비트코인의 고속 블록 생성을 위한 타임스탬프 탐색 양자 회로 설계

오지수, 박영훈*
숙명여자대학교

lucy27@sookmyung.ac.kr, *yh.park@sookmyung.ac.kr

Design of a Quantum Circuit for Searching Timestamp To Accelerate Bitcoin Block Generation

Oh Jisoo, Park Younghoon*
Sookmyung Women's University

요 약

본 연구는 비트코인 블록 생성의 가속화를 위해 블록 헤더에서 타임스탬프를 확장된 탐색 공간으로 활용하는 양자 회로 설계 방안을 제시한다. 타임스탬프의 가변 범위를 합의 규칙 내에서 최대 2 시간 후까지 설정하고, 이를 통해 확보된 탐색 공간을 nonce 와 결합하여 양자 컴퓨터가 병렬 연산을 수행하도록 하였다. 제안된 회로는 Grover 알고리즘을 적용하여 비트코인 채굴의 효율성을 증대시키고 채굴 과정에서 필요한 컴퓨팅 자원 및 전력 소모를 감소하는 데 기여할 것으로 기대된다.

Ⅰ. 서 론

블록체인 기술은 탈중앙화된 신뢰 구조를 제공함으로써 금융, 데이터 관리, 공급망 추적, DID 등 다양한 분야에서 폭넓게 활용되고 있다. 블록체인에서 블록을 생성하는 과정을 합의 알고리즘이라고 하며, 블록체인에서 가장 중요한 역할을 담당하고 있다. 현재 매우 많은 합의 알고리즘들이 개발되었지만, 비트코인을 포함한 작업증명(Proof of Work) 기반 블록체인이 여전히 가장 많이 거래되고 있다. 비트코인의 블록 생성을 위해 전 세계에서 채굴(Mining)[1]을 시도하고 있지만, 채굴을 위한 과정은 엄청난 컴퓨팅 자원과 전력을 요구하기에, 채굴 과정에서 환경 문제는 블록체인 기술이 해결해야 할 도전 과제 중 하나이다.

최근 양자 컴퓨터 기술의 급속한 발전은 기존 작업증명 채굴 방식의 효율성을 극대화하는 새로운 대안으로 주목받고 있다. 양자 컴퓨터는 중첩과 얽힘 등 양자역학 특성을 기반으로 하여, 현재 디지털 컴퓨터 연산 체계로는 효율적인 처리가 어려운 문제를 해결할 잠재력을 지니고 있다. 특히 Grover 양자 탐색 알고리즘[2]은 크기 N 의 무작위 탐색 문제에서 고전 알고리즘 대비 약 $O(N)$의 시간 복잡도 우위를 제공한다. 따라서, Grover 알고리즘은 해시함수의 역상(pre-image) 값을 효율적으로 찾는 데 활용할 수 있으며, 이를 바탕으로, 작업증명 블록체인의 채굴 과정에도 적용할 수 있다.

이에 따라 비트코인 채굴에 양자 컴퓨팅 기술을 적용하는 연구가 진행되어 왔다. 기존 작업증명 기반 블록체인 채굴에 양자 컴퓨팅 기술을 적용하는 연구는 헤더 nonce 및 extra nonce 와 같이 채굴자가 직접 제어 가능한 핵심 입력 변수를 효율적으로 탐색하는 데 주력해 왔다. Benkoczi 등이 수행한 연구[3]에서는 블록 헤더의 가변 필드를 양자 회로에 도입하여 Grover 양자 탐색 알고리즘을 비트코인 채굴에 통합하고자 하였다. 그러나 이러한 양자 채굴 알고리즘들은 양자 연산의 대상이 되는 가변 필드(Nonce, Extra nonce)를 탐색하는 과정에서, 여전히 타임스탬프 조정과 같은 연산에서 고전 컴퓨터와 양자 컴퓨터 간의 연산을 반복적으로 전환하는 등 비효율적인 연산 흐름을 내포하고 있어, 양자 컴퓨팅의 병렬성을 충분히 활용하지 못하는 한계가 존재한다.

본 연구는 블록 헤더의 입력값 중 상대적으로 부차적 요소로 다루어졌던 타임스탬프(Timestamp)를 새로운 탐색 공간으로 확장하는 방안을 제안한다. 타임스탬프의 가변 범위를 합의 규칙을 만족하도록 설정하고, 이를 nonce 와 결합한 확장된 탐색 공간에 대해 Grover 기반 양자 탐색을 적용하여 채굴 효율성을 증대시키는 양자 회로 설계에 초점을 맞춘다.

Ⅱ. Timestamp 가변 범위 설정

블록체인의 타임스탬프 합의 규칙을 준수하기 위하여, 본 연구에서는 양자 회로가 조작할 수 있는 타임스탬프의 가변 범위를 현재 시각부터 최대 2 시간 후까지로 제한하였다.

현재 시각과 2 시간 후의 시각을 UNIX epoch time 으로 환산하여 이진 표현으로 나타내면 상위 20 비트들은 고정되어 있으며, 변화가 발생하는 것은 하위 약 12 비트이다. 즉, 타임스탬프 범위 내에서 가능한 값들은 약 2^{12}개의 조합이 유효한 타임스탬프로 허용될 수 있다.

이러한 추가 탐색 공간은 양자 회로가 병렬적으로 탐색할 수 있는 후보 해시 입력값의 수를 확장한다.

Ⅲ. 양자 회로

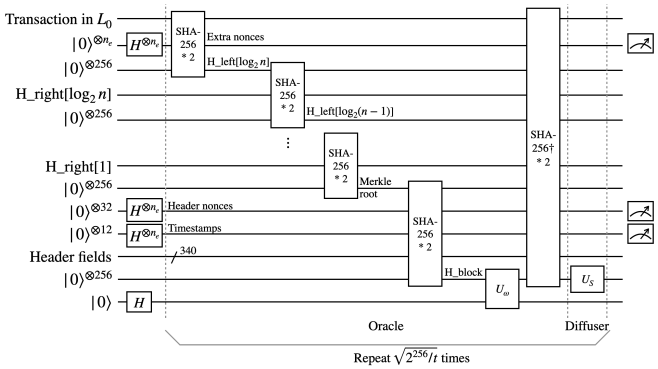

그림 1. 타임스탬프 가변 양자 회로

양자 회로는 크게 머클 트리의 가변 노드 계산 회로와 최종적으로 블록 해시를 산출하고 Grover 탐색을 적용하는 PoW 연산 회로로 구성된다.

머클 트리는 이진 트리 구조로, 각 리프 노드는 개별 트랜잭션의 해시값으로 구성되며, 상위 부모 노드는 두 자식 노드의 해시값을 결합해 생성된다. 따라서 채굴 과정에서 extra nonce 를 갱신하면, 최좌측 리프 노드(L_0)에서 머클 루트까지의 경로에 있는 노드들은 갱신되지만, 그 외 노드들은 갱신되지 않기에 불변 노드들은 기존의 고전 컴퓨터에서, 가변 노드는 양자 컴퓨터에서 계산하도록 회로를 설계하였다.

머클 트리의 가변 노드 계산 회로는 extra nonce 를 포함하는 L_0 부터 머크 루트 까지의 경로상 해시값을 병렬적으로 계산한다. 그림 1 과 같이 고전 컴퓨터로 미리 계산된 머클 트리의 불변 노드 해시값들 $\mathrm{H\_right}[\log_2 n], \ldots, \mathrm{H\_right}[1]$, extra nonce, 해시값을 저장할 추가 큐비트를 회로의 입력값으로 설정한다. 여기서 n_e 는 extra nonce 의 길이이며, $\mathrm{H\_left}[\log_2 n]$ 은 레벨이 $\log_2 n$ 인 가변 노드의 해시값을 의미한다. $\mathrm{H\_right}[\log_2 n]$ 는 불변 노드 중 레벨이 $\log_2 n$ 인 가변 노드의 바로 우측에 위치하는 노드의 해시값을 의미한다.

extra nonce 입력 레지스터에 Hadamard 게이트를 적용하여 extra nonce 의 가능한 모든 이진값의 균일한 중첩 상태를 준비한다. 준비된 중첩상태는 이를 L_0 트랜잭션과 함께 SHA-256 이중 해시 함수를 통과하여 머클 트리의 최하위 가변 노드 해시값 $\mathrm{H\_left}[\log_2 n]$ 을 얻는다. 이후, 이미 계산해둔 L_1 의 해시값과함께 해시함수를 통과시켜 $\mathrm{H\_left}[\log_2(n-1)]$ 를 구한다. 이와 같은 연산을 $\log_2 n$ 번 반복하면 최종적으로 머클루트 값을 산출하는 회로를 설계하였다.

블록의 해시값을 구하기 위해, 이전 단계에서 산출된 Merkle root, 12 비트의 가변 범위를 가진 timestamp , 32 비트 header nonce, 그리고 그 외 헤더 필드(340 비트)들을 회로의 입력으로 설정한다. header nonce 와 timestamp 역시도 Hadamard 게이트를 통과하여 각각 가능한 모든 이진값들의 균일한 중첩 상태를 준비함으로써, 기존 nonce 들과 timestamp 가 결합한 확장된 탐색 공간에 대해 병렬 연산이 가능하도록 한다. 이 중첩 상태의 입력값을 SHA-256 이중 해시 함수를 통과시켜 블록의 해시값인 $\mathrm{H\_block}$ 을 산출할 수 있다. 산출된 해시값으로 Grover Algorithm 의 조건부 위상 반전 연산 U_ω 를 수행하도록 한다. 블록의 해시값이 target 값보다 작은 경우 위상을 반전시키는 역할을 수행한다.

U_ω 연산이 완료된 후, 해시 계산에 사용되었던 보조 큐비트들을 초기 상태로 되돌리고 재사용하기 위해 SHA-256 의 역연산(SHA-256†)을 수행한다. 이 역연산은 해시 함수의 계산 흐름을 역순으로 따라가며, 보조 큐비트들을 초기 상태로 복구한다. 만약 이러한 역연산을 생략할 경우, 매 반복 시마다 새로운 큐비트를 할당해야 하므로 전체 양자 회로에 요구되는 큐비트 수가 급증한다. 따라서 회로의 효율성과 자원 최적화를 위해 필수적이다. 이후, 진폭 연산 U_S 가 수행되고, 그림 1 과 같이 Oracle 과 Diffuser 연산을 포함한 Grover Algorithm 이 총 $\sqrt{2^{256}/t}$번 반복 수행된다.

Ⅳ. 결론 및 향후 연구

본 연구는 블록 헤더의 불변 부분을 고전 계산으로 분리하여 양자 회로의 자원(qubit 및 gate) 소모를 줄이고, 12 비트 가변 범위의 타임스탬프를 확장된 탐색 공간으로 통합함으로써 Grover 알고리즘의 제곱근 수준 탐색 가속을 PoW 채굴에 효율적으로 적용할 수 있는 양자 회로 설계 방안을 제시하였다. 제안된 회로는 header nonce, extra nonce 와 더불어 타임스탬프의 가능한 모든 입력값의 중첩 상태를 준비하여, 양자 컴퓨터가 이 확장된 공간에 대해 병렬적으로 해시 연산을 수행하도록 설계되었다.

향후 연구는 제안된 양자 회로의 정량적인 성능 검증을 목표로 한다. 현존하는 양자 시뮬레이터 또는 하드웨어에서 회로를 구현하여 큐비트 수, 게이트 깊이, 연산 시간 등 구체적인 성능 지표를 확보하고, 고전 채굴 방식과의 속도 우위를 명확히 입증하고자 한다.

ACKNOWLEDGMENT

본 논문은 2025 년도 과학기술정보통신부 및 정보통신기획평가원의 ‘SW 중심대학사업’ 지원을 받아 (제작, 구축, 설치, 확보 등) 되었습니다. (2022-0-01087)

참 고 문 헌

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.

[2] L. K. Grover, "A fast quantum mechanical algorithm for database search," in Proc. of Twenty-Eighth Annual ACM Symposium on Theory of Computing, pp. 212-219.

[3] R. Benkoczi, D. Gaur, N. Nagy, M. Nagy, and S. Hossain, "Quantum Bitcoin Mining," Entropy, Vol. 24, no. 3, pp. 323, 2022.