블록체인 기반 영지식 증명에서의 프로토콜 시퀀스처리

백영태[O], 민연아[*]
[O]김포대학교 멀티미디어과,
[*]한양사이버대학교 응용소프트웨어공학과
e-mail: hannae@kimpo.ac.kr[O], yah0612@hycu.ac.kr[*]

Protocol sequence processing in blockchain-based zero-knowledge proof

Baek YeongTae[O], Min Youn A[*]
[*]Dept. of Multimedia, Kimpo university,
[O]Dept. of Applied Software engineering, Hanyang cyber university

● 요 약 ●

블록체인 기술은 데이터 공유를 통하여 투명한 데이터 관리가 가능하다. 하지만 데이터삭제의 비가역성 및 투명한 데이터 공개가 데이터 프라이버시 침해의 원인이 될 수 있다. 최근 블록체인 기술상의 데이터 프라이버시 보호를 위하여 영지식 증명이 활발하게 적용되고 있다. 본 논문에서는 블록체인 기술 적용 시 데이터 프라이버시를 보호하고 효율적인 데이터 증명 및 검증이 가능하도록 하기 위해 기존의 영지식 증명방법을 변형하여 증명자와 검증자의 신뢰도에 따른 상호 신뢰 기반의 차별화된 프로토콜 처리과정을 제안하였다. 해당 제안을 위하여 신뢰도 측정 변수가 필요하며 해당 변수를 통한 프로토콜 시퀀스의 차별적 적용을 통하여 증명 및 검증을 위한 경제적.시간적 효율성을 높일 수 있다.

키워드: 블록체인(block chain), 영지식 증명(zero-knowledge proof)

I. Introduction

블록체인 기술은 분산 네트워크에 참여한 모든 노드들에게 정보를 공유하여 데이터의 투명한 관리가 가능하다[1]. 하지만 투명한 데이터 관리가 데이터 프라이버시 침해의 원인이 될 수 있음을 감안할 때 증명자에 대한 비밀정보를 노출하지 않고 검증할 수 있는 방법이 필요하다.

영지식 증명은 증명자의 비밀스러운 정보를 노출하지 않고 증명함수를 통하여 해시 처리한 commit 값을 블록체인 온체인에 업로드 함으로써 검증자가 증명자의 비밀정보를 확인하지 않고도 검증자의 자격을 검증할 수 있다[2][3].

본 논문에서는 블록체인 기술에 영지식증명을 효율적으로 적용하기 위한 방법으로 비대화식 ZNP기반하에서 증명자와 검증자간 데이터 약정(commit)에 대한 효과적인 상호증명(Interactive Proof)을 위한 방법으로 상호 신뢰를 검증하는 차별화된 프로토콜을 제안한다.

II. Preliminaries

1. Related works

1.1 블록체인과 영지식 증명

2008년 블록체인 기술이 소개된 이후 블록체인은 투명한데이터 관리를 위한 기술로 활용되고 있다. 하지만 이러한 장점으로 인하여 블록체인을 통한 데이터 프라이버시 침해의 논란이 발생될 수 있다[1].

블록체인의 특징은 거래속도 증가 및 정확성 증가, 인적 오류감소 및 인프라비용 감소, 거래의 투명성 확보 및 감시 가능성 증가를 들 수 있다[1][2].

영지식 증명은 증명자의 비밀정보 노출없이 검증자에게 유효성을 증명할 수 있는 암호학적 방법이다[3].

fig. 1은 영지식증명을 위한 증명자와 검증자간 데이터 증명 과정을 간소화한 것이다[3][4].

```
[Prover]
Proof function (witness variable, parameter: input,
output, secret value){
Function processing
return proof data}

----Verifying ----

[Verifier]
Verification function (proof data, parameters: ){
Function processing
return verification result
}
```

Fig. 1. Certification process

최근 zk-SNARK (zero-knowledge Succinct Non-interactive ARgument of Knowledge)와 같이 블록체인 기술에 영지식 증명 적용 및 변형이 활발하게 연구되고 있다[5]. 블록체인 기술의 장점을 활용하면서 과도한 정보 노출을 피하고 신뢰할 수 있는 데이터 거래가 가능하도록 영지식 증명의 적용이 활발하게 이루어지고 있다[5]. ZNP은 증명자와 검증자간 interaction이 필수적인 대화식 증명방식과 증명자와 검증자간 interaction이 필요하지 않은 비대화식 증명방식(Non-Interactive Zero-knowledge Proof; NIZKP)으로 구분된다[3][5]. 비대화식 증명방식에서는 증명자가 증명을 생성하게 되면 어떠한 검증자도 검증과정에 참여할 수 있으므로 현재의 전자서명과 유사한 방식이다[6]. schnorr protocal, Pedersen protocal 등은 ZKP를 활용한 대화식 프로토콜이며 zk-SNARKs는 대표적인 비대화식 ZKP이다[6][7].

III. The Proposed Scheme

본 논문에서는 블록체인 기술에 영지식증명을 효율적으로 적용하기 위한 방법으로 비대화식 ZNP기반하에서 증명자와 검증자간 데이터 약정(commit)에 대한 효과적인 상호증명(Interactive Proof)을 위한 방법으로 상호 신뢰를 검증하는 차별화된 프로토콜을 제안한다.

fig. 2는 본 논문에서 제안하는 프로토콜의 기본 처리 과정으로 증명자의 신뢰에 따라 처리과정이 차별적으로 진행된다.

[Prover]
↓
Commitment (SHA 256+ Discrete log polynomial of reliability variables) through hash function
↓
Request for verification
↓
Response through verification using polynomial
(Adjust the degree of polynomial operation according to the reliability of the prover and verifier)
↓
[Verifier]

Fig. 2. Protocol processing

증명자와 검증자가 같은 신뢰도를 갖는 경우이다. 기관 A와 기관 B가 유사한 신뢰도를 갖는 경우 키들 간 대수적 연산을 N/2번의 다항식으로 증명시간을 간소화 하고 기관 간 빠른 검증이 가능하도록 한다. 증명자가 검증자 대비 낮은 신뢰도를 갖는 경우는 증명자인 기관 A의 신뢰를 확인하는 시간이 필요하다. 이 경우 키들 간 N번의 다항식으로 하여 증명시간보다는 신뢰확인에 중점을 둔다. 증명시간이 오래 걸리지만 영지식 증명의 검증시간은 상수에 해당하므로 검증시간은 매우 빠르다. 다항식은 이산로그를 활용한 다항식을 사용하며 해당 다항식 증명자가 검증자 대비 높은 신뢰도를 갖는 경우는 증명자가 높은 신뢰도를 갖는 경우로써 증명자와 검증자가 같은 경우의 검증 경험 유무에 따라 N/2 미만의 다항식으로 하여 증명시간을 최소화 한다.

IV. Conclusion

본 논문의 제안을 위하여 영지식 증명을 위한 증명자와 검증자를 신뢰를 기반으로 하는 기관으로 제한하고 증명자의 신뢰에 따라 영지식 증명과정에서 사용하는 프로토콜의 시퀀스를 차별화 하였으며 세부 상법으로는 신뢰도를 측정하는 변수에 의해 이산로그다항식의 복잡도를 차별화하였으며 이를 통하여 검증과정에 대한 경제적, 시간적 효율성을 높일 수 있었다.

REFERENCES

[1] Kosba Ahmed, et al, “Hawk: The blockchain model of cryptography and privacy-preserving smart contracts”, 2016 IEEE symposium on security and privacy IEEE, 2016.

[2] Zyskind Guy, Oz Nathan, “Decentralizing privacy: Using blockchain to protect personal data” Security and Privacy Workshops (SPW), 2015IEEE. IEEE, 2015.

[3] Lee.J.H, Hwang.J.Y, Oh.H.O, Kim.J.H, "Personal Information Management System with Blockchain Using zk-SNARK" kiisc, Vol.29, N0.2m pp.299-309, 2019.

[4] Groth Jens, “On the size of pairing-based non-interactive arguments” Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer, Berlin, Heidelberg, 2016.

[5] Groth Jens, et al, “Updatable and universal common reference strings with applications to zk-SNARKS” Annual International Cryptology Conference. Springer, Cham, 2018.

[6] Zyskind Guy, Oz Nathan, “Decentralizing privacy: Using blockchain to protect personal data” Security and Privacy Workshops (SPW), 2015 IEEE. IEEE, 2015.