KIPS Trans. Comp. and Comm. Sys.
Vol.10, No.2 pp.47~52
ISSN: 2287-5891 (Print), ISSN 2734-049X (Online)

https://doi.org/10.3745/KTCCS.2021.10.2.47

A Study on the Current Status and Performance of OTP Utilization of Blockchain Technology

Deok Gyu Lee†

ABSTRACT

As blockchain technology develops, encryption for blockchain blocks is also becoming more important. Encryption in the blockchain is used to secure the identity of the person who created the transaction and to prevent manipulation of information in the past block. However, increasing the security of encryption decreases the speed of block creation, one of the biggest drawbacks of the blockchain. Therefore, in this paper, we propose a method to minimize the performance of the current OTP and the degradation of the blockchain by comparing the status and performance of OTP used in the blockchain.

Keywords : Blockchain, OTP

블록체인 기술의 OTP 활용 현황과 성능에 관한 연구

이 덕 규†

요 약

블록체인 기술이 발전함에 따라 블록체인 블록에 대한 암호화 또한 중요시되고 있다. 블록체인에서의 암호화는 트랜잭션을 생성한 사람의 신원보안과, 과거 블록의 정보를 조작 할 수 없도록 하게 이용된다. 하지만 암호화의 보안성을 증가시키면 블록체인의 가장 큰 단점중의 하나인 블록생성의 속도가 감소하게 된다. 따라서 본 논문에서는 블록체인에 사용되는 OTP의 현황과 성능을 비교하여 현재 OTP의 성능 및 블록체인의 성능저하를 최소화 할 수 있는 방안을 제시한다.

키워드 : 블록체인, OTP

1. 서 론

블록체인 에서는 암호화가 주로 두 가지 용도로 사용된다. 첫째, 트랜잭션 보낸 사람의 신원 보안 둘째, 과거 기록을 훼손 할 수 없다 블록체인 기술은 사용자의 신원을 보호하는 수단으로 암호화를 사용하여 트랜잭션이 안전하게 수행되고 모든 정보와 저장 장치를 안전하게 보호한다. 따라서 블록체인을 사용하는 사람은 무엇인가가 블록체인에 기록되면 합법적으로 보안을 유지하는 방식으로 완료한다는 확신을 가질 수 있다. 블록체인은 “해시함수”, “공개키 암호”, “랜덤 수”, “키 관리”, “암호 프로토콜(비잔틴 프로토콜, 멀티 파티 프로토콜 등)”, “영지식증명(ZKIP)” 등이 사용된다. 하지만 암호화 방식을 어떤 것을 채택하느냐에 따라서 블록체인의 성능이 좌우된다. 본 논문은 블록체인에 사용되는 OTP의 현황과 성능을 비교하여 블록체인에 OTP를 사용할 때의 성능저하를 최소화 할 수 있는 방안을 제안 한다. 2장에서는 관련연구, 3장에서는 성능 분석, 4장에서는 결론으로 마무리한다.

2. 배경 지식

2.1 블록체인의 개요

블록체인은 2008년 Satoshi Nakamoto라는 가명을 사용하는 사람이 발명한 비트 코인(Bitcoin)의 등장과 함께 소개되었다. 네트워크상에서 새로운 거래가 발생되면 모든 참여자가 해당 거래의 타당성을 검증 한다.

승인된 거래는 새롭게 형성된 블록으로 인정되고, 기존의 블록과 체인으로 연결된다.

이후 업데이트된 블록체인에 대한 사본을 참여자들이 분산해 저장하면 거래 하나가 완료되는 것이다. 블록체인은 네트

※ 본 논문은 2020년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임(No. 2020-0-00326, 블록체인 기반 물류정보의 실시간 트래킹을 통한 스마트 항만 응용 플랫폼 개발).
† 종신회원 : 서원대학교 정보보안학과 조교수
Manuscript Received : December 2, 2020
Accepted : December 8, 2020
* Corresponding Author : Deok Gyu lee(deokgyulee@gmail.com)

워크에 참여하는 모든 구성원이 거래 내역을 공유하는 일종의 분산장부(Distributed ledger)이다[1].

2.2 컨소시엄 블록체인

컨소시엄 블록체인은 여러 기관들이 공동주체가 되어 구성하는 반 중앙형 블록체인으로 프라이빗 블록체인과 같이 인가 받은 대상만 참여할 수 있으며, 각각에 대한 권한이 존재하며, 트랜잭션 유형 및 상호간의 합의에 따라 트랜잭션 인장 공개대상을 결정한다. 컨소시엄 블록체인에서는 공동주체 기관이 합의한 규칙에 따라 원장이 이루어진다. 기록관리 측면에서 컨소시엄 블록체인 유형을 살펴보면, 프라이빗 블록체인과 동일하게 관리주체가 존재하지만, 단일 관리주체가 아닌 공동 관리주체에 의해 이루어지는 관계로 기록의 출처와 신뢰성이 높으며, 마찬가지로 권한설정 및 부여가 가능해 트랜잭션 내역에 대한 프라이버시가 높다. 그리고 프라이빗 블록체인과 다르게 한 조직의 관리자가 임의로 특정 기록을 조작하기가 매우 어렵다는 점에서도 기록의 신뢰성이 높다고 볼 수 있다. 하지만 공동주체가 동일한 권한을 갖고 합의과정이 필요하다는 점에서 영주체가 조직 위계상 동일선상에 위치하는 기관들로 구성되어야 하므로, 전체 기록관리프로세스에 적용시키기는 어렵다. 그렇기 때문에 다른 유형의 블록체인과 적절하게 융합하거나 병행하여 활용하는 방안으로 모색해 볼 필요성이 있다.

2.3 블록체인의 국내외 동향

가상화폐를 기반으로 한 블록체인은 금융 산업에서 가장 활발하게 논의되고 있지만, 최근에는 금융산업은 물론 비 금융 산업분야에서도 기존산업의 단점을 보완할 수 있는 혁신적 아이템으로 블록체인 기술을 전망하고 있다. 더 나아가 블록체인은 핀테크 기술 등과 융합하여 다양한 산업분야에 적용하기 위한 발전이 이뤄지고 있으며, 최근에는 스타트업의 혁신적인 아이디어와 기술과의 융합 그리고 금융업체와 정부가 주도하는 협력을 통해 보다 다양한 산업과의 적용 및 변화를 촉진, 확장시켜 나가고 있다.

3. 기존 OTP 활용 블록체인 연구 분석

3.1 부인방지가 강화된 블록체인 OTP 시스템의 설계 및 구현[2]

기존의 OTP기기나 모바일 앱은 업체마다 달라서 여러 업체를 이용할 경우각기 다른 매체를 사용하거나 하나의 매체를 사용하고자 한다면 각 업체에 내가 어떤 OTP 기기를 사용하는지 등록하는 절차를 거쳐야만 한다. 이에 블록체인을 이용하여 OTP 시스템을 하나의 블록체인을 사용하여 통합하고 사용자가 OTP를 이용하기 위해 블록체인의 스마트 컨트랙트에 등록되어 있는 업체라면 손쉽게 OTP를 요청할 수 있도록 한다. 그리고 이 OTP를 보내준 업체가 보낸 블록체인 트랜잭션과 스마트 컨트랙트에 저장된 정보를 이용하여 사용자가 불이익을 당하지 않도록 하기 위해 블록체인을 이용하여 부인방지 기능이 강화되었다. 여기서 사용자가 블록체인을 직접 이용하여 트랜잭션을 발생시키도록 설계한 부분에 대해 OTP는 매우 중요한 서비스이고 보안강화와 DDoS 공격 예방을 위해 이번 설계에서는 그대로 가져갔다. 실제 서비스를 하는 업체에서 이 부분에 대해 추가적으로 고려하면 사용자가 더 편하게 사용할 수 있을 것이라는 생각을 한다. 그리고 네트워크로 전송되는 부분이 오프라인 OTP에 비해 취약할 수 있는 부분이 있으므로 중간에 탈취되어도 사용할 수 없게 업체가 블록체인 트랜잭션에 사용하는 데이터는 사용자의 공개키로 암호화하여 등록하도록 하였고 사용자도 최초에 업체에 OTP 사용등록을 하면서자신의 공개키를 보내고 업체에서도 응답으로 업체의 공개키를 보내 주어 이후 주고 받는 데이터를 암호화하여 보내도록 하였다. 이런 기능들로 통합성, 보안성, 및 부인방지 기능을 강화하여 전체 OTP 정보를 신뢰하고 사용할 수 있도록 하였다.

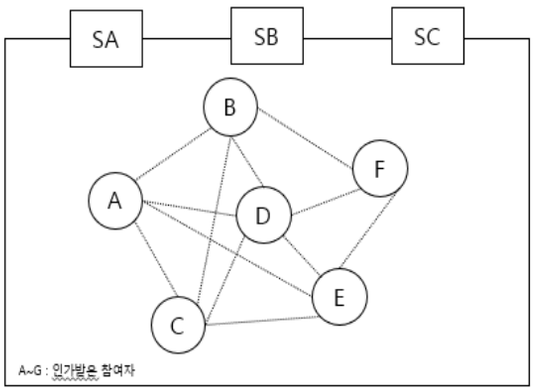

Fig. 1. Consortium Block Chain Principle

1) 요구사항 정의

블록체인 OTP를 사용하기 위한 전체 기능은 다음과 같이 구성된다.

a) 서비스 업체 구현 목록

ㄱ) 블록체인 OTP에 업체가 사용 등록
ㄴ) 사용자가 업체에 블록체인 OTP 사용자임을 등록
ㄷ) 난수(OTP) 생성 및 사용자 공개키로 암호화
ㄹ) 사용자에게 OTP 등록 완료 Push
ㅁ) 사용에게 받은 OTP를 복호화하여 SmartContract에서 검증

b) 블록체인 OTP SmartContract 기능

ㄱ) requestOTP (Event Log)
ㄴ) regOTPFromCompany (struct regOTPs에 저장)
ㄷ) getRequestOTP (userEthAddress)
ㄹ) verifyOTP (struct regOTPs에서 검증)

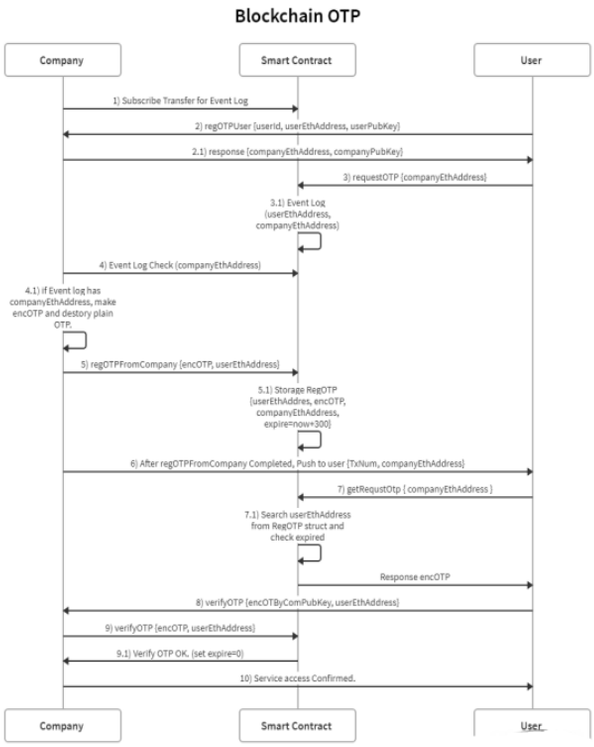

Fig. 2. BlockChain OTP Principle

Evaluation	Conventional ID/PW	General OTP	Blockchain OTP
Convenience	Good	Low	Low
Security	Low	High	Very High
Step	Easy	Inconvenience	Inconvenience
Integration	Low	Very Low	Good
Confidentiality	Low	High	Very High
Usurpation	High	None	None
DDos Attack	High	None	None (Gas Limit)
Vulnerability	Very High	None	None
Source Open	None	None	Public (Open Source)

Fig. 3. Performance Evaluation

c) 사용자 앱

ㄱ) 개인키, 공개키, EthAddress 생성 및 저장 월렛

ㄴ) 업체에 블록체인 OTP 사용 등록 요청

ㄷ) 블록체인 OTP에서 받은 encOTP를 개인키로 복호화 및 업체 공개키로 암호화한 encOTPByComPubKey 데이터 생성

2) 블록체인 OTP의 장단점

a) 범용적으로 제작되어 업체는 사용 의사만 있으면 되고 사용자도 통일되게여러 업체에 블록체인 OTP 사용을 쉽게 등록하고 안전하게 사용할 수 있다.

b) 각자의 공개키로 암호화하여 기밀성이 보장된다.

c) 블록체인을 사용하여 사용자는 해당 트랜잭션을 발생시킨 업체의주소를 알고 있고 공개키도 가지고 있으므로 부인방지를 할 수 있다.

d) OTP는 오프라인이라는 장점이 있는데 네트워크를 통해 OTP를 주고 받는것에 대한 이슈를 생각할 수 있으나, 이미 네이버 로그인 OTP,구글 인증 OTP 등의 사례가 있다. 즉 최근에는 각 서비스에 대해 보안 강화를 위해 등록된 스마트기기를 통해 OTP를 전송하는 기능을 구현하고 있다. 하지만 이 OTP 들은 각자의 서비스에 가입이 되어 있어야만 이용할 수 있는 문제를 해결하였다고 볼 수 있다.

e) 단점으로는 사용자가 OTP를 요청할 때마다 gas 비용이 들어간다는 이슈가 있다.

3.2 블록체인의 보안과 TPS 균형에 관한 연구[3]

비트코인의 TPS는 다음으로 식으로 계산될 수 있다. TPS (초당 거래 처리 속도) = 블록에 저장되는 거래량 / 블록 생성 주기 비트코인의 경우 평균 블록 생성 시간은 약 10분(600초)이다. 한 블록의 크기는 1 메가바이트(MegaByte)로 고정되어 있다. 이를 바이트(byte) 로 환산하면 104,8576 바이트로 나타낼 수 있다. TXID(Transtion ID)하나당 약 250바이트를 저장하기 때문에 하나의 블록에는 약 4200건의거래가 저장된다. 위 계산 방식에 대입해보면 “7 = 4200건/600초” 임이 성립된다. TXID가 항상 일정한 바이트를 저장하는 것은 아니지만, 공식에 따르면 초당 평균 거래 처리량은 약 7 TPS가 된다. 실세계인 비트코인 시스템에서는생성 시간 및 네트워크 부하 등에 의해서 비트코인의 실제 트랙잭션은 초당 7 TPS보다 낮은 경우가 대부분이다. 반면 이더리움의 트랜잭션은 비트코인의 트랜잭션과는 조금 다르다. 이더리움은 비트코인처럼 블록사이즈에 대한 제한은 없으나 Ether(gas)를 통해 토큰을 보내거나, 이더리움 내에서 수행할 수 있는 모든 작업을 수행한다. 이 때 지불은 가스(gas)를 통해 이루어진다. 이때 가스는 이더로 계산된다. 사용자는 이 가스의 증감을 통해 좀 더 빠르게 트랜잭션을 블록에 담을 수 있다. 이로 인해 이더리움은 비트코인과는 달리 블록의 크기보다 한 블록에 담을 수 있는 가스 크기 제한 때문에 속도 지연 문제가 발생한다. 사실 높은 단위의 가스를 펀딩할 경우 더 빠르게 트랜잭션이 처리 될 수 있으나 이는 총 거래량에서 수수료가 높은 수준을 차지할 수 있음을 보여줘 기형적이라고 할 수 있다. 가스란 이더리움 플랫폼에서 발생하는 거래의 수수료 개념이라고 할 수 있다. 하나의 이더리움 블록에 담을 수 있는 가스는 약 800만 가스로 제한되어 있다. 더 오래전에는 670만 가스가 한 블록의 제한이었다. 이 제한을 “블록 가스 리미트(block gas limit)”라고 하며, 하나의 이더리움 블록에 담을 수 있는 가스 리미트(gas limit)의 총합으로 볼 수있다. 즉, 가스 리미트가 21000인 트랜잭션을 약 380개 묶어서 한 블록에 담을 수 있다. 이더리움의 블록은 약 15~20초 마다

생성이 된다. 다시 위의 수식에 대입해 보면 아래와 같은 속도가 계산적으로 가능한 수치임을 확인할 수 있다.

3.3 Hyperledger Fabric 블록체인을 위한 TOTP기반 2차 인증 기법 [4]

TOTP(Time-Based One-Tome Password)는 시간기반의 인증방식으로 OTP 방식의 한 종류이다. TOTP는 클라이언트와 서버가 공유하고 있는 비밀정보인 Secret Key와 함께 현재시간 값을 인자로 사용한다. 동일한 Secret Key와 시간이라면 같은 결과가 나오게 되고, 인증에 성공하게 된다. 따라서 TOTP는 시간이 다를 경우 계산결과가 달라지므로 시간 동기화가 매우 중요하다. TOTP의 패스워드는 다음과 같이 계산된다.

$$TOTP = HOTP(K, T)$$

$$T = floor(\frac{T_{curr} - T_0}{X})$$

여기서 X는 시간간격을 초단위로 나타낸 값으로 기본 값은 30초이다. Tcurr는 현재시간 시점을, T0는 유닉스 시간의 시점을 나타낸다. 따라서 T는 현재 시간 에서 유닉스 시간 단위를 뺀 정수이며 시간간격 X로 나누어 floor 함수를 처리한 결과이다. HOTP 함수는 HMAC를 이용하여 K와 T를 입력으로 인증코드를계산하는 함수이다. 클라이언트에서 등록된 사용자 ID와 Password로 로그인을 하면 멤버십 서버는 사용자가 회원가입 시 설정한 권한을 통해 Acess Token과 OTP Token 그리고 Refresh Token을 발급한다. Refresh Token은 Acess Token이 만료되면 재발급을 위한 토큰으로 TOTPS를 통해 재발급하게 된다. 생성된 JWT 토큰은 Header, Payload, Signature의 3부분으로 구성되는데 여기서 발급되는Acess Token은 AT, OTP Token은 OT로 다음 식으로 표시하였다.

$$AT = HMAC(Header, Payload, secret)$$

HMAC은 서명생성함수로 공개된 Header, Payload 그리고 공개되지 않는 서버의 비밀값 secret를 입력받아 각각의 토큰을 발급한다.OTP 패스워드를 생성하기 위해서는 OTP 발급 서버와 개인 사용자 간에 서로공유하고 있는 동일한 비밀정보를 통해 OTP패스워드를 생성하게 된다. 회원등록 시 TOTPS는 해당 사용자에 대한 고유한 사용자 인증 코드 정보를 생성하게 된다[4].

4. 성능 향상 방법

4.1 이더리움 기반 OTP

이더리움의 트랜잭션은 비트코인의 트랜잭션과는 조금 다르다. 이더리움은 비트코인처럼 블록사이즈에 대한 제한은 없으나 이더, 혹은 가스를 통해 토큰을 보내거나, 이더리움 내에서 수행할 수 있는 모든 작업을 수행한다. 이 때 지불은 가스(gas)를 통해 이루어진다. 이때 가스는 이더로 계산된다. 사용자는 이 가스의 증감을 통해 좀 더 빠르게 트랜잭션을 블록에 담을 수 있다. 이로 인해 이더리움은 비트코인과는 달리 블록의 크기보다 한 블록에 담을 수 있는 가스 크기 제한 때문에 속도 지연 문제가 발생한다. 높은 단위의 가스를 펀딩할 경우 더 빠르게 트랜잭션이 처리 될 수 있으나 이는 총 거래량에서 수수료가 높은 수준을 차지할 수 있음을 보여준다. 가스란 이더리움 플랫폼에서 발생하는 거래의 수수료 개념이라고 할 수 있다. 하나의 이더리움 블록에 담을 수 있는 가스는 약 800만 가스로 제한되어 있다. 더 오래전에는 670만 가스가 한 블록의 제한이었다. 이 제한을 “블록 가스 리미트(block gas limit)”라고 하며, 하나의 이더리움 블록에 담을 수 있는 가스 리미트(gas limit)의 총합으로 볼 수있다. 즉, 가스 리미트가 21000인 트랜잭션을 약 380개 묶어서 한 블록에 담을 수 있다. 따라서 성능저하가 발생한다.

4.2 TOTP 기반 블록체인 인증

OTP 패스워드를 생성하기 위해서는 OTP발급 서버와 개인 사용자 간에 서로공유하고 있는 동일한 비밀정보를 통해 OTP 패스워드를 생성하게 된다. 회원등록 시 TOTPS는 해당 사용자에 대한 고유한 사용자 인증 코드 정보를 생성하게 된다. TOTPS에서 생성한 사용자 인증 코드는 사용자를 식별하기 위한정보로 사용되며 서버내부에 DB에서 해당사용자에 대한 사용자 인증 코드 정보를 저장한다. 패스워드를 생성하기 위한 비밀정보는 멤버십서버에서 발급한 OTP Token을 사용하게 된다. 멤버십 서버로부터 OTP Token을 발급 받은 클라이언트는 OTP Token과 현재시간 값을 이용해 패스워드 V를 계산하게 된다. TOTP값의 계산식은 앞서 설명한 식과 같다.

Equation (1)에서의 K는 멤버십 서버에서 발급받은 OTP Token으로 TOTP 패스워드 생성의 특성상 클라이언트와 TOTPS가 서로 공유하고있는 동일한 비밀정보가 된다. T는 Equation (2)와 같이 현재시간을 유닉스 시간단위로 나타낸 정수를 시간간격 X로 나누어 floor함수를 처리한 정수를 나타낸다. 클라이언트는 Peer에게 요청할 트랜잭션 제안, 생성된 패스워드 V 그리고 사용자 개인의 사용자 인증 코드를 TOTPS에게 전송하게 된다. TOTPS는 멤버십서버에서 발급한 OTP Token과 현재시간을 이용해 V'임을생성해 클라이언트에서 전송한 V와 비교한다. V와 V'이 같으면 사용자 인증코드 정보를 이용해 Access Token의 사용자와 같은지 비교하여 인증하게 된다. 클라이언트에게 Acess Token을 전송하지 않아 공격자에게 Access Token이 도청될 수 없으며 OTP Token을 도청하여 패스워드를 생성하더라도 사용자개인의 사용자 인증 코드 정보를 해킹할 수 없기 때문에 다른 사용자의 신분으로 위장할 수 없다. 하지만 클라이언트에서 TOTP 값을 계산하고 인증하는 과정이 추가되어 사용자의 안전성을 보장한다는 장점이 있지만 성능 측면에서 살펴보면 인증을

위한 수행시간이 증가하여 트랜잭션의 속도가 저하되는 단점이 있다. Membership 서비스에서 2차 인증을 통한 수행시간의 증가로 TPS성능이 떨어지는 단점을 해결할 수 있는 연구가 필요하다.

4.3 블록체인의 성능 향상 기법

1) 세그윗(SegWit)

세그윗(SegWit: Segregated Witness (Consensus layer))은 비트코인의 블록체인의 크기 제한 문제를 완화하기 위한 목적으로 비트 코인 개발자 Pieter Wuille에 의해 공식화되었다. 세그윗은 소프트포크로 특정 프로토콜 제한을 우회한다. 첫 번째 블록의 크기는 1메가바이트로 제한되어 있는데, 이 때 블록의 구조를 보면 디지털 서명란과 거래내역이 하나로 만들어져 있다. 서명란에서 서명이 실제로 차지하는 크기는 작지만, 서명란 자체의 크기는 매우 크다고 할 수 있다. 세그윗은 이 부분을개선하여 블록의 크기는 1메가바이트로 유지하고 트랜잭션을 처리할 수 있는 속도를 더 빠르게 한다. 즉 세그윗은 서명 부분을 따로 "Witness"라는 데이터 영역으로 분리시켜 더 많은 거래를 담을 수 있도록 업데이트 하는 것이다. 이때 개선된 세그윗에 담을 수 있는 데이터의 크기는 약 4메가바이트로 알려져 있다. 추가적으로 더 기술 필요. 사실 비트코인 진영에서는 세그윗을 기준으로 다음과 같은 소프트 포크 (Soft Fork)가 있었다. 비트코인 진영에서 제너시스 블록을 기준으로 478,557번째 블록 이후에 SegWit을 수용한 프로토콜과 SegWit을 수용하지 않고 블록 사이즈 자체를 늘린 비트코인 캐시(bitcoin cash) 프로토콜로 분리되었다. 이를 통해서 기존에 생성된 블록들은 비트코인 또는 비트코인 캐시 진영으로 이동할지 결정해야 한다. 이후 블록들은 서로 호환되지 아니한다.

2) 라이트닝 네트워크(Lighting Network)

라이트닝 네트워크(Lightning Network)는 블록 내부에 크기를 키워서 대량의 거래를 가능하게 하는 "On-chain Scaling"이 아닌, 블록체인 바깥에서 결제 채널을 따로 만들어 낮은 수수료로 다량의 소액거래를 처리 할 수 있게 만드는 "Off-chain Scaling"이다. 라이트닝 네트워크를 사용 할 경우도 수수료 없이 당사자 간에 즉각적인 거래를 가져오기 때문에 속도 개선을 할 수 있다. 예를 들어 라이트닝 네트워크를 사용하는 방식은 구독 경제 등에서 한 달 동안의 사용 요금을 미리 지불하는 경우를 들 수 있는데, 개별적으로 거래할 경우 개별 건으로 트랜잭션이 발생시켜서 비용과 시간을 지출하기보다는 한 번에 처리하는 것이 좀 더 수수료와 트랜잭션이 처리되는 시간을 감소시킬 수 있다. 라이트닝 네트워크의 경우 블록 내부의 크기를 확장하여 더 많은 거래를 가능하게 하는 온-체인 스케일링(On-chain Scaling)이 아닌, 블록체인 외부에 결제 채널을 따로 만들어서 낮은 수수료로 다량의 소액 거래를 처리할 수 있게 만드는 오프-체인 스케일링(Off-chain Scaling)방식이다. 오프 체인 트랜잭션은 블록체인의 외부 가치 이동이다. 보통 단순한 '거래'라고 불리는 온체인거래가 블록체인(blockchain)을 수정하고 유효성을 결정하기 위해 블록체인(blockchain)에 의존하는 반면, 오프체인 거래는 거래를 기록하고 검증하기 위해 다른 방법에 의존한다. 이는 다시 말하면 블록체인 블록 밖에 결제 채널을 빠르게 하기 위해 거래 기록소 개념을 추가하는 것이다. 이때의 거래기록소를 결제 채널이라고 부르고, 이 결제 채널은 거래 당사자들의 "공개키"로 형성된다. 라이트닝 네트워크는 결제 채널을 이용하여, 블록체인 상 등록되는 거래 건수를 줄이는 솔루션이다. 이를 통해, 사용자의 거래 수수료를 낮출 뿐만 아니라 비트코인의 낮은 TPS로 인한 확장성의 문제를 해결 할 수 있다.사실 이 부분은 대량의 거래를 처리하는 환전소 또는 거래소에서도 유용하다. 대량의 거래가 일어나는 거래소의 경우 모든 트랜잭션을 처리하는 것은 생각보다 많은 비용을 발생시키고 시간을 소모한다. 하지만 비트코인 거래소에서 다른 비트코인 거래소의 송금할 경우 모든 트랜잭션을 처리하기 보다는 거래의 당사자인 각각의 거래소가 보내고 받을 암호화폐의 증감만 전송하고 나머지는 거래소의 계정에 보유할 수도 있다. 즉 총 보유량의 증감만 보내고, 내부의 거래 장표를 보유한다면 실제로 거래에서 발생되는 트랜잭션보다 작은 트랜잭션이 발생한다. 2018년 1월 이후 라이트닝 네트워크의 거래수용량, 즉 라이트닝 네트워크를 통해 처리 가능한 비트코인 총 거래량은 지속적으로 증가하고 있다. 비트코인의 블록체인에서 일일 거래량과 비교했을 시 라이트닝 네트워크가 2018년 1월 수용할 수 있는 거래량은 약 0.002% 였으나, 현재는 약 250 배인 0.5% 정도 수용할 수 있다. 즉 하루에 100 비트코인이 거래된다면 이 중 약 0.5 비트코인은 블록체인에 등록하지 않고 라이트닝 네트워크를 통해 처리할 수 있다는 것을 의미한다.

3) 이더리움의 플라즈마(Plasma)

이더리움의 플라즈마(Plasma)는 2017년 8월 비탈릭 부테린(VitalikButerin) 이조셉 (Joseph Poon)과 함께 "Plasma: ScalableAutonomous Smart Contracts"를 통해 처음 제안되었다[5]. 플라즈마와 라이트닝 네트워크는 모두 블록체인을 위한 스케일링 솔루션으로 제안되었지만 각각 고유한 동작방식과 특수성을 가지고 있다. 다만 플라즈마 단독으로 사용되는 프로젝트가 아니며 오프 체인 스케일링 기술 또는 확장 가능한 응용 프로그램을 구축하기 위한 프레임워크(FrameWork)라고 볼 수 있다. 이더리움 플라즈마의 주요 아이디어는 메인체인(이더리움의 블록체인)과 가능한 적게 통신하고, 메인체인과 상호 작용할 사이드 체인의 프레임워크를 구축하는 것이다. 이 구조를 좀 더 확장해 보면 블록체인 구조하에 블록체인으로 설명할 수 있다. 이러한 프레임워크는 블록체인 트리로 동작하도록 설계되어 있다.플라즈마 구조는 스마트 컨트랙트(Smart Contract)와 머클 트리(Merkletree)를 사용하여 구축된다. 본질적으로 이더리움 메인체인인 블록체

인에작은 하위 레벨의 체인을 만들 수 있게 설계되어 있다. 각 하위 체인 위에 더 많은 체인을 만들 수 있으며 이것이 트리와 같은 구조로 생성된다. 기본적으로 각 플라즈마 하위 체인은 개별 요구에 맞는 단일 방식으로 작동하도록 설계 할 수 있는 맞춤형 스마트 계약이다. 즉 체인은 공존하고 독립적으로도 동작할 수 있다. 이런 구조를 가지게 되면 플라즈마는 기업과 회사가 특정 상황과 요구 조건에 따라 다양한 방법으로 확장 가능한 솔루션을 구현 가능할 수 있게 한다. 플라즈마가 이더리움에 성공적으로 개발되고 구현되면, 각 하위 체인은 특정 목표를 향한 뚜렷한 방식으로 작동하도록 설계될 수 있다. 플라즈마가 구현된 이더리움은 혼잡할 가능성이 적어진다. 플라즈마로 구축된 서브 체인은 메인체인의 트랙잭션을 완화시켜 결과적으로 이더리움 메인체인의 전체적인 트랜잭션을 감소시키는 것으로 이어진다[6].

5. 결 론

블록체인 에서는 암호화가 주로 두 가지 용도로 사용된다. 첫째, 트랜잭션 보낸 사람의 신원 보안 둘째, 과거 기록을 훼손 할 수 없다 블록체인 기술은 사용자의 신원을 보호하는 수단으로 암호화를 사용하여 트랜잭션이 안전하게 수행되고 모든 정보와 저장 장치를 안전하게 보호한다. 따라서 블록체인을 사용하는 사람은 무엇인가가 블록체인에 기록되면 합법적으로 보안을 유지하는 방식으로 완료한다는 확신을 가질 수 있다. 블록체인은 “해시함수”, “공개키 암호”, “랜덤 수”, “키 관리”, “암호 프로토콜(비잔틴 프로토콜, 멀티 파티 프로토콜 등)”, “영지식증명(ZKIP)” 등이 사용된다. 하지만 암호화 방식을 어떤 것을 채택하느냐에 따라서 블록체인의 성능이 좌우된다. 본 논문에서 제안한 성능 향상 방식을 사용하여, OTP의 단점인 블록체인의 블록생성시간 증가 및 가스의 사용량 증가에 따른 단점을 성능향상을 위해 발표된 플랫폼을 이용하여 성능향상을 최소화 하는 것을 제안한다.

References

[1] G. Y. Lee and I. H. Kim, “A Study on Application of Record Management System Block Chain Technology,” *The Korean Journal of Archival Studies*, No.60, pp.317-358, 2019.

[2] B. J. Cho, “Design and Implementation of Blockchain OTP System with Enhanced Nonrepudiation,” Master, Korea University, Korea, 2020.

[3] Y. Haung, “A Study on the tradeoff between TPS and Security in Blockchain,” Master, Dongguk University, Korea, 2020.

[4] K. H. Kim, “A TOTP-based Two Factor Authentication Scheme for Hyperledger Fabric Blockchain,” Master, Ajou University, Korea, 2018.

[5] Fork (blockchain) [Internet], https://en.wikipedia.org/wiki/Fork_(blockchain)

[6] J. Poon and V. Buterin, “Plasma: Scalable Autonomous Smart Contracts,” White paper, 2017.

[7] I. Eyal, A. E. Gencer, E. G. Sirer and R. Renesse, “Bitcoin-NG: A Scalable Blockchain Protocol,” *13th USENIX Symposium on Networked Systems Design and Implementation (NSDI ’16)*, pp.45-59, 2016.

[8] D. H. Shin and J. H. Lee, “Smart Contract Security for Fintech,” *Korea Information Processing Society Review*, Vol.22, No.5, pp.54-62, 2015.

[9] F. Ritz and A. Zugenmaier, "The Impact of Uncle Rewards on Selfish Mining in Ethereum," *Conference: 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 2018.

이 덕 규

https://orcid.org/0000-0003-4057-9558
e-mail : deokgyulee@gmail.com
2006년 순천향대학교 전산학과(박사)
2006년 ~ 2014년 한국전자통신연구원 정보보호연구본부 선임연구원
2014년 ~ 현 재 서원대학교 정보보안학과 조교수
관심분야 : 블록체인, IoT 보안, 인증