암호 화폐에 대한 동향 연구: 비트코인 및 양자 컴퓨팅을 대비하는 가상화폐 기반

노융두, 최지호, 강홍철, 유민재, 원유재*
충남대학교 컴퓨터공학과
yoongdoo0819@naver.com, cheekorkind@naver.com, khc7362@gmail.com,
vicerascal@cnu.ac.kr, yjwon@cnu.ac.kr
*Corresponding author : Yoojae Won

A Study on Trends in Cryptography: Virtual Currency Based on Bitcoin and Quantum Computing

Yoongdoo Noh, Jiho Choi, Hongcheol Kang, Minjae Yoo, Yoojae Won
Dept of Computer Engineering, Chungnam National University

요 약

올해 초, 구글(Google)이 SHA-1의 충돌 현상을 입증했다. 이것은 모든 타 암호 알고리즘 역시 안전할 수 없다는 것을 뜻하며, 향후 SHA-256을 사용하는 비트코인도 취약해질 수 있음을 의미한다. 이유인즉슨, 비트코인에서 사용되는 암호 및 해시 알고리즘은 답을 찾기 위해 상당한 시간이 소요되지만, 양자 컴퓨터의 큐비트를 바탕으로 하는 연산처리 능력은 그 시간을 대폭 감소시킬 수 있기 때문이다. 본 논문에서는 이와 같은 양자 컴퓨터가 비트코인에 얼마나 위협적일 수 있는지와 더불어 양자 컴퓨터 출현에 대비하고자 등장한 새로운 암호 화폐인 Byteball 및 QRL코인을 살펴보고자 한다.

1. 서론

비트코인은 대표적으로 두 가지 암호 알고리즘을 사용한다. 첫 번째는 거래자들의 거래를 위한 타원곡선 암호(Elliptic Curve Cryptography) 알고리즘이며, 두 번째는 작업 증명(Proof of Work)을 위한 SHA-256 해시 알고리즘이다. 암호 화폐에서 이러한 암호 기법은 굉장히 중요한데, 이러한 알고리즘을 적용하기 때문에 가상화폐로서의 가치를 가질 수 있기 때문이다.

그러나 올해 초, SHA-256의 이전 버전인 SHA-1이 뚫렸으며, 향후 양자 컴퓨터의 시대가 도래함에 따라 큐비트의 '중첩'과 '얽힘'의 특성을 이용한 연산 능력은 기존 암호 체계 및 비트코인을 위협하는 데 충분할 것으로 보여진다. 그에 따라 양자 컴퓨팅을 대비한 'post-양자 암호(해시 기반 암호, 격자 기반 암호, 부호 기반 암호)'에 대한 연구가 이루어지고 있으며, 해당 암호를 기반으로 하는 새로운 암호 화폐도 출현하고 있다.

본 논문에서는 현재 존재하는 수많은 암호 화폐 중 가장 많은 관심을 받는 비트코인을 토대로, 비트코인에서 사용되는 암호 알고리즘에 관해 설명한다. 또한 관련된 암호들이 양자 컴퓨팅에 취약할 수 있기 때문에 새롭게 등장하고 있는 암호 화폐인 Byteball과 QRL코인을 살펴본다.

2. 관련 연구

2.1. 타원 곡선 암호 알고리즘

비트코인을 이용한 거래는 기존의 방식과 다소 차이가 있다. 이루어지는 모든 거래가 검증받고 블록체인에 포함되기 위해서는 디지털 서명이 필요하며, 해당 서명에 필요한 것이 공개키와 개인키 암호 방식이다. 개인키는 무작위로 추출된 숫자로 구성되어 있으며(4비트씩 64개의 16진수로 표현된 수, 2^256)[1], 공개키는 구해진 개인키를 타원곡선 암호 알고리즘에 적용하여 생성한다.

타원곡선 암호는 이산 대수 문제의 어려움을 이용한 것이다. 예를 들면, K = k * G라는 식에서 K는 공개키, k는 개인키, G는 상수이다. 즉 미리 정의한 개인키와 상수를 곱한 결과가 공개키가 된다. k를 알고 있다면 G를 곱하여 K를 쉽게 계산할 수 있다. 그러나 K만 알고 있는 상태에서 k를 찾는다는 것은 대입할 수 있는 모든 값을 고려해야하기 때문에 굉장히 어려워진다. 결론적으로, 거래자들이 거래하는 시점에 타인에게 표출되어도 괜찮은 공개키 주소가 다른 사람으로부터 코인을 전송받을 때 사용되고, 자신의 코인을 상대방의 공개키 주소로 전송할 때 해당 코인이 자신의 것임을 입증하기 위한 서명으로써 개인키가 사용된다.

2.2. 작업증명 알고리즘

P2P 네트워크를 제공하는 비트코인에서 모든 노드는 중앙 관리자 없이 코인을 전송하고, 거래가 유효한지 인증해야 한다. 즉 모든 노드는 특정 시간 동안 승인된 모든 거래를 블록 안에 포함시키고, 블록을 완성해야 한다. 완성된 블록은 비트코인 네트워크에서 모두에게 공유되기 때문에, 결과적으로 모든 거래 기록을 가지고 있는 분산 장부인 블록체인은 무결성을 제공할 수 있게 되는 것이다. 이렇게 위와 같이 블록을 생성하는 과정(채굴)이 필요하며, 이 과정에는 '작업증명'이라고 불리는 합의 알고리즘이 적용된다.

작업증명 알고리즘에는 일방향성을 가지는 해시 함수인 SHA-256 암호화 알고리즘이 사용된다. 작업증명은 새로 생성하려는 블록의 헤더부분을 SHA-256으로 해시하여(블록 해시값) 출력된 값이 특정 목표치 값보다 작은 값이 나올 때 까지 Nonce(블록 헤더에 포함되어 있는 변수)의 값을 지속적으로 변경시키며 답을 찾아내는 알고리즘이다. 특정 목표치 값보다 작은 값을 찾아낸다면 블록을 생성하는 데 성공한 것이다.

2.3. 양자 컴퓨터

양자 컴퓨터는 큐비트라는 양자 비트를 사용한다. 에너지의 최소 단위를 뜻하는 양자를 이용하는 큐비트는 상태를 중첩시키고, 둘 이상의 큐비트를 얽히게 할 수 있기 때문에, 기존의 컴퓨터가 작업을 순차적으로 처리하는 데 반해 양자 컴퓨터는 동시에 수행할 수 있게 되었다.

고전적인 컴퓨터에서의 비트는 0 아니면 1의 상태를 가질 수 있다. 그러나 '중첩'현상에 의해 큐비트는 0과 1의 상태를 동시에 취할 수 있게 되었고, 또한 두 개의 양자는 거리에 무관하게 서로 연결되어 있기 때문에 하나의 상태가 다른 양자의 상태에 영향을 미치게 된다. 즉 양자의 상태가 1이면 다른 양자도 1이 되며(1, 1), 또한 반대도 가능하다(1, 0). 이러한 '중첩' 현상과 '얽힘' 현상에 의하여 두 개의 큐비트가 얽히게 되면, 두 개의 큐비트가 동시에 표현할 수 있는 상태는 총 4가지(00, 01, 10, 11)가 된다.

양자의 이러한 특성 때문에 큐비트의 개수(n)를 증가시킬 때마다 상태의 수는 2의 지수 단위로 증가하게 되며[2], 결국 기존 컴퓨터보다 월등한 처리능력을 가질 수 있는 것이다.

3. 양자 컴퓨팅을 대비하는 화폐

올해 초, 구글(Google)이 SHA-1의 충돌 현상을 입증했으며, 연산 횟수는 약 922경(9,223,372,036,854,775,808)번에 달한다. 비트코인에서 사용되는 SHA-256은 256비트의 해시 출력 값을 생성하는 데 반해 SHA-1 해시 알고리즘은 160비트의 해시 값을 생성한다. 즉 SHA-1보다 훨씬 긴 비트수를 가지기 때문에 현재 SHA-256은 안전하지만, 그러나 양자 컴퓨터의 상용화 및 큐비트 증가에 따라 미래에까지 안전하다고는 할 수 없는 것이다

양자컴퓨터 개발 현황 자료: <사이언스> 2016.12.2

	초전도 회로(루프)	이온 덫	다이아몬드 접결합	위상학 큐비트
주요 개발기관	구글, IBM 등	아이온큐(ionQ) 등	퀀텀다이아몬드테크 등	마이크로소프트 등
최대 큐비트	9	14	6	입증 안 됨
유지 시간(초)	0.00005	최대 1000	10	입증 안 됨
논리 성공률(%)	99.4	99.9	99.2	입증 안 됨
장점/단점	빠른 작동, 기존 반도체산업 기반 / 극저온 환경 조건	안정성, 신뢰성 / 느린 작동, 많은 레이저들 필요	상온 작동 / 양자얽힘 구현 난점	오류 대폭 감소 가능 / 아직 입증 안 됨

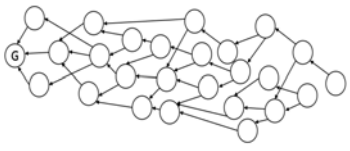
<표 1> 양자 컴퓨터 개발 현황

<표 1>에서 보는 것과 같이 큐비트의 개발은 꾸준히 진행되는 중이다. 향후 큐비트의 개수가 54개를 넘어서면 초당 1경 이상의 상태를 갖게 된다. 즉 SHA-1 알고리즘의 충돌 현상을 발견하는 데 수 분이 채 안 걸린다는 것이다. 물론 SHA-256은 SHA-1보다 훨씬 더 걸리겠지만 앞서 말했듯이 안심할 수는 없는 것이다.

비트코인에서 사용하는 타원곡선 암호와 SHA-256 해시함수는 양자 컴퓨팅 연산에 취약한 알고리즘이다. 혹여나 비트코인의 암호 및 해시 알고리즘이 양자 컴퓨팅 때문에 뚫리게 된다면 공개키 주소를 더 이상 사용할 수 없을 것이며, 채굴 과정 중 적용되는 작업증명 알고리즘 역시 '합의'라는 개념이 무너져 이용할 수 없게 될 것이다.

3.1. Byteball & QRL 코인

비트코인의 암호 알고리즘에 대한 이러한 우려 때문에 이미 양자 컴퓨팅을 대비하는 'Byteball 코인'이 구현되었다. Byteball은 비트코인과 달리 기본 구조가 다르다.



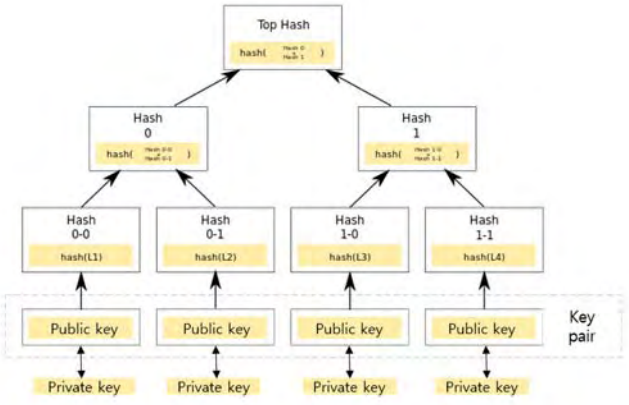
(그림 1) DAG 구조

비트코인은 하나의 체인만 유지하는 블록체인 기술을 사용하고 지속적으로 블록을 생성하기 위해 작업증명 알고리즘을 통한 채굴 과정을 행한다. 그러나 Byteball은 블록체인을 사용하지 않고 (그림 1)처럼 DAG(Directed Acyclic Graph)를 사용하기 때문에 채굴 과정이 존재하지 않는다.[3] 대신 모든 unit들이 서로 협력 관계에 있기 때문에, 거래가 이루어지는 즉시 임의의 노드가 거래를 승인해준다. 또한 비트코인에서는 블록이 이전 블록의 해시만 참조하는

반면, Byteball은 생성된 unit이 부모 unit의 해시값을 참조 및 확인 하고, 해당 부모의 조상 unit까지 순차적으로 모두 확인하는 구조이다. 만약 unit을 변경시키려면 해시값까지 변경시켜야 하기 때문에, 부모를 참조하는 순차적인 모든 자식 unit들의 해시 값 역시 변경되어야 한다.

즉 DAG 구조는 기존보다 더욱더 안전성을 제공할 뿐만 아니라 추가적인 장점으로는 이중 지불 문제 해결 및 블록을 생성하지 않기 때문에, 채굴을 위한 컴퓨팅 소모도 없앨 수 있으며, 또한 모든 거래들이 동시에 생성되고 승인받을 수 있다는 점이다.

Byteball 외에 'Quantum Resistant Ledger'의 의미를 갖는 QRL 코인도 존재한다. QRL 코인의 암호 알고리즘은 양자 컴퓨팅을 대비한 'post-양자 암호'(해시 기반 암호, 부호 기반 암호, 격자 기반 암호 등)를 사용하는데, 이 중 일회성 해시 기반 암호를 사용한다. 일회성 서명은 한 번의 거래에 대해서는 만족스럽지만, 그러나 거래가 이루어질 때마다 모든 화폐가 옮겨져야 되는 문제점이 있다. 그것을 해결하기 위한 방안으로 QRL 코인은 머클 트리를 사용한다.[4]



(그림 2) 여러 개의 public key로 구성한 머클 트리

(그림 2)과 같이 QRL 코인에서의 머클 트리를 만드는 방법은 미리 생성한 여러 개의 키 쌍(공개키-기본키)들 중 공개키를 해싱하여 터미널 노드를 생성하고, 머클 루트를 만들 때까지 해싱한 노드들을 반복 작업하는 것이다. 즉 여러 개의 키 쌍을 해싱하고 묶어 일회성을 탈피하고자 하는 방법이다.

그러나 이렇게 머클 트리를 구성하려면, 생성한 키만큼의 서명만 유효하기 때문에 추가적인 작업이 들어가고, 머클 트리의 높이만큼 키가 필요하기 때문에 여러 개의 키 쌍들을 미리 생성해야만 하는 단점이 있다.

이처럼 post-양자 암호 및 암호 화폐에 대한 개발이 현재 확립된 것은 아니며, 양자 컴퓨터 역시 마찬가지이다. 양자 컴퓨터가 상용화된다면 에너지, 기후 예측, 신약 개발 등 다양한 긍정적인 측면이 예상되지만, 그러나 상상을 초월하는 연산 속도는 암호 체계를 무너뜨릴 수 있기 때문에, 그에 대비한 'post-양자 암호'에 대한 연구와 암호 화폐에 대한 연구도 지속적으로 이루어져야 할 것이다.

4. 결론

본 논문에서는 양자 컴퓨터가 도래하면 취약할 수 있는 비트코인의 암호체계를 살펴보았다. 또한 이산 대수의 어려움을 이용한 ECC 혹은 해시 알고리즘인 SHA-256에 대하여 양자 컴퓨팅 연산을 적용하면 비트코인 시스템이 무너질 수 있기 때문에, 그에 대비하는 암호 화폐들의 출현도 살펴보았다.

비트코인이 사상 첫 암호 화폐로써의 가치는 존재하지만, 여러 단점도 존재하듯이 현재 출현하는 양자 컴퓨팅을 방어하기 위한 암호 화폐들 역시 완벽할 수는 없을 것이다. 양자 컴퓨팅이 현재 상용화 된 것은 아니지만, 양자 컴퓨팅을 대비하는 post-양자 암호 및 암호 화폐들에 대한 연구도 끊임없이 이루어져야 할 것이다.

감사의글

본 연구는 과학기술정보통신부 및 정보통신기술진흥센터의 SW중심대학지원사업의 연구결과로 수행되었음 (2015-0-00930)

참고문헌

[1] 안드레아스 M 외 1명, "비트코인, 블록체인과 금융의 혁신", 2015. 10.

[2] 임현식, "양자역학 원리를 이용한 컴퓨터 개발: 양자컴퓨터", 2008. 7

[3] Anton Churyumov, "Byteball: A Decentralized System for Storage and Transfer of Value", 2016.

[4] Peter Waterland, "Quantum Resistant Ledger (QRL)", 2016. 11.