Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.28, NO.1, Feb. 2018 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2018.28.1.5

블록체인 시스템의 보안성 분석: 암호 화폐에서의 사례 연구*

이 성 범,† 이 부 형, 명 세 인, 이 종 혁‡
상명대학교 프로토콜공학연구실

Security Analysis of Blockchain Systems: Case Study of Cryptocurrencies*

Sungbum Lee,† Boohyung Lee, Sein Myung, Jong-Hyouk Lee‡
Protocol Engineering Lab., Sangmyung University

요 약

최근 4차 산업혁명으로 인해 사물인터넷 기반의 다양한 기술들이 활발하게 연구되고 있다. 사물인터넷 시대에는 기존 서버-클라이언트 구조의 중앙 집중형 운영보다는 서버에 부하를 줄이고 자율적인 사물간 데이터 통신에 적합한 피어-피어 구조의 분산형 운영방식이 요구 되고 있다. 본 논문에서는 데이터에 대한 무결성과 영속성을 지원하는 새로운 형태의 분산형 데이터베이스 기술인 블록체인에 대해 설명하고, 보안성을 분석한다. 이를 위해 블록체인의 주요한 동작을 합의 과정, 네트워크 통신 과정, 키 관리 과정으로 구분하여 각 과정에서의 가능한 공격과 대응책을 설명한다. 또한 대표적인 암호화폐 플랫폼인 비트코인과 이더리움에서 발생했던 공격들에 대해 기술한다.

ABSTRACT

With the advance of the 4th industrial revolution, Internet of Things (IoT) technology is actively being studied. In the era of the IoT, a decentralized operation is required to reduce load on servers and enable autonomous IoT data communication rather than focusing on centralized operation of being server client structures. This paper analyzes the security of a blockchain, a new form of distributed database platform that supports integrity and permanence of data. To achieve this, we divide the blockchain's major operations into a consensus process, network communication process, and key management process, and then describe possible attacks and countermeasures in each process. We also describe the attack occurred in typical cryptocurrency platforms such as Bitcoin and Ethereum.

Keywords: Blockchain, Consensus, Network, Security, Cryptocurrency

I. 서 론

4차 산업혁명이 도래하면서 사물인터넷 기반의 다양한 기술들이 활발하게 연구되고 있고, 기술을 이용한 서비스들이 개발되고 있다. 사물인터넷 환경에서는 다양하고 많은 종류의 기기들이 네트워크에 연결되어 통신을 하게 된다. 따라서 네트워크에 연결되는 기기들의 숫자는 기하급수적으로 늘어나고 있다. 이에 따라 기존의 서버-클라이언트 구조의 중앙 집중형 데이터 운영이나 관리 기법의 한계점들이 도출되고

Received(09. 19. 2017), Modified(12. 27. 2017), Accepted(12. 27. 2017)
* 본 논문은 2017년도 한국정보보호학회 하계학술대회에 발표한 우수논문을 개선 및 확장한 것임.
* 본 논문은 2017년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No. NRF-2017R1A1A1A05001405).
† 주저자, sungbum@pel.smuc.ac.kr
‡ 교신저자, jonghyouk@pel.smuc.ac.kr(Corresponding author)

있다. 특히 서버에 연결되는 기기들의 수가 늘어나거나 해당하는 기기들의 요청 및 데이터 전송은 특정 서비스를 제공하는 서버에 무리를 줄 수 있다. 이에 따라 분산형 데이터 저장 및 운용에 관한 요구사항이 사물인터넷 시대에 높아지고 있는 실정이다.

블록체인은 피어-피어 환경에서 안전한 데이터 저장을 제공하는 기술이다. 블록체인은 암호화폐 비트코인의 기반 기술로 소개되었고, 유엔 미래 보고서 2050에서 미래를 변화시킬 기술로 선정 되었다[1]. 또한 국내/외에서 활발히 연구되고 있다. 특히 블록체인을 다양한 상용 서비스 영역에 도입하기 위해서 연구들이 활발히 이루어지고 있고, 다양한 형태로 블록체인 플랫폼이 개발되고 있다[2,3].

블록체인 기술을 활용하기 위한 연구와 개발은 많이 이루어지고 있지만, 블록체인의 보안성 분석은 수학적 모델링과 증명에 머물러 있는 실정이다. 또한 블록체인 보안성에 대한 분석은 대부분 합의 알고리즘의 수학적 모델링에 집중되어 있다. 본 논문에서는 블록체인의 대표적인 플랫폼인 비트코인에서 블록체인 기술의 주요한 동작 과정을 설명한다. 주요 동작 과정은 합의 과정, 네트워크 통신과정, 키 관리 과정으로 나눌 수 있고, 각 과정에서 가용한 공격을 기술하고 그에 따른 대응책을 기술한다. 또한 비트코인과 이더리움에서 플랫폼을 위협하기 위해 발생하였던 공격들에 대해 기술한다.

본 논문의 2 장에서는 분산형 데이터베이스 플랫폼으로써의 비트코인 블록체인 기술에 대해 설명한다. 또한 합의과정, 네트워크 통신 과정, 키 관리 과정에서 발생할 수 있는 공격에 대해 설명하고 대응책에 대해 설명한다. 3 장에서는 블록체인 기술의 대표적인 플랫폼인 비트코인과 이더리움에서 발생하였던 공격에 대해서 기술한다. 4 장에서 본 논문의 결론을 짓는다.

II. 블록체인

비트코인(Bitcoin)[4]은 2008년 사토시 나카모토가 제안하였고, 블록체인 기술을 이용한 대표적인 암호화폐이다. 기존 서버-클라이언트 구조의 중앙 집중형 통화 발행 및 관리 방식이 아닌 인터넷 환경에서 은행과 같은 제3자의 개입이 없고, 사용자간 신뢰 관계가 없이 안전하게 암호화폐 거래가 가능하도록 개발되었다. 다시 말해, 비트코인은 중앙에서 통화를 발행하고 관리하는 기관 없이 피어-피어 네트워크 환경에서 사용자 간 직접적인 암호화폐를 통한 안전한 거래를 제공한다. 이러한 비트코인의 하부 기술로써 블록체인은 데이터 무결성 제공을 위해 해시함수와 데이터 체이닝 기법을 사용한다. 또한 데이터에 대한 신뢰성 제공을 위해 공개키 기반의 전자서명을 사용한다.

비트코인 블록체인에 참여하는 사용자들(노드들)은 거래를 작성하고 자신의 개인키로 거래에 서명한다. 작성된 거래들은 다른 사용자들에게 브로드 캐스팅하여 전달하고, 합의 과정에서 특정 합의 알고리즘을 통해 거래들을 하나의 블록으로 생성한다. 생성된 블록은 기존 블록체인에 연결되게 되고, 블록의 정보를 다른 사용자들에게 브로드캐스팅 한다. 사용자들은 블록체인에 연결된 블록의 정보들을 바탕으로 중앙 시스템 없이 사용자들 간에 데이터의 무결성과 신뢰성을 확인 할 수 있다.

비트코인 블록체인을 구성하는 블록은 블록 헤더와 블록 바디로 구성 된다. 비트코인에서 블록 헤더는 비트코인 버전, 이전의 블록 헤더의 해시 값, 블록에 들어있는 거래의 Hash 값인 Merkel root, Timestamp, bits, nonce가 들어있다. 블록 바디에는 블록에 포함되어있는 거래의 정보, 거래들의 Merkel Tree가 들어있다. 이러한 블록들은 Fig. 1. 과 같이 체인 형식으로 연결되어 있다.

블록체인 기술은 구현된 플랫폼마다 조금씩 다르게 구현되어 있지만 본 장에서는 비트코인을 기준으로 보안성을 분석한다. 비트코인 이외의 다른 플랫폼에서도 본 논문에서와 같이 동작과정을 나누고 보안성 분석이 가능하다.

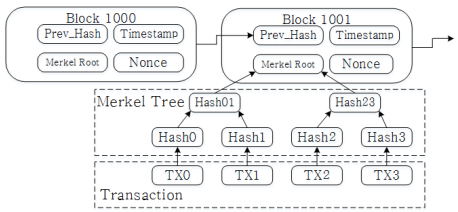

Fig. 1. Blocks of the Bitcoin Blockchain

2.1 합의 과정

블록체인 시스템에서 노드들 간에 무결성과 신뢰성을 제공하는 블록을 생성하기 위해서 노드 간의 블록을 합의하는 과정이 필요하다. 합의하는 과정에서 합의 알고리즘을 사용하여 특정 조건을 만족하는 노

드가 블록을 생성하고 블록체인에 생성된 블록을 연결하게 된다. 대표적인 합의 알고리즘으로는 작업증명(PoW, Proof of Work), 지분증명(PoS, Proof of Stake), 지분위임증명(DPoS, Delegated PoS)이 있다[5]. 합의하는 과정을 통해서 생성된 블록의 무결성과 신뢰성을 제공한다. 이 장에서는 합의 과정에서의 공격 방법인 Double Spending과 Selfish Mining에 대해서 설명한다.

2.1.1 Double Spending

Double Spending[6]은 합의 과정에서 발생할 수 있는 공격으로, 같은 돈을 두 번 이상 지출하는 공격이다. 거래에 포함된 코인은 블록에 포함되기 전에 감소되지 않기 때문에, 블록에 포함되기 전에 같은 코인을 여러 차례 거래에 포함하여 사용할 수 있다. Double Spending 공격 절차는 다음과 같다.

1. Alice가 Bob에게 10 btc 전송 거래 발생
2. Alice가 자신에게 10 btc 전송 거래 발생
3. 블록이 동시간대에 만들어지면 위 Fig. 2. 와 같이 블록체인이 분기되고 블록 경쟁이 발생
4. Bob은 Alice가 자신에게 보낸 거래가 포함된 블록이 생성된 것을 확인하고 물건을 Alice에게 전달
5. 블록 경쟁 발생
   - 비트코인에서는 블록 경쟁 시 다음 블록은 먼저 만드는 블록이 블록체인에 연결됨
6. Alice가 자신에게 보낸 10btc 거래가 포함된 블록이 블록 경쟁에서 이긴다면, 위 Fig. 2. 와 같이 블록이 블록체인에 연결되고, Alice가 Bob에게 보낸 10 btc 거래가 포함된 블록은 삭제

위와 같은 Double Spending 공격의 대응책으로서 비트코인에서는 6-confirmation을 권장한다.

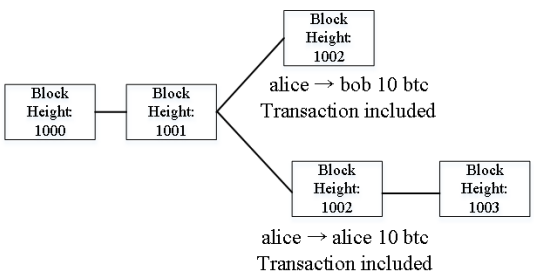

Fig. 2. Forked Blockchain

6-confirmation은 블록체인에서 1000번째 블록이 생성된 후 1005번째 블록이 생성될 때까지 1000번째 블록은 Double Spending 공격에 충분히 안전하지 못하다고 수학적으로 증명하고 있다[4].

2.1.2 Selfish Mining

Selfish Mining[7][8]은 합의 과정에서 발생할 수 있는 공격으로, 선의의 노드가 만든 블록이 아닌 공격자가 만든 블록이 블록체인에 연결되게 만드는 공격이다. 블록이 동시간대에 생성되었을 때 블록체인은 분기되고 블록 경쟁이 발생된다. 비트코인에서는 블록경쟁이 발생했을 때 다음 블록을 빠르게 생성한 블록을 채택하여 블록체인에 연결하도록 되어있다. 공격자인 Selfish Miner는 블록을 생성한 뒤 공개하지 않고 다음 블록을 미리 생성하여 블록 경쟁이 발생하였을 때 미리 생성해놓은 블록을 공개함으로써 블록 경쟁에서 이기게 되고, 공격자가 만든 블록이 블록체인에 채택되게 된다. 비트코인 환경에서 Selfish Mining의 공격 절차는 다음과 같다.

1. 초기화 과정
   공격자는 Fig. 3. 과 같이 공개된 블록체인을 Private Chain, Public Chain 으로 Fork
2. Selfish Miner가 블록을 생성한 경우
   - Private Chain에 블록을 추가
   - (Private Chain Length - Public Chain Length) ≤ 0 인 경우 Public Chain을 Private Chain에 복사
3. Honest Miner가 블록을 생성한 경우
   - (Private Chain Length - Public Chain Length) 〈 0 인 경우 Public Chain을 Private Chain에 복사
   - (Private Chain Length - Public Chain Length) = 0 or 1 인 경우 Private Chain의 블록 공개
   - (Private Chain Length - Public Chain Length) ≥ 2 인 경우 Private Chain의 비공개된 첫 번째 블록 공개

Selfish Mining 공격의 대응책으로서 블록 경쟁이 발생하였을 때 블록 채택 방법을 다음 블록을 빠르게 만든 블록체인의 블록을 채택하는 것이 아닌 다음과 같은 방법으로 변경하여 대응할 수 있다.

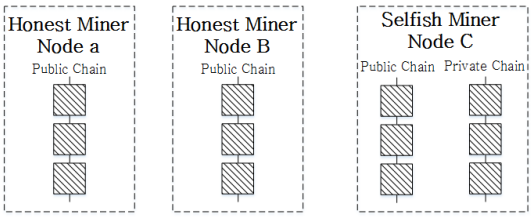

Fig. 3. Blockchain Copy for Selfish Mining

1. 블록을 랜덤하게 채택하는 방법[8]
   경쟁 상태일 때 블록을 랜덤하게 채택하는 방법
2. 분기 처벌 규칙[9]
   분기한 블록을 처벌하기 위해 보상을 없애고, 분기된 첫 번째 채굴자의 보상을 반으로 줄이는 방법
3. Freshness 활용 방법[10]
   블록에 타임스탬프를 포함하게 하고, 블록 경쟁시 더 최근에 만들어진 블록을 선정하는 방법

또한, 미리 생성된 블록(Stale Block) 생성을 방지하도록 하는 방법이 있다. Stale Block이 발생하는 요인은 다음과 같다.

1. Block Interval
   - Block Interval은 블록체인에 블록이 연결되고, 다음 블록이 생성되기까지의 시간으로, 블록 간격이 길수록 트랜잭션의 처리가 늦어져 Stale Block 생성 확률이 증가함
2. Block Size
   - 블록의 크기가 클수록 전파속도가 느려지고, Stale Block 생성 확률이 증가함

공격에 악용될 수 있는 Stale Block의 생성 확률을 줄이기 위해 블록체인을 이용한 플랫폼을 구현할 때 보안 모델을 정립하여, 적절한 Block Interval과 Block Size를 고려하여야 한다[11].

2.2 네트워크 통신 과정

블록체인에서 노드간의 연결은 P2P(Peer to Peer)로 연결된다. 비트코인 플랫폼에서는 노드간의 연결을 위해서 다음과 같은 과정을 통해 연결되게 된다.

- Propagating Network Information
  - 노드들의 정보를 전달하는 과정
- Storing network information
  - 노드들의 정보를 저장하는 과정
- Selecting Peers
  - 연결할 노드를 선정하는 과정
- Network Connection
  - 선정된 노드들을 연결하는 과정

위 과정을 통해서 노드 간 연결이 되고 통신하게 된다. 이 장에서는 네트워크 과정에서 발생할 수 있는 공격인 Eclipse Attack과 BGP Hijacking에 대해서 설명한다.

2.2.1 Eclipse Attack

Eclipse Attack[12]은 희생자 노드의 연결을 공격자 노드에게만 연결되게 하여 희생자 노드를 다른 노드로부터 고립시키는 공격이다. 이 공격을 통해 희생자 노드는 공격자가 제공하는 데이터만 전달받게 된다. 아래 Fig. 4. 에서는 공격자 노드 D가 노드 E를 공격하여 다른 노드들로부터 고립되게 만든 그림이다.

비트코인 v0.9.3 에서는 노드가 초기 연결 시 다른 노드로부터 노드들의 정보를 수신하고, 수신한 정보를 Table에 저장한다. 저장된 노드들의 정보에서 연결할 노드를 선정하여 Connection을 유지한다. 이러한 환경에서 Eclipse Attack을 위해서는 다음과 같은 절차를 통하여 공격하게 된다.

1. 공격자 노드가 희생자 노드에게 자신의 정보를 전달하여 희생자의 Table에 공격자의 정보가 저장되도록 함
   - 비트코인 버전 0.9.3은 희생자 Table에 저장할 수 있는 노드의 개수 보다 더 많은 노드의 정보가 수신되면 저장되어 있던 시간이 오래된 노

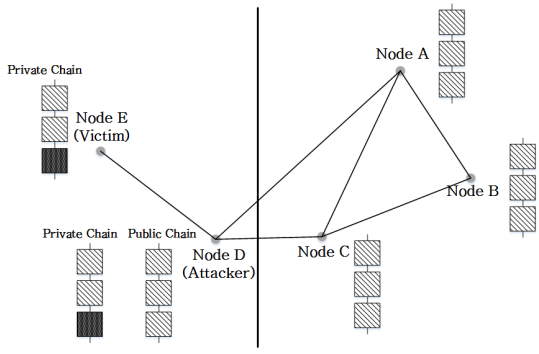

Fig. 4. Eclipse Attack

드의 정보를 삭제하고 새로운 요청을 한 노드의 정보를 Table에 저장
2. 희생자 노드에게 다수의 요청을 하여 희생자 노드의 Table에 공격자의 정보로만 채움
3. 희생자 노드와 다른 노드의 Connection을 끊기 위해 공격자 노드는 DDoS 공격을 하여 희생자 노드가 재시작 되도록 함
4. 희생자 노드는 재시작 되고, Table에 있는 정보를 바탕으로 재 연결됨
   - Table에 공격자의 정보만 있기 때문에 공격자에게만 연결됨

위와 같은 과정을 통해서 Eclipse Attack이 가능하다. 이러한 공격을 막기 위해서 비정상적인 Packet을 탐지하는 Anomaly Detection을 하거나, 희생자 노드의 Table에 저장된 노드만 선택하여 연결하는 것이 아닌 Table에 저장된 노드의 정보 이외에도 랜덤하게 선택하여 연결 되도록 해야 한다.

2.2.2 BGP Hijacking

블록체인의 노드들은 인터넷 서비스 공급자(ISP)에 의해서 연결 된다. 악의적인 ISP는 블록체인에서 발생하는 트래픽을 공격할 수 있다. BGP Hijacking[13]은 악의적인 ISP가 주변 라우터에게 잘못된 라우팅 정보를 광고하여 비정상 처리되도록 하는 공격 방법이다. BGP Hijacking을 통해 Partitioning Attack과 Delay Attack이 가능하다[14].

Partitioning Attack은 네트워크를 두 개로 분할하는 공격으로, 위 Fig. 5. 에서 Attacker는 ISP1에 연결되어있는 노드(192.168.0.1)가 자신에게 연결되어있는 것처럼 Fake IP주소(192.168.0.1)를 생성하고 라우팅 테이블을 업데이트하여 인접한 ISP로 전송한다. 인접한 ISP는 Attacker가 보낸 라우팅정보로 업데이트하고 192.168.0.1로 전송되는 패킷을 Attacker에게 전송하게 된다. Attacker는 수신한 패킷들을 중간에서 가로채 전달해주지 않음으로써 네트워크를 분할시킬 수 있다.

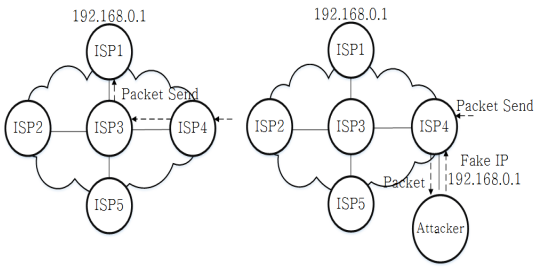

Fig. 5. BGP Hijacking Partitioning Attack

Partitioning Attack을 방어하기 위해서는 Monitor Round-Trip time 방법이 있다. 이 방법은 RTT를 모니터링 하여서 패킷이 잘 전달되는지 확인하고, 잘 전달되지 않는다면 다른 ISP로의 연결을 통해 패킷을 송수신한다.

Delay Attack은 네트워크에서 발생하는 트래픽(거래, 블록) 전달을 지연시키는 공격으로, 다음과 같은 과정을 통해 공격한다.

1. 희생자(노드 C)는 노드 A에게 블록을 요청
2. 공격자는 희생자가 노드 A에게 보낸 요청을 이전 블록을 요청하도록 변경하여 전송
3. 노드 A는 희생자에게 이전 블록을 전달
4. 희생자가 블록을 요청하고 20분이 지나기 전에 공격자는 Step 2에서 희생자가 보냈던 블록 요청 메시지를 노드 A에게 전달- 블록은 20분 제한 시간 직전에 전달해야 희생자는 노드 A와의 연결을 끊지 않음
5. 노드 A는 희생자에게 블록을 전달

위와 같은 과정을 통해서 희생자는 요청한 블록을 수신하기까지 약 20분 지연되어 수신하게 된다. Delay Attack을 방어하기 위해서는 Encrypt Bitcoin Communication and/or adopt MAC(Message Authentication Code) 방법이 있다. 이 방법은 메시지를 암호화하여 어떤 메시지인지 공격자가 확인할 수 없도록 , 메시지 인증 코드를 사용하여 메시지의 내용이 변경되지 않았음을 확인할 수 있도록 하는 방법이다.

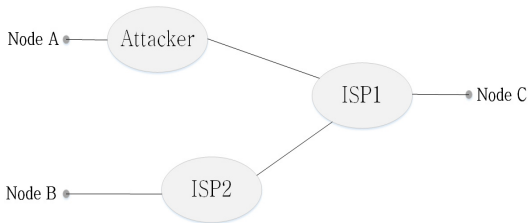

Fig. 6. BGP Hijacking Delay Attack

2.3 키 관리 과정

블록체인에서는 공개키 방식(Public Key, Private Key)을 이용하여 노드의 익명성과 거래의 신뢰성을 제공한다. 공개키는 거래의 서명을 확인할 때 사용하고, 개인키는 거래에 서명 하기 위해 사용된다. 비트코인 환경에서 공격자에게 개인키를 탈취당한다면 공격자는 희생자의 비트코인을 이용할 수 있다. 개인키를 관리하기 위해 다음과 같은 방법들이 있다[15].

1. Local Storage: PC Local에 개인키를 저장하는 방법
2. Password-Protected Wallets: 개인키를 Password로 암호화하여 저장하는 방법
3. Offline Storage of Keys: 개인키를 QR Code로 생성하거나, USB Memory에 저장하는 방법
4. Server Wallet: Server에 개인키를 저장하는 방법

이와 같이 개인키를 저장하는 다양한 방법이 있다. 블록체인에서 키를 보다 안전하게 저장하기 위해서 TEE(Trusted Execution Environment)와 같은 기술을 이용하여 저장하여야 한다[16].

III. 암호화폐 시스템

본 장에서는 2장에서 설명한 블록체인 기술을 이용하여 개발된 암호화폐 플랫폼인 비트코인, 이더리움에서 실제 발생했던 공격들에 대하여 설명한다. 제 1절에서는 합의 과정에서의 공격으로 인해 발생하였던 블록체인 하드포크에 대해 설명하고, 2절에서는 네트워크 과정에서의 공격인 BGP Hijacking에 대해서 설명한다. 제 3절에서는 키 관리 과정에서의 공격인 코인 거래소에서의 키 관리 공격들에 대하여 설명하고, 4절에서는 비트코인을 목표로 하는 악성코드에 대하여 설명한다. 마지막으로 제 5절에서 는 암호화폐 플랫폼의 특징적으로 발생할 수 있는 공격인 화폐환율조작 공격에 대해 설명한다.

3.1 블록체인 하드포크

블록체인 기술의 대표적인 암호화폐 플랫폼인 이더리움은 DoS(Denial of Service) 공격을 지속적으로 받게 되었다. Fig. 7. 과 같이 이더리움의 거래내역이 담긴 블록체인이 1919999번째 블록을 기점으로 두 개의 체인으로 분기 되었다[17]. 2016년 7월 20일 이더리움의 창립자인 비탈릭 부테린은 1920000번째 블록을 기준으로 두 개의 체인중 하나의 체인을 선정하고, 다른 체인의 블록들은 삭제하게 된다[18]. 2016년 7월 24일 해외 대형 코인 거래소인 폴로닉스(Poloniex)에서는 이더리움 하드포크과정에서 삭제된 블록체인을 기반으로 이더리움 클래식(Ethereum Classic:ETC)이라는 이름으로 새로운 블록체인 암호화폐 플랫폼을 만들게 된다. 이더리움이 하드포크하면서 삭제된 블록체인을 기반으로 한 이더리움 클래식이 개발 되면서 이더리움의 화폐 가치는 폭락하게 된다. 또한 이더리움 클래식의 암호화폐의 가치가 인정되고, 코인 거래소 에서도 거래가 가능해지게 되었다.

이와 같이 블록체인 합의과정에서의 DoS 공격으로 인해 두 개의 블록이 생성되고, 블록체인이 하나의 체인이 아닌 체인이 분기되어 유지 되는 경우가 발생할 수 있다. 이더리움에서는 하드포크를 함으로써 체인을 다시 하나로 유지하게 되었다. 하지만 블록체인의 핵심기술인 합의과정에서 공격이 발생이 가능함을 보여주었던 사례였고, 이 공격을 막기 위한 방안이 없기 때문에 하드포크를 했던 사례이다.

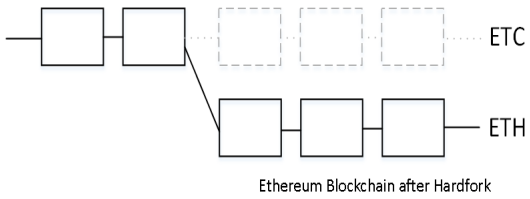

Fig. 7. Ethereum Hardfork

3.2 BGP Hijacking

BGP Hijacking은 블록체인 네트워크 통신과정에서의 공격방법이다. Dell SecureWorks Counter Threat Unit(CTU)에서는 2014년 2월에서 5월 사이에 비트코인에서 BGP Hijacking이 발생했다고 발표하였다[19]. 공격 대상은 Amazon, Digital Ocean, OVH 및 기타 대규모 호스팅 회사에 속한 특정 네트워크로 향하는 트래픽을 반복적으로 하이재킹하는 공격이다. 세부 공격 방법의 절차

는 아래와 같다.

1. 마이너는 마이닝을 위해 합법적인 풀에 지속적으로 연결
2. 공격자는 마이너의 합법적인 풀에 대한 연결요청 메시지를 하이재킹하여 공격자가 관리하는 풀로 트래픽 전송
3. 공격자의 풀에서는 마이너에게 client.reconnect 명령을 전송하여 공격자의 두 번째 풀에 연결하도록 함.
4. 마이너는 공격자의 풀에서 작업을 하지만 보상을 받을 수 없음

위와 같은 공격이 가능했던 이유는 캐나다의 ISP에서 일했었던 직원이 악의적으로 BGP Hijacking 한 사례이다. 공격자들은 희생자들을 공격함으로써 4개월 간 $83,000의 이익을 얻게 되었다.

3.3 코인 거래소

코인 거래소에서의 공격은 블록체인에서 키 관리 과정에서의 공격이다. 블록체인에서의 트랜잭션에 서명을 하기 위해서는 사용자의 개인키를 사용한다. 사용자들은 개인키를 관리하기 어렵기 때문에 거래소에 위탁하는 경우가 있다. 이때 위탁 된 개인키를 사용하는데 사용자의 아이디와 패스워드를 통해 접근하게 된다. 공격자는 사용자의 개인키를 사용하기 위해 코인 거래소를 공격한다. 공격하는 방법은 크게 두 가지가 있다.

1. 코인 거래소 키 저장소 공격
   코인 거래소는 사용자들로부터 위탁받은 개인키를 보관하기 위해 데이터베이스를 유지한다. 공격자들은 코인 거래소의 데이터베이스에 접근하기 위해 악성코드 및 취약점을 이용해 공격할 수 있다.
2. 사용자 정보를 이용한 키 접근
   사용자들은 코인 거래소에 위탁한 키에 접근하기 위해서 사용자의 정보를 이용하여 접근한다. 공격자들은 사용자 정보들을 수집하여 코인 거래소에 사용자 정보를 이용하여 키를 사용 하게 된다.

위의 두가지 방법으로 공격자는 코인 거래소에 위탁된 키에 접근할 수 있게 되고, 사용자들의 화폐를 사용할 수 있게 된다. 이러한 공격은 2016년 8월 2일에 홍콩에 소재한 비트코인 거래소인 비트피넥스가 해킹되어 6,300만 달러의 피해를 입었고[20], 2017년 4월 22일에 한국 비트코인 거래소인 야피존이 해킹되어 55억 규모의 피해를 입었다[21]. Youbit로 이름을 변경한 야피존은 또다시 2017년 12월 해킹을 당해 파산했다. 코인 거래소에 키를 위탁하는 경우 코인 거래소 해킹에서 자유롭지 못하다.

3.4 비트코인 악성코드

비트코인을 목표로 하는 악성코드는 대표적으로 두가지가 있다. 첫 번째는 비트코인의 개인키를 보관하고 있는 지갑을 탈취하는 악성코드이고, 두 번째는 비트코인에서 마이닝을 위한 악성코드이다.

1. 지갑 탈취 악성코드
   비트코인에서 사용자들은 자신의 화폐를 이용하기 위해서는 거래를 작성하게 된다. 거래는 자신의 개인키로 서명함으로써 사용자가 가진 화폐를 정상적으로 사용함을 증명할 수 있다. 지갑 탈취 악성코드는 암호 화폐에서 개인키를 탈취하기 위한 악성코드이다. 공격자는 희생자의 개인키를 탈취하여 희생자의 화폐를 이용할 수 있게 된다. 대표적인 지갑 탈취 악성코드는 BTMINE이 있다[22].
2. 마이닝 악성코드
   비트코인에서 마이너들은 노드들의 거래들을 블록으로 생성하여 보상을 받을 수 있다. PoW 에서는 마이너들이 블록을 생성하기 위해서는 컴퓨팅 파워를 사용하여 블록을 생성하게 된다. 공격자들은 마이닝 악성코드를 이용하여 희생자들의 컴퓨팅 파워를 비정상적으로 사용한다. 따라서 마이닝 악성코드에 감염된 희생자들의 컴퓨팅 파워는 저하되게 된다. 이와 같이 Botnet을 이용한 채굴을 하는 악성코드들이 증가하고 있고, 대표적인 마이닝 악성코드로 BitcoinMiner가 있다[23].

3.5 화폐 환율 조작

암호화폐인 비트코인과 이더리움은 코인 거래소를 이용하여 가상 화폐를 실제 화폐로 환전이 가능하다. 가상 화폐도 실제 화폐와 마찬가지로 수요자에 따라 화폐의 환율이 변동된다. 최근 2017년 5월 12일에 워너크라이 랜섬웨어가 대규모 감염되는 사건이 발생하였다. 워너크라이에 감염된 희생자는 공격자로부터 300$ 상당의 금액에 상응되는 비트코인을 요구받게

된다. 감염된 희생자들은 자신의 컴퓨터를 복구하기 위해 실제 화폐를 가상 화폐로 환전하여 공격자에게 전송하게 된다. 2017년 5월 1일에는 1 비트코인의 가격이 1,635,000원 이였다. 워너크라이가 발생하기 전날인 5월 11일에는 1 비트코인의 가격이 2,352,000 원까지 오르게 된다. 워너크라이가 대규모로 감염된 후 5월 25일에는 1비트코인에 4,681,000 원까지 상승하게 되었다[24].

사이버 보안업체인 타이코틱에서는 워너크라이 랜섬웨어는 비트코인의 환율을 조작하기 위한 공격이라고 주장하였다[25]. 환율을 조작하고, 조작 한 환율로서 이익을 취하는 공격을 Goldfinger라고 한다[26].

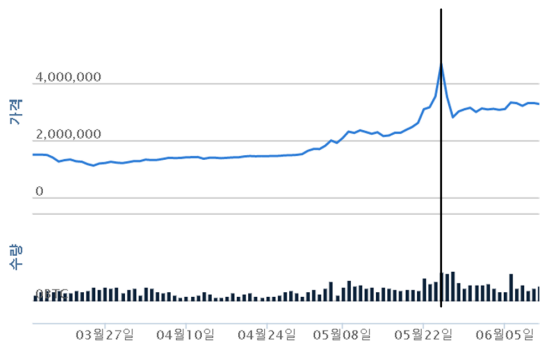

Fig. 8. Bitcoin Exchange Rate

IV. 결 론

본 논문에서는 블록체인의 동작과정을 합의과정, 네트워크 통신과정, 키관리 과정으로 나누어 설명하였다. 각 과정에서 가능한 공격 방법과 대응책에 대해서 알아보았다. 또한 블록체인의 대표적인 플랫폼인 암호화폐 시스템(비트코인, 이더리움)에서 발생했던 공격에 대해서 알아보았다. 블록체인 플랫폼을 개발하는데 있어서 각 동작과정에서의 가능한 공격들을 고려하여 대응책을 마련해야 한다. 더욱이 합의 과정에서 주요한 요소인 합의알고리즘에 따라 블록을 생성하는 알고리즘이 다르기 때문에, 합의 알고리즘에 따라 발생할 수 있는 공격에 대하여 고려해야 할 필요가 있다. 또한 블록체인의 주요 동작과정 이외에도 플랫폼의 특징에 따라 발생할 수 있는 공격(예, 암호화폐 환율 조작)들이 있다. 따라서 이러한 공격들을 대응할 수 있는 대응책을 강구해야 한다. 추후 연구로는 합의과정에서 합의알고리즘의 보안성을 측정할 수 있는 연구[11]를 바탕으로 개발된 블록체인 플랫폼의 특징을 바탕으로 모든 동작과정에서의 보안성을 측정하고, 보호 할 수 있는 방법론을 연구하고자 한다.

References

[1] Jerome Glenn et al., "World Future Report 2050". Kyobo Book, Korea, 2016.

[2] Korea Institute of Finance and Information Technology., "Block Chain Technology Application Areas and Case Studies", KISA, Korea, 2016.

[3] B. Lee and J.-H. Lee, "Blockchain based secure firmware update for embedded devices in an Internet of Things environment", *Journal of Supercomputing*, vol. 73, no. 3, pp. 1152-1167, 2017

[4] Satoshi Nakamoto, "Bitcoin:A peer-to-peer electronic cash system.", 2008.

[5] B. Lee, Y.-J. Lim and J.-H. Lee, "Consensus algorithms in block-chain platforms", *Proceedings of Symposium of the Korean Institute of communications and Information Sciences*, pp. 386-387, 2017.

[6] bitcoin wiki page, https://en.bitcoin.it/wiki/Double-spending, last accessed 2017/09/13.

[7] SoHee Kim, JiYeon Yang and Yoonjeong Kim, "A Study on the Selfish Mining of Block Chain", *Proceedings of Symposium of the Korean Institute of communications and Information Sciences*, pp. 422-423, 2015.

[8] I. Eyal, Emin G. Sirer, "Majority is not Enough: Bitcoin Mining is Vulnerable", *In Financial Cryptography*, pp. 436-454, 2014.

[9] Bahack Lear, "Theoretical Bitcoin Attacks with less than Half of the Computational Power (draft)." *arXiv preprint arXiv*:1312.7013, 2013.

[10] HEILMAN, Ethan. One weird trick to

stop selfish miners: Fresh bitcoins, a solution for the honest miner. In: International Conference on Financial Cryptography and Data Security. *Springer, Berlin, Heidelberg,* pp. 161-162, 2014.

〔11〕 Gervais, A., Karame, G. O., Wüst, K., Glykantzis, V., Ritzdorf, H., and Capkun, S. "On the security and performance of proof of work blockchains." *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. ACM,* pp. 3-16, October. 2016.

〔12〕 HEILMAN, E., KENDLER, A., ZOHAR, A., AND GOLDBERG, S., " Eclipse Attacks on Bitcoin's Peer-to-Peer Network.", *In 24th USENIX Security Symposium,* pp. 129 - 144, 2015

〔13〕 Sung Bok Jeon, "Analysis of BGP Routing Protocol's Vulnerability and it's improvement measures.", *Department of Information & Technology, master thesis, sogang University* , August, 2008.

〔14〕 Apostolaki, Maria, Aviv Zohar, and Laurent Vanbever. "Hijacking bitcoin: Routing attacks on cryptocurrencies." *Security and Privacy (SP), 2017 IEEE Symposium on. IEEE,* 2017.

〔15〕 S. Eskandari, D. Barrera, E. Stobert, and J. Clark. "A first look at the usability of bitcoin key management.", *In Workshop on Usable Security (USEC),* 2015.

〔16〕 Gentilal, Miraje, Paulo Martins, and Leonel Sousa. "TrustZone-backed bitcoin wallet." *Proceedings of the Fourth Workshop on Cryptography and Security in Computing Systems. ACM,* 2017.

〔17〕 Reason of Ethereum Hardfork, https://bitcoinmagazine.com/articles/op-ed-why-ethereums-hard-fork-will-cause-problems-coming-year/, last accessed 2017/09/13.

〔18〕 Notification of Ethereum Hardfork, https://blog.ethereum.org/2016/07/20/hard-fork-completed/, last accessed 2017/09/13.

〔19〕 BGP Hijacking, https://www.secureworks.com/research/bgp-hijacking-for-cryptocurrency-profit, last accessed 2017/09/13.

〔20〕 Bitfinex Coin Exchange Hacking, http://www.itworld.co.kr/news/100594, last accessed 2017/09/13.

〔21〕 Yapizon Coin Exchange Hacking, http://www.boannews.com/media/view.asp?idx=54483&kind=1&search=title&find=%BA%F1%C6%AE%C4%DA%C0%CE, last accessed 2017/09/13.

〔22〕 BTMINE bitcoin malware, https://themerkle.com/top-3-types-of-bitcoin-mining-malware/, last accessed 2017/09/13.

〔23〕 BitCoinMiner bitcoin malware, http://blog.alyac.co.kr/54, last accessed 2017/09/13.

〔24〕 ethereum price, https://www.bithumb.com/, last accessed 2017/09/13.

〔25〕 bitcoin exchange manipulation, http://www.boannews.com/media/view.asp?idx=55031, last accessed 2017/09/13.

〔26〕 Kroll, Joshua A., Ian C. Davey, and Edward W. Felten. "The economics of Bitcoin mining, or Bitcoin in the presence of adversaries.", *Proc. of WEIS.* Vol. 2013. 2013.

〈저자소개〉

이 성 범 (Sungbum Lee) 학생회원
2016년 8월: 상명대학교 컴퓨터소프트웨어공학과 공학학사
2016년 9월~현재: 상명대학교 소프트웨어학과 석사과정
〈관심분야〉 시스템 보안, 임베디드 보안, 블록체인

이 부 형 (Boohyung Lee) 정회원
2016년 2월: 상명대학교 컴퓨터소프트웨어공학과 졸업
2017년 8월: 상명대학교 소프트웨어학과 공학석사
〈관심분야〉 네트워크 보안, 블록체인

명 세 인 (Sein Myung) 학생회원
2013년 3월~현재: 상명대학교 컴퓨터소프트웨어공학과 학부과정
〈관심분야〉 정보보호, 바이너리 분석, 블록체인

이 종 혁 (Jong-Hyouk Lee) 종신회원
2010년 2월: 성균관대학교 공학박사
2009년 6월~2012년 2월: 프랑스 INRIA 연구원
2012년 3월~2013년 8월: 프랑스 그랑제꼴 TELECOM Bretagne 조교수
2013년 9월~현재: 상명대학교 소프트웨어학과 조교수
〈관심분야〉 프로토콜 분석 및 성능 평가, 바이너리 분석, 블록체인