ISSN : 1226-7244 (Print)
ISSN : 2288-243X (Online)
논문번호 20-03-15

j.inst.Korean.electr.electron.eng.Vol.24,No.3,791~796,September 2020
http://dx.doi.org/10.7471/ikeee.2020.24.3.791
115

보안성 및 범용성이 강화된 3세대 블록체인 플랫폼 "큐본"

"Q-Bone", a 3rd Generation Blockchain Platform with Enhanced Security and Flexibility

임 노 간*, 이 요 한*, 조 지 연*, 이 성 수**★

Noh-Gan Im, Yo-Han Lee, Ji-Yeon Cho* and Seongsoo Lee**★

Abstract

In this paper, "Q-Bone", a 3rd generation blockchain platform with enhanced security and flexibility, was developed. As a 3rd generation blockchain platform, it exploits BP (block producer) to increase processing speed. It has many advantages as follows. It improves both security and speed by mixing RSA (Rivest-Shamir-Adleman) and AES (advanced encryption standard). It improves flexibility by exploiting gateway to convert between apps and blockchain with different programming language. It increases processing speed by combining whole transactions into one block and distribute it when too many transactions occur. It improves search speed by inserting sequence hash into transaction data. It was implemented and applied to pet communication service and academy-instructor-student matching service, and it was verified to work correctly and effectively. Its processing speed is 3,357 transactions/second, which shows excellent performance.

요 약

본 논문에서는 보안성이 강화된 3세대 블록체인 플랫폼인 "큐본"을 개발하였다. "큐본"은 3세대 블록체인의 특징인 BP (block producer)를 도입하여 처리 속도를 높였다. "큐본"의 장점으로는 보안성이 높은 RSA (Rivest-Shamir-Adleman)와 속도가 빠른 AES (advanced encryption standard)를 혼용하여 보안성과 속도를 모두 높였으며, 서로 다른 프로그래밍 언어를 사용하는 앱과 블록체인을 연결해주는 게이트웨이를 채용하여 범용성을 높였으며, 과도한 횟수의 트랜잭션이 발생하는 경우에는 이 트랜잭션을 하나로 묶어서 배포함으로서 처리 속도를 높였으며, 트랜잭션 데이터에 시퀀스 해쉬를 삽입하여 검색 속도를 높였다. "큐본"은 펫 커뮤니티 서비스, 학원-강사-학생 매칭 서비스에 적용되어 정확하고 효과적으로 동작하는 것을 확인하였으며, "큐본"의 트랜잭션 처리 속도는 3,557 TPS (transactions per second)로 매우 높은 성능을 보여주었다.

Key words : Blockchain, 3rd Generation, Security, Flexibility, Q-Bone

* Hoyun Inc. (CEO, Team Leader)
** School of Electronic Engineering, Soongsil University (Professor)
★ Corresponding author
(E-mail : sslee@ssu.ac.kr, Tel : 02-820-0692)
※ Acknowledgment
This work was supported by the Industrial Strategic Technology Development Program funded by the Ministry of Trade Industry and Energy (MOTIE)/Korea Evaluation Institute of Industrial Technology (KEIT) (20009043)
Manuscript received Sep. 1, 2020; revised Sep. 13, 2020; accepted Sep. 15, 2020.

Ⅰ. 서론

블록체인은 분산 컴퓨팅을 기반으로 하여 모든 거래 기록을 모든 노드가 공유함으로서 누구도 임의로 수정할 수 없고 누구나 결과를 열람할 수 있다. 블록체인은 P2P(peer-to-peer) 네트워크에서 수많은 어플리케이션 프로그램을 운용할 수 있는 플랫폼으로 발전하고 있으나, 낮은 트랜잭션 처리 속도, 비효율적인 합의 알고리즘 등의 문제를 가지고 있다[1]. 3세대 블록체인은 이러한 문제를 해결하기 위해 블록을 생산하는 주체이자 투표로 선출되는 노드인 블록 생성자(BP : block producer)를

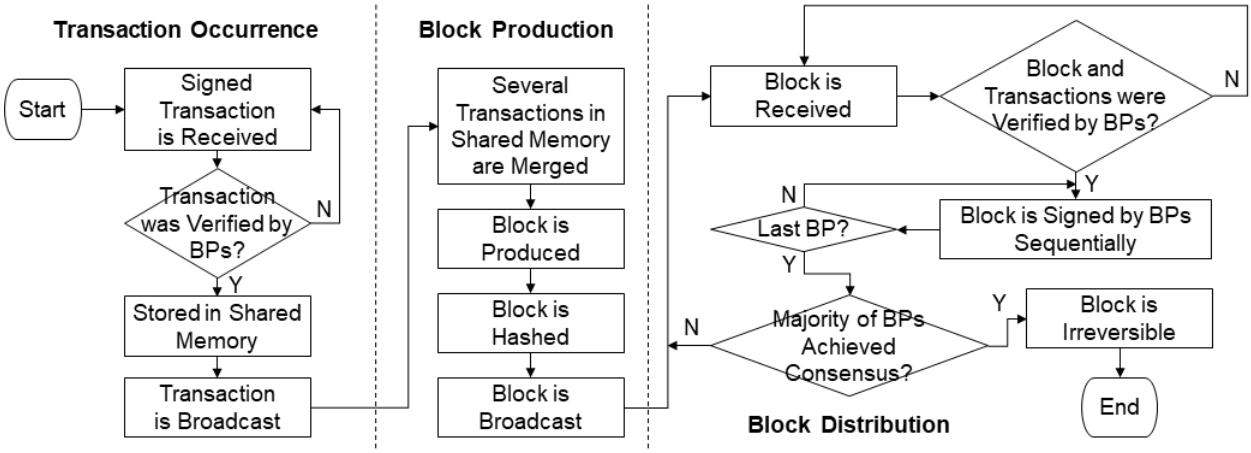

Fig. 1. Processing sequence of "Q-Bone" blockchain platform.
그림 1. "큐본" 블록체인 플랫폼의 처리 시퀀스

도입하였으며[2] 이들 BP가 트랜잭션의 이상 유무를 판단하고 블록에 서명하며 합의에 의해 운영함으로서 처리 속도를 획기적으로 높였다.

본 논문에서는 보안성이 강화된 3세대 블록체인 플랫폼인 "큐본(Q-Bone)"을 개발하였으며 다음과 같은 장점을 가지고 있다. (1) 보안성이 높은 RSA (Rivest-Shamir-Adleman)와 속도가 빠른 AES (advanced encryption standard)를 혼용하여 보안성과 속도를 모두 높였으며, (2) 서로 다른 프로그래밍 언어를 사용하는 앱과 블록체인을 연결해주는 게이트웨이를 채용하여 범용성을 높였으며, (3) 과도한 횟수의 트랜잭션이 발생하는 경우에는 이 트랜잭션을 하나로 묶어서 배포함으로서 처리 속도를 높였으며, (4) 트랜잭션 데이터에 시퀀스 해쉬를 삽입하여 검색 속도를 높였다.

II. 구조 및 동작

본 논문에서 개발한 블록체인 플랫폼은 3세대 블록체인 플랫폼으로서 펫 커뮤니티 서비스[3], 학원-강사-학생 매칭 서비스 등 다양한 O2O(online to offline) 서비스에 적합하도록 개발되었으며 그림 1과 같은 구조를 가진다.

스마트 컨트랙트가 실행되어 거래가 발생하게 되면 트랜잭션이 만들어지고, 이 트랜잭션은 검증 단계를 거쳐 공유 메모리에 저장된 후 배포된다. 트랜잭션 발생 단계가 정상적으로 종료되면 공유 메모리에 저장된 트랜잭션은 블록 생성 단계를 거치게 된다. 블록 생성 단계는 일정 시간동안 발생한 트랜잭션들을 하나로 묶는 단계이며, 여기에서는 블록체인 시스템에서 0.5초간 발생한 트랜잭션들을 포함하게 개발하였다. 트랜잭션들의 집합인 블록은 서명을 거쳐 블록 배포 단계로 넘어가게 된다. 블록 배포 단계에서 BP는 블록과 그 내부의 트랜잭션의 이상 유무를 판단하며 블록과 트랜잭션이 정상일 경우 블록 서명을 수행하고 합의 알고리즘에 따라 블록의 체결 여부를 결정한다.

그림 2는 개발된 블록체인 플랫폼의 실행 결과를 나타낸 것이다. 먼저 그림 2(a)와 같이 블록체인 플랫폼이 각종 플러그인을 초기화시키고 정상적으로 블록을 생성하기 시작한다.

스마트 컨트랙트를 실행시키기 위해서는 계정이 필요하고 계정을 생성하기 위해서는 지갑 생성이 필수적이다. 계정과 지갑의 연동을 위해 개인키와 공개키를 한 쌍으로 하는 오너키와 액티브키를 생성해야 한다. 그림 2(b), (c)는 각각 지갑 생성과 키 쌍 생성을 보여준다. 다음으로 계정을 생성하고 계정과 지갑을 연결한다. 계정에는 그림 2(d)와 같이 2개의 공개 키를 연결하고 지갑에는 그림 2(e)와 같이 2개의 개인키를 연결한다.

그림 2(f)는 개발된 블록체인 플랫폼 상에서의 스마트 컨트랙트 실행 결과를 보여준다. 스마트 컨트랙트를 실행시켜 토큰 발행 기능을 활성화한 후 토큰을 발행하려면 토큰 발행 권한을 가진 계정이 필요하다. 이때 그림 2(g)와 같이 토큰의 최대 공급량을 설정해주어야 한다. 그림 2(h)는 100.0000개의 토큰을 발행한 결과를, 그림 2(i)는 10.0000개의 토큰을 전송한 결과를 보여준다.

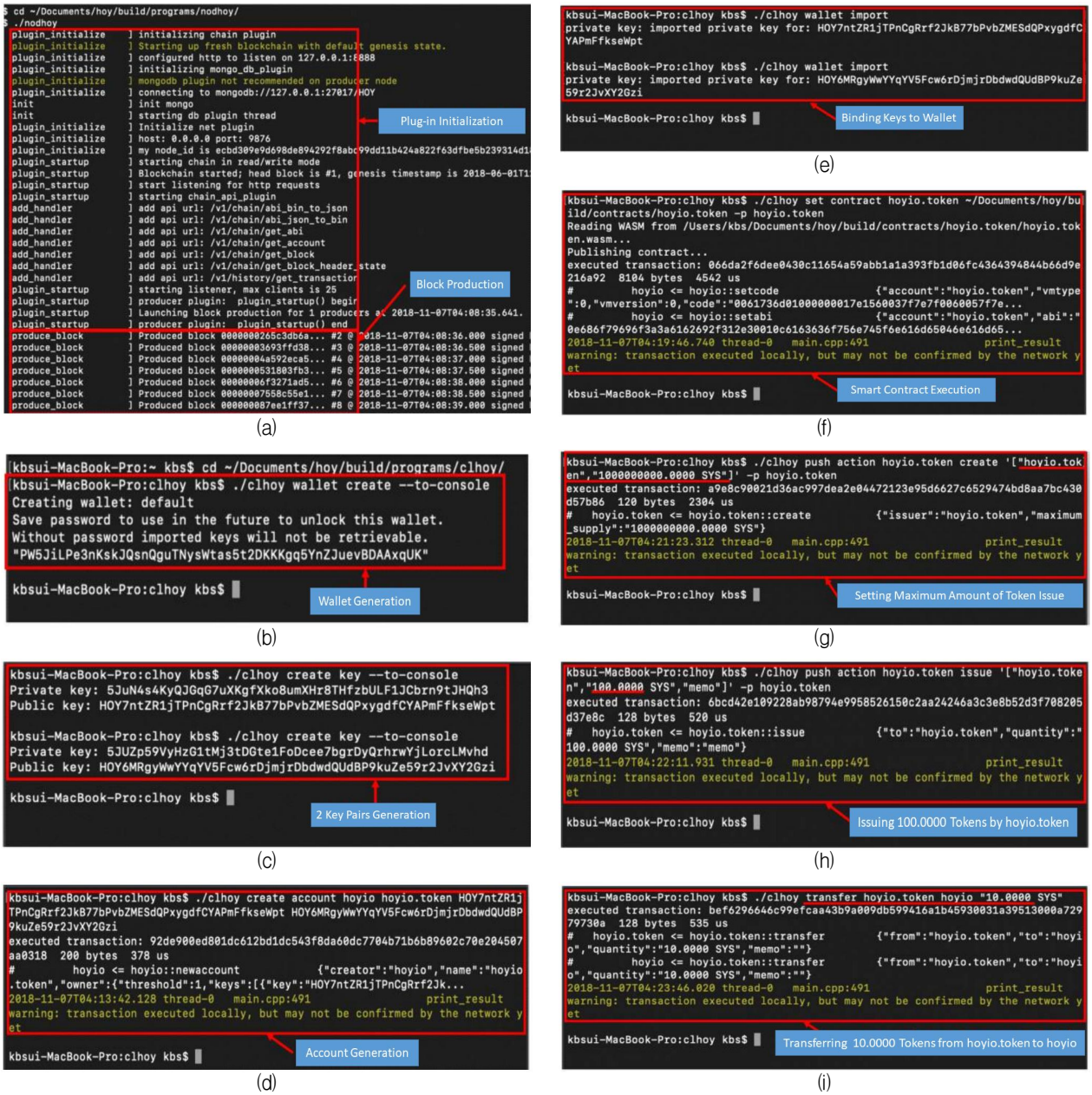

Fig. 2. Operation of "Q-Bone" blockchain platform : (a) Block production, (b) Wallet generation, (c) Key pairs generation, (d) Account generation, (e) Binding keys to wallet, (f) Smart contract execution, (g) Setting maximum amount of token issue, (h) Token Issuing, (i) Token Transferring.

그림 2. "큐본" 블록체인 플랫폼의 동작 : (a) 블록 생성, (b) 지갑 생성, (c) 키 쌍 생성, (d) 계정 생성, (e) 지갑에 키 연결, (f) 스마트 컨트랙트 실행, (g) 최대 토큰 공급량 설정, (h) 토큰 발행 (i) 토큰 전송

표 1은 본 논문에서 개발한 블록체인 플랫폼의 성능 측정 결과를 나타낸 것인데, 비교 대상인 기존 상용 블록체인 플랫폼 EOS가 훨씬 노드 개수가 많다는 점을 감안하더라도 본 논문의 블록체인 플랫폼이 여러 가지 측면에서 우수한 결과를 보여주고 있다.

Table 1. Performance measurement results.
표 1. 성능 측정 결과

Performance	Proposed	EOS
Transaction Processing Speed (transactions/sec)	3,557	Approx. 3,000
Block Production Time (sec)	0.5	Approx. 0.5
Block Data Search Time (sec)	0.001	Approx. 1

III. 보안성 및 범용성의 강화

1. RSA와 AES의 혼합 사용으로 보안성과 속도를 모두 개선

데이터를 각 노드들끼리 공유하는 태생적인 특징으로 인해 블록체인 플랫폼에서 보안은 매우 중요하다. 대표적인 보안 방식으로 RSA와 AES 방식을 들 수 있는데 RSA 방식은 AES 방식에 비해 보안성능이 강력하다는 장점을 가진 반면에 처리 속도가 느리다는 단점이 있다. 본 논문에서는 그림 3과 같이 보안 성능이 탁월한 RSA 방식을 초기에 한 번 사용하여 세션키를 만들고 이후에는 세션키를 이용하여 속도가 빠른 AES 방식으로 통신하는 혼합 방식을 제안하여 보안성과 속도를 모두 높일 수 있다.

블록체인 시스템을 설치하고 처음으로 시스템을 구동하게 되면 보안 모듈의 1단계로 진입하게 된다. 1단계는 시스템의 무결성(integrity)를 보장해 주는 단계로서, BP는 보안서버로 접속 요청을 하게 되고 보안서버에서는 인증서를 발생시켜 BP로 전달한다. BP는 보안서버로부터 받은 인증서를 검증하여 시스템의 무결성을 보장할 수 있게 한다. 2단계에서는 보안 성능이 강력한 RSA 방식을 이용하여 세션키를 만들어낸다. BP는 보안서버로부터 받은 인증서에서 공개키를 추출한다. BP와 보안서버는 각각의 임의 문자열을 생성한 후, BP는 공개키를 이용하고 보안서버는 비밀키를 이용해 각자의 세션키를 만들어낸다. 3단계에서 BP와 보안서버는 각자의 세션키를 이용하여 RSA방식 대비 속도가 빠른 AES 통신을 시작한다.

2. 다양한 앱 개발 언어를 모두 지원하여 범용성을 개선

비지니스용 플록체인 플랫폼에서 이를 이용하는 사용자 수와 앱 개발자수는 많으면 많을수록 좋다. 블록체인 플랫폼에서 개발 환경의 범용성을 제공하면 앱 개발자들을 많이 유입시킬 수 있는 장점이 있으나 현재 시장에 나와 있는 블록체인 스마트 컨트랙트는 각 블록체인 플랫폼이 제공하는 단일 개발 언어만을 지원한다.

본 논문에서는 개발 언어의 범용성을 확보하기 위해 그림 4와 같이 게이트웨이를 사용한다. 공개부분(Public portion)은 블록체인 플랫폼에 사용될

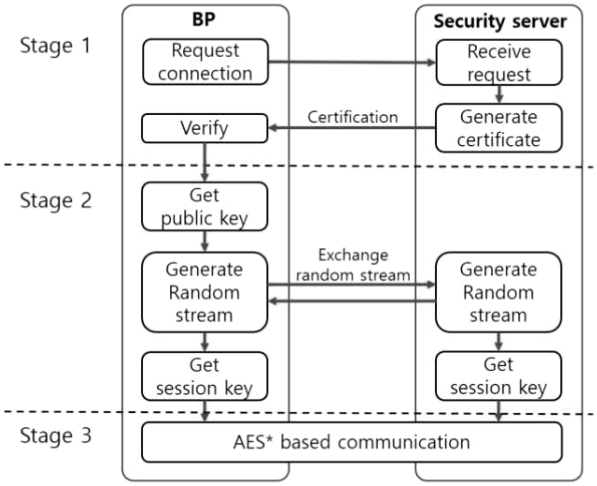

Fig. 3. Mixed exploitation of RSA and AES.
그림 3. RSA와 AES의 혼합 사용

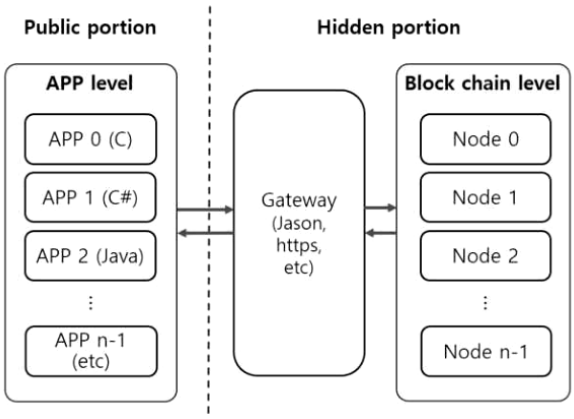

Fig. 4. Support of various app development languages.
그림 4. 다양한 앱 개발 언어의 지원

앱의 개발자가 접근할 수 있는 부분이고 비공개부분(Hidden portion)은 블록체인 플랫폼 개발자가 접근할 수 있는 부분이다. 각 앱이 블록체인 플랫폼의 노드들에 접근할 때 필수적으로 게이트웨이를 거치도록 하였다. 게이트웨이는 스마트 컨트랙트로 하여금 필수적이거나 선택적인 기능을 수행하게 할 수 있는 다수의 API(Application programming interface)를 제공하여 앱 개발자가 선호하는 언어를 이용하여 앱을 개발할 수 있게 해줌으로서 범용성을 크게 높일 수 있다.

3. 트랜잭션 일괄처리를 사용하여 처리 속도를 개선

블록체인 플랫폼에서는 단위시간동안 발생한 트랜잭션들을 묶어 블록을 생성을 하는 단계에서 한 번에 너무 많은 트랜잭션이 발생한 경우에 오버헤드 문제가 생길 수 있다. 종래의 블록체인 시스템

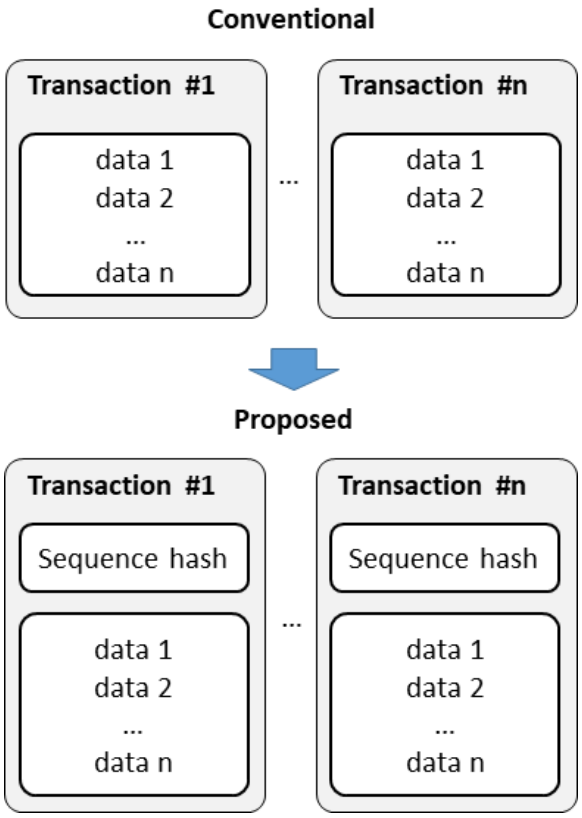

Fig. 5. Exploitation of sequence hash.
그림 5. 시퀀스 해쉬의 사용

에서는 발생한 트랜잭션의 수가 1만개면 트랜잭션 생성 → 전달 → 검증 → 블록 저장 → 블록 배포의 과정이 1만번 진행되어야 하기 때문에 처리 속도가 느린 문제점이 있었다. 본 논문에서는 이러한 문제를 해결하기 위해 블록을 생성하는 노드에 대량의 트랜잭션이 삽입된 블록을 송신하여 해당 노드에서 생성된 블록과 수신된 블록을 같이 체인 연결하여 배포하기 때문에 일괄처리가 가능하다. 이로써 한 번에 대량의 트랜잭션이 발생해도 오버헤드 문제 없이 처리 속도를 크게 높일 수 있다.

4. 시퀀스 해쉬 정보를 사용하여 검색 속도를 개선

정상적으로 블록체인에 결합된 블록에 저장된 특정 데이터를 조회를 하려고 하는 경우 대량의 데이터로 인해 조회 시간이 많이 소요될 수 있다. 블록체인의 특성 상 필요한 데이터를 조회하려면 블록 내의 데이터를 모두 조회하여야만 한다. 시스템을 장기간 운영하며 블록체인에 무수히 많은 블록들이 쌓이고 블록 내의 데이터를 매번 전수조회하면 많은 시간이 소요될 수 있다. 이 문제를 해결하기 위해 본 논문에서는 시퀀스 해쉬 정보를 사용하였다.

일반적으로 블록체인의 블록들은 모든 BP에 분산 저장되어진다. 현재는 데이터 조회 시에 여러 작업을 순차적으로 참조하여 결과를 생성한 다음에 이를 이용하여 검색하기 때문에 처리 속도가 느릴 뿐아니라 블록체인의 신뢰성을 얻기 위하여 모든 데이터가 담긴 블록을 모든 노드가 소유하고 있어야 하는 문제점이 있었다. 하지만 본 논문에서는 그림 5와 같이 시퀀스 해쉬를 이용한 블록체인 생성 시스템에 트랜잭션과 시퀀스 해쉬가 삽입된 바디와 헤더를 포함하는 블록을 생성함으로써 서비스 제공자가 분류하고자 하는 프로세스별로 동일한 시퀀스 해쉬를 가지게 한다. 이 시퀀스 해쉬 정보를 이용하여 데이터를 빠르게 조회하고 검색 속도를 크게 높일 수 있다.

Ⅳ. 결론

본 논문에서는 보안성이 강화된 3세대 블록체인 플랫폼을 개발하였다. 제안하는 블록체인 플랫폼은 다양한 기법을 사용하여 보안성과 확장성을 크게 높였으며 동작 속도도 크게 높였다. 다양한 서비스에 적용하여 검증을 완료하였으며 기존의 상용 블록체인 플랫폼인 EOS와 비교하였을 때에도 우수한 성능을 보였다. 측정된 트랜잭션 처리 속도는 3,557 TPS이다.

References

[1] J. Park, J. Park, S. Choi, J. Oh, and K. Kim, "Past, Present, and Future of Blockchain Technology," *Electronics and Telecommunications Trend*, vol.33, no.6, pp.139-153, 2018.

[2] M. Kim and Y. Kim, "Development of IoT Device Management System Using Blockchain DPoS Consensus Algorithm," *j.inst.Korean.electr.electron.eng,* vol.23, no.2, pp.508-516, 2019.
DOI: 10.7471/ikeee.2019.23.2.508

[3] J. Cho and S. Lee, "Animal Administration System Using Nose-Print Recognition and Blockchain Network," *j.inst.Korean.electr.electron.eng,* vol.23, no.4, pp.1477-1480, 2019.
DOI: 10.7471/ikeee.2019.23.4.1477

BIOGRAPHY

Noh-Gan Im (Member)

1995 : BS degree in International Trade, Chonnam National University.
2010~2018 : Software Engineer, Samsung Electronics.
2018~Now : Team Leader, Hoyun Inc.

Yo-Han Lee (Member)

2000 : BS Mobile Software, Sejong Cyber University.
2005 : MS Information Technology, Dankook University.
2012~2015 : Software Engineer, Pokevian inc.
2015~Now : Team Leader, Hoyun Inc.

Ji-Yeon Cho (Member)

2003 : BS degree in Electrical Engineering, Soongsil University.
2005 : MS degree in Electrical Engineering, Soongsil University.
2005~2008 : Software Engineer, Chips&Media Inc.
2008~2013 : Software Engineer, Samsung SDS
2015~Now : CEO, Hoyun Inc.

Seongsoo Lee (Life Member)

1991 : BS degree in Electronic Engineering, Seoul National University.
1993 : MS degree in Electronic Engineering, Seoul National University.
1998 : PhD degree in Electrical Engineering, Seoul National University.
1998~2000 : Research Associate, University of Tokyo.
2000~2002 : Research Professor, Ewha Womans University.
2002~Now : Professor in School of Electronic Engineering, Soongsil University.
<Main Interest> Automotive SoC, Low-Power SoC, Multimedia SoC, Battery Management