석사학위논문

PQ-DPoL: 효율적인 양자 후 블록체인 합의 알고리즘

2024년

한 성 대 학 교 대 학 원

I T 융 합 공 학 과

I T 융 합 공 학 전 공

김 원 웅

석 사 학 위 논 문
지도교수 서화정

PQ-DPoL: 효율적인 양자 후 블록체인 합의 알고리즘

PQ-DPoL: An Efficient Post-Quantum Blockchain Consensus Algorithm

2023년 12월 일

한 성 대 학 교 대 학 원

I T 융 합 공 학 과

I T 융 합 공 학 전 공

김 원 웅

석 사 학 위 논 문
지도교수 서화정

PQ-DPoL: 효율적인 양자 후 블록체인 합의 알고리즘

PQ-DPoL: An Efficient Post-Quantum Blockchain Consensus Algorithm

위 논문을 공학 석사학위 논문으로 제출함

2023년 12월 일

한 성 대 학 교 대 학 원

I T 융 합 공 학 과

I T 융 합 공 학 전 공

김 원 웅

김원웅의 공학 석사학위 논문을 인준함

2023년 12월 일

심사위원장 박 명 서 (인)

심 사 위 원 이 웅 희 (인)

심 사 위 원 서 화 정 (인)

국 문 초 록

PQ-DPoL: 효율적인 양자 후 블록체인 합의 알고리즘

한 성 대 학 교 대 학 원
I T 융 합 공 학 과
I T 융 합 공 학 전 공
김 원 웅

양자 컴퓨터의 발전과 쇼어 알고리즘을 통한 타원 곡선 암호(Elliptic Curve Cryptographic, ECC)의 다항 시간 솔루션은 블록체인 보안에 대한 취약점으로 작용한다. 본 논문은 새로운 합의 알고리즘을 적용한 효율적인 양자 내성 블록체인을 제시한다. 또한 블록체인의 트랜잭션 서명 및 검증 과정에 양자 후 서명 체계를 적용하여 양자 공격에 대한 내성을 보장한다. 구체적으로, NIST 양자 후 암호(Post-Quantum Cryptographic, PQC) 표준에서 선택된 알고리즘 중 하나인 FALCON 서명 체계를 사용한다. 양자 후 서명 체계를 적용함으로써 필연적으로 블록체인이 처리하는 초당 트랜잭션 수(TPS, Transaction Per Second)가 감소하게 된다. 이러한 성능 저하를 완화하기 위하여 행운 증명(Proof-of-Luck, PoL) 매커니즘에 위임 기법을 적용하는 새로운 합의 알고리즘을 제안한다. 본 논문에서는 FALCON의 보안 매개변수를 조절하고 합의 알고리즘의 구성 요소를 조정함으로써 양자 후 시대를 위한 효율적이고 안전한 블록체인을 구축하고자 한다.

【주요어】 보안, 양자 후 암호, 블록체인, 합의 알고리즘, 신뢰 실행 환경

목 차

표 목 차

그 림 목 차

제 1 장 서론

제 1 절 연구 목적

타원 곡선 암호(ECC) 기반 서명 체계는 높은 효율성을 지니고 있어 대다수의 블록체인에서 트랜잭션 서명 및 검증 체계로써 선택되어 사용되고 있다. 그러나 다음 두 가지 요인으로 인해 타원 곡선 암호를 양자 후 암호로 교체하고자 한다.

첫 번째, Shor 알고리즘은 타원 곡선에서 이산 로그 문제를 효과적으로 모델링하며 다항 시간 솔루션을 제공한다.

두 번째, Shor 알고리즘을 실행할 수 있는 양자 컴퓨터가 근 미래에 등장할 것으로 예상되고 있다.

Grover 알고리즘은 해시 함수의 보안에 대해 검색 복잡도를 제곱근으로 감소시켜 해시 암호의 위험 요소로써 작용한다. 그러나 해시 함수의 출력 크기를 증가시킴으로써 양자 보안성을 만족하는 간단한 대책이 존재한다. 또한 Grover 알고리즘에서 필요한 상당한 양의 양자 회로 깊이로 인해 Shor 알고리즘에 비해 공격을 수행하는 것에 어려움이 있다. 이러한 이유로 본 논문에서는 Grover 알고리즘이 아닌 Shor 알고리즘에 의해 발생하는 취약점에 중점을 둔다.

양자 내성 블록체인을 설계하기 위해서는 Shor 알고리즘에 의한 취약점을 해결할 수 있는 서명 체계를 도입하는 것이 중요하다. 그러나, 양자 후 암호는 서명의 크기가 크고 서명 및 검증 속도가 느리다는 문제점은 널리 알려진 사실이다. 따라서, 이러한 문제점은 블록체인의 성능 저하 및 확장성 저하로 연결되고 이는 탈중앙성, 확장성을 중요시하는 블록체인의 특성으로 인해 더욱 주요하게 작용한다.

이러한 특성을 기반으로, 본 논문에서는 양자 후 위임 행운 증명(Post-Quantum Delegated Proof-of-Luck, PQ-DPoL)이라는 효율적이고 양자 공격에 대해 안전성을 지닌 블록체인 합의 알고리즘을 설계한다. 양자 후

위임 행운 증명은 NIST의 양자 후 암호 표준화에서 최근 표준화된 서명 체계 중 하나인 FALCON을 사용한다.

앞서 말했듯 블록체인에서 양자 후 서명 체계를 사용하는 것은 큰 서명 및 키 사이즈로 인해 불가피하게 성능 저하를 유발한다. 따라서 본 논문에서는 이러한 문제에 대처하기 위하여 행운 증명(Proof-of-Luck, PoL) 알고리즘에 위임 기법을 적용함으로써 합의에 참여하는 노드를 줄여 지연 시간을 줄임으로써 성능을 향상시킨다.

제 2 절 연구 기여

본 논문의 기여는 다음과 같다.

1) 양자 후 서명 체계을 활용한 양자 후 블록체인

본 논문에서는 블록체인 구성요소, 대상 장치 및 합의 알고리즘을 신중하게 고려한 후, 양자 후 서명 체계인 FALCON을 채택한다. 이를 통해 양자 공격에 대비하여 블록체인의 양자 보안성을 보장한다.

2) 효율적인 블록체인을 위한 새로운 합의 알고리즘.

본 논문에서는 처음으로 행운 증명과 위임 기법을 결합한 위임 행운 증명(Delegated Proof-of-Luck, DPoL)을 제안한다. 위임 행운 증명은 신뢰 실행 환경(Trusted Execution Environment, TEE)내에서 합의 과정을 간소화하여 블록 생성 속도를 향상시킨다. 위임 행운 증명 알고리즘의 구현을 통해 양자 후 암호 체계를 사용함과 동시에 높은 성능을 달성한다.

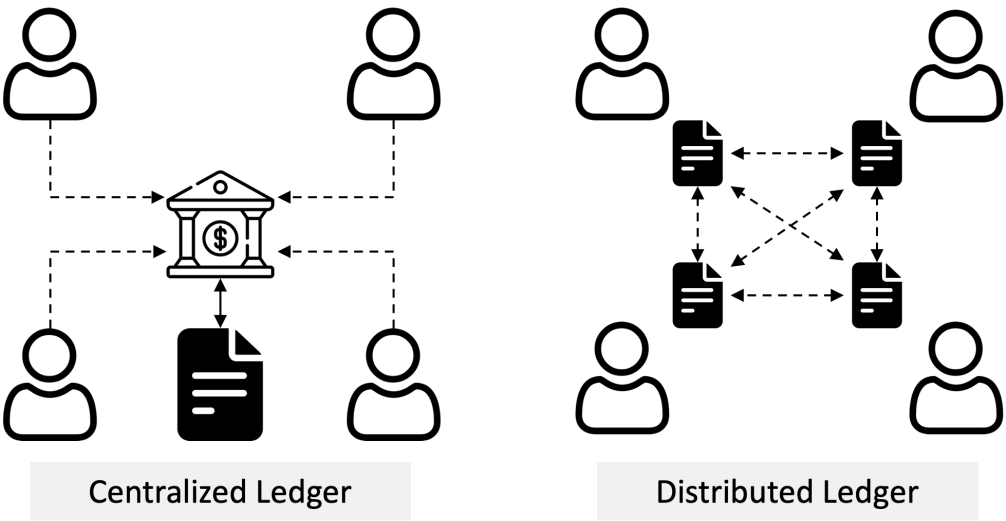
3) 다양한 구성 및 벤치마크.

본 논문에서는 노드 수나 FALCON의 매개변수를 조정하거나, FALCON 외의 양자 후 서명 체계인 CRTYSTALS-Dilithium, SPHINCS+의 보안 매개변수 또한 변경해가며 성능을 측정한 후 벤치마크를 수행한다. 즉 본 논문에서는 다양한 옵션으로 블록체인을 구축하면서 호환성과 최적의 성능을 보장하기 위한 다양한 벤치마크를 제공함으로써 FALCON을 사용하고자 하는 이

유에 대한 타당성을 제공한다.

제 2 장 관련 연구

제 1 절 합의 알고리즘

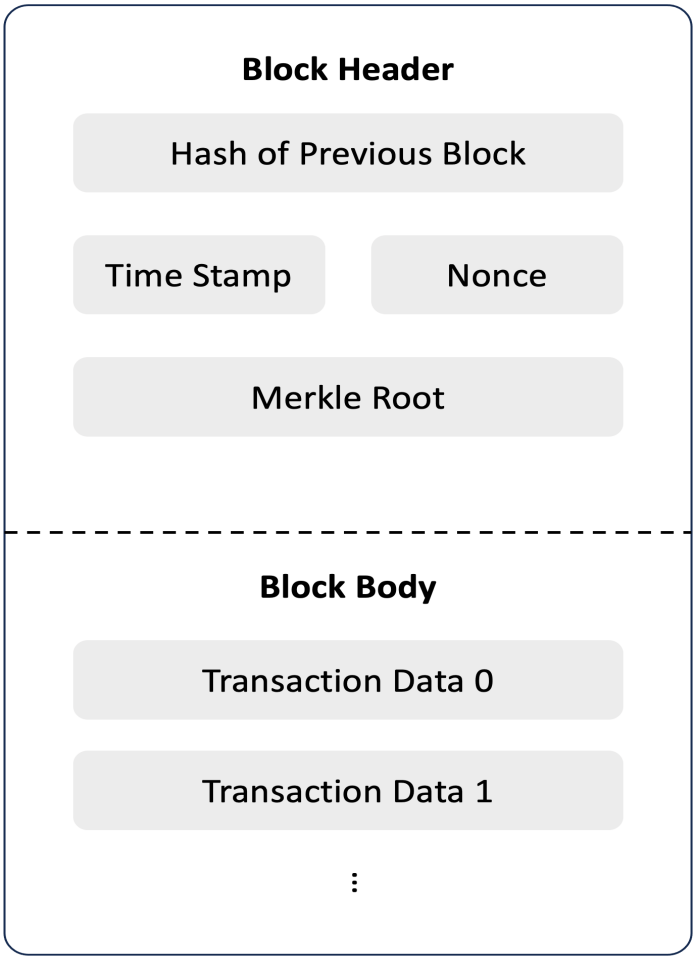


[그림 2-1] Construction of Blockchain Network

[그림 2-1]은 블록체인의 전체적인 네트워크 구조를 나타낸다. 블록체인은 네트워크 내 노드들이 P2P(Peer-to-Peer)로 통신하여 원장을 공유하는 분산 원장 기술이다. 기존의 네트워크 구조는 제 3자가 존재하는 중앙집중식 구조로써, 만약 해당 중앙 기관이 보안 취약점을 가지고 있거나 보안성 또는 가용성을 만족하지 못할 경우 전체 네트워크가 정상적으로 동작하지 못한다. 이러한 문제를 해결하기 위해 블록체인은 각 노드가 원장을 소유하며 제 3자가 존재하지 않는 분산된 구조로 동작한다. 따라서 노드들은 직접 블록을 생성하고 검증하며. 이러한 과정을 위해 합의 알고리즘이라는 특정 프로토콜이 수행된다.

합의 알고리즘은 블록체인의 노드들이 특정 절차를 통해 데이터 무결성을 보장하고 동일한 결정을 내리도록 하는 데 사용된다. 각 합의 알고리즘에는 블록 생성자와 검증자가 존재한다. 블록 생성자는 트랜잭션을 포함한 블록을

생성하고 검증자에게 전송한다. 검증자는 블록의 헤더가 유효한지 확인하고, 블록에 포함된 트랜잭션의 서명을 검증하여 유효성을 확인한다. 합의 알고리즘에는 다양한 종류가 존재한다. 대표적으로 비트코인에서 사용되는 작업 증명(Proof-of-Work, PoW)와 이더리움에서 사용하는 지분 증명(Proof-of-Stake, PoS)가 있다. 또한 지분 증명에 위임 기능을 추가한 위임 지분 증명(Delegated Proof-of-Stake)도 있다. 이외에도 신뢰 실행 환경을 기반으로 하는 행운 증명, 경과 시간 증명(Proof-of-Elapsed-Time, PoET)가 있다.



[그림 2-2] Construction of Block in PoW

[그림 2-2]는 작업 증명에서 사용되는 블록의 구조를 나타낸다. 작업 증명에서는 노드가 블록 생성자가 되기 위해 채굴이라는 일련의 작업 과정을 수행해야 한다. 채굴 과정에서는 nonce라고 하는 무작위 값을 증가시켜가며 해시 함수의 입력 값으로 사용하여 특정 조건을 만족하는 해시 값을 찾는 것을 목표로 한다. 해시 값을 찾은 후 해당 값을 블록의 헤더 내에 포함하여 브로드캐스트 하게 되고, 이를 다른 노드들이 검증을 하게 된다. 검증 시에 해시 값이 조건을 만족하는 것이 확인되면 해당 블록을 블록체인에 추가되고 블록 생성자는 그에 맞는 보상을 얻는다.

그러나 채굴 과정 중 과도한 에너지를 소비한다는 문제점이 존재한다. 이를 해결하기 위해 지분 증명은 충분한 지분을 가진 노드가 블록 생성자가 되도록함으로써 작업 증명의 무의미한 작업 과정을 없앴다. 그러나 지분이 없는 노드는 블록을 생성할 수 없어 부익부빈익빈 문제가 존재한다.

위임 지분 증명은 지분 증명을 기반으로 한 합의 알고리즘이다. 위임 지분 증명에서는 투표를 통해 대표자를 선출하며, 선출된 대표자들끼리 지분 증명을 수행한다. 일부 선출된 위임자들만이 지분 증명을 수행함으로써 초당 트랜잭션 수가 향상되며 부익부빈익빈 문제를 해결할 수 있다. 그러나 대표자 수가 네트워크 규모에 비해 적다면 중앙 집중화 문제가 발생할 수 있다.

경과 시간 증명에서는 무작위로 주어진 대기 시간을 먼저 경과한 노드가 블록 생성자가 된다. 신뢰 실행 환경을 통해 실제로 시간을 경과하였는지 확인하기 때문에 높은 속도 성능으로 검증이 가능하다. 경과 시간 증명은 무작위로 대기 시간을 부여하므로 모든 노드에게 동등한 기회를 제공하며 작업 증명과 같은 컴퓨팅 자원을 소모하는 문제가 존재하지 않다.

제 2 절 블록체인 성능 평가 지표

블록체인은 네트워크 구조 및 합의 알고리즘과 같은 다양한 요소를 가지고 있다. 이로 인해 블록체인의 성능을 단일 지표로 평가하는 것은 바람직하지 않다. 공정한 평가를 위해 블록체인 성능 평가에 대한 다양한 연구가 수행되었다.

[표 2-1] The Importance of Identified Criteria

Performance Evaluation Criteria	Weight(%)
Transactions Per Second (TPS)	8.68
Transaction fees	4.57
51% attack	8.03
Latency	5.29
Governance	4.24
Virtual mining	2.29
Block size	4.18
Routing attack	2.38
Trust model	5.75
Crash Fault Tolerance (CFT)	2.93
Hardware dependency	4.41
Time jacking attack	2.54
Double spending attack	8.85
Number of forks	2.29
Verification time	5.37
Permission model	5.48
Power consumption	7.52
Block withholding	2.87
Mining reward	4.32
Sybil attack	7.99

[표 2-1]은 각 성능 평가 지표의 영향력에 대해서 나타낸다. 주로 사용되는 대표적인 성능 지표로는 초당 트랜잭션 수와 지연 시간이 있다. 두 성능 지표는 각각 8.68%, 5.29%의 영향력으로 매우 높은 수치를 보여준다. 또한 블록 검증 시간, 탈중앙화 정도, 전력 소비와 같은 다른 지표도 존재한다. 이러한 지표는 블록 크기, 노드 수 및 전자 서명 알고리즘과 같은 블록체인의 다양한 요소에 의해 영향을 받는다. 본 절에서는 이러한 블록체인 평가 지표에 대해 설명한다.

초당 트랜잭션 수는 1초 동안 처리할 수 있는 트랜잭션의 수를 의미한다. 이는 현재 주로 사용되는 블록체인 성능의 가장 일반적인 지표이다. 최근 많은 블록체인들이 높은 초당 트랜잭션 수를 달성할 수 있는 구조로 설계되고 있다. 그러나 초당 트랜잭션 수는 블록체인의 유연성을 고려하지 않으므로 다른 평가 지표와 함께 고려되어야 한다. 가장 유명한 암호화폐인 비트코인은 7 TPS, 이더리움은 20 TPS, 이오스는 3000 TPS를 갖는다. 그러나 이오스는 중앙집중식 시스템에 가깝기 때문의 블록체인의 탈중앙화성을 만족하지 못한다.

지연 시간은 트랜잭션이 네트워크에 나타난 시점부터 검증이 완료될 때까지 걸리는 시간을 의미한다. 지연 시간이 높으면 한 트랜잭션을 처리하는 데 많은 시간이 소요된다는 의미이며, 이는 블록체인의 성능 저하를 초래한다. 비트코인의 지연 시간은 10분으로 매우 크며 이더리움의 경우 0.22분이다. 또한 낮은 지연 시간을 목표로 설계된 리플은 약 4초의 지연 시간을 갖는다.

제 3 절 양자 후 서명 체계

1) FALCON

FALCON은 Fast Fourier Lattice-based Compact Signatures over NTRU(의 약어로, 격자 기반 서명 알고리즘의 일종이다. Short Integer Solution(SIS) 문제가 NTRU 격자 상에서 양자 알고리즘으로도 효율적으로 해결하기 못한다는 점을 기반으로 설계되었다. FALCON은 보안 수준에 따라 FALCON-512, FALCON-1024로 구분된다.

[표 2-2] Details of FALCON (unit: Bytes)

	NIST level	Public Key Size	Private Key Size	Signature Size
FALCON-512	1	897	1,281	666
FALCON-1024	5	1,793	2,305	1,280

[표 2-2]는 FALCON의 보안 수준에 따른 공개/개인 키 및 서명의 크기를 보여준다. FALCON의 공개 키의 크기는 각각 897, 1,793 바이트, 개인 키의 크기는 1,281, 2,305 바이트, 서명의 크기는 666, 1,280바이트로 구성되어 있다. FALCON은 다른 양자 후 암호 체계와 비교하였을 때 가장 작은 키/서명 크기와 비교적 빠른 실행 속도를 제공한다.

2) CRYSTALS-Dilithium

CRYSTALS-Dilithium은 NIST에서 표준화 알고리즘으로 선정된 양자 후 암호 기술이다. CRYSTALS-DIlithium은 최단 벡터 문제(Shortest Vector Problem, SVP)를 기반으로 하는 격자 기반의 암호 체계이다. 최단 벡터 문제는 다항 시간 내에 격자 상의 임의의 위치에 가장 가까운 벡터를 찾는 것이 어렵다는 것에 기인한 문제이다. 이는 양자 컴퓨터 상에서도 해결하기 어렵다.

[표 2-3] Details of CRYSTALS-Dilithium (unit: Bytes)

	NIST level	Public Key Size	Private Key Size	Signature Size
Dilithium-2	1	1,312	2,528	2,420
Dilithium-3	3	1,952	4,000	3,293
Dilithium-5	5	2,592	4,864	4,595

[표 2-3]은 CRYSTALS-Dilithium의 보안 수준에 따른 공개/개인 키 및 서명의 크기를 보여준다. CRYSTALS-Dilithium은 보안 수준에 따라 CRYSTALS-Dilithium-(2, 3, 5)로 나뉘어져 있다. CRYSTALS-Dilithium의 공개 키의 크기는 1,312에서 2,592 바이트, 개인 키의 크기는 2,528에서 4,864 바이트, 서명 크기는 2,420에서 4,595 바이트로 구성되어 있다. CRYSTALS-Dilithium은 FALCON 양자 후 서명 체계와 비교하였을 때, 더 큰 키와 서명 크기를 가지지만 빠른 연산 속도를 제공한다.

3) SPHINCS+

SPHINCS+는 기존 SPHINCS의 속도와 서명 크기를 개선한 양자 후 서명 알고리즘이다. 상태를 저장하지 않는 stateless 해시 기반 알고리즘이며, SHAKE256, SHA-256, Haraka를 각각 기반으로 하는 3가지의 알고리즘으로 구성되어 있다.

[표 2-4] Details of SPHINCS+ (unit: Bytes)

	NIST level	Public Key Size	Private Key Size	Signature Size
SPHINCS+ SHA256-128f simple	1	32	64	17,088
SPHINCS+ SHA256-192f simple	3	48	96	35,664
SPHINCS+ SHA256-256f simple	5	64	128	49,856

[표 2-4]는 SPHINCS+의 보안 수준에 따른 공개/개인 키 및 서명의 크기를 보여준다. SPHINCS+는 보안 수준에 따라 SPHINCS+ SHA256-(128f, 192f, 256f) simple로 나뉘어져 있다. SPHINCS+의 공개 키의 크기는 32에서 64 바이트, 개인 키의 크기는 64에서 128 바이트, 서명의 크기는 17,088에서 49,856 바이트로 구성되어 있다. SPHINCS+의 경우 다른 양자 후 서명 체계와 비교하였을 때 매우 작은 키 크기를 가지지만, 서명의 크기가 매우 크며, 이는 블록의 크기가 한정된 블록체인의 특성상 트랜잭션 처리량이 감소하기에 적합하지 않은 특성이다. 실행 속도 또한 다른 양자 후 서명 체계에 비해 낮은 성능을 보여준다.

제 4 절 신뢰 실행 환경 (Trusted Execution Environment, TEE)

신뢰 실행 환경은 메인 프로세서의 보안 영역을 의미한다. 해당 보안 영역은 프로세서 내부의 코드와 데이터가 기밀성과 무결성 측면에서 보호될 수 있도록 보장한다. 이를 위한 다양한 기법들이 존재한다. 대표적으로 신뢰 시간, 모노토닉 카운터(Monotonic Counter), 난수 생성, 증명(Attestation)이 있

다. 신뢰 실행 환경의 대표적인 플랫폼으로는 Intel SGX, ARM TrustZone, RISC-V MultiZone, 그리고 AMD SEE가 있다. 본 절에서는 신뢰 실행 환경에서의 기법에 대해 설명한다.

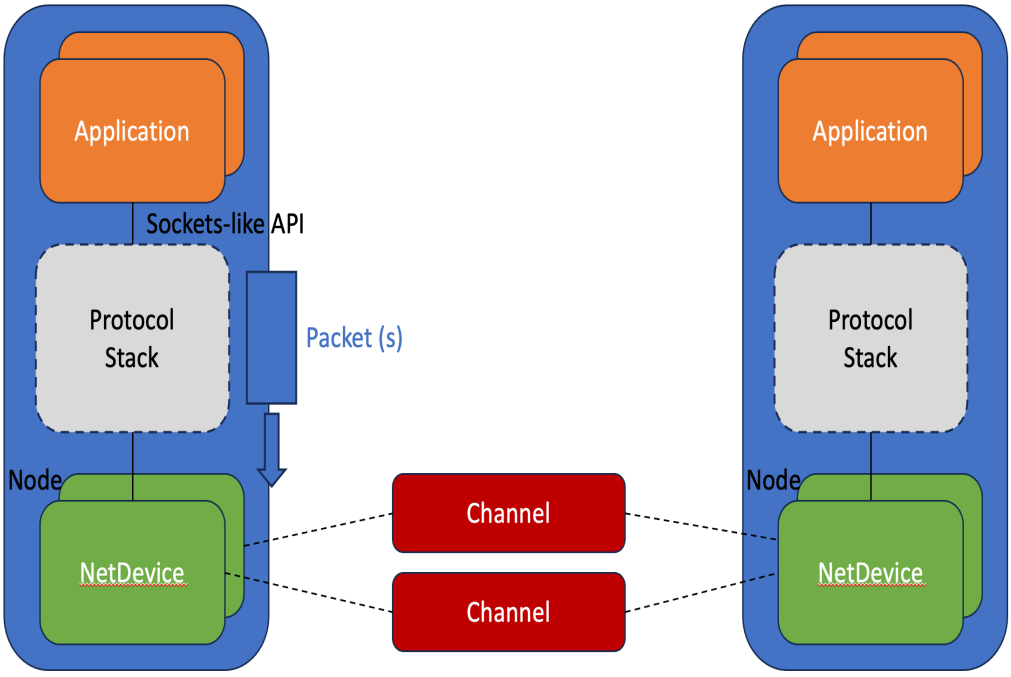
신뢰 시간은 서비스 제공을 위한 Protected Read-Time Clock(PRTC) 기반 타이머를 제공한다. 이 신뢰 시간 서비스를 사용하여 이전 타이머를 읽은 이후 경과된 시간을 측정할 수 있다. Timer Source Epoch을 사용하여 Read Time 지점 간의 불연속성을 감지할 수 있다. 여기서 불연속성은 배터리 교체와 같은 이벤트로 인해 PRTC가 재설정되거나 소프트웨어 공격과 같은 예기치 못한 이벤트로 인해 타이머가 다른 PRTC와 연결되었을 때를 의미한다. 이 경우 사용자는 두 Read-Time 사이의 계산된 기간을 신뢰해서는 안 되며 오류 조건을 적절히 처리하여야 한다. 이는 Intel SGX SDK의 라이브러리 API 함수인 *sgx_get_trusted_time*()을 통해 사용할 수 있다.

모노토닉 카운터는 사용자의 고유 식별자인 ID를 가진다. 사용자는 Intel SGX SDK를 통해 모노토닉 카운터를 생성하고 값을 증가시키거나 읽거나 삭제할 수 있다.

증명은 다양한 이유로 통신과 같은 여러 상황에서 사용자들끼리 협력해야 하는 경우에, 상호 간의 신뢰성을 증명하기 위한 기능으로써 사용된다. 증명은 로컬 증명과 원격 증명으로 나뉜다. CPU 내에 두 신뢰 실행 환경 보안 영역이 존재하는 경우 로컬 증명으로 검증이 가능하며, 서로 다른 CPU 내에 존재하는 경우 원격 증명을 통해 검증하여야 한다.

난수 생성은 *RDRAND*라는 명령을 통해 온칩 엔트로피 소스에 의해 시드화된 Intel 온칩 하드웨어 난수 생성기에서 신뢰할 수 있는 난수를 생성할 수 있다.

제 5 절 NS-3 (Network Simulator)



[그림 2-3] Basic NS-3 Data Flow Model

[그림 2-3]은 NS-3에서의 데이터 흐름에 대한 모델을 나타낸다. NS-3란 분산 네트워크 프로토콜 개발 시 사용되는 시뮬레이터로, 실제 네트워크와 유사한 환경을 구축하기 위해서 사용된다. NS-3에서는 데이터 전송을 위해 애플리케이션에서 기존 네트워크에서 소켓 API를 사용하는 것과 유사한 방식으로, 프로토콜 스택에서 넷디바이스를 이용하여 채널을 거쳐 다른 넷디바이스로 보내는 과정을 수행한다.

제 3 장 제안 기법

본 장에서는 효율적인 양자 후 블록체인 합의 알고리즘인 PQ-DPoL을 설계하기 위한 다양한 방법론을 소개한다. 본 논문의 방법론을 소개하기 전 양자 후 블록체인에 대한 주요 관점 및 고려사항에 대한 주의사항을 제시한다.

1) 키 크기

블록체인에 사물 인터넷(Internet of Things, IoT) 장치를 사용할 때, 작은 공개/개인 키를 가진 양자 후 암호를 선택하는 것이 좋다.

2) 서명 크기

블록체인 내의 트랜잭션에는 사용자 서명이 포함된다. 따라서 블록에 포함할 수 있는 트랜잭션의 수를 늘리기 위해서는 작은 서명 크기를 가진 양자 후 암호를 채택하는 것이 좋다.

3) 실행 속도

양자 후 암호 체계는 초당 많은 트랜잭션을 처리하여 높은 속도의 블록체인 운영이 가능하도록 하여야 한다.

4) 계산 복잡도

빠른 실행을 하는 것은 바람직하지만 계산 복잡성 또한 고려되어야 한다. 특정 하드웨어에서는 빠르게 실행될 수 있지만, 다른 하드웨어에서는 더 느리게 동작할 수 있으므로 계산 복잡성, 실행 시간 및 지원하는 하드웨어 디바이스 간의 균형을 맞추어야 한다.

5) 전력 소모

비트코인의 작업 증명과 같은 에너지 집약적인 합의 알고리즘에서는 전력 소모 또한 고려되어야 한다. 하드웨어, 통신 트랜잭션 및 보안 체계와 같은 요인들이 에너지 사용에 영향을 미친다. 따라서 양자 후 암호 체계는 효율적인 에너지 소모를 목표로 하여야 한다.

제 1 절 FALCON을 활용한 양자 후 블록체인

FALCON은 많은 다른 양자 후 서명 체계와 비교하였을 때 가장 작은 키/서명 크기와 빠른 서명 및 검증 속도라는 장점을 가진다. 그러나 이러한 이러한 장점은 타원 곡선 암호에 비해 큰 키/서명 크기로 인해 초당 트랜잭션 수의 감소라는 성능 저하로써 나타난다.

앞서 언급한대로(제 3장), 사물인터넷을 고려할 때 블록체인에는 되도록이면 작은 키 크기의 양자 후 암호 체계를 사용하는 것이 좋다. 그러나 본 설계에서의 대상 장치는 행운 증명 합의 알고리즘을 위해 신뢰 실행 환경을 지원하는 CPU를 사용한다. 이는 FALCON의 큰 키 크기를 수용할 수 있음을 나타낸다. 따라서 FALCON 키/서명 크기는 문제를 일으키지 않으며, 빠른 서명 및 검증 속도를 활용할 수 있다는 것을 의미한다. 이러한 측면에서 FALCON은 본 논문의 블록체인 설계에 적합하다.

그러나 FALCON의 타원 곡선 암호에 비해 큰 서명 크기는 트랜잭션의 크기를 증가시킨다. 따라서 블록에 포함될 수 있는 트랜잭션의 수가 감소하며, 결과적으로 타원 곡선 암호 기반 서명을 지닌 블록체인에 비해 낮은 초당 트랜잭션 수를 보여준다.

3장 3절에서는 감소된 초당 트랜잭션 수를 증가시킬 수 있는 위임 기법을 적용한 합의 알고리즘에 대해 제시한다.

제 2 절 신뢰 실행 환경을 활용한 합의 알고리즘

본 논문에서는 신뢰 실행 환경 중 하나인 Intel SGX를 기반으로 시스템을 설계하였다. 신뢰 실행 환경은 알고리즘이나 중요한 작업 프로세스가 올바르게 작동하도록 강제한다. 대표적으로 위임자 또는 블록 생성자로 선출되기 위해 신뢰 실행 환경을 통한 난수 생성 과정이 필요하다. 또는 병렬 실행을 방지하기 위해 모노토닉 카운터가 생성되거나 올바르게 동작하였는지 검증하기 위한 원격 증명이 수행된다. 또한 신뢰 시간 서비스는 특정 대기 시간을 경과

했는지에 대해 신뢰할 수 있는 확인 방법을 제공한다.

이러한 이유로 블록체인 네트워크에 참여하기 위해서는 신뢰 실행 환경을 소지해야 한다. 또한 신뢰 실행 환경을 보유한 다수의 CPU를 통해 대다수의 네트워크를 통제하는 악의적인 행동은 신뢰 실행 환경을 구축하는 데에 필요한 비용으로 인해 불가능에 가깝다.

그러나 본 논문에서는 구현에 있어서 실제 신뢰 실행 환경을 사용하지 않고 인터페이스 형태로 구현되어 있다. 실제 신뢰 실행 환경을 적용하여 성능을 측정하는 것은 추후 연구과제이다. 사용된 신뢰 실행 환경의 기능에 대한 자세한 내용은 다음과 같다.

첫 번째, 신뢰 시간 서비스를 제공한다. 이를 통해 경과 시간을 측정하는 기능에 신뢰성을 보장하는 것이 가능하다. 신뢰 실행 환경을 통해 합의 알고리즘이 시작되는 시간을 *roundTime*으로 설정한다. 그 후 해당 라운드의 블록을 검증하고 *ROUND_TIME* 만큼의 시간이 경과하였는지 확인한다. 이를 통해 노드들은 결정론적인 블록 검증 시간을 갖게 되어 추가 작업 없이 블록 생성 시간을 동기화할 수 있다. 이때 시간을 경과하기 위한 *Sleep*은 busy-wait이므로 이 동안에 다른 작업이 가능하며, 시간과 에너지가 낭비되지 않는다. 또한 busy-wait중에 다른 더 나은 체인이 브로드캐스트되면 해당 체인으로 전환할 수 있다. NS-3(Network Simulator)에서는 Schedule 기능의 Delay를 *ROUND_TIME* 만큼 주어 해당 기능을 제공할 수 있다.

두 번째, 모노토닉 카운터를 제공한다. 악의적인 사용자는 동일한 CPU에서 알고리즘을 병렬로 실행하여 불공정한 이득을 취하려고 할 수 있다. 이때, 신뢰 실행 환경의 모노토닉 카운터 값을 매번 증가시킴으로써 병렬 실행을 방지할 수 있다. 이를 위해 매 알고리즘이 실행될 때 모노토닉 카운터 값을 저장한다. 그 후 블록을 검증할 때 현재 모노토닉 카운터 값과 알고리즘이 실행될 때의 모노토닉 카운터 값을 비교한다. 두 값이 다르면 동일한 CPU내에서 알고리즘이 병렬로 실행되었다는 것을 의미한다. 이 경우 모노토닉 카운터에 대한 검증이 실패하게 되고 해당 노드는 블록을 생성할 수 없다.

세 번째, 원격 증명을 제공한다. 알고리즘 또는 데이터가 조작되었는지를 각 노드들이 서로 확인할 수 있는 증거를 생성하는 프로세스인 원격 증명 기

능을 제공한다.

Algorithm 1: Remote Attestation.

```
1: function RemoteAttestation(nonce, luck)
2:     input ← nonce || luck
3:     proof ← Base58-Encoding(input)
4:     return proof
5: end function
```

[그림 3-1] Algorithm of Remote Attestation using TEE

[그림 3-1]은 원격 증명을 위한 *proof*를 생성하는 과정을 보여준다. *proof*는 알고리즘 또는 데이터가 변조되었는지 여부를 기록하기 위해 사용된다. 원격 증명에 의해 신뢰 실행 환경의 작업 프로세스와 데이터는 조작될 수 없다.

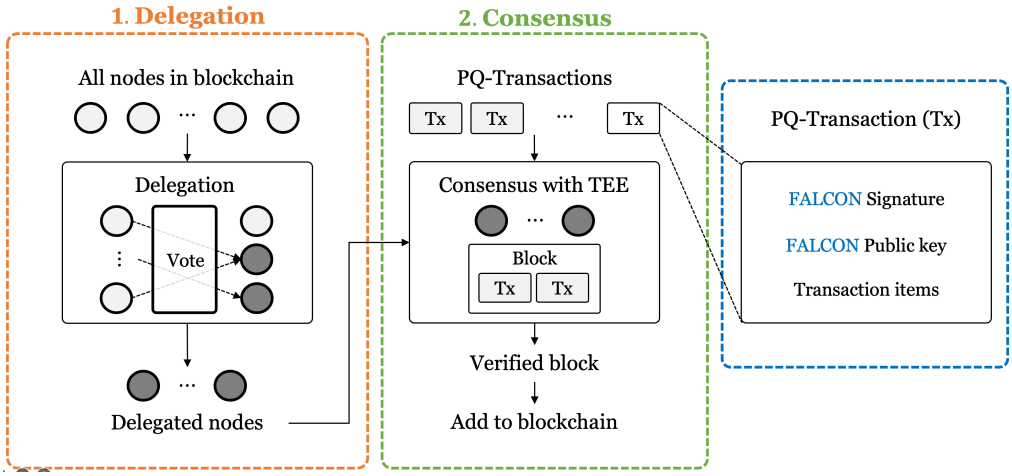
*proof*는 생성될 블록 헤더의 해시 값인 *nonce*와 신뢰 실행 환경의 *RDRAND*를 통해 생성된 실수 난수인 *luck*을 연접하여 Base58 인코딩한 데이터의 값이다. 이 값은 블록에 포함된 후 합의 알고리즘의 마지막 과정에서 다른 노드들에게 브로드캐스트된다. 노드는 브로드캐스트된 블록에 포함된 *proof*를 Base58 디코딩하여 *nonce*와 *luck*을 추출한다. 추출된 데이터를 통해 *proof*의 값이 조작되었는지 또는 올바른 *nonce*와 *luck*으로부터 생성된 값인지 확인한다.

결과적으로 어떠한 블록이나 트랜잭션도 조작되지 않았음을 증명할 수 있다. 또한 이를 통해 노드가 서로 신뢰 관계를 갖지 않더라도 통신을 할 수 있도록 한다.

네 번째, 난수 생성을 제공한다. 신뢰 실행 환경을 통해 공격자가 영향을 미칠 수 없는 신뢰할 수 있는 난수를 생성할 수 있다. Intel SGX의 *RDRAND*를 사용하여 신뢰할 수 있는 난수 값이 생성되는 이는 알고리즘에서 *luck*으로 사용된다. 이 *luck*은 투표 또는 합의 알고리즘에서 블록 생성자를 결정할 때 사용된다. 가장 높은 *luck* 값을 갖는 블록을 가진 노드가 블록 생성자로 선택된다.

제 3 절 위임 기법을 활용한 행운 증명

본 논문에서 제안하는 양자 후 위임 행운 증명은 위임 및 합의 단계로 구성된 양자 후 합의 알고리즘이다.

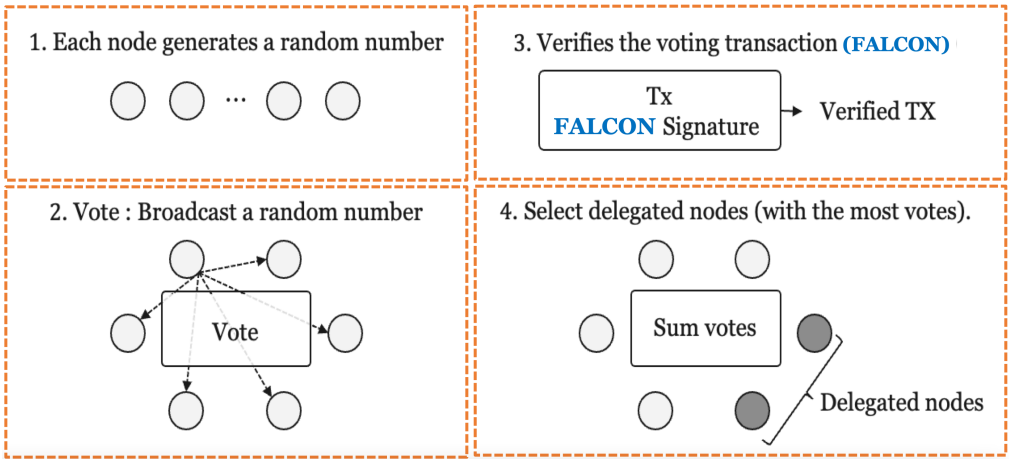


[그림 3-2] System Overview of PQ-DPoL

[그림 3-2]는 양자 후 위임 행운 증명의 개요를 보여준다. 위임 단계에서는 블록체인의 모든 노드들의 투표를 통해 위임 노드가 선출된다. 합의 단계에서는 선출된 노드들이 번갈아가며 블록을 생성한다. 이때 생성된 블록에는 FALCON의 서명과 공개 키가 포함된다. 마지막으로 위임 노드들이 블록을 검증한 후, 검증된 블록은 체인에 추가된다.

1) 위임 과정

FALCON을 적용하면 서명 크기가 증가하기 때문에 초당 트랜잭션 수가 감소하게 되어 한 블록에 포함될 수 있는 거래의 수가 감소한다. 그러나 위임 기법을 통해 블록체인의 일부 노드만이 합의를 수행하므로 합의에 참여하는 노드 수가 감소함에 따라 트랜잭션을 검증하는데에 걸리는 시간이 감소한다. 결과적으로 합의에 소요되는 시간이 감소한다. 즉, 위임 기법을 통해 FALCON으로 인해 감소된 초당 트랜잭션 수에 대한 단점을 극복할 수 있다. 더 나아가 블록체인의 중요한 요소 중 하나인 확장성을 향상시키는 장점이 있다.



[그림 3-3] Delegation Phase of PQ-DPoL

[그림 3-3]은 양자 후 위임 행운 증명의 위임 과정을 보여준다. 위임 과정의 자세한 내용은 다음과 같다.

가) 난수 생성: 각 노드는 난수를 생성한다. 이 난수는 투표 값으로 사용된다.

나) 투표: 각 노드는 투표 트랜잭션을 브로드캐스트한다. 투표 트랜잭션에는 난수(투표 값)와 FALCON의 서명 및 공개 키가 포함된다.

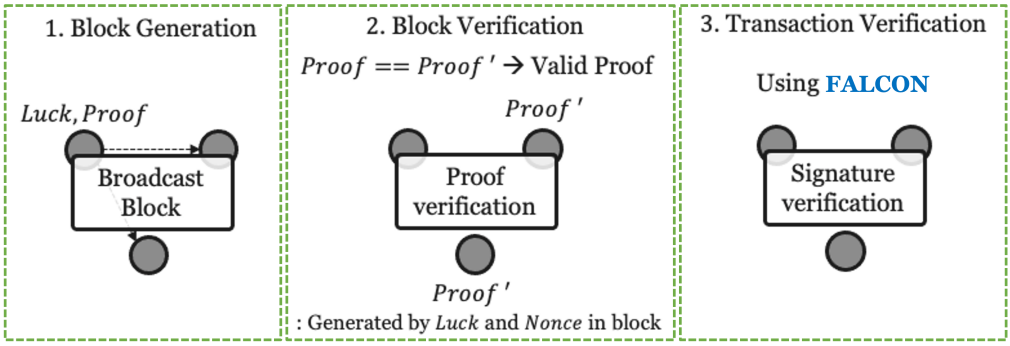
다) 검증: 각 노드는 다른 노드의 투표 트랜잭션을 검증한다. 투표 트랜잭션의 서명 검증에 성공하면 투표 트랜잭션이 유효하다는 것을 나타낸다. 서명 검증에 실패하면 트랜잭션이 조작되었음을 의미하며 투표가 무효화된다.

라) 위임 노드 선출: 각 노드가 받은 투표 값을 합산한다. 그 후 가장 높은 합산 투표 값을 얻은 상위 N개의 노드가 위임 노드로 선출된다.

2) 합의 과정

합의 과정에서는 위임 과정에서 선택된 노드들만이 신뢰 실행 환경을 사용하여 합의 알고리즘을 수행한다. 다시 말해 합의 과정에서는 블록에 포함된 요소(*nonce*, *luck*, *proof*)의 값들을 확인하여 적법한 블록이 생성되었는지를 보장하는 프로세스이다. 앞서 언급했듯이 트랜잭션을 검증하기 위해 FALCON을 사용하면 키 및 서명의 크기로 인해 블록에 포함된 트랜잭션의 수가 감소한다. 그러나 합의에 위임 노드만이 참여하기 때문에 합의에 소요되는 시간을

줄일 수 있다. 따라서 양자 후 경량 합의 알고리즘을 사용함으로써 키 및 서명 크기로 인한 초당 트랜잭션 수의 감소를 완화하면서도 양자 보안성을 보장할 수 있다.



[그림 3-4] Consensus Phase of PQ-DPoL

[그림 3-4]는 양자 후 위임 행운 증명의 합의 과정을 보여준다. 합의 과정의 자세한 내용은 다음과 같다.

가) 블록 생성: 블록을 생성하려면 블록의 무결성을 검증해야 한다. 또한, 행운 증명은 $ROUND_TIME$만큼의 시간이 경과하고 모노토닉 카운터의 값이 변경되지 않았는지에 대해 검증한다. 현재 시간이 $roundTime+ROUND_TIME$보다 크면 시간이 경과하였다고 판단한다. 그리고 신뢰 실행 환경을 기반으로 설정된 모노토닉 카운터의 값이 합의 과정의 시작 지점에서 호출된 모노토닉 카운터의 값과 동일한지 검증하고 그렇지 않다면 검증에 실패한다. 검증이 완료되면 신뢰 실행 환경을 통해 $luck$을 생성하고 원격 증명 프로세스에서 $proof$를 생성한다. 그 후 최종적으로 다른 위임 노드들에게 블록을 브로드캐스트한다.

나) 블록 검증: 블록 검증 과정에서 $nonce$, $prevHash$ 그리고 $proof$에 대한 검증을 수행한다. 생성할 블록의 헤더를 해싱하여 생성된 $nonce$가 현재 블록에 포함된 $proof$에서 추출한 $nonce$와 동일한지 검증한다. 해당 프로세스는 $nonce$의 무결성을 보장한다.

$proof$의 검증을 위해 수신한 블록에 포함된 $proof$와 합의 과정에서 생성된 새로운 $proof$를 비교한다. 다시 말해, 수신된 $proof$가 실제 유효한 $nonce$와 $luck$을 사용하여 생성된 값인지 확인한다.

다) 트랜잭션 검증: 마지막 단계로써 블록에 포함된 트랜잭션의 검증이 수행되어야 한다. 위임 노드들은 브로드캐스트받은 블록에 포함된 트랜잭션의 서명을 검증한다. 해당 프로세스에서 위임 단계(3장 3절 참조)에서 언급된 대로 FALCON을 사용한 서명 검증 과정이 수행된다.

제 4 장 실험 및 평가

제 1 절 실험 환경

본 실험에서는 C++ 언어 및 Ubuntu 20.04.6 LTS에서 실행되는 Intel i5-8295U CPU와 16GB RAM을 사용한다. 실제 블록체인 네트워크와 유사한 환경을 구축하기 위해 오픈 소스 네트워크 시뮬레이터인 NS-3를 사용한다.

제 2 절 성능 평가

본 절에서는 FALCON, CRYSTALS-Dilithium, SPHINCS+를 사용한 실행 속도 및 성능(초당 트랜잭션 수, 지연 시간)을 제시한다. 성능 지표로는 초당 트랜잭션 수와 지연 시간을 사용한다. 초당 트랜잭션 수는 위임 및 합의 과정에서 동일하게 측정된다. 그러나 지연 시간은 위임과 합의 과정에서 각각 다르게 정의된다. 다음과 같은 세부사항이 존재한다. 우선 위임 과정에서의 지연 시간은 트랜잭션 생성에서 트랜잭션 검증까지의 시간을 나타낸다. 합의 과정에서의 지연 시간은 위임 노드가 트랜잭션을 포함하는 블록을 생성한 후 블록 검증을 완료하기까지의 시간을 나타낸다. 블록체인 네트워크의 크기 및 적용된 양자 후 암호의 유형에 따라 초당 트랜잭션 수와 지연 시간을 측정한다.

1) FALCON과 그 외 양자 후 서명 체계와의 실행 속도 비교

[표 4-1] Execution speed comparison of PQCs (unit: second)

	KeyGen	SigGen	SigVerify
FALCON-512	0.011444	0.000512	0.000075
FALCON-1024	0.033799	0.000838	0.000142
Dilithium-2	0.000045	0.000163	0.000047
Dilithium-3	0.000098	0.000196	0.000077
Dilithium-5	0.000119	0.000228	0.000110
SPHINCS+ SHA256-128f simple	0.000581	0.012447	0.001029
SPHINCS+ SHA256-192f simple	0.000880	0.021434	0.001475
SPHINCS+ SHA256-256f simple	0.002116	0.043421	0.001500

[표 4-1]은 블록체인 네트워크에서 양자 후 서명 체계에 따른 실행 속도 성능을 보여준다. 구체적으로 FALCON-(512, 1024), CRYSTALS-Dilithium-(2, 3, 5), SPHINCS+ SHA256-(128f, 192f, 256f) simple의 키

생성 시간, 서명 생성 시간 및 서명 검증 시간을 측정한다. FALCON은 CRYSTALS-Dilithium보다는 느린 실행 속도를 보여주지만 SPHINCS+에 비해 키 생성 시간을 제외한 서명 생성 시간 및 서명 검증 시간에서 월등히 높은 성능을 보여준다. 키 생성 시간의 경우 네트워크 상에서 드물게 일어나므로 블록체인 성능에 많은 영향을 끼치지 않는다.

2) 초당 트랜잭션 수

해당 실험에서 실험 환경의 한계로 인해 매우 큰 서명 크기를 갖는 SPHINCS+ SHA256-(192f, 256f) simple의 성능은 측정할 수 없다. 따라서 해당 성능을 제외한 나머지 양자 후 암호의 성능을 비교 분석한다.

[표 4-2] TPS of PQ-DPoL

nodes / scheme	2^1	2^2	2^3	2^4	2^5
FALCON-512	307.0817	72.2645	18.4524	4.5700	1.1110
FALCON-1024	116.2432	30.5676	7.4315	1.9117	0.4669
Dilithium-2	102.9905	25.8397	6.5516	1.6370	0.4088
Dilithium-3	68.5390	15.8406	4.1040	1.0632	0.2669
Dilithium-5	36.3322	9.9926	2.3893	0.6356	0.1567
SPHINCS+ SHA256-128f simple	4.9496	1.3056	0.3473	0.0908	0.0227

[표 4-3] The Number of Transactions in One Block (BlockSize: 50KB)

	The number of transactions
ECDSA	356
FALCON-512	29
FALCON-1024	15
Dilithium-2	12
Dilithium-3	9
Dilithium-5	6
SPHINCS+ SHA256-128f simple	2
SPHINCS+ SHA256-192f simple	측정 불가
SPHINCS+ SHA256-256f simple	측정 불가

[표 4-2]는 양자 후 서명 체계에 따른 초당 트랜잭션 수를, [표 4-3]은 양자 후 서명 체계에 따른 블록 내 트랜잭션의 개수를 나타낸다. FALCON을 사용할 경우 실행 속도 자체는 CRYSTALS-Dilithium에 비해 낮은 성능을 보여주지만, 작은 공개 키 및 서명에 의해 블록 내에 다수의 트랜잭션이 포함될 수 있다. 마찬가지로 SPHINCS+의 경우 매우 큰 서명 크기를 갖기 때문에 블록 내에 트랜잭션이 소량만 담기게 된다. 따라서 FALCON의 초당 트랜잭션 수가 가장 높게 측정되며, 서명 크기에 따라 SPHINCS+의 초당 트랜잭

션 수가 가장 낮게 측정된다.

3) 지연 시간

[표 4-4] Latency of PQ-DPoL

nodes / scheme	2^1	2^2	2^3	2^4	2^5
FALCON-512	0.0958	0.4071	1.5943	6.4375	26.4582
FALCON-1024	0.1290	0.7907	2.0184	7.8461	32.1206
Dilithium-2	0.1165	0.4644	1.8316	7.3300	29.3506
Dilithium-3	0.1313	0.5681	2.1929	8.4643	33.7204
Dilithium-5	0.1651	0.6004	2.5111	9.4387	38.2889
SPHINCS+ SHA256-128f simple	0.4040	1.5317	5.7581	22.0108	87.7281

[표 4-4]은 양자 후 서명 체계에 따른 지연 시간을 보여준다. CRYSTALS-Dilithium의 빠른 실행 속도에도 불구하고([표 4-1] 참고) FALCON이 가장 낮은 지연 시간을 보여준다.

초당 트랜잭션 수 및 지연 시간에 있어 노드 수가 증가함에 따라 전체적으로 성능이 감소하는 것을 볼 수 있다([표 4-2], [표 4-4] 참고). 노드 수가 512인 경우는 하드웨어 환경의 한계로 인해 측정할 수 없지만 측정 결과를 기반으로 성능이 감소할 것으로 추정된다. 따라서 노드 수가 증가와

FALCON의 타원 곡선 암호에 비해 큰 공개 키/서명 크기로 인해 감소된 초당 트랜잭션 수를 증가시키기 위하여 위임 기법을 적용한다. 이를 통해 노드의 수를 줄이며 합의에 필요한 시간 즉, 지연 시간을 축소시킴으로써 초당 트랜잭션 수에 관한 문제점을 완화하면서 보안성을 보장할 수 있다.

제 5 장 결론

본 연구에서는 양자 후 서명 체계와 새로운 합의 알고리즘을 포함한 다양한 기여를 통해 효율적이고 양자 보안성을 보장하는 블록체인 네트워크를 구축하였다. 또한, 다양한 환경에서의 호환성과 최적의 성능을 보장하기 위하여 다양한 측면에서의 실험을 진행하였다.

실험 결과를 요약하자면, FALCON을 적용한 양자 후 위임 행운 증명의 초당 트랜잭션 수는 타원 곡선 암호 기반의 합의 알고리즘보다 낮은 성능을 보여준다. 이는 양자 후 서명 체계의 더 큰 공개 키 및 서명의 크기에 의해 나타나는 현상이다. 따라서 성능을 향상시키기 위해 행운 증명에 위임 기법을 적용하였으며, 이는 여전히 타원 곡선 암호 기반의 합의 알고리즘보다 낮은 성능을 보여줄 수 있지만, 양자 보안성을 제공함과 동시에 합리적인 성능을 제공한다.

성능 측정 결과, 키 생성, 서명 생성, 서명 검증 측면에서 FALCON이 SPHINCS+보다는 월등히 빠른 실행 속도를 보여주지만, CRYSTALS-Dilithium 보다는 비교적 낮은 성능을 보여주는 것을 알 수 있다. 그러나, 블록체인 네트워크의 성능 평가 지표인 초당 트랜잭션 수, 지연 시간 측면에서는 오히려 FALCON이 CRYSTALS-Dilithium보다 높은 성능을 보여주는 것을 알 수 있다. 초당 트랜잭션 수는 약 2.6~2.9배, 지연 시간은 약 1.1~1.2배 높은 성능을 보여준다. 이는 FALCON의 공개 키/서명의 크기가 비교적 작아 블록 내에 더욱 많은 트랜잭션이 담길 수 있게 되어 나타나는 현상이다.

실험 결과를 기반으로, 다양한 양자 후 서명 체계 중 FALCON을 선택하였다. 앞서 말했듯이, FALCON은 비록 CRYSTALS-Dilithium보다 키 생성 시간, 서명 시간, 서명 검증 시간에 있어 비교적 낮은 성능을 보여주지만 유사한 실행 속도를 가지고 있다. 또한 비교적 작은 공개 키 및 서명 크기로 인해 블록에 담길 수 있는 트랜잭션의 수가 증가하여 초당 트랜잭션 수에 대해서는 오히려 CRYSTALS-Dilithium보다 뛰어난 성능을 보여준다. 따라서 본 실험을 통해 양자 후 합의 알고리즘을 구현하기 위한 가장 적합한 서명 체계

는 FALCON이라고 결론지을 수 있다.

참 고 문 헌

1. 국외문헌

A. I. Sanka and R. C. Cheung, “A systematic review of blockchain scalability: Issues, solutions, analysis and future research,” Journal of Network and Computer Applications, vol. 195, p. 103232, 2021.

Fouque, Pierre-Alain, et al. "Falcon: Fast-Fourier latticebased compact signatures over NTRU." Submission to the NIST's post-quantum cryptography standardization process 36.5 (2018): 1-75.

F. Yang, W. Zhou, Q. Wu, R. Long, N. N. Xiong, and M. Zhou, “Delegated proof of stake with downgrade: A secure and efficient blockchain consensus algorithm with downgrade mechanism,” IEEE Access, vol. 7, pp. 118541-118555, 2019.

G. Wood et al., “Ethereum: A secure decentralised generalised transaction ledger,” Ethereum project yellow paper, vol. 151, no. 2014, pp. 1 -32, 2014.

J. Lee, S. Lee, Y.-S. Lee, and D. Choi, “T-depth reduction method for efficient sha-256 quantum circuit construction,” IET Information Security, vol. 17, no. 1, pp. 46-65, 2023.

L. Chen, L. Xu, N. Shah, Z. Gao, Y. Lu, and W. Shi, “On security analysis of proof-of-elapsed-time (poet),” in Stabilization, Safety, and Security of Distributed Systems: 19th International Symposium, SSS 2017, Boston, MA, USA, November 5-8, 2017, Proceedings 19, pp. 282-297, Springer, 2017.

L. K. Grover, “A fast quantum mechanical algorithm for database search,” in Proceedings of the twenty-eighth annual ACM

symposium on Theory of computing, pp. 212-219, 1996.

M. Amy, O. Di Matteo, V. Gheorghiu, M. Mosca, A. Parent, and J. Schanck, "Estimating the cost of generic quantum pre-image attacks on sha-2 and sha- 3," in International Conference on Selected Areas in Cryptography, pp. 317-337, Springer, 2016.

M. Raavi, P. Chandramouli, S. Wuthier, X. Zhou, and S.-Y. Chang, "Performance characterization of post-quantum digital certificates," in 2021 International Con- ference on Computer Communications and Networks (ICCCN), pp. 1-9, IEEE, 2021.

M. Salimitari and M. Chatterjee, "A survey on consensus protocols in blockchain for iot networks," arXiv preprint arXiv:1809.05613, 2018.

Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." Decentralized business review (2008).

NIST., "Submission requirements and evaluation criteria for the post-quantum cryptography standardization process," 2016. https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/ call-for-proposals-final-dec-2016.pdf.

P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete log- arithms on a quantum computer," SIAM review, vol. 41, no. 2, pp. 303-332, 1999.

S. Cen and B. Zhang, "Trusted time and monotonic counters with intel soft- ware guard extensions platform services," Online at: https://software. intel. com/sites/default/files/managed/1b/a2/Intel-SGX-Platform-Services . pdf, 2017.

S. M. H. Bamakan, A. Motavali, and A. B. Bondarti, "A survey of blockchain consensus algorithms performance evaluation criteria," Expert Systems with Appli- cations, vol. 154, p. 113385, 2020.

W. K. Lee, K. Jang, G. Song, H. Kim, S. O. Hwang, and H. Seo, “Efficient implementation of lightweight hash functions on gpu and quantum computers for iot applications,” IEEE Access, vol. 10, pp. 59661-59674, 2022.

ABSTRACT

PQ-DPoL: An Efficient Post-Quantum Blockchain Consensus Algorithm

Kim, Won-Woong

Major in IT Convergence Engineering

Dept. of IT Convergence Engineering

The Graduate School

Hansung University

The advancement of quantum computers and the potential polynomial-time solution of Elliptic Curve Cryptography (ECC) using the Shor's algorithm pose a significant threat to blockchain security. This paper presents an efficient quantum-secure blockchain with our novel consensus algorithm, We integrate a post-quantum signature scheme into the transaction signing and verification process of our blockchain, ensuring its resistance against quantum attacks. Concretely, we adopt the FALCON signature scheme, which is one of the selected algorithms in the NIST Post-Quantum Cryptography (PQC) standardization. Not surprisingly, the incorporation of a post-quantum signature scheme leads to a reduction in the number of Transactions Per Second (TPS) processed by our blockchain. To mitigate this performance degradation, we introduce a new consensus algorithm that effectively combines the

Proof-of-Luck (PoL) mechanism with a delegated approach. We strive to build an efficient and secure blockchain for the post-quantum era by benchmarking our blockchain, adjusting the security parameters of FALCON, and refining the components of the consensus algorithm

【KEYWORD】Security, Post-Quantum Cryptographic, Blockchain, Consensus Algorithm, Trusted Execution Environment