양자내성 전자서명 도입을 위한 블록체인 키 사용 패턴 연구 동향 분석

(A Survey on Key Usage Patterns in Blockchain for Adopting Post-Quantum Digital Signatures)

이재흥*
(Jae Heung Lee)

요 약

NIST 양자내성암호 표준화 이후 블록체인 전자서명의 양자내성 전환이 실질적 과제로 떠올랐으나, 해시 기반 전자서명의 큰 서명 크기로 인해 발생하는 온체인 비용이 도입의 장벽이 되고 있다. 블록체인 키는 대부분 한 번만 사용되고 예외적인 상황에서만 재사용되는 소수회 사용 구조를 가지고 있기 때문에, 실제 키 사용 패턴이 서명 크기 축소 가능성을 결정한다. 본 논문은 블록체인 키 사용 패턴에 대한 연구를 주소 및 키 재사용의 실증적 측정, 공개키 노출량 측정, 이더리움 계정 활동 분포, 소수회 사용 전제에 기반한 서명 설계의 네 범주로 분류하고 측정 단위, 대상 체인, 측정 지표의 관점에서 비교 분석을 수행한다. 분석 결과, 키 사용 횟수에 대한 확률 분포 모델, 재사용 원인에 대한 분류 체계, 실증적 증거와 설계 간의 연관성이 부재함을 확인하였다. 따라서 분포 실측, 사용 모델 정형화, 분포 기반 파라미터 최적화로 이어지는 단계적 연구 방향을 제시한다.

■ 중심어 : 블록체인 ; 양자내성암호 ; 해시 기반 서명 ; 키 재사용 ; 소수회 서명

Abstract

Following NIST's PQC standardization, migrating blockchain signatures to quantum-resistant schemes is now a practical challenge, yet the on-chain cost of large hash-based signatures hinders adoption. Since blockchain keys are mostly used once and reused only exceptionally (few-time usage), actual usage patterns determine the potential for signature size reduction. This paper classifies blockchain key usage studies into four categories (address/key reuse measurement, public-key exposure measurement, Ethereum account activity distributions, and few-time signature design) and compares their measurement units, target chains, and metrics. The analysis reveals no distribution model of key usage counts, no taxonomy of reuse causes, and no link between empirical evidence and design, motivating a staged agenda of distribution measurement, usage-model formalization, and distribution-based parameter optimization.

■ keywords : Blockchain ; PQC ; Hash-Based Signature ; Key Reuse ; Few-Time Signature

Ⅰ. 서 론

최근 스마트 미디어 및 콘텐츠 서비스 분야에서 블록체인은 콘텐츠 저작권 관리, NFT 기반 디지털 자산 거래, 콘텐츠 배포 이력 검증 등에 기반 기술로 활용되고 있다. 이러한 블록체인 기반 콘텐츠 서비스에서는 전자 서명을 통해 자산 소유권과 거래 무결성이 보장되며, 서명 체계의 보안성이 전체 서비스의 신뢰성을 결정한다. 또한 온체인에 기록되는 서명 데이터의 크기와 검증 비용은 블록당 허용 가능한 트랜잭션 수와 처리 지연 시간에 직접적인 영향을 미치므로, 서명 체계의 선택은 보안 측면뿐만 아니라 서비스 품질(QoS) 측면에서도 중요한 설계 요소이다.

* 정회원, 경기대학교 AI컴퓨터공학부

접수일자 : 2026년 07월 10일
게재확정일 : 2026년 07월 23일
교신저자 : 이재흥 e-mail : jhlee@kyonggi.ac.kr

한편 양자 컴퓨터의 발전은 현재 블록체인에서 사용되는 전자서명 체계에 근본적인 위협을 가하고 있다. 많은 블록체인에서 사용하는 ECDSA는 Shor 알고리즘을 실행할 수 있는 양자 컴퓨터에 의해 무력화될 수 있다. 이에 대응하여 NIST는 2024년에 양자내성암호(PQC) 표준을 최종 확정했으며, 특히 FIPS 205(SLH-DSA)[1]는 해시 기반 전자서명인 SPHINCS+[2]를 채택하여 격자 기반 서명과는 독립적인 수학적 기반을 가진 대안으로서 해시 기반 전자서명의 장기적인 표준 지위를 확립하였다. 해시 함수의 안전성에만 의존하는 해시 기반 전자서명은 보수적인 보안 가정과 높은 성숙도 덕분에 블록체인의 양자내성 전환에 유력한 후보로 여겨진다.

그러나 해시 기반 전자서명을 블록체인에 들여오려면 온체인 비용이라는 장벽부터 넘어야 한다. SPHINCS+[2]의 서명은 SHAKE-128s 기준 7,856바이트다. 약 72바이트인 ECDSA의 100배가 넘고, 그만큼 블록 용량을 잠식하며 수수료를 끌어올린다. 주목할 지점은 이 크기가 어디서 오는가이다. SPHINCS+를 비롯한 기존 해시 기반 서명은 단일 키로 사실상 무한정 서명하는 범용 시나리오를 전제로 설계되었다. 그런데 블록체인의 키 사용은 이 전제와 거리가 멀다. 비트코인과 이더리움의 사용자는 익명성과 키 관리 단순화를 위해 키를 최대한 일회용으로 쓰고, 체인 포크나 트랜잭션 실패 후 재전송, 소유권 증명, RBF(Replace-By-Fee) 같은 제한적 상황에서만 같은 키를 다시 쓴다. 설계 전제와 실제 사용 사이의 이 간극이야말로 사용 횟수 제한으로 서명 크기를 압축할 수 있다는 본 논문의 출발점이다.

이러한 최적화가 가능하려면 블록체인에서 키가 실제로 몇 회 사용되는지부터 정확히 알아야 한다. 문제는 그 답이 한 분야에 모여 있지 않다는 데 있다. 주소 재사용 측정, 공개키 노출량 정량화, 계정 활동 분석, 소수회 전제의 서명 설계가 각자의 목적을 위해 따로 진행되어 왔을 뿐이다. 이들을 키 사용 패턴이라는 관점에서 종합하고 양자내성 전자서명 설계의 근거로 연결한 조사 연구는 필자가 확인한 범위에서는 아직 없다. 공백은 더 구체적이다. 기존 실증 연구들은 재사용 비율이나 취약 잔액 총량 같은 집계 지표에 머물러 키 하나가 몇 회 사용되는지의 확률 분포를 모델링하지 않았고, 소수회 전제의 서명 설계들은 그 분포를 실측 대신 가정으로 채워 왔다.

본 논문은 이 흩어진 증거들을 (1) 주소 및 키 재사용 실증 측정, (2) 양자 취약성 관점의 공개키 노출량 측정, (3) 이더리움 계정 활동 분포 분석, (4) 소수회 사용 전제의 블록체인 특화 서명 설계의 네 범주로 묶어 검토한다. 분류 자체가 목적은 아니다. 각 범주가 무엇을 어떤 단위로 측정했는지 나란히 놓고 비교해야, 서명 설계에 정말 필요한 증거가 무엇이고 무엇이 비어 있는지 드러나기 때문이다. 이 비교로부터 세 가지 연구 공백을 도출하고, 이를 메우는 단계적 연구 방향을 제안한다.

이후 구성은 다음과 같다. 2장에서 블록체인 전자서명 구조와 해시 기반 서명의 배경을 정리하고, 3장에서 네 범주의 연구를 검토한다. 4장에서 이들을 비교해 공백과 향후 방향을 논의하고, 5장에서 결론을 맺는다.

Ⅱ. 배경 지식

1. 블록체인 전자서명 구조와 키 노출

블록체인에서 전자서명은 자산 소유자만이 자산을 쓸 수 있게 보장하는 핵심 수단이다. 그런데 키가 언제 노출되고 얼마나 재사용되는지는 원장 모델이 좌우한다. 두 모델을 차례로 보자.

비트코인의 UTXO(Unspent Transaction Output) 모델에서 대표적인 스크립트 유형인 P2PKH(Pay-to-Public-Key-Hash)는 주소를 공개키의 해시로 표현한다. 공개키가 온체인에 영구히 드러나는 것은 자금을 받을 때가 아니라 쓸 때다. 지출 트랜잭션에 서명과 공개키가 함께 기록되기 때문이다. 비트코인 지갑들은 프라이버시를 위해 주소를 한 번만 쓰도록 권장하지만, 어디까

지나 권장일 뿐 프로토콜이 강제하지 않는다. 실제로는 다양한 이유로 주소와 키가 재사용된다.

이더리움의 사정은 다르다. 계정 기반 모델에서는 트랜잭션 서명 검증에 ECDSA 공개키 복원이 쓰이기 때문에, 트랜잭션을 한 건이라도 보낸 계정의 공개키는 사실상 공개된다. 주소를 트랜잭션마다 바꾸는 관행도 없어 한 키의 반복 사용이 구조적으로 흔하다. 여기서 유용한 점은 각 계정의 nonce가 해당 키로 서명되어 온체인에 포함된 트랜잭션의 누적 수를 그대로 기록한다는 것이다. 물론 한계도 있다. nonce는 EIP-712 기반 오프체인 서명이나 메타트랜잭션처럼 트랜잭션 전송을 수반하지 않는 서명을 세지 않으므로 총 서명 수의 하한으로 해석해야 하고, 이 대응은 외부 소유계정(EOA)에만 성립한다.

요컨대 두 모델은 키가 노출되는 시점도, 재사용되는 양상도 다르다. 키 사용 패턴의 실증 분석을 원장 모델별로 나누어 수행해야 하는 이유다.

분석 범위는 레이어 1의 온체인 서명으로 한정한다. 라이트닝 네트워크 같은 페이먼트 채널은 채널 상태를 갱신할 때마다 같은 키로 서명을 반복하므로 소수회 사용 전제가 통하지 않는 영역이다. 그러나 그 서명들은 대부분 온체인에 오르지 않고, 채널을 닫을 때의 최종 상태만 기록된다. 본 논문의 문제가 온체인 서명 크기인 이상 이들을 제외하는 것이 타당하다고 판단했으며, 오프체인 프로토콜의 키 사용 패턴은 별도 연구가 필요한 주제로 남겨 둔다.

2. 해시 기반 양자내성 전자서명

해시 기반 전자서명은 암호학적 해시 함수의 안전성에만 기대는 서명 체계다. 가정이 단순한 만큼 양자 컴퓨터 환경에서도 보안 여유가 잘 파악되어 있다. 본 논문이 이 계열에 주목하는 일차적 이유는 분류 체계 자체에 있다. 해시 기반 서명은 키 쌍당 허용 서명 횟수에 따라 일회용(OTS), 소수회용(FTS), 다회용으로 나뉘는데, 이 구분이 키 사용 횟수라는 축과 정확히 겹치기 때문이다.

NIST는 해시 기반 SLH-DSA(FIPS 205)와 함께 격자 기반 ML-DSA(FIPS 204)를 표준화했고, Falcon 기반 FN-DSA(FIPS 206)의 표준화를 진행 중이다. 크기만 보면 격자 쪽이 앞선다. ML-DSA-44의 서명은 약 2,420바이트, Falcon-512는 약 666바이트에 불과하다. 그럼에도 본 논문이 해시 기반에 초점을 맞추는 근거는 두 가지다. 우선 보안 가정의 보수성이다. 격자 기반 서명은 역사가 비교적 짧은 구조적 격자 문제에 기대고 있고, Falcon은 부동소수점 가우시안 샘플링의 구현 및 부채널 위험에 대한 우려로 표준화가 늦어지고 있다. 자산이 수십 년씩 온체인에 남고 서명 체계를 바꾸려면 하드포크까지 필요한 블록체인이라면, 가장 보수적인 가정을 고르는 것이 옳다고 본다. 다른 하나는 앞서 언급한 분류 축이다. 사용 횟수와 서명 크기의 트레이드오프는 해시 기반 서명만의 구조적 특성으로, 격자 기반 서명에는 사용 횟수를 제한해 크기를 줄일 여지 자체가 없다. 블록체인의 소수회 사용 패턴을 설계에 반영할 수 있는 것은 결국 해시 기반뿐이다.

일회용 서명은 Lamport 서명[3]과 이를 개선한 WOTS 계열이 대표적으로, 하나의 키 쌍으로 한 번의 서명만 안전하게 생성할 수 있다. 소수회용 서명은 HORS[4]와 그 파생 기법(HORST, FORS, HORSIC+[5] 등)이 대표적으로, 여러 개의 서명을 허용하지만 서명 수가 증가함에 따라 보안 수준이 점진적으로 감소한다. 따라서 소수회용 서명의 파라미터는 목표 서명 수와 요구되는 보안 수준의 함수로 결정되며, 허용되는 서명 수를 더 작게 설정함으로써 서명 크기를 줄일 수 있다. 키 사용 횟수 분포의 실증이 서명 설계와 직결된다고 보는 이유가 여기에 있다.

다회용 구조는 여러 OTS/FTS 키 쌍을 Merkle 트리로 묶어 하나의 공개키로 인증하는 방식으로 구현된다. XMSS(RFC 8391)[6] 및 LMS(RFC 8554)[7]는 서명 크기가 비교적 작은 대신 어떤 OTS 키가 사용되었는지 기록을 유지해야 하는 상

태 기반(stateful) 기법이다. 상태 손실 시 동일한 OTS 키를 재사용하면 보안이 즉시 무너지기 때문에 NIST SP 800-208[8]에서는 이러한 기술의 사용을 통제된 환경으로 제한하고 있으며, 여러 기기에서 서명하고 백업 및 복구가 일반적인 블록체인 지갑 환경에는 적합하지 않다. 반면 SPHINCS+는 하이퍼트리와 FORS를 결합하여 상태 관리를 없앤 무상태(stateless) 기법으로 FIPS 205[1]로 표준화되었다. 하지만 단일 키로 2^{64}회의 서명을 지원하도록 설계하면 SHAKE-128s 기준으로 서명 크기가 7,856바이트에 이른다. 요컨대 기존 기법들은 무제한 사용을 위해 크기를 희생하는 방식(SPHINCS+)과 크기를 위해 위험한 상태 관리를 감수하는 방식(XMSS, LMS)이라는 두 가지 극단적인 입장에 치우쳐 있으며, 블록체인의 소수회 사용 구조에 부합하는 중간 지점은 충분히 탐구되지 않았다.

3. 키 재사용과 양자 취약성

Shor 알고리즘은 노출된 ECDSA 공개키로부터 다항 시간 내에 비밀키를 계산할 수 있지만, 공개키의 해시만 온체인에 존재하는 경우에는 해시 함수의 역상을 알아야 하므로 Grover 알고리즘의 제곱 가속만이 적용되기 때문에 위협이 제한적이다[9]. 따라서 블록체인의 양자 취약성은 노출된 공개키를 가진 자산의 규모, 즉 키 사용 패턴과 직접적으로 관련된다.

공개키 노출 경로는 다음과 같이 정리할 수 있다[10]. 첫째, P2PK(Pay-to-Public-Key) 및 Taproot(P2TR)와 같이 잠금 스크립트에 (조정된) 공개키가 직접 기록되는 유형이다. 둘째, P2PKH 계열 주소를 재사용하는 경우, 해당 주소에서 자금이 사용되면 공개키가 노출되므로 이후 동일 주소로 수신된 모든 자금은 양자 공격에 노출된다. 셋째, 이더리움에서 최소 한 건의 트랜잭션을 전송한 계정이다. 이 중 두 번째와 세 번째는 모두 키의 사용 및 재사용에서 비롯되며, 3장에서 살펴볼 노출량 측정 연구들은 이러한 경로들을 기반으로 취약 자산의 규모를 정량화한다.

Ⅲ. 블록체인 키 사용 패턴 연구 동향

키 사용 패턴을 정면으로 다룬 연구는 아직 존재하지 않는다. 관련 연구는 목적이 서로 다른 네 범주의 연구, 즉 재사용 측정, 노출량 정량화, 계정 활동 분석, 블록체인 특화 서명 설계에 흩어져 있다. 본 장에서는 이들을 "키가 실제로 몇 회 사용되는가"라는 하나의 물음 아래 재배치하여 검토한다.

1. 주소 및 키 재사용 실증 측정 연구

출발점은 Ron과 Shamir[11]의 비트코인 전체 트랜잭션 그래프 전수 분석이다. 2012년까지의 데이터에서 소유자의 97%가 10회 미만의 트랜잭션만 수행했다는 이 관찰을, 본 논문은 소수회 사용 구조의 첫 실증 증거로 읽는다. 다만 당시 저자들의 관심은 사용자 행태와 자금 흐름에 있었기 때문에, 키 사용 횟수의 분포 자체를 모델링하려는 시도는 아니었다.

주소 재사용을 명시적인 측정 대상으로 삼은 것은 Gong 등의 일련의 실증 연구[12, 13]다. 이들은 연간 주소 재사용률이 초기 상승 후 약 10% 수준에서 등락함을 보였고, 제네시스 블록부터 2023년 말까지를 전수 분석해 주소 유형별 구성비와 재사용 패턴을 정량화했다. 장기 추세를 확보했다는 점에서 가치가 크지만, 재사용 발생률이라는 측정 단위에 묶여 있어 개별 키가 몇 회 사용되는지는 여전히 알 수 없다.

이 한계를 처음 벗어난 것이 측정 단위를 주소에서 공개키로 옮긴 2026년의 다중 체인 분석[14]이다. Stütz 등은 주소 형식이 달라도 여러 체인이 같은 타원곡선 연산을 공유한다는 점을 이용해 비트코인과 이더리움을 포함한 6개 체인에서 공개키 수준의 재사용을 추적했고, 160만 개가 넘는 키가

둘 이상의 체인에서 재사용되고 있음을 확인했다. 키 재사용은 과거의 유물이 아니라 지금도 진행 중인 현상인 것이다. 주소 교체 관행이 키 재사용을 가릴 수 있음을 고려하면, 우리의 관심사인 키 사용 횟수 분포에 가장 근접한 접근은 이 키 수준 측정이라고 판단한다.

한편 분포의 함수형에 대한 단서는 네트워크 과학 쪽에서 나온다. Fischer 등[15]은 비트코인 트랜잭션 네트워크의 차수 분포와 주소 클러스터 크기 분포에서 멱법칙(power-law)을 반복적으로 관측했다. 키 사용 횟수 분포 역시 비슷한 heavy-tail 특성을 따를 가능성이 높다고 본다. 다만 이를 직접 검증한 연구는 아직 찾지 못했다.

2. 양자 취약성 관점의 공개키 노출량 측정 연구

두 번째 범주는 양자 위협 평가를 위해 공개키가 노출된 자산의 규모를 정량화한다. 이 분야의 기준을 세운 것은 Aggarwal 등[9]으로, 이들은 비트코인에 대한 양자 공격의 실제 위협 지점이 작업증명이 아니라 ECDSA 서명임을 밝혔다. Deloitte[16]는 P2PK 주소와 재사용된 P2PKH 주소의 잔액을 합산해 전체 비트코인의 약 25%가 노출되어 있다고 추정했고, 이후의 업계 분석들은 P2TR 같은 새 노출 유형을 더해 이 수치를 갱신해 왔다. 여기서 주목할 것은 수치 자체보다 추정치가 분석 시점과 노출 유형의 포함 범위에 따라 움직인다는 사실이다. 노출량 측정이 키 사용 패턴의 정의와 가정에 그만큼 민감하다는 뜻이다.

이더리움은 트랜잭션을 전송한 계정의 공개키를 복구할 수 있다는 구조적 특성 때문에 노출 비율이 비트코인보다 훨씬 높은 것으로 측정된다. 2026년 평가 연구[17]에서는 공개키가 노출된 계정에 2천만 ETH 이상이 있는 것으로 추정했으며, 이더리움 재단 또한 양자내성 전환 로드맵[18]을 공식화하여 이 문제를 프로토콜 수준의 과제로 인식하고 있다.

이 범주의 연구들은 노출 잔액을 정확하게 측정하지만, 관심 단위가 자산 가치이기 때문에 키당 사용 횟수는 노출 여부를 이진으로 판별하는 것으로 축약된다. 한 번 노출된 키와 수백 번 사용된 키가 동일하게 취급되므로, 소수회 서명 설계에 필요한 횟수별 세분화는 이루어지지 않는다.

3. 이더리움 계정 활동 분포 연구

세 번째 범주는 이더리움 계정 활동을 분석한 연구들이다. 2.1절에서 논의한 바와 같이 계정별 트랜잭션 전송 횟수(nonce)의 분포는 키 사용 횟수 분포를 직접적으로 보여준다.

실증 분석들이 그리는 그림은 하나로 수렴한다. 극단적인 heavy-tail 분포다. Said 등[19]은 주소의 99%가 트랜잭션을 한 번 보내거나 받는 데 그친다는 것을 보였고, Heimbach 등의 2026년 EVM 워크로드 분석[20]은 이더리움과 Base 모두에서 소수의 고활동 주소가 트랜잭션 볼륨의 대부분을 차지함을 확인했다. 계정 기반 체인에서도 대다수 키는 일회성 내지 소수회 사용에 그치고, 장기 재사용은 거래소나 컨트랙트 운영 계정 같은 소수의 특수 주체에 몰려 있다고 읽는 것이 자연스럽다.

아쉬운 것은 결과의 정리 방식이다. 이들 연구의 목적이 네트워크 구조나 성능 특성 파악에 있다 보니, 서명 설계에 필요한 형태, 즉 일회성·소수회·장기 재사용의 횟수 구간별 확률로는 결과를 정리하지 않는다. nonce라는 정확한 사용 횟수 지표가 있는데도 이를 키 사용 횟수 관점에서 직접 집계한 연구는 찾지 못했다. 비교적 적은 비용으로 메울 수 있는 공백이 그대로 남아 있는 셈이다.

4. 소수회 사용을 전제한 블록체인 특화 서명 연구

네 번째 범주는 블록체인의 키 사용 특성을 설계에 직접 반영한 양자내성 서명들이다. 최초의 사례는 QRL[21]이다. XMSS를 채택하되 계정당 서명 가능 횟수를 트리 높이로 제한하고, 그 상한을 사용자가 키 생성 시점에 고르게 했다. BPQS[22]

는 미리 정한 횟수만큼만 재사용을 허용하는 모드를 통해 소수회 사용 시 XMSS나 SPHINCS+보다 작은 서명 크기를 달성했다. XNYSS[23]는 일회용 서명 체인을 트랜잭션 체인에 결합해 블록체인의 순차적 서명 구조에 맞추려 한 시도다.

이 설계들은 사용 횟수를 제한하면 서명이 작아진다는 것을 입증했다. 문제는 그 핵심 파라미터인 허용 사용 횟수를 정하는 방식이다. 셋 모두 실측 데이터가 아니라 설계자의 가정에 기대고 있다. BPQS의 사전 생성 키 수가 대표적인 예로, 실제 재사용 분포와 무관하게 정해지므로 부족하면 키가 고갈되고 넘치면 오버헤드만 남는다. 3.1~3.3절의 실증 연구가 쌓아 온 관측 결과가 정작 이 파라미터 결정에는 쓰이지 않고 있는 것이다. 본 논문이 이 분야의 구조적 공백으로 지목하는 실증과 설계의 단절이 바로 여기서 드러난다.

Ⅳ. 비교 분석 및 연구 공백

1. 연구 간 비교

표 1은 3장에서 분석한 주요 연구들을 대상 체인, 측정 단위, 측정 지표, 키 사용 횟수 분포 제시 여부의 관점에서 비교한다.

표 1. 블록체인 키 사용 패턴 관련 주요 연구 비교

연구	범주	대상 체인	측정 단위	측정 지표	횟수별 분포
Ron & Shamir (2013) [11]	재사용 실증	비트코인	주소/엔티티	트랜잭션 그래프 통계	부분적(집계 통계)
FSI 시뮬레이션 연구 (2022) [12]	재사용 실증	비트코인	주소	연도별 재사용률	미제시
FSI 전수 분석 (2025) [13]	재사용 실증	비트코인	주소	유형별 구성비·재사용 패턴	미제시
다중체인 키 재사용 연구 (2026) [14]	재사용 실증	6개 체인	공개키	체인 내·간 재사용 건수	미제시
네트워크 과학 계열 (2021) [15]	재사용 실증	비트코인	주소/클러스터	차수·클러스터 크기 분포	간접적(멱법칙)
Aggarwal et al. (2018) [9]	노출량 측정	비트코인	프로토콜	공격 벡터 분석	해당 없음
Deloitte 분석 [16]	노출량 측정	비트코인	잔액	노출 잔액(약 25%)	미제시(이진 판정)
Quantum Horizon (2026) [17]	노출량 측정	비트코인, 이더리움	잔액/계정	노출 자산 규모	미제시(이진 판정)
이더리움 네트워크 분석 (2021) [19]	계정 활동 분포	이더리움	주소	차수 분포(99% 1회)	간접적(차수 분포)
EVM 워크로드 분석 (2026) [20]	계정 활동 분포	이더리움, Base	주소	활동 분포·자원 사용	간접적(heavy-tail)
QRL [21]	서명 설계	자체 체인	키	XMSS 트리 높이	가정(사용자 선택)
BPQS [22]	서명 설계	범용 블록체인	키	서명 크기·횟수 모드	가정(설계자 결정)
XNYSS [23]	서명 설계	범용 블록체인	키	서명 체인 길이	가정(설계자 결정)

비교를 통해 두 가지 특징이 드러난다. 첫째, 측정 단위가 주소, 잔액, 키로 서로 다르다. 주소 교체 관행으로 주소 기반 측정은 키 사용 횟수를 과소 추정할 수 있고, 잔액 기반 측정은 사용 횟수 정보를 없애며, 횟수 파악에 가장 적합한 공개키 기반 측정은 2026년에야 등장하였다. 둘째, 키 사용 횟수를 확률 분포 형태로 제시한 연구는 없다. 실증 연구들은 인접 지표를 측정하고 설계 연구들은 단순히 분포를 가정할 뿐, 이 둘을 연결하는 정식 분포 모델은 존재하지 않는다.

2. 연구 공백

위의 비교를 통해 세 가지 연구 공백을 확인할 수 있다.

첫째, 키 사용 횟수에 대한 확률 분포 모델이 부재하다. 소수회용 서명에 대한 파라미터 최적화에는 "키가 k회 사용될 확률"이 필요하다. 예를 들어, 일회성 사용, 예외적 소수회 재사용(2~5회), 장기 재사용과 같은 구간에 대한 확률을 제공해야 허용 가능한 횟수의 상한과 서명 크기 및 보안 수준의 기대 비용을 계산할 수 있다. 그러나 기존의 실증 연구는 재사용률(약 10%)이나 노출된 잔액(25%)과 같은 집계 지표에만 초점을 맞추었으며, 비트코인의 키 수준 데이터나 이더리움의 nonce 데이터를 사용하여 사용 횟수별 분포를 집계한 연구는 아직 없다.

둘째, 키 재사용의 원인을 분류하는 체계가 부재하다. 키 재사용은 단일한 현상이 아니다. 체인 포크 시 양쪽 체인에서의 서명, 트랜잭션 실패 후 재전송, RBF에 의한 수수료 갱신처럼 짧은 시간 창

안에서 끝나는 재사용이 있는가 하면, 소유권 및 지급능력 증명이나 거스름돈 주소 미사용 관행, 서비스 운영 계정처럼 장기간 지속되는 재사용도 있다. 원인에 따라 시간적 패턴과 요구 보안 수준이 다르므로, 분포 모델이 설계에 쓰이려면 원인별 분해가 선행되어야 한다. 그러나 기존 연구는 재사용을 단일 지표로 취급할 뿐이며, 원인별 발생 빈도를 정량화한 연구는 확인되지 않는다.

셋째, 실증 연구와 설계 사이의 단절이다. 3.4절에서 보았듯 QRL, BPQS, XNYSS 등 소수회 사용을 전제한 설계들은 허용 사용 횟수를 실측 근거 없이 정한다. 실증 연구 쪽도 사정은 같다. 서명 설계가 어떤 지표를 요구하는지 고려하지 않은 채 측정 대상을 고르기 때문에, 소수회 전제가 실제 사용 패턴에 부합하는지, 부합한다면 어떤 파라미터가 최적인지에 대한 근거가 어느 쪽에서도 나오지 않고 있다.

3. 향후 연구 방향

이러한 공백을 메우기 위한 연구는 아래와 같이 세 단계로 이루어질 수 있다.

1단계는 키 사용 횟수 분포를 측정하는 것이다. 이더리움에서는 모든 계정의 nonce를 집계하는 것만으로 정확한 사용 횟수 분포를 얻을 수 있으므로 비용이 상대적으로 낮다. 비트코인에서는 주소 수준이 아닌 공개키 수준에서 서명 이력을 추적해야 하므로, 2026년 다중체인 연구[14]에서 제시한 키 수준 추적 방법론을 횟수 집계로 확장하는 접근이 유효하다. 측정 결과는 일회성, 소수회(2~5회), 장기 재사용의 구간별 확률과 분포의 함수형(멱법칙 여부 등)으로 정리해야 한다.

2단계는 재사용 시나리오의 정형화이다. 측정된 재사용 사례는 원인별로 분류하고, 각 시나리오의 발생 빈도, 시간적 특성, 요구 보안 수준을 정의하여 블록체인 전자서명 사용 모델을 구축한다. 이 모델은 특정 서명 기법에 구애받지 않으므로, 이후 다양한 양자내성 서명 연구에서 활용할 수 있는 평가 기준으로 기능할 수 있다.

3단계는 분포 기반 서명 설계이다. 실측 분포와 사용 모델이 확보되면 소수회용 서명의 파라미터 최적화가 가능해진다. 예컨대 HORSIC+[5]와 같은 FTS의 허용 횟수를 실측 상위 구간(2~5회)에 맞추면, 2^{64}회 서명을 전제로 7,856바이트를 소비하는 SPHINCS+와 달리 실제 위험에 필요한 만큼만 서명 크기를 지불하게 된다. 상태 관리도 같은 논리로 선택적으로 적용할 수 있다. 대다수를 차지하는 일회성 사용은 무상태로 처리하고, 예외적 재사용에만 제한적 상태 관리를 두는 것이다. 설계의 평가는 서명 크기 단독이 아니라 온체인 누적 서명 비용, 블록당 수용 트랜잭션 수 같은 시스템 지표로 이루어져야 한다.

V. 결론

본 논문은 블록체인 키 사용 패턴에 관한 연구들을 네 범주로 분류하고 측정 단위, 대상 체인, 측정 지표의 관점에서 비교하였다. 분석의 결론은 두 가지다. 대다수 키가 극소수 횟수만 사용된다는 사실은 범주를 가리지 않고 일관되게 확인되지만, 그 증거는 서명 설계에 쓸 수 있는 형태로 존재하지 않는다. 키 사용 횟수의 확률 분포 모델과 재사용 원인의 분류 체계가 없고, 실증 연구와 설계 연구가 서로를 참조하지 않기 때문이다. 이 공백을 메우는 경로로 분포 실측에서 사용 모델 정형화를 거쳐 파라미터 최적화에 이르는 단계적 연구를 제안하였다. 서명 크기가 곧 수수료와 처리량으로 이어지는 NFT와 콘텐츠 서비스 환경에서, 실측에 근거한 소수회 서명 설계는 양자내성 전환의 온체인 비용을 낮추는 실질적 수단이 될 것이다.

REFERENCES

[1] NIST, "Stateless Hash-Based Digital Signature Standard," *Tech. Rep., FIPS 205*, Aug. 2024.

[2] D.J. Bernstein, A. Hülsing, S. Kölbl, R. Niederhagen, J. Rijneveld, and P. Schwabe, "The SPHINCS+ Signature Framework," *Proc. of ACM SIGSAC Conference on Computer and*

Communications Security (CCS), pp. 2129-2146, Nov. 2019.
[3] L. Lamport, "Constructing Digital Signatures from a One-Way Function," *Tech. Rep.*, No. SRI-CSL-98, Oct. 1979.
[4] L. Reyzin and N. Reyzin, "Better than BiBa: Short One-Time Signatures with Fast Signing and Verifying," *Proc. of Australasian Conference on Information Security and Privacy (ACISP)*, pp. 144-153, Jul. 2002.
[5] J. Lee and Y. Park, "HORSIC+: An Efficient Post-Quantum Few-Time Signature Scheme," *Applied Sciences*, vol. 11, no. 16, 7350, 2021.
[6] A. Hülsing, D. Butin, S. Gazdag, J. Rijneveld, and A. Mohaisen, "XMSS: eXtended Merkle Signature Scheme," *Tech. Rep., IETF RFC 8391*, May 2018.
[7] D. McGrew, M. Curcio, and S. Fluhrer, "Leighton-Micali Hash-Based Signatures," *Tech. Rep., IETF RFC 8554*, Apr. 2019.
[8] D. Cooper, D. Apon, Q. Dang, M. Davidson, M. Dworkin, and C. Miller, "Recommendation for Stateful Hash-Based Signature Schemes," *Tech. Rep., NIST SP 800-208*, Oct. 2020.
[9] D. Aggarwal, G.K. Brennen, T. Lee, M. Santha, and M. Tomamichel, "Quantum Attacks on Bitcoin, and How to Protect Against Them," *Ledger*, vol. 3, pp. 68-90, 2018.
[10] Chaincode Labs, "Bitcoin and Quantum Computing: Current Status and Future Directions," *Tech. Rep.*, 2025. https://chaincode.com/bitcoin-post-quantum.pdf (accessed Jul., 8, 2026).
[11] D. Ron and A. Shamir, "Quantitative Analysis of the Full Bitcoin Transaction Graph," *Proc. of Financial Cryptography and Data Security (FC)*, pp. 6-24, Apr. 2013.
[12] Y. Gong, K.P. Chow, S.M. Yiu, and H.F. Ting, "Sensitivity Analysis for a Bitcoin Simulation Model," *Forensic Science International: Digital Investigation*, vol. 43, 301449, 2022.
[13] Y. Gong, K.P. Chow, and S.M. Yiu, "Improved Bitcoin Simulation Model and Address Heuristic Method," *Forensic Science International: Digital Investigation*, vol. 53, 301935, 2025.
[14] R. Stütz, N. Stifter, M. Dragaschnig, B. Haslhofer, and A. Judmayer, "Reuse of Public Keys Across UTXO and Account-Based Cryptocurrencies," *Proc. of Financial Cryptography and Data Security (FC)*, 2026.
[15] J.A. Fischer, A. Palechor, D. Dell'Aglio, A. Bernstein, and C.J. Tessone, "The Complex Community Structure of the Bitcoin Address Correspondence Network," *Frontiers in Physics*, vol. 9, 681798, 2021.
[16] I. Barmes and B. Bosch, Quantum Computers and the Bitcoin Blockchain(2020). https://www.deloitte.com/nl/en/services/consulting-risk/perspectives/quantum-computers-and-the-bitcoin-blockchain.html (accessed Jul., 8, 2026).
[17] I.M. Gershteyn and J.A. Alber, "Quantum Horizon: An Evaluation of Quantum Computing as a Threat to Bitcoin and Ethereum," *arXiv preprint*, arXiv:2606.14484, 2026.
[18] Post-Quantum Ethereum(2025). https://pq.ethereum.org/ (accessed Jul., 8, 2026).
[19] A. Said, M.U. Janjua, S.U. Hassan, Z. Muzammal, T. Saleem, T. Thaipisutikul, S. Tuarob, and R. Nawaz, "Detailed Analysis of Ethereum Network on Transaction Behavior, Community Structure and Link Prediction," *PeerJ Computer Science,* vol. 7, pp. e815, 2021.
[20] L. Heimbach, K. Babel, and J. Milionis, "EVM Workloads in the Wild: Evidence for Multi-Dimensional Gas Metering, State Growth, Delayed Execution, and Parallelism," *arXiv preprint*, arXiv:2606.19869, 2026.
[21] P. Waterland, "The Quantum Resistant Ledger (QRL)," *Tech. Rep.*, 2016.
[22] K. Chalkias, J. Brown, M. Hearn, T. Lillehagen, I. Nitto, and T. Schroeter, "Blockchained Post-Quantum Signatures," *Proc. of IEEE International Conference on Blockchain*, pp. 1196-1203, Jul. 2018.
[23] W. van der Linde, "Post-Quantum Blockchain Using One-Time Signature Chains," *Research Report*, Radboud University, 2018.

저 자 소 개

이재흥(정회원)
2001년 서울대학교 컴퓨터공학부 학사 졸업.
2003년 서울대학교 전기·컴퓨터공학부 석사 졸업.
2013년 서울대학교 전기·컴퓨터공학부 박사 졸업.
2016년~2023년 대전대학교 정보보안학과 부교수.
2024년~ 경기대학교 AI컴퓨터공학부 부교수.
<주관심분야 : 정보 보안, 시스템 보안, 인공 지능, 분산 처리 시스템>