https://doi.org/10.33778/kcsa.2020.20.3.071

블록체인 기법의 확장가능성을 위한 병행 수행 제어 기법에 대한 연구

강 용 혁*, 박 원 형**

요 약

비트코인에 기반한 블록체인 기술은 익명성이 있는 스마트 계약, 저렴한 송금, 온라인 거래 등을 가능하게 하는 하부구조를 제시하고 있다. 하지만, 비트코인을 구현하는 블록체인 기술은 처리량과 지연시간 간의 트레이드오프 관계에 있는 확장가능성 제한을 갖고 있다. 이러한 문제를 해결하기 위한 비잔틴 고장 감내 기반 블록체인 기술이 제안되었다. 이 기법은 리더를 선출하고 리더에 의해 기존 블록 내에 작업증명을 포함하지 않는 많은 마이크로 블록을 구성하여 지연시간 증가 없이 처리량을 향상시켰다. 하지만 이 기법은 리더를 선출하는 부분에서 기존 기법보다 보안성이 떨어질 수 있다. 본 논문에서는 마이크로 블록기술과 병행수행 기법을 통해 블록체인 기술의 확장가능성을 위한 기법을 제안한다. 하나의 마이크로 블록 내에는 여러 개의 거래에 대한 정보가 있다.

A Study on Concurrency Control Scheme for Scalability of Blockchain

Yong-Hyeog Kang*, Wonhyung Park**

ABSTRACT

Bitcoin-based blockchain technology provides an infrastructure that enables anonymous smart contracts, low-cost remittances, and online payments. However, the block-chain technology that implements the bitcoin has scalability constraints in tradeoffs between throughput and latency. To solve these problems, the Byzantine fault tolerant block-chain technique has been proposed. This technique improves throughput without increasing latency by selecting a leader and constructing many microblocks that do not contain proofs of work within the existing block by the leader. However, this technique may be less secure than existing techniques in selecting the reader.

Key words : Blockchain, Proof of Work, Direct Acyclic Graph, Byzantine fault tolerant, Microblocks, POS

접수일(2020년 06월 01일), 게재확정일(2020년 07월 06일)

* 극동대학교 글로벌경영학과 교수(주저자)
** 상명대학교 정보보안공학과 부교수(교신저자)

1. 서 론

블록체인(Blockchain)은 서로서로 완전히 신뢰하지 않는 참여자들이 글로벌 상태 집합을 유지할 수 있는 분산 원장(distributed ledger)이다[1]. 분장원장이라고 불리는 블록은 분산되어 있는 여러 노드들에 의해 유지되며 다수의 트랜잭션들에 대한 정보를 갖고 있다. 블록체인은 이러한 블록들을 체인처럼 연결하는 추가 만 가능한(append only) 자료구조이다. 블록체인은 노드들이 데이터 복제본(replica)들을 유지하고 트랜잭션의 실행순서를 동의한다는 측면에서 분산 트랜잭션 관리 솔루션으로 볼 수 있다. 분산 원장은 세 가지 주요한 컴포넌트가 있다. 블록체인 자료구조가 있으며, 블록체인을 유지하는 노드들의 P2P 네트워크가 있으며, 어떻게 새로운 블록을 추가할지를 결정하는 피어들 간의 합의 프로토콜(consensus protocol)이 있다[3].

블록체인의 유형으로는 공개(public)형 블록체인, 사설(private)형 블록체인, 컨소시엄(consortium)형 블록체인이 있으며, 노드들의 참여를 제한하는 것과 관련하여 승인을 요구하는(permissioned) 블록체인과 승인이 필요없는(permissionless) 블록체인으로 구분할 수 있다. 블록체인의 응용은 암호화폐(Crypto-currency) 뿐만 아니라 수많은 분야에서 여러 가지 유형으로 나오고 있다[2]. 하지만 더많은 응용을 위해서는 확장성 및 보안 문제와 같은 해결해야 할 문제들도 있다.

블록체인의 기반 기술로는 분산 원장 기술, 합의 프로토콜, 암호학, 스마트 계약 등이 있다. 분산 원장 기술은 분산시스템과 데이터베이스 기술이며 합의 프로토콜은 분산시스템의 복제본에 대한 동일한 값을 유지하는 기술이다. 또한 블록체인에서는 암호학적 기술을 아주 많이 사용하는 데 공개키 기반 암호화기법, 해시를 이용한 무결성 지원 기법 등이다. 암호 화폐를 제외한 다양한 응용으로의 확장을 위해 스마트 계약(smart contract)이라는 개념이 소개되어 암호화폐 뿐만 아니라 여러 응용에도 적용되고 있다[4][5].

블록체인 기법의 핵심 메커니즘은 합의 프로토콜이며 현재까지 수많은 기법들이 제안되었다. 대표적으로는 비트코인에 사용된 PoW(Proof of Work) 기법과 PoW의 단점인 자원 낭비를 줄이기 위한 PoS(Proof of Stake) 기법이 대표적이다. 본 논문에서는 PoS를 기반으로 트랜잭션의 동시성 제어 기법을 적용한 확장성을 고려한 DAG(Direct Acyclic Graph) 형태인 블록체인 기법을 제안한다[6][7].

본 논문의 구성은 다음과 같다. 2장에서 여러 가지 합의 알고리즘과 관련된 기존 연구를 기술하고 문제점들을 기술한 다음, 3장에서 제안기법을 설명하고 4장에서 PoS 관련 블록체인의 여러 가지 보안 위협에 대한 제안기법의 해결방안을 설명하고 제안기법의 확장성과 성능에 대한 평가를 수행하고, 5장에서 결론 및 향후 연구 과제를 제시한다.

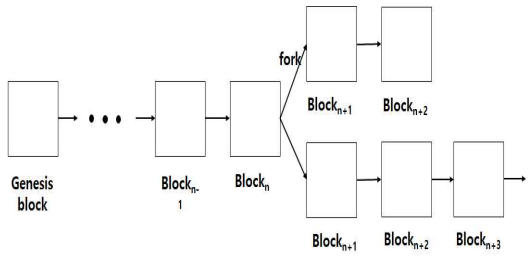
2. 관련연구

분산 환경에서의 합의 프로토콜은 오류(faulty)나 사기적인(deceptive) 노드들이 존재하기에 다음과 같음 문제를 해결해야 한다[5]. 통신 장애나 악의적인 노드들에 대한 문제로 비잔틴 장군 문제(Byzantine generals problem)를 해결해야 한다. 비잔틴 장애 감내(BFT: Byzantine Fault Tolerance)는 임의적인 데이터를 생성하는 노드가 있는 환경에서 합의에 도달하는 문제를 해결하는 복제본 문제의 일종이다. BFT는 어떤 조건하에서 안정성(safty)과 생존성(liveness)를 보장할 수 있다. 합의 프로토콜은 증명 기반(proof-based)과 리더 기반(leader-based) 기법을 구분할 수 있다[3]. 증명 기반 방식은 블록 제안(block proposal) 알고리즘과 가지 선정(branch selection) 알고리즘으로 구성된다. 블록 제안 알고리즘은 임의의 피어(peer)가 블록을 네트워크에 제안하고 나머지 피어에 의해 검증(validation)될 수 있다. 다수의 블록이 동시에 제안될 수 있으며, 가지 문제를 해결하기 위해 가지 선정 알고리즘이 사용된다. 비트코인 기법은 PoW 기법을 이용하여 블록 제안 기법을 사용했으며, 가장 긴 체인(longest chain)을 가지 선정 정책으로 사용했다. 리더 기반 기법은 선출된 리더에 의해 다음 블록 연계가 결정되는 기법이다. 리더를 선출하는 방식에는 지분을 이용하는 방법과 난수를 이용하는 방법 등이 있다[8]. 합의 프로토콜의 주요한 네 가지 타입은 PoW, PoS, DPoS(delegated PoS), PBFT(Practical BFT)기법이다[8]. PoW 기법은 비트코인 네트워크

에서 사용되는 합의 전략이다. 노드가 블록을 발행(publish)하려면 많은 작업을 수행하여 자신이 네트워크를 공격하지 않는다는 것을 증명한다. 이 기법은 노드들로 하여금 상당히 많은 계산 작업을 요구하여 너무 많은 자원을 낭비하게 된다. PoS 기법은 PoW 기법의 자원 낭비 문제를 해결하는 기법이다. 이 기법은 더많은 화폐를 가진 사람은 네트워크를 공격하지 않을 것이라는 믿음에서 시작한다. 이 기법의 단점은 화폐를 가장 많이 가진 노드가 네트워크를 장악할 위험성이 있다는 점이다. PoW 기법과 비교했을 때 PoS 기법은 에너지 절약하고 더 효과적이지만, 공격 위험성이 높아진다. DPoS 기법은 PoS 기법은 직접적인 방식인데 비해 DPoS 기법은 간접적인 방식이다. 상당히 적은 노드들만이 블록의 검증(validation)에 참여한다는 점이다. 이로 인해 빠른 확약(confirmation)이 가능하다. PBFT 기법은 비잔틴 고장에 대한 감내할 수 있는 복제 알고리즘이다. Hyperledger Fabric[9][10]이 대표적으로 사용한다. 세 단계로 이루어지며 모든 노드의 2/3으로부터 투표를 받으면 다음 단계로 넘어갈 수 있다. 하지만 이 기법의 단점은 모든 노드가 네트워크에 알려져 있어야 한다. 즉, 자유롭게 노드의 참여가 제한되며 많은 트래픽을 발생시킬 수 있어서 확장성에 제한이 있다. 블록체인 기술이 발전하면서 트랜잭션의 양은 날마다 증가하고 있으며 블록체인은 대용량(bulky)이 되었다. 블록체인의 확장성 문제를 다루기 위해 많은 노력이 제안되었다[2]. 이 기법들은 크게 두 가지 유형으로 나눌 수 있다. 첫 번째 방식은 블록체인의 스토리지(storage)를 최적화하는 것이다. 각 노드가 완전한 복제본을 가지고 운영하는 것이 어렵기 때문에 오래된 트랜잭션 레코드를 제거하는 기법도 있으며[2-37], 계정 트리(account tree)라는 다른 데이터베이스를 이용하여 잔액을 유지하는 데 사용하는 방식도 있으며, 경량(lightweight)의 클라이언트를 이용하여 해결하는 방식도 있다. 두 번째 방식은 블록체인을 새롭게 설계하는 방식이다. Bitcoin-NG에서는 블록은 리더를 선출하는 키블록과 트랜잭션을 저장하는 마이크로 블록으로 나눠서 수행하는 방식이다. 트랜잭션의 병행 수행 기법은 대표적으로 잠금(locking) 기법과 낙관적(Optimization) 기법이 있다. 잠금 기법은 공유 자원을 잠금으로써 공유 자원에 대한 접근을 제어하여 데이터에 대한 일치성을 유지하면서 병행 수행 하는 기법이다. 낙관적 기법은 병행 수행을 최대한 수행하고 커밋(commit)을 수행하기 전에 공유자원에 대한 충돌이 있는지 확인하여 충돌이 있는 트랜잭션은 취소(abort)하는 기법이다. 블록체인과 같은 분산 환경에서는 잠금 기법을 구현하려면 해당 자원에 대한 정보를 공유하여 접근하는 공간이 있어야 한다. 낙관적 기법은 공유되는 자원이 적고 트랜잭션의 수행시간이 짧은 환경에서 좋은 효율을 보인다. 본 논문에서는 낙관적 기법을 이용하여 트랜잭션의 병행 수행을 최대한 허용하고 충돌을 탐지하여 취소하는 기법을 사용한다.

3. 제안하는 블록체인 기법

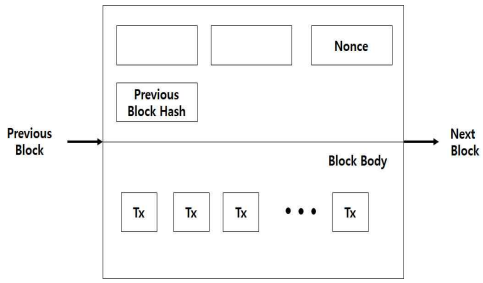
전형적인 블록체인 시스템은 서로 완전히 믿지 않는 많은 노드들로 이루어진다[1]. 노드들은 공유된 글로벌 상태의 집합을 유지하고 있으며 트랜잭션을 수행하여 상태를 수정한다. 블록체인의 일반적인 형태는 그림 1과 같다. 각 블록은 선행자와 암호학적 포인터를 통해 연결된다. 모든 노드는 최초의 제네시스(genesis) 블록과 연결되어 있다. 블록체인 내의 트랜잭션은 ACID를 요구하며 어떤 상태에 적용되는 명령문들의 시퀀스(sequence)로써 기존 트랜잭션과 거의 유사하다. 기존 트랜잭션과의 차이점은 장애에 대한 처리 모델에 있다. 블록체인 내의 트랜잭션은 보다 더 적대적인 환경에서 동작하는 것을 고려하여 비자틴 장애도 처리해야 한다.



(그림 1) LU의 활성화 비율에 따른 정상 감지된 AN의 비율의 변화

각 블록은 (그림 2)와 같이 블록 헤더와 블록 본체로 이루어진다. 블록 헤더에는 블록의 버전과 머클 트리(Merkle tree) 루트 해시값, 타임스탬프, 논스(nonce), 목적 임계값(target threshold)과 부모 블록

해시값 등을 가지고 있다. 블록 본체에는 트랜잭션 개수와 트랜잭션들로 구성된다. 블록이 트랜잭션을 포함할 수 있는 최대값은 블록의 크기와 트랜잭션의 크기에 의존한다. 트랜잭션의 인증을 검증(verify)하기 위해서 공개키를 기반으로 하는 비대칭키 암호화 기법인 디지털 서명을 사용한다. 전송자는 자신의 개인키를 이용하여 트랜잭션을 서명하고 수신자는 공개된 전송자의 공개키를 이용하여 트랜잭션을 검증할 수 있다.

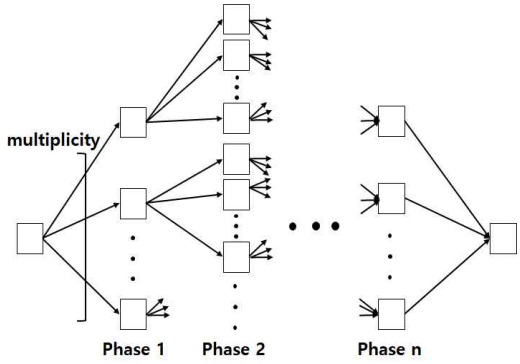


(그림 2) LU의 활성화 비율에 따른 정상 감지된 AN의 비율의 변화

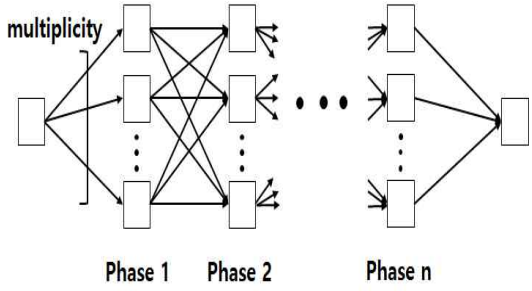
본 논문에서는 블록체인의 확장성을 높이기 위하여 체인 구조가 아닌 DAG(Direct Acyclic Graph) 구조를 사용하며 확장성과 일관성을 높이기 위해 데이터베이스의 병행수행 기법을 적용한다. 제안 기법은 병행 수행을 시작하는 한 개의 블록으로 구성된 시작 단계와 병행 수행을 종료하는 한 개의 블록으로 구성된 종료 단계가 있다. 종료 단계는 새로운 단계들의 시작 단계가 된다. 제안 기법은 시작 단계에서 참여자의 수에 따라 시작 단계에서 종료 단계까지의 단계의 수가 정해진다. 제안 기법은 병행 수행 다중도에 따라 다음과 같은 형태가 존재할 수 있다.

- 자유형
- 증감형(증가 후 감소형)
- 고정형

자유형은 다중도와 실행 단계에 따라 동시에 실행할 수 있는 블록체인의 수가 자유롭게 증가하거나 감소할 수 있는 방식이다. 가장 자유도가 높아서 병행 수행 정도가 자유롭게 높일 수 있으나 관리의 어려움이 많아 본 논문에서는 다루지 않는다. 증감형(증가 후 감소형)은 하나의 블록에서 여러 개의 블록으로 분기할 수 있는 확장 단계와 분기된 것을 하나의 블록으로 축소되는 감소 단계로 나눌 수 있다. 여러 개의 블록으로 확장될 때에는 병행성을 높여서 많은 트랜잭션이 실행될 수 있도록 하며 축소될 때에는 트랜잭션 간의 일치성의 충돌에 대한 해결을 수행한다. 확장 단계에서도 트랜잭션간의 일치성을 체크할 수 있으며 축소단계에서도 병행 수행은 일어난다. 고정형은 모든 단계에서 동시 실행될 수 있는 블록체인의 최대 개수가 고정된 방식이다. 증감형과 고정형의 일례는 다음 (그림 3)과 (그림 4)와 같다.



(그림 3) LU의 활성화 비율에 따른 정상 감지된 AN의 비율의 변화



(그림 4) LU의 활성화 비율에 따른 정상 감지된 AN의 비율의 변화

이전 블록을 가리키는 포인터의 형태에 따라 완전형과 불완전형으로 구분할 수 있다. 완전형은 현재 블록이 직전 단계 모든 블록에 대한 포인터를 갖고 있는 형태이며, 불완전형은 직전 단계 모든 블록에 대한 포인터 중의 일부 포인터만을 갖고 있는 형태

이다. [그림 4]는 완전형 형태이며, [그림 3]은 불완전형 형태의 예시이다. 직전 단계 블록에 대한 포인터를 너무 많이 가져야 한다면 현재 블록에 이전 블록에 대한 정보를 저장하게 되어 블록의 효율성을 저하시킬 수 있을 뿐만 아니라 네트워크에서 모든 블록에 대한 정보를 가져와야 하기 때문에 송수신 지연 시간으로 인해 블록 생성 실행 시간이 느려질 수 있다. 따라서 불완전형은 완전형 보다 충돌을 탐지하는 데 단점이 있지만, 실행시간이나 메모리 효율성측면에서 좋은 구조이다.

충돌을 탐지하는 방식은 불록 안에 있는 입력을 검색하여 같은 입력이 두 블록 이상에 있는 경우 충돌이 된다. 입력 충돌이 발생한 경우 출력에 따라 다음과 같이 구분할 수 있다.

- 약한 충돌: 출력이 같은 경우이며 동일 내용 충돌
- 강한 충돌: 출력이 다른 경우이며 상이 내용 충돌

약한 충돌과 같은 경우에는 동일한 트랜잭션이 두 군데 이상의 블록에 쓰여진 경우로 이중 지불 문제는 발생하지 않지만 수수료를 어떤 블록 생성자에게 할당해야 하는 문제가 있다. 강한 충돌과 같은 경우에는 이중 지불 문제가 발생하며 해당 트랜잭션을 무효화하고 입력의 소유자에게는 패널티를 부가하고 검색한 탐지자(detector)에게는 인센티브를 주는 방식으로 해결할 수 있다.

채굴자는 채굴에 참여하기 위해서는 주주(stakeholder)가 되어야 하며 stake가 되려면 보증액을 등록해야 한다. 이 보증액은 부정행위를 할 경우 패널티를 부여하기 위한 것이며 블록 생성 시에 참여시키는 트랜잭션들의 거래 금액에 대한 어느 정도 이상의 비율로 사용된다. 이로 인해 더 많은 보증액을 갖고 있는 stake가 거래 금액이 큰 트랜잭션들을 포함시킬 수 있다. 채굴자는 stake 또는 작은 보증금액들을 모은 stake 그룹으로 등록할 수 있다. 제안기법은 공모 공격을 막기 위해 시작단계에서 등록된 stake들 중에서 램덤으로 선정되며 선정된 채굴자들은 종료단계까지 블록을 생성시킬 수 있다. 한번 선정된 stake는 한동안 선정되지 않게 할 수 있다. 선정되지 않는 채굴자나 일반 참여자는 블록체인 상의 부정행위를 탐지할 수 있으며 탐지한 경우 인센티브를 받을 수 있다. 제안기법의 합의 알고리즘으로는 PoS 기법을 사용하며 각 블록 생성자가 책임을 지는 방식을 사용한다. 채굴자는 stake 또는 stake 그룹으로 등록한다. PoS 기법의 부정 사용 문제점은 채굴자가 부정한 작업을 수행할 경우인데 자신의 부정하거나 오류를 범할 경우에 대한 책임을 지기 위해 보증액을 등록하도록 한다. 채굴자가 거짓을 수행한 것을 발견할 경우 채굴자의 보증액을 탐지자에게 인센티브로 줌으로써 부정한 작업을 하지 못하도록 한다. PoS 기법의 불균형 문제점은 stake를 많이 가진 사람이 더 많이 얻어가는 문제점이 있다. 왜냐하면, 보증액이 높은 stake은 블록을 생성할 때 보증액에 따라 더 많은 수수료가 있는 트랜잭션 위주로 블록을 생성할 수 있는 권리가 주어지기 때문이다. 이 문제를 해결하기 위해 다음과 같은 두 가지 기법을 적용한다.

- 충돌나는 경우 발생하는 수수료를 보증액이 작은 stake에게 더 많이 할당한다.
- 한 사용자가 여러 개의 stake를 생성한 경우를 방지해야 한다.

첫 번째 기법은 경쟁률이 높은 수수료가 큰 트랜잭션을 보증액이 큰 stake가 덜 수행하게 되는 기법이다. 왜냐하면 충돌 날 경우 보증액이 작은 트랜잭션이 유리하기 때문이다. 두 번째 기법은 보증액을 많이 낼 수 있는 stake가 여러 개의 stake를 만들어서 참여하는 경우 그만큼 더 많은 수수료를 얻을 수 있는 문제점을 방지하기 위한 기법으로 여러 개의 stake를 사용하는 것을 탐지한 발견자에게 보증액과 수수료를 포함하여 해당 stake가 생성한 블록들에 대한 소유권을 가져가게 하는 방식이다.

이전 레벨 블록에 있는 트랜잭션을 뒤쪽 레벨 블록에서 포함시켜서 작성한 경우에도 충돌이 발생한다. 약한 충돌인 경우에는 이전레벨 우선으로 하여 현재 레벨 트랜잭션은 수수료를 받지 않고 강한충돌인 경우에는 소유자가 이중지불하기 위한 것이므로 이전 레벨 트랜잭션과 현재 레벨 트랜잭션을 취소시키고 해당 금액에 대한 패널티를 부가하고 발견자에게 인센티브로 줌으로써 문제를 해결한다. 발견자는 해당 블록을 생성한 블록 생성자가 될 수도 있고 추후 블록 생성자가 될 수도 있다. 블록 생성자들은 이전 레벨 블록을 더많이 포함시킬수록 더많은 수수료 및 인센티브를 얻을 수 있게 된다.

불완전형 구조의 또다른 문제점은 이전 블록이 다음레벨 블록에 의해 참조되지 않는 고아 블록

(Orphan Block)이 생길 수 있다. 이 블록에 대한 해결방안은 두 가지가 있다. 현재 레벨 이후 레벨에서 한 단계 이상 이전의 블록을 참조하는 것을 허용하는 방식과 마지막 레벨에서 모든 고아 블록들을 포함시키는 방식이 있다. 마지막 레벨에서 포함시키는 방식은 마지막 단계에서 많은 연산을 해야 할 수도 있으므로 최소화하고 고아 블록인 경우 한 단계 이상 이전의 블록도 현재 블록에서 참조하는 것을 허용하는 방식이 효율적이다.

4. 보안 및 성능 분석

블록체인을 PoS 기법을 많은 기법들이 제안되었지만 보안 위협으로 인해 넓게 사용되지 못하고 있다[12]. 이러한 보안 위협에는 Nothing at stake 공격과 long range 공격이 있다. Nothing at stake 자신의 stake에 손해 없이 충돌하는 블록을 만들 수 있다는 것이며, long-range 공격은 대다수 stake를 소유한 사용자가 전체 블록체인 히스토리를 변경할 수 있는 공격이다. 제안기법에서는 이중 지불이나 불공정한 행위에 대하여 패널티를 부가하기 때문에 Nothing at stake 공격은 방지할 수 있으며 stake를 랜덤으로 선출하는 방식으로 인해 한 stake가 대부분을 차지하는 경우를 방지하기 때문에 long-range 공격을 방지할 수 있다. PoS 기법을 쓰는 블록체인이 해결해야 할 가장 큰 문제는 이중 지불 문제와 stake를 많이 가진 소유자가 더 많은 이익을 얻는 문제이다. 제안 기법은 이중 지불을 탐지하고 취소하고 이중 지불한 사용자에게 패널티를 부가함으로써 이중 지불을 방지할 수 있다. 또한, stake를 많이 가진 소유자보다는 stake가 적은 소유자에게 수수료를 더 우선적으로 할당하고 stake를 더많이 가진 소유자의 부정행위를 탐지하고 패널티를 부가함으로써 문제를 해결한다. 제안 기법의 성능은 기존 기법보다 더많은 블록을 동시에 생성하여 블록체인의 확장성 및 효율성을 향상시킬 수 있다는 점이다. 고정형의 성능향상은 다중화 파라메터인 m에 비례하여 증가한다. 왜냐하면 레벨이 많아질수록 블록의 개수는 기존기법보다 m배 증가하기 때문이다. 레벨이 n인 경우 고정형 기법의 블록의 개수는 (n-1)*m+1이 된다. 이 값을 n+1로 나누면 고정형이 기존기법보다 얼마나 많은 비율로 블록을 가지는 지 알 수 있다. 이것을 수식으로 나타내면 다음과 같다. 이 식을 통해 n이 증가할 경우 약 m배 증가함을 알 수 있다.

$$\frac{(n-1)\times m+1}{n+1} \qquad (1)$$

증감형인 경우 완전형이나 불완전형이냐에 상관없이 <표 1>과 같은 성능향상을 가져온다. 최대항만을 고려하면 기존기법에 비해 $\frac{m^{\frac{l+1}{2}}}{l+1}$ 만큼이 비율로 블록의 개수가 증가함을 의미한다. 이는 l이 증가할수록 지수적으로 증가함을 의미한다.

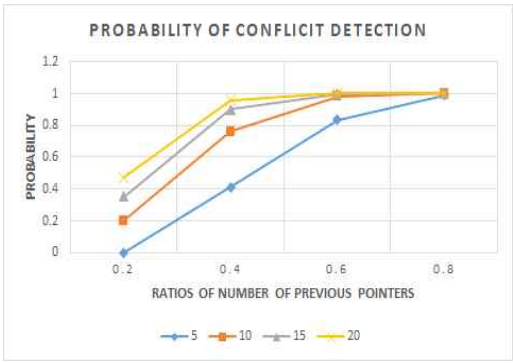
<표 1> 블록 수의 증가율

레벨(l)	블록 수의 증가율
1	$\frac{1+m}{+1}$
3	$\frac{1+2m+m}{l+1}$
5	$\frac{1+2m+2m^2+m^3}{l+1}$
2a-1 (a≥2)	$\frac{1+\sum_{t=1}^{a-1}(2m^t)+m^a}{2a}$

다중도 m과 이전 링크의 수 p를 파라메터로 하여 1000회 시뮬레이션을 통해 성능 평가를 수행하였다. 다중도는 5, 10, 15, 20값을 가지며 이전 링크의 수는 비율로 하여 0.2, 0.4, 0.6, 0.8로 하였다. 다중도가 5와 20인 경우 이전 링크의 수의 비율이 0.2인 경우 이전 링크의 수는 각각 1과 4개가 된다. 트랜잭션의 충돌을 검출할 확률을 구하기 위해 충돌하는 이전 블록 2개의 쌍을 다음 m개의 블록에서 아무도 동시에 링크하지 못하는 경우로 하였다. 이를 구하기 위해 이전 블록 2개의 쌍에 대한 전체 경우 중에 이전 블록 2개를 동시에 다음 블록에서 포함되지 않는 경우를 구하여 (그림 5)에 보였다. (그림 5)에서 보듯이 m이 5이고 p가 0.2인 경우 이전 링크의 수는 1이므로 동시에 2개의 블록을 가리킬 수 없어서 충돌을 전혀 검출하지 못하는 결과를 가져오지만 p가 0.4인 경우에는 이전 링크의 수가 2개 이므로 40% 확률로

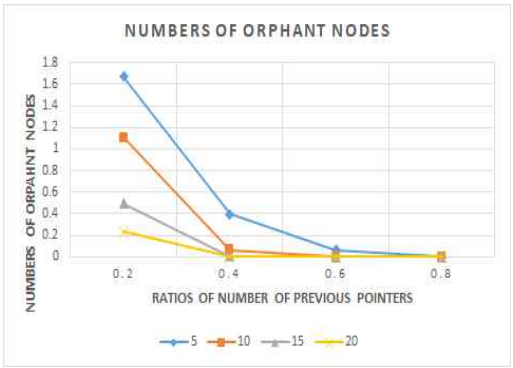
충돌을 검출할 수 있다. 이전하였다.

전체 경우 중에 동시에 링크하지 못하는 하는 구하여 블록 내의 이중 지불이나 트랜잭션 처리가 잘못되는 경우를 구한다. 완전형은 다음 단계에서 바로 검출되지만, 불완전형은 두 개의 충돌되는 트랜잭션이 있는 같은 단계이든 다른 단계이든 상관없이 블록들에 대한 이전 링크를 가지게 되면 검출된다. 이는 이전 링크에 대한 직접적인 연결이나 이전 링크를 통한 간접적인 연결을 갖고 있을 경우에도 검출할 수 있다. 다중도가 m이고 이전 링크의 수가 p(p<=m)인 고정형 불완전형인 경우 이전 레벨 블록들에 들어있는 트랜잭션의 충돌을 검출할 확률은 다음과 같다.



(그림 5) 트랜잭션의 출돌 검출 확률

다음 그림은 고아 블록이 될 확률을 구한 것이다. 그림에서 보이듯이 해당 블록체인이 기본형은 축약 단계에서 검출되기 시작하며 최종 단계에서 완전히 검출된다. 네트워크형은 바로 검출할 수도 있고 마지막에서 검출될 수도 있다.



(그림 6) 고아 블록이 될 확률

5. 결 론

본 논문에서는 데이터베이스의 병행 수행 제어기법을 이용하여 이중 지불 방지 기법과 속도 및 확장 가능성을 갖는 블록체인 기술을 제안하였다. 향후 연구과제로는 제안 기법에 대한 상세 설계와 검증을 수행하고 성능평가를 수행하는 것이다. 제안기법은 레벨이 증가할수록 성능은 향상되지만 충돌가능성이 높아진다. 향후 연구과제로는 제안기법을 구현하는 것과 실험을 통해 성능평가를 수행하는 것이다.

참고문헌

[1] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system.", 2008.

[2] www.3.weforum.org/

[3] https://www.coinhills.com/ko/market/exchange/

[4] www.ccn.com/privacy-coin-verge-succumbs-to-51-attack-again/.

[5] Chen, L., Chen, L., Jordan, S., Liu, Y. K., Moody, D., Peralta, R., and Smith-Tone, D. Report on post-quantum cryptography. National Institute of Standards and Technology, 2016.

[6] Eyal, I., & Sirer, E. G., Majority is not enough: Bitcoin mining is vulnerable. Communications of the ACM, Vol. 61, No. 7, pp. 95-102. 2018.

[7] Kwon, Y., Kim, D., Son, Y, Vasserman, E., and Kim, Y, Be selfish and avoid dilemmas: Fork after withholding attacks on bitcoin. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, pp. 195-209, 2017.

[8] Bonneau, Joseph. Hostile blockchain take-overs, Bitcoin'18: Proceedings of the 5th Workshop on Bitcoin and Blockchain

Research. 2018.

[9] Aggarwal, D., Brennen, G. K., Lee, T., Santha, M., and Tomamichel, M, Quantum attacks on Bitcoin, and how to protect against them. arXiv preprint arXiv:1710.10377, 2017.

[10] Boyer, M., Brassard, G., Høyer, P., and Tapp, A., Tight bounds on quantum searching. Fortschritte der Physik: Progress of Physics, Vol. 46, No. 45, pp. 493-505, 1998.

〔저자소개〕

강 용 혁(Yong-Hyeog Kang)
1996년 2월 성균관대학교 정보공학과(공학사)
1998년 2월 성균관대학교 정보공학과(공학석사)
2003년 8월 성균관대학교 전기전자 및컴퓨터공학과(공학박사)
2003년 3월 ~ 현재 극동대학교 글로벌경영학과 교수
email: yhkang@kdu.ac.kr

박 원 형 (Wonhyung Park)

서울과학기술대 산업정보시스템 공학사/ 공학석사
경기대 정보보호학과 이학박사
성균관대학교 컴퓨터교육학 박사수료
극동대학교 사이버보안학과 부교수/학과장
2020년~ 현재 상명대학교 정보보안공학과 부교수
email : whpark@smu.ac.kr