다. 하지만, 국내 블록체인 활용에 대한 환경조성이 미흡하고 전반적인 블록체인에 대한 이해도와 사회적인 공감대가 형성되지 못해 구체적인 성과를 달성하지는 못하고 국방정보체계에 대한 적용도 이루어지지 못하였다.

<표 4> 대한민국 국방정보체계의 블록체인 연구현황

연구 주체 / 연도	내용
안재홍 (2018) 국방과학연구소	**[블록체인 기술의 군내 도입방안 연구]** • 국방 분야의 블록체인 기술 적용 필요성에 관한 연구 • 시범체계, 유/무선망용 기반 체계, 운용조직 양성, 기술교육 활성화 등을 통해 장기적 군용 블록체인 기술 도입 로드맵 제시
김선재 (2021) 한국군사학논집	**[국방시설분야의 블록체인 기술 적용방안 연구]** • 국방시설업무와 블록체인 기술의 접목을 통해 현대화되고 첨단화된 국방/군사시설을 건설하고 유지관리하는데 기여할 수 있는 방안을 제시 • 블록체인의 다양한 특성을 바탕으로 국방시설 분야에 적용할 수 있는 방안 제시

연구 주체 / 연도	내용
김기원 (2022) 국방정책연구	**[블록체인 기술의 글로벌 동향과 한국 국방 적용 연구]** • 블록체인 기술의 한국 국방에서의 활용 필요성과 활용방안을 검토 • 블록체인 기술이 출현한 이후 이 기술은 어떻게 진화하고 있는지와 AI, 빅데이터, 클라우드 등 4차 산업혁명 신기술과 블록체인의 융합을 통한 시너지와 기술의 효과를 확인 • 공공분야와 산업체 등 국내외에서의 블록체인 기술 적용 동향 분석
이경진 (2022) 한국통신학회논문지	**[국방 분야에서의 블록체인 기반 신원증명 서비스의 수용 의도에 영향을 미치는 요인에 관한 연구]** • 블록체인 기반 신원증명 서비스의 시스템 특성, 블록체인 기반 서비스 특성이 수용 의도에 미치는 요인을 실증적으로 검증하고 이를 통해 국방 분야에 블록체인 기반 신원증명 서비스가 성공적인 도입 및 활성화가 될 수 있도록 통합기술수용모델 제시

또한, 현재까지 진행된 국방 분야 블록체인 관련 연구는 전반적인 정책적 제언이나 개념 파악, 기술적 동향에 관한 연구 및 적용 가능 분야 식별 정도에서 그치는 경우가 대부분이었다. 그러다 보니 문서로는 보안시스템 또는 물류시스템 등에 적용하기에 적절하다고 주장되지만, 실 체감이 어려워 현실과의 괴리가 존재하는 것이 사실이다.

이러한 관점에서 기존 국방 분야 블록체인 연구에서 한 발짝 더 진일보한 형태의 연구가 필요하다. 실제 가까운 미래에 국방정보화업무훈령[6]과 같은 법제도 및 블록체인의 정책이 변화된다면, 그것에 부합하는 표준 및 근간이 될 수 있는 모델을 제시하고 국방 정보체계 적용 여부를 실증하는 테스트 모듈의 개발 및 실험을 통한 의미 있는 근거를 제시해야 한다.

---

6) 국방정보화업무훈령: 국방정보화업무훈령은 국방정보화 기반조성 및 국방정보자원관리에 관한 법률(국방정보화법)에 근거하여 국방정보화사업 추진, 정보자원관리, 정보화평가, 정보기술의 연구 및 실험, 정보화 기반기술의 적용, 전담기관·전문기술지원기관 지정·운영, 국방정보화책임관협의회 운영 등에 관한 절차, 기준, 원칙을 정하는 것을 목적으로 한다.

제4절 국방정보체계의 블록체인 적용사례

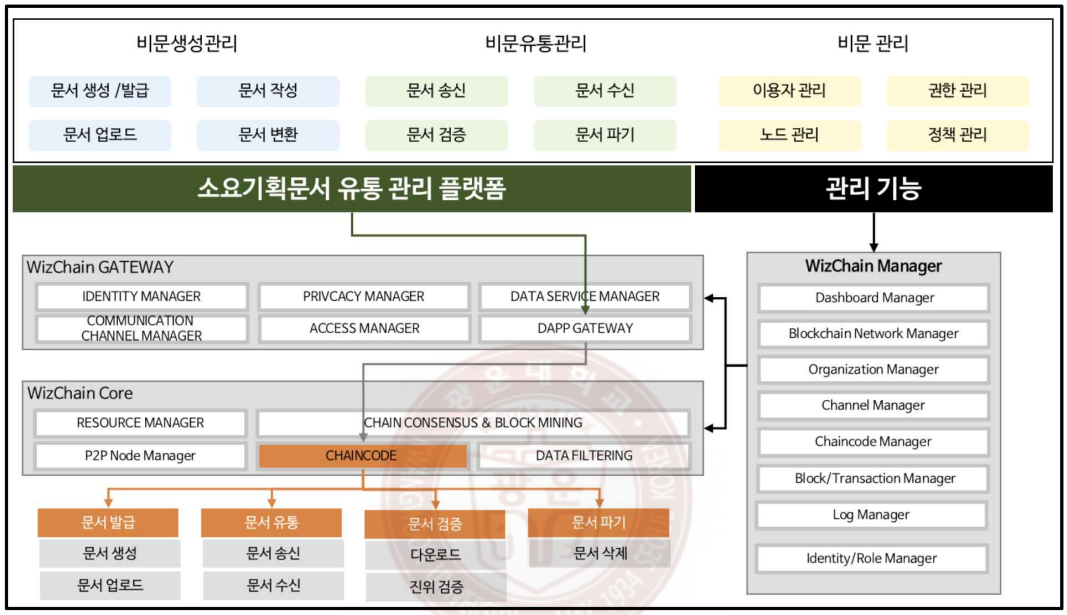
대한민국 국방부의 블록체인에 관한 연구는 앞선 글로벌 동향과는 사뭇 다른 접근성을 보여준다. 그것은 옳고 그름의 차이라기보다는 방향성의 차이인데, 한국 국방정보체계는 군의 전략자산, C4I 체계 등 전술 지휘체계 및 전술 네트워크보다는 군사자료[7] 등 비문을 관리하는 시스템 위주로 개발이 진행되었다. 아마도 복잡하고 막대한 자원이 소모되는 TOP-DOWN 형태의 대규모 프로젝트보다는 현실적인 수준에서의 구축을 시작으로 점차 블록체인 시스템을 확장해 나가는 방향으로 전략을 모색하였다고 판단된다.

비문을 관리하는 시스템은 정보통신 기술이 발전하면서 그동안 오프라인에서 관리하였던 군사 자료를 컴퓨터에 의해 생성, 보관 등 관리한다. 또한, 이러한 전산 자료의 비중이 점점 증가함에 따라 자연스럽게 비밀 관리 시스템의 보안 수준이 큰 관심을 받게 되었다.

2020년 국방전산정보원에서 공개된 보도자료에 따르면 군은 2023년 전력화를 목표로 약 74억 원 규모로 보안 문서의 이력 관리를 위해 국방획득정보체계(DAIS, Defense Acquisition Information System) 신규 구축 사업을 시행하였다. 이 체계는 국방부, 합참, 각 군 본부, 방위사업청, 국방과학연구소 등에서 사용하며 기존 수기 문서 위주의 무기체계 소요 기획, 예산, 사업, 시험평가 등의 업무를 정보화하고 관련 기관 간 데이터를 공유를 위해 구축되었는데, [그림 5]의 구성도처럼 사업 시 블록체인 기술로 개발된 보안 플랫폼의 도입으로 그간 무기체계의 소요 기획 및 예산 관련 업무를 비밀문서로 작업하면

7) 군사자료: 군사 관련 정보가 포함된 기록물을 말하여 일반군사자료, 군사비밀, 대외비로 구분한다.

서 행정 소요 기간이 과다하게 발생하거나 관련 기관 간 공유가 제한되는 등의 문제를 해소하였다.



[그림 5] 국방획득정보체계 구성도

자료: http://www.ksign.com/image/popup_img03.png

하지만 국방획득정보체계는 국방 분야 최초의 블록체인 기술 도입 사례임에도 불구하고 국방부 자체 기술 개발이 아닌 이미 상용화되어 있는 민간의 상용솔루션[8]을 도입하여 일부 기능에 적용한 것에 지나지 않는다는 한계가 존재한다. 이것은 해당 사업의 성과를 평가절하하는 것이 아니다. 다만, <표 3>의 사례에서 소개한 글로벌 동향 대비 현재 대한민국의 국방 블록체인 기술 개발 수준이 아직은 뒤처져 있음을 알리는 부분이다.

8) 상용솔루션: 민간 기업에 의해 개발되어 판매되고 있는 소프트웨어 제품

제3장 국방 블록체인 적용방안 검토

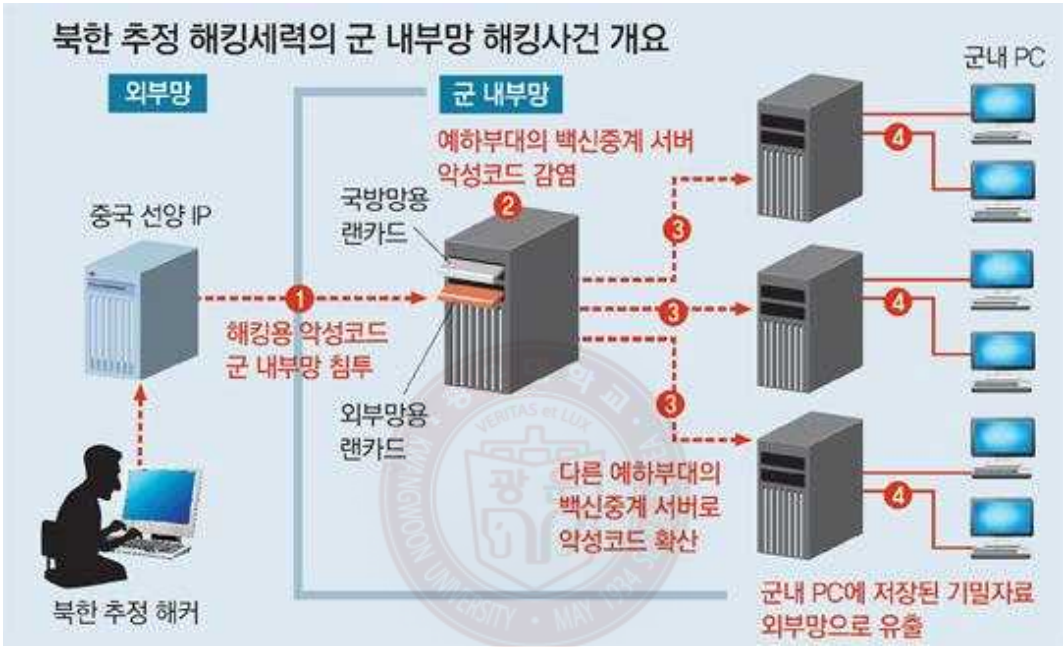
제1절 블록체인 국방 분야 적용의 타당성

본 절은 우리 군의 정보체계에 블록체인 기술을 적용하는 방안을 검토하기에 앞서 과연 국방 시스템에 블록체인 기술을 적용하는 것이 타당한지 또는 정말 실효성이 있을지 과거 사고사례를 통해서 논의한다. 앞서 서론에서 언급한 바와 같이 중요한 논제이기 때문에 다시 한번 요약하면 다음과 같다.

국방 블록체인 도입의 타당성을 논하기 위해서는 우리 군에서 그동안 발생했던 정보보안 해킹 사고사례를 알아볼 필요가 있다. 첫 번째 사례는, 2016년 8월경에 발생한 '군 내부망 해킹으로 인한 핵심 군사 기밀자료 외부 유출사건'이다. 이 사건은 우리 군의 인트라넷이 직접 해킹된 최초의 사례로, [그림 6]의 흐름도와 같이 북한군 해커가 관리부실로 인해 외부망용 NIC[9]와 내부망용 NIC가 동시에 설치된 채 2년 동안 인터넷망에 연결되어 운용되던 국방통합데이터센터의 백신 중계 서버에 악성 코드를 침투시켜 망 분리를 무력화시킨 후 감염된 서버를 이용하여 700대의 내부망 PC를 포함 한 약 3,200대의 PC에 악성 코드를 감염시켜 군사기밀을 유출한 사건이다. 단순히 기술적으로는 군의 한 부대가 관리하는 백신 중계 서버의 관리부실로서 외부 인터넷망(외부망)과 군 내부망이 함께 연결되는 접점에서 랜카드 두 개가 동시에 꽂혀 있었고, 이를 통해 악성 코드가 군 내부망에 침입하여 해킹된 사례이지만, 군 인트라넷이 해킹된 것은 창군 이래로 처음이었으며, 맹신하듯이 안전하다고 여겨져 왔

9) NIC(Network Interface Card): 흔히 랜카드라고 부르며, 컴퓨터 등 단말 장치를 네트워크에 연결하여 통신하기 위해 사용하는 하드웨어 장치이다.

던 망 분리 단독폐쇄망까지도 접점 관리 등의 허술함으로 인해 한순간에 해킹 될 수 있다는 것을 보여준 최초의 사례가 되었다.



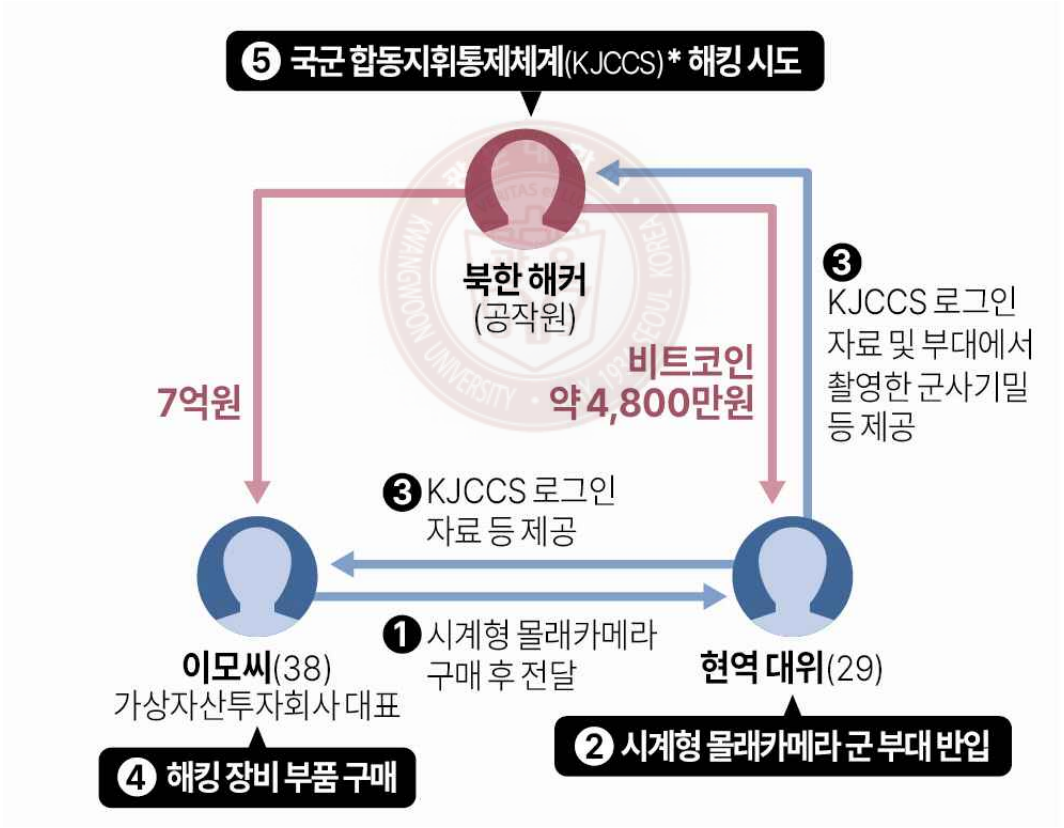
[그림 6] 2016년 군 내부망 해킹 사건 개요

자료: 윤상호, "軍 허술한 보안이 해킹 자초", 동아일보, 2016.12.07.

두 번째 사례는, 2022년 4월 28일 발생한 '한국군 합동지휘통제체계(KJCCS)[10] 해킹 시도사건'이다. 이 사건은 우리나라 군 현역 장교가 직접 간첩행위를 하여 군사기밀을 유출하다 검거된 최초의 사례다. 사건의 개요는 [그림 7]과 같다. 가상화폐 거래소 대표 'A'씨와 현역 장교 'B'씨는 북한 공작원에게

10) KJCCS(Korean Joint Command & Control System): 대한민국 합동참모본부에서 사용하는 지휘, 통제, 통신 및 정보(Command, Control, Communication, computer and Intelligence, C4I) 기능을 수행하는 C4I 체계이다.

포섭되어 군사 2급 비밀인 한국군 합동지휘통제체계(KJCCS) 해킹을 시도하였고 범행 직전 검거되어 해킹은 불발되었지만, 일부 군사기밀은 이미 대포폰 등으로 촬영 후 유출한 이후였다. 이들은 해킹을 위해 [그림 8]과 같은 포이즌 탭을 사용하기도 하였다. 이것은 기판 형태의 소형 PC에 휴대전화 유심칩, SD카드 등을 결합한 후 해킹프로그램을 입력해 PC에 삽입 시 자료 절취 등 해킹을 할 수 있도록 제작되었다.



[그림 7] 2022년 현역 장교 군사기밀 유출 사건 개요

자료: 김영은, "현역 장교 군사기밀 유출 상황도", 연합뉴스, 2022.4.28.

A씨는 KJCCS 해킹을 목적으로 군사기밀 탐지에 사용되는 USB 형태의 해킹 장비(포이즌 탭[11], Poison Tap) 부품을 구매하여 조립한 후 해외에서 북한 공작원이 원격으로 설치할 수 있도록 인터넷 접속이 가능한 자신의 노트북에 연결했다. 이 과정에서 B씨는 A씨와 공작원에게 '한국군 합동지휘통제체계'(KJCCS)의 로그인 자료 등을 제공했다. (김두환, 박호정, "군보안상 해킹대응방안에 관한 연구", 융합보안논문지, 제17권 제5호, pp. 133-142, 2017.)

[그림 8] A씨가 현역 장교 B에 전달한 시계형 몰래카메라(좌)와
A씨가 제작한 해킹 장비(Poison Tap)(우)

자료: 오동준, "충격! 현역 육군 장교 '간첩' 혐의 구속...북에 군사기밀 유출", 국방신문, 2022.04.29.

11) 포이즌 탭: 2016년 유명 해커인 '새미 캄카르(Samy Kamkar)'가 개발한 해킹 장비로, PC의 USB에 연결하면 공격 대상을 원격으로 조정할 수 있게 하는 장비이다.

위 두 사건의 공통점은 사건의 원인이 담당자의 관리 부재 또는 실수에 의한 것이든 아니면 내부자의 고의적인 소행이든 결국 보안시스템 내부에서부터 허점이 발견된 사례라는 것이며 이러한 형태의 공격에는 아무리 철저하게 보안시스템을 구축한다고 하더라도 기존의 보안시스템으로는 허점이 있다는 것을 여실히 보여주고 있다. 물론 시스템 문제 외적으로 보안 규정상 군내 개인 업무 PC에는 기밀자료를 저장할 수 없고, 보안 USB에 별도로 비밀을 저장하도록 규정되어 있는 등 관련 지침을 따르지 않은 인원 또는 악의적으로 내부에서 공격을 시도한 자들 또한 문제이지만, 현실적으로 이런 허술한 방법으로도 얼마든지 독립된 망이 해킹될 수 있다는 사실은 우리에게 시사해주는 바가 크다고 할 수 있다.

만약 앞선 사례에서 시스템 또는 네트워크가 블록체인으로 구축이 되어 있었다면, 기존의 알려진 공격기법 또는 내부자에 의한 해킹은 이루어지지 않았을 것이다. 이제는 국방 정보보안시스템도 첨단기술 기반의 복잡한 미래 환경에 대응하기 위해 새로운 패러다임으로 변화하여야 한다.

다만 지금까지의 논리대로라면 이미 벌써 국방 분야에도 민간과 마찬가지로 블록체인에 관한 연구의 진척도가 상당했어야 했다. 하지만 현실은 빅데이터, AI, 클라우드를 비롯한 타 4차산업 신기술 대비 기술 개발의 진척도가 애무미진하다. 이것은 분명 블록체인이라는 훌륭한 분산 원장 기술을 국방정보체계에 적용할 방법을 찾지 못했기 때문이다.

제2절 블록체인 적용 분야 선정

1. 적용 분야 선정 기준

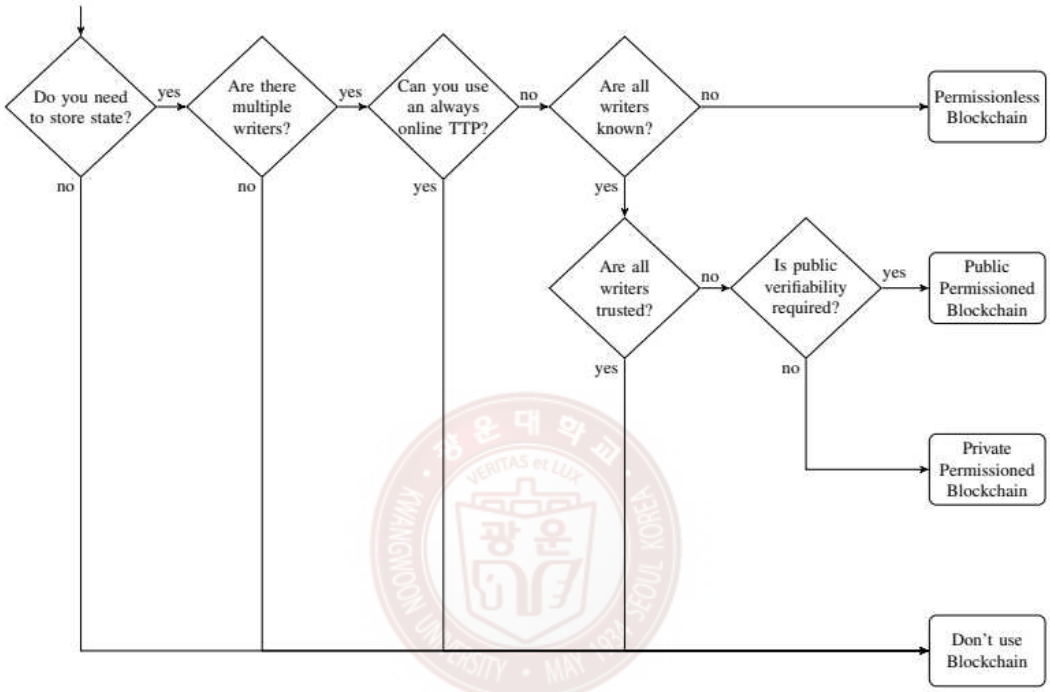
가. 선정 방식

보편적으로 특정 기술을 업무에 적용하려고 할 때, 실무자들은 비용, 안정성, 효율성 등 해당 조직에서 정한 일정한 기준에 따라 기술 도입 여부를 평가한다. 당연히, 평가 시 기술 성숙도가 높은 기술일수록 참고할 사례가 많고, 실제 운용 환경에서 나타날 문제점을 기존 활용 사례에서 찾을 수 있는 등 기술 성숙도가 높은 기술은 실무자가 기술 적용 여부를 상대적으로 쉽게 평가할 수 있다. 하지만, 본 연구에서 국방정보체계에 적용이 필요하다고 주장하는 블록체인 기술은 아직 기술 성숙도가 낮다. 적용사례 대부분은 시험평가, 개념검증(PoC, Proof Of Concept) 단계이다. 기술 도입에 참고할만한 사례가 마땅히 없어 많은 실무자가 일정한 기준 없이 기술 도입 여부를 평가할 수밖에 없다. (안재홍, “블록체인 기술의 군내 도입방안 연구”, 국방과학연구소, p. 40, 2018.)

이러한 고민은 대한민국 보다 서둘러 블록체인이 도입되었던 해외의 블록체인 연구자들도 마찬가지였다. 따라서, 그들은 이것을 해결하고자 블록체인 기술 적용 여부의 판단 지표를 마련하려는 다양한 연구를 하였고 그중 가장 대표적인 방법이 [그림 9]의 Karl Wüst와 Arthur Gervais 가 2018년 Crypto Valley Conference[12]에서 발표한 보고서 Do you need a Blockchain에서 제시

12) Crypto Valley Conference: 크립토 밸리 컨퍼런스는 스위스 루체른 대학교와 비정부 협회인 크립토 밸리가 주관하는 세계 최고의 블록체인 및 암호화 기술 생태계 구축을 위한 회의이다.

한 블록체인 선택 모델이다.



[그림 9] 블록체인 선택 모델

자료: Karl Wüst, Arthur Gervais ,"Do you need a Blockchain", Crypto Valley Conference, 2018.

블록체인 선택 모델은 흐름도(Flow Char)를 따라가며 의사결정을 하는 방식이다. 예를 들어 [그림 9]와 같이 'Karl Wüst, Arthur Gervais 모델'은 6개 평가 항목으로 구성되었다. 각 항목을 따라가면 평가자는 최종적으로 업무에 블록체인을 적용할 것인지, 어떤 블록체인 기술을 적용할 것인지를 결정할 수 있게 된다. 선택 모델은 평가 항목 배치에 따라 최종 결과가 달라진다. 따라서 평가 항목의 내용뿐만 아니라, 각 항목을 적절한 위치에 배치해야만 올바른

결과를 얻을 수 있다. 본 연구에서는 Do you need a Blockchain에서 제시하였던 기본 모델을 그대로 사용하도록 한다.

나. 블록체인 적용 가능 국방정보체계

국방정보화업무훈령 제5조 '국방정보시스템의 범주 및 분류'에서 <표 5>와 같이 국방정보체계의 구성을 정의하고 있다.

<표 5> 국방정보시스템의 범주 및 분류

대분류	중분류	소분류	주요 해당시스템
전장관리 정보체계	지휘통제체계		연합지휘통제체계(AKJCCS) 합동지휘통제체계(KJCCS) 지상전술C4I체계(ATCIS) 후방지역지상전술C4I체계(ATCIS-R) 해군전술C4I체계(KNCCS) 공군전술C4I체계(AFCCS)
	전투지휘체계		대대급이하전투지휘체계(B2CS) 포병대대 전술지휘체계(BTCS) 전구합동화력운용체계(JFOS-K) 해군전술자료처리체계(KNTDS) 공군자동화방공체계(MCRC) 위성전군방공경보체계
	군사정보체계		군사정보통합처리체계(MIMS) 연합군사정보유통체계(MIMS-C) 군사지리정보체계(MGIS)
자원관리 정보체계	기획재정 정보체계	기획	국방통계DW체계 조직정원관리시스템
		재정	국방통합재정정보체계

대분류	중분류	소분류	주요 해당시스템
			급여관리체계
		정책기획	정보의제관리시스템
		정보화	국방정보자원관리시스템(DRIMS) 국방정보화사업관리체계(PIMS) 상호운용성포털(DIPS) 국방아키텍처관리체계(MND-ARMS)
	인사동원 정보체계	인사	국방통합인사정보체계 e-사람(행안부체계) 군무원채용/시험/인사관리시스템 성과관리시스템
		교육	정훈교육원격지원체계 생도학사관리통합정보체계 교육훈련종합정보시스템
		동원	국방동원정보체계
		복지보건	국방의료정보체계(DEMIS) 의료영상저장전송장치(PACS) 의료종합정보체계(간사교등) 종합의료정보시스템 군전염병정보체계 군인연금체계
	군수시설 정보체계	군수통합	군수통합정보체계 국방전시군수정보체계
		장비정비	육군장비정비정보체계(보급창,정비관리등) 해군장비정비정보체계(함정정비,잠수함정비등) 공군장비정비정보체계(항공기정비,장비관리등)
		탄약	국방탄약정보체계
		물자	국방물자정보체계 육군보급관리/보급창정보체계 해군보급관리/항공종합정보체계 공군보급관리체계
		수송	국방수송정보체계
		조달	국방전자조달체계 부대조달정보체계 통합사업관리정보체계
		시설	국방시설통합정보체계

대분류	중분류	소분류	주요 해당시스템
국방M&S 체계	연습·훈련용		태극 합동전장모의모델(태극JOS) 창조21 청해 창공 천자봉 전투21 화랑21 보라매 과학화전투훈련체계(KCTC) 공중전투기동훈련체계(ACMI)
	분석용		통일분석모델(JOAM-K) 장차작전간이분석모델(SAMFO) 전시자원소요산정모델 전투표본생성모델(COSAGE) 합동작전분석모델(JICM) 전구급공중전분석모델(STORM) C4ISR효과분석모델 비전21 육군항공분석모델 한국형 전시자원소요산정모델 성분작전/전시자원소요분석모델 작전탄약소요산정평가모델 지상무기효과분석모델(AWAM) 전구급방공작전 분석모델(EADSIM) 전구급해상전분석모델(ITEM) 여단급이하전투효과분석모델(OneSAF)
	획득용		JANUS 적외선 탐색기 유도탄모의 비행시험 시스템 AMIOS 함대공 교전 효과도 분석모델 전차 가상운용 시뮬레이터 잠수함 작전효과도 분석모델 어뢰음향대항체계시뮬레이터

대분류	중분류	소분류	주요 해당시스템
			공대공 전투효과도 분석모델 합성전장 3D 전투모의기술
기반운영 환경	정보통신망	고정통신망	국방광대역통합망(M-BcN) 전군화상회의(VTC)망 전화교환망 마이크로웨이브망 인트라넷망 인터넷망 기무망 정보망 특수부대통신망 재해통신망
		기동통신망	전략기동통신노드 전술통신체계(SPIDER) 전술정보통신체계(TICN) 공중중계UAV 전투무선망
		위성통신망	군위성통신체계(ANASIS) 해상작전위성통신체계(MOSCOS)
		전술데이터 링크체계	합동전술데이터링크체계(JTDLS) 지상전술데이터링크(KVMF)

자료: 국방부(정보화기획담당관), “국방 정보화업무 훈령”, 국방부훈령, 제2649호, 2022.5.6.

이처럼 수많은 시스템 분류 가운데 블록체인과 시너지 효과가 있을 것으로 판단되는 분야를 중분류 수준에서 정리하여 선정 후보군을 식별하면 군수관리, 기록관리, 전장 정보관리, 연동체계 분야로 추려진다. 해당 분야는 군내에서 데이터 무결성 및 분산 환경이 요구되는 시스템을 기준으로 식별하였다.

그리고 최종적으로 하나의 적용 대상을 선정하기 위해 간추려진 분야의 특징 및 기대효과를 정리하면 <표 6>과 같은 국방 블록체인 적용 대상체계 선정 기준표를 얻을 수 있다. 본 연구는 이 표를 통해 블록체인의 무결성, 분산

서버, 신원 관리 등의 특성과 가장 시너지 효과가 있을 분야는 연동체계로 판단하였으며 그 이유는 '3장-2절-2-나'에서 논의한다.

<표 6> 국방 블록체인 적용 대상체계 선정기준표

특징	군수관리	기록관리	전장 정보관리	연동체계
저장 데이터	• 물자 획득 계약 정보 • 물자 생산 정보 • 실시간 위치 정보	• 문서 정보 • 문서 관리 정보 • 문서 이력 정보	• 생체 정보 • 메시지	• 연동통제문서[13] 정보 • Meta Data[14] • 연동 Log
네트워크 구성	• 블록체인 노드 • 부착식 소형 태그 • 물자 인식 단말	• 블록체인 노드 • 개인 문서 작성 단말 • 문서 저장 서버	• 블록체인 노드 • 사용자 단말 • 전투무선망용 소형기기	• 블록체인 노드 • 연동 서버
통신 데이터	• 군수 재고 정보 • 군수 이동 정보	• 문서 기록 • 문서 접근 로그	• 개인의 생체 정보 • 실시간 생체 이력 • 각종 실시간 메시지	• 연동체계 기준정보 • Meta Data • 연동 Log
핵심 기대효과	• 청구, 수불, 정비 등 군수물자의 수명주기 과정에서 생성되는 정보를 블록체인에 저장함으로써 군수 데이터 무결성 보장 및 업무 자동화 가능	• 블록체인에 공문서/공공 기록을 보관함으로써 기록 위·변조 방지	• 실시간/이동형 전장 정보를 블록체인에 저장하여 체계 생존성 향상, 데이터 무결성 보장	• 체계 간 연동에 필요한 기준정보, Meta Data, Log 정보 등을 블록체인에 저장하여 연동의 신뢰성 및 생존성 향상 • 블록체인 네트워크를 통한 연동 대상 노드의 접근통제 가능
적용 가능 체계	• 국방군수통합정보체계 • 군수품현장관리자동화체계 • 국방수송정보체계	• 국방부기록관리시스템 • 온나라시스템 • 보안나라 • 국방획득정보체계	• 전술정보통신체계	• 국방통합연동관리체계(DIMS) • 통합연동모듈(IIM) • 국방군수통합연동모듈

13) 연동통제문서(ICD, Interchange Control Document): 연동체계 상호 간 연동 합의에 따라 주고받을 연동 메시지의 통제기법부터 구조까지 모든 것을 정의하는 문서로 연동체계에서는 메타데이터를 생성하기 위한 기본 정보가 된다.

14) 메타데이터(Meta Data): 데이터에 관한 구조화된 데이터로, 대량의 정보 가운데에서 확인하고자 하는 정보를 효율적으로 검색하기 위해 원시데이터(Raw Data)를 일정한 규칙에 따라 구조화 혹은 표준화한 정보를 의미

2. 국방연동체계의 블록체인 적용

가. 국방연동체계 개념

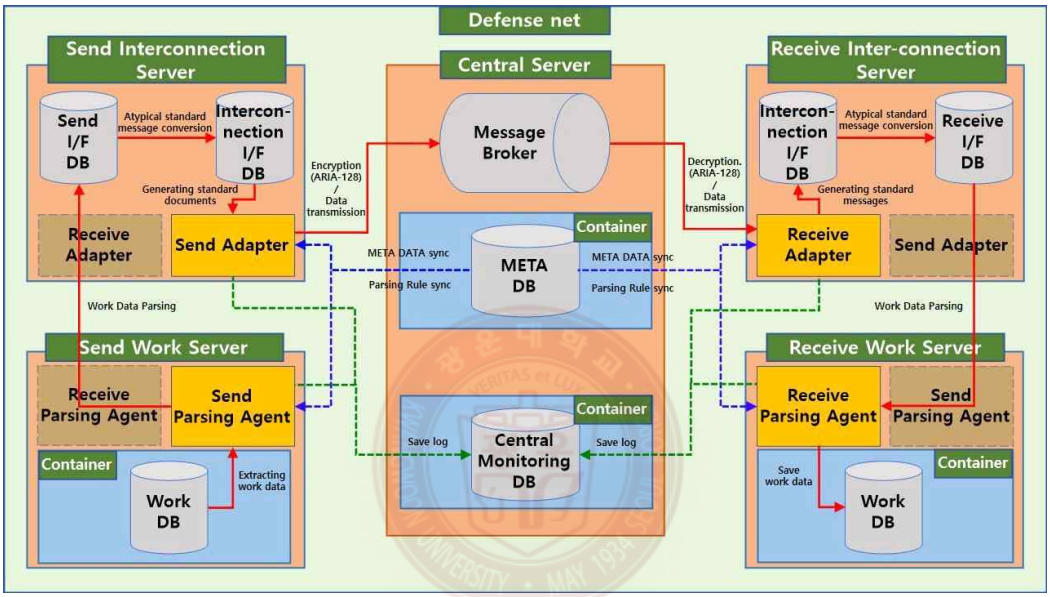
대한민국 국군의 네트워크 중심 정보공유 환경(NCE, network centric environment)중 국방 정보체계는 전장관리정보체계(지휘통제, 전투지휘, 군사정보체계), 자원관리정보체계(기획·재정, 인사·동원, 군수·시설, 전자행정, 군사정보지원, 상호운용성), 국방M&S체계(연습·훈련용, 분석용, 획득용) 등 분야별로 수십 가지의 크고 작은 정보체계들로 이루어져 있다. 또한, 이렇게 필요에 따라 다양한 형태로 개발된 정보체계들은 각각 의존적인 관계에 있으며 상호운용성 관점에서 유기적으로 연동 기술을 통해 하나로 연결되어 있다.

국방정보체계의 연동개념은 크게 두 가지로 구분된다. 첫 번째는 [그림 10]과 같이 업무적인 연관성보다는 순수하게 데이터 또는 정보의 전달만을 목적으로 하는 방식이다. 이 방식은 enterprise application integration(EAI)[15] 및 EAI Hub & Spoke[16] 방식 그리고 enterprise service bus(ESB) 아키텍처로 구현되며 소켓 통신을 통해 비실시간 연동을 서비스한다. 현재 군에서 운용중인 대부분의 연동 모듈이 이에 속한다. 두 번째는 [그림 11]처럼 각각 End-Node 사이에서 발생하는 단순한 형태의 데이터 송·수신뿐만 아니라 분산된 시스템을 하나의 업무 프로세스로 묶어 사용자는 마치 통합된 하나의 시스템을 실시간으로 사용하는 듯 느낄 수 있도록 하는 개념으로

15) EAI(Enterprise Application Integration) : 전사적 응용프로그램 통합, Point to Point 방식의 mesh topology를 사용

16) EAI Hub & Spoke : 전사적 응용프로그램 통합의 한 유형으로, star topology의 형태로 구현

representational state transfer(REST) application programming interface(API)[17] 또는 simple object access protocol(SOAP)[18] 아키텍처 기반으로 통합된 실시간 서비스를 제공한다.



[그림 10] EAI Hub & Spoke 기반 국방 연동체계 구조

자료: 박용탁, “국방정보체계 실시간 서비스 통합 방안 연구”, 선진국방연구, 2021.

국방 정보체계에 전력화된 연동체계는, 전장망에서는 Korean message text format(KMTF) 2.0[19] 기반 integrated interoperability module(IIM)[20]이 자원

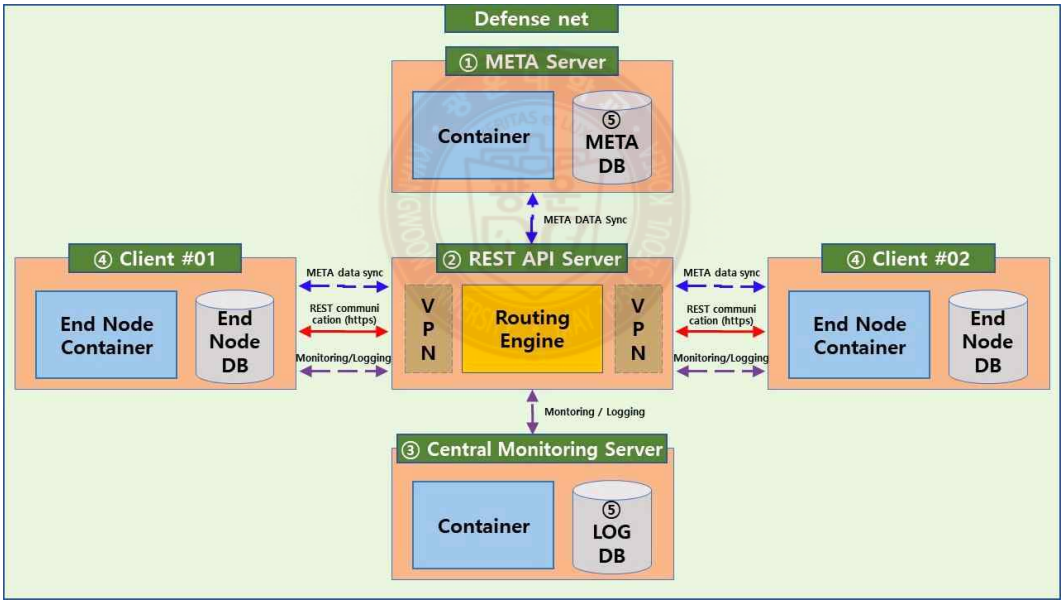
17) REST(Representational State Transfer) : 분산 하이퍼미디어 시스템을 위한 소프트웨어 아키텍처의 한 형식

18) SOAP(Simple Object Access Protocol) : HTTP, HTTPS, SMTP 등을 통해 XML 기반의 메시지를 컴퓨터 네트워크상에서 교환하는 프로토콜

19) KMTF(Korean Message Text Format) : 한국형 메시지 텍스트 포맷

20) IIM(Integrated Interoperability Module) : KMTF 메시지 기반으로 개발된 통합연동모듈로 전장망에서 주로 사용

망에서는 국방연동관리체계(DIMS, Defense Interconnection Management System)[21]가 각각 표준으로 사용되고 있다. 또한 일부 체계들은 국방군수통합(DELIIS, Defense Logistics Integrated Information System) 연동 모듈[22]과 같이 개별 체계에서 자체 개발 또는 민간 솔루션을 도입하여 연동체계를 운용중이다. 이들 연동시스템은 대부분 EAI 또는 EAI Hub & Spoke 아키텍처를 토대로 개발되어 미리 정의된 대량의 데이터 송·수신에 적합하다. (박용탁, "국방정보체계 실시간 서비스 통합 방안 연구", 선진국방연구, 2021.)



[그림 11] 국방 REST API Server 참조모델

자료: 박용탁, "국방정보체계 실시간 서비스 통합 방안 연구", 선진국방연구, 2021.

---

21) DIMS(defense interconnection management system) : 국방연동관리체계로 자원망에서 사용

22) DELIIS(defense logistics integrated information system) 연동 모듈 : 군수체계에서 사용하는 자체 개발 연동 모듈로 Socket, Webservice, 망전환(XML 형태의 파일 교환) 등 지원

다음은 [그림 11]의 국방 REST API Serer 기준 구성 요소에 대한 상세 설명과 함께 각 요소에서 블록체인이 어떤 방식으로 적용될지 간략하게 정리한다.

① Meta Server: 서버 정보, Meta 정보 등 연동에 필요한 중요 정보를 각 Node에 동기화한다. 블록체인 적용 시 해당 정보의 신뢰성을 높일 수 있고 분산 서버를 통해 가용성을 확보할 수 있으며 추가적인 동기화 작업 소요를 줄일 수 있다.

② REST API Server: Client로부터 JSON Message를 받으면 Meta Server의 WSDL 명세를 참조하여 Message를 해석 및 검증 후 목적지로 Routing 한다. 블록체인 적용 시 REST API Server에 블록체인 SDK를 적용하여 Client와 블록체인 네트워크 간 통신을 지원할 수 있다.

③ Central Monitoring Server: 중앙관제 서버로서 REST API Server 및 각 End Node에서 이루어지는 모든 작업의 이력을 기록하며 연동에 필요한 각종 관제 및 명령을 수행한다. 블록체인 적용 시 각종 이력 정보의 신뢰성과 투명성을 확보할 수 있다.

④ Client: REST API Server를 통해서 실시간 통합되는 대상체계로 End Node 또는 Client라고 부른다. Client는 블록체인 네트워크에 참여자로 멤버십 관리의 대상이 된다. 멤버십 관리에서 권한을 얻은 대상만이 블록체인의 CA[23]를 통해 인증서를 발급받고 네트워크에 참여할 수 있다.

---

23) CA(Certification Authority): PKI(Public Key Infrastructure) 기반 암호화 통신을 위한 인증기관이며, 공개키인증서 및 이에 대응하는 개인키를 발급한다. 블록체인 네트워크를 구성하는 조직에는 루트 인증서를, 블록체인 네트워크에 접속하는 사용자에게는 신원 등록 인증서를 발급한다.

⑤ Meta DB / Log DB: 연동에 필요한 Meta 정보 및 이력 정보를 저장하고 있는 데이터베이스로 일반적으로 RDBMS와 UDDI[24]를 사용한다. 해당 구조를 블록체인으로 대체한다면 비가역적인 신뢰성 있는 정보를 유지 할 수 있다.

또한, 국방 REST API Serer에 블록체인을 적용하기 전과 후의 차이에 대해서 각 구성 요소 별로 정리하면 <표 7>과 같이 다양한 부분에서 장점이 있음을 알 수 있다.

<표 7> 국방 REST API Server 구성 요소의 블록체인 적용 전/후 비교

구성 요소	블록체인 적용 전	블록체인 적용 후
Meta Server	• 관리자 임의로 Meta 정보 변조 가능 • Meta 정보 동기화를 위해 주기적으로 전 네트워크에 데이터 송신 • Meta Server 단절 시 전체 시스템 마비	• 관리자도 임의로 합의되지 않은 Meta 정보 변경 불가 • 불필요한 동기화 작업 소요 절감 • 분산 서버로 인한 시스템 가용성 향상
REST API Server	• 기밀성을 위해 별도의 암호화 솔루션 도입 필요	• 플랫폼에서 제공하는 SDK를 통해 블록체인 네트워크와 통신 • PKI 기반으로 암호화된 gPRC 통신
Central Monitoring Server	• 이력 정보를 RDBMS에 저장 • 관리자 임의로 연동 이력 변조 가능	• 연동 이력 변조 불가능
Client	• Meta Server의 연동체계 정보를 통해 Client 접근 권한 통제	• 블록체인 네트워크 자체 CA/멤버십 기능을 통해 Client 접근 권한 통제
Meta DB / Log DB	• 데이터 저장소로 RDBMS 사용 • 관리자 임의로 수정 가능	• 데이터 저장소로 블록체인 사용 • 관리자도 데이터 수정 불가

24) UDDI(Universal Description, Discovery and Integration): 웹 서비스를 위한 전역 비즈니스 레지스트리이다. 연동에서는 Client의 서비스 정보를 등록하는 XML 기반의 등록 저장소이다.

나. 국방연동체계의 블록체인 적용 선정 사유

본 연구는 '3장-2절-1-가~나'를 토대로 국방 분야에 블록체인을 적용하기 위한 대상으로 국방연동체계를 선정하였다. 선정 사유는 다음과 같다.

① 블록체인 선택 모델에 의하면 국방정보체계는 허가형 블록체인을 통한 시스템 구축이 적합할 것으로 판단

② 국방연동체계의 Meta Data, Log, 서버 정보 등의 관리에 블록체인의 비가역적 특성 및 무결성을 응용하기에 적합

③ 블록체인은 분산 데이터베이스이므로 연동에 참여하는 체계들이 언제나 최신화된 연동 정보를 유지하기에 유리함. 연동합의서 등 연동의 관리정보 동기화를 위한 추가작업 불필요

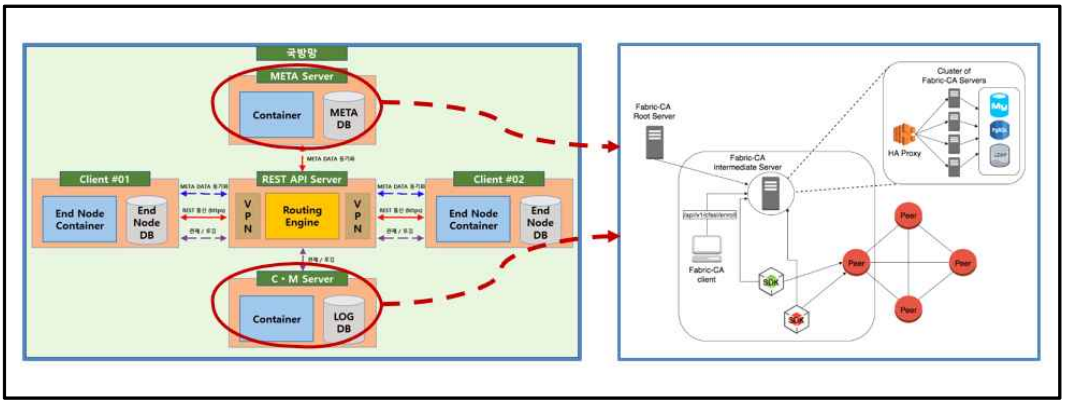
④ 블록체인의 신원인증 기능인 멤버십 관리를 통해 허가된 노드만 네트워크에 접근할 수 있으므로 신뢰성 있으며 책임추적이 가능한 연동 네트워크 구축 가능(멤버십 관리 기능이 있는 플랫폼에 한정)

⑤ 국방연동체계는 비교적 단순한 형태의 정보를 대량으로 관리해야 하므로 블록체인 Ledger를 적용하기에 적합

⑥ 비즈니스 로직이 간단하여 Meta Data, Log 관리, 접근통제 관리, 암호화 등의 요소만 모듈식으로 구현하기에 적합

⑦ 국방연동체계는 전 군을 대상으로 운용되므로 대상이 되는 정보체계들에 블록체인의 경험을 제공하여 생소한 국방 블록체인의 저변 확대에 적합

[그림 12]는 국방연동체계에 블록체인을 적용하는 방법을 표현하였다.



[그림 12] 국방연동체계의 블록체인 적용도

자료: Hyperledger fabric read the docs 내용을 활용하여 재구성

기존 Meta 서버, 중앙관제 서버를 블록체인으로 대체하여 연동 서버를 구축한다. Client는 허가형 블록체인의 접근통제 기능을 통해 연동 서버에 접근하며 스마트 계약으로 DATA에 접근한다. 이때 연동 대상 체계들은 블록체인의 Client로서 기능을 할 수도 있고 피어 노드로 네트워크에 참여할 수도 있다. Client는 블록체인을 적용하기 전에 사용하던 기존 프로그램을 변경 없이 REST API Server와 RESTful[25]로 통신하며 REST API Server는 Client의 request[26]를 받으면 블록체인 SDK[27]를 통해 블록체인 네트워크에 접근한다. 따라서 Client 들은 추가적인 개발 노력을 최소화한 상태로 블록체인 서비스에 참여할 수 있다. 이와 관련된 자세한 논의는 아래 '4장-1절-2'에서 국방 블록체인 모델설계를 통해 상세하게 진행하도록 한다.

---

25) RESTful: 일반적으로 REST라는 아키텍처를 구현하는 웹 서비스를 말하며, REST API를 제공하는 웹 서비스를 RESTful 하다고 표현한다. 즉, RESTful은 REST API의 구현체이다.

26) request: 클라이언트에 의해 서버로 전송되는 메시지 요청

27) SDK(Software Development Kit): 소프트웨어 개발자가 특정 운영체제용 응용프로그램을 만들 수 있게 해주는 소스(Source)와 도구 패키지이다.

제3절 개발 플랫폼 선정

1. 개발 플랫폼 선정 방법

블록체인 기술을 군에 적용하려면 블록체인 플랫폼을 직접 개발하거나 군에 적합한 상용 오픈소스 플랫폼을 도입해야 한다. 블록체인 플랫폼을 직접 개발하면 군 환경에 최적화된 체계를 개발할 수 있다는 장점이 있지만 독자 개발은 상대적으로 많은 시간과 비용이 소모된다는 단점이 존재한다. 따라서, 빠른 기간 내 블록체인 기술을 군에 도입하기 위해서는 이미 민간에서 많이 사용중인 상용 오픈소스 플랫폼을 적극적으로 활용해야 한다. 이번 절에서는 다양한 오픈소스 블록체인 플랫폼을 비교 분석하여 군에 가장 적합한 오픈소스 플랫폼을 선정하고자 한다. 선정 과정은 2018년 국방부 차원에서 연구했던 '블록체인 기술의 군내 도입방안 연구'를 참고하였으며 그 순서와 상세 내용은 아래와 같다.

① 비교 분석 대상 선정
② 플랫폼 비교 분석 기준 설정
③ 플랫폼 비교 분석
④ 분석 결과 최상위 점수 플랫폼을 군에 적용

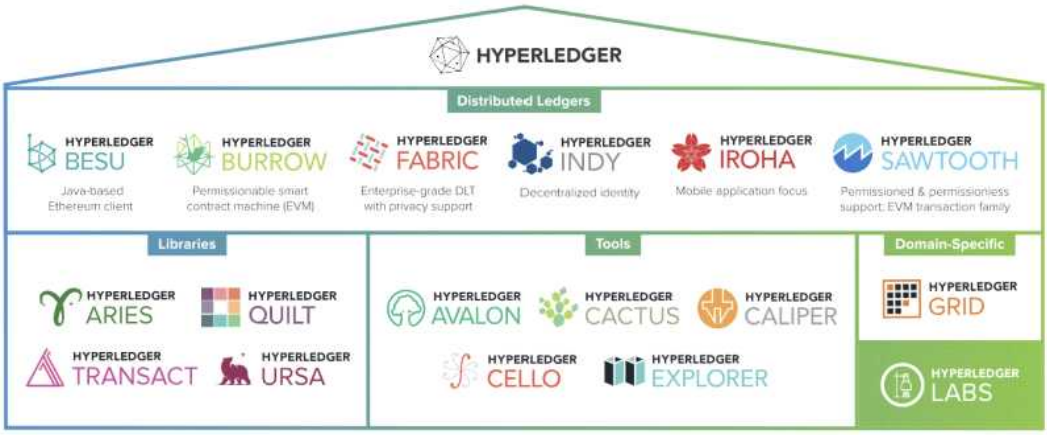
비교 분석 대상은 총 3개로 이더리움(Ethereum), 클레이튼(KLAYTN), 하이퍼레저 패브릭(Hyperledger Fabric) 이다. 대상 플랫폼은 국내외에서 엔터프라이즈용 블록체인 플랫폼으로서 가장 널리 알려진 것들이다.

2. 하이퍼레저 패브릭 개념

가. 하이퍼레저 프로젝트

하이퍼레저 프로젝트는 리눅스 재단에서 주관해 세계 여러 기업이 참여하여 개발하고 있는 범 산업용 분산원장 표준화 프로젝트이며 블록체인 오픈소스 프로젝트로 금융, 사물 인터넷, 물류, 제조 및 다양한 기술 분야 등 여러 산업 전반에 걸쳐 응용할 수 있는 블록체인 기술을 만드는 것이 목표다.

하이퍼레저는 주로 기업결제, 상품추적 및 관리 등을 위한 엔터프라이즈 플랫폼으로서 블록체인 기술이 갖춰야 할 기능들에 집중하고 있다. 대표적인 참가 기업으로는 액센츄어, 시스코, IBM, 인텔, J.P.Morgan 등이 있고 블록체인 유관 기업으로는 R3, DA, ConsenSys, Blockstream 등이 있다. 국내 기업으로는 한국예탁결제원, 삼성SDS, 코스콤, 블로코, 코인플러그 등이 있다.



[그림 13] 하이퍼레저의 프로젝트 구성

자료: Hyperledger official site

현재 하이퍼레저 산하에는 [그림 13]과 같은 10여 가지가 넘는 블록체인 프로젝트가 진행되고 있으며, 분산원장을 위한 프레임워크와 라이브러리, 도구, Domain-Specific으로 구성되어 있다. 본 연구에서 선정한 하이퍼레저 패브릭 프레임워크 또한 이 중 하나의 프로젝트이다.

나. 하이퍼레저 패브릭

하이퍼레저 패브릭은 모듈러 아키텍처 기반의 애플리케이션 개발 프레임워크로 합의 알고리즘, 멤버십 서비스 등의 구성 요소를 플러그 앤 플레이 방식으로 구현할 수 있도록 지원한다.

그리고, 하이퍼레저 패브릭은 Java, Go, Python, Node.js 등 일반적인 프로그래밍 언어 기반의 체인코드(스마트 컨트랙트)를 지원하여 개발자는 블록체인 네트워크에서 블록 생성 시 작동될 핵심 프로그램을 편리하게 개발할 수 있으며 이러한 체인코드의 특성으로 프로젝트의 용역 개발 시 개발자 수급과 유지관리의 안정성에 매우 큰 장점이 있다.

또한, 하이퍼레저 패브릭은 여러 가지 커스터마이징 가능한 옵션을 제공한다. 원장 데이터(World State DB)는 CouchDB, LevelDB 중 해당 프로젝트에서 원하는 형태로 저장할 수 있으며, 합의 알고리즘 또한, Kafka, Raft 등 지원되는 알고리즘 중 선택하여 원하는 방식으로 오더링 서비스를 구현할 수 있도록 설계되어 있다. 이외에도 MSP(Membership Service Provider) 기술을 활용하여 블록체인 네트워크에 대한 권한 관리를 위해 서명, 인증, 검증 등 다양한 접근 통제 기법으로 확장성을 제공한다.

하이퍼레저 패브릭 프로젝트는 다음과 같은 세 가지 목표가 있다.

① 허가된 참여자에게만 접근을 허용하는 엔터프라이즈용 블록체인
② 여러 분산 애플리케이션 서비스의 다양한 요구사항을 효율적으로 지원할 수 있는 개발 플랫폼
③ 모듈러 아키텍처 기반 분산 응용 플랫폼(블록체인 서비스, 멤버십 서비스, 체인코드 서비스의 각종 모듈을 필요에 따라 교체)

그리고 이러한 목표에 따라 아래 다섯 가지의 특징을 가진다.

① 허가형(Permissioned) 블록체인 : 하이퍼레저 패브릭은 MSP를 통해 허가된 참여자만 접근을 허용하고, 접근 권한을 제어할 수 있다. 이를 통해 폐쇄망 형태의 프라이빗 블록체인을 구성하는 데 최적화되어 있다. 이와 달리 퍼블릭 블록체인의 대표 주자인 비트코인과 이더리움의 경우 네트워크에 참여를 원하는 누구나 참여할 수 있다.

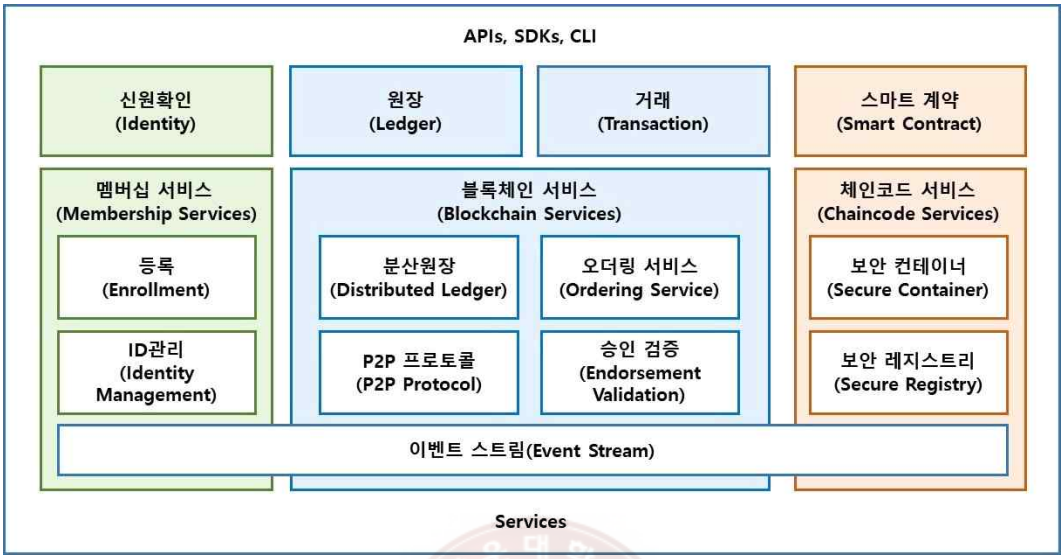
② 일반 프로그래밍 언어 사용 : 하이퍼레저 패브릭은 별도의 전용 프로그래밍 언어를 사용하지 않고, Go, 자바 등 범용성이 높은 언어로 개발한다. 이더리움의 경우 스마트 컨트랙트를 개발하기 위해서 전용 언어인 솔리디티를 사용해야만 한다. 그 이유는 이더리움은 블록체인의 비결정적 오류를 솔리디티를 통해 해결하여 모든 노드에서 실행된 스마트 컨트랙트의 결과를 항상 동일하게 보장하기 때문이다. 하이퍼레저 패브릭의 경우는 내부 키의 상태 변화 값에 의해 비결정적 오류를 해결한다.

③ 높은 성능 : 하이퍼레저 패브릭은 서로 다른 엔도싱 피어 노드에게 체인코드를 실행시키도록 할 수 있다. 이 과정에서 키에 대한 버전관리를 통해 동시처리에 따른 비결정적 실행 문제점을 해결해 높은 성능을 낼 수 있다. 반면 기존 비트코인이나 이더리움과 같은 블록체인은 채굴자들이 채굴하고 네트워크상에 있는 풀 노드에 채굴된 블록을 보내 검증해야 한다. 이런 작업 뒤에 스마트 컨트랙트를 실행하기 때문에 상대적으로 속도가 느리다.

④ 교체 가능한 모듈러 아키텍처 : 하이퍼레저 패브릭은 신원확인, 분산원장, 트랜잭션, 체인코드 등 네 가지 컴포넌트로 분류되어 있으며 상세 기능들은 모듈화 구성되어 있다. 따라서, 네트워크 구성 시 개발자에게 다양한 옵션을 제공하여 비스니스 목적에 맞는 형태로 블록체인 플랫폼을 구축할 수 있도록 한다. 예를 들어 오더링 서비스 노드에서 Solo, Kafka, Raft의 세 가지 합의 알고리즘 중 하나를 선택하여 순서화를 개발할 수 있다.

⑤ 멀티 블록체인 지원 : 하이퍼레저 패브릭은 채널이라는 분할된 네트워크로 멀티 블록체인을 지원한다. 하나의 블록체인 네트워크를 논리적으로 독립된 여러 개의 블록체인으로 분할 할 수 있다.

앞서 언급한 특징과 같이 하이퍼레저 패브릭에서 제공하는 레퍼런스 아키텍처는 [그림 14]처럼 컴포넌트 단위로 구성되어 있다. 레퍼런스 아키텍처를 이루는 신원확인, 분산원장, 트랜잭션, 체인코드의 상세 내용은 다음과 같다.



[그림 14] 하이퍼레저 패브릭 아키텍처 구성

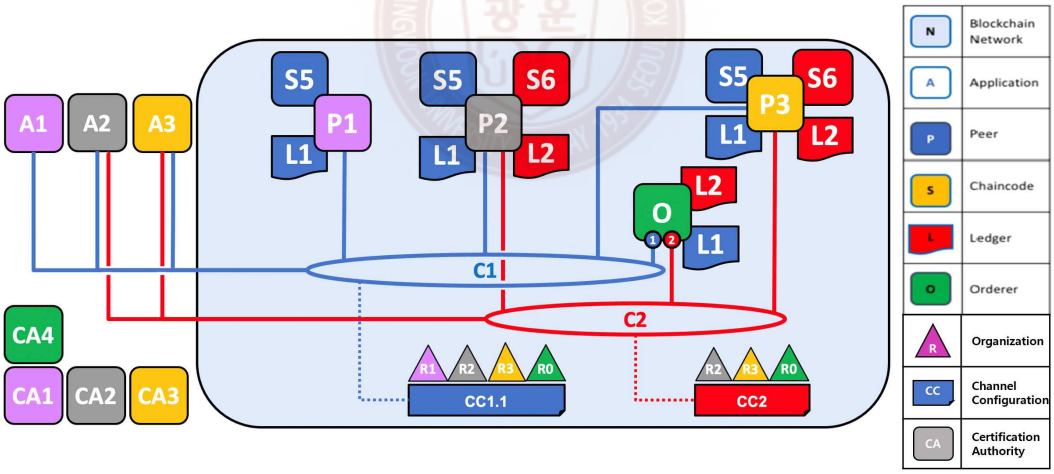
자료: Hyperledger fabric read the docs 내용 참고하여 재구성

❖ 신원확인 : 사용자가 하이퍼레저 패브릭의 네트워크에 접속하려면 신원확인을 가장 먼저 해야한다. 그 이유는 하이퍼레저 패브릭은 폐쇄형 구조인 프라이빗 블록체인을 지향하고 있으며 권한을 가진 참여자만이 분산원장에 데이터를 기록, 수정, 삭제할 수 있기 때문이다. 신원확인은 MSP를 통해 이뤄진다.

❖ 원장 : 원장은 블록에 트랜잭션 정보가 실제 저장되는 공간으로 블록체인의 데이터를 관리하는 분산 원장 데이터베이스를 말한다. 하이퍼레저 패브릭의 원장은 현재 상태를 나타내는 World state DB와 원장의 생성 시점부터 현재까지의 사용 기록을 저장하는 블록체인 두 가지로 구성된다. 또한 한 채널 안에 속한 피어 노드는 동일한 원장의 복사본을 가진다. 원장은 업데이트되며 채널 안에서 합의를 통해 일관성을 유지한다.

❖ 트랜잭션 : 트랜잭션은 스마트 컨트랙트인 체인코드의 실행을 의미한다. 트랜잭션 시에는 엔도싱 피어 노드를 통해 보증검증을 하고 오더링 서비스 노드를 통해 프라이빗 블록체인 네트워크에 참여하고 있는 모든 피어 노드에 분기하는 역할을 한다.

❖ 체인코드 : 체인코드는 하이퍼레저 패브릭의 스마트 컨트랙트다. 체인코드를 통해 프라이빗 블록체인에서 기업 및 컨소시엄으로 구성된 서비스에 맞게 블록체인을 활용할 수 있도록 비즈니스 로직을 구현할 수 있다. 하이퍼레저 패브릭은 이와 같은 비즈니스 로직을 구현할 수 있도록 다양한 개발 언어를 지원하고 있는데, Go, Node.js, Java 등을 지원한다.



[그림 15] 하이퍼레저 패브릭 네트워크 구조

자료: Hyperledger fabric read the docs

하이퍼레저 패브릭의 네트워크 구조는 [그림 15]와 같이 구성되며 Client, Peer, Orderer, CA, channel 등 요소별 상세 내용은 아래와 같다.

❖ 클라이언트(Client) : 웹 또는 DApp(Decentralized Application) 등을 통해 블록체인 네트워크에 트랜잭션을 발생시키는 주체

❖ 노드(Node) : 일종의 물리적인 시스템 단위로 블록체인 네트워크를 구성하는 서버. 노드의 종류에는 피어 노드와 오더링 서비스 노드가 있다.

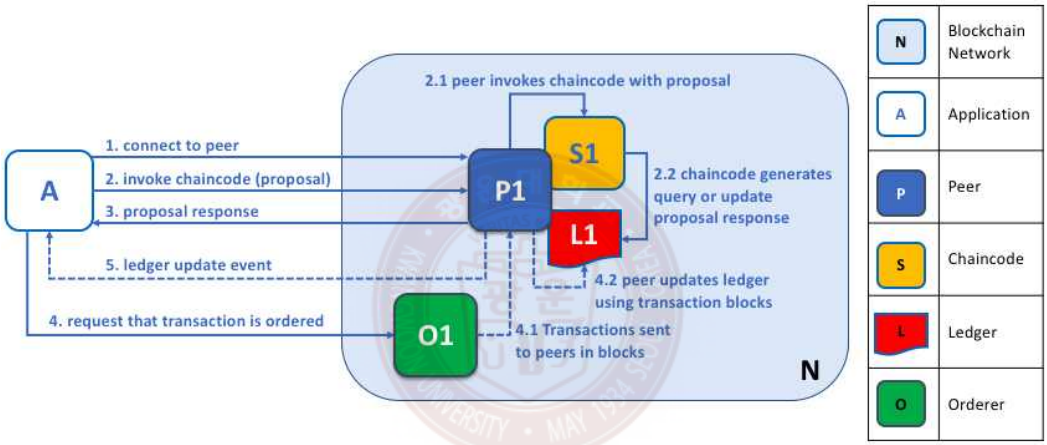
❖ 피어 노드(Peer Node) : 가장 기본적인 네트워크 구성 요소로, 블록체인 네트워크를 유지하고 트랜잭션의 제안 및 응답을 처리하며, 원장과 체인코드를 관리하고 저장하는 임무를 수행한다.

❖ 오더링 서비스 노드(Ordering Service Node) : 네트워크 내의 채널에 대한 구성 정보를 소유하고, 이를 기반으로 전체 시스템의 관리자 임무를 수행하며 피어 노드에 트랜잭션을 전달해 전체 블록체인 네트워크가 작동하도록 제어하여 네트워크에 참여하고 있는 모든 피어 노드의 분기 및 정렬 역할을 하는 노드. 즉, 동시다발적으로 발생하는 트랜잭션의 순서를 관리하고 검증된 트랜잭션을 이용해 최종적으로 블록을 생성한다. 이 과정에서 합의 알고리즘에 따라 클라이언트로부터 발생하는 거래를 순서화시켜 피어 노드에 전달하여 모든 거래가 안전하게 수행되는 것을 보장한다.

❖ 조직(Organization) : 네트워크는 조직 단위로 구성되는데, 조직 별로 피어 노드 관리 및 권한 부여, 보증 정책 등을 수행하며, 클라이언트 등 참여자의 접근 권한도 관리한다.

❖ 채널(Channel) : 네트워크에서 구성 요소간 그룹을 나눠 트랜잭션을 수행해야 할 때 사용한다. 트랜잭션의 접근 권한을 그룹별로 설정하고 관리하는 중요한 프라이빗 블록체인의 기술 요소다.

하이퍼레저 패브릭의 트랜잭션은 [그림 16]과 같이 작동한다.



[그림 16] 하이퍼레저 패브릭의 트랜잭션 흐름

자료: Hyperledger fabric read the docs

① 클라이언트 애플리케이션에서 피어 노드로 통신 연결

② 피어 노드에서 체인코드 실행

③ 피어 노드에서 클라이언트로 응답

④ 오더링 서비스 노드를 통해 합의 및 블록 처리

위와 같은 특징으로 인해 하이퍼레저 패브릭은 엔터프라이즈 환경에서 가장 범용적인 블록체인 기술로 채택되어 사용되고 있다.

3. 개발 플랫폼 선정 및 기준

국방 블록체인 플랫폼 선정기준은 개발, 관리, 성능 세 가지로 구분했다. 개발 기준은 해당 플랫폼을 사용해 개발할 때 고려해야 할 사항이나 개발 과정에 영향을 줄 수 있는 사항이며, 관리 기준은 개발 또는 유지 보수 과정 중 관리 측면에서 고려해야 할 사항이고, 마지막으로 성능 기준은 플랫폼 자체의 기능 및 성능과 관련된 사항이다. 비교분석 기준 세부 사항은 아래와 같다.

가. 내부망 활용 가능성

내부망 활용 가능성이란 해당 플랫폼을 내부망 환경에서 개발 및 활용할 수 있는지에 대한 기준이다. 가령 어떤 플랫폼이 PoW 방식의 합의 알고리즘만을 사용한다면, 그 플랫폼은 내부망 환경에서 사용하기에 적절하지 않다. 왜냐하면 PoW 방식은 노드들이 서로의 신원을 알 수 없는 환경에서, 노드 간 경쟁을 이용하는 방식이기 때문이다. 내부망 환경은 노드끼리 신원을 미리 알고 있어 서로 경쟁할 필요가 없다. 내부망 환경에서 PoW 방식은 무의미한 전기에너지 낭비일 뿐이다. 합의 알고리즘 외에도 P2P 네트워크를 구성하는 방식 등이 내부망 환경에서의 활용 가능성을 판단하는 주요 요인이 될 수 있다.

나. 커스터마이징 가능성

커스터마이징 가능성이란 주어진 조건이나 환경에 따라 해당 플랫폼을 커스

터마이징할 수 있는지에 대한 기준이다. 즉 합의 알고리즘, 노드 간 통신하는 트랜잭션, 스마트 계약, 네트워크 참여 노드 인증 기능 등을 개발자가 수정할 수 있는지에 대한 것이다.

다. 이식성

이식성이란 해당 플랫폼이 운영체제와 같은 시스템 환경과 상관없이 구축할 수 있는지에 대한 기준이다. 블록체인 플랫폼은 노드 클라이언트라는 소프트웨어 형태로 배포되고 구동된다. 노드 클라이언트는 각 서버 또는 노드에 설치되어 P2P 통신, 합의, 채굴 등의 기능을 하도록 하는 소프트웨어이다. 이식성은 노드 클라이언트 소프트웨어가 시스템 환경에 무관하게 설치되어 동작할 수 있는지의 여부이다.

라. 개발 문서화

개발 문서화란 개발에 필요한 사용 매뉴얼, API 또는 관련 문서 등이 상세히 제시되어 서비스 구축에 도움을 주는지에 대한 기준이다. 블록체인 플랫폼을 군에 도입할 때나, 체계 운용 중 문제가 발생할 수 있다. 기업 상용 소프트웨어는 판매 기업으로부터 기술 지원을 받을 수 있지만 오픈소스 플랫폼은 그렇지 않다. 따라서 기술 문서가 상세히 제시되어 있는지 여부는 매우 중요하다.

마. 커뮤니티 활성화

커뮤니티 활성화란 해당 플랫폼을 활용하여 서비스를 구축하는 개발자들 간의 커뮤니티가 활성화되어 있는지 여부이다. 기술 문서가 아무리 상세하게 제기됐더라도 해당 자료에 기록되지 않은 내용이 있을 수 있다. 개발 단계에서 예상하지 못한 오류가 대표적인 예이다. 개발자 커뮤니티를 이용해 동일한 오류를 경험한 개발자가 있는지, 있다면 어떻게 해결하였는지 등을 질문하고 답을 얻을 수 있다.

바. 라이선스

라이선스란 해당 플랫폼의 라이선스에 관한 문제이다. 본 연구에서 비교 분석하는 대상들은 모두 오픈소스이다. 오픈소스는 공공에 공개되어 자유롭게 사용할 수 있는 소스코드이다. 하지만 완전한 자유가 부여되는 것은 아니다. 오픈소스에도 라이선스가 존재하는데, Apache, GPL, AGPL, LGPL, MIT, artistic, Eclipse, BSD, MPL 등으로 구분된다. 각 라이선스별로 필수 요구사항, 허락 조건, 금지 조건 등이 다르다. 이중 AGPL, GPL과 같은 라이선스는 AGPL/GPL 소스코드를 활용한 소프트웨어를 AGPL/GPL로 공개해야 하는 등의 강력한 제약조건이 있다, 만약 AGPL 라이선스를 가진 플랫폼을 군에 적용하면, 플랫폼을 이용한 체계 소스코드를 AGPL 라이선스로 공개해야 하는 문제가 발생한다. 따라서 라이선스 문제가 발생하지 않는 플랫폼을 선정해야 한다.

사. 업데이트 지속성

업데이트 지속성이란 개발 주체가 지속적으로 업데이트를 진행하고 있는지에 대한 기준이다. 예를 들어 하이퍼레저 패브릭 플랫폼은 개발 주체인 IBM 사에서 지속적으로 업데이트하는지 여부이다. 이 기준은 깃 허브를 이용해 오픈소스가 얼마나 릴리스 되었는지를 기준으로 평가하였다.

아. 활용 선례

활용 선례란 해당 플랫폼을 활용하여 블록체인 플랫폼을 구축한 사례가 있는지에 대한 기준이다. 다른 곳에서 분석 대상 플랫폼을 사용하고 있다면, 해당 플랫폼은 운용할 수 있는 플랫폼으로 신뢰할 수 있다.

자. 처리 속도

처리 속도란 초당 처리되는 트랜잭션 개수를 나타내는 지표인 TPS(Transaction per Second) 수치가 얼마나 되는지에 대한 기준이다. 예를 들어 블록체인 네트워크가 1시간 동안 트랜잭션 36,000개를 처리했다고 가정하면, 이 네트워크는 1초에 약 10개 트랜잭션을 처리(36,000개/3,600초)했으므로 처리 속도는 10TPS이다. TPS는 서버 성능 등 블록체인의 네트워크 환경에 따라 달라질 수 있으므로, 공식 spec sheet에 공개된 수치로만 참고한다.

차. 스마트 계약(Smart Contract)

스마트 계약이란 블록체인 기반으로 금융거래, 부동산 계약, 공증 등 다양한 형태의 비즈니스 로직을 구동시키는 일종의 프로그램을 말하며 블록체인 2.0의 핵심 가치로 분류된다. (위키백과) 이 항목은 해당 플랫폼에서 스마트 계약을 구동할 수 있는지, 구동할 수 있다면 어떤 언어로 스마트 계약을 구현할 수 있는지에 대한 기준이다.

카. 상호운용성

상호운용성이란 해당 플랫폼이 기존 시스템이나 타 블록체인 체계와 연동할 수 있는지에 대한 기준이다. 여기서 기존 시스템이란 낡은 기술, 방법론, 컴퓨터 시스템, 소프트웨어 등을 말한다. 오래전에 개발된 기술이지만 효율성이 높아 널리 사용되는 RDBMS(관계형데이터베이스)가 그 사례이다. 블록체인 플랫폼을 도입한다고 하더라도 기존의 모든 시스템을 뒤엎기는 힘들다. 블록체인을 적용했을 때 비효율적인 업무 분야가 있기 때문이다. 따라서 블록체인이 업무를 원활하게 처리하려면 기존 시스템과 연동이 되어야 한다. 또한 향후 목적에 따라 여러 블록체인 플랫폼이 도입·개발될 수 있다. 다양한 플랫폼이 도입·개발된다면 플랫폼 간에 데이터를 주고받아야 하는 경우가 발생할 수 있다. 이때도 플랫폼이 서로 연동되어야 하므로 상호운용성이 중요하다.

이러한 비교분석 기준을 수치화시킬 수 있도록 분석표 만들면 <표 8>과 같다. 해당 표의 총 11가지 항목에 '매우 좋음: 5, 좋음: 4, 보통: 3, 나쁨: 2, 매우 나쁨: 1, 해당 사항 없음: -'의 배점표를 적용하여 플랫폼별로 총점을 계산한 후 가장 높은 점수를 받은 블록체인 플랫폼을 본 연구에서 국방정보체계에 적용할 플랫폼으로 선정한다.

<표 8> 국방 블록체인 플랫폼 선정기준표

구분	번호	항목	설명
개발	1	내부망 활용 가능성	내부망 환경에서 활용할 수 있는가?
	2	커스터마이징 가능성	주어진 조건이나 상황에 따라 적합한 형태로 커스터마이징하여 구축할 수 있는가?
	3	이식성	운용 시스템 환경에 상관없이 구축할 수 있는가?
	4	개발 문서화	사용 매뉴얼, API, 관련 문서 등이 서비스 구축에 문제없도록 상세히 제기되어 있는가?
	5	커뮤니티 활성화	개발자 커뮤니티가 활성화되어 있는가?
관리	6	라이선스	서비스 구축에 라이선스로 인한 문제가 없는가?
	7	업데이트 지속성	개발 주체가 지속적으로 업데이트하고 있는가?
	8	활용 선례	신뢰할 수 있는 활용 선례가 있는가?
성능	9	처리 속도	TPS(Transactions per Second)는 얼마인가?
	10	스마트 계약	스마트 계약을 구동할 수 있는가?
	11	상호운용성	기존 시스템 또는 타 블록체인 체계와의 연동이 수월한가?

<표 9>는 <표 8>의 국방 블록체인 플랫폼 선정기준표에 이더리움 플랫폼의 상세 분석 내용을 적용한 내용이다.

<표 9> 이더리움 분석표

구분	번호	항목	설명
개발	1	내부망 활용 가능성	POA 합의 알고리즘으로 구동 가능함
	2	커스터마이징 가능성	합의 알고리즘을 PoA로 변경하는 것 이외에는 별도의 커스터마이징 기능이 없음. 직접 소스코드를 분석하여 수정하여야 함
	3	이식성	리눅스, 윈도우, 맥OS 등 각 운영체제별로 노드 클라이언트가 제공될 뿐만 아니라 도커 이미지 또한 제공됨
	4	개발 문서화	공식 홈페이지 및 깃허브를 통해 상당히 자세하게 사용 매뉴얼이 안내되어 있음. 또한 이더리움 네트워크 구축과 개발에 대한 저서가 다수 출판되어 있음
	5	커뮤니티 활성화	비트코인과 함께 타 블록체인 플랫폼에 비하여 압도적으로 다양한 소통 매체가 활성화되어 있음
관리	6	라이선스	GPL-3.0으로 수정, 배포, 상업적 이용, 특허신청, 자석 이용은 가능하나 2차 라이선스는 불가하고 보증 책임이 없음. 수정한 소스코드 및 GPL 소스코드를 활용한 소프트웨어를 모두 GPL 라이선스로 공개하여야 함. 라이선스 및 저작권을 명시하여야 함
	7	업데이트 지속성	go-ethereum 레파지토리 기준, 2014년 7월 18일부터, 깃허브를 통해 약 171회 릴리스 되었음
	8	활용 선례	① UN 세계식량계획 기구의 난민 지원 자금 조달 시스템 ② Share&Charge 사의 전기 자동차 충전소 공유 플랫폼 ③ Energy Web Foundation의 에너지 거래 플랫폼
성능	9	처리 속도	표준 랩탑 환경에서 프라이빗 체인 모드로 구동 시 3000 TPS
	10	스마트 계약	스마트계약 구동 가능함. 이더리움에 특화된 언어인 솔리디티, LLL, 서펀트, 바이퍼 등을 통해 스마트 계약을 구현하여야 함
	11	상호운용성	타 블록체인 시스템과 연동하기 위한 프레임워크 폴카닷 개발중임. 또한 IPFS와 연동하여 구동할 수 있음

<표 10>은 <표 8>의 국방 블록체인 플랫폼 선정기준표에 KLAYTN 플랫폼의 상세 분석 내용을 적용한 내용이다.

<표 10> KLAYTN 분석표

구분	번호	항목	설명
개발	1	내부망 활용 가능성	KLAYTN의 git repository에서 제공하는 도커라이즈된 로컬 네트워크 구동 가능
	2	커스터마이징 가능성	KLAYTN 2.0부터 자체 L2 솔루션인 서비스 체인을 통해 커스터마이징 가능
	3	이식성	리눅스, 윈도우, 맥OS 등 각 운영체제별로 노드 클라이언트가 제공될 뿐만 아니라 도커 이미지 또한 제공됨
	4	개발 문서화	KLAYTN DEVELOPER HUB를 통해 공식적으로 개발가이드를 제공해주고 있음, 이더리움 또는 Hyperledger fabric에 비해 시중에 출판된 개발 관련 도서는 부족함
	5	커뮤니티 활성화	KlaytnDevForum을 통해 개발에 필요한 정보 참조 확인 가능
관리	6	라이선스	KLAYTN은 오픈소스 프로젝트로 서비스 체인을 구성하는데 추가적인 라이선스 비용은 발생하지 않음
	7	업데이트 지속성	klaytn 레파지토리 기준, 2019년 6월 25일부터, 깃허브를 통해 약 34회 릴리스 되었음
	8	활용 선례	① 한국은행 'CBDC 모의실험 연구사업' 진행 ※ 이더리움, Hyperledger fabric 대비 후발주자로 사용 선례가 부족함
성능	9	처리 속도	KLAYTN 메인넷 CYPRESS 기준 4,000TPS로 이더리움보다 상대적으로 빠름
	10	스마트 계약	솔리디티(Solidity)를 기본 프로그래밍 언어로 지원하여 스마트 컨트랙트 프로그래밍 가능
	11	상호운용성	DEX, Bridge, Oracle과 같은 다양한 생태계들과 협력 진행 중 앞으로 클레이튼과 이종 블록체인 간 자산 전송 및 교환이 편해질 것(현재 개발 중)

<표 11>은 <표 8>의 국방 블록체인 플랫폼 선정기준표에 하이퍼레저 패브릭 플랫폼의 상세 분석 내용을 적용한 내용이다.

<표 11> 하이퍼레저 패브릭 분석표

구분	번호	항목	설명
개발	1	내부망 활용 가능성	프라이빗 블록체인을위한 플랫폼으로 개발되어 내부망에서의 활용이 적절함
	2	커스터마이징 가능성	BFT Smart, SBFT, Honey Badger, Kafka, Raft 등의 합의 알고리즘을 선택할 수 있음. 멤버십 서비스, 체인코드 서비스 등 핵심 기술 요소를 커스터마이징하는 기능이 제공됨
	3	이식성	운영체제 이식성이 좋은 도커 이미지 파일 형태로 제공되어 이식성이 높음
	4	개발 문서화	공식 홈페이지 및 깃허브를 통해 상당히 자세하게 사용 매뉴얼이 안내되어 있음. 또한 하이퍼레저 H브릭 구축과 개발에 대한 저서가 다수 출판되어 있음
	5	커뮤니티 활성화	공식 홈페이지를 중심으로 Stack-Overflow, Youtube Rocketchat, 깃허브 등의 소통 매체를 통해 활성화되어 있음
관리	6	라이선스	Apache-2.0으로 수정, 배포, 상업적 이용, 특허 신청, 사적 이용 2차 라이선스 모두 가능하나 보증 책임이 없고 상표권 침해가 금지됨. 라이선스 및 저작권을 명시하여야 함
	7	업데이트 지속성	fabric 레파지토리 기준, 2017년 11월 1일부터, 깃허브를 통해 약 61회 릴리스 되었음
	8	활용 선례	① 스마트계약을 활용한 채널파이낸싱 업무 혁신 ② 미국 중앙예탁청산기관 ③ Digital Trade Chain ④ IBM Universal Payment Solution ⑤ 월마트의 식품 원산지 추적 플랫폼
성능	9	처리 속도	총 100개의 노드(홍콩, 멜버른, 도쿄, 시드니, 오슬로 등 5개 데이터 센터에 각각 20개의 노드가 존재) 환경에서 약 2000~2500 TPS
	10	스마트 계약	스마트 계약 구동 가능. 범용 프로그래밍 언어인 Go 언어, Java 등을 통해 구현할 수 있음.
	11	상호운용성	분산원장 간 연동 프로토콜인 하이퍼레저 퀼트(Quilt), 이더리움 소스코드를 하이퍼레저에서 동작할 수 있도록 지원하는 프레임워크인 하이퍼레저 버로우(Burrow) 지원

<표 12> 블록체인 플랫폼 선정 최종 결과표

구분	번호	항목	이더리움	KLAYTN	하이퍼레저 패브릭
개발	1	내부망 활용 가능성	4	4	5
	2	커스터마이징 가능성	2	2	5
	3	이식성	5	5	5
	4	개발 문서화	5	3	5
	5	커뮤니티 활성화	5	4	5
관리	6	라이선스	3	5	5
	7	업데이트 지속성	5	5	5
	8	활용 선례	3	2	4
성능	9	처리 속도	2	5	5
	10	스마트 계약	4	4	5
	11	상호운용성	3	2	4
종합			41	41	53

매우 좋음: 5, 좋음: 4, 보통: 3, 나쁨: 2, 매우 나쁨: 1, 해당 사항 없음: -

<표 12>는 플랫폼별로 획득한 최종점수를 비교분석 하였다. 그 결과 군 적용을 위한 블록체인 플랫폼으로 가장 적합한 플랫폼은 하이퍼레저 패브릭으로 결정되었다. 특히 기준 항목 중 ① 내부망 활용에 적합하다는 점, ④ 개발 문서화가 우수하다는 점, ⑥ 라이선스로 인한 제약이 낮다는 점, ⑨ 처리 속도가 높다는 점이 두드러졌다. 하이퍼레저 패브릭에 이어 높은 종합 점수를 획득한 이더리움도 활용 후보군에 선정할 수 있지만 하이퍼레저 패브릭과 비교해 경쟁하기에는 상대적으로 커스터마이징에 적합하지 않다는 점, 라이선스로 인한 문제가 발생할 수 있다는 점 등에서 설득력이 부족하다.

제4장 블록체인 기술의 국방연동체계 적용

제1절 모델설계

1. 국방 연동체계의 블록체인 적용 개념

가. 개요

국방 연동체계에서 사용할 프라이빗 블록체인을 선정하기 위해 평가한 결과 이더리움, KLAYTN, 하이퍼레저 패브릭 등 여러 프라이빗 블록체인 중 하이퍼레저 패브릭이 가장 적합한 것으로 선정되었다. 이에 따라 하이퍼레저 패브릭 기반으로 구축한 시스템의 기술적 한계나 부수적인 문제점들을 파악하기 위해 모델설계 및 테스트 모듈을 개발하여 분석하기로 한다. 시범체계인 국방 연동체계의 구조를 단순화하여 최대한 가벼운 형태의 기본 기능들 위주로 구현하는 것을 목표로 하였고 대표적인 기능인 기준 정보관리, META 정보관리, LOG 관리를 하이퍼레저 패브릭을 이용하여 구현하였다.

하이퍼레저 패브릭은 전 세계적인 오픈소스 프로젝트로 리눅스 재단 주도하에 개발되고 있으며 Hyperledger fabric read the docs라는 공식 채널을 통해서 개발자들은 설치 방법, API 사용법 등 기본적인 개발 기술을 습득할 수 있다. 본 연구에서 소개할 테스트 모듈 또한 Hyperledger fabric read the docs의 레퍼런스 정보를 기반으로 구축하였다.

클라우드 환경에서 하이퍼레저 패브릭을 사용하고자 할 때는 IBM 클라우드

또는 아마존 AWS를 이용하여 블록체인 시스템을 구축할 수 있다. 반면 로컬 또는 단독 망에서 개발하고자 할 때는 하이퍼레저 패브릭을 공식 채널에서 제공하는 Git 레파지토리[28] 등에서 다운로드 후 도커[29] 기반으로 시스템을 구축한다.

나. 구조 및 흐름

테스트 모듈 시스템은 OS(Operating system)로 Ubuntu 18.04 LTS, 블록체인 플랫폼으로 하이퍼레저 패브릭 v1.4.3을 사용하고 언어는 Node.js 및 Go 언어를 사용하여 개발하였다. 또한, 웹 애플리케이션, 서버 프로그램, 체인코드, 블록체인 네트워크 등 네 가지 부분으로 구성되어 있다.

Client가 브라우저를 통해 시스템에 접근을 시도하면 애플리케이션으로부터 하이퍼레저 패브릭 네트워크에 gRPC[30] 통신을 통해 실행시키고자 하는 함수에 대한 질의(Query) 또는 호출(Invoke) 요청을 하게 된다. 패브릭 네트워크 내의 피어(Peer)에 트랜잭션 요청은 이러한 질의 또는 호출을 통해 이루어진다. 피어에서는 키-값(key-value)의 World State DB에 저장된 정보에 대해서

28) Git 레파지토리(Git Repository): Git으로 관리하는 프로젝트의 저장소로, Local Repository, Remote Repository로 구분하여 관리한다.

29) 도커(Docker): Docker는 애플리케이션의 모든 코드 및 종속성을 표준 형식으로 패키징할 수 있게 해주는 컨테이너이다. 개발자가 컨테이너화된 애플리케이션을 빠르게 빌드, 테스트 및 배포할 수 있게 해주는 소프트웨어 플랫폼이기도 하다.

30) gRPC(Google Remote Procedure Call): gRPC는 구글이 개발한 오픈 소스 원격 프로시저 호출(RPC) 시스템이다. 전송을 위해 HTTP/2를, 인터페이스 정의 언어로 프로토콜 버퍼를 사용하며 인증, 양방향 스트리밍 및 흐름 제어, 차단 및 비차단 바인딩, 취소 및 타임아웃 등의 기능을 제공한다.

체인코드에 의해 요청받은 작업을 처리하게 된다. 그 후 오더링 서비스 노드에서 트랜잭션을 순서대로 정렬하여 블록을 생성하게 된다. 이와 같은 과정을 통해 도출된 결괏값은 테스트 모듈 애플리케이션으로부터 브라우저로 전달되고 이는 적절한 형태로 변형되어 사용자에게 노출된다.

하이퍼레저 패브릭 애플리케이션은 일반적으로 두 가지 인증 정보가 필요한데 첫째는 하이퍼레저 패브릭에서 지원하는 자체 DB인 CouchDB[31] 기반으로 개발된 애플리케이션 자체 사용자 인증이고, 두 번째는 네트워크에 참여할 수 있게 해주는 CA 노드로부터 받은 PKI 기반 인증서이다. 인증서는 파일 형식으로 되어 있으며 테스트 모듈 애플리케이션은 파일 형태로 저장된 인증서를 패브릭 네트워크에 접근할 때 사용해 피어들과 통신하여 체인코드 내의 함수들을 호출할 수 있게 된다.

테스트 모듈 시스템은 기본적으로 하이퍼레저 패브릭에서 제공되는 피어, Fabric-CA, 오더링 서비스 노드들을 도커에 이미지로 올려서 사용하도록 구성되어 있다. 도커 위에 이미지를 올린 후 요청에 대한 결괏값을 도출할 수 있도록 체인코드를 피어 이미지에 설치하고 초기화시켜 주게 된다. 이와 같은 행위를 하는 스크립트도 코드 내에 포함되어 있다. 더해서 브라우저에서 발생하는 User Action을 처리하는 코드와 테스트 모듈 애플리케이션의 기능들을 명시해놓은 Node.js 코드들, 테스트 모듈 애플리케이션과 하이퍼레저 패브릭을 연결해주는 하이퍼레저 SDK, Go 언어로 작성된 체인코드 등도 테스트 모듈 시스템의 구성 요소이다.

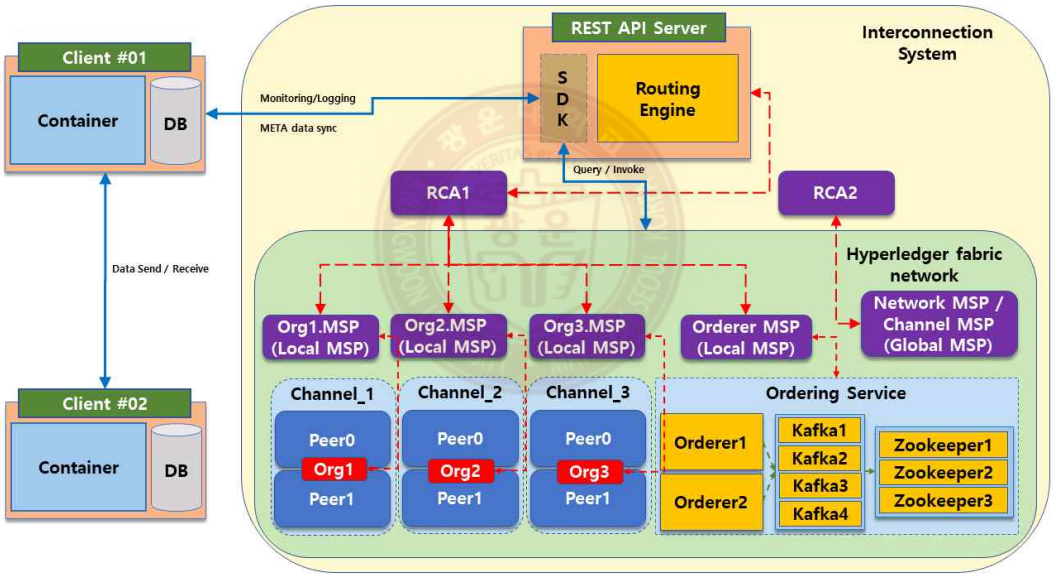
테스트 모듈 시스템 웹 프로그램의 화면은 국방 연동체계의 기준정보, Meta 정보, Log 정보 등 각 기능을 처리할 수 있도록 설계되어 있다.

---

31) CouchDB: 하이퍼레저 패브릭에서 지원하는 NoSql 형태의 데이터베이스로 하이퍼레저 패브릭에서는 원장의 최신 상태를 알리는 World State DB로 사용된다.

2. 개념설계

지금까지 언급한 내용을 토대로 본 연구에서 주장하는 하이퍼레저 패브릭 기반 국방연동체계에 대한 개념을 [그림 17]과 같이 설계하였다. 또한, 해당 설계는 추후 언급되는 테스트 모듈에도 활용되며, 지속해서 국방연동체계 이외에 타 국방정보체계에도 다양하게 적용할 수 있다.



[그림 17] 하이퍼레저 패브릭 기반 국방연동체계 개념도

하이퍼레저 패브릭 기반 국방연동체계의 상세 구성은 <표 13>과 같다.

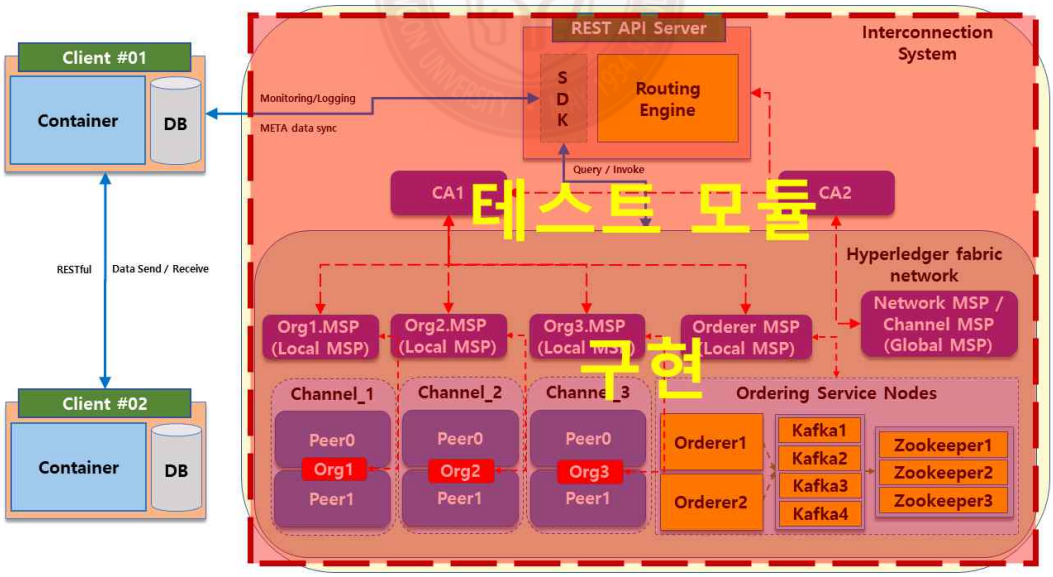
<표 13> 하이퍼레저 페브릭 기반 국방연동체계 구성 요소

구성 요소	상세 설명
Channel_1	• 연동 대상 정보체계들의 기준정보, Meta Data, 연동 이력을 관리하는 채널 • 연동 대상체계들이 피어 노드로 참여 • 피어 노드는 각 연동체계가 사용하는 블록체인, world state DB, chain-code로 구성 • 피어 노드에는 연동 데이터가 아닌 LOG 데이터를 적재, 연동 데이터는 Client to Client 간 RESTful 통신
Channel_2	• 연동체계의 중앙관제를 위한 채널 • 연동 대상체계의 최신상태정보를 블록체인에 기록 • 연동 서비스 제공 체계(REST API Server)의 피어 노드들로 구성
Channel_3	• Channel_1과는 별도의 독립된 연동집단의 채널 • Channel_1과 Channel_3의 권한을 동시에 가지는 Org가 있을 수 있음 • 동작 기능과 개념은 Channel_1과 동일 • Channel_3부터 Channel_n까지 확장가능
Org1	• 연동 대상 체계들의 피어 노드로 구성
Org2	• REST API Server의 피어 노드로 구성
Org3	• 연 동대상 체계들의 피어 노드로 구성
Ordering Service Nodes	• 오더러 이중화 구성 • Zookeeper 통신 기술 기반, Kafka 알고리즘의 오더링 서비스 구축
(R)CA	• Certificate Authority • 국방연동체계에서 사용할 인증서를 발급 및 관리
Global MSP	• 블록체인 네트워크와 채널에 참여한 모든 구성원에게 영향 • 네트워크 MSP와 채널 MSP로 구성됨
Local MSP	• 각각의 피어 노드, 오더러, Client 등의 파일 시스템에 탑재 • 노드에 대한 사용 권한을 정의 • 모든 노드에는 Local MSP가 정의되어 있어야 함 • 피어 MPS, 오더러 MSP로 구성됨
REST API Server	• 연동 서비스를 제공하는 주체 • 대상체계로부터 JSON Message를 받으면 Hyperledger fabric SDK를 통해서 블록체인 네트워크에 Query 또는 Invoke 시도
Client	• REST API Server를 통해서 실시간 통합되는 연동의 대상체계 • Client이면서 동시에 피어 노드로 구성될 수 있음

제2절 테스트 모듈 구현

1. 구현범위

본 연구의 테스트 모듈의 구현범위는 [그림 18]과 같이 하이퍼레저 패브릭 기반 국방연동체계 개념도의 전체 범위 중 연동 대상체계가 되는 Client를 제외한 나머지 부분 즉, REST API Server, 하이퍼레저 패브릭 네트워크 부분까지로 한정한다. 이는 전체 서비스 구현이 목적이 아닌 국방 분야에 블록체인 적용이 가능한지 판단을 위한 유닛 테스트 차원에서는 불필요하게 전체 서비스를 구현할 필요가 없기 때문이다.

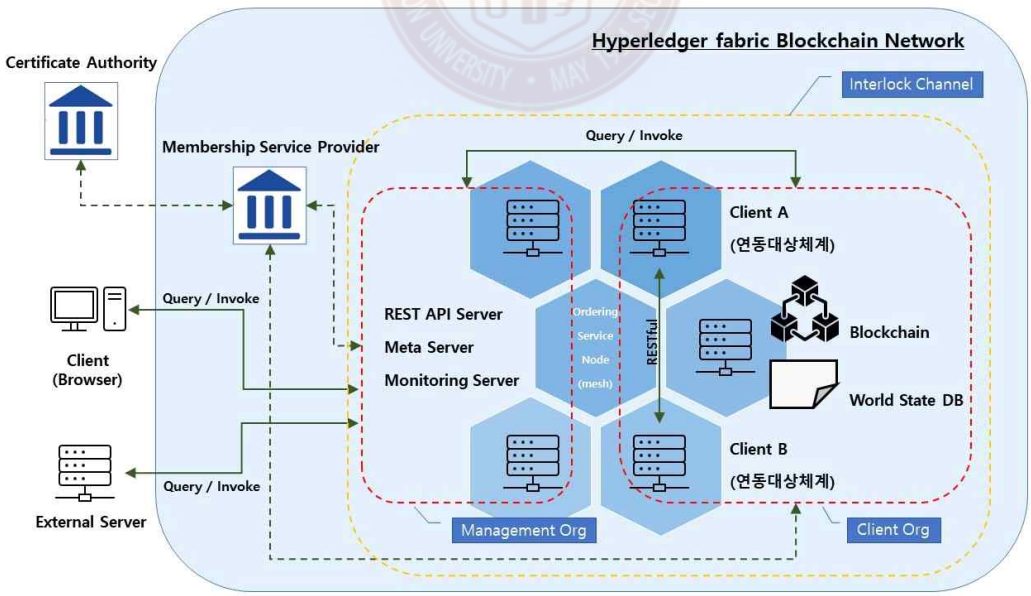


[그림 18] 테스트 모듈 구현 범위

또한, Client의 역할은 REST API Server에 간단한 웹 애플리케이션을 구현하여 브라우저를 통해 request, response 통신을 하는 것으로 대체 한다.

2. 시스템 상세 구성도

테스트 모듈 개발에 앞서 이미 설계한 '하이퍼레저 패브릭 기반 국방연동체계 개념도'를 바탕으로 [그림 19]와 같은 시스템 구성도를 작성하였다. 시스템 구성도는 정보체계 제안 및 개발 단계에서 작성해야 하는 필수 산출물로 본 연구에서는 테스트 모듈 수준의 개발이라는 점을 고려하여 간소하게 작성하였으며 구성 요소의 상세 설명은 <표 13>과 같다.

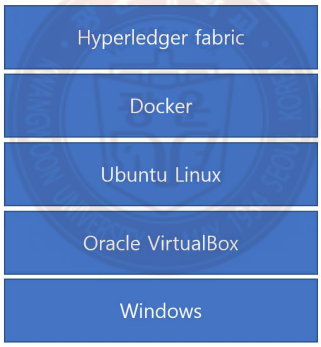


[그림 19] 하이퍼레저 패브릭 기반 국방연동체계 상세 구성도

다음은 [그림 19]의 구성도를 토대로 테스트 유닛 구축을 위한 환경을 구성하고 개발 및 테스트를 통한 실증을 진행한다.

3. 개발 및 테스트 환경

‘4장-1절’에서 작성한 개념설계를 바탕으로 ‘하이퍼레저 패브릭 기반 국방 연동체계’ 테스트 모듈 구현에 앞서 우선 개발 및 테스트 환경을 정의한다.



[그림 20] 개발환경 구성

개발환경은 단어 표현 의미 그대로 해당 모듈을 개발하는 환경이고 테스트 환경은 구현체를 실험할 환경을 의미한다.

테스트 모듈은 실험실 수준에서 주장하는 바가 실전에서 적용 가능한지를 판단하기 위한 도구로서, 전력화를 위한 목적이 아닌 비교적 단순한 테스트를 그 목적으로 한다. 따라서, 개발환경은 대규모 개발사업에 필요한 구성이 아닌 일반적으로 개발자가 사용하는 Windows OS에 가상화 소프트웨어인 Oracle

VirtualBox로 Ubuntu Linux 기반의 가상 환경을 구축하고, 구축된 가상화 환경에 도커 컨테이너를 활용하여 하이퍼레저 패브릭 프레임워크 및 각종 애플리케이션을 구동하는 방식의 형태로 구성한다. 또한 테스트 환경은 소형 워크스테이션 수준의 물리 서버 위에 4 core(CPU), 8 GB(Memory)로 가상화 서버를 구성하여 운용하도록 한다.

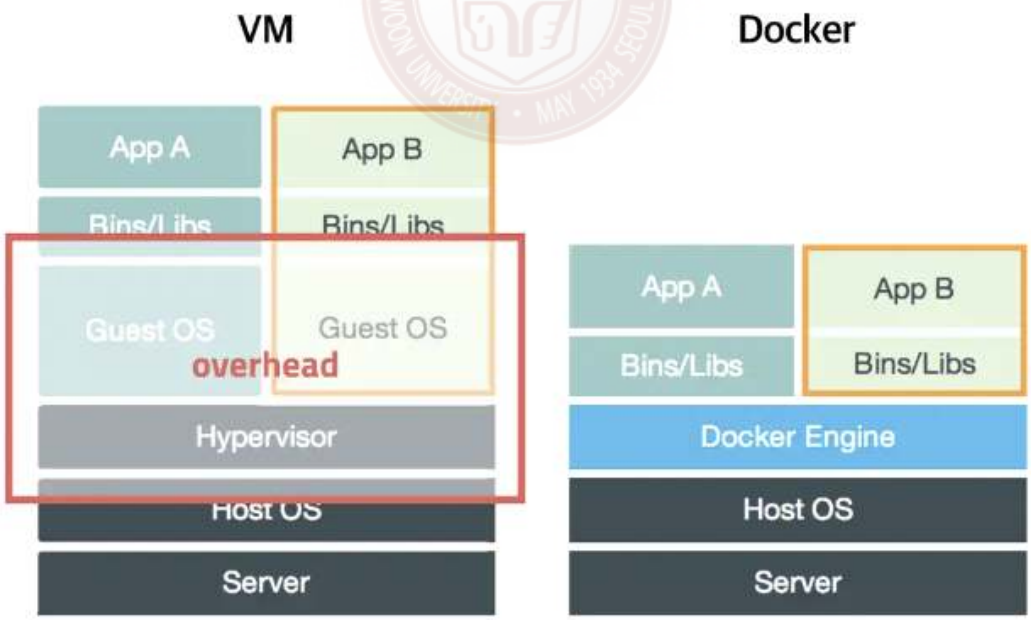
<표 14> 테스트 환경 구성

구분	물리 서버	가상화 서버
CPU	13th Gen Intel(R) Core(TM) i7-13700H, 14 core, 2.40 GHz	13th Gen Intel(R) Core(TM) i7-13700H, 4 core
MEMORY	LPDDR5 32 GB	8 GB
NIC	Intel(R) 82579V Gigabit Network Connection	VirtualBox Host-Only Ethernet Adapter
Router	ipTIME T5008 1000Mbps LAN Interface	ipTIME T5008 1000Mbps LAN Interface
Network	1000Mbps LAN	1000Mbps LAN
OS	Windows 11 PRO	Ubuntu 18.04 LTS

4. 실증결과

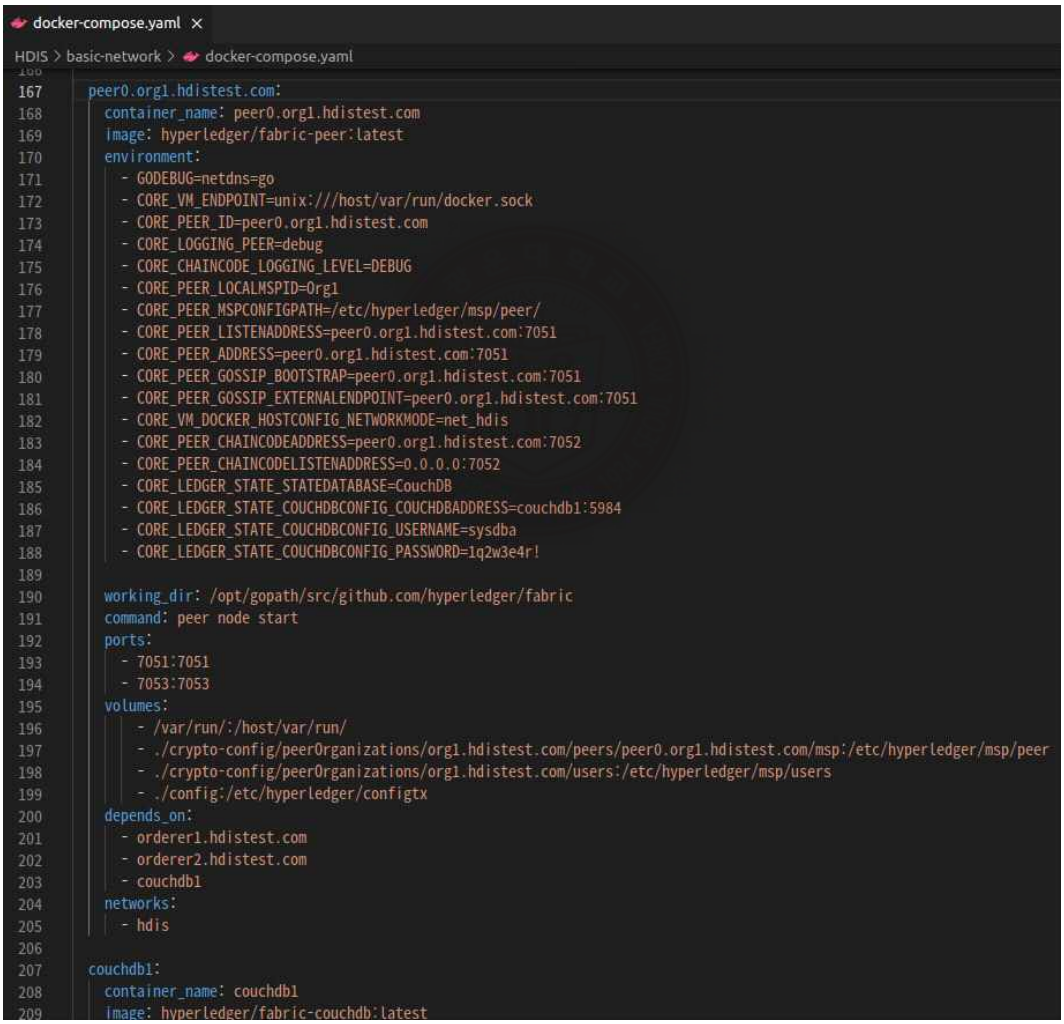
가. 컨테이너 구성

앞선 '4장-2절-3'에서 테스트 모듈은 도커 기반으로 개발하는 것으로 결정하였다. 도커(Docker)는 리눅스의 응용프로그램을 프로세스 격리 기술을 활용해 컨테이너로 실행하고 관리하는 오픈소스 프로젝트를 말한다. 간단히 말하면, 리눅스에서 제공하는 컨테이너를 통해 애플리케이션 프로세스를 격리하고 하나의 서버에 여러 개 컨테이너를 실행하면 서로에게 독립적으로 구동되어 일반 가상화 솔루션 대비 매우 가볍고 빠르게 작동한다.



[그림 21] 가상화와 도커 비교

본 연구의 도커 컨테이너는 도커 컴포즈(Docker Compose)를 통하여 구축하였다. 도커 컴포즈는 도커를 쉽게 사용하고 관리하기 위한 도구로서 복잡하게 구성된 도커 컨테이너를 파일로 설정하여 상대적으로 편리하게 운용할 수 있도록 해준다.



[그림 22] 테스트 모듈의 도커 컴포즈 설정 파일

[그림 20]은 하이퍼레저 패브릭 기반 연동체계 구축을 위한 컨테이너 기동을 목적으로 작성된 도커 컴포즈 설정 파일의 일부이며, 해당 설정 파일에는 피어 노드 6개, 오더링 서비스 노드 2개, Kafka 4개, Zookeeper3개, CA 2개, CLI 노드 2개가 구동되도록 구성되었으며 각 컨테이너의 이미지는 하이퍼레저 패브릭의 저장소(Repository)에서 제공된다.

나. 하이퍼레저 패브릭 네트워크 구축

하이퍼레저 패브릭은 리눅스 기반 OS에서 명령어 인터페이스인 CLI 환경에서 동작하고 GUI[32]를 제공하지 않으므로, 네트워크를 구현하려면 <표 15>와 같이 제공되는 도구들을 활용하여 개발해야 한다.

<표 15> 하이퍼레저 패브릭 네트워크 관리 도구

도구	기능
Cryptogen	조직 및 인증서 생성 도구
Configtxgen	블록 및 트랜잭션 생성 도구
Configtxlator	블록 및 트랜잭션 구문 분석 도구
Peer	블록체인 데이터를 저장하고 유지보수 체인코드를 실행하는 마스터 노드 도구
Orderer	트랜잭션 패키징, 정렬 도구

32) GUI(Graphical User Interface): 그래픽 사용자 인터페이스

Cryptogen 도구는 네트워크에서 운영되는 오더링 서비스 노드 및 피어 노드 등 조직에서 사용할 각종 신원 증명 정보에 대한 인증서를 발급할 때 사용하며, crypto-config.yaml과 같은 설정 파일을 통해 인증서 발급에 필요한 각종 정보를 설정한다. Configtxgen 도구는 채널을 구성하고 검사하며 제네시스 블록을 만들고 검사할 수 있고 Configtxlator 도구는 REST 서버를 구성하는 기능을 제공한다. Orderer 도구는 오더링 서비스 노드에서 실행되는 도구이며 트랜잭션을 순서화 시키고 정렬된 트랜잭션을 패키징 하는 역할을 한다. Peer 도구는 피어 노드에서 실행되는 명령어의 집합이며 주로 블록체인 데이터를 저장하고 유지, 관리하며 체인코드 설치와 초기화, 실행 및 외부 서비스 인터페이스를 제공한다.

network_create

```
# 인증서 생성
./bin/cryptogen generate --config=./crypto-config.yaml

# 네트워크 구동
docker-compose -f docker-compose.yaml -p net up -d orderer.hdistest.com peer0.org1.hdistest.com peer1.org1.hdistest.com peer0.customer

# peer 모듈로 Sales1 조직의 peer0 노드에서 channelorg1 채널 생성
peer channel create -o orderer.hdistest.com:7050 -c channelorg1 -f /etc/hyperledger/configtx/channel1.tx

# Sales1 조직의 peer0 노드를 channelorg1 채널에 가입 및 앵커 피어 지정 업데이트
peer channel join -b channelorg1.block
peer channel update -o orderer.hdistest.com:7050 -c channelorg1 -f /etc/hyperledger/configtx/Org1anchors.tx

# 체인코드 설치
peer chaincode install -l golang -n hdis-cc -v 1.0 -p github.com/chaincode/go/

# 체인코드 초기화
peer chaincode instantiate -o orderer.hdistest.com:7050 -C channelorg1 -n hdis-cc -v 1.0 -c '{"Args":[""]}' -P "OR ('Org1.member')"

# 체인코드 실행
peer chaincode invoke -o orderer.hdistest.com:7050 -C channelorg1 -n hdis-cc -c'{"function":"initSystem","Args":[""]}'
```

[그림 23] 하이퍼레저 패브릭 네트워크 구축 명령어

이러한 도구들은 앞서 언급한 바와 같이 GUI 환경을 지원하지 않으므로 CLI 노드에 직접 커맨드 명령어로 입력해 실행하거나 별도의 쉘 프로그래밍

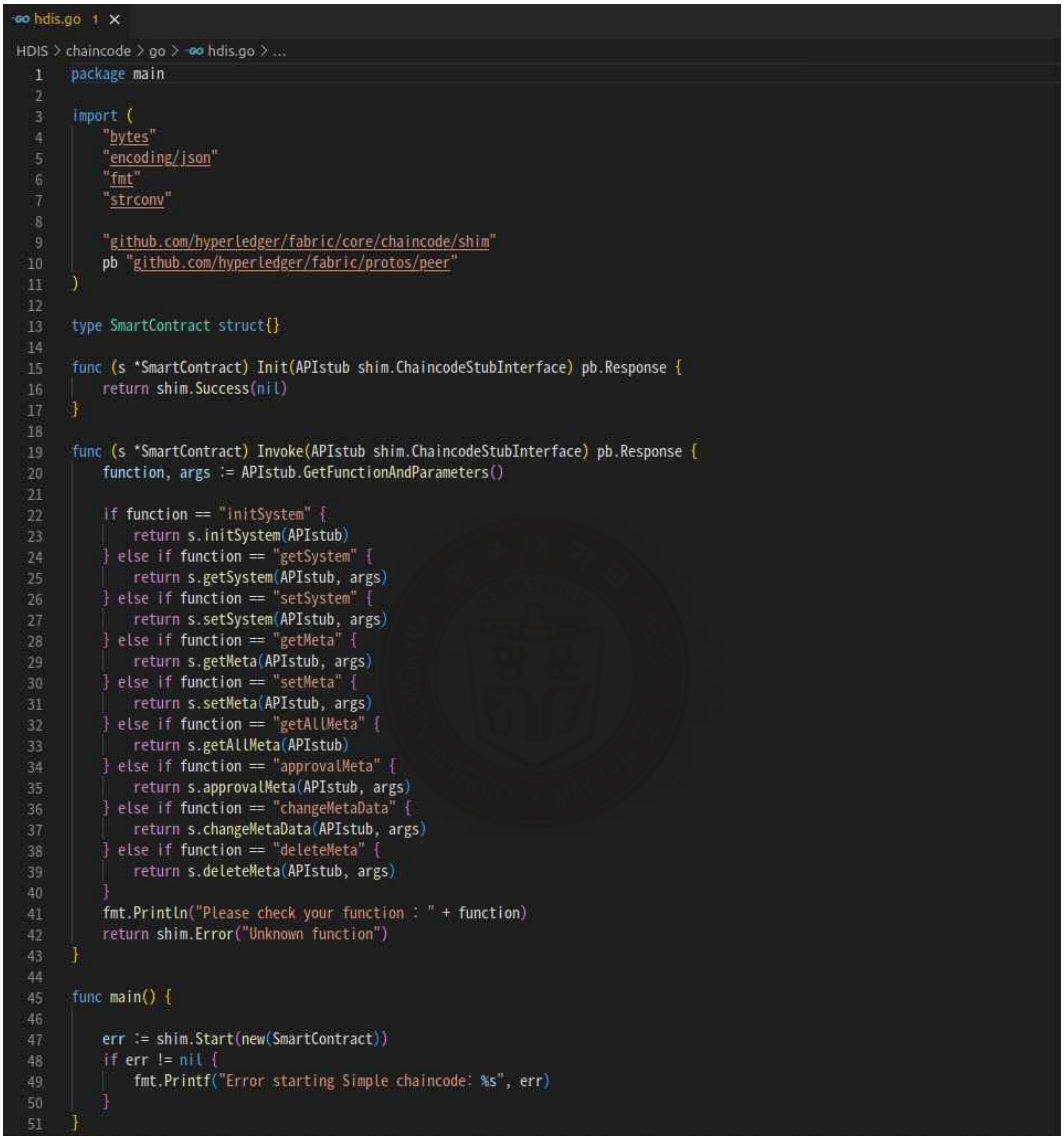
을 통해 구동되며 작업 순서는 ① 네트워크 생성 ② 인증서 생성 ③ 노드를 채널에 가입 ④ 체인코드 설치, 승인 및 커밋 ⑤ 채널에서 응용프로그램 사용 순으로 진행하며 상세 명령어는 [그림 22]와 같다.

다. 체인코드 개발

체인코드는 Go, Node.js, Java로 개발할 수 있고 도커 컨테이너 위에 기동된 피어 노드에 설치 및 실행된다. 테스트 모듈에서 사용될 체인코드는 Go 언어로 개발하였는데, 그 이유는 각종 엔터프라이즈급 시스템에서 체인코드 개발 시 가장 많이 사용된 언어이며 가장 쉽게 레퍼런스를 구할 수 있는 체인코드 언어가 Go이기 때문이다.

체인코드에는 클라이언트의 Request 통신으로 작동되는 다양한 함수가 존재한다. 테스트 모듈에서는 유닛 테스트에 필요한 기능으로 필수적인 요소만 구현하였고 상세 목록은 아래와 같다.

① initSystem(): 연동체계 초기화
② getMeta(): 메타 데이터 조회
③ setMeta(): 메타 데이터 작성
④ changeMetaData() : 메타 데이터 수정
⑤ deleteMeta(): 메타 데이터 삭제
⑥ approvalMeta(): 메타 데이터 승인
⑦ getAllMeta(): 전체 메타 데이터 조회



hdis.go 1 ×

HDIS > chaincode > go > hdis.go > ...

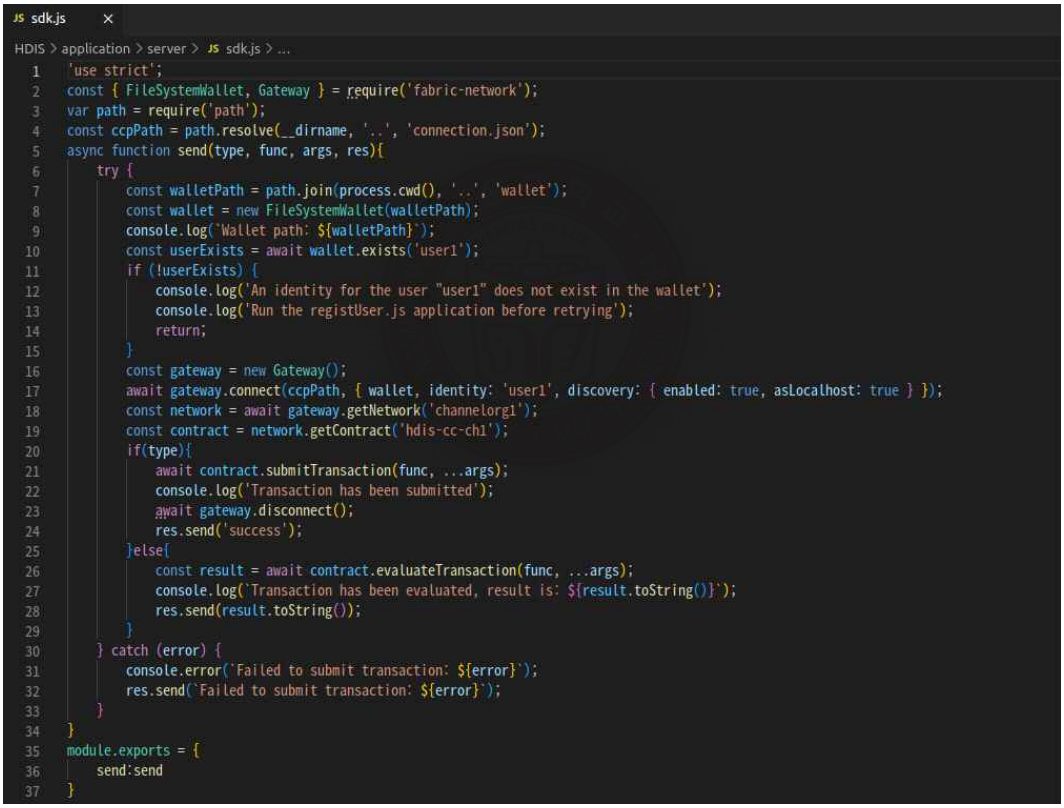
```go
package main

import (
    "bytes"
    "encoding/json"
    "fmt"
    "strconv"

    "github.com/hyperledger/fabric/core/chaincode/shim"
    pb "github.com/hyperledger/fabric/protos/peer"
)

type SmartContract struct{}

func (s *SmartContract) Init(APIstub shim.ChaincodeStubInterface) pb.Response {
    return shim.Success(nil)
}

func (s *SmartContract) Invoke(APIstub shim.ChaincodeStubInterface) pb.Response {
    function, args := APIstub.GetFunctionAndParameters()

    if function == "initSystem" {
        return s.initSystem(APIstub)
    } else if function == "getSystem" {
        return s.getSystem(APIstub, args)
    } else if function == "setSystem" {
        return s.setSystem(APIstub, args)
    } else if function == "getMeta" {
        return s.getMeta(APIstub, args)
    } else if function == "setMeta" {
        return s.setMeta(APIstub, args)
    } else if function == "getAllMeta" {
        return s.getAllMeta(APIstub)
    } else if function == "approvalMeta" {
        return s.approvalMeta(APIstub, args)
    } else if function == "changeMetaData" {
        return s.changeMetaData(APIstub, args)
    } else if function == "deleteMeta" {
        return s.deleteMeta(APIstub, args)
    }
    fmt.Println("Please check your function : " + function)
    return shim.Error("Unknown function")
}

func main() {

    err := shim.Start(new(SmartContract))
    if err != nil {
        fmt.Printf("Error starting Simple chaincode: %s", err)
    }
}
```

[그림 24] 테스트 모듈의 체인코드

체인코드는 [그림 23]과 같이 작성되며 각 피어 노드에 저장된다. 또한 체인코드의 추가 및 변경 시 피어 노드로 재배포 할 수 있다.

라. 서버 프로그램 개발

하이퍼레저 패브릭 네트워크 내의 체인코드가 국방 연동체계의 Client와 통신하기 위해서 블록체인 네트워크 외부에서 블록체인 서비스를 쉽게 사용할 수 있도록 해주는 SDK 및 API를 활용한 REST API Server를 구축하였다.



sdk.js

HDIS > application > server > sdk.js > ...

```
'use strict';
const { FileSystemWallet, Gateway } = require('fabric-network');
var path = require('path');
const ccpPath = path.resolve(__dirname, '..', 'connection.json');
async function send(type, func, args, res){
    try {
        const walletPath = path.join(process.cwd(), '..', 'wallet');
        const wallet = new FileSystemWallet(walletPath);
        console.log(`Wallet path: ${walletPath}`);
        const userExists = await wallet.exists('user1');
        if (!userExists) {
            console.log('An identity for the user "user1" does not exist in the wallet');
            console.log('Run the registUser.js application before retrying');
            return;
        }
        const gateway = new Gateway();
        await gateway.connect(ccpPath, { wallet, identity: 'user1', discovery: { enabled: true, asLocalhost: true } });
        const network = await gateway.getNetwork('channelorg1');
        const contract = network.getContract('hdis-cc-ch1');
        if(type){
            await contract.submitTransaction(func, ...args);
            console.log('Transaction has been submitted');
            await gateway.disconnect();
            res.send('success');
        }else{
            const result = await contract.evaluateTransaction(func, ...args);
            console.log(`Transaction has been evaluated, result is: ${result.toString()}`);
            res.send(result.toString());
        }
    } catch (error) {
        console.error(`Failed to submit transaction: ${error}`);
        res.send(`Failed to submit transaction: ${error}`);
    }
}
module.exports = {
    send:send
}
```

[그림 25] 테스트 모듈의 SDK

하이퍼레저 패브릭의 공식 문서인 Hyperledger fabric read the docs에서 SDK는 JAVA, Node.js, Go, Python을 지원한다고 알리고 있다. 따라서 테스트 모듈에서는 서버 프로그램을 간편하게 구축할 수 있는 Node.js를 선택하여 개발하였다.

server.js

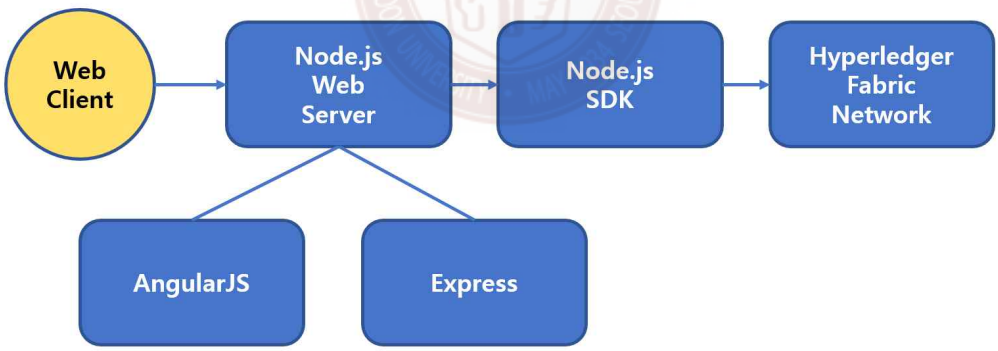
HDIS > application > server > server.js > ...

```
1   var express       = require('express');
2   var app           = express();
3   var bodyParser    = require('body-parser');
4   var http          = require('http')
5   var fs            = require('fs');
6   var Fabric_Client = require('fabric-client');
7   var path          = require('path');
8   var util          = require('util');
9   var os            = require('os');
10
11  app.use(bodyParser.urlencoded({ extended: true }));
12  app.use(bodyParser.json());
13
14  var app = express();
15
16  require('./controller.js')(app);
17
18  app.use(express.static(path.join(__dirname, '../client')));
19  var port = process.env.PORT || 8000;
20  app.listen(port,function(){
21    console.log("Live on port: " + port);
22  });
```

[그림 26] 테스트 모듈의 REST API Server

REST API Server는 연동 대상체계 또는 Client로부터 RESTful 통신으로 데이터를 수신한 뒤 [그림 24]의 SDK를 활용해 블록체인 내부와 gRPC 방식으로 통신한다. 이때 SDK를 참조하는 서버 프로그램은 Express[33]를 활용하여 [그림 25]와 같이 웹 애플리케이션을 구현 및 가동한다. 이때 서버는 순차적으로 Express 모듈과 SDK 모듈을 호출한 다음, 하이퍼레저 패브릭 네트워크에 접속하도록 코드가 작성되었으며 8080 포트를 서비스 포트로 사용하도록 하였다.

마. 웹 클라이언트 애플리케이션



[그림 27] 웹 클라이언트 애플리케이션 구성 및 흐름도

33) Express: Node.js를 위한 웹 프레임워크로 웹 서버를 가동하고 웹 애플리케이션을 개발

국방 연동 서비스의 구성 요소에는 연동 송신체계, 연동 수신체계 그리고 연동을 서비스 및 관리하는 체계가 존재한다. 앞선 '가'에서 '라'는 연동을 서비스 및 관리하는 체계의 요소였다면 '마' 웹 클라이언트 애플리케이션은 연동 송·수신체계의 영역에 해당한다.

일반적으로 연동 서비스에서 클라이언트 프로그램은 Agent, Adaptor 또는 API 형태로 구현하여 연동 대상체계에 설치된다. 하지만, 본 테스트 모듈의 클라이언트 애플리케이션은 웹(Web) 방식으로 브라우저를 통해 연동 서버로 접속할 수 있도록 개발한다. 그 이유는, 연동 송수신의 출발지와 목적지가 되는 Client Node를 모두 구성하고 테스트를 할 수도 있겠지만 그렇게 되면 유닛 테스트 목적에 비해 시스템이 불필요하게 거대해지는 문제가 발생한다. 또한, 비교적 간단한 작동 및 데이터를 확인하기에는 웹 브라우저의 UI/UX 환경이 상대적으로 효율적이라고 판단 되었기 때문이다.

웹 클라이언트 프로그램의 아키텍처는 MVC(Model View Controller)[34] 모델을 기반으로 설계하였다. 뷰 영역에 대한 웹 화면 개발 프레임워크는 AngularJS[35]를 사용하고, MVC 패턴의 컨트롤러를 포함한 전체 구조 및 웹 서버를 위한 프레임워크는 Express를 사용하였다. 개념 구조는 [그림 26]과 같이 구성하였다.

웹 화면의 소스 코드는 [그림 27]처럼 작성하였다. 일반적인 html 문서로 개발하였고 [그림 28]과 같이 스크립트를 추가하여 작동되도록 하였다.

---

34) MVC(Model View Controller): 애플리케이션을 모델, 뷰 컨트롤러 세 가지 역할로 구분하여 개발하는 개발 방법론.

35) AngularJS: 뷰 생성을 위한 강력한 템플릿 언어로 HTML 페이지 내 지시자(Directive)로 표현되는 영역 안의 각종 데이터 및 기능을 자바스크립트로 간단하게 처리할 수 있도록 한다. 구글이 지원하는 오픈 소스 웹 애플리케이션 프레임워크이며, MIT 라이선스로 무료로 배포된다.

index.html

HDIS > application > client > index.html > ...

```html
<!DOCTYPE html>
<html>
  <head>
    <title>Hyperledger Fabric Defense Iterchange System Application</title>
    <link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.min.css">
    <script src="https://ajax.googleapis.com/ajax/libs/jquery/3.2.0/jquery.min.js"></script>
    <script src="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/js/bootstrap.min.js"></script>
    <script src="https://ajax.googleapis.com/ajax/libs/angularjs/1.4.3/angular.min.js"></script>
    <style type="text/css">
      header{
        background-color: lightgray;
        font-size:20px;
        padding:20px;
      }
      header, .form-group{
        margin-bottom: 3%;
      }
      .form-group{
        width:50%;
      }
      #body{
        margin-left:3%;
        margin-right:3%;
      }
      .form-control{
        margin: 8px;
      }
       #right_header{
        width:20%;
        font-size:15px;
        margin-right:0px;
      }
      #left_header{
        margin-left:0;
        width:40%;
        display:inline-block;
      }
      #id {
        width:49%;
        display: inline-block;
      }
      table {
          font-family: arial, sans-serif;
          border-collapse: collapse;
          width: 100%;
      }
      td, th {
          border: 1px solid #dddddd;
          text-align: left;
          padding: 8px;
      }
      tr:nth-child(even) {
          background-color: #dddddd;
      }
    </style>
  </head>
```

[그림 28] 웹 화면 소스 코드

app.js

HDIS > application > client > app.js > ...

```
'use strict';
var app = angular.module('application', []);
app.controller('AppCtrl', function($scope, appFactory){
        $("#success_setmeta").hide();
        $("#success_getallmeta").hide();
        $("#success_getmeta").hide();
        $("#success_getsystem").hide();
        $("#success_changemetadata").hide();
        $("#success_deletemeta").hide();
        $scope.getSystem = function(){
                appFactory.getSystem($scope.systemid, function(data){
                        $scope.search_system = data;
                        $("#success_getsystem").show();
                });
        }
        $scope.getAllMeta= function(){
                appFactory.getAllMeta(function(data){
                        var array = [];
                        for (var i = 0; i < data.length; i++){
                                parseInt(data[i].Key);
                                data[i].Record.Key = data[i].Key;
                                array.push(data[i].Record);
                                $("#success_getallmeta").hide();
                        }
                        array.sort(function(a, b) {
                        return parseFloat(a.Key) - parseFloat(b.Key);
                        });
                        $scope.allMeta = array;
                });
        }
        $scope.getMeta = function(){
                appFactory.getMeta($scope.hdiskey, function(data){
                        $("#success_getmeta").show();
                        var array = [];
                        for (var i = 0; i < data.length; i++){
                                data[i].Id = $scope.hdiskey;
                                data[i].m_name = data[i].M_name;
                                data[i].at_1 = data[i].At_1;
                                data[i].at_2 = data[i].At_2;
                                data[i].at_3 = data[i].At_3;
                                data[i].systemid = data[i].SystemID;
                                array.push(data[i]);
                        }
                        $scope.allMeta = array;
                });
        }
        $scope.setMeta = function(){
            appFactory.setMeta($scope.meta, function(data){
                        $scope.create_meta = data;
                        $("#success_setmeta").show();
            });
        }
```

[그림 29] AngularJS 스크립트

웹 브라우저에서 REST API Server로 request를 보내면 서버의 컨트롤러에서 request의 쿼리스트링 또는 바디 정보에 따라 작동되는 체인코드를 분기 처리한다. 이때 컨트롤러는 하이퍼레저 패브릭의 SDK를 참조한다.

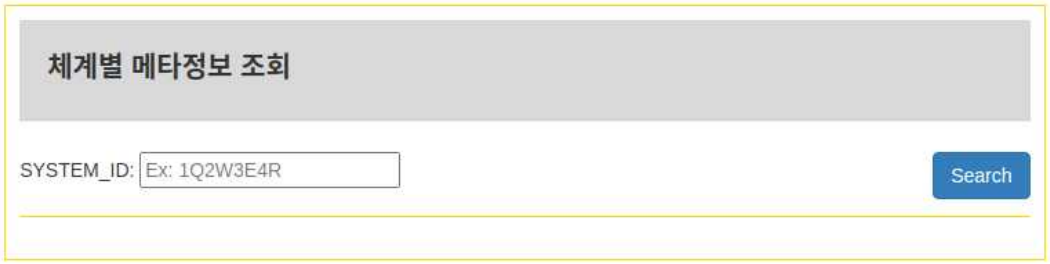
controller.js

HDIS > application > server > controller.js > ...

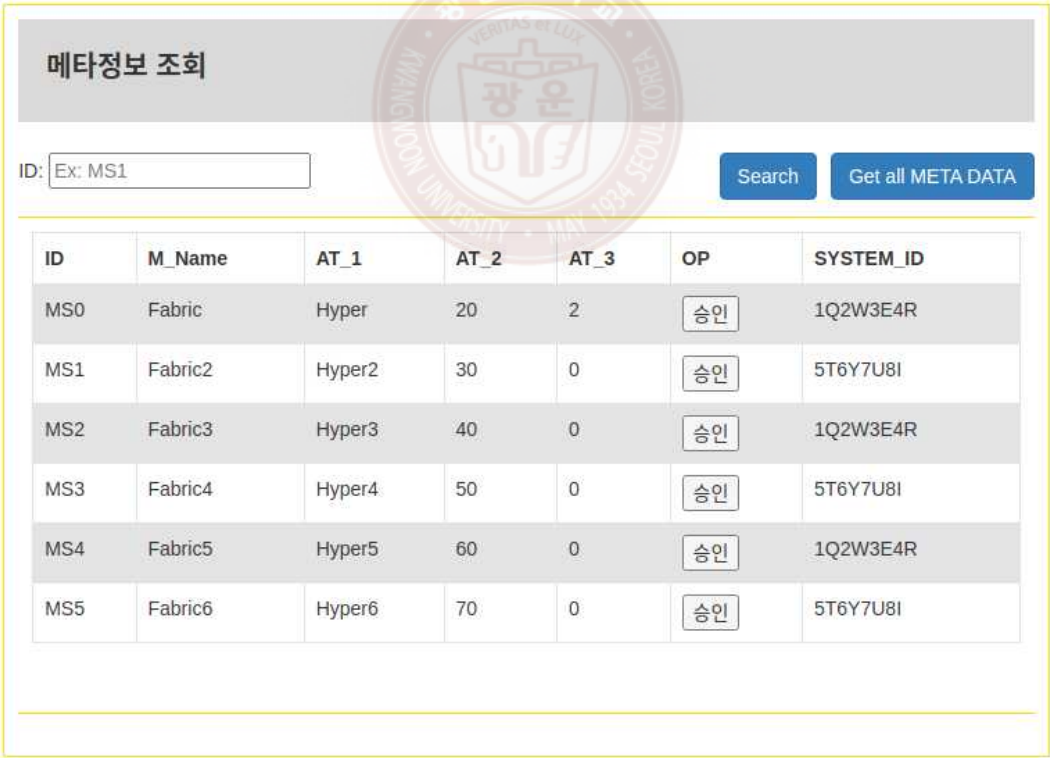
```
var sdk = require('./sdk.js');
module.exports = function(app){
  app.get('/api/getSystem', function (req, res) {
    var walletid = req.query.walletid;
    let args = [walletid];
    sdk.send(false, 'getSystem', args, res);
  });
  app.get('/api/setSystem', function(req, res){
    var name = req.query.name;
    var id = req.query.id;
    var coin = req.query.coin;
    let args = [name, id, coin];
    sdk.send(true, 'setSystem', args, res);
  });
  app.get('/api/getMeta', function(req, res){
    var hdiskey = req.query.hdiskey;
    let args = [hdiskey];
    sdk.send(false, 'getMeta', args, res);
  });
  app.get('/api/setMeta', function (req, res) {
    var title = req.query.title;
    var singer = req.query.singer;
    var price = req.query.price;
    var walletid = req.query.walletid;
    let args = [title, singer, price, walletid];
    sdk.send(true, 'setMeta', args, res);
  });
  app.get('/api/getAllMeta', function (req, res) {
    let args = [];
    sdk.send(false, 'getAllMeta', args, res);
  });
  app.get('/api/approvalMeta', function (req, res) {
    var walletid = req.query.walletid;
    var hdiskey = req.query.hdiskey;
    let args = [walletid, hdiskey];
    sdk.send(true, 'approvalMeta', args, res);
});
  app.get('/api/changeMetaData', function(req, res){
    var hdiskey = req.query.hdiskey;
    var price = req.query.price;
    let args = [hdiskey, price];
    sdk.send(true, 'changeMetaData', args, res);
  });
  app.get('/api/deleteMeta', function(req, res){
    var hdiskey = req.query.hdiskey;
    let args = [hdiskey];
    sdk.send(true, 'deleteMeta', args, res);
  });
}
```

[그림 30] REST API Server 컨트롤러 소스 코드

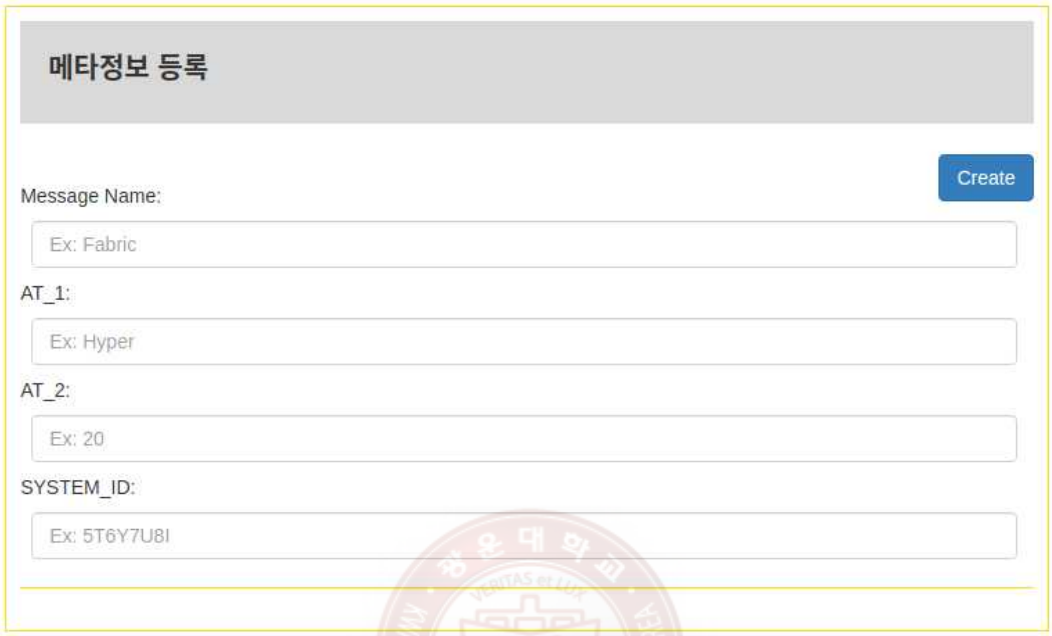
이렇게 전체 코드 개발하고 REST API Server를 구동 후 브라우저를 통해 서비스 URL인 localhost:8080으로 접속하여 [그림 30] ~ [그림 34]와 같이 완성된 테스트 모듈을 확인한다.



[그림 31] 테스트 모듈 구동 화면 - 체계별 메타정보 조회



[그림 32] 테스트 모듈 구동 화면 - 메타정보 조회



[그림 33] 테스트 모듈 구동 화면 - 메타정보 등록

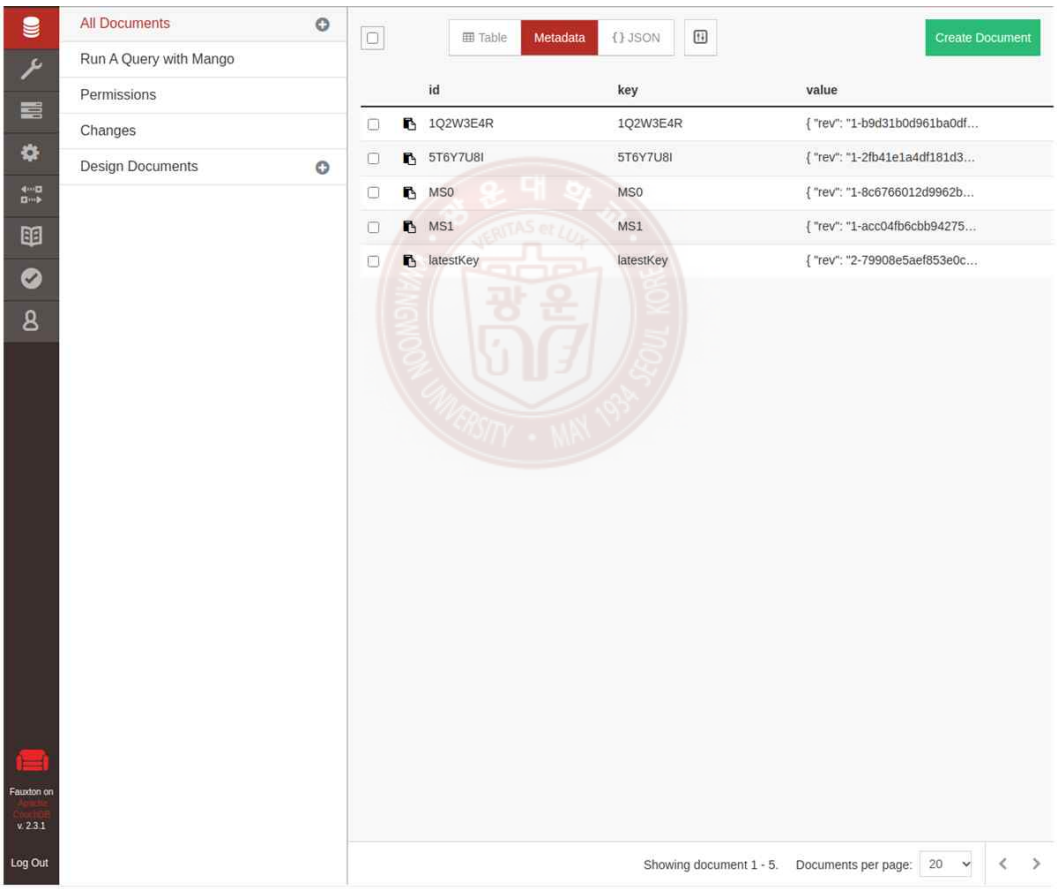
[그림 34] 테스트 모듈 구동 화면 - 메타정보 수정

[그림 35] 테스트 모듈 구동 화면 - 메타정보 삭제

개발된 테스트 모듈 화면을 통해 간단하게 META DATA 조회, META DATA 등록, META DAT 수정, META DATA 삭제의 테스트를 할 수 있다. 실제 연동 서버의 관리 기능이라고 보기에는 다소 미흡하지만, 유닛 테스트를 목적으로 하기에는 충분한 기능이다.

바. 데이터베이스

하이퍼레저 패브릭은 블록체인과 함께 CouchDB를 World State DB로 사용한다. 가에서 마까지 구축을 완료 후 자료를 저장하면 [그림 35]와 같이 상태 DB와 블록체인 원장에 데이터가 저장되는 것을 확인할 수 있다.



[그림 36] 하이퍼레저 패브릭의 World State DB

제3절 검증 및 성능 분석

1. 보안성 검증

테스트 모듈의 보안성에 대한 검증은 첫째, 기존 국방정보체계의 소프트웨어 검증에 사용되는 보안 훈령 및 평가 기준을 활용한 검증과 둘째, 패킷 분석 도구 Wireshark를 활용하여 네트워크 내에서 전송되는 데이터의 암호화 여부를 확인하는 방법으로 진행한다.

보안성 검증의 범위는 테스트 모듈의 구현 범위와 같으며 소프트웨어 개발 보안 가이드 충족 여부는 현재 블록체인을 정량적으로 평가할 수 있는 기준이 존재하지 않는 점을 고려하여 적용할 수 있는 부분만 체크 하도록 한다.

가. 소프트웨어 개발 보안 가이드 충족 여부 확인

‘국방보안업무훈령’과 ‘국방사이버안보훈령’의 국방 정보시스템 보호 관리의 기본원칙으로 소프트웨어 개발 보안 업무는 행정안전부 장관이 공지한 ‘소프트웨어 개발 보안 가이드’를 충족하게 되어 있다. 그리고 소프트웨어 개발 보안 가이드의 소프트웨어 개발 보안 대상 및 진단기준은 설계단계의 보안 설계 기준 총 20개 항목과 구현단계의 보안 약점 제거 기준 총 49개 항목을 따르게 되어 있다. 본 테스트 모듈의 보안 가이드 충족 여부는 개발 방법상의 시큐어 코딩 여부를 따지는 것이 아니라 모델설계의 보안 적절성 여부를 판단하는 것이므로 <표 16>~<표 19> 설계단계의 보안 설계 기준으로 검증을 진행한다.

❖ 입력데이터 검증 및 표현: 사용자와 프로그램의 입력데이터에 대한 유효성 검증 체계를 갖추고, 유효하지 않은 값의 처리 방법 설계

<표 16> 입력데이터 검증 및 표현(설계단계 보안기준)

번호	설계항목	설 명
1	DBMS 조회 및 결과 검증	DBMS 조회시 질의문(SQL) 내 입력값과 그 조회결과에 대한 유효성 검증방법(필터링 등) 설계 및 유효하지 않은 값에 대한 처리방법 설계
2	XML 조회 및 결과 검증	XML 조회시 질의문(XPath, XQuery 등) 내 입력값과 그 조회결과에 대한 유효성 검증방법(필터링 등) 설계 및 유효하지 않은 값에 대한 처리방법 설계
3	디렉토리 서비스 조회 및 결과 검증	디렉토리 서비스(LDAP 등)를 조회할 때 입력값과 그 조회결과에 대한 유효성 검증방법 설계 및 유효하지 않은 값에 대한 처리방법 설계
4	시스템 자원 접근 및 명령어 수행 입력값 검증	시스템 자원접근 및 명령어를 수행할 때 입력값에 대한 유효성 검증방법 설계 및 유효하지 않은 값에 대한 처리방법 설계
5	웹 서비스 요청 및 결과 검증	웹 서비스(게시판 등) 요청(스크립트 게시 등)과 응답결과(스크립트를 포함한 웹 페이지)에 대한 유효성 검증방법 설계 및 유효하지 않은 값에 대한 처리방법 설계
6	웹 기반 중요 기능 수행 요청 유효성 검증	비밀번호 변경, 결제 등 사용자 권한 확인이 필요한 중요기능을 수행할 때 웹 서비스 요청에 대한 유효성 검증방법 설계 및 유효하지 않은 값에 대한 처리방법 설계
7	HTTP 프로토콜 유효성 검증	비정상적인 HTTP 헤더, 자동연결 URL 링크 등 사용자가 원하지 않은 결과를 생성하는 HTTP 헤더·응답결과에 대한 유효성 검증방법 설계 및 유효하지 않은 값에 대한 처리방법 설계
8	허용된 범위내 메모리 접근	해당 프로세스에 허용된 범위의 메모리 버퍼에만 접근하여 읽기 또는 쓰기 기능을 하도록 검증방법 설계 및 메모리 접근요청이 허용범위를 벗어났을 때 처리방법 설계
9	보안기능 입력값 검증	보안기능(인증, 권한부여 등) 입력 값과 함수(또는 메소드)의 외부입력 값 및 수행결과에 대한 유효성 검증방법 설계 및 유효하지 않은 값에 대한 처리방법 설계
10	업로드·다운로드 파일 검증	업로드·다운로드 파일의 무결성, 실행권한 등에 관한 유효성 검증방법 설계 및 부적합한 파일에 대한 처리방법 설계

자료: KISA, “소프트웨어 개발보안 가이드”, 행정안전부, 2021.11.

❖ 보안 기능: 인증, 접근통제, 권한관리, 비밀번호 등의 정책이 적절하게 반영될 수 있도록 설계

<표 17> 보안 기능(설계단계 보안기준)

번호	설계항목	설 명
1	인증 대상 및 방식	중요정보·기능의 특성에 따라 인증방식을 정의하고 정의된 인증방식을 우회하지 못하게 설계
2	인증 수행 제한	반복된 인증 시도를 제한하고 인증 실패한 이력을 추적하도록 설계
3	비밀번호 관리	생성규칙, 저장방법, 변경주기 등 비밀번호 관리정책별 안전한 적용방법 설계
4	중요자원 접근통제	중요자원(프로그램 설정, 민감한 사용자 데이터 등)을 정의하고, 정의된 중요자원에 대한 신뢰할 수 있는 접근통제 방법(권한관리 포함) 설계 및 접근통제 실패 시 처리방법 설계
5	암호키 관리	암호키 생성, 분배, 접근, 파기 등 암호키 생명주기별 암호키 관리방법을 안전하게 설계
6	암호연산	국제표준 또는 검증필 암호모듈로 등재된 안전한 암호 알고리즘을 선정하고 충분한 암호키 길이, 솔트, 충분한 난수 값을 적용한 안전한 암호연산 수행방법 설계
7	중요정보 저장	중요정보(비밀번호, 개인정보 등)를 저장·보관하는 방법이 안전하도록 설계
8	중요정보 전송	중요정보(비밀번호, 개인정보, 쿠키 등)를 전송하는 방법이 안전하도록 설계

자료: KISA, “소프트웨어 개발보안 가이드”, 행정안전부, 2021.11.

❖ 에러처리: 에러 또는 오류 상황을 처리하지 않거나 불충분하게 처리되어 중요정보 유출 등 보안 약점이 발생하지 않도록 설계

<표 18> 에러처리(설계단계 보안기준)

번호	설계항목	설 명
1	예외처리	오류메시지에 중요정보(개인정보, 시스템 정보, 민감 정보 등)가 노출되거나, 부적절한 에러·오류 처리로 의도치 않은 상황이 발생하지 않도록 설계

자료: KISA, “소프트웨어 개발보안 가이드”, 행정안전부, 2021.11.

❖ 세션 통제: 다른 세션 간 데이터 공유 금지 등 세션을 안전하게 관리할 수 있도록 설계

<표 19> 세션통제(설계단계 보안기준)

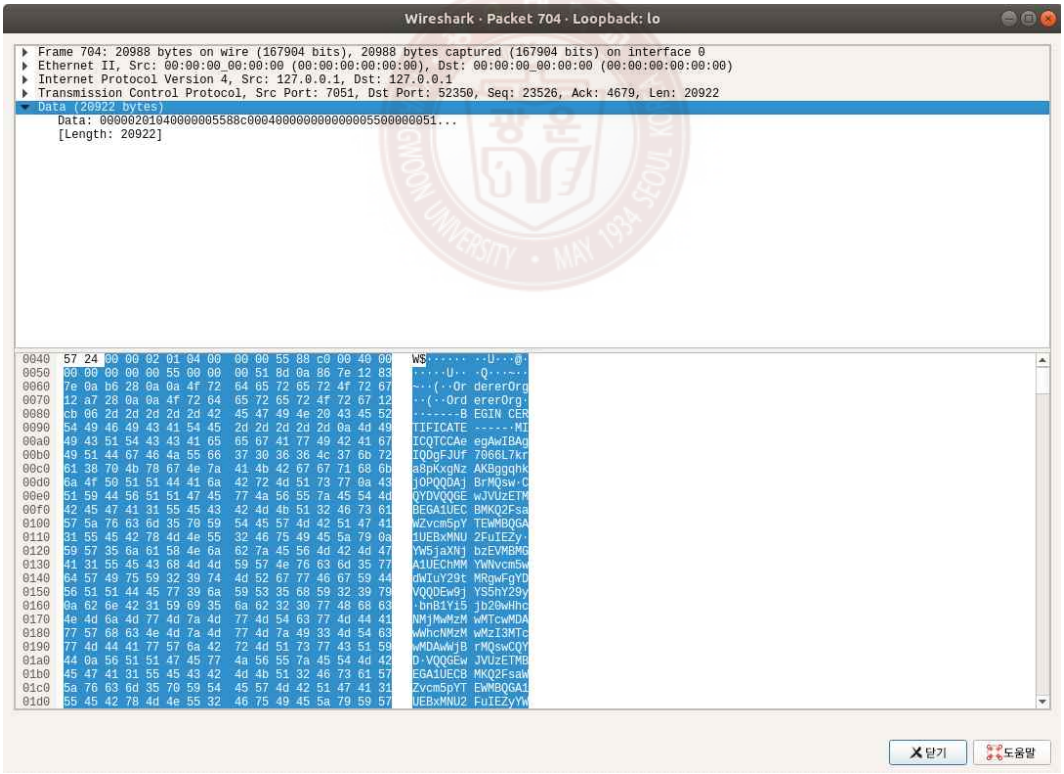
번호	설계항목	설 명
1	세션통제	다른 세션 간 데이터 공유금지, 세션ID 노출금지, (재)로그인시 기존 세션ID 재사용금지 등 안전한 세션 관리방안 설계

자료: KISA, “소프트웨어 개발보안 가이드”, 행정안전부, 2021.11.

상기 <표 16>부터 <표 19>까지 총 20개의 항목을 하이퍼레저 패브릭의 특성 및 [그림 17]의 하이퍼레저 패브릭 기반 국방연동체계 개념설계에 비교해 보면 블록체인 자체를 특정할 수 있는 항목이 별도로 구분되어 있지는 않지만, 개념적인 의미로 해석해 봤을 때 본 연구에서 제시한 개념설계의 국방정보체계 적용에는 특별한 문제가 없다는 것을 확인할 수 있다.

나. 패킷 분석 도구를 활용한 패킷 암호화 여부 검증

테스트 모듈이 구동되는 환경에 패킷 분석 도구(Wireshark)를 작동시킨 후 체인코드를 실행시켜 gRPC 통신 및 Transaction을 발생시키면 [그림 36]과 같은 데이터 패킷을 캡처할 수 있다. 그리고, 캡처된 패킷을 통해 모듈의 블록체인 네트워크는 PKI 기반으로 암호화 되어 통신이 이루어지고 있는 것을 확인할 수 있다. 이는 소프트웨어 개발 보안 가이드의 암호화 여부를 충족하여 국방 정보체계의 권장 수준에 부합한다고 판단할 수 있다.



[그림 37] Wireshark를 활용한 패킷분석(암호화 검증)

2. 효율성 검증

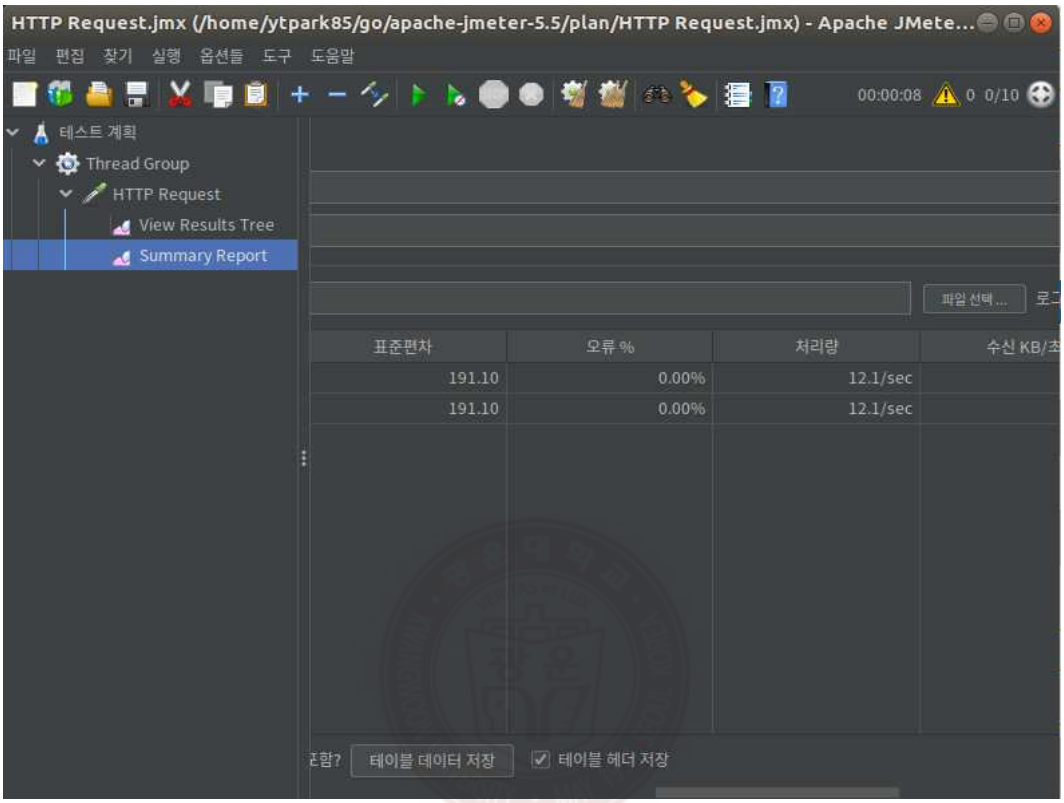
테스트 모듈의 효율성에 대한 검증은 시스템 성능점검 도구인 JMeter를 활용하여 Client가 Transaction을 발생시키면 REST API Server의 Node.js 코드에서 하이퍼레저 패브릭 네트워크 내 피어 노드의 체인코드로 액세스 후 비즈니스 로직을 처리하고 다시 Client로 응답하는 시간을 체크 하여 블록체인의 초당 원장 처리 속도인 TPS(Transaction Per Seconds)를 측정한 값을 토대로 판단한다. 다만, 본 연구에서 유닛 테스트를 구동하는 환경이 개인용 컴퓨터 수준의 소규모 장비라는 점, 그리고 Oracle Virtual Box 가상화 환경에서 Docker Container 기반으로 작동하는 애플리케이션이라는 점을 고려해볼 때 TPS가 보여주는 절대적인 수치는 실험의 성패를 논할 정도의 의미가 있다고 말하긴 힘들다. 이러한 환경에서 산출된 결괏값을 해당 시스템에서 낼 수 있는 최적의 퍼포먼스라고 볼 수 없고, 소규모 연구의 특성상 최상의 환경을 구축하기에는 현실적으로 어려움이 따르기 때문에, 주어진 환경에서 원하는 작동과 테스트가 수행되는지에 초점을 둔다.

따라서, 테스트 모듈의 조회, 등록, 수정, 삭제 등 구축된 기능이 웹 클라이언트 프로그램 ↔ REST API Server ↔ SDK ↔ 블록체인 네트워크(체인코드 포함)를 통해 유기적으로 동작하고 JMeter를 통해 속도를 측정하는 데 문제가 없다면 실험의 개념설계와 테스트 모듈이 실제 국방정보체계에 적용할 수준으로 효율성이 검증되었다고 판단한다.

TPS 산출 공식은 「거래 횟수 / 응답시간」이며 실험방법은 JMeter에 Thread 10, 반복 횟수 10으로 설정 후 HTTP Request를 통해 초당 Transaction의 처리량을 구하고 해당 작업을 10회 반복하여 평균을 산출한다.

<표 20> 테스트 모듈 TPS 측정표

순번	Data Volume	TPS(Transaction Per Seconds)
1	500 Byte	12.1
2	500 Byte	12.2
3	500 Byte	11.4
4	500 Byte	12.2
5	500 Byte	12.2
6	500 Byte	12.6
7	500 Byte	11.8
8	500 Byte	12.1
9	500 Byte	11.6
10	500 Byte	12.1
평균		12.03



[그림 38] 성능점검 도구(JMeter) 작동 화면

<표 27>은 테스트 모듈의 TPS를 산출한 값이고 [그림 37]은 성능점검 도구 작동 화면이다. 테스트의 평균값은 12.03TPS이다. 이 값은 일반에 알려진 하이퍼레저 패브릭의 처리 속도가 수천 TPS 이상이라는 점을 미루어볼 때 비교적 낮은 수치라고 할 수 있지만, 구현환경에 따른 많은 제약적 조건으로 인하여 나타난 결과이며 앞서 설명한 바와 같이 본 실험은 유닛 테스트 자체의 수행 가능 여부에 중점을 두고 진행했다는 점에서 그 의미가 있고 해당 실험 결과는 충분히 의미 있는 성과를 얻었다고 생각한다. 그러므로, 본 연구의 테스트 모듈은 효용성 측면에서도 적합하다고 판단한다.

제5장 결론

이른바 4차 산업혁명이라 불리는 차세대 기술의 혁신은 우리 민간 사회뿐만 아니라 국방 기술의 패러다임과 더 나아가 기반 기술의 근간 자체를 크게 뒤흔들고 있다. 일부 전문가들은 선사시대부터 지금까지 인류가 겪은 변화의 크기보다 4차 산업혁명을 통한 변화가 더 크다고 표현할 정도다.

이렇듯 하루가 다르게 급변하는 시대적 상황 속에서 국방 정보체계에서 요구되는 보안기술의 개념은 블록체인 기술을 중심으로 새롭게 변화하였고, 이 블록체인 기술을 국방 분야에 적용하는 일은 매우 중요한 연구 주제가 되었다. 이는 현시대의 대한민국 국방 보안 관련 종사자 모두가 함께 해결해야 할 시급한 당면과제 중 하나이다.

이런 관점에서 본 연구는, 국방정보체계에 대한 기밀성, 가용성, 무결성, 인증 등 다양한 보안 요구사항을 충족시키기 위해 아래의 절차에 따라 연구를 진행하였다.

① 국방 정보체계 분야의 정보보안 수준 향상을 위한 블록체인 기술의 잠재적 활용 가능성을 탐색

② 국방 정보체계의 특성 파악 및 분류를 통해 블록체인 기술을 적용할 수 있는 대상체계 선정: 국방 블록체인 적용 대상체계 선정기준표 작성 및 활용

③ 현존하는 다양한 블록체인 플랫폼 중 국방 특성에 가장 부합하는 플랫폼이 무엇인지 선정: 국방 블록체인 플랫폼 선정기준표 작성 및 활용

④ 개념모델 설계: 하이퍼레저 패브릭 아키텍처를 활용하여 하이퍼레저 패브릭 기반 국방연동체계 개념도 설계

⑤ 테스트 환경 구축: 13th Gen Intel(R) Core(TM) i7-13700H, LPDDR5 32GB 성능의 워크스테이션급 PC를 활용하여 가상화 시스템(VM, Virtual Machine) 기반으로 Ubuntu(Linux) 운영체제 시스템을 구축 후 리눅스의 응용프로그램들을 프로세스 격리 기술을 사용해 컨테이너 형태로 실행하고 관리하는 DOCKER를 통해 테스트 모듈의 구현 및 실험을 위한 환경을 구축

⑥ 테스트 모듈 개발: 하이퍼레저 패브릭 기반 국방연동체계 상세 구성도를 통해 시스템을 설계 후 웹 애플리케이션 프레인워크로 AngularJS, 서버 프레임워크로 Express, 서버 애플리케이션 언어로 Node.js, 체인코드 언어로 Go를 선정하여 개발

⑦ 보안성 및 효율성 실험을 통해 이 기술을 정말 국방 분야에 적용할 수 있을지에 대한 실증

위 절차는 어떠한 신기술을 특정 분야에 적용하는 데 필요한 모든 단계를 포함하는 것이며 본 연구는 국방 분야에서 그러한 절차를 모두 완료한 최초의 연구라는 점에서 그 의미가 크다고 할 수 있다. 또한, 이와 같은 연구 성과가 지속된다면 타 신기술 대비 상대적으로 소외된 국방 분야 블록체인 기술에 관한 대규모 연구와 투자가 대대적으로 이루어지게 되는 기폭제가 될 수 있다는

데에 큰 의미가 있다고 할 수 있다.

블록체인 기술은 정보체계의 인프라를 구성하는 기반 기술이므로 군내 도입을 위해서는 장기적인 관점에서 접근이 필요하다. 본 연구는, 그 절차의 시작점에서 블록체인 기술의 군 도입을 위한 가능성을 탐색하고 의미 있는 수준으로 실험에 성공하였다. 하지만 소규모 실험실 수준의 개발환경에 따른 제약사항으로 하이퍼레저 패브릭이 제공하는 성능 전체를 활용하는 테스트를 진행할 수 없었음에 한계가 존재한다. 따라서, 추후 지금까지의 연구와 경험을 바탕으로 진행되어야 할 세 가지 향후 과제를 제시한다.

첫째, 국방부 차원에서 국방통합데이터센터(DIDC, Defense Integrated Data Center)를 활용한 IaaS(Infrastructure as a Service), PaaS(Platform as a Service) 또는 SaaS(Software as a Service) 환경을 구축하여 블록체인과 다양한 차세대 기술의 융복합 연구를 주도해야 한다. 이것은 비단 블록체인뿐만 아니라 AI를 비롯한 국방 관련 신기술 전체의 창의적 발전에 훌륭한 밑거름이 될 것이다. 둘째, 기술 도입 초기 단계의 핵심은 신속한 시범사업 발굴이다. 이는 국방 정보체계에서 블록체인의 저변을 확대하는 동시에 사업수행 간 발생하는 개발 기준과 활용방안의 표준화 그리고 블록체인 기술이 가지는 특이점에 대한 정책과 법 제도적 측면의 한계 극복을 위한 많은 시사점을 제시할 것이다. 셋째, 하이퍼레저 패브릭을 국방에 도입하기 전 필수 연구로, 플랫폼이 제공하는 기본 모듈 구성 중 커스터마이징을 통해 성능개선이 가능한 부분에 관한 연구가 선행되어야 한다. 예를 들어, 하이퍼레저 패브릭이 기본 제공하는 World State DB인 CouchDB를 Scale-Out 및 In-Memory 구조에서 상대적으로 더 나은 성능을 보이는 Couchbase나 MongoDB로 대체한다면 한층 더 효율적인 원장(Ledger)을 구성하는 데 도움이 될 수 있다.

군의 기술 개발은 그 특성상 국내·외를 막론하고 다양한 환경에서 신기술을 적용할 수 있는 적합한 조건을 지니고 있다. 그러한 과정에서 국방 기술은 늘 인류에게 새로운 경험을 제시해주곤 하였으며, 그 대표 사례로 꼽히는 인터넷의 시초 알파넷(ARPANET)을 통해 기술의 발전은 언제나 새로운 시도와 끊임없는 연구로 혁신을 만들어낸다는 것을 알 수 있다. 이처럼 우리 군은, 앞으로도 지속적인 블록체인 기술의 국방적용에 관한 연구를 통해 증가하는 사이버 위협에 대한 대응뿐만 아니라 국방 정보화 업무의 질적 개선과 미래 전투환경에 대응할 수 있도록 근본적인 패러다임의 변혁을 맞이할 것이다.

또한, 2023년 현재 대한민국 정부가 추진하는 국방혁신 4.0은 전력증강체계 혁신을 통해 4차 산업혁명 과학기술 기반의 미래 합동작전개념을 구현하고, 전장을 주도할 수 있는 AI 기반의 핵심 첨단전력을 적기에 확보여 AI 과학기술 강군을 육성하는 것을 목표의 한 축으로 하며, 세부 사항으로 유·무인 복합전투체계 구축, 우주·사이버·전자기 스펙트럼 영역 작전수행능력 강화, 합동 전 영역 지휘통제(JADC2) 체계 구축을 제시하였다. 이러한 상황에서 사이버안보는 그 무엇보다 중요한 요소이고 그중 블록체인을 적용한 AI, 미래 네트워크의 융복합 개발은 국방혁신 4.0 시대의 한 축을 담당할 수 있다고 생각한다.

결과적으로, 대한민국 국방은 이러한 시대적 흐름에 맞춰 블록체인을 통한 차세대 융복합 기술의 노하우가 쌓여 궁극적으로 글로벌 군사 강국들과 견줘도 뒤지지 않는 미래의 첨단군대로 발돋움할 수 있을 것이다.

참고 문헌

1. 국내 문헌

[1] 안재홍, “블록체인 기술의 군내 도입방안 연구”, 국방과학연구소, 2018.

[2] 김두환, 박호정, “군보안상 해킹대응방안에 관한 연구”, 융합보안논문지, 제17권 제5호, pp. 133-142, 2017.

[3] 박건, “국방보안과 블록체인의 활용”, 월간군사저널, 2022.

[4] 이경휴, 박혜숙, “국방 블록체인 기술 동향 및 국방 ICT 융합 전략 연구”, (ETRI)전자통신동향분석 35권 제1호, 2020.

[5] 김세용 외 2인 “국방분야 인공지능과 블록체인 융합방안 연구”, 인터넷정보학회논문지, 2020.

[6] 김기원, “블록체인기술의 글로벌 동향과 한국 국방 적용 연구”, (한국국방연구원)국방정책연구 통권137호, pp. 105-132, 2022.

[7] 강석율, “미국의 3차 상쇄전략 추진 동향과 시사점”, KIDA Briefs 2022-안보-3, pp. 1-4, 2022.

[8] 한혜경, 황희정, “하이퍼레저 패브릭과 비대칭키 암호화 기술을 결합한 건강정보 관리서버”, 한국멀티미디어학회논문지, 2022.

[9] 박용탁, “국방정보체계 실시간 서비스 통합 방안 연구: 국방 REST API Server 참조모델 설계 분석”, 선진국방연구, 2021.

[10] 국방부(정보화기획담당관), “국방 정보화업무 훈령”, 국방부훈령, 제2649호, 2022.5.6.

[11] 국방부, “국방보안업무훈령”, 국방부훈령, 제2425호, 2020.5.11.

[12] 국방부, “국방사이버보안훈령”, 국방부훈령, 제2361호, 2019.12.19.

[13] KISA, “소프트웨어 개발보안 가이드”, 행정안전부, 2021.11.

[14] 과기부, “블록체인 산업 진흥 전략”, 제15차 정보통신전략위원회, 2022.

[15] 국방부, “국방혁신 4.0 기본계획 발표”, 국방부 보도자료, 2023.3.3.

2. 국외 문헌

[1] Karl Wüst & Arthur Gervais, “Do you need a Blockchain?”, Crypto Valley Conference, 2018.

[2] USA DoD, “DIGITAL MODERNIZATION STRATEGY - Block Chain Cybersecurity Shield”, DoD Information Resource Management Strategic Plan FY 19-23, 2019.

[3] Satoshi Nakamoto, “A Peer-to-Peer Electronic Cash System”, www.bitcoin.org, 2008.

[4] Hyperledger fabric Official Document, “hyperledger fabric read the docs”, https://hyperledger-fabric.readthedocs.io/en/release-2.5/, 2023.

[5] AneraAlahbabiet al., “ESTABLISHING SECURITY CONTROLS FOR BLOCKCHAIN TECHNOLOGY IN P2P ENERGY TRADING”, 2023 IEEE PES Conference on Innovative Smart Grid Technologies - Middle East, 2023.

[6] Soto, Daren, “Potential Uses of Blockchain by the U.S. Department of Defense”, Value Technology foundation, 2020.

[7] Alessia et al., “Blockchain in Defense: A Breakthrough?”, Finabel European Army Interoperability Center, 2020.

3. 기타

[1] AWS, “블록체인 기술이란 무엇입니까?”, (https://aws.amazon.com/ko/what-is/blockchain/?aws-products-all.sort-by=item.additionalFields.productNameLowercase&aws-products-all.sort-order=asc, 검색일 2022.12.01.).

[2] 해시넷, “블록체인”, (http://wiki.hash.kr/index.php/블록체인, 검색일 2022.12.01.).

[3] CCTVnews, “고성능 블록체인 속도의 허와 실”, (https://www.cctvnews.co.kr/news/articleView.html?idxno=212435, 검색일 2022.12.15.).

[4] LG CNS, “쉽게 이해하는 블록체인”, (https://blog.lgcns.com/1597, 검색일 2022.12.20.).

[5] 동아일보, “軍 허술한 보안이 해킹 자초”, (https://www.donga.com/news/Politics/article/all/20161207/81705840/1, 검색일 2022.12.22.).

[6] 연합뉴스, “현역장교 군사기밀 유출 상황도”, (https://www.yna.co.kr/view/GYH20220428002400044, 검색일 2022.12.22.).

[7] 한국일보, “현역 장교가 北 공작원에 군사기밀 유출...대가는 비트코인”, (https://m.hankookilbo.com/News/Read/A2022042816070004389, 검색일 2022.12.22.).

[8] DB-ENGINES, “DB-Engines Ranking - Trend Popularity”, (https://db-engines.com/en/ranking_trend, 검색일 2022.12.27.).

[9] 위키백과, “스마트 계약”,
(https://ko.wikipedia.org/wiki/%EC%8A%A4%EB%A7%88%ED%8A%B8_%EA%B3%84%EC%95%BD, 검색일 2023.04.27.).