Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.34, NO.2, Apr. 2024 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2024.34.2.289

블록체인 기반 클라우드 프락시 서버의 키 효율성 연구*

성 순 화†‡
중부대학교 (교수)

Key Efficiency Evaluation of Blockchain Based Cloud Proxy Server*

Soon-hwa Sung†‡
Joongbu University (Professor)

요 약

블록체인은 증가하는 트랜잭션 수와 사용자 수로 인해 많은 계산과 네트워크 통신을 지연시켜 실시간 처리에 효율적이지 않다. 이를 해결하기 위하여, 본 연구는 클라우드 프락시 서버를 제안하므로 적법한 사용자가 블록체인을 사용할 뿐만 아니라 네트워크 지연 시간을 단축할 수 있다. 블록체인 트랜잭션 진행을 위해, 블록체인 복사 서버에서는 트랜잭션 관련 모든 데이터를 검증하지만 클라우드 프락시 서버는 간단한 영지식 증명 알고리즘으로 적법한 사용자를 검증하므로 효율적인 블록체인 실시간 처리가 가능하다. 클라우드 프락시 서버는 블록체인 사용자의 키 쌍을 등록 받아 제안한 영지식 증명으로 적법한 사용자를 검증할 수 있는 블록체인 익명성, 보안성, 확장성을 지원할 수 있다. 제안 연구 분석에서 블록체인 기반 클라우드 프락시 서버는 이전 연구들과 비교하여 네트워크 지연 시간을 단축시키고, 클라우드 프락시 서버의 키 프로세싱은 이전 연구들보다 키 계산 비용을 감소시킨다.

ABSTRACT

Blockchains are not efficient for real-time processing because the growing number of transactions and users delays many computations and network communications. This study proposes a cloud proxy server, so that legitimate users can use blockchain as well as reduce network latency. To proceed with a blockchain transaction, the blockchain copy server verifies all transaction-related data, but the cloud proxy server verifies legitimate users with a simple zero-knowledge proof algorithm, enabling efficient blockchain real-time processing. The cloud proxy server can support blockchain anonymity, security, and scalability that can verify legitimate users with the proposed zero-knowledge proof by receiving the registered key pair of the blockchain user. In the proposed research analysis, blockchain-based cloud proxy server reduces network latency compared to previous studies and key processing on cloud proxy servers reduces the cost of key computation compared to previous studies.

Keywords: Blockchain based Cloud Proxy Server, Key, P2P Cloud Proxy Server, Zero-knowledge Proof

I. 서 론

블록체인 기술을 활용할 때, 큰 장애물로 확장성과 프라이버시가 있다. 확장성의 경우는 많은 블록체인 플랫폼들이 고민하고 있는 여러 가지 합의 알고리즘 문제로, POS(Proof of Stake)[1], POS(Proof of Stake)[2], DPOS(Delegated Proof of Stake)[3], Casper[4], Practical

Received(01. 08. 2024), Modified(02. 21. 2024), Accepted(02. 21. 2024)
* 이 논문은 2023년도 중부대학교 학술연구비 지원에 의하여 이루어진 것임.
† 주저자, shsung@joongbu.ac.kr
‡ 교신저자, shsung@joongbu.ac.kr(Corresponding author)

Byzantine Fault Tolerance(PBFT)[5], Proof of Elapsed Time(PoET)[6] 등의 많은 방식으로 해결책을 고민하고 있다. 이러한 알고리즘은 많은 에너지를 소모하며 통신을 지연시켜 실시간 처리에 효율적이지 않다.

프라이버시 경우는 추적 불가한 암호화폐 해킹으로 암호화폐 사용자에게 많은 피해를 준다. 블록체인(Blockchain)은 분산 컴퓨팅 기술 기반의 데이터 위 변조 방지 기술로서, 공개 블록체인 기반 암호화폐로 많이 사용된다[7]. 암호화폐(cryptocurrency)는 암호 기술을 이용하여 만든 디지털 화폐이다. 암호화폐는 네트워크로 연결된 인터넷 공간에서 암호화된 데이터 형태로 사용된다. 암호화폐 지갑은 개인이 암호화폐를 저장하는 하드웨어 또는 소프트웨어이며, 지갑을 만들면 개인 키와 공개 키라는 두 개의 키를 받게 된다. 즉, 암호화폐 지갑은 지갑 주소와 암호로 구성되며, 지갑의 주소는 다른 사람들이 암호화폐를 송금할 수 있도록 공개해도 되는 공개키로 계좌번호에 해당된다. 개인 암호는 오직 지갑 소유자 본인만 알고 있는 개인키로 모든 거래를 암호화된 방식으로 서명한다[8].

공개 블록체인은 투명하여 외부에서 체인에 저장된 데이터를 볼 수 있다. 해싱 기술은 데이터 소유자를 숨기지만, 데이터 자체는 여전히 공개되어 있다. 이는 암호화폐 지갑을 통해 자금 흐름을 추적할 수 있다는 것이다. 따라서 공개 블록체인의 공개키, 안전한 비밀키의 프라이버시를 보장하면서 트랜잭션 처리 속도와 한정된 처리량 문제를 극복하기 위한 블록체인 확장성 문제가 필요하다.

그러므로 본 연구에서는 블록체인 네트워크 지연시간을 고려한 블록체인 익명성과 보안성, 확장성을 보장할 수 있는 Fig. 1.의 클라우드 프락시 서버를 제안한다.

클라우드 프락시 서버는 사용자(장치) A의 비밀키를 노출하지 않으면서 사용자(장치) B에게 사용자 A가 비밀키를 가지고 있다는 것을 증명하고자, 새로운 영지식 증명(Zero-Knowledge Proof) 알고리즘을 제안하며, 안전성과 확장성을 위한 연합 비잔틴 합의 알고리즘과 P2P 클라우드 환경을 제안한다.

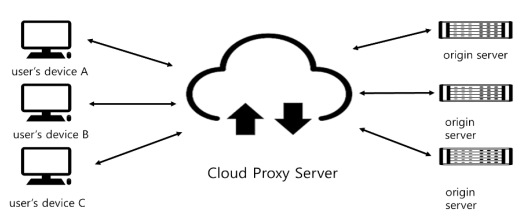

Fig. 1. Cloud Proxy Server

본 논문 구성은 2장 연구 배경, 3장 3장 블록체인 기반 클라우드 프락시 서버, 4장 분석, 5장 결론으로 구성된다.

II. 연구 배경

2.1 관련 연구

블록체인 기술은 미래 산업을 혁신적으로 바꾸어 놓을 수 있는 잠재력을 가지고 있다. 그러나 이 기술은 우리가 원하는 혁신을 이루기 위해서는 여러 가지 문제를 해결해야 한다. 블록체인 기술을 사용하는 사용자 증가에 대처할 수 있는 확장성과 확장성으로 인한 개인정보보호 소홀에 집중할 필요가 있다.

Miersr et al.[9]는 사용자의 거래 주소 유출 문제를 해결하기 위해 zero-knowledge proof[10] 기반 제로 코인(Zerocoin) 프로토콜을 제안하였다. 사용자는 트랜잭션 연결 불가를 만드는 제로 코인을 통한 거래의 양 당사자의 주소를 숨길 수 있다. 그러나 제로 코인은 발행만 가능하다. 영지식 증명의 제로 코인의 데이터는 상대적으로 크기 때문에 추가적인 블록체인 저장 공간 및 컴퓨팅 리소스를 요구한다. Sasson et al.[11]는 새로운 유형의 디지털 통화인 제로 코인 기반의 제로 캐시(Zerocash)를 제안하였다. 제로 캐시는 트랜잭션을 캡슐화하고 거래 당사자의 주소와 거래 금액을 모두 유지하는 목적을 달성하기 위해 매개변수를 커밋(commitment) 함수로 트랜잭션을 캡슐화 한다. 동시에 제로 캐시는 현재 최고 수준의 프라이버시와 익명성 통화 거래를 위해 간단한 비대화형 영지식 증명을 사용한 현금 기술(zk-SNARK)을 적용한다.

그러나, 영지식 증명 알고리즘을 사용하는 증명은 매우 느리며, 새로운 증명을 생성하는 데 보통 1분이 소요되어 비효율적이다. 블록체인의 데이터는 공개 분산 원장에 저장되므로 사용자의 기밀 정보와 트랜잭션 정보가 공개 데이터베이스에서 삭제되면 블록체인의 근본적인 문제가 해결될 것이다. 이 아이디어를 바탕으로 많은 오프체인 결제 방식이 제안되었다. 라이트닝 네트워크[12], 양방향 소액 결제 채널[13], Sprites[14], Bolt[15] 등의 오프체인 결재 기술은 신뢰할 수 있는 오프체인 거래를 제공하기 위

해 사용된다. 링 서명을 사용한 Monero[16]는 링 기밀 트랜잭션, 암호화 소스, 금액 및 대상을 난독화하는 주소가 사용자에게 더 큰 프라이버시를 제공하나, 링 서명 과정에는 많은 시간이 필요하였다. Boyen[17]은 연동 가능한 링 서명과 제품을 사용한 VOTOR 같은 실용적인 원격 투표 방식을 제안했다. 이는 더 높은 수준의 프라이버시를 제공하는 익명성 채널을 사용하였으나, 역시 링 서명 과정에 많은 시간을 소비하였다. Mourad et al.[18]는 새로운 공급망을 도입하여 민감한 개인 정보에 기반한 체인 추적 시스템을 적용하였다. 정보의 기밀성을 달성하기 위한 MLSAG 링 서명 프로토콜을 사용하였지만 MLSAG 링 서명 프로토콜은 네트워크 지연 시간을 초래했다. Patil and Wasnik[19]은 인증서 검증 프로세스를 구축하고 ID 기반 링 서명 기술을 사용하였으나 많은 사용자와 그들의 데이터를 지원할 수 없는 현재의 PKI 시스템의 병목 현상을 야기하였다. Pandey and Kulkarni[20]은 데이터 공유 중 개인 익명성 및 순방향 보안을 위한 신원기반 링 서명 기술을 채택하여 ID 링 서명과 함께 데이터 보안을 향상시켰고, J. Lui et al.[21]은 인터넷 차량의 프라이버시를 보호하기 위한 격자 기반의 새로운 링 서명 방식을 제안하였으나 기존의 공개키 암호화 방식과 달랐고, 양자 알고리즘 공격에서 보안을 보장할 수 있는 격자 링에 잘못된 학습 문제를 기반으로 설계되었다. Surmila와 Dilip[22]은 신뢰할 수 없는 클라우드 스토리지에서 아웃 소싱된 정적 사용자와 정적 그룹 간에 공유되는 동적 데이터의 무결성 확인을 위한 링 서명 기반 체계를 제안하였지만 서명자 추적이 필요한 소그룹과 애플리케이션에 적합하므로 블록체인 기반의 확장성이 미비하다.

2.2 영지식 스나크 알고리즘

영지식 스나크 알고리즘은 간결한 비대화형 영지식으로 증명 계산이 올바르다는 사실 외에는 증인 값에 대해 아무 정보도 노출하지 않도록 보장한다. 이는 키생성(Keygen), 증명(Prove), 검증(Verify) 세 과정으로 이루어진다.

1. Keygen : key generator G를 이용해 key pair (pk, vk)를 생성하는 과정

증명자가 알고 있다고 주장하는 값인 witness(w)가 있다. 이때 이를 매개변수로 받는 특정 프로그램 C가 있다고 하자. 프로그램 C는 다음과 같다고 가정한다.

```
function C(x,w) {
return (hash(w)==x);
}
```

이와 같이 내가 w를 알고 있음을 증명할 수 있는 프로그램 C와 무작위 표본추출 시드(random sampling seed)인 람다(lambda)를 제너레이터에 매개변수로 삽입함으로써 키 쌍을 생성할 수 있다. 여기서 람다는 증명자 및 외부에 노출되어서는 안 된다. 왜냐하면 이 값을 알고 있는 증명자가 거짓 증명을 생성할 수 있기 때문이다. 그렇기 때문에 키 생성은 검증자가 수행하게 된다.

- G(C, lambda) = (pk, vk)
- pk = proving key
- vk = verifying key

C의 program size bound를 1, input(x) size의 bound를 n, execution time bound를 T라고 할 때, 키 생성의 시간 복잡도는 아래와 같다.

$$O(1+n+T) \cdot \log(1+n+T)$$

즉, 프로그램이 길고, 투입 사이즈가 크고, 실행 시간이 길수록 키 생성에 소요되는 시간이 길다.

2. Prove : prover가 proof(prf)를 생성하는 과정

증명 알고리즘을 P, 증명하고자 하는 증인인 w, w의 해시를 x라고 할 때, 증명을 구하는 방법은 다음과 같다.

$$prf = P(pk, w, x)$$

증명자는 prf를 계산한 후, 검증자에게 prf만을 전달한다. prf을 계산하는 데 걸리는 시간은 입력값 x와 w의 크기에 비례하여 길어진다. prf가 계산된 이후에는 당연히 prf로부터 w값을 유추할 수 없으며, prf의 길이는 매우 짧다. 이는 기존의 영지식 증명이 가지고 있지 않은 간결함의 특성을 갖게 해주는 요소이다.

3. Verify : verifier가 prf를 검증하는 과정

검증자는 증명자로부터 prf를 전달받은 후, 검증 알고리즘 V(verifying algorithm V)를 수행하여 prf의 진위 여부를 판단한다. 검증에 걸리는 시간은 매우 짧은데, 이 역시 영지식 스나크가 간결함의 특성을 가지는 요소 중 하나이다. 아래 불형에서 검증키 vk로 증명 알고리즘 prf의 x와 검증 알고리즘 v의 x가 일치하면 증명자는 w값을 정말 알고 있다고 TRUE라 할 수 있고, FALSE이면 증명자는 w값을 속였다고 판단할 수 있다.

boolean: v(vk, x, prf) [23]

2.3 영지식스나크(zk-SNARKs: zero-knowledge Succinct Non-interactive Argument of Knowledge) 알고리즘의 단점

영지식 스나크는 블록체인 환경에서 증명의 크기가 작고 신속하게 증명자와 검증자 사이의 상호작용이 거의 없거나 전혀 없는 영지식 증명을 구현할 수 있게 했다. 영지식 스나크를 활용한 블록체인 트랜잭션의 경우 수신자, 송신자, 전송금액 등의 정보를 노출하지 않고도 해당 트랜잭션의 유효성을 송수신 노드 외의 다른 노드들에게 알릴 수 있다. 반면에 비상호작용 구조에서는 증명자와 검증자가 하나의 증거만 주고받아도 된다. 영지식 스나크는 증명자와 검증자 사이의 신뢰할 수 있는 초기 설정에 의존한다. 즉 영지식 증명 및 개인거래를 구축하기 위하여 일련의 고객 매개 변수가 필요한 것이다. 이 매개 변수는 게임의 규칙과 거의 상응하며 프로토콜에 인코딩 되어 트랜잭션이 유효하다는 것을 증명하기 위해 필요한 요소이다. 그러나 매개 변수가 매우 작은 그룹에 의하여 공식화되는 경우가 있기 때문에 잠재적으로 중앙집중화 문제가 존재한다. 즉, 영지식 스나크의 가장 큰 문제점은 신뢰기관(trusted party)의 존재이다. 프로토콜 내에서 신뢰기관의 역할은 매우 크며, 증명을 생성하는 데 있어서도 큰 비중을 차지하고 있다. 신뢰기관은 노출되면 안 되는 정보를 통해 거짓 증명(fake proof)을 생성할 수 있으며, 외부의 다른 집단과 공모할 가능성 또한 있다. 그리고 영지식 스나크는 복잡성이 증가할수록 점점 더 높은 연산처리능력이 필요하다. 증명 데이터와 검증 과정이 획기적으로 간결해졌지만 증명자가 증명을 생성하는 시간이 매우 느리다는 문제점이 있다[23].

따라서 본 연구는 블록체인 시스템에서 공격자가 스스로 비밀키를 생성하여 영지식 증명을 통과하는 것을 막기 위하여 검증자가 키 생성 등록을 하고 증명자가 증명을 생성하는 시간을 줄이기 위해 블록체인 기반 클라우드 프락시 서버에 적합한 영지식 증명(Zero-knowledge proof) 알고리즘을 제안한다.

III. 블록체인 기반 클라우드 프락시 서버

공개 블록체인 기반 P2P 클라우드 프락시 서버는 영지식 스나크의 문제점인 신뢰기관 존재를 해결하기 위한 탈중앙화에 적합한 P2P를 도입한다. 이는 개인정보의 키만 관리하기 위한 메커니즘으로 P2P 클라우드 프락시 서버의 악의적인 노드와 오류 발생 노드가 존재할 경우, 연합 비잔틴 합의 알고리즘으로 해결한다. 이는 제안한 새로운 영지식 증명을 사용하여 익명성과 블록체인 트랜잭션 지연 시간을 개선하며, P2P 도입으로 블록체인 확장성에 기여할 수 있다.

3.1 P2P(Peer to Peer) 클라우드 프락시 서버

클라우드 프락시 서버는 블록체인의 탈중앙화 환경에 적합한 P2P 클라우드 프락시 서버 네트워크를 구성한다. P2P는 상호 연결된 노드(peer)들이 서로 자원을 공유하는 네트워크이다. 제안 서버는 블록체인과 블록체인 복사 서버인 원래 서버(origin server) 혹은 거래소의 중간 지점으로 정당한 사용자임을 키로만 검증하여 사용자의 거래 내역, 거래금액 등을 검증하는 시간을 줄일 수 있다. 사용자 키 생성 등록 시, 키 증명을 마친 키 검증자가 키 등록을 한다. 이는 공격자가 비밀키 생성을 막기 위함이다. 클라우드 프락시 서버 CPS_1에 사용자 키 생성을 한번 등록하면 생성된 사용자 키는 클라우드 프락시 서버 CPS_2, CPS_3,…..CPS_{n-2}, CPS_{n-1}, CPS_n에 공유된다. 또한, 임의의 클라우드 프락시 서버 CPS_n에 사용자 키 오류 공격을 받아도 다른 클라우드 프락시 서버에서 동일한 사용자 키를 공유하기 때문에 정상적인 키 프로세스가 이루어진다. 이는 악의적이거나 고장 발생 노드가 존재하는 상황에서 Fig.2.에서와 같이 연합 비잔틴 합의(FBA : Federated Byzantine Agreement) 메커니즘을 적용하기 때문이다.

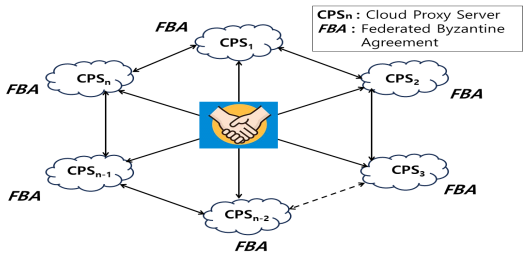

Fig. 2. P2P cloud proxy server with FBA

3.2 클라우드 프락시 서버의 새로운 영지식 증명

클라우드 프락시 서버는 블록체인 공격자가 스스로 비밀키를 생성하여 영지식 증명을 통과할 수 없도록 검증자가 키 등록을 진행한다. 그리고 제안 서버는 개인거래를 구축하기 위한 일련의 고객 매개 변수로 트랜잭션 유효성을 증명하기 위한 시간을 단축하는 메커니즘이다.

트랜잭션 유효성을 증명하려면 누구의 트랜잭션인가를 익명성으로 증명하면 되므로 블록체인 사용자의 암호화폐 지갑에 있는 공개키와 비밀키가 서로 일치한다는 사실만 증명하면 된다. 이를 위한 새로운 영지식 알고리즘은 키 생성에서 증명자가 유효한지를 확인 후, 검증자가 키 등록을 진행한다. 이때 클라우드 프락시 서버는 데이터 소유자의 검증된 키 생성을 한 번만 등록한다.

클라우드 프락시 서버는 원본 콘텐츠에 액세스하지 않고 사용자 유효성 검사를 수행하여 블록체인 공개 분산 원장에 저장된 사용자의 기밀 정보인 사용자 키 쌍을 가져온다. Fig.3.에서와 같이 클라우드 프락시 서버는 분산 원장에서 가져온 사용자 키 쌍만 관리하고, 공개 분산 원장에는 사용자의 기밀 정보와 트랜잭션 정보가 그대로 저장된다. 필요시 클라우드 프락시 서버와 공개 분산 원장은 서로 통신하여 사용자의 기밀 정보와 트랜잭션 정보가 일치하는지 확인

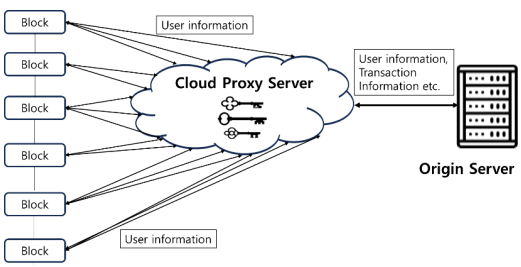

Fig. 3. User information flow in blockchain based cloud proxy server

할 수 있다. 따라서 검증자는 전체 암호화 데이터를 다운로드하지 않고도 클라우드 프락시 서버에 등록된 사용자 키 쌍으로만 사용자 검증을 할 수 있다. Fig.4.에서 클라우드 프락시 서버는 새로운 영지식 증명 알고리즘으로 사용자 키를 검증한다.

다음은 클라우드 프락시 서버에 적합한 새로운 영지식 증명 알고리즘의 6단계를 기술한다. 1~3단계는 익명성을 고려한 사용자(증명자) A 증명과 검증이 유효한지를, 4~6단계는 사용자(검증자) B가 증명과 검증이 유효한가를 기술한 알고리즘이다.

1. Set up(설정)
   P_{KI} :사용자 A 공개키
   S_{KI} :사용자 A 비밀키
   p_1: large prime number
   r_1: random number
   g_1: generator
   t_1: time stamp
   tsn_1: tag serial number
   H: hash function

2. Prove(증명자가 증명 생성)
   (1) r_1선택
   (2) $C_1 = H(g_1,\ p_1,\ t_1,\ tsn_1)$
   (3) $S_1 = (r_1 + S_{KI} * C_1) \bmod p_1$

3. Verify(검증자가 증명 검증)
   (1) S_1를 받아온다
   (2) $C_1 = H(g_1,\ p_1,\ t_1,\ tsn_1)$
   (3) $g_1^{\wedge S1} \equiv P_{KI}^{\wedge C1 (\mathrm{mod}\ p1)}$ 만족하면 증명자 A 증명이 유효

4. Reset up(재설정)
   P_{K2} :증명자 B 공개키
   S_{K2} :증명자 B 비밀키

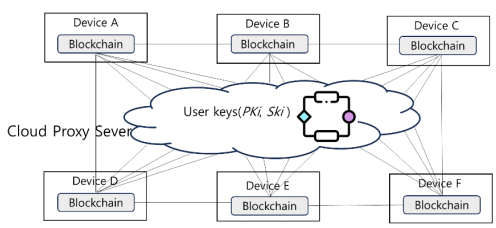

Fig. 4. User keys of blockchain based cloud proxy server

p_2: large prime number
r_2: random number
g_2: generator
t_2: time stamp
tsn_2: tag serial number

5. Reprove(증명자가 재증명 생성)
   (1) r_2선택
   (2) $C_2 = H(g_2,\ p_2,\ t_2,\ tsn_2)$
   (3) $S_2 = (r_2 + S_{K2} * C_2) \bmod p_2$

6. Reverify(검증자가 재증명 검증)
   (1) S_2를 받아온다
   (2) $C_2 = H(g_2,\ p_2,\ t_2,\ tsn_2)$
   (3) $g_2^{S2} \equiv P_{K2}^{C2} \pmod{p2}$ 만족하면 증명자 B 증명이 유효

클라우드 프락시 서버에서는 블록체인 개인 정보만 다루기 때문에 기존의 영지식 알고리즘에서 커밋 함수의 매개 변수를 제거하는 대신 타임 스탬프(time stamp)와 태그 시리얼 넘버(tag serial number)를 추가하였다. 또한 새로운 영지식 알고리즘은 블록체인 공격자가 스스로 비밀키를 생성하여 영지식 증명을 통과할 수 없도록 검증자가 키 등록을 진행한다. 따라서 제안 서버는 영지식 스나크 알고리즘의 증명자가 증명 생성하는데 많은 시간이 걸린 것을 단축시킬 수 있으며, 블록체인 공격자를 방어할 수 있다.

3.3 블록체인 기반 클라우드 프락시 서버의 키 프로세스

사용자는 키 등록 시 클라우드 프락시 서버에게 시리얼 넘버가 있는 태그를 발급받는다. 태그는 키와 함께 존재하며 태그와 키는 단 한번 만 부여 받는다. 태그 시리얼 넘버가 같으면 에러를 발생시킬 수 있도록 설정한다. 클라우드 프락시 서버는 Fig.5.와 같이 키 프로세스를 진행한다. 단, 원래 서버는 인증된 안전한 서버임을 가정한다.

1. 클라우드 프락시 서버는 사용자(장치) 키 등록을 받는다.
2. 사용자는 클라우드 프락시 서버로부터 암호화 키와 태그 시리얼 넘버를 받는다.

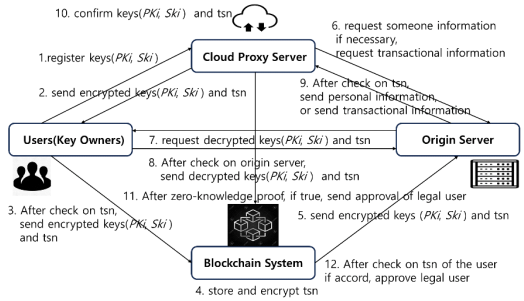

Fig. 5. Sequential diagram of blockchain based cloud proxy server

3. 사용자는 암호화 키와 태그 시리얼 넘버를 블록체인 시스템으로 보낸다.
4. 블록체인 시스템은 태그 시리얼 넘버를 저장하고 암호화한다.
5. 블록체인 시스템은 암호화 키와 태그 시리얼 넘버를 원래 서버에게 보낸다.
6. 클라우드 프락시 서버가 개인 정보(필요 시 트랜잭션 정보)를 원래 서버에게 요청한다.
7. 원래 서버는 사용자에게 복호화 키와 태그 시리얼 넘버를 요구한다.
8. 사용자는 원래 서버를 확인 후, 복호화 키와 태그 시리얼 넘버를 원래 서버로 보낸다.
9. 원래 서버는 블록체인 시스템으로부터 받은 태그 시리얼 넘버와 일치하는지 확인한다. 일치하면, 원래 서버는 클라우드 프락시 서버로 개인 정보(필요 시 트랜잭션 정보)를 보낸다.
10. 클라우드 프락시 서버는 키와 태그 시리얼 넘버를 확인한 후, 제안한 영지식 증명을 진행한다.
11. 영지식 증명 후 참이면, 클라우드 프락시 서버는 적법한 사용자의 승인을 블록체인 시스템으로 보낸다.
12. 블록체인 시스템은 태그 시리얼 넘버를 체크한 후, 일치하면 적법한 사용자로 인정한다.

IV. 분 석

4.1 네트워크 분석

본 연구에서는 노드가 체인에 새로운 블록을 삽입하기 전, 네트워크 신뢰를 위해 사용자 키 쌍 증명을 위한 클라우드 프락시 서버를 제안하여 네트워크 지연 시간을 단축하려고 하였다. 네트워크 지연 시간을

실험 분석하기 위하여 Intel(R) CoreTM i5-10210U CPU @ 1.60GHz 2.11GHz, RAM 8.00GB, 64비트 운영체제를 사용하였다. 그리고 단위 시간당 트랜잭션 지연 시간을 클라우드 시뮬레이션으로 비교 분석하기 위하여 클라우드 시뮬레이션을 위한 설정 입력으로 트랜잭션 수, 트랜잭션 평균 프로세싱, 프로세싱 편차, 트랜잭션 부하 등으로 정하였고 Amazon CloudFront[24]를 사용하였다.

M. T. de Oliveira et al.[25]는 새로운 블록을 삽입하기 전에 네트워크 신뢰를 위해 주어진 네트워크 신뢰 임계값보다 높은 평가 점수를 가져야 하는 BRBC(Blockchain Reputation-Based Consensus) 메커니즘을 제안하였다. 불필요한 메시지 교환을 피하면서 각 노드의 평가를 모니터링하기 위해 모든 노드 네트워크 대신 심사 노드를 선택하기 위하여 진입 요청, 진입 승인, 모든 진입 승인, 새 마이너의 유효성 확인, 모든 새 마이너의 승인을 하는 단계를 진행한다. 이러한 여러 단계를 진행하기 위하여 많은 네트워크 시간을 요구하였지만 H. Wang et al.[26]보다는 네트워크 지연 시간이 짧게 걸렸다. H. Wang et al.[26]은 퍼블릭 클라우드 스토리지 감사를 위한 블록체인 기반 공정 지불 스마트 계약을 설계하여 계약 실행에서 상호작용의 수를 줄이기 위해 비대화형 공공 증명 가능 데이터 소유의 개념을 제시하였다. 제안한 시스템 모델의 비대화형 공개 증명 데이터 소유(NI-PPDP) 방식은 4개의 알고리즘으로 구성된다. 스마트 계약을 배포한 후에는 사용자 및 시스템의 모든 스마트 계약 플랫폼 간의 챌린지 응답 상호 작용이 필요하지 않는다. 하지만 클라우드 서비스 공급자가 정기적으로 데이터 소유 증명을 제출하도록 요구하고, 공유 감사 메커니즘을 필요로 하므로 M. T. de Oliveira et al.[25]와 A. Li et al.[27]보다 네트워크 지연 시간이 길었다. A. Li et al.[27]은 블록체인 기반 교차 사용자 데이터 공유 감사를 위한 암호 인증 키 교환 프로토콜을 활용하여 공유 감사 및 암호문 중복 제거를 달성하고 데이터 저장 및 데이터 사용자에 대한 감사 비용을 줄이는 제안을 하였다. 그러나 공유 감사의 추가 키 교환 단계로 인한 네트워크 지연 시간을 초래하였지만 M. T. de Oliveira et al.[25]와 H. Wang et al.[26]보다 지연 시간이 짧았다.

제안한 연구는 적법한 사용자를 블록체인 기반 클라우드 프락시 서버의 사용자 키만 검증하여 트랜잭션을 진행하므로 원래 서버의 트랜잭션 관련 모든 데이터를 링 서명 및 검증하는 시간을 줄일 수 있다. Fig.6.에서와 같이 제안한 연구가 가장 향상된 네트워크 시간 효율성을 보여 주었다.

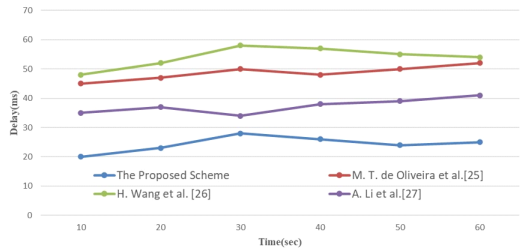

Fig. 6. Comparison of network delay time for time complexity

4.2 보안 분석

클라우드 프락시 서버의 키 프로세스는 새로운 영지식 알고리즘으로 공격자가 스스로 비밀키를 생성할 수 없도록 하였다. 제안한 서버는 3.2에서 $g_1^{\wedge S1} \equiv P_{K1}^{\wedge C1 (\mathrm{mod}\ p1)}$ 에서 증명자 A 증명이 유효하고, $g_2^{\wedge S2} \equiv P_{K2}^{\wedge C2 (\mathrm{mod}\ p2)}$ 에서 증명자 B 증명이 유효할 때, 키 생성 등록을 할 수 있다. 제안 서버의 새로운 영지식 알고리즘은 증명자의 증명 생성과 검증자의 증명 검증을 진행함으로써, 증명자 A가 증명자 B에게 증명자 A의 공개키에 해당하는 비밀키 값을 노출하지 않고 익명성을 유지하면서 증명자 B에게 비밀키 값을 가지고 있는다 것을 증명할 수 있다.

P2P 클라우드 프락시 서버의 악의적인 노드와 고장 발생 노드가 존재할 경우, 연합 비잔틴 합의 알고리즘으로 해결한다. 이때 원래 서버는 인증된 안전한 서버임을 가정한다. 연합 비잔틴 합의 알고리즘은 N이 P2P 클라우드 프락시 서버 내 모든 노드 집합이고, Q는 모든 정족수 슬라이스 집합, $Q(i)$는 노드 i의 정족수 슬라이스, T는 합의에 필요한 임계치라 할 때, 장애 허용성은 잘못된 노드 수가 T보다 작은 경우에 유지된다. 클라우드 프락시 서버 CPS_1에 등록된 사용자 키는 CPS_2, CPS_3,…..CPS_{n-2}, CPS_{n-1}, CPS_n에 공유된다. 만약 CPS_1의 키가 공격을 받거나 악의적인 키가 있다고 하더라도, 모든 서버 CPS_n에 키를 공유하고 있기 때문에 연합 비잔틴 합의 알고리즘에 의하여 키 프로세스는 정상적으로 진행된다. 따라서 제안 서버는 연합 비잔틴 합의 알고리즘으로 동시 다발적인 많은 사용자 키 정보 검

증 요청에도 능동적으로 대처할 수 있다.

4.3 키 계산 비용

블록체인 시스템은 거대한 네트워크로 참가자의 키 또한 많다. 클라우드 프락시 서버에 등록한 사용자 키 컴퓨팅 비용을 분석하려고 한다. 통신을 할 때마다 모든 키 $K=\{K_1,K_2,\cdots,K_i,\cdots K_m\}$ $\forall i=1$ to m, m는 데이터가 변함에 따라 달라진다. 키 K_i가 만족하면 집합 $S=\{S_1,S_2,\cdots,S_i,\cdots,S_m\}$, $\forall i=1$ to m 에 결합된다. 모든 키가 S_i에 결합될 때, 사용자는 블록체인에 참가하고 결합하고 떠날 수 있다.

본 연구는 단위 시간당 트랜잭션 1개가 사용하는 키 프로세싱에 필요한 계산 비용을 응답 시간으로 분석하기 위하여 4.1 분석을 위한 환경을 그대로 사용하였다. 클라우드 시뮬레이션을 위한 설정 입력으로 키 개수, 도전키 요소 개수, 키 프로세싱 평균 및 편차, 키 인증, 키 프로세싱 부하 등으로 정하였고 Amazon CloudFront[24]를 사용하였다. Fig.7.에서 Kalyani and Pallavi[28]은 헤더 수준 패턴 분석으로 최소한의 오버헤드로 효율적인 소유권 제어를 허용하는 컨소시엄 블록체인 모델을 제안하였다. 헤더 수준 패턴 분석과 컨소시엄 블록체인의 결합으로 인해 모델은 추적성, 신뢰성, 불변성 및 분산 컴퓨팅 기능을 유지할 수 있으나, IP 주소와 매핑된 사용자를 위한 생성 데이터와 사용자 인증에 걸리는 시간이 많았다.액세스 제어 및 패턴 분석 모델과 통합되어 제안된 프레임워크는 여러 유형의 공격 가능성을 줄일 수 있으나, 다양한 공격이 클라우드 배포에 주입되어 키 프로세싱 검증 비용이 Zhou et al.[29]보다 높았다.

Zhou et al.[29]는 전체 파일 대신 문제가 있는 부분 블록만 암호화하면 되는 후속 업로드를 확인하기 위해 서버가 추가 메타데이터를 저장할 필요가 없는 클라이언트 측 중복 제거 프로토콜을 제안하였다.

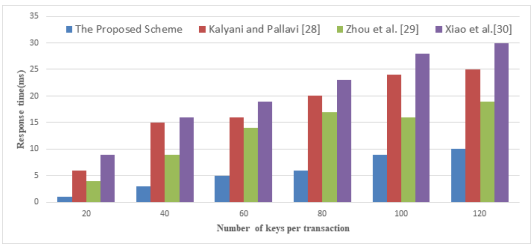

Fig. 7. Comparison of key computation cost

사용자가 데이터를 잃지 않도록 보호하기 위해 스마트 계약을 기반으로 한 전투 메커니즘을 설계하였고, 보안성 강화에 집중된 메커니즘 프로세싱에 많은 시간이 필요했으나, Kalyani and Pallavi[28]과 Xiao et al.[30]보다는 키 비용이 절감되었고 제안 연구보다는 키 비용이 증가하였다. Xiao et al.[30]은 동적 데이터에 대한 블록체인 기반 협업 공공 감사 체계를 제안하여 최신 블록 해시를 사용한 챌린지 세트를 생성하도록 클라우드 서비스 공급자를 설계하였고, 데이터 업데이트를 위해 블록체인의 특성에 맞게 인덱스 관리 구조의 크기를 줄이고 업데이트 작업을 일정한 시간 복잡도로 만드는 인덱스 관리 구조를 도입하였다. 또한, 블록체인과 클라우드 서비스 공급자, 데이터 소유자로 데이터 소유자는 클라우드 서비스 공급자에 데이터 업로드를 해야 하며, 셋업 알고리즘에서 키 공유 알고리즘 등 검증과 업데이터 알고리즘 모두 7단계 알고리즘으로 구성되어 Kalyani and Pallavi[28]과 Zhou et al.[29] 연구보다 키 프로세싱에 많은 시간이 소요되었다.

V. 결 론

본 연구는 클라우드 프락시 서버를 제안하여 블록체인 트랜잭션에서 필요한 키의 소유권을 검증할 수 있는 별도의 메커니즘을 구현하였다. 이로 인해 키 소유자를 빨리 검증할 수 있으며, 익명성 제공과 함께 지연 시간을 단축시키는 트랜잭션 처리 효율성을 향상 시켰다.

클라우드 프락시 서버는 제안한 영지식 증명 알고리즘과 익명성을 보장한 블록체인 기반 키 프로세스를 구성하였다. 이러한 메커니즘은 블록체인 익명성을 보장하면서 네트워크 지연 시간을 감소시킴으로써 탈중앙화의 블록체인 단점인 실시간 처리 시간 향상에 기여하였다. 제안한 키 프로세스는 클라우드 프락시 서버와 블록체인 시스템 그리고 블록체인 복사 서버인 원래 서버와 연합 비잔틴 동의로 안전하고 효율적인 통신으로 네트워크 지연 시간을 감소시켰다.

이전 연구인 M. T. de Oliveira et al.[25], H. Wang et al.[26], A. Li et al.[27]와 비교 분석한 결과, 본 연구는 효율적인 알고리즘 계산으로 네트워크 지연 시간이 가장 향상되었다. 또한 클라우드 프락시 서버의 키 계산 비용은 Kalyani and Pallavi[28], Zhou et al.[29], Xiao et al.[30]과 비교 분석한 결과, 본 연구가 가장 키 계산 비용이 낮음을 알 수 있

었다.

제안 연구는 비밀 블록체인 기반 비즈니스 프로세스 자동화에 기여할 수 있으며, 제안 클라우드 프락시 서버는 모든 네트워크와 호환할 수 있으며, 다수의 공개 블록체인을 연결하는 가용성 데이터 레이어 기반 확장성이 있다.

References

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," https://www.klausnordby.com/bitcoin/Bitcoin_Whitepaper_Document_HD.pdf, 2008.

[2] Hui, Ken YK et al., "Small-world overlay P2P networks: Construction, management and handling of dynamic flash crowds." Computer Networks vol.50, no.15 , pp. 2727-2746, 2006.

[3] Y. Zhu, "Security architecture and key technologies of blockchain," International Journal of Information Security Research, vol. 2, no. 12, pp.1090-1097, 2016.

[4] L. Lamport et al., "The Byzantine generals problem," International Journal of ACM Transactions on Programming Languages and Systems, vol. 4, no. 3, pp. 382-401, 1982.

[5] D. Liu and J. Camp, "Proof of work can work," International Workshop on the Economics of Information Security, Apr. 2006.

[6] P. Vasin, "BlackCoin's proof-of-stake protocol v2," White paper, https://blackcoin.org/blackcoin-pos-protocol-v2-whitepaper.pdf

[7] Google,"Blockchain," https://namu.wiki/w/%EB%B8%94%EB%A1%9D%EC%B2%B4%EC%9D%B8, Oct. 2023.

[8] Google,"Cryptocurrency," http://wiki.hash.kr/index.php/%EC%95%94%ED%98%B8%ED%99%94%ED%8F%90, Nov. 2023.

[9] I. Miers et al., "Zerocoin: Anonymous distributed E-cash from bitcoin," Proceedings of IEEE Symposium on Security and Privacy, pp. 397-411, May 2013.

[10] C. Rackoff and D.R. Simon, "Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack," Proceedings of Annual International Cryptology Conference pp. 433-444, 1991.

[11] E.B. Sasson et al., "Zerocash: Decentralized anonymous payments from bitcoin," Proceedings of IEEE Symposium on Security and Privacy, pp. 459-474, May 2014.

[12] C. Decker and R. Wattenhofer, "A fast and scalable payment network with bitcoin duplex micropayment channels," Proceedings of International Symposium on Stabilization, Safety, and Security of Distributed Systems, pp. 3-18, Aug. 2015.

[13] J. Poon and T. Dryja, "The bitcoin lightning network :Scalable off-chain instant payments," Draft Version 0.5, https://static1.squarespace.com/static/6148a75532281820459770d1/t/61af971f7ee2b432f1733aee/1638897446181/lightning-network-paper.pdf, Nov.2023.

[14] A. Miller et al., "Sprites and State Channels: Payment channels that go faster than lightning," https://doi.org/10.48550/arXiv.1702.05812, Dec. 2023.

[15] M. Green and I. Miers, "Bolt: Anonymous payment channels for decentralized currencies," Proceedings of ACM Conference on Computer and Communications Security, pp. 473-489, 2017.

[16] Kumar A. et al., "A traceability analysis of monero's blockchain", Proceedings of European Symposium on Research in Computer Security, pp. 1-14, Apr. 2017.

[17] X. Boyen and T. Haines , "VOTOR: Conceptually simple remote voting against tiny tyrants," Proceedings of Australian Computer Science Week Multiconference, pp. 1-13, Feb. 2016.
[18] Mourad E.M. et al., "DECOUPLES: A decentralized, unlinkable and privacy-preserving traceability system for the supply chain," Proceedings of the ACM Symposium on Applied Computing, pp. 364-373, Apr. 2019.
[19] K. Patil and C.T. Wasnik, "An ID-based block ring signature system for secret sharing of data," Proceedings of International Conference Computer Communication and Informatics, pp.1-5, Jan. 2017.
[20] V. Pandey and U. Kulkarni, "Effective data sharing with forward security: Identity based ring signature using different algorithms," Proceedings of International Conference Intelligent Computing and Control, pp.1-6. Jun. 2017.
[21] J. Lui et al., "Ring signature based on latice and VANET privacy preservation," International Journal of Tsinghua Science and Technology, vol. 24, no. 5, pp. 575-584, Oct. 2019.
[22] Surmila. T. and Dilip K.S., "Efficient scheme for dynamic cloud data shared within a static group with privacy preserving auditing and traceability," Proceedings of International Conference on Cloud Computing and Internet of Things, pp. 25-32, Oct. 2018.
[23] Google,"zk-SNARKs": http://wiki.hash.kr/index.php/%EC%98%81%EC%A7%80%EC%8B%9D_%EC%8A%A4%EB%82%98%ED%81%AC, Nov. 2023.
[24] "Amazon CloudFront", https://aws.amazon.com/ko/cloudfront, Nov. 2023.
[25] M.T. de Oliveira et al., "Blockchain reputation-based consensus: A scalable and resilient mechanism for distributed mistrusting applications," International Journal of Computer Networks, vol. 179, Oct. 2020.
[26] H. Wang et al, "Blockchain-based fair payment smart contract for public cloud storage auditing," International Journal of Information Sciences, vol. 519, pp. 348 - 362, May 2020.
[27] A. Li et al. "Blockchain-based cross-user data shared auditing," International Journal of Connection Science, vol. 34, no. 1, pp.83 - 103, Jul. 2021.
[28] Kalyani N.P. and Pallavi V.C., "CBSOACH: Design of an efficient consortium blockchain-based selective ownership and access control model with vulnerability resistance using hybrid decision engine," International Journal of Computational Science and Engineering, Vol. 26, No. 2, pp. 129-142, Mar. 2023.
[29] Zhou J. et al., "Blockchain-based secure deduplication against duplicate-faking attack in decentralised storage," International Journal of Computational Science and Engineering, vol.26. no.4, pp. 406-417, 2023.
[30] Xiao J. et al.,"A collaborative auditing scheme with dynamic data updates based on blockchain", International Journal of Connection Science, vol. 35 no. 1, jun. 2023.

〈저자소개〉

성 순 화 (Soon-hwa Sung) 종신회원
1983년 2월: 경북대학교 전자공학과(전산) 졸업
2005년 8월: 충남대학교 컴퓨터공학과 박사
2002년 9월~2020년 2월: 충남대학교 강사, 전임연구원, BK전임교수, 초빙교수
2020년 3월~2021년 8월: 충북대학교 초빙교수
2023년 3월~현재: 중부대학교 교수
〈관심분야〉 키 인증, 모바일 결제시스템, 블록체인 기반 미래 인터넷