

---

저자 (Authors)	김희열 Heeyoul Kim
출처 (Source)	<a href="#">한국정보기술학회논문지 16(5)</a> , 2018.5, 103-112 (10 pages) <a href="#">The Journal of Korean Institute of Information Technology 16(5)</a> , 2018.5, 103-112 (10 pages)
발행처 (Publisher)	<a href="#">한국정보기술학회</a> Korean Institute of Information Technology
URL	<a href="http://www.dbpia.co.kr/journal/articleDetail?nodeId=NODE07442113">http://www.dbpia.co.kr/journal/articleDetail?nodeId=NODE07442113</a>
APA Style	김희열 (2018). 블록체인 플랫폼의 보안 위협과 대응 방안 분석. 한국정보기술학회논문지, 16(5), 103-112.
이용정보 (Accessed)	한림대학교 210.115.***.23 2021/11/05 12:51 (KST)

---

### 저작권 안내

DBpia에서 제공되는 모든 저작물의 저작권은 원저작자에게 있으며, 누리미디어는 각 저작물의 내용을 보증하거나 책임을 지지 않습니다. 그리고 DBpia에서 제공되는 저작물은 DBpia와 구독계약을 체결한 기관소속 이용자 혹은 해당 저작물의 개별 구매자가 비영리적으로만 이용할 수 있습니다. 그러므로 이에 위반하여 DBpia에서 제공되는 저작물을 복제, 전송 등의 방법으로 무단 이용하는 경우 관련 법령에 따라 민, 형사상의 책임을 질 수 있습니다.

### Copyright Information

Copyright of all literary works provided by DBpia belongs to the copyright holder(s) and Nurimedia does not guarantee contents of the literary work or assume responsibility for the same. In addition, the literary works provided by DBpia may only be used by the users affiliated to the institutions which executed a subscription agreement with DBpia or the individual purchasers of the literary work(s) for non-commercial purposes. Therefore, any person who illegally uses the literary works provided by DBpia by means of reproduction or transmission shall assume civil and criminal responsibility according to applicable laws and regulations.

## 블록체인 플랫폼의 보안 위협과 대응 방안 분석

김 희 열\*

### Analysis of Security Threats and Countermeasures on Blockchain Platforms

Heeyoul Kim\*

---

본 연구는 경기도의 경기도지역협력연구센터사업의 일환으로 수행하였음. [GRRC경기 2017-B03, 지능정보기반 보안 및 네트워크 기술 연구]

---

#### 요 약

블록체인 기술은 4차 산업혁명의 핵심 기술로 주목받고 있으며, 중앙의 신뢰기관이 필요 없는 탈중앙화된 구조와 합의를 통한 원장 관리를 통해 높은 신뢰성과 고가용성을 제공한다. 블록체인을 암호화폐 및 금융 분야뿐만 아니라 물류, 의료, 공공 분야 등 다양한 분야에서 적용하려는 시도가 진행되고 있다. 하지만, 블록체인에 대한 기대를 충족하기 위해서는 핵심 기술의 발전이 필요하며, 특히 블록체인 보안에 대한 많은 연구가 필요하다. 본 논문에서는 블록체인 기술과 대표적인 블록체인 플랫폼들에 대해 분석하고, 현재의 기술 수준과 문제점을 살펴본다. 특히 블록체인 시스템을 위협하는 다양한 형태의 보안 위협을 분석하고 이를 해결할 수 있는 대응 방안을 제시한다.

#### Abstract

The blockchain technology is attracting attention as a core technology of the 4<sup>th</sup> industrial revolution, and it provides trustworthiness and high availability through a decentralized structure without a centralized trusted third party and a distributed ledger based on participants' consensus. Various attempts are being made to apply blockchain in logistics, medical, and public sector as well as cryptocurrency and finance. However, in order to meet the expectation, it is necessary to develop the core technology, especially in the security area. In this paper, we analyze blockchain technology and representative blockchain platforms, and discuss current levels and problems. Especially, we analyze various security threats and propose corresponding countermeasures to solve them.

#### Keywords

blockchain, blockchain platform, security, consensus

---

\* 경기대학교 컴퓨터공학부 교수  
- ORCID: <https://orcid.org/0000-0001-6341-580X>

· Received: Apr. 06, 2018, Revised: May 16, 2018, Accepted: May 19, 2018  
· Corresponding Author: Heeyoul Kim  
Dept. of Computer Science, Kyonggi University, 94-6 Iuidong, Yeongtonggu, Suwon, Gyeonggi, 443-760, Korea,  
Tel.: +82-31-249-9675, Email: [heeyoul.kim@kgu.ac.kr](mailto:heeyoul.kim@kgu.ac.kr)

## I. 서 론

블록체인 기술은 비트코인(Bitcoin)[1] 등의 암호 화폐에서 사용되고 있는 핵심 기술이며, 많은 금융 기관과 IT 기업, 정부 등 다양한 분야에서 블록체인을 적용하려는 시도를 진행하고 있다. 블록체인은 탈중앙화와 분산 원장에 기록된 정보의 비가역성을 제공하는 장점을 가지며, 향후 5년 내에 주요 산업 분야에 적용되어 4차 산업을 이끌어갈 핵심 기술로 주목받고 있다.

블록체인 시스템 내에서 주기적으로 사용자 간의 신규 거래내역들을 포함한 새로운 블록이 생성되며, 이 블록은 기존 블록체인의 뒤에 연결되는 방식을 사용한다. 이때 신규 거래내역과 블록은 사용자들에 의해 검증되고 합의가 이루어져야 추가될 수 있으며, 블록체인에 참여하는 노드들은 동일한 정보가 기록된 원장을 공유하게 된다. 블록체인 기술의 핵심은 중앙의 신뢰해야 하는 기관(TTP)이 필요 없는 분산 원장 관리 기술이며, 이러한 탈중앙화된 구조는 중앙 서버와 중재 기관의 필요성을 없앨 수 있어서 기존 시스템의 비용과 저가용성 문제를 해결할 수 있다. 그리고 블록체인 원장에 기록되는 정보는 참여 노드들의 합의를 통해서만 추가될 수 있기 때문에 원장 기록에 대한 높은 신뢰성을 확보하게 되며, 일부 노드들의 장애/악의적 변조 시도가 발생해도 전체의 합의를 유지할 수 있다.

이러한 장점을 기반으로 블록체인은 Bitcoin과 같은 암호화폐의 신뢰성을 확보하고 이중지불 문제 등을 해결하는 핵심 요소로 활용되고 있다. 그리고 금융 산업에서는 암호화폐를 활용해서 해외송금과 크라우드 펀딩 등의 서비스에 적용하고 있으며, 기존 금융 서비스 대체와 신규 금융 서비스 창출을 위해 R3 CEV 등과 같은 컨소시움을 구성해 노력하고 있다.

또한, 블록체인은 금융 분야 외에도 다양한 영역으로 적용이 확장되고 있다. 물류/유통 분야에서는 다양한 중개기관이 연계된 복잡한 운송 과정의 효율성을 높이기 위해 블록체인을 적용하는 방안을 시도 중이다. 의료 분야에서는 환자의 프라이버시를 보호하면서도 의료 기관 간 공유되는 진료정보의

신뢰성을 높이기 위해 블록체인을 고려 중이다. 사물인터넷 분야에서는 IoT 기기의 인증과 스마트 계약 기반 자동 제어를 위해 블록체인과 연계하기 위한 연구가 진행되고 있다. 이처럼 블록체인은 다양한 산업 분야에서 활용될 수 있으며, 여러 예시와 계획이 발표되고 있다.

하지만, 블록체인에 대한 매우 높은 관심과 기대에도 불구하고 블록체인 기술의 발전이 이를 충족시키는 수준까지는 도달하지 못하고 있다. 블록체인 처리 성능과 확장성에 관련된 문제, 정보 저장 용량의 증가와 과도한 연산 작업에 대한 비판 등의 문제가 제기되어 왔다. 또한, 블록체인 시스템의 보안 위협에 대한 분석과 대응 방안에 대한 연구도 부족한 상황이다.

본 논문에서는 대표적인 블록체인 플랫폼들의 특성을 비교 분석하고, 블록체인 시스템을 위협하는 다양한 형태의 보안 위협과 이를 해결하기 위한 기술 및 방안에 대해 제시한다.

본 논문의 구성은 다음과 같다. 2장에서는 블록체인 기술의 개요와 합의 알고리즘에 대해 분석하고, 3장에서는 대표적인 개방형 블록체인 플랫폼과 폐쇄형 블록체인 플랫폼에 대한 비교 결과를 제공한다. 4장에서는 현 블록체인 기술의 한계점을 분석하고, 5장에서는 블록체인 시스템을 위협하는 보안 위협을 도출하고 이에 대한 보안 기술과 대응 방안을 제시한다. 마지막으로 6장에서 결론을 맺는다.

## II. 관련 연구

### 2.1 블록체인 기술 개요

블록체인 기술은 특정 기간 동안 신규 발생한 거래 정보가 기록된 새로운 블록을 생성, 모든 참여 노드에게 전달하고 합의와 블록의 유효성이 검증된 이후 기존의 블록체인에 새 블록이 연결되는 방식을 취한다. 이렇게 블록들이 순차적으로 연결되어 분산 원장을 이루게 되고, 참여 노드들은 동일한 정보가 기록된 원장을 저장/관리하게 된다.

블록체인에서 정보가 기록되는 구조는 그림 1과 같으며, 여러 블록들이 순차적으로 연결되어 체인을 형성하게 된다.

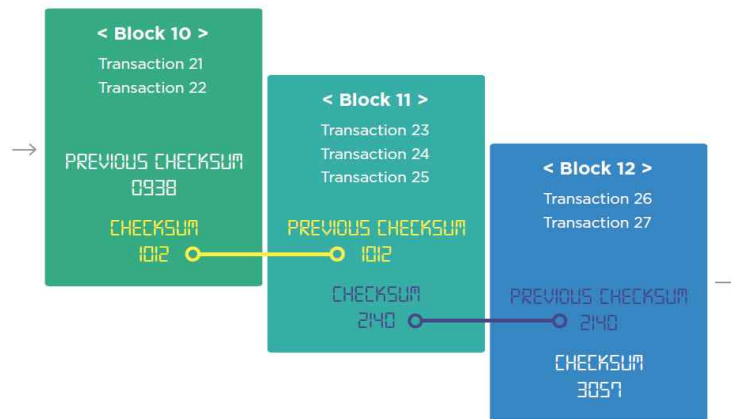


그림 1. 블록체인 구조[2]

Fig. 1. Blockchain structure

여기서 블록들이 연결된다는 의미는 새로운 블록 안에 이전 블록 정보에 대한 해쉬값이 포함되어 기록되는 것을 말한다. 해쉬값은 SHA256 등의 암호학적 해쉬 함수를 통해 계산되며, 해쉬 함수는 결과값으로부터 입력값을 유추하기 어렵다는 단방향성을 제공하기 때문에 블록체인에 기록된 내용을 위변조하려는 시도가 매우 어려워진다. 만약 공격자가 특정 블록을 위변조해서 다른 노드들의 검증을 통과하기 위해서는 해당 블록 뿐 아니라 이후 생성된 모든 블록에 대해 적합한 해쉬값을 계산해서 참여 노드들의 합의를 통과해야 하며, 이를 우회하는 것은 현실적으로 매우 어렵다고 알려졌다. 또한, 한번 블록체인에 기록된 정보는 적법한 참여자라고 할지라도 수정을 할 수 없게 되며, 이러한 특성으로 인해 블록체인 정보의 비가역성이 보장된다.

블록체인을 활용하면 원장에 기록되고 공유되는 정보의 무결성을 보장받고 정보 자체에 대한 신뢰성을 확보하게 된다. 즉, 블록체인 시스템 내의 모든 거래 내역과 이력이 기록되고 공유되기 때문에 악의적인 공격자가 거래 기록을 수정하거나 삭제, 변경하기 어렵다. 또한, 거래의 검증을 위해 블록체인 참여 노드들의 합의를 요구하기 때문에 일부 노드들의 공격만으로는 목표를 달성할 수 없다.

그리고 블록체인은 분산 원장의 형태를 가지고 탈중앙화된 구조이기 때문에 중앙의 신뢰기관을 및 중개기관을 유지할 필요가 없어 비용 면에서도 장점을 가지며 단일장애점(Single Point of Failure) 문

제를 해결한다. 또한, 블록체인 내의 스마트 계약(Smart Contract) 기술을 이용하면, 계약 내용과 비즈니스 로직이 코드의 형태로 배포되고 조건에 부합하는 거래 발생 시 자동으로 계약 내용이 수행됨을 보장할 수 있는 장점을 가진다.

## 2.2 합의 알고리즘

블록체인은 분산 원장이 공유/관리되는 분산 시스템 형태이며, 시스템 참여 노드간의 신뢰성을 보장하기 어려운 환경에서 전체 분산 시스템의 신뢰도를 보장하기 위해 합의 알고리즘을 사용한다. 즉, 악의적인 의도를 가진 노드가 분산 시스템에 참여한 상황에서도 전체 시스템은 신뢰도 있는 서비스를 제공할 수 있다는 것을 보장해야 한다는 비잔틴 장군 문제[3]를 해결하기 위해 합의 알고리즘을 사용하며, 블록체인에서 합의 알고리즘은 새로운 블록을 기존 블록체인에 추가하는 시점에서 사용되어 전체 참여노드가 동일한 정보를 공유할 수 있도록 한다.

PoW(Proof of Work, 작업증명) 방식은 비트코인에 적용된 합의 알고리즘으로, 합의에 참여하기 위해 컴퓨팅 파워 등 리소스를 투입했다는 것을 증명하는 방식이다. 비트코인에서는 신규 블록을 추가하기 위해서 채굴이라는 과정을 통해 해쉬 함수 기반의 수학적 문제를 푸는 값을 찾아야 하며, 해쉬 연산을 많이 수행할수록 채굴에 성공할 가능성이 높

아진다. 그래서 공격자가 잘못된 블록을 추가하기 위해서는 정상적인 노드 전체와 경쟁해서 전체 해쉬 파워의 과반 이상인 51%를 차지해야 하며, 이는 현실적으로 매우 어렵다고 주장된다. 하지만, PoW 방식은 과도한 연산 능력과 전력 소모를 필요로 하고 합의에 도달하는 시간이 길다는 비판이 제기되어 왔다.

PoS(Proof of Stake, 지분증명)[4] 방식은 PoW 방식의 단점을 보완하기 위해 제안되었으며, 연산 능력이 아닌 지분의 보유량에 따라 합의시 각 노드의 결정권이 달라지는 방식이다. 즉, 각 노드는 자신이 소유한 암호화폐나 지분의 비율이 높을수록 블록을 생성할 가능성이 높아지게 된다. 이 방식은 연산 능력과 전력 소모가 매우 낮은 장점을 가지며, 이더리움(Ethereum)등의 플랫폼에서 PoS 방식을 적용하기 위해 시도 중이다.

PBFT(Practical Byzantine Fault Tolerance)[5] 방식은 암호화폐 지급 등의 보상이 필요한 PoW와 PoS 방식과 달리 노드들의 자발적 참여와 검증을 기반으로 합의를 수행하는 방식이다. 즉, 비동기 네트워크 환경에서 참여 노드간에 두 번의 브로드캐스트 과정을 거쳐 합의에 도달하게 된다. 이런 특성으로 인해 PBFT는 주로 기업 내부 시스템에 적용될 수 있는 프라이빗 블록체인에서 사용되고 있다. PBFT를 개선한 다양한 방식이 제안되고 있으며, 특히 Tendermint[6]는 PBFT 방식과 DPoS(Delegated Proof of Stake)방식을 혼합한 방식을 제안했다.

### III. 블록체인 플랫폼 비교

2009년 비트코인이 처음 제안된 이후 현재까지 다양한 형태의 블록체인 플랫폼들이 개발되고 있다. 여러 플랫폼들을 분류하기 위해 다양한 기준을 적용할 수 있으며, 가장 대표적인 분류 기준은 블록체인에 새로운 블록을 추가할 수 있는 주체에 따른 분류 방식이다. 퍼블릭 블록체인은 누구나 블록체인에 참여해서 기록된 정보에 접근할 수 있고 블록 생성에도 참여할 수 있는 공개된 형태의 플랫폼이고, 프라이빗 블록체인은 미리 선정된 노드들에 의해 블록체인이 구성되고 신규 블록의 생성이 제어되는 형태의 플랫폼이다.

표 1. 퍼블릭 블록체인과 프라이빗 블록체인 플랫폼 비교 분석

Table 1. Comparison of public blockchain platform and private blockchain platform

Classification	Public Blockchain	Private Blockchain
block create right	anyone	member
block read right	anyone	policy-based
rule change	difficult	medium (member agree)
characteristic	slow transaction	fast transaction, scalability
adopting area	cryptocurrency, notarization	financial, supply chain
consensus	PoW, PoS	PBFT
platform	Bitcoin, Ethereum	Hyperledger fabric, Corda, Quorum

표 1은 퍼블릭 블록체인과 프라이빗 블록체인에 대한 비교 분석 결과를 보여준다.

퍼블릭 블록체인은 누구나 쉽게 참여 가능하고 합의 알고리즘으로 PoW, PoS 등을 사용하기 때문에, 공격자가 정보의 위변조에 성공하기 위해서는 51% 공격 등과 같이 네트워크 전체의 과반수를 차지해야 하며 이는 현실적으로 불가능하다고 인식된다. 이러한 특성을 바탕으로 다양한 암호화폐와 문서의 공증 등의 영역에서 활발히 사용되고 있으나, 신규 거래가 블록체인에 등록되기까지의 확정시간이 길고 거래의 처리성능이 떨어지는 단점을 가지고 있다.

프라이빗 블록체인은 허가된 멤버들만이 참여해서 블록체인에 접근할 수 있으며, 합의를 위해 PBFT와 유사 알고리즘을 사용하기 때문에 상대적으로 거래의 확정시간이 짧고 처리성능도 비교적 높은 편이다. 멤버에 대한 인증과 정보에 대한 암호화, 접근제어 등이 가능하기 때문에 주로 기밀 정보를 다루는 기업 내부나 여러 기업의 연계 시스템에서 선호하며, 회사 간 거래 및 정보공유, 공급망 추적 등에 활용되고 있다. 하지만, 폐쇄적인 형태이고 탈중앙화에 맞지 않기 때문에 투명성이 떨어지고 블록체인의 기본 개념에 위배된다는 비판도 있다.

### 3.1 비트코인

2009년 사토시 나카모토라는 익명의 인물에 의해 제안되었으며, 중앙기관의 개입 없이 P2P 네트워크에서 사용자간에 교환 가능한 암호화폐를 구현한 플랫폼이다. 거래 내역을 저장하고 관리하기 위한 블록체인의 형태를 사용하고, P2P 형태로 거래와 블록을 전파하기 위한 비트코인 프로토콜, 수학적 결정론적 방식의 채굴을 통한 통화 발행, 전자서명을 기반으로 스크립트를 이용한 검증 방식을 사용한다.

블록에 포함되는 대규모 거래 내용의 무결성 검증을 위해 Merkle Tree[7]를 사용하고, UTXO(Unspent Transaction Output)를 기반으로 암호화폐를 관리한다. 또한 블록체인 원장을 모두 저장하고 독립적으로 검증하는 full 노드 외에 경량의 참여자를 위해 SPV 노드를 제공하며 프라이버시 강화를 위해 블룸 필터(Bloom Filter)를 사용한다.

### 3.2 이더리움

2015년에 비탈릭 부테린에 의해 제안되었으며, 분산형 응용프로그램인 DApp의 동작을 위한 플랫폼이다[8]. 계약 내용이 코드의 형태로 표현된 스마트 계약 개념이 제공되며, 그림 2와 같이 스마트 계약이 블록체인 상에서 배포, 검증되고 특정 조건을 만족하면 계약 내용이 블록체인 내에서 자동으로 실행되는 장점을 가진다.

스마트 계약의 개발을 위해 Solidity라는 전용 언어를 사용하며, 스마트 계약은 EVM(Ethereum Virtual Machine) 가상머신에서 실행된다. 또한, 거래의 실행과 스마트 계약 코드의 실행을 관리하기 위해 Gas라는 개념을 사용하며, 이를 통해 무한 루프의 발생을 막아 DoS 공격에 대비하고 있다. 현재는 PoW 방식의 합의를 적용하고 있고, Casper 프로젝트를 통해 PoS 방식으로의 전환을 시도하고 있다.

### 3.3 Hyperledger Fabric

Hyperledger Fabric은 대표적인 프라이빗 블록체인 플랫폼으로, 리눅스 재단 산하의 hyperledger 프로젝트

트에 속해있다[10]. IBM이 주도적으로 플랫폼 개발을 진행하고 있으며, 2017년 7월 1.0 버전이 공개되었고 상당수의 기업에서 적용을 시도하고 있다.

그림 3은 Fabric의 시스템 구조와 동작 흐름을 설명하고 있다. 블록체인 참여자에 대한 인증과 접근 제어를 위해 멤버십 서비스가 존재하며, 인증서와 PKI를 활용하고 있다. Ordering service는 신규 거래들을 취합해서 순서를 결정하고 신규 블록을 생성하는 역할을 하며, 각 peer는 거래의 검증을 수행하는 endorser의 역할과 거래를 시행하는 committer의 역할을 수행한다.

또한 Fabric은 모듈화된 구조를 제공해서 다양한 합의 알고리즘을 채택할 수 있으며, 주로 PBFT와 유사한 합의 알고리즘을 사용한다. 그리고 스마트 계약과 유사한 체인코드 기능을 제공하며, 이벤트 처리를 지원한다.

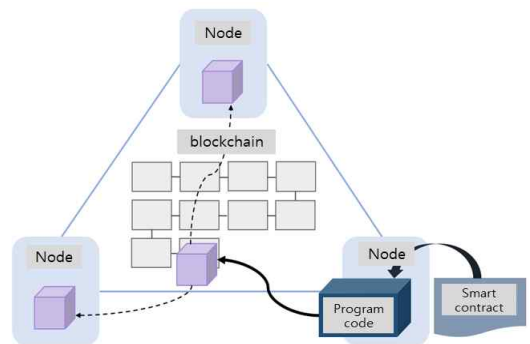


그림 2. 이더리움 구조와 스마트 계약[9]  
Fig. 2. Ethereum structure and smart contract

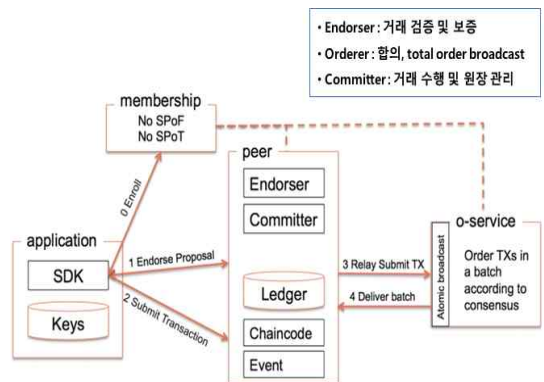


그림 3. Hyperledger fabric 구조와 동작 흐름[10]  
Fig. 3. Hyperledger fabric architecture and process flow

### 3.4 코다(Corda)

코다는 금융권에 특화된 형태의 블록체인 플랫폼으로, 2017년 10월 R3에 의해 개발되었다[11]. 금융권에서 요구하는 정보의 비공개성, 노드별 권한 제어, 빠른 속도 제공을 위해 개발되었으며, 기존 블록체인 플랫폼들과 달리 특정 계약의 당사자들 간에만 정보가 공유되는 특징이 있다. 전체 참여자들의 합의가 아닌 거래 당사자들 간에 개별적인 합의를 통해 거래의 유효성이 검증되며, notary 개념을 통해 감독기구나 금융사 그룹이 거래의 유일성을 검증한다.

## IV. 현 블록체인 기술의 한계

블록체인은 4차 산업혁명의 핵심 기술로 관심을 받고 있지만, 현재의 기술로는 해결하기 어려운 몇 가지 한계를 가지고 있다. 특히 블록체인 기반 거래의 처리 속도와 성능에 관련된 확장성 문제, 대규모 정보의 저장 및 처리 문제, 보안과 관련된 문제가 제기되고 있다.

블록체인의 성능을 표현하기 위해 초당 처리할 수 있는 트랜잭션의 수를 나타내는 TPS(Transaction Per Second)를 사용하며, 블록체인 성능을 높이기 위해서는 TPS 수치를 향상시켜야 한다. PoW, PoS 방식 등을 사용하는 비트코인, 이더리움 등의 암호화폐에서는 7~30 TPS의 성능이 나오며, 기존 신용카드 시스템과 비교했을 때 대규모 거래를 처리하기에는 크게 부족하다. PBFT 기반의 프라이빗 블록체인은 1000~1500 TPS의 성능을 제공하며, 시스템의 규모에 따라 달라지지만 여전히 충분한 수준에 도달하지 못하고 있다. 그러므로 많은 트랜잭션이 발생하는 대규모의 서비스 제공을 위해서는 블록체인의 성능 개선이 필요한 상황이다.

블록체인의 TPS를 개선하기 위해 크게 두 가지 방식이 진행되고 있다. 첫째, 하나의 신규 블록에 포함되는 트랜잭션의 수를 늘리는 방식으로, 기존 블록 구조를 수정해서 블록 크기를 늘리는 방법과 가변적으로 트랜잭션들을 포함시키는 방법이 진행 중이다. 둘째, 합의를 통해 신규 블록이 생성되는데 소요되는 시간을 단축하는 방식으로, 기존의 10

분마다 새 블록이 생성되는 PoW방식을 개선하기 위해 PoET, DPoS 등의 합의 알고리즘이 제안되고 있다.

블록체인은 분산 형태의 원장을 관리하기 때문에 모든 참여자는 동일한 원장을 각자 저장해야 하며, 규모가 커지고 시간이 지남에 따라 원장의 크기가 증가해 이를 저장하기 위한 비용 문제가 발생한다. 예를 들어, 현재 비트코인에서는 전체 원장을 저장하기 위해 참여자들이 120GB의 저장 공간을 필요로 한다. 또한, 대용량 데이터의 경우 블록체인에 직접 저장하기 어려운 문제가 있다.

이를 해결하기 위해 블록체인에는 데이터의 메타 정보만을 기록하고 실제 데이터는 별도의 분산 저장 공간을 사용하는 오프체인 방식이 개발되고 있다. 그리고 안정적인 데이터의 분산 저장을 위해서 DHT를 활용하거나 글로벌 파일 시스템인 IPFS를 사용하는 방식이 제안되어왔다.

흔히 블록체인은 보안이 강화된 시스템이라고 인식되고 있지만, 블록체인은 여러 보안 기능 중 원장 정보에 대한 무결성과 비가역성을 제공하는 데 집중되었으며 다른 보안 기능이 부족한 경우가 많다. 예를 들어, 비트코인 등의 퍼블릭 블록체인은 원장 정보를 누구나 확인할 수 있기 때문에 기밀 정보를 저장하기에 부적합하다. 또한 일부 블록체인의 경우 높은 수준의 사용자 익명성을 제공하지 못하기 때문에 참여자의 프라이버시를 침해할 가능성이 있다. 이를 해결하기 위해 인증과 정보의 암호화, 영지식 증명 기반의 익명성 제공[12] 방식이 진행되고 있다.

## V. 블록체인 보안 위협 분석과 대응 방안 제안

블록체인 기술은 원장에 기록된 정보의 무결성을 강하게 보장하지만, 상대적으로 정보의 기밀성과 사용자 인증 및 접근 제어 등 다른 보안 기능을 충분히 제공하지 못하고 있다. 특히 프라이빗 블록체인을 사용하려는 기업의 경우 이런 보안 기능이 필수적인 요구사항이며, 기존 보안 기술과 블록체인의 결합을 통해 보안 위협을 해소하려는 연구가 진행되고 있다. EU 산하의 ENISA와 금융보안원에서는 금융권에서 블록체인 시스템을 도입할 때 고려해야 할 보안 이슈를 제시했다[13].

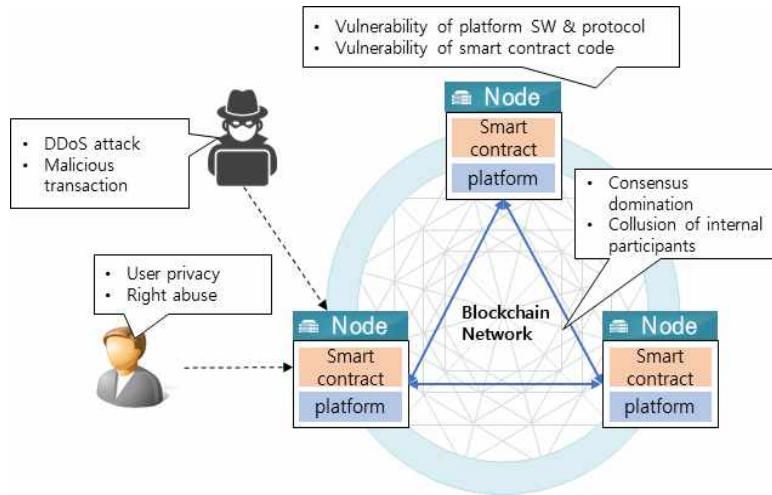


그림 4. 블록체인 주요 보안 위협과 대상  
Fig. 4. Security threats and targets on Blockchain

표 2. 블록체인 보안 위협 대응 방안 제안

Table 2. Proposal of countermeasures against security threats on Blockchain

	Threat	Countermeasure
transaction validation & consensus	consensus domination	monitoring consensus status
	collusion of internal participants	verification based on anchoring
privacy & access control	privacy	adopting FHE
	right abuse	smart contract based access control
blockchain software security	vulnerability of SW & protocol	standard, certification
	vulnerability of smart contract	detecting vulnerability focused on smart contract
blockchain service security	DDoS attack	spam filtering based on reputation
	malicious transaction	fraud detection system for blockchain

그림 4는 블록체인 시스템에서 보안 위협의 대상과 주요 보안 위협을 도식화해서 보여준다. 보안 위협에 대해 본 논문에서 제안하는 대응 방안은 표 2에서 제공하며, 자세한 내용은 다음과 같다.

## 5.1 거래 검증과 합의

### 5.1.1 공격자의 합의 장악

#### 가) 보안 위협

퍼블릭 블록체인의 경우 공격자가 과반수를 장악하면 거래의 검증 과정과 블록 내용을 조작할 가능성이 있다. 이런 공격은 현실적으로 힘들 것이라고 예상했지만, 실제로 비트코인에서 채굴을 위한 해쉬

파워가 중국 내의 몇몇 채굴장에 집중되면서 51% 공격의 실현 가능성에 대한 우려가 높다.

#### 나) 제안 대응 방안

PoW 방식은 특정 채굴장의 담합에 취약할 수 있으며, 이는 PoS, DPoS 등 다른 합의 알고리즘도 마찬가지이다. 본 논문에서는 공격자의 합의 주도권 장악을 감시할 수 있는 합의 현황 모니터링 기술을 제안한다. 퍼블릭 블록체인은 거래뿐만 아니라 채굴에 성공하고 신규 블록을 생성한 주체에 대한 신원도 투명하게 확인할 수 있다. 이러한 정보를 수집하고 분석해 합의 현황을 모니터링하고 특정 집단에게 합의가 편중되었는지 혹은 잘못된 합의가 시도되는지 감시해서 공격자의 장악에 대응하게 된다.



### 5.1.2 내부 참여자의 담합

#### 가) 보안 위협

프라이빗 블록체인의 경우 공격자가 내부 참여자에 침투해 장악할 위험성을 가지고 있다. 그리고 외부의 공격이 아니라, 폐쇄적인 시스템 내부 참여자들이 악의적으로 담합을 해서 블록체인 내용을 위변조할 가능성을 염두해 두어야 한다.

#### 나) 제안 대응 방안

블록체인 내부 참여자의 담합을 방지하고 대외 투명성을 확보하기 위해 앵커링[14]에 기반한 검증 방식을 제안한다. 앵커링은 프라이빗 블록체인과 퍼블릭 블록체인을 연계하는 기술이다. 이를 기반으로 보안 대상인 프라이빗 블록체인의 대표 해시값을 주기적으로 비트코인등의 퍼블릭 블록체인에 기록하고, 내부 담합이 의심되면 이 기록과 프라이빗 블록체인 정보를 비교해서 검증을 수행한다. 제안 방식을 통해 내부 담합으로 프라이빗 블록체인 내용을 변경하려는 시도를 방지할 수 있다.

## 5.2 사용자 프라이버시와 접근제어

### 5.2.1 프라이버시 침해

#### 가) 보안 위협

퍼블릭 블록체인은 공격자가 모든 거래내역과 정보를 쉽게 볼 수 있기 때문에 참여자의 프라이버시를 침해할 가능성이 높다. 또한 스마트 계약 코드도 실행중에 사용자 개인정보에 접근해서 개인정보 침해가 발생할 가능성도 있다.

#### 나) 제안 대응 방안

사용자의 프라이버시 보호를 위해 익명성을 강화해야 하며, 현재 영지식 증명 등의 기술이 적용되고 있다. 본 논문은 블록체인에 완전동형암호(Fully Homomorphic Encryption)[15]를 적용할 것을 제안한다. 완전동형암호는 암호화된 정보의 복호화 없이 정보의 처리 및 연산이 가능해진다. 블록체인 내의 사용자 정보와 거래 내역에 대해 이를 적용해서 개인정보의 유출을 방지하고 거래내역을 숨겨 익명성을 강화할 수 있다.

### 5.2.2 권한 오남용

#### 가) 보안 위협

탈중앙화된 블록체인 시스템에서는 참여자들에 대한 접근제어와 권한 통제에 어려움이 있다. 특히 프라이빗 블록체인에서는 특정 참여 노드나 내부 직원의 권한 오남용으로 정보의 조작과 보안 사고가 발생할 가능성이 높다.

#### 나) 제안 대응 방안

참여자들의 권한을 제어하고 오남용을 방지하기 위해서는 블록체인 내에서의 접근제어가 필요하다. 본 논문에서는 스마트 계약 기반의 접근제어를 제안한다. 참여자 권한에 대해 설정된 정책 자체가 스마트 계약의 형태로 배포되며, 요청에 대한 접근제어도 스마트 계약 시행을 기반으로 동작한다. 이 방식은 분산 환경에서 누구나 정책을 검증할 수 있고, 자동화되고 안전한 방식으로 접근 제어를 수행할 수 있다.

## 5.3 블록체인 소프트웨어 보안

### 5.3.1 블록체인 플랫폼 SW와 프로토콜 취약성

#### 가) 보안 위협

블록체인 시스템의 개념과 기술들도 결국 소프트웨어의 형태로 구현되며, 블록체인 소프트웨어에 취약점이 존재할 가능성이 높다. 또한 P2P 네트워크 형태로 정보를 전송하는 프로토콜 내에도 취약점이 존재할 수 있다.

#### 나) 제안 대응 방안

블록체인 소프트웨어에 대해 자체적인 혹은 외부 신뢰기관을 통한 코드 분석 및 검증 과정을 거쳐야 한다. 또한 코드 및 프로토콜의 취약점을 탐지하고 개선해야 한다. 이를 위해서는 블록체인 소프트웨어와 프로토콜의 표준화 및 인증 제도가 시행되어야 한다.

### 5.3.2 스마트 계약 코드 취약성

#### 가) 보안 위협

스마트 계약 코드도 소프트웨어와 마찬가지로 결

합과 취약성이 존재할 수 있으며, 스마트 계약 코드에 대한 분석 및 검증 과정이 미약한 상황이다. 또한 스마트 계약 코드는 전파를 통해 모든 블록체인 노드에서 실행되기 때문에 위험성이 더 증폭된다. 예를 들어, 이더리움 플랫폼의 DAO 사건 등이 실제로 발생하기도 했다.

#### 나) 제안 대응 방안

스마트 계약이 배포되기 전에 코드 분석과 검증을 통해 결함과 취약성 분석, 악성코드 탐지 작업이 선행되어야 한다. 기존에 SW 취약성 탐색을 위해 Peach Fuzzer, Driller, KLEE, Cloud9[16] 등의 도구들이 제안되었지만, 스마트 계약은 실행을 위한 Gas 소비 등 기존 SW와 차이점이 많다. 본 논문에서는 이러한 스마트 계약 코드의 특성을 고려하고 Solidity 등의 스마트 계약 전용 언어를 기반으로 하는 새로운 SW 취약성 탐지 기술을 개발할 것을 제안한다.

## 5.4 블록체인 서비스 보안

### 5.4.1 가용성 저하

#### 가) 보안 위협

블록체인은 분산 형태이기 때문에 중앙집중 형태에 비해 가용성이 높다. 하지만 공격자가 블록체인의 가용성을 저하시키는 DDoS 공격이 가능하며, 예를 들어 대량의 스팸거래 발생을 통한 공격이 Bitcoin에 대해 발생하기도 했다. 이러한 형태의 DDoS 공격에 대해서는 아직까지 분석이 부족한 상황이며, 대응도 어렵다.

#### 나) 제안 대응 방안

DDoS 공격에 대응하기 위해서는 정상거래와 스팸거래를 분류하고 차단할 수 있는 기술의 개발이 필요하다. 본 논문에서는 사용자들의 평판 관리를 기반으로 스팸거래를 차단하는 기술을 제안한다. 기존 시스템과 달리 블록체인에서는 거래를 발생시킨 사용자의 신원을 확인할 수 있다. 제안 방식에서는 사용자의 평판 자체도 블록체인을 기반으로 관리하며, 지속적으로 스팸거래를 발생시키는 사용자의 평판도를 낮추게 된다. 특정 공격집단이 대량의 스팸거래를 발생시키면 해당 사용자들의 평판이 낮아지

고, 발생한 스팸거래를 사전에 차단함으로써 블록체인의 가용성을 유지할 수 있게 된다.

### 5.4.2 비정상거래 탐지 어려움

#### 가) 보안 위협

퍼블릭 블록체인은 (유사)익명성을 가지기 때문에 거래 사기, 자금 세탁 등 비정상거래에 대한 탐지가 어렵다. 또한 블록체인의 특성상 수행된 거래를 취소할 수 없기 때문에, 비정상거래에 대한 복구가 어렵다.

#### 나) 제안 대응 방안

블록체인 내의 거래를 감시하고 거래 사기 및 자금 세탁 등을 탐지할 수 있는 방안이 필요하며, 본 논문에서는 머신러닝 기반의 이상거래 탐지시스템의 도입을 제안한다. 현재 국내외 금융권에서는 기존 시스템에 이상거래 탐지시스템(FDS)를 활용하고 있으며[17], 블록체인에 특화된 FDS를 개발해 블록체인 내의 이상거래를 탐지할 것을 제안한다. 특히 머신러닝과 딥러닝을 기반으로 다양한 이상거래를 자동화된 형태로 탐지할 수 있을 것으로 예상된다.

## VI. 결 론

본 논문에서는 4차 산업혁명의 핵심기술로 부각되고 있는 블록체인 기술의 보안 위협을 분석하고 대응 방안을 제안했다. 우선 대표적인 퍼블릭 블록체인 플랫폼인 비트코인과 이더리움, 대표적 프라이빗 블록체인 플랫폼인 Hyperledger Fabric, 코다, 쿼럼(Quorum)을 살펴보고 퍼블릭/프라이빗 플랫폼의 특징과 장단점을 비교했다. 또한 현 수준의 블록체인 기술의 한계를 분석했으며, 구체적으로는 낮은 TPS 성능 문제, 저장 공간의 증가 문제, 보안 문제를 서술하고 관련된 연구 방향을 정리했다. 이후 블록체인에 대한 다양한 보안 위협들 각각에 대해 새로운 대응 방안들을 제시했다. 합의 현황 모니터링을 통한 합의 장애 감시, 앵커링 기반 검증을 통한 내부 담합 방지, 완전동형암호 적용을 통한 프라이버시 보호, 스마트 계약 기반의 자동화된 접근 제어, 평판 기반 스팸거래 차단 기술을 통한 가용성 강화, 블록체인 특화 이상거래 탐지시스템 등 제안된 대응 방안을 통해 보안 위협들을 해소할 것으로

기대된다.

향후에는 본 논문에서 제안된 각 대응 방안들을 구체화하고 구현 및 테스트를 통해 검증하는 연구를 진행할 계획이다. 그리고 이 방안들을 통합해 보안성이 강화된 블록체인 플랫폼을 설계할 계획이다. 특히 보안 문제가 강조되고 있는 IoT 환경에 맞춰 위 블록체인 플랫폼을 개발해, IoT 블록체인의 확산에 기여할 것으로 기대된다.

## References

- [1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", <https://bitcoin.org/bitcoin.pdf>, [Accessed: Apr. 05, 2018]
- [2] "Blockchain Primer", Korbit, Mar. 2016.
- [3] L. Lamport, R. Shostak, and M. Pease, "The Byzantine Generals Problem", ACM Transactions on Programming Languages and Systems, Vol. 4, No. 3, pp. 382-401, Jul. 1982.
- [4] V. Buterin and V. Griffith, "Casper the Friendly Gadget", <https://ethresear.ch/uploads/default/original/1X/fdbebd67c8a9671efabf4e53d6267789cd91d96c.pdf>, Oct. 2017.
- [5] M. Castro and B. Liskov, "Practical Byzantine Fault Tolerance and Proactive Recovery", ACM Transactions on Computer Systems, Vol. 20, No. 4, pp. 398-461, Nov. 2002.
- [6] J. Kwon, "Tendermint: Consensus without Mining", <https://tendermint.com/static/docs/tendermint.pdf>, Nov. 2014.
- [7] R. C. Merkle, "A Digital Signature Based on a Conventional Encryption Function", CRYPTO '87, LNCS, Vol. 293, pp. 369-378, Aug. 1987.
- [8] V. Buterin, "A Next-Generation Smart Contract and Decentralized Application Platform", <https://github.com/ethereum/wiki/wiki/White-Paper>, Jan. 2014.
- [9] A. Yoshiharu, "Blockchain structure and theory", Wikibooks, Jun. 2017.
- [10] "Hyperledger Fabric", <https://www.hyperledger.org/projects/fabric>, [Accessed: Apr. 05, 2018]
- [11] M. Hearn, "Corda: A distributed ledger", [https://docs.corda.net/\\_static/corda-technical-whitepaper.pdf](https://docs.corda.net/_static/corda-technical-whitepaper.pdf), Nov. 2016.
- [12] "zk-SNARKs" <https://z.cash/technology/zksnarks.html>, [Accessed: Apr. 05, 2018]
- [13] "Blockchain technology and security considerations", Financial security institute, Aug. 2017.
- [14] T. Stein, "Faizod.Anchoring", <https://www.faizod.com>, [Accessed: Mar. 08, 2018]
- [15] E. Jo, S. Moon, and Y. Lee, "Performance analysis of fully homomorphic encryption libraries", Journal of KIIT, Vol. 16, No. 2, pp. 131-143, Feb. 2018.
- [16] S. Oh, T. Kim, and H. Kim, "Technology analysis on automatic detection and defense of SW vulnerabilities", Journal of Korea Academia-Industrial cooperation Society, Vol. 18, No. 11, pp. 94-103, Nov. 2017.
- [17] "Fraud detection system based on machine learning", Financial security institute, Aug. 2017.

## 저자소개

김 희 열 (Heeyoul Kim)



2000년 2월 : 한국과학기술원

전산학과(공학사)

2002년 2월 : 한국과학기술원

전산학과(공학석사)

2007년 2월 : 한국과학기술원

전산학과(공학박사)

2009년 3월 ~ 현재 : 경기대학교

컴퓨터과학과 부교수

관심분야 : 정보보호, 암호학, 블록체인