Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.30, NO.1, Feb. 2020 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2020.30.1.87

블록체인의 양자 내성 전자서명 호환성을 증대하기 위한 트랜잭션 구조 제안

김 미 연,[1†] 이 준 영,[2] 윤 기 순,[3] 염 흥 열[4‡]
[1,2,3]NSHC (연구원, 책임연구원, 소장), [4]순천향대학교 (교수)

Proposal of A Transaction Structure to Improve Compatibility of Blockchain regarding Post-Quantum Digital Signatures

Mee Yeon Kim,[1†] Jun Yeong Lee,[2] Kisoon Yoon,[3] Heung Youl Youm[4‡]
[1,2,3]NSHC (Researcher, Senior researcher, Director),
[4]Soonchunhyang University (Professor)

요 약

양자 내성 암호와 블록체인을 결합한 것을 양자 내성 블록체인(Post-Quantum Blockchain)이라 부르며[1], 양자 컴퓨터를 대비한 양자 내성 블록체인에 대한 연구가 이루어지고 있다. 그러나 양자 내성 블록체인을 구현하기 위해 임의의 양자 내성 암호를 기존 블록체인에 그대로 도입하게 되면, 비대한 공개키, 서명 크기가 문제가 되거나, 서명 검증 시간이 길어지는 등의 문제가 발생한다. 본 논문은 비대한 공개키와 서명 크기를 가진 전자서명 알고리즘을 고정된 사이즈로 감소시켜 저장하는 방식을 제안한다. 양자 내성 암호를 블록체인에 도입하기 위한 새로운 트랜잭션 구조와 프로토콜을 제안하며, 제안 메커니즘을 적용하여 오픈소스 기반의 양자 내성 블록체인을 구현했다. 본 연구를 통하여 블록체인의 양자 내성 전자서명 호환성을 증대시키고, 전체적인 블록체인의 크기도 감소시킬 수 있다.

ABSTRACT

Researches on Post-quantum blockchain, which is a synthesis of blockchain and post-quantum cryptography[1], are relatively unrevealed areas but have needs to be studied with the regard to the quantum computers. However there could be several fundamental problems, e.g. unsustainably large size of public key and signature, or too lengthy time for sign and verification, if any post-quantum cryptography is adopted to the existing blockchain to implement post-quantum blockchain. Thus, a new method was proposed in this paper that produces fixed length of references for massive signatures and corresponding public keys to enable relatively lightweight transactions. This paper proposed the mechanism that included a new transaction structure and protocols, and demonstrated a post-quantum blockchain that the proposed mechanism was adopted. Through this research, it could enhance compatibility of blockchain regarding post-quantum digital signature, possibly reducing weights of the whole blockchain.

Keywords: Post-quantum blockchain, Distributed Ledger Technologies, Blockchain

Received(10. 30. 2019), Modified(01. 13. 2020), Accepted(01. 13. 2020)

† 주저자, kimmy03@nshc.net
‡ 교신저자, hyyoum@sch.ac.kr(Corresponding author)

I. 서 론

전자서명에는 보통 RSA와 ECC 등 비대칭 암호 알고리즘에 기반한 전자서명 스킴이 사용된다. 그러나 실용적으로 사용가능한 양자 컴퓨터가 구현될 시 프로세서의 성능이 막대하게 향상될 수 있으며, 쇼어 알고리즘(Shor's algorithm), 그로버 알고리즘(Grover's algorithm)등 양자 알고리즘을 이용하여, 기존 컴퓨터로 연산할 수 없던 문제를 풀 수 있다. 쇼어 알고리즘은 공개키 암호 알고리즘의 근간이 되는 인수분해, 이산 로그 문제를 다항식 시간 내로 연산할 수 있어, RSA, ECC는 취약한 암호 알고리즘으로 전락하게 된다. 그로버 알고리즘은 기존 암호 알고리즘의 보안 복잡도를 반감할 수 있어 해시함수, 대칭키 등의 암호 알고리즘의 보안성이 반감된다.[2]

대부분의 분산원장 및 블록체인은 ECC 기반의 전자서명 스킴(ECDSA)을 사용한다. 이를 이용하는 분산원장 및 블록체인은 양자 컴퓨터를 고려할 시 장기적인 사용을 기대할 수 없다. 이에 대비해 양자 내성 암호(Post-Quantum Cryptography)를 블록체인에 도입하는 연구가 진행되고 있다. 양자 내성 암호와 블록체인을 결합한 것을 양자 내성 블록체인(Post-Quantum Blockchain)이라 부르며, 쇼어 알고리즘, 그로버 알고리즘 등 양자 알고리즘 공격에 내성을 갖는다[1]. 양자 내성 블록체인을 구현하기 위해 임의의 양자 내성 암호를 블록체인에 그대로 도입하게 되면, 비대한 공개키, 서명 크기가 문제가 되거나, 서명 검증 시간이 길어지는 문제가 발생할 수 있다.

따라서 본 논문은 양자 내성 암호를 블록체인에 도입하기 위한 새로운 트랜잭션 구조와 프로토콜을 제안하며, 제안을 적용하여 양자 내성 블록체인을 구현한다. 새로운 트랜잭션은 발신자의 서명과 수신자의 공개키 대신 그의 해시값을 가지는 구조로 변경하고, 공개키, 서명 쌍을 같이 배포해 트랜잭션을 검증한다. 또한 블록을 구별하여 검증과정을 달리한다. 논문의 구성은 다음과 같다. 2장은 관련 연구로 블록체인 및 그의 보안성, 연구 동향을 서술한다. 3장은 배경으로 양자 내성 전자서명의 사양을 검토하고, 기호를 정의한다. 4장은 양자 내성 합의 메커니즘을 제안하고, 5장은 그를 도입해 양자 내성 블록체인을 구현하고 그 성능을 실험한다. 본 연구를 통하여 비대한 공개키와 서명 크기를 가진 전자서명 알고리즘을 고정된 사이즈로 감소시켜 저장하는 방식을 제안한다. 이를 통해 다양한 양자 내성 전자서명을 블록체인에 도입할 수 있으며, 궁극적으로 블록체인의 양자 내성 전자서명 호환성을 증대시키고, 전체적인 블록체인의 크기도 감소시킬 수 있을 것으로 사료된다.

II. 관련 연구

2.1 비트코인과 블록체인

블록체인은 탈중앙화되고 변경 불가능한 디지털 분산 원장 시스템으로 신뢰가 없는 개인끼리 P2P(Peer-to-Peer) 네트워크 기반 디지털 거래에서의 이중지불을 막고자 고안된 기술이다. 비트코인은 블록체인을 도입하여 만든 대표적인 암호화폐이다. 비트코인은 P2P 네트워크를 통해 거래에 대한 정보를 주고받는다. 네트워크에 참여하는 노드는 인증을 받을 필요 없이 'bitcoin core'와 같은 소프트웨어를 설치하여 자신의 개인키, 공개키를 생성해 거래할 수 있다. 노드 간의 위계가 없고 모두 동등한 권한을 가지기 때문에 비트코인은 탈중앙화(decentralized)된 특징을 갖는다.

각 블록은 이전 블록의 해시값을 포함하기 때문에 이전 블록의 내용을 변경하면 해시값이 일치하지 않아 쉽게 위변조를 탐지할 수 있다. 위변조가 탐지되지 않기 위해서는 그 뒤에 이어지는 모든 블록의 해시값을 조작해야 하기 때문에 사실상 변경이 힘든 특성을 가진다.

블록체인에서의 거래는 공개키 암호 알고리즘 기반의 전자서명을 활용하여 이루어진다. Fig. 1.과 같이 개인키로 전자서명하여 발신자를 검증하고 공개키를 기반으로 만들어진 주소를 입력하여 코인을 전송한다. 이렇게 블록체인 상의 거래는 전자서명을 통

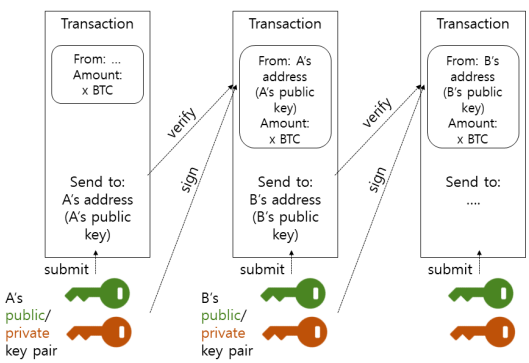


Fig. 1. Flow of the transaction transfers[3]

해 소유권을 데이터에 연결하여 증명, 검증한다. 거래가 생성되면 시스템에 참여하는 모든 노드에게 거래가 전파된다. 노드는 거래를 수집하여 합의 알고리즘에 따라 블록을 생성하고, 블록을 체인 끝에 덧대어 블록체인을 증식해나간다.

2.2 승인되지 않은 트랜잭션 풀

트랜잭션이 전파되면 노드는 트랜잭션을 검증하고 그를 트랜잭션 풀에 일시적으로 저장한다. 이 풀을 승인되지 않은 트랜잭션 풀 (Unconfirmed transaction pool)이라 하고 반대로 블록에 담긴 트랜잭션을 승인(Comfirmed)되었다고 표현한다. 즉 새로 생성되어 블록에 담기기 전의 트랜잭션을 모아두는 곳이 승인되지 않은 트랜잭션 풀이다. 블록이 생기면 블록에 기록된 트랜잭션을 확인하여 승인되지 않은 트랜잭션 풀에서 해당 트랜잭션을 제거한다.

트랜잭션의 승인 횟수가 많아질수록 해당 거래는 이중지불로부터 안전하다[3]. 아직 블록에 담기지 않은 상태의 트랜잭션의 상태는 승인 0번으로 표현하며, 블록에 담긴 상태를 승인 1번, 뒤이어 블록 1개가 생성되었다면 승인 2번으로 표시한다. 블록체인의 블록 위치는 높이(Height)로 표현된다.

2.3 비트코인 보안성

[3]에서는 비트코인에 대한 가장 기본적인 공격으로 공격자가 빠르게 블록을 작성하여 조작된 트랜잭션이 포함된 블록을 유효하게 만드는 이중지불 공격에 대한 보안성을 검토했다. 즉 이미 결제한 돈을 다른 곳에 사용하는 이중지불 거래를 생성하고, 그를 포함한 블록 뒤에 연속적으로 블록을 생성함으로써 유효한 체인이 되게끔 하는 것이 공격의 목표이다.

[3]에서는 공격자가 z블록 떨어진 블록에서부터 착한 노드와 블록 경쟁을 벌여 이길 확률을 구하기 위해서 Binomial Random Walk와 Gamblers Ruin Problem[4]를 적용하여 확률을 구했다. 착한 노드가 다음 블록을 구할 확률은 p이고, 공격자가 다음 블록을 구할 확률은 q이며, $p+q=1$ 일 때, 공격자가 z블록 뒤에서 시작하여 체인을 따라잡을 확률은 q_z로 나타냈다[3]. 이를 Binomial Random Walk에 따라, 착한 노드가 블록을 생성하면 z값에 +1을 하고, 공격자가 블록을 생성한 경우는 -1을 하면 q_z는 (1)과 같다[3].

$$q_z = p \cdot q_{z+1} + q \cdot q_{z-1} \tag{1}$$

그리고 Gambler Ruin Problem을 적용하여, 갬블러, 즉 공격자가 무한하게 공격을 시도를 할 수 있는 상황을 가정하여 확률 (2)를 도출했다[3].

$$q_z = \begin{cases} 1 & \text{if } p \le q \\ (q/p)^z & \text{if } p > q \end{cases} \tag{2}$$

공격자는 조작된 체인이 합의된 체인보다 길어지기 전까지는 체인을 공개하지 않는다. 착한 노드들이 블록을 생성하여 덧이어 나가는데 걸리는 시간이 평균 블록 생성 시간 T 만큼이 걸린다면, 모든 착한 노드들은 매 T 마다 p블록을 생성한다. 그렇다면 z개의 블록을 생성하기 위해서는 zT/p만큼의 시간이 필요하다. 공격자는 매 T 마다 q블록을 생산하고 zT/p 시간 동안 공격자가 생성하는 블록의 개수는 푸아송 분포값 $\lambda = zq/p$ 와 같다[3]. 그렇다면 착한 노드가 z블록을 생성할 동안 공격자가 더 많은 블록을 생성할 확률은 Poisson density function[12]에 따라 (3)으로 정리됐다[3].

$$1 - \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!}(1-(q/p)^{z-k}) \tag{3}$$

따라서 공격자가 유효한 체인을 따라잡을 확률은 수식 (3)을 통해 구할 수 있으며[3], 각 요인의 증감에 따른 성공률이 [6]에 기술됐다.

비트코인에서는 이중지불 공격을 방지하기 위해, 6번 이상 승인 후 거래를 사용할 수 있도록 설정했다. 따라서 공격자는 이중지불 공격을 시행하고 6번 이상 블록을 생성하여 기존 체인보다 길어지는 경우 이중지불에 성공할 수 있다. 이에 더해 최근 통계(19' 4월 14일 09:00 (GMT+0900)시 기준)를 이용하여 51% 공격에 필요한 자원량을 예측한다.

Fig. 2.은 지난 2년간 비트코인에 참여한 노드 수 통계이다. 평균적으로 9949 개의 노드가 참가했으며, 가장 최근값은 9515 개다[7]. Fig. 3.는 지난 2년간 비트코인 네트워크의 해시율 통계이다. 가장 해시율이 높을 때는 61,866,256 TH/s 이고, 가장 최근값은 38,771,476 TH/s 이다[8]. 통계값을 기준으로 한 노드 당 가지는 평균 해시율은 4074.77 TH/s 이고, 6개 블록 수를 따라잡기 위해서는 최소 6%의 해시율을 가져야 0.003%의 성공확

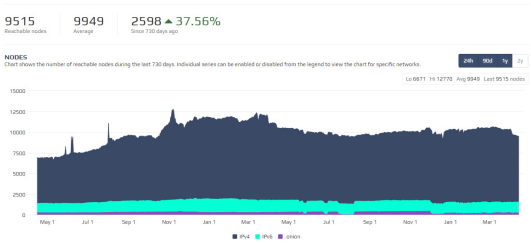


Fig. 2. The estimated number of reachable nodes during the last 2 years[7]

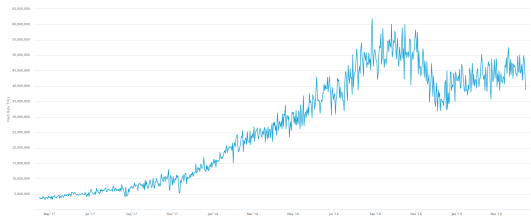


Fig. 3. The estimated number of tera hashes per second during the last 2 years[8]

률을 가진다[3][6]. 공격을 성공시키기 위해서는 약 2,326,288.56 TH/s의 해시율을 가져야 하며, 평균 571개 이상의 노드가 영구적으로 담합하여 공격을 수행하거나, 공격자가 571개 이상의 노드가 가진 컴퓨팅 파워를 가져야 한다.

2.4 관련 연구

양자 내성 블록체인과 관련하여 현재 서비스를 제공하는 대표적인 벤더는 Corda[9], QRL[10] 등이 있다. Corda는 해시(hash) 기반 전자서명인 XMSS를 블록체인에 도입하는 논문을 발표했고[11] 이 전자서명을 이용할 수 있도록 서비스를 제공한다고 밝혔다[9]. Corda에서 제안하는 BPQC는 modified XMSS 기반 One Time Signature 스킴을 도입했다. OTS이기 때문에 서명키는 1번 혹은 적은 횟수만 사용가능하고, 다른 해시 기반 전자서명인 XMSS나 SPHINCS보다 작은 서명, 빠른 키생성, 서명/검증 시간을 장점으로 꼽았다. 실제 토큰 발행 및 계약 서명 시, ECDSA, RSA와 동시에 사용 가능하다고 한다[9]. QRL은 XMSS 기반 분산원장 플랫폼을 이더리움으로 개발하여, 2018년 06월에 메인넷을 런치했다. 현재는 PoW를 기반으로 합의를 도출하며, PoS를 도입할 예정이라고 밝혔다[10].

양자 내성 블록체인에 대한 연구는 주로 해시 혹은 격자 기반 전자서명에 대한 연구가 주를 이뤘다[1][11]. 또한 양자암호통신을 기반으로 노드를 선별하는 연구가 진행되고 있다[12]. 국내의 관련 논문은 거의 없으나 트랜잭션과 머클트리에 해시 기반 양자 내성 서명 알고리즘을 도입하여 성능을 측정한 연구가 있다[13].

[12]에서는 양자 컴퓨터의 위협에 대비하여 양자암호통신 기반으로 한 블록체인을 제시했으며, PoW 대신 PBTF 브로드캐스트 프로토콜을 이용했다. [12]에서는 1개의 faulty 노드를 포함한 총 4개의 노드로 구성된 네트워크에서 제안한 블록체인의 성능을 실험했다. 실험 결과, 블록에는 유효한 트랜잭션만이 기록되었고, 트랜잭션에 포함되는 양자암호키의 용량은 40bit, 브로드캐스트 프로토콜에 포함되는 양자암호키의 용량은 80bit로 나타났다.

[13]에서는 기존의 ECDSA 전자서명 알고리즘을 대신하여 해시 기반 양자내성 서명 알고리즘 중 서명 길이가 짧은 편인 Winternitz One-Time Signature를 적용했다. 또한 머클트리에 Merkletree Signature Scheme을 도입하여 트랜잭션의 검증과 블록의 무결성을 강화했다.

한편 블록체인 크기를 감소시키는 방안에 대한 연구는 주로 자료구조를 변형하여 보관하는 데이터를 감소시키는 방안이 주로 연구되었다. 블록체인 중 오래된 데이터를 삭제하고 그를 대체하는 메타데이터를 보관하는 방안과,[14][15] SQLite를 적용하여 블록체인을 감소시키는 방안[16] 등이 연구되었다.

[14]에서는 사용하지 않은 트랜잭션 아웃풋 집합을 별도의 자료구조로 보관하고, 사용한 트랜잭션 아웃풋을 '사용한 블록'에 저장하는 새로운 방식을 제안하였다. 그리고 블록체인 네트워크에 참여하는 노드를 타입별로 나누어 한 그룹의 노드가 사용한 블록을 나누어 보관하여 한 노드 당 보관하는 블록체인의 사이즈를 줄이는 방안을 제안하였다.

[15]에서는 머클트리를 기반으로 한 'account tree'를 새로 제안하여 계정의 잔고를 기록하고 업데이트 한다. 그리고 신규 블록 중 수백개 내지 수천개만 보관하고, 오래된 블록은 삭제하여 블록체인의 사이즈를 대폭 감소시키는 방안을 제안하였다.

[16]에서는 SQLite를 적용하여 직렬형 데이터를 관계형으로 저장하므로써 불필요한 인덱스와 위치 데이터 값을 삭제하는 방안을 제안하였다.

III. 배경

3.1 전자서명의 크기 및 서명시간 검토

모든 양자 내성 암호는 ECDSA보다 비대한 공개키 크기와 서명 크기를 가진다. 본 논문은 비트코인을 포함한 여러 암호화폐에 이용되는 ECDSA 전자서명 알고리즘과 파라미터 secp256k1을 비교군으로 제시한다. Table 1.에 ECDSA secp256k1 의 공개키/서명 크기가 나타나 있다. Table 2.에는 해시 기반 SPHINCS$^+$ -SHA256[18], XMSS-SHA-256[19], 아이소제니(isogeny) 기반 Supersingular isogeny[20], 격자 기반 pqNTRUSign[21] 등 양자 내성 전자서명의 공개키/서명 크기가 정리되어 있다.

양자 내성 전자서명은 ECDSA 전자서명보다 큰 공개키, 서명 크기를 가진다. 공개키는 2배~64배 차이가 나며, 서명은 22배~1920배가 차이난다. 이러한 양자 내성 전자서명이 그대로 적용되면, 트랜잭션의 크기 또한 비례하여 증가하고, 블록, 블록체인의 크기 또한 비례하여 차이날 것이다. 블록체인 저장 공간이 매우 비대해지기 때문에 한 노드가 부담하는 자원, 비용 등이 증폭될 것으로 예측된다.

2019년 4월 14일 09:00(GMT+0900)시 기준 비트코인 블록체인의 전체 크기는 약 207.66 GB, 평균 거래수 2,763, 블록 수는 578,151개이다[22]. 이에 기반하여 각 양자 내성 전자서명에 대해 평균 거래 크기, 블록 크기, 체인 전체의 크기를 추측하였다. Table 3.에 추측치가 기술되어 있으며, 현재 비트코인과 같은 블록수가 쌓였다고 가정하면 최소 약 54 Tb ~ 최대 1,924 Tb 정도로 추측됐다. 공개키/서명 쌍의 사이즈 증가는 블록체인의 무게를 배로 증가시켜 상당한 부담이 될 것이다. 때문에 공개키/서명 크기에 대한 부담을 줄일 수 있는 방안이 필요하다.

양자 내성 전자서명은 알고리즘에 따라 서명 생성 및 검증 시간이 달라진다. Table 4.는 ECDSA secp256k1(Intel Core i7 4790K @ 4.0GHz)의 서명/검증 시간이 나타나 있다. Table 5.에는 양자 내성 전자서명의 서명 및 검증 시간이 정리되어 있다. 해시 기반 전자서명 SPHINCS$^+$-SHA256 (3.5 GHz Intel Core i7-4770K CPU)[18], XMSS-SHA-256 (Intel Core i5 CPU M540 @ 2.53GHz) [19], 아이소제니 기반 Supersingular isogeny 전자서명 스킴 (Intel Xeon E5-2637 v3 3.5 GHz,)[20], 격자 기반은 pqNTRUSign[21]을 비교한다. 각 알고리즘 연산을 수행한 머신의 성능을 괄호 안에 표기하였다.

모든 노드는 트랜잭션의 유효성을 판단하기 위해

Table 1. Sizes(bytes) of public key and signature of ECDSA secp256k1 and security strength (bits)[17]

Signature scheme	public key	signature	security strength
ECDSA secp256k1	32	64	128

Table 2. Size (bytes) of public key and signature of PQC and security strength (bits)[18]-[21]

Signature scheme	public key	signature	security strength
SPHINCS$^+$-SHA256 -256s[15]	64	29792	128
XMSS-SHA-256[16]	1696	2083	146
Supersingular isogeny[17]	336	122880	128
pqNTRUSign[18]	2048	1408	128

Table 4. Time of sign and verification of ECDSA secp256k1(μs)[17][23]

Signature	Sign	Verification
ECDSA secp256k1	506	1100

Table 3. Estimated size of Transaction(kb), block(Mb) and chain(Tb) size for each signature scheme

scheme	Transaction size (kb)	Block size (Mb)	Chain size (Tb)
SPHINCS+-SHA256-256s[18]	313.377	845.568	466.219
XMSS-SHA-256[19]	39.665	107.027	59.011
Supersingular isogeny[20]	1,293.311	3,489.667	1,924.090
pqNTRUSign[21]	36.275	97.879	53.967

Table 5. Time of sign and verification of PQC(μs) [18]-[21]

Signature	Sign	Verification
SPHINCS$^+$-SHA 256-256s[15]	12893347756	19141296
XMSS-SHA-256 [16]	15170	1020
Supersingular isogeny[17]	28776	19679
pqNTRUSign[18]	120000	960

전송받는 모든 트랜잭션의 서명 검증을 수행한다. 때문에 긴 서명 검증시간을 갖는 전자서명 스킴은 지양하는 것을 권고한다.

3.2 개념 및 기호

본 논문은 제안 메커니즘을 설명하기 위해 다음과 같은 개념과 기호를 사용하며, 블록과 트랜잭션의 구조를 단순화하여 표현한다.

블록: Table 6.은 블록 구조를 표현한 예제이며, 본 논문은 다음 구조를 기본 블록 구조로 따른다.

메인체인: 노드들이 합의를 통해 유효한 것으로 여기는 가장 긴 체인을 메인체인(mainchain)이라 부른다.

팁: 메인체인의 가장 끝단에 있는 블록을 팁(tip)이라 부른다.

Table 6. Block structure

```
BlockStructure:=
  Block := SEQUENCE{
  header          BlockHeader,
  transaction     SEQUENCE OF TX
                          }

    BlockHeader := SEQUENCE{
    prevBhash     BYTE STRING(SIZE(HashSizes)),
    difficulty    REAL (1..MAX),
    nonce         INTEGER (0..MAX)
                                }

    TX := SEQUENCE {
    pubS        BYTE STRING,
    sigS        BYTE STRING,
    pubR        BYTE STRING,
    amount      INTEGER (0..MAX)
                          }

  HashSizes := INTEGER (32)
END
```

트랜잭션: 트랜잭션은 TX 로 나타낸다. 코인을 사용하기 위해 발신자는 이전에 받은 코인 전송 내역을 담은 트랜잭션을 호출하는 경우가 있으며, 그럴 경우 호출되는 트랜잭션은 Pr$evTX$ 로 나타낸다.

공개키 개인키 쌍: 본 논문에서는 발신자(Sender)의 키쌍을 나타내기 위해 pub_s,$priv_s$ 로 표기하며, 수신자(recipient)의 키쌍은 pub_r, $priv_r$ 로 표기한다.

금액: 트랜잭션에서 발신자가 받는 코인 금액의 양을 $amount$ 라 부른다.

해시함수: 해시함수를 수행하는 함수식 $H(x)=h$ 이며 임의의 유한 비트 길이의 입력 x에서 고정된 비트 길이의 해시값 h를 출력으로 맵핑한다.
해시함수는 (a)preimage resistance, (b) 2nd-preimage resistance, (c) collision resistance, 세가지 속성을 만족해야 안전하다고 볼 수 있다.

서명: 트랜잭션에는 일반적으로 발신자의 서명이 포함된다. 본 논문에서는 발신자의 서명 σ_s에 들어가는 요소를 하단의 요소와 같이 축약하며, 식 (4)를 통해 만들어진다.

$$\sigma_s = Sign_{priv_s}(H(\mathrm{Pr}evTX), pub_r, amount) \quad (4)$$

사용하려는 코인의 수신 내역이 담긴 이전 트랜잭션의 해시값 $H(\mathrm{Pr}evTX)$을 참조를 위해 넣고, 수신자의 공개키 pub_r, 금액 $amount$를 발신자의 개인키 $priv_s$로 서명한다. 이를 통해 서명 σ_s을 도출한다.

서명검증: (10)은 서명을 검증하는 함수식이다. 서명 σ은 노드의 공개키 pub를 이용하여 유효성을 검증할 수 있다.

$$v = Verify(\sigma, pub), v \in \{0,1\} \quad (5)$$

노드의 공개키 pub와 서명 σ을 검증하면 검증값 v가 나오며, 검증값 0은 true를 1은 false를 의미한다. 즉 $v=0$이면, 트랜잭션은 유효하다.

보안 파라미터: 트랜잭션이 블록에 포함되면, 그 트랜잭션은 승인(confirmed)받았다고 말한다. 또한 트랜잭션이 포함된 블록에 뒤이어 블록이 더해지면, 더해진 블록 수만큼 승인 횟수(Confirmation Number)가 증가한다. 승인 횟수가 증가할수록 트

랜잭션이 조작될 가능성은 낮아지며, 승인 횟수가 k번 이상일 때 트랜잭션의 상태(status)는 안정적(stable)이라고 표현한다. 이 때 k는 보안 파라미터이다. 승인횟수는 트랜잭션이 포함된 블록의 높이에 따라 달라지고, 보안 파라미터 k는 고정 상수로, 개발자/운영자가 설정할 수 있다.

$$\begin{cases} Confirmation < k, & TX.status = 1 \\ Confirmation \geq k, & TX.status = 0 \end{cases} \quad (6)$$

트랜잭션의 승인횟수가 k보다 작으면, 트랜잭션의 상태는 불안정적(unstable)이며 1로 표현된다. 트랜잭션의 승인횟수가 k 이상일 시, 트랜잭션의 상태는 안정적이며 0으로 표현된다.

고정블록 / 비고정블록: 블록 내에 포함된 모든 TX가 안정적인(stable) 상태를 가질 시, 해당 블록을 고정 블록(fixed block)이라 칭한다. 즉, 고정블록은 메인체인의 팁에서 k 블록 이상 떨어진 블록을 말한다.

또한 메인체인의 팁에서 k 미만으로 떨어진 블록은 비고정 블록(unfixed block)이라 불리며 비고정 블록에 포함되는 TX는 불안정적(unstable)이다. Fig. 4.은 메인체인에서의 고정 블록과 비고정 블록을 나타낸 그림이다.

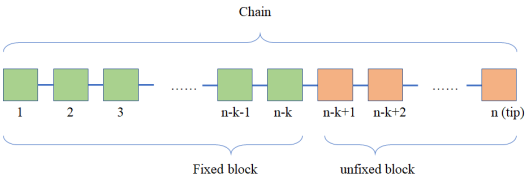


Fig. 4. Fixed block and unfixed block

IV. 전자서명 호환성을 증대하기 위한 제안

4.1 새로운 트랜잭션 구조 및 합의 메커니즘 제안

본 절에서는 양자 내성 전자서명 적용을 위한 새로운 트랜잭션 구조 및 합의 메커니즘을 제안한다. 기존 트랜잭션의 구조를 단순화하면 발신자의 서명과 공개키 쌍, 수신자의 공개키, 송금금액으로 이루어진다. 기존 트랜잭션의 구성요소는 크게 2종류로 나뉜다. 사용하려는 금액의 소유권 증명을 위한 발신자의 서명 σ_s, 공개키 pub_s가 있고, 금액의 수신자에 대한 정보로 수신자의 공개키 pub_r, 받는 금액의 양 $amount$가 기록된다. 이때 서명은 이전 트랜잭션의 해시값과, 수신자의 공개키, 금액을 서명한 값이다. Table 6.에 기존 트랜잭션 구조가 기술됐다.

그러나 기존 구조에 양자 내성 암호를 그대로 적용한다면 3.1절에 기술된 바와 같이 트랜잭션의 크기가 비대해질 수 있다. 따라서 발신자의 서명과 수신자의 공개키를 해시한 값과 금액으로 이루어진 트랜잭션을 제안하여 공개키/서명 크기를 줄이고자 한다. 제안 트랜잭션은 발신자의 서명 σ_s의 해시값, 수신자의 공개키 pub_r의 해시값과 받는 금액의 양 $amount$만으로 이루어진다. 발신자의 공개키 pub_s는 트랜잭션에서 제거되고, 서명 해시값은 서명 확인 용도로, 공개키 해시값, 금액은 수신자에 대한 정보로 저장된다.

서명 검증에는 공개키/서명 쌍이 필요하기 때문에, $\{pub_s, \sigma_s\}$를 같이 전송하여 검증에 이용하고, 일정 기간이 지난 뒤에는 $\{pub_s, \sigma_s\}$를 파기하는 새로운 방식을 제안한다. Table. 7.은 트랜잭션에 대한 정보와 제안 트랜잭션 구조를 나타내는 예제이다. 트랜잭션에 대한 정보 $TXinfo$에는 트랜잭션 데이터 그 자체와 트랜잭션의 해시값, 검증결과, 트랜잭션이

Table. 7. Proposed transaction structure

```
NewTXStructure::=
  TXinfo ::= SEQUENCE{
  txdata          TX,
  hashvalue       BYTE STRING (SIZE(HashSizes)),
  v               BOOLEAN,
  height          INTEGER (0..MAX),
  pubS            BYTE STRING,
  sigS            BYTE STRING,
  pubR            BYTE STRING,
  status          ENUMERATED {stable(0),
                  unstable(1)} DEFAULT unstable
                        }

    TX ::= SEQUENCE {
    sigSHash        BYTE STRING
                    (SIZE(HashSizes)),
    pubRHash        BYTE STRING
                    (SIZE(HashSizes)),
    amount          INTEGER (0..MAX)
                        }

  HashSizes ::= INTEGER (48)
END
```

포함되는 블록의 높이, 발신자의 공개키와 서명, 수신처를 확인하기 위한 수신자의 공개키, 그리고 트랜잭션이 안정적인지(stable) 불안정적인지(unstable)를 나타내는 상태 필드(stauts)가 있다. 이 트랜잭션 정보는 승인되지 않은 거래 풀(Unconfirmed Transaction Pool)에서 보관된다. 이때, 해시 함수에 그로버 알고리즘과 생일 공격을 접목하여 수행하면 비도가 $O(\sqrt{N})$이 아닌 $O(\sqrt[3]{N})$으로 낮아진다. 따라서 해시함수의 길이를 늘려 같은 안정성을 유지하고자 한다[24].

트랜잭션은 Fig 5.과 같은 방식으로 생성되고 전파된다.

거래 생성 알고리즘의 인풋은 서명과 검증에 쓰이는 발신자의 키쌍 $pub_s, priv_s$, 수신자의 공개키 pub_r와 받는 금액 $amount$, 코인을 사용하기 위해 참조하는 이전 TX의 해시 $H(\mathrm{Pre}vTX)$이고, 아웃풋은 트랜잭션 TX를 포함한 트랜잭션에 대한 데이터인 $TXinfo$가 된다. 우선 수신자 공개키의 해시값과 금액을 TX에 넣는다①②. 서명 함수를 불러와③ 이전 트랜잭션의 해시값, 수신자의 공개키, 받는 금액을 발신자의 개인키로 서명하여, 서명값 σ_s의 해시값을 생성하여 트랜잭션에 입력한다④⑤. 이렇게 ①~⑤에 걸쳐 트랜잭션 TX를 생성한다. 트랜잭션에 대한 부가 정보까지 포함하는 $TXinfo$ 에 TX를 넣고⑥, 검증을 위한 정보 $\{pub_s, \sigma_s\}$를 첨부한다⑦⑧. 수신자 확인하기 위한 pub_r을 첨부하고⑨, 트랜잭션의 해시값을 추가한다⑩. 이렇게 만들어진 정보 $TXinfo$는 승인되지 않은 거래 풀에 추가되며, 노드는 정보를 전파한다.

트랜잭션에 대한 정보는 상태가 안정적으로 변할 때까지 승인되지 않은 거래 풀에 보관되다가, 상태가 변하면 거래풀에서 제거되고 그에 따라 서명 쌍 $\{pub_s, \sigma_s\}$을 포함한 $TXinfo$가 소거된다.

트랜잭션의 상태를 파악하기 위해 풀은 주기적으로 업데이트 되어야 한다. Fig 6.은 전파된 트랜잭션을 검증을 거쳐 받아들이고 안정적인 트랜잭션을 풀에서 제거하는 기능을 수행한다.

프로토콜의 인풋으로는 $TXinfo$와 TX, 트랜잭션의 상태를 확인하기 위해 필요한 보안 파라미터 k, 메인체인의 팁 높이 n이 있다. 아웃풋으로는 트랜잭션의 검증 결과인 v와 트랜잭션의 상태를 나타내는 $status$가 업데이트되어 $TXinfo$가 나온다. 우선 트랜잭션에 대한 검증을 수행하기 위해 트랜잭션에 기록된 수신자의 서명과 발신자의 공개키가 적절한지 확인한다. TX의 서명 해시값이 $TXinfo$의 서명 해시값과 동일하지 않은 경우, TX의 공개키 해시값이 $TXinfo$의 공개키 해시값과 동일하지 않은 경우, 프로토콜을 종료한다①. 서명 검증 함수를 불러와 트랜잭션 정보에 있는 발신자의 서명과 공개키를 넣고 ②~④, 검증값을 트랜잭션 정보에 다시 추가한다⑤⑥. 검증값이 유효하지 않은 경우에는 프로토콜을 종료하고⑦ 유효한 경우에만 트랜잭션 정보를 풀에 추

Transaction creation algorithm

Input: pub_s, $priv_s$, pub_r, amount, H(PrevTX)
Output: TX(TXinfo.txdata), TXinfo
1: TX.pubRHash ← H(pub_r)
2: TX.amount ← amount
3: CALL Sign()
4: σ_s ← $Sign_{privs}$(H(PrevTX), pub_r, Amount)
5: TX.sigSHash ← H(σ_s)
6: TXinfo.txdata ← TX
7: TXinfo.pubS ← pub_s
8: TXinfo.sigS ← σ_s
9: TXinfo.pubR ← pub_r
10: TXinfo.hashvalue ← H(TX)

Fig. 5. Proposed transaction creation protocol

Pool update protocol

Input: TXinfo, TX(TXinfo.txdata), k, n /*n stands for block heigh of tip*/
Output: TXinfo
1: IF (TX.sigSHash ≠ H(TXinfo.sigS) or TX.pubRHash ≠ H(TXinfo.pubR)) THEN Return false
2: CALL Verify()
3: σ ← TXinfo.sigS
4: pub ← TXinfo.pubS
5: υ ← Verify(σ, pub)
6: TXinfo.v ← υ
7: IF (TXinfo.v = 1) THEN Return false
8: Pool ← TXinfo //Pool is unconfired transanction pool
9: FOR (TXinfo in Pool that TXinfo.height ≤ n - k) DO
10: TXinfo.status ← 0

Fig. 6. Proposed pool update protocol

가한다⑧. 또한 풀에서 트랜잭션이 담긴 블록의 높이가 $n-k$보다 낮아져 고정 블록에 포함되는 경우⑨ 트랜잭션의 상태를 안정적(stable)으로 변경한다⑩. 추후 상태가 안정적인 $TXinfo$는 승인되지 않은 거래 풀에서 제거한다.

제안된 트랜잭션 구조와 검증 방식을 도입할 시, 비고정 블록에 대해서 트랜잭션 검증에 필요한 발신자의 공개키와 서명 쌍을 첨부하기 때문에 기존 방식(e.g. P2PKH)과 동일하게 블록 검증할 수 있다.

고정 블록을 전송받을 시에는 블록과 블록 헤더에 대한 검증을 수행하여 블록의 유효성을 확인한다. 다음 Fig 7.은 고정 블록 $Block$에 대한 검증 프로토콜 예제이다.

우선 현재 블록헤더의 이전 블록 해시가 실제 이전 블록의 해시와 일치하는지 확인하고 일치하지 않는 경우 false값을 반환한다①. 생성된 블록의 PoW가 제대로 수행되었는지 확인하기 위해 블록의 해시값이 기존에 설정되어 있는 타겟 난이도보다 작게 나왔는지 확인하고 그렇지 않은 경우 false값을 반환한다②. 이렇게 블록에 대한 검증을 수행하며, 검증이 참인 경우에만③ 블록을 추가한다.

Fig. 7. Proposed verification protocol for fixed block

Verification protocol for fixed block
Input: Block, BlockHeader(Block.header) B_{n-1} //B_{n-1} stands for previous block of the Block Output: Bool 1: IF H(B_{n-1}) ≠ BlockHeader.prevBhash THEN Return false 2: IF (H(Block) 〉 BlockHeader.difficulty) THEN Return false 3: Return true

4.2 보안성 검토

본 절에서는 제안 메커니즘이 이전 블록체인과 마찬가지로 체인 구조를 통해 각 블록의 무결성을 보장하고, PoW를 통해 공격자의 변조된 블록을 받아들이기 어렵게 하는 특성이 유지되는지 검토한다. 검토를 위해 [3]의 51% 공격 방식을 차용하여 2가지 공격 시나리오를 상정한다. 중간에 조작된 블록을 삽입하는 공격 시나리오를 통해 제안 메커니즘에서 블록체인의 무결성이 유지되는지 검토하고, 조작된 블록을 이어 메인체인을 탈취하는 공격 시나리오를 통해 PoW의 보안성이 유지되는지 검토한다.

제안 메커니즘 상 악의적인 사용자가 메인체인의 팁 높이에서 z만큼 떨어진 체인 C 에 이어 조작된 블록을 작성하여 불법적인 자산 탈취를 시도한다고 가정해보자. 조작된 블록이 포함된 체인 C'에 블록을 덧대어 메인체인으로 만들기 위해서는 고정 블록과 비고정 블록에 대해 다음과 같은 조건을 만족하여야 한다. 이때 각 블록은 B_i로 나타내며, i는 해당 블록의 높이를 의미한다. x는 공격자의 체인 C 의 블록 수, k 는 보안 파라미터를 의미한다.

① 고정 블록 B_i 에 대해서는 수식 (7)를 충족해야 노드들이 블록을 받아들인다.

$$\begin{aligned} &For\, B_i,\, Where\, i \le x+z-k \\ &H(B_{i-1}) = BlockHeader.prevBhash \\ &H(B_i) < target difficulty \end{aligned} \tag{7}$$

② 비고정 블록 B_i 에 대해서는 수식 (8)을 충족해야 노드들이 블록을 받아들인다.

$$\begin{aligned} &For\, B_i,\, Where\, x+z-k < i \le x+z \\ &H(B_{i-1}) = BlockHeader.prevBhash \\ &H(B_i) < target difficulty \\ &For\, TX \in B_i,\, TXinfo.v = 0 \\ &TX.sigSHash = H(TXinfo.sigS) \\ &TX.pubRHash = H(TXinfo.pubR) \end{aligned} \tag{8}$$

위 조건에 따라 공격 시나리오 a), b)를 검토한다.

a) 중간에 조작된 블록을 삽입하는 공격

체인 C 중간에 조작된 블록 B_i'를 삽입하고 뒤이어 기존의 체인을 덧붙인다고 하면, 블록 B_{i+1}에 대해

$$H(B_i') = BlockHeader.prevBhash \tag{9}$$

가 만족해야 한다. 이는

$$\begin{aligned} &B_i \neq B_i' \\ &H(B_i) = H(B_i') \end{aligned} \tag{10}$$

를 만족하는 $H(B_i)$의 2^{nd} preimage를 구하는 것과 같으며, 해시함수의 보안성에 위배된다. 고정/비고정블록에 대하여 (10) 조건을 모두 만족해야 하기 때문에 변조된 고정/비고정 블록을 체인 중간에 삽입하는 것이 불가능하다. 따라서 블록체인이 가지는 무결성 특징은 제안 메커니즘에서도 동일하게 유지된다고 볼 수 있다.

b) 조작된 블록 뒤에 블록을 연이어 생성하여 메인체인을 탈취하는 공격

메인체인을 탈취하기 위해서는 공격자가 착한 노드보다 빨리 블록을 생성해야 하고, 합의 알고리즘에 따라 공격 성공률이 좌우된다. 제안 메커니즘은 PoW 합의 알고리즘에 따라 블록을 생성한다. 고정/비고정 블록에 상관없이 생성되는 블록 B_i에 대하여 수식 (11)을 만족해야 하므로

$$H(B_{i-1}) = BlockHeader.prevBhash \\ H(B_i) < target difficulty \quad (11)$$

고정/비고정 블록은 PoW를 따라 합의된다고 볼 수 있다. PoW에서 공격자가 z블록만큼 떨어진 체인을 따라잡는 확률은 수식 (3)과 같다[3].

이때 성공 확률은 착한 노드가 다음 블록을 발견할 확률 p, 공격자가 다음 블록을 발견할 확률 q, 따라잡아야 하는 블록 수 z에 따라 달라진다. 블록 생성 확률은 공격자와 착한 노드의 해시율과 높은 상관성을 가지며 제안 메커니즘은 이에 영향을 끼치지 않는다. 그리고 따라잡아야 하는 블록 수 z는 트랜잭션이 안정적으로 변하여 사용가능해지는 기준이 되는 보안 파라미터 k와 동일하며, 제안 메커니즘에서 k는 독립 상수로 제안 메커니즘에 따라 변경되지 않는다. 그러므로 제안 메커니즘은 PoW에 따라 블록을 생성하며, 제안 메커니즘에서의 공격 b)가 성공할 확률은 기존의 51% 공격 확률과 동일하다.

따라서 제안된 메커니즘에서는 기존의 블록체인과 PoW가 갖는 고유의 보안성을 크게 해치지 않는다.

V. 구현 및 성능

5.1 구현

구현된 양자 내성 블록체인(이하 BPQB)은 비트코인 오픈소스인 bitcoin core version 0.15.1을 기반으로 개발/구현하였다. Bitcoin core는 정해진 블록크기, 스마트 컨트랜트 실행 불가 등 한계가 많은 대표적인 블록체인이다. Bitcoin core는 블록체인이 갖고 있는 한계성을 잘 나타내기 때문에 향후 양자 내성 암호를 도입하기 위해 개선해야할 부분들에 대해 연구하기 적합한 것으로 판단하고 이를 기반 소스로 선정한다.

또한 양자 내성 알고리즘은 격자 기반의 pqNTRUSign 전자서명 알고리즘[21]을 적용한다. pqNTRUSign은 모듈러 격자 기반의 전자서명 스킴으로 가우시안 샘플러(Gaussian sampler) 또는 유니폼 샘플러(uniform sampler)와 함께 NTRU 래티스를 사용한다[21]. pqNTRUSign은 공개키/서명 크기가 다른 암호 알고리즘에 비해 작은 편에 속해, 각 노드가 부담할 승인되지 않은 트랜잭션 풀의 용량을 최소화할 수 있을 것이다. 모든 노드가 서명 검증을 통해 트랜잭션을 전송받는 것을 고려할 때, 서명 검증 시간이 다른 암호 알고리즘에 비해 짧은 편이여서, 검증 속도가 실용적인 블록체인을 구현하는 데에 적절할 것으로 판단했다. 자세한 개발 환경은 Table 8.와 같다.

BPQB는 4.1절의 합의메커니즘을 적용한다. 또한 키관리 방식으로 HD wallet 방식(계층 결정적 지갑, hierarchical deterministic wallet)을 적용한다. 이 방식은 단일 시드(seed)로부터 많은 키를 생성하여 트리 구조를 형성하는 방식으로, 한 개의 개인키로 수많은 공개키를 가질 수 있기 때문에 백업, 복원이 간편하여 사용자 편의성을 증대할 수 있다. HD wallet을 pqNTRUSign 스킴에 적용하는 경우, 서명시간이 늘어나는 단점이 있다. ECDSA 스킴에서는 개인키가 난수이기 때문에 쉽게 키를 복원할 수 있어 서명시간이 길어지지 않으나

Table 8. Underlying software for the Bitcoin-based Post-Quantum Blockchain(BPQB)

Item	Software	Version
Blockchain source	Bitcoin Core	version 0.15.1
Item	Software	Parameter
Post-quantum digital signature	pqNTRUSign [21]	EESS1v1-pqNTRUSign-Parameters
Item	Software	Version
Development environment	Visual Studio 2017	version 15.8.9

pqNTRUSign 스킴은 개인키를 복원하는데 연산을 추가적으로 수행해야 하는 경우가 발생하여 서명시간이 다소 늘어나는 경향이 있다.

5.2 성능

BPQB의 성능을 측정하고자, 2개의 PC 실험환경에서 서명과 검증 시간을 각 50회 측정했다. 각 실험 환경은 Table 9.와 같다.

각 실험환경에서의 평균 서명 및 검증 시간과 표준편차는 Table 10.과 같으며, 평균 서명 생성 시간은 602,749.6 μs, 서명 검증 시간은 3,529.37 μs이다. 또한 기존의 비트코인 블록체인과의 비교를 위해 bitcoin core version 0.15.1(이하 bitcoin 0.15.1)에서의 서명 시간과 검증 시간을 측정했다. 실험환경과 측정방식은 동일하며 평균 서명 및 검증 시간과 표준편차를 Table 11.과 같다. 평균 서명 생성 시간은 약 401.25 μs이고, 서명 검증 시간은 46.87 μs이다.

블록체인은 트랜잭션 유효성 확인을 위해 전파되는 모든 트랜잭션의 서명 검증을 수행한다. 때문에 성능 부문에 있어 가장 중요한 요소는 검증 시간이 된다. Table 10.을 살펴보면, bitcoin 0.15.1이 BPQB보다 빠르나, BPQB의 평균값은 μs로 10,000 μs이하의 값이기 때문에 실용적으로 사용할 수 있을 것이다. 서명 시간은 BPQB는 약 602,749 μs이고, bitcoin 0.15.1은 약 46 μs로 현저한 차이를 보이나 이는 개인이 트랜잭션을 생성하는 시간에만 영향을 주기 때문에 실용적인 사용에 있어 큰 무리가 없을 것으로 판단된다.

BPQB는 양자 내성 전자서명을 위해 최적화가 되지 않은 상태이다. pqNTRUSign 명세서에서는 서명 및 검증 시간을 각각 120,000μs / 960μs로 기술하고 있기 때문에[21] 최적화를 통한 시간 단축이 가능할 것으로 예상된다.

Table 9. Experiments environments

	Environment 1	Environment 2
OS	Microsoft Windows 10 Pro	Microsoft Windows 10 Home
Processor	Intel(R) Core(TM) i7-4500U CPU 1.80GHz, 2401Mhz, 4 core, 8 logical processor	Intel(R) Core(TM) i5-4590 CPU 1.60GHz, 1800Mhz, 4 core, 8 logical processor
RAM	8.00GB	16.00GB

VI. 결 론

본 논문은 양자 내성 암호를 블록체인에 도입하기 위한 새로운 트랜잭션 구조를 제안하며, 이를 구현한 양자 내성 블록체인을 기술한다. 새로운 트랜잭션은 발신자의 서명과 수신자의 공개키 대신 그의 해시값을 가지는 구조로 변경한다. 그에 따라 검증 과정도, 변경 가능성이 높은 비고정 블록, 변경 가능성이 적은 고정 블록을 구별하여, 비고정 블록 내의 트랜잭션은 공개키, 서명 쌍을 같이 배포하여 트랜잭션을 검증하고, 고정 블록은 거래 검증을 제외한 블록 검증을 통해 받아들이는 메커니즘으로 변경한다. 제안 메커니즘이 블록체인의 무결성과 PoW 합의 알고리즘이 갖는 고유의 보안성을 해치지 않는다는 것을 검토한다. 또한 비트코인 오픈소스 블록체인을 기반으로 격자 기반의 pqNTRUSign[21]을 적용한 양자

Table 10. The results of the experiments (μs)

	Environment	bitcoin 0.15.1 (ECDSA)		BPQB (pqNTRUSign)	
		Average	standard deviation	Average	standard deviation
Sign	1	563.2	241.734000	771,219.00	712,837.40000
	2	239.30	61.636110	434,280.20	293,570.90000
	avg.	**401.25**	**151.685055**	**602,749.60**	**503,204.15000**
Verification	1	53.32	21.613370	4,486.62	3,095.39100
	2	40.42	21.044800	2,572.12	465.83570
	avg.	**46.87**	**21.329085**	**3,529.37**	**1,780.61335**

내성 블록체인을 개발/구현한다. 양자 내성 블록체인의 평균 서명 생성 시간은 602,749.6 μs이고, 서명 검증 시간은 3,529.37 μs로 측정되었다. 모든 노드는 비고정 블록 내의 트랜잭션의 서명 검증을 실시하기 때문에 검증시간이 중요하며 측정 결과 10,000 μs이하로 실용적인 사용에 있어 큰 무리가 없을 것으로 예상된다.

새로운 트랜잭션 구조를 통해 비대한 키 크기, 서명크기를 가진 양자 내성 암호이더라도 블록체인에 적용할 것을 고려할 수 있고, 궁극적으로 블록체인의 양자 내성 암호에 대한 호환성을 증대시킨다는 의의를 가지며 블록체인의 크기가 일정 이상 비대해지는 것을 방지할 수 있을 것으로 사료된다.

그러나 제안된 방식은 블록체인을 대신해 승인되지 않은 트랜잭션 풀과 네트워크에서 키를 일시적으로 보관해야 하므로 부하를 줄 수 있어, 메모리 풀, 네트워크에 대한 공격과 승인되지 않은 풀에서 발생할 수 있는 추가 연산에 대한 검토가 필요하다.

References

〔1〕 Y. Gao, X. Chen, Y. Chen, Y. Sun, X. Niu and Y. Yang, "A Secure Cryptocurrency Scheme Based on Post-Quantum Blockchain," in IEEE Access, vol. 6, pp. 27205-27213, Apr. 2018.

〔2〕 K. Yoon, J.Y. Lee, S. Kim, J. Kwon, Y. Park, "An Implementation of Supersingular Isogeny Diffie-Hellman and Its Application to Mobile Security Product," *Journal of The Korea Institute of Information Security & Cryptology*, 28(1), pp. 73-83, Feb. 2018.

〔3〕 S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," *bitcoin.org.*, Oct. 2008. 〔Online〕. Available: https://bitcoin.org/bitcoin.pdf. 〔Accessed Dec. 14, 2018〕

〔4〕 A.W.F. Edwards, "Pascal's Problem: The 'Gambler's Ruin," *International Statistical Review/ Revue Internationale de Statistique*, vol.51, no. 1, pp. 73-79, Apr. 1983.

〔5〕 R. E. Walpole, R. H. Myers, S. L. Myers, and K. Ye, *Probability & Statistics for Engineers & Scientists*. Prentice Hall, 9th edition, 2012.

〔6〕 M. Rosenfeld, "Analysis of hashrate-based double-spending," *ArXiv.org*, arXiv:1402.2009, Feb. 2014, 〔Online〕 Available: https://arxiv.org/abs/1402.2009. 〔Accessed Apr. 12, 2019〕

〔7〕 BITNODES.COM, "Dashboard: NODES," 〔Online〕 Available: https://bitnodes.earn.com/dashboard/?days=730. 〔Accessed Apr. 15, 2019〕

〔8〕 Blockchain.com, "charts/hash-rate," 〔Online〕 Available: https://www.blockchain.com/charts/hash-rate?timespan=2years&showDataPoints=true. 〔Accessed Apr. 15, 2019〕

〔9〕 "R3 publishes a new post-quantum signature algorithm tailored to blockchains," *Medium,* Aug. 10, 2018. 〔Online〕, Available: https://medium.com/corda/r3-publishes-a-new-post-quantum-signature-algorithm-tailored-to-blockchains-51719c64fd4c, 〔Accessed Mar, 21, 2019〕.

〔10〕 *QRL*, "FAQ: What is QRL?" 〔Online〕, Available: https://theqrl.org/faq/what/, 〔Accessed Mar, 21, 2019〕.

〔11〕 K. Chalkias, J. Brown, M. Hearn, T. Lillehagen, I. Nitto, T. Schroeter, "Blochcained Post-Quantum Signatures," *IACR Cryptology ePrint Archive,* pp. 1196-1203. Jul. 2018

〔12〕 E.O. Kiktenko, N.O. Pozhar, M.N. Anufriev, A.S. Trushechkin, R.R. Yunusov, Y.V. Kurochkin, A.I. Lvovsky, and A.K. Fedorov, "Quantum-secured blockchain," *Quantum Science and Technology,* vol. 3, no.3, pp.035004, May. 2018.

〔13〕 B. Bae, "Hash-based signature scheme for blockchain," M.S. thesis,

Pusan National University, Aug. 2017.

〔14〕 S. Yu, "Stateprune :reduce blockchain size by chainstate based block pruning," M.S. thesis, Korea University, Aug. 2017.

〔15〕 R.C. Nana Mbinkeu, B. Batchakui, "Reducing Disk Storage with SQLite into BitCoin Architecture," *International Journal of Recent Contributions from Engineering, Science & IT (iJES)*, vol.3, No.2, pp.10-14, May. 2015.

〔16〕 J.D. Brue, "The Mini-Blockchain Scheme," Cryptonite.info, Jul. 2017 〔Online〕. Available: http://cryptonite.info/files/mbc-scheme-rev3.pdf 〔Accessed Jan. 13, 2020〕

〔17〕 Certicom Research, "SEC 2: Recommended Elliptic Curve Domain Parameters, v1.0.," Standards for Efficient Cryptography Group, pp. 1-51, Sep. 2000.

〔18〕 D. J. Bernstein, C. Dobraunig, M. Eichlseder, S. Fluhrer, S. Gazdag, A. Hülsing, P. Kampanakis, S. Kölbl, T. Lange, M. M. Lauridsen, F. Mendel, R. Niederhagen, C. Rechberger, J. Rijneveld, P. Schwabe, "SPHINCS$^+$," *National Institute of Standards and Technology,* pp. 1-55, Nov. 2017

〔19〕 J. Buchmann, E. Dahmen, A. Hülsing, "XMSS- A Practical Forward Secure Signature Scheme based on Minimal Security Assumption," In Proc. 4th International Conference on Post-Quantum Cryptography (PQCrypto 2011) - Taipei, Taiwan, pp.117-129, Nov. 2011

〔20〕 Y. Yoo, R. Azarderakhsh, A. Jalali, D. Jao, V. Soukharev, "A Post-quantum Digital Signature Scheme Based on Supersingular Isogenies." Financial Cryptography and Data Security, pp.163-181, Jan. 2017.

〔21〕 C. Chen, J. Hoffstein, W. Whyte, Z. Zhang, "NIST PQ Submission: pqNTRUSign A modular lattic signature scheme," *National Institute of Standards and Technology,* pp. 1-17, Aug. 2017, 〔Online〕. Available: https://www.onboardsecurity.com/nist-post-quantum-crypto-submission. 〔Accessed: Dec 14, 2018〕

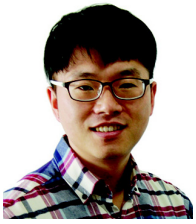
〔22〕 Blockchain.com, "charts," 〔Online〕 Available: https://www.blockchain.com/charts. 〔Accessed Apr. 15, 2019〕

〔23〕 Warner/python-ecdsa, "Pure-Python ECDSA: release 0.15," 〔Online〕, Available: https://github.com/warner/python-ecdsa 〔Accessed Jan. 13, 2020〕

〔24〕 V. Mavroeidis, K. Vishi, M.D. Zych, A. Jøsang, "The Impact of Quantum Computing on Present Cryptography," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol.9, no.3, pp. 405-414, Mar. 2018.

〈저자소개〉

김 미 연 (Mee Yeon Kim) 정회원
2019년 2월: 순천향대학교 융합서비스보안학과 공학석사
2019년 3월~현재: 엔에스에이치씨 레드알러트팀 사원
〈관심분야〉 정보보호, 블록체인



이 준 영 (Jun Yeong Lee) 정회원
2008년 2월: 명지대학교 컴퓨터소프트웨어학과 공학사
2017년 2월: 세종사이버대학교 정보보호학과 공학석사
2008년 3월~현재: 엔에스에이치씨 암호기술연구소 책임연구원
〈관심분야〉 암호구현, 정보보호, 블록체인

윤 기 순 (Kisoon Yoon) 정회원
1998년 8월: 경희대학교 수학과 이학사
2007년 8월: 고려대학교 정보보호학과 공학석사
2013년 11월: Université de Caen 수학과 이학박사
2013년 11월~현재: 엔에스에이치씨 암호기술연구소 소장
〈관심분야〉 정수론, 아벨리언 다양체 응용, 암호학, 정보보호

염 흥 열 (Heung Youl Youm) 종신회원
1981년 2월: 한양대학교 전자공학과 학사
1983년 9월: 한양대학교 대학원 전자공학과 석사
1990년 2월: 한양대학교 대학원 전자공학과 박사
1982년 12월~1990년 9월: 한국전자통신연구원 선임연구원
1990년 9월~현재: 순천향대학교 공과대학 정보보호학과 정교수
2011년 1월~12월: 한국정보보호학회 회장(역), 명예회장(현재)
2007년 3월~현재: 한국인터넷진흥원 ISMS/PIMS 인증위원회 위원장
2009년~2016년: ITU-T SG17 부의장, ITU-T SG17 WP2/WP3 의장
2017년~현재: ITU-T SG17 국제 의장
2016년 5월~현재: 개인정보보호표준포럼 의장
〈관심분야〉 정보보호관리체계, 개인정보보호, IoT 보안, 개인정보영향평가, 암호 프로토콜