PQ-PoRR

: 라운드 로빈 기반 양자 내성 블록체인 합의 알고리즘

김원웅*, 강예준*, 김현지*, 오유진* 서화정 *†
*한성대학교 대학원 IT융합공학부

요 약

● 양자 컴퓨터의 발전으로 인한 기존 블록체인의 **양자 위험성** 대두

● **Round-Robin** 기반 알고리즘을 통해 **공정한 블록 생성 기회** 제공

● **CRYSTALS-Dilithium** 적용을 통한 **양자 보안성** 제공

PQ-PoRR

1) 모든 노드로부터 **무작위 값** 생성

2) 이전 블록의 생성자에게 전송

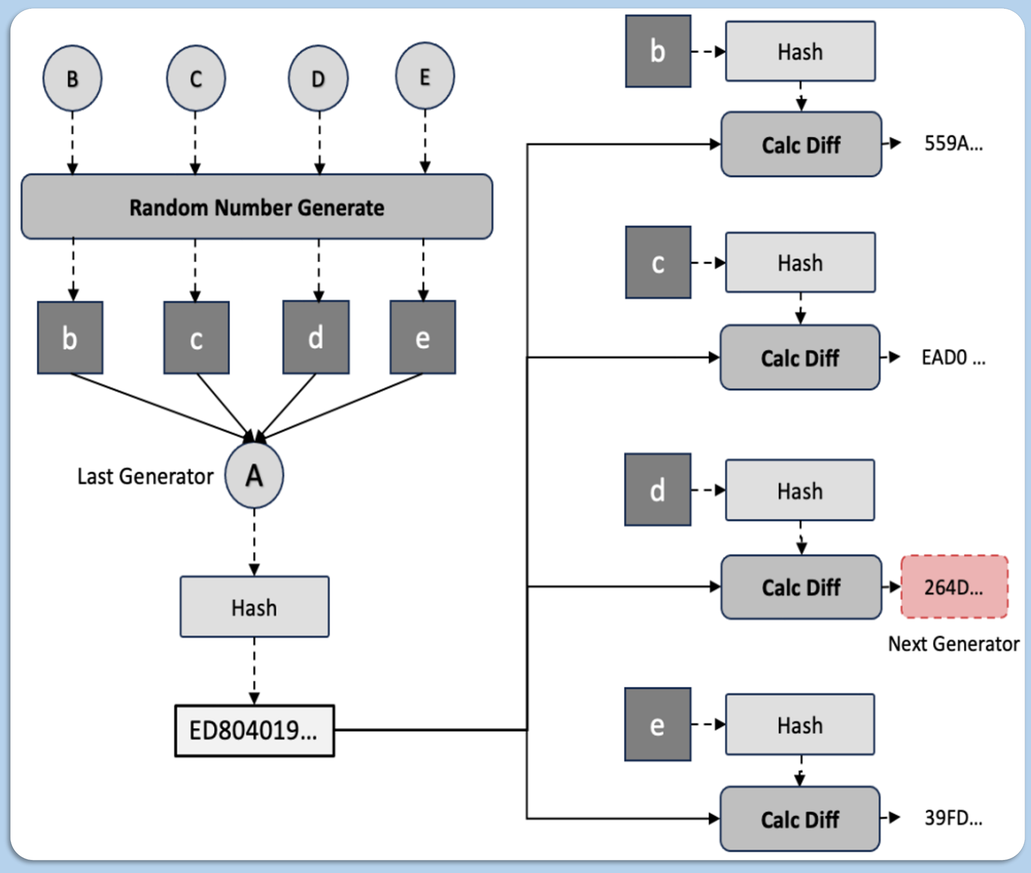
3) 전송 받은 무작위 값을 연접하여 **해시 함수의 입력값**으로 사용

4) 각 노드들의 랜덤 값을 **해시한 값과 비교**

5) **가장 적은 차이**를 갖는 노드가 다음 블록 생성자로 선정

6) 해당 라운드에 생성한 적이 있는 노드는 **생성자 후보에서 제외**

7) **모든 노드가 동일한 블록 생성 횟수를 가질 때까지** 1) ~ 6) 반복



성능 지표

- TPS(Transaction Per Second): 1초 동안 처리된 트랜잭션의 수
- Latency: 트랜잭션이 네트워크에 나타나고 검증되기까지의 시간

TPS

● 노드의 수가 증가함에 따라 **성능 저하**

→ 검증 횟수가 기하급수적으로 증가하기 때문

● Dilithium을 적용하였을 때 ECDSA 보다 낮은 성능

→ **서명 및 키 사이즈 때문**

→ 그러나, **양자** 내성을 보장

→ Latency 향상을 통해 극복

N	ECDSA	Dilithium
2^1	2068.8	1366.1
2^2	692.3	277.5
2^3	293.9	163.1
2^4	136.7	55.8
2^5	61.5	16.8
2^6	26.2	4.7
2^7	9.3	1.1

Latency

● TPS와 마찬가지로 노드가 증가함에 따라 **성능 저하**

● Dilithium을 적용하였을 때 **ECDSA 보다 높은 성능**

→ Dilithium의 **실행속도가 ECDSA에 비해 빠르기 때문**

→ **실시간성이 중요한 IoT 분야에서 실용적**

N	ECDSA	Dilithium
2^1	0.048	0.004
2^2	0.144	0.021
2^3	0.340	0.036
2^4	0.731	0.107
2^5	1.625	0.356
2^6	3.816	1.272
2^7	10.649	5.399