컨소시엄 블록체인에서의 Privacy를 위한 익명프로토콜에 관한 기법 및 연구+)

라경진*, 이임영**
*순천향대학교 컴퓨터학과
e-mail:rababi@sch.ac.kr*, imylee@sch.ac.kr**

A Study on Anonymous Protocol for Privacy in Consortium Block Chain

Gyeong-Jin Ra*, Im-Yeong Lee**
*,**Dept of Computer Science and Engineering, Soonchunhyang University

요 약

컨소시엄 블록체인은 허가된 멤버로 구성된 여러그룹이 하나의 원장을 공유한다. 이때 하위멤버의 트랜잭션 및 멤버 인증은 블록생성에 참여하는 신뢰된 노드로부터 유효성을 검증받는다. 따라서 컨소시엄 블록체인의 그룹 간 멤버의 트랜잭션 공유는 Privacy문제를 야기한다. 본 논문에서 컨소시엄 블록체인에서의 privacy를 위해 익명신용장기반의 익명프로토콜을 제안한다. 본 제안 방식은 다중블룸필터를 이용하여 긍정오류율을 높이고 효율적으로 검색하도록 한다. 또한 Blind Signature를 통해 컨소시엄 멤버간 메시지에 대한 익명성을 보존하면서 인증에 대한 서명은 유지하도록 한다. 결과적으로 컨소시엄 멤버 간 Privacy를 보존하면서 인증 트랜잭션을 블룸필터의 다중패턴으로 검증하여 컨소시엄 블록체인에서의 익명프로토콜(Anonymous protocol)을 제안한다. 이로써 컨소시엄 블록체인에서의 신뢰기반의 서버 시스템의 확장과 privacy 향상을 제공한다.

1. 서론

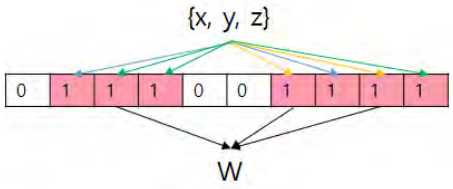
컨소시엄 블록체인은 허가된 멤버와 이로 구성된 그룹끼리 원장을 블록체인 형태로 공유한다. 따라서 멤버의 인증을 수행하면서 다른 그룹멤버간의 Privacy는 보장해야 한다[1]. 이와 유사한 형태로 퍼블릭 블록체인에서는 Lightweight Node는 SPV의 블룸필터를 통해 자신의 정보를 노출하지 않으면서도 Full Node로부터 안전하고 효율적으로 트랜잭션을 검증 값을 받는다. 이는 Full Node가 블록의 헤더와 바디를 모두 갖고 있어 스스로 검증 가능이 가능하기 때문이다. 하지만 컨소시엄 블록체인은 트랜잭션의 검증뿐만 아니라 멤버의 인증이 필요하다. 또한 블룸필터는 패턴의 수와 검증에 대한 확률이 Trade-off를 가지고 있어 많은 패턴을 만들수록 긍정오류가 높아지지만 오버헤드가 증가한다. 따라서 본 논문에서는 컨소시엄 블록체인 환경에 적합하도록 다중블룸필터를 이용하여 긍정오류율을 높이고 멤버 인증 및 트랜잭션을 효율적으로 검색하도록 한다.한 Blind Signature를 통해 컨소시엄 멤버간 메시지에 대한 익명성을 보존하면서 인증에 대한 서명은 유지하도록 한다. 결과적으로 컨소시엄 멤버 간 Privacy를 보존하면서 인증 트랜잭션을 블룸필터의 다중패턴으로 검증하여 컨소시엄 블록체인에서의 안전하고 효율적인 익명프로토콜 기법을 제안한다.

+) 본 연구는 과학기술정보통신부 및 정보통신기기획평가원의 대학ICT연구센터육성지원사업의 연구결과로 수행되었음 (IITP-2019-2015-0-00403)

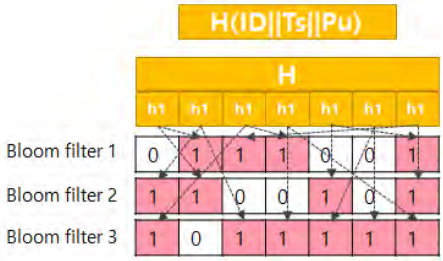
2. 관련연구

2.1 블룸필터

블룸 필터(Bloom filter)는 원소가 집합에 속하는지 여부를 검사하는데 사용되는 확률적 자료 구조이다. 1970년 Burton Howard Bloom에 의해 고안되었다[2]. 블룸 필터에 의해 어떤 원소가 집합에 속한다고 판단된 경우 실제로는 원소가 집합에 속하지 않는 긍정 오류가 발생하는 것이 가능하지만, 반대로 원소가 집합에 속하지 않는 것으로 판단되었는데 실제로는 원소가 집합에 속하는 부정 오류는 절대로 발생하지 않는다는 특성이 있다(그림 1). 집합에 원소를 추가하는 것은 가능하나, 집합에서 원소를 삭제하는 것은 불가능하다. 이와 같은 성질 때문에 추가만 가능하고 삭제가 불가능한 블록체인에 적합하며 트랜잭션 값이 해당 블룸필터 집합에 속해있는지 여부를 확인 할 수 있기 때문에 요청자의 Privacy를 보호하면서 빠르게 검증이 가능하도록 한다. 하지만 집합 내 원소의 숫자가 증가할수록 긍정 오류 발생 확률도 증가하는 Trade-Off 이므로 긍정오류를 높이기 위해선 여러 번 해시함수를 사용해야하므로 오버헤드가 증가된다.



(그림 1) 블룸필터



(그림 2) 다중 블룸필터

2.2 다중블룸필터

다중블룸필터는 블룸필터의 익명성을 통한 Privacy특성을 이용하면서 긍정오류율을 높이기 위해 인증 특성 다중으로 하여 패턴을 여러 가지로 이용한다. 이는 특정 인증값을 해시하여 조각으로 분할 한 다음 여러 블룸필터에 대응하여 패턴 값을 생성한다(그림 2)[3]. 블룸필터는 패턴의 결과를 다음 블룸필터 대입하지만 다중 블룸필터는 하나의 해시 조각을 여러 블룸필터에 대입하는 것이 특징이다. 또한 이 조각은 Blind Signature를 통해 서버의 서명으로 컨소시엄 블록체인에 전파된다. 따라서 다중블룸필터 및 Blind Signature를 활용하여 컨소시엄 멤버 간 인증을 Privacy 유출을 최소화 하면서 안전하고 효율적으로 트랜잭션 인증을 수행한다.

3. 보안요구사항

본 연구에서 제안하는 컨소시엄 블록체인에서의 Privacy를 위한 다중블룸필터 및 Blind Signature기반의 익명프로토콜 기법은 다음과 같은 보안 요소가 요구된다.

• 사용자 인증(Authentication): 정당한 사용자는 사용자의 공개키-개인키를 통해 네트워크의 올바른 사용자임을 보장하여야 한다.

• 신뢰성(Reliability) : 네트워크 참여자는 네트워크의 무결성과 가용성을 보장받아 전체 네트워크를 신뢰할 수 있어야한다.

• 효율성(Efficiency) : 다중블룸필터 기반 인증 기술은 안전하면서 전체 처리량의 오버헤드를 최소화하여 효율적으로 계산 및 가용이 되어야 한다.

• 프라이버시(Privacy) : 컨소시엄 블록체인 내 다른 그룹원 멤버의 트랜잭션 검증 및 인증은 요청자의 정보를 노출시키지 않으며 수행되어야 한다.

4. 제안방식

본 논문의 제안방식은 인증서기반의 사용자 인증을 위해 사용자의 인증서 발급요청과정, 발급, 다중블룸필터기반의 인증서 검증 과정으로 구성된다. 객체는 사용자, 컨소시엄 블록체인 네트워크이며 블록체인의 스마트컨트랙트에 따라 구현된다.

4.1 키 생성 및 인증서 발급 요청 과정

이 단계에서는 Client A가 키 쌍을 생성하여 컨소시엄 블록체인에게 공개키 인증서를 요청하는 단계이다.

Step 1: 사용자는 공개키 인증서 발급 요청을 위해 ECC(Elliptic Curve Cryptography)을 통해 개인키와 공개키를 생성한다. 생성자(점) G와 타원형 그룹 $E_P(a,b)$에서의 개인키를 SK_A선택하고 $PU_A = SK_A * G$에 따라 공개키 PU_A를 생성한다.

Step 2: 사용자는 자신의 ID 와 공개키 및 공개키 생성 시점의 타임스탬프 값 T_S을 컨소시엄 블록체인에 전송하여 공개키 인증서 발급을 요청한다. 이는 사용자의 정당한 개인키에 유효한 공개키만이 EOA(External Own Accounts)로 메시지가 생성되어 컨소시엄 블록체인에 수행된다.

4.2 인증서 발급 과정

이 단계에서는 컨소시엄 블록체인은 인증서 발급을 위해 Client A의 인증 값을 다중블룸필터를 사용하여 생성한다.

Step 1: 컨소시엄 블록체인은 사용자의 ID와 공개키에 해당하는 값을 해시하여 인증요소를 결합 및 해시를 수행한다.

$$h_1....h_n = H(T_S||ID_A||P_A)$$

Step 2: 분리된 해시 조각을 각각의 필터에 대입한다. 이때 블룸필터의 해시함수대신 임의의 개수로 분리된 조각을 배열에 대입한다.

Step 3: 컨소시엄 블록체인은 최종블룸필터 값을 내부 합의를 통하여 블록체인에 컨소시엄 블록체인의 서명에 따라 등록한다.

Step 4: 사용자의 EOA에 해당하는 SC(Smart Contracts)가 생성되어 수행된다.

4.3 인증서 검증 과정

이 단계에서는 Client A가 생성한 트랜잭션을 다른 컨소시엄 멤버인 Client B가 올바른 트랜잭션 및 컨소시엄 멤버인지를 검증한다.

Step 1: Client A는 트랜잭션에 ECDSA(Elliptic Curve Digital Signature Algorithm)을 통해 개인키로 서명을 생성한다.

$$(x_1, y_1) = k * G(x,y) \bmod P$$

<표 1> 기존 방식과 제안방식 비교 분석표

	[4]	[5]	[6]	제안방식
Authenticati on/ Integrity	Offer			
Non-Repudiation	Offer			
Replay Attack	Strength	Weakness	Weakness	Strength
MITM Attack	Strength	Weakness	Weakness	Strength
Member Privacy	Not Offer		Offer	

$$r = x_1 \bmod N$$

$$\sigma = (k^{-1}(H(M) + SK_A * r) \bmod N$$

Step 2: Clinet A의 공개키는 컨소시엄 블록체인의 다중블룸필터를 통해 빠르게 검증되고 이후 트랜잭션의 서명을 검증한다.

$$W = \sigma^{-1} \bmod N$$

$$R' = \sigma^{-1}(H(M)G + rPU_A = x_r, y_r$$

$$x_r \bmod n = r?$$

Step 3: 컨소시엄 블록체인은 내부 합의를 통해 블록체인 생성 이후 다중블룸필터 패턴을 형성한다.

Step 4: Client A와 Client B는 블록체인의 블록헤더를 가지고 다중블룸필터를 형성하여 컨소시엄 블록체인에 검증을 요청한다.

Step 5: 컨소시엄 블록체인은 다중블룸필터를 통해 공개키 및 서명을 검증하여 검증 할 수 있는 머클트리 경로 형태의 검증 값을 반환한다.

5. 제안방식 분석

본 제안방식은 다중블룸필터와 Blind Signature를 사용하여 컨소시엄 블록체인에서의 Privacy를 향상시키고자 한다. 본 제안방식은 기존방식에 비해 다음과 같은 보안요구사항을 만족한다.

• 사용자 인증(Authentication): 정당한 사용자는 해시체인 및 해시트리로 생성한 공개키-개인키 쌍과 글로벌 타임스탬프가 포함 된 공개키 인증서를 통해 올바른 사용자임을 보장한다.

• 신뢰성(Reliability) : 네트워크 참여자는 컨소시엄 블록체인을 통해 위·변조로부터 안전하고 Fault Tolerance를 가진 신뢰 네트워크를 형성한다.

• 효율성(Efficiency) : 사용자 및 인증 네트워크는 다중블룸필터를 활용하여 블룸필터의 k번 해시함수 대신 한 번의 해시 함수를 통해서 효율적이고 안전하게 인증이 수행된다.

• 프라이버시(Privacy) : 컨소시엄 블록체인 내 다른 그룹원간의 트랜잭션 검증 및 인증은 확률적 자료구조인 다중블룸필터 및 Blind Signature를 통해 검증 요청자의 정보를 노출시키지 않으면서 검증 수행을 가능하게 한다.

6. 결론

본 논문에서 컨소시엄 블록체인에서의 Privacy를 위한 익명프로토콜에 관한 기법을 제안하였다. 제안방식분석에 따라 보안요구사항을 만족하면서 블룸필터가 가지고 있는 안전성에 따라 Privacy를 높이고 해시연산을 여러 번 하지 않도록 하여 효율을 개선시켰다. 향후 구체화 된 환경에 적용하여 필요한 기반 프로토콜을 구현 및 실제 구현까지 확대 적용이 필요할 것으로 생각된다.

참고문헌

[1] Nakamoto, S., “Bitcoin: A peer-to-peer electronic cash system”, 2008

[2] Broder, A & Michael M., "Network applications of bloom filters: A survey." Internet mathematics 1.4, pp. 485-509, 2004

[3] FENG, F., & WU, J., “Research of RFID middleware data filtering algorithm based on Bloom filter“, Application Research of Computers, 5, 041, 2015.

[4] R. Longo, F. Pintore, G. Rinaldo, M. Sala, “On the security of the Blockchain Bix Protocol and Certificates”, In Cyber Conflict (CyCon), 2017 9th International Conference on, IEEE, pp. 1-16, 2017.

[5] N. Emmadi, H. Narumanchi, “Reinforcing Immutability of Permissioned Blockchains with Keyless Signatures′ Infrastructure”, Proceedings of the 18th International Conference on Distributed Computing and Networking ACM, pp.46, 2017.

[6] T. Hardjono, A. S. Pentland, “Verifiable Anonymous Identities and Access Control in Permissioned Blockchains”, manuscript in preparation, 2016.