https://doi.org/10.33778/kcsa.2019.19.2.011

블록체인에서 대용량 컴퓨팅 공격 보호 기술★

이 학 준*, 원 동 호**, 이 영 숙***

요 약

블록체인은 중앙신뢰 기관의 개입 없이 분산 컴퓨팅 환경에서 데이터를 관리하는 기술이다. 블록체인의 보안성, 효율성, 응용성으로 인하여 현재 금융 분야뿐만 아니라 제조, 문화, 공공 등 다양한 분야에서 블록체인 기술이 활용되고 있다. 그동안 블록체인에서 공격자는 51% 이상의 해시 파워를 갖출 수 없다고 여겨졌지만 최근 이에 대한 공격과 피해사례가 발생하고 있으며, 이기적인 채굴자 공격을 포함한 대용량 컴퓨팅 능력을 갖춘 공격의 빈도가 증가하고 있다. 또한, 일반 컴퓨터와 차원이 다른 성능을 발휘하는 양자컴퓨터의 발전은 블록체인의 새로운 위협이 되고 있다. 본 논문에서는 블록체인 특징과 합의 알고리즘에 대해 소개하고 컴퓨팅 연산력을 이용한 블록체인 공격기법을 설명한다. 그리고, 대용량 컴퓨팅 환경 구축방법과 양자 컴퓨터를 사용하는 공격 알고리즘이 블록체인 보안성에 미치는 영향을 분석한다. 마지막으로, 블록체인의 보안성을 향상하기 위한 대용량 컴퓨팅 공격 보호 기술 및 앞으로의 발전 방향을 제시한다.

Protection Technologies against Large-scale Computing Attacks in Blockchain

Hakjun Lee*, Dongho Won**, Youngsook Lee***

ABSTRACT

The blockchain is a technique for managing transaction data in distributed computing manner without the involvement of central trust authority. The blockchain has been used in various area such as manufacturing, culture, and public as well as finance because of its advantage of the security, efficiency and applicability. In the blockchain, it was considered safe a gainst 51% attack because the adversary could not have more than 50% hash power. However, there have been cases cau sed by large-scale computing attacks such as 51% and selfish mining attack, and the frequency of these attacks is increas ing. In addition, since the development of quantum computers can hold exponentially more information than their classical computer, it faces a new type of threat using quantum algorithms. In this paper, we perform the security analysis of block chain attacks composing the large computing capabilities including quantum computing attacks. Finally, we suggest the te chnologies and future direction of the blockchain development in order to be safe against large-scale computing attacks.

Key words : Blockchain, Large-scale Attack, Quantum Computing Attack, Post-Quantum Cryptography

접수일(2019년 5월 7일), 수정일(1차: 2019년 6월 19일), 게재확정일(2019년 6월 30일)

★ 본 논문은 2019년 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. 2019R1A2C1010159).

* 성균관대학교 전자전기컴퓨터공학과
** 성균관대학교 소프트웨어학과
*** 호원대학교 사이버보안학과(교신저자)

1. 서 론

2008년 나카모토 사토시는 중앙기관의 개입 없이 분산된 네트워크 환경에서 트랜잭션의 이중 지불 문제를 해결하기 위한 블록체인 기반의 비트코인을 제안했다[1][2]. 블록체인은 P2P(Peer-to-Peer) 네트워크상의 자치적인 분산 컴퓨팅 환경에서 데이터를 관리하는 기술이다. 블록체인에서 일정 기간에 한 번씩 만들어지는 트랜잭션 묶음을 블록(Block)이라 하며, 블록들은 시간적 순서에 따라 연결리스트 형태로 연결된 체인을 구성한다.

현재 블록체인의 보안성, 효율성, 응용성은 제조, 문화, 공공 분야 등 다양한 분야에서 비즈니스 모델의 혁신적인 변화를 끌어내는 파급적인 영향을 미치고 있다. 2018년 세계 블록체인 시장의 규모는 약 12억 달러이며, 2023년에는 233억 달러로 연평균 80.2%씩 성장할 것으로 예상되고 있다. 2016년 세계경제포럼(World Economic Forum, WEF)에서는 앞으로 전 세계은행의 80%가 블록체인 기술을 도입할 것이며, 2025년에는 전 세계 GDP의 10%가 블록체인 기반 기술에서 발생할 것으로 전망했다[3].

제3자의 개입 없이 참가자들 간 동일한 정보가 기록된 분산원장을 공유하고 저장하는 블록체인의 신뢰성과 비가역성이 입증된 후, 블록체인 기술은 암호화폐 기반 기술로 활용되었다[4]. 대표적인 암호화폐로는 비트코인과 이더리움이 있으며, 비트코인의 경우 2019년 3월 기준 평균 하루 약 6백만 개의 거래가 이루어지고 있다[5].

하지만, 최근 비트코인과 이더리움 등 암호화폐 시스템의 신뢰성과 비가역성을 위배하려는 공격이 발생하고 있다. 2018년 4월, 그동안 이론적으로 불가능하다고 여겨진 51% 공격이 버지코인을 대상으로 발생했으며 약 250,000XVG가 손실되었다. 2018년 5월, 모나코인에서는 이기적인 채굴 공격으로 시가 약 9만 달러의 암호화폐가 손실되었고, 2018년 5월에 비트코인 골드를 대상으로 51% 공격이 발생하여 트랜잭션 무효화 및 새로운 체인 형성을 통해 공격자는 약 1,800만 달러 상당의 코인을 탈취했다[6-7].

이처럼 대용량 컴퓨팅 능력을 갖춘 공격자의 블록체인 네트워크를 대상으로 하는 공격시도 및 피해사례가 증가하고 있다. 또한, 일반 컴퓨터뿐만 아니라 큐비트(Quantum bit)를 이용하여 일반 컴퓨터 대비, 지수(exponential)배 이상의 성능을 발휘하는 양자 컴퓨터의 등장과 양자 알고리즘의 발전으로 블록체인은 새로운 위협에 국면하게 되었다.

양자역학적 현상을 이용하여 다수의 정보를 동시에 연산할 수 있도록 구현된 양자 컴퓨터는 병렬 연산 처리 능력을 기반으로 일반 컴퓨터와 차원이 다른 연산 성능과 기능을 제공한다. 암호 프리미티브(Cryptographic primitive)를 공격할 목적의 양자 알고리즘을 이용하면 대칭키 암호, 공개키 암호, 해시 함수 등 현재 널리 사용되고 있는 대부분의 기존 암호 시스템이 취약해진다[8]. 현재 대부분의 블록체인 기술들은 트랜잭션 서명과 합의 알고리즘에서 타원곡선 기반의 공개키 전자서명 알고리즘인 ECDSA(Elliptic Curve Digital Signature Algorithm)와 해시 함수를 사용하고 있으므로, 블록체인 역시 양자 컴퓨팅 공격으로부터 취약해진다. 이렇게, 과거에는 블록체인상에서 불가능하다고 여겨져 보안 위협으로 고려되지 않았던 공격들에 대한 실현 가능성이 커지고 있다.

본 논문에서는 대용량 컴퓨팅 공격으로부터 블록체인의 보안성을 높이기 위한 대응기술과 이에 관한 연구의 중요성을 강조한다. 2장에서 블록체인 특징과 합의 알고리즘에 대해 설명하고, 3장에서 작업증명 합의 알고리즘 공격방법에 대해 설명한다. 4장에서는 대량 컴퓨팅 환경 구축방법과 양자컴퓨터를 이용한 블록체인 공격의 영향을 분석한다. 마지막으로, 5장에서 블록체인의 보안성 향상을 위한 대용량 컴퓨팅 공격 보호 기술 및 앞으로의 발전 방향을 제시한다.

2. 블록체인 특징과 합의 알고리즘

이 장에서는 블록체인의 특징과 각 목적에 따른 블록체인 네트워크 구성 형태, 새로운 블록의 유효성을 검증하며 블록체인을 구성하는 다양한 합의 알고리즘에 대해 소개한다.

2.1 블록체인 특징

- 익명성(Anonymity): 블록체인 시스템상의 모든 트랜잭션 내역은 공개되어 있으나, 거래 당사자에 대

한 정보는 공개키로 암호화되어 있음

- 탈중앙성(Decentralization): 블록체인은 P2P 형태의 분산적으로 데이터를 저장하기 때문에, 중앙 집중형 데이터베이스를 가질 필요가 없음
- 위변조 방지(Tamper proof): 트랜잭션 내역을 포함하는 블록의 정보가 변경되지 않음을 증명하고, 해시값 형태의 디지털 서명을 사용하여 거래정보의 무결성을 입증 가능함
- 이중지불방지(Preventing double spending): 합의 알고리즘을 통해 트랜잭션을 순서화하고, 거래에 한 번이라도 사용된 화폐는 소비되어 다른 거래에 사용될 수 없음

2.2 블록체인 유형

- 공개 블록체인(Public blockchain): 블록체인의 참여자들이 익명의 노드로 이루어져 있으며 데이터가 공개되어 있어 누구나 접근 가능함
- 사설 블록체인(Private blockchain): 블록체인의 참여자는 익명이 아닌 중앙 관리자가 허가한 사람만이 참여할 수 있고, 데이터에 접근하기 위해서도 중앙 관리자의 허가를 받아야 함
- 컨소시엄 블록체인(Consortium blockchain): 블록체인 네트워크가 중앙기관에 의해 관리되는 것이 아닌 여러 기관에서 노드를 구성하여 네트워크를 운영할 수 있으며, 여러 기관이 하나의 컨소시엄을 이루어 블록체인을 형성하므로 다수의 관리자가 존재함

2.3 블록체인 합의 알고리즘

2.3.1 작업증명

작업증명(Proof of Work, PoW) 과정은 컴퓨터의 연산력을 이용해 임의의 난이도를 선택하여 이를 만족하는 해시값을 찾는 과정이다. 채굴자가 목푯값보다 작은 해시값을 갖는 블록을 발견하면 해당 블록이 블록체인에 추가되며 보상을 획득한다. 컴퓨터 연산 능력에 따라 얻는 보상이 증가하기 때문에 작업증명 기반의 블록체인 네트워크에 참가하기 위해서는 많은 초기 비용이 발생한다. 만약 전체 네트워크의 51% 이상 컴퓨팅 파워를 차지한 공격자가 존재하면 트랜잭션 위변조 및 이중지불 공격이 발생할 수 있다.

2.3.2 지분증명

지분증명(Proof of Stake, PoS) 합의 과정에서는 보유한 암호화폐의 지분에 비례하여 다음 블록을 검증하는 검증자 노드로 선택될 확률이 높아지며, 검증자는 이에 대한 보상으로 해당 블록과 관련된 수수료를 지급 받는다. 하지만, 누구나 여러 블록에 자신의 지분을 증명할 수 있는 구조이기 때문에 지분을 많이 가진 공격자가 거짓으로 지분을 증명할 수 있으며, 많은 지분을 가진 소수에 의해 전체 네트워크가 좌우될 수 있다.

2.3.3 위임지분 증명

위임지분 증명(Delegated Proof of Stake, DPoS)은 지분 위임 결과(투표결과)에 따라 선출된 상위 노드에게 블록을 검증할 권한을 위임하여 합의를 수행한다. 상위노드는 암호 화폐 보유하고 있는 노드들로부터 투표를 통해 선출되며 일반 노드들은 본인이 소유한 암호화폐의 수 만큼 투표 권리를 행사한다. 상위 노드의 수가 제한되어 있어 합의 시간을 줄여 높은 TPS(Transaction Per Seconds)를 제공한다는 장점이 있지만, 상위노드 수가 적기 때문에 해커가 공격해야 할 노드가 적어 상위노드 대상으로 공격이 발생할 확률이 커진다. 또한, 투표율이 저조할 경우 상위노드 간의 담합 또는 투표라는 민주적 시스템이 왜곡될 수 있다[9].

2.3.4 중요도 증명

중요도 증명(Proof of Important, PoI)에서는 거래량, 거래금액 등 네트워크 참여도에 따라 결정되는 신뢰 점수라는 중요도가 높은 사람에게 더 많은 수수료를 분배한다. 하지만, 가짜 트랜잭션(Dummy transaction)을 사용하여 부정적인 방법으로 중요도를 올릴 수 있다는 단점이 있다.

앞서 소개한, 작업증명, 자산증명, 위임 지분증명, 중요도 증명 외에도 Ripple, PBFT(Practical byzantine falut tolerance), Tendermint 등 다양한 합의 알고리즘이 있다[10][11]. 본 논문에서는 컴퓨터의 연산 능력을 사용하는 작업증명 알고리즘을 기반으로 하여 발생할

수 있는 대용량 컴퓨팅 공격방법에 대해 고려한다.

3. 작업증명 합의 알고리즘 공격방법

3.1 전체 네트워크 관점에서의 블록체인 공격

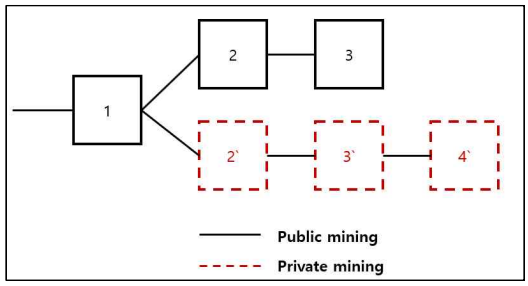
공격자는 자신의 컴퓨팅 능력을 이용하거나 네트워크 노드를 공격하여 51% 공격, 이중 지불, 이기적인 채굴(Selfish mining) 공격 등을 수행할 수 있다.

51% 공격이란 공격자가 전체 블록체인에서 합의 알고리즘에 사용되는 컴퓨팅 능력의 51% 이상을 장악하여 체인이 구성되는 과정을 인위적으로 조작하는 행위이다. 공격자는 51% 공격을 통해 자신의 자산을 여러 대상에 동시에 송금하여 자신이 소유한 자산보다 많은 트랜잭션을 발생시키는 이중 지불 행위를 할 수 있다. 또한, 방대한 연산 능력을 통해 트랜잭션 내역을 조작하고 합의 알고리즘을 왜곡하여 부당한 이익을 취할 수 있다. 공격자는 (그림 1)과 같이 우월한 컴퓨팅 능력을 통해 현재 트랙잭션 정보들에 대한 해시 문제를 먼저 풀어 생성한 블록을 바로 전파하지 않고 최대한 늦게 지연시킨 뒤에, 지연 시간 동안 다음 해시 문제를 풀어 다른 채굴자들보다 채굴 확률을 높이는 이기적인 채굴 공격을 수행할 수 있다[12].

이에 더해, 공격자는 악성코드를 사용하거나 네트워크를 장악하여 네트워크 내 노드들의 동작을 방해하여 블록체인 네트워크를 공격할 수 있다. 예로 들면, DDoS(Distributed Denial-of-Service) 공격을 통해 공격자는 짧은 시간 동안 무수히 많은 트랜잭션을 연결 노드에 전송하여 트랜잭션 처리에 대한 시간 증가, 중지 및 데이터 삭제를 유도할 수 있다. Eclipse 공격이란 공격자가 목표 노드와 연결된 후, 목표 노드를 다른 노드로부터 고립시킴으로써 공격 노드의 데이터만 수신하도록 하는 행위이다. 이를 통해 공격자와 타깃 노드가 동시에 블록 문제를 해결했을 때, 타깃 노드가 발견한 블록을 숨기거나 51% 공격을 더 쉽게 수행하기 위해 네트워크상의 다른 노드들을 제거할 수 있다.

3.2 마이닝 풀에서의 블록체인 공격

마이닝 풀(Mining pool)이란 점점 어려워지는 작업증명의 난이도 때문에, 다수 참가자가 그룹을 이루어



(그림 1) 이기적인 채굴자 공격방법

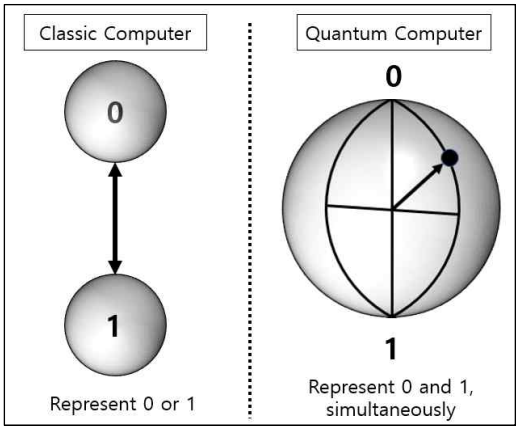
함께 해시 문제를 해결하고 각 노드의 기여도에 따라 보상을 나눠 갖는 구조이다. 마이닝 풀에서 공격자는 자신의 컴퓨팅 능력을 조절하여 BWH(Block Withholding) 공격을 수행할 수 있다[13]. 예로 들어 공격자는 Pool(A)와 Pool(B)라는 2개의 마이닝 풀에 참가했다고 가정하자. 공격자는 Pool(A)에서의 기여도를 낮추고 Pool(B)에서의 기여도를 높임으로써 Pool(B)가 해시 문제를 해결할 확률을 높인다. 결국, Pool(A)에 불공정한 손실이 발생하게 되고, 공격자는 Pool(B)에서 상대적으로 더 많은 보상을 획득하게 된다. 마이닝 풀을 관리하는 관리자는 BWH 공격이 발생했다는 것을 쉽게 식별할 수 있다. 하지만, 기여도가 낮은 공격자 역시 해당 마이닝 풀에서 해시 문제에 대한 답을 제출하는 것이기 때문에 공격자를 저지한다면 해당 마이닝 풀의 해시 파워 역시 줄어든다. 결과적으로 Pool(A)이 얻는 보상이 낮아짐으로 마이닝 풀 관리자는 BWH 공격을 무작정 저지할 수 없는 딜레마가 존재한다[14].

4. 대용량 컴퓨팅 구축 및 공격

공격자는 현재 일반 범용 컴퓨터를 이용하여 대용량 컴퓨팅 공격을 수행하기 위해 컴퓨팅 자원을 임대하거나 다른 채굴자들과 공모 또는 자신이 직접 구축할 수 있다[15]. 또한, 양자 컴퓨터 시대의 도래 및 발전으로 인하여 새로운 유형의 공격을 수행할 수 있다.

4.1 일반 컴퓨터의 대용량 컴퓨팅 구축과 공격

4.1.1 컴퓨팅 자원 임대



(그림 2) 일반 비트와 양자비트(큐비트)의 차이

공격자는 클라우드 컴퓨팅 시스템으로부터 컴퓨팅 파워 또는 저장공간을 빌리거나 대규모 봇넷(Botnet)의 제어권을 임대하여 작업증명 과정이 공격자의 의도대로 비정상적으로 동작하도록 공격할 수 있다. 예를 들어, 아마존의 Elastic Compute Cloud(EC2)에서 컴퓨팅 자원을 대량 구매할 경우 약 1달러에 50~100MH/s의 GPU 능력을 대여할 수 있다. 즉, 백만 개의 달하는 GPU를 백만 달러에 대여하면 공격자는 약 최대 95TB/s의 성능을 얻게 되고 이는 2017년 8월 이더리움 전체 네트워크의 해시율과 상응하다.

4.1.2 직접 컴퓨팅 자원 구축

공격자가 직접 대량의 하드웨어를 구매하여 대용량 컴퓨팅 능력을 구축해 작업증명 과정을 공격할 수 있다. 이 방식은 자산증명 과정에는 적용할 수 없지만, 모든 유형의 작업증명 시스템에는 적용할 수 있다. 만약 블록체인 네트워크의 해시율이 0^{8}H/s인 경우, 공격자가 약 15억 달러 상당의 ASIC 채굴 장비를 구입하면 블록체인 네트워크를 장악할 수 있다.

4.1.3 뇌물수수

공격자는 블록체인 내 기존 채굴자의 컴퓨팅 능력을 빌리거나 같이 공모하여 작업증명 과정을 공격할 수 있다. 컴퓨팅 자원의 임대 또는 직접 구축에 투입되는 비용의 절반만으로 블록체인 네트워크를 장악하기 위한 공격을 수행할 수 있지만, 뇌물수수를 통한 공격이 성공적으로 수행되기 위해서는 다른 채굴자의 충성도가 중요하다.

<표 1> 양자 컴퓨팅 도입 시 암호 알고리즘에 미치는 영향

Algorithm	Type	Impact
AES	Symmetric key	Lager key sizes needed
SHA-2 SHA-3	Hash function	Lager key sizes needed
RSA	Public key	No longer secure
ECDSA ECC	Public key	No longer secure
DSA	Public key	No longer secure

4.2 양자 컴퓨터 소개 및 공격

양자컴퓨터란 양자중첩, 양자측정, 양자얽힘과 같은 양자역학적 현상을 이용하여 연산을 수행하는 컴퓨팅 기술로서 (그림-2)와 같이 일반 컴퓨터와 달리 큐비트를 사용하여 0과 1을 동시에 나타낼 수 있다. 양자중첩 현상을 이용하면 개의 큐비트는 2 비트를 표현하고, 양자얽힘 현상을 이용하여 데이터 처리에 있어 일반 컴퓨팅보다 지수 배의 효율을 발휘한다. 최근 몇 년 동안 양자 알고리즘 이론에 상당한 발전이 있었으며, 대규모 양자 컴퓨터의 실용화가 가까워지고 있다. 양자컴퓨터가 도입되면 <표 1>과 같이 기존에 사용되는 암호 알고리즘의 기능이 무효화 되거나 키 크기를 늘려 보안성을 높여야 한다.

4.2.1 Grover 알고리즘

1996년 Lov Grover가 양자 컴퓨팅을 이용한 데이터베이스 검색 알고리즘을 개발했다. 비 정렬 상태의 데이터베이스에서 자료를 검색할 경우, 고전적인 알고리즘은 $O\ N$)의 시간복잡도를 보이나, Grover 알고리즘은 $O(\ \ N)$의 시간복잡도를 보인다. 이 알고리즘을 이용하여 비트코인의 작업증명 과정을 공격할 경우, 무어의 법칙에 의해 큐비트가 증가함에 따라 양자컴퓨

터의 성능이 발전하더라도 State distillation, Error syndrome extraction 등 양자 오류 정정 과정에서 발생하는 오버헤드가 성능을 저하시켜 2040년에도 비트코인 전체 해시율의 약 1000배 느린 성능을 발휘하여, 양자 컴퓨터의 해시 파워를 통해 비트코인의 작업증명 과정을 공격하기 힘들다는 연구가 있다[16].

하지만, Grover 알고리즘을 응용한 BHT(Brassard, Hoyer, Trapp) 알고리즘을 사용할 경우 해시 함수의 충돌 쌍 문제(Collision problem)를 해결하는 시간복잡도가 N)에서 $O(\sqrt{N})$으로 감소하기 때문에 [17], 양자 컴퓨터를 이용한 공격기법은 점점 고도화될 것이다. 지금까지 불가능해 보였던 해시 함수에 대한 무차별 대입 공격은 현실화될 것으로 전망되며 NIST는 해시 함수의 보안 레벨을 높여 양자컴퓨터로부터 안전한 SHA-384 개발 및 표준화를 진행 중이다.

4.2.2. Shor 알고리즘

1994년 Peter Shor는 양자 컴퓨팅을 이용한 인수분해 알고리즘을 개발했다. Shor 알고리즘은 확률론적 알고리즘으로, 인수분해 문제를 푸는데 다중 로그 시간인 $O((\log N)\ (\log\log N)(\log\log\log N))$의 시간복잡도를 보인다. 양자컴퓨터 성능의 발전에 따라 2027년이면 양자컴퓨터는 10분 만에 인수분해 문제를 해결하여 서명 알고리즘을 무력화시킬 수 있어 Grover 알고리즘보다 더 위협적인 공격 성능을 발휘한다.

Shor 알고리즘을 이용하면 새로운 트랜잭션이 블록체인 네트워크에 전파되었으나 아직 블록으로 내재되지 않았을 때 해당 트랜잭션에 나타나는 공개키로부터 비밀키를 추출할 수 있으며, 공격자는 이 비밀키를 이용하여 같은 주소의 새로운 트랜잭션을 발생시켜 희생자보다 먼저 자신의 트랜잭션을 블록체인에 내재시킬 수 있다. 따라서 공격자는 원래 주소로 서명된 트랜잭션을 탈취할 수 있다

5. 대용량 컴퓨팅 공격 보호 기술

컴퓨터 성능 향상과 병렬성의 증가로 과거에는 불가능하다고 여겨지던 블록체인을 목표로 하는 공격으로부터의 피해사례 및 공격시도에 대한 빈도가 증가하고 있다. <표 2>는 공격자가 자신의 컴퓨팅 자원을 이용하거나 압도적인 해시 연산 능력을 통해 다양한 방법으로 네트워크를 장악하여 블록 내 거래정보를 위변조하고 불법적인 이익을 얻으려는 공격기법과 이에 대응하기 위한 방어기법을 설명한다. 작업증명 기반의 합의 알고리즘을 사용하는 블록체인 환경에서 투입되는 컴퓨팅 자원이 많을수록 정직한 채굴자가 얻는 수입이 증가하듯이, <표 2>에 설명된 공격들 역시 우월한 컴퓨팅 연산량을 기반으로 하면, 이에 대한 피해가 더욱 막대해진다. 따라서, 이와 같은 공격이 발생했을 시 이를 조기 탐지하고 대응하는 것이 중요하다.

또한, 4.2장에서 설명했듯이 양자 컴퓨팅 알고리즘을 사용하면 현존하는 대부분의 암호 시스템이 취약해진다. 현재 NIST는 양자 공격으로부터 안전한 양자내성 암호(Post-Quantum Cryptography)를 2022년까지 표준화하기 위한 프로젝트를 진행 중이다. 대표적인 양자 내성 암호체계로는 격자기반(Lattice-based), 다변수(Multivariate), 해시기반(hash-based), 코드기반(Code-based) 암호 알고리즘 등이 있다. 이러한 국내외 동향을 고려하면 앞으로 블록체인은 다음과 같은 방향으로 발전할 수 있다.

첫 번째, 양자 내성 공개키/비밀키 생성과 블록 서명 과정에서 양자 내성 전자서명 알고리즘을 적용하여 블록체인의 보안성을 높인다. 양자 내성 암호 후보군으로 제출된 KEM(Key Encapsulation Mechanism)과 서명 알고리즘들은 각각 IND-CCA(Indistinguishability under chosen ciphertext attack)와 EUF-CMA(Existential Unforgeability under Chosen Message Attack)를 만족한다. 즉, 양자 내성 암호는 기존 소인수분해 문제를 기반으로 하는 공개키 기반의 암호들보다 뛰어난 보안성과 함께 양자 안전(Quantum-safe)을 보장한다. 따라서 양자내성 암호를 블록체인에 적용할 경우, 안전한 공개키/비밀키 생성을 통해 트랜잭션과 사용자의 암호화폐 지갑(Cryptocurrency wallet)을 안전하게 보호할 수 있다. 하지만, 각 양자 내성 암호 알고리즘마다 키 생성 속도, 암/복호화 속도, 키 크기, 서명문 크기 등 성능 측면에서의 지표가 상이하기 때문에 블록체인에 어떤 암호 알고리즘 적용하는 것이 효율적인지에 대한 연구가 필요하다.

두 번째, 블록체인에 사용하는 해시 알고리즘의 보안 레벨을 높인다. 현재 대부분의 블록체인 기술들은

<표 2> 대용량 컴퓨팅 능력을 이용한 작업증명 과정에 대한 공격과 대응방안

Attack	Description	Impact	Countermeasures
Double Spending	Make more than one transactions using one asset	Provider may lose their products or services	Place observers on blockchain network and notify double spend
Finney attack	Attacker premines the block and broadcasts it for double spending	Provider may lose their products or services	Multiple confirmations for transactions
51% attack	Control blockchain system, with more than 50% hash power of total hash power	Attacker can reverse transactions and perform double spending, modify the ordering of transactio -ns and control the confirmation operation	Inserting observers in network, communicating double spending alerts among peers and disincent -ivizing large mining pools
Selfish mining	When attacker finds blocks, he does not immediately broadcast them but publish them on selective time	Potentially allowing for 51% attacks	Using random branch selection, timestamp based techniques, fork punish rule
Bribery attack	Adversary bribes miners to mine or control blockchain system	Potentially allowing for 51% attacks	Increase the rewards for honest miners, make aware the miners to the long-term losses or bribery
BWH	Miner in a pool submits only PPoWs, but not FPoWs	Waste resources of miners in pool, decrease target pool's profits and get extra revenue of attacker	Compare the number of PPoWs and FPoWs distributed to miners in the pool and the number of sub missions submitted by the miners
FAW	Improvement on attack effects by generating fork using combin -ations of selfish mining and BWH attack	Waste resources of miners in pool, decrease target pool's profits and get extra revenue of attacker	There is no practical defense
Quantum attack	Use large quantum computer and perform PoW using Grover algorithm.	Attacker may maximize 51% atta -ck impact and break existing cry -ptographic scheme in blockchain	Apply new cryptographic scheme based on post-quantum cryptography in blockchain

SHA-256을 사용한다. 만약 이를 SHA-512로 대체하면 공격자는 해시 충돌 값을 찾아내기 어려워진다. 해시 알고리즘의 보안 레벨이 높아지면, 블록 크기가 커지므로 결국, TPS가 낮아져 블록체인 네트워크의 성능이 저하될 수 있다. 따라서, 양자컴퓨터를 포함한 대용량 컴퓨팅 공격으로부터 안전하고 적합한 해시 알고리즘에 대한 추가적인 연구가 필요하다.

마지막으로, 새로운 블록체인 합의 알고리즘 및 블록체인 네트워크 프로토콜에 대한 제안 또는 기존 알고리즘을 개선한다. 컴퓨팅 능력을 이용하는 작업증명 과정에서 이기적인 채굴자 및 BWH 공격과 같은 연산 능력의 상대적 우월성을 통해 이득을 취하는 공격에 대한 대응방안이 연구되고 반면에, BWH 공격의 발전 형태인 FAW(Fork After Withholding)라는 공격이 새로 출현했다. 즉, 작업증명을 보완하기 위해 지분증명 과정이 등장했듯이, 이와 같은 문제점을 보완할 수 있는 새로운 블록체인 합의 알고리즘 및 프로토콜에 관한 연구가 필요하다. 하지만, 많은 사용자가 동일한 프로토콜을 사용하는 환경에서, 합의 알고리즘 또는 네트워크 프로토콜에 갑자기 상당한 변화를 적용하는 것은 현실적 어려움이 존재한다. 따라서, 기존 알고리즘 체계에서 하위 호환성(Backward compatibility)을 만

족할 수 있도록 사소한 변경만으로도 대용량 컴퓨팅 공격을 방어할 수 있는 대안이 필요하다.

6. 결 론

본 논문에서는 대용량 컴퓨팅 능력을 이용한 블록체인 공격기법과 이에 대한 영향을 분석한 후, 블록체인의 보안성 향상을 위한 대응기술과 발전 방향을 제시했다. 고도화되고 있는 대용량 컴퓨팅 공격으로부터 블록체인의 보안성을 보장하기 위해 새로운 암호 프리미티브를 적용하거나 기존의 합의 알고리즘 및 네트워크 프로토콜을 개선해야 한다. 더불어, 블록체인의 보안성 향상과 함께 네트워크 성능을 유지하기 위한 연구가 동행 되어야 한다. 블록의 생성 간격, 크기, 전파 속도에 따라 네트워크 성능 및 메인체인에 포함되지 않는 stable 블록이 생성되는 확률은 각각 다르다. 그러므로, 이러한 다양한 요인들을 종합하여 안전한 블록체인의 설계 및 개발을 위한 선험적 연구 또한 필요하다.

참고문헌

[1] Nakamoto, Satoshi. “Bitcoin: A peer-to-peer electronic cash system.”, 2008.

[2] 양환석, 최대수, “MANET 환경에서 데이터 무결성 보장을 위한 블록체인 적용에 관한 연구”, 융합보안논문지, 제18권, 제5호, pp. 53-58, 2018.

[3] “WEF”, www.3.weforum.org.

[4] “coinhills, “https://www.coinhills.com/ko/market/exchange.

[5] 백승수, “환자의 익명성이 보장되는 암호문 정책 속성중심 암호를 활용한 블록체인 기반 전자의무기록 공유 프레임워크”, 융합보안논문지, 제19권, 제1호, pp. 49-60, 2019.

[6] CCN, “Privacy Coin Verge Succumbs to 51% Attack [Again]”, https://www.ccn.com, 2018.

[7] FORTUNE, “Bitcoin Spinoff Hacked in Rare 51% Attack”, http://fortune.com, 2018.

[8] Chen, L., Chen, L., Jordan, S., Liu, Y. K., Moody, D., Peralta, R., and Smith-Tone, D., “Report on post-quantum cryptography”, National Institute of Standards and Technology, 2016.

[9] 김준상, “블록체인 기반 암호화폐의 조사”, 한국컴퓨터정보학회논문지, 제24권, 제2호, pp. 67-74, 2019.

[10] Zheng, Z., Xie, S., Dai, H., Chen, X., and Wang, H., “An overview of blockchain technology: Architecture, consensus, and future trends”, In 2017 IEEE International Congress on Big Data, pp. 557-564, 2017.

[11] Bach, L. M., Mihaljevic, B., and Zagar, M., “Comparative analysis of blockchain consensus algorithms”, In 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics, pp. 1545-1550, 2018.

[12] Eyal, I., and Sirer, E. G., “Majority is not enough: Bitcoin mining is vulnerable”, Communications of the ACM, Vol. 61, No. 7, pp. 95-102. 2018.

[13] Courtois, N. T., & Bahack, L., “On subversive miner strategies and block withholding attack in bitcoin digital currency.” arXiv preprint arXiv:1402.1718, 2014.

[14] Kwon, Y., Kim, D., Son, Y, Vasserman, E., and Kim, Y., “Be selfish and avoid dilemmas: Fork after withholding attacks on bitcoin” In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, pp. 195-209, 2017.

[15] Bonneau and Joseph. “Hostile blockchain takeovers”, Bitcoin’18: Proceedings of the 5th Workshop on Bitcoin and Blockchain Research, 2018.

[16] Aggarwal, D., Brennen, G. K., Lee, T., Santha, M., and Tomamichel, M., “Quantum attacks on Bitcoin, and how to protect against them”, arXiv preprint arXiv:1710.10377, 2017.

[17] Boyer, M., Brassard, G., Høyer, P., and Tapp, A., “Tight bounds on quantum searching”, Fortschritte der Physik: Progress of Physics, Vol. 46, No. 45, pp. 493-505, 1998.

〔저자소개〕

이 학 준 (Hakjun Lee)
2018년 3월~현재 성균관대학교 전자전기컴퓨터공학 박사과정
2018년 2월 성균관대학교 전자전기컴퓨터공학 석사
2015년 2월 한국교통대학교 소프트웨어공학 학사
email : hjlee@security.re.kr

원 동 호 (Dongho Won)
2018년 3월~현재 성균관대학교 소프트웨어학과 명예교수
2015년~2018년 성균관대학교 컴퓨터공학과 행단석좌 교수
1982년~2015년 성균관대학교 컴퓨터공학과 교수
2002년~2003년 한국정보보호학회장
1985년~1986년 일본 동경공업대학교 객원연구원
1978년~1980년 한국전자통신연구원 전임연구원
1976년~1988년 성균관대학교 전자공학 (학사, 석사, 박사)
email : dhwon@security.re.kr

이 영 숙 (Youngsook Lee)
2009년 3월~현재 호원대학교 사이버보안학과 부교수
2008년 8월 성균관대학교 컴퓨터공학 박사
2005년 2월 성균관대학교 석사
1987년 2월 성균관대학교 정보공학사
email : ysooklee@howon.ac.kr