5

블록체인과 영지식 증명의 활용: 온라인 투표

장재혁 박사과정 (GIST 전기전자컴퓨터공학부)
이흥노 교수 (GIST 전기전자컴퓨터공학부)

목차

Ⅰ 서 론

블록체인은 peer-to-peer(P2P) 네트워크에서 작동하는 데이터 기록소이다. 블록체인에 기록된 데이터는 불변하며, 누구나 데이터에 접근 가능하다. 블록체인이 다른 P2P 데이터 공유 네트워크들과 비교하였을 때 갖는 우위는 데이터의 불변성이다. 블록체인의 모든 데이터는 검증된 후 기록되며, 한번 기록된 데이터는 이후에 기록될 모든 데이터와 체인으로 연결된다. 이 때문에 과거에 기록된 하나의 데이터를 변경하면 이후의 모든 데이터들이 무효화된다. 블록체인에 데이터를 기록하고 검증하는 모든 과정은 불특정 다수의 제 3자에 의해 수행된다. 하나의 데이터를 기록하기 위해서 수많은 제 3자의 검증이 필요하도록 설계되었기 때문에 [1],[2], 특정한 신뢰받는 제 3자의 개입 없이도 기록된 데이터가 신뢰받을 수 있다.

블록체인의 데이터를 검증하고 기록하는 과정에는 특정한 신뢰받는 제 3자의 개입이 없다. 이는 데이터 기록을 요청한 자의 신원을 가려줄 장치가 없다는 것을 의미할 수 있다. 이러한 불편함을 극복하기 위해, 블록체인 사용자의 익명성 보장을 위해 최근 영지식 증명 기술을 적용하는 연구가 활발히 진행되고 있다. 영지식 증명(zero-knowledge proof)이란 증명 프로토콜로써 증명자가 검증자에게 어떤 명제(statement)가 참임을 납득시키는 프로토콜이다. 이때, 영지식 증명 프로토콜은 검증자에게 그 명제가 참 혹은 거짓이라는 사실 외의 다른 정보는 일절 전달하지 않는 영지식(zero-knowledge) 특성을 가져야 한다. 영지식 특성 덕분에 영지식 증명이 익명성을 보장하며 데이터를 주고받기 위한 암호학적 방법으로 사용되고 있다.

영지식 증명을 정의하면, 공개된 정보와 비공개 정보로 구성된 주어진 명제에 대하여, 어떤 증명 프로토콜이 영지식 증명 프로토콜이 되기 위한 필요충분조건 세 가지는[3]

① 완전성(completeness): 만약 명제가 참이면, 진실한 증명자가 검증자에게 명제가 참임을 납득시킬 수 있어야 한다.

② 건실성(soundness): 만약 명제가 참이 아니면, 거짓 증명자가 검증자에게 명제가 참임을 납득시킬 수 없어야 한다.

③ 영지식성(zero-knowledge): 검증자는 명제가 참 혹은 거짓이라는 사실 외에, 어떤 비공개 정보도 알 수 없어야 한다. 즉, 증명자가 명제의 참/거짓에 결정적 관련이 있는 정보들 중 일부를 선택적으로 공개하지 않을 수 있어야 한다.

영지식증명 프로토콜은 증명과정과 검증과정의 두 과정으로 구분 될 수 있다. 증명과정은 증명자가 명제가 참임을 스스로 검증 한 후, 그 증거를 생성하는 과정이다. 검증과정은 검증자가 증명자로부터 증거를 받아 증거에 문제가 없는지를 확인하는 과정이다. 만약 증거에 문제가 없다면, 증명자가 명제의 자가 검증을 잘 수행했다는 사실이 수학적으로 보장되어 있어야 한다.

블록체인에 영지식 증명이 활용된 대표적인 사례로 Zcash[4]가 있다. Zcash는 사용자간의 거래기록을 담는 블록체인으로, 거래 당사자의 신원을 공개하지 않으면서 거래의 유효성을 검증하는 방안으로써 영지식 증명을 활용하였다. 기존 블록체인에서는 거래의 유효성을 검증하기 위해서는 거래에 사용된 암호화폐의 소유권을 증명하기 위해 거래자의 계정(주소)이 반드시 기록되어야 하였다. 반면 Zcash는 암호화폐의 소유권자가 소유권 증명을 자가 수행한 후 그 증거만을 거래내용과 함께 블록체인에 기록하는 방식이다. 거래기록을 검증하는 불특정 다수의 제 3자들은 증거가 올바르게 생성되었는지를 검증함으로써 암호화폐의 소유자가 누군인지 알지 못한 채 소유권 검증을 수행할 수 있다.

블록체인에 영지식 증명이 사용될 수 있는 또 다른 사례로 온라인 투표 시스템이 있다. 온라인 투표시스템은 경제적이며 언제, 어디서든 의사표현을 할 수 있다는 장점이 있지만, 영지식 증명과 블록체인이 활용되기 이전의 온라인 투표 시스템은 투표의 기본원칙을 지키기 어렵다는 단점이 있었다. 투표 시스템을 블록체인상에서 구현하면 블록체인의 정의에 의해 투표의 투명성과 위조 방지가 해결될 수 있다. 그러나 블록체인만으로는 투표자의 투표권 인증과 투표 내용간의 연결을 숨길 수 없기 때문에 익명성 보장이 어렵다. 영지식 증명은 그 정의에 의해 온라인 투표 시스템이 익명성을 만족하도록 만드는 도구가 될 수 있다.

이 글에서는 영지식 증명의 작동 원리를 설명하고, 영지식 증명과 블록체인을 활용한 온라인 투표 시스템의 예를 소개한다. 먼저 영지식 증명의 작동 원리를 설명하기 위해 단순하면서 활용도가 높은

제1장 블록체인 전문가 기고문

제1장 블록체인 전문가 기고문

프로토콜인 Schnorr 인증 프로토콜을 소개하고 분석한다. 이후 영지식 증명이 활용된 온라인 투표 시스템을 소개하며, 투표의 원칙에 의거해 성능을 분석한다.

II 영지식 증명의 작동 원리

2장에서는 영지식 증명 프로토콜의 한 예인 Schnorr 인증 프로토콜[5]과 Fiat-Shamir heuristic[6]을 소개하고, 영지식 증명의 정의에 의거한 분석을 통해 이들의 작동 원리를 논의한다. Schnorr 인증 프로토콜과 Fiat-Shamir heuristic은 그 구조가 단순하지만, 3장에서 소개될 온라인 투표 시스템에도 적용 될 만큼 활용범위가 넓다.

Schnorr 인증 프로토콜은 서론에서 기술한 영지식 증명의 정의를 충족하는 증명 프로토콜이다. Schnorr 인증 프로토콜은 대화형 (interactive) 영지식 증명으로 분류된다. 대화형 영지식 증명의 특징은 증명자와 검증자가 함께 증거를 만드는 것이다. 먼저 증명자가 증거의 일부를 생성하고, 검증자가 증명자에게 도전적 문제 (challenge)를 제출한다. 도전적 문제란 증명자는 비공개 정보를 알지 못하면 응할 수 없는 문제를 말한다. 최종적으로 증명자는 스스로 생성한 일부의 증거와 검증자의 도전적 문제에 답하는 증거를 합쳐 최종 증거를 검증자에게 제출한다. Schnorr 인증 프로토콜을 일반화하여 정의한 프로토콜로써 시그마($\sum$)프로토콜이 있다 [7].

비대화형(Non-interactive) 영지식 증명(NIZK, non-interactive zero knowledge)은 이름 그대로 증거 생성과정에서 검증자와 증명자간의 대화가 필요 없는 증명을 의미한다. 즉, 증명자 혼자서 증거를 생성하는 것이다. 대화형 영지식 증명에서는 증거 생성과정에서 증명자가 검증자의 도전적 문제(challenge)를 받고 이에 응해야하기 때문에 둘 간의 대화(conversation)가 필요했다. 이 대화 과정을 생략하면서 그 역할을 유지하기 위해 제안된 방법 중 하나가 Fiat-Shamir heuristic이다. Fiat-Shamir heuristic은 random oracle 이라는 이상적인 랜덤 프로그램의 존재를 가정하여 검증자의 도전적 문제를 대체한다. 다시 말해, 증명자 스스로 도전적 문제를 랜덤하게 생성 한 후 이를 공개해 누구나 도전적 문제의 공정성을 납득할 수 있게 하는 것이다.

NIZK의 이점은 증명 과정에서 시간적 제약이 사라지는 것이다. 이러한 특성은 영지식 증명 프로토콜이 블록체인에 활용되기 적합하게 만들어준다. 대화형 영지식 증명의 경우 증명자와 검증자간의 대화가 필요했기 때문에, 증명을 완료하기 위해서는 두 사람이 같은 시간대에 서로 약속된 온라인 공간에 함께 접속해야하는 시공간적 제약이 있었다. NIZK는 더 이상 대화과정이 필요 없기 때문에, 증명자가 원하는 시간과 장소에 증거 파일을 업로드 해 놓으면, 검증자가 언제든 파일을 다운받아 검증을 수행 할 수 있다. No-interaction 특성은 특히 영지식 증명이 블록체인에 적용될 때 반드시 필요하다. 블록체인은 그 정의에 의해, 사용자가 데이터 업로드를 요청하면, 채굴자 혹은 블록체인 관리자가 요청된 데이터를 모은 후 어느 정도의 시간이 지난 후에 검증 및 업로드를 완료한다. 만약 사용자가 증명자라면, 증거를 업로드 한 후 언제가 될지 모를 시간 후에 검증자가 검증을 수행한다는 의미이다. 증명자가 NIZK 프로토콜을 따른다면 증명자가 그 불확실한 시간을 온라인상에서 기다리고 있을 필요가 없다.

1 대화형 영지식 증명: Schnorr 인증 프로토콜

Schnorr 프로토콜은 구조가 단순하면서도 활용도가 높은 대화형 영지식 증명 프로토콜이다. 증명하고자 하는 명제는 "공개된 값 y와 공개된 값 $g \in F_p^*$에 대하여, $y = g^x$를 만족시키는 비공개 값 x $(0 \le x < p-1)$를 알고 있음"을 납득시키는 상황이다. 여기서 p는 공개된 값이며 소수(prime number)이다. 집합 F_p는 특성(characteristic)이 p인 유한 체(finite field)이다. $F_p := \{0,1,\cdots,p-1\}$이고, 모든 원소간의 더하기 및 곱하기 연산에는 $\mathrm{mod} p$가 적용된다. F_p^*는 F_p에서 원소 0을 제외한 집합이다. 그리고 g는 F_p의 primitive element이다. 어떤 원소 $a \in F_p$가 primitive element이면, a의 제곱으로 구성된 집합, 즉, $\{a^i, \forall i \in Z_0^*\}$의 원소의 개수는 $p-1$이다. 이 글에서 다룰 Schnorr 프로토콜은 다음과 같다:

1. 증명자는 하나의 (비공개) 무작위 값 v $(0 \le v < p-1)$로 $t = g^v \mathrm{mod} p$를 계산하여 검증자에게 보낸다.
2. 도전적 문제: 검증자는 하나의 무작위 값 c $(0 < c < p-1)$를 증명자에게 보낸다.
3. 증명자는 $r = v - cx \bmod (p-1)$를 계산하여 검증자에게 보낸다.
4. 검증자는 $t \equiv g^r y^c \mathrm{mod} p$임을 확인한다.

[프로토콜1] Schnorr 인증 프로토콜

프로토콜1에서, 증명자는 검증자에게 x를 직접적으로 전송하지 않는다. 대신 증거로써 r과 t를 전송한다. 검증자가 r로 x부터를 알아내는 것은 매우 어렵다. 그럼에도 불구하고 검증자는 $t \equiv g^r y^c \mathrm{mod} p$를 계산함으로써 증명자가 올바른 x를 사용하였는지 확인 할 수 있다. 다음의 분석을 통해 그 이유를 설명하겠다.

프로토콜 1이 서론에서 기술된 영지식 증명의 정의를 만족하는지를 확인하면 다음과 같다:

(완전성) 만약 증명자가 x를 알고있다면, 검증자는 $t \equiv g^r y^c \mathrm{mod} p$를 확인함으로써 이를 납득할 수 있는가?

증명자가 검증자가 납득시킬 수 있다. Fermat's little theorem에 의해, $g^{cx} \equiv g^{cx \bmod (p-1)} \mathrm{mod} p$이다. 만약 증명자가 $r = v - cx \bmod (p-1)$를 계산 할 때 사용한 값 x가 $y = g^x \mathrm{mod} p$를 만족시킨다면, $t \equiv g^r y^c \mathrm{mod} p$이다. 즉, 증명자가 올바른 x를 사용하였다면 검증자는 이를 검증할 수 있다.

(건실성) 만약 거짓 증명자가 x를 모른다면, 검증자에게 $t \equiv g^r y^c \mathrm{mod} p$임을 납득시킬 수 있는가?

거짓 증명자가 검증자를 납득시키기 어렵다. 거짓 증명자가 주장하는 값을 x'라 하자. 여기서 $x' \neq x$이다. 거짓 증명자가 검증자를 속이기 위해 목표하는 바는 합동방정식 $t \equiv g^{r'} y^c \mathrm{mod} p$를 만족시키는 값 r'을 찾는 것이다. 이 문제는 discrete logarithm 문제이다. 거짓 증명자가 택할 수 있는 다른 방법은 F_{p-1}의 원소들 중 무작위로 r'를 선택하여 그 값이 discrete logarithm 문제의 해답이 되는지 확인 하는 것이다. 한번 무작위 값을 선택하여 조건이 달성 될 확률은 $(p-1)^{-1}$이다. 실제 사용 환경에서 p는 아주 큰 숫자로 설정되므로, 거짓 증명자가 검증자를 납득시킬 확률은 아주 작다.

만약 검증자가 아닌 증명자가 도전적 문제 c를 임의로 선택한다면, 거짓 증명자가 검증자를 기만 할

제1장 블록체인 전문가 기고문

수 있다. 구체적으로, 거짓 증명자가 임의로 값 c와 r을 증명 수행 이전에 선택한 후, 증명이 시작되면 가장 먼저 $t=g^r y^c \bmod p$를 계산하여 검증자에게 보낸다. 이후 미리 선택해둔 c와 r을 검증자에게 건넨다. 이 방법으로 거짓 증명자는 x를 알지 못하여도 검증자를 기만 할 수 있게 된다.

또 다른 경우로 도전적 문제를 검증자가 직접 제출하더라도, 만약 검증자가 도전적 문제를 증명이 시작됨과 동시에 증명자에게 보낸다면, 거짓 증명자가 검증자를 기만 할 수 있다. 거짓 증명자가 임의로 r을 선택 후, 증명이 시작되면 가장 먼저 $t=g^r y^c \bmod p$를 계산하여 검증자에게 보낼 수 있기 때문이다. 따라서 올바른 증명을 위해서는 증명자가 먼저 값 t를 제출 하게 한 후, 검증자는 이를 확인하고 도전적 문제 c를 제출하는 방식의 대화형 구조가 반드시 필요하다.

(영지식성) 검증자는 r로부터 x를 알아 낼 수 있는가?

검증자는 비공개 정보 x를 알 수 없다. 검증자가 건네받는 $r=v-cx \bmod (p-1)$에서, 검증자가 알고 있는 값은 r, p, c이며, 알지 못하는 값은 x와 v이다. 정보 탈취함수를 $f: F_{p-1} \times F_{p-1} \rightarrow F_{p-1}$,여기서 $f(v',x')=v'-cx' \bmod (p-1)$이라 정의하겠다. 검증자가 x를 알아내는 행위는 $f^{-1}(r)$의 원소를 찾는 것과 동등하다. 그러나 함수 f는 injective이므로 inverse image $f^{-1}(r)$의 원소는 유일하지 않다. 결국 검증자는 v를 알지 못하는 한 r로부터 x를 알아 낼 수 없다.

2 Fiat- Shamir Heuristic을 활용한 비대화형 영지식 증명으로의 확장

앞 절의 Schnorr 인증 프로토콜의 분석에서 대화형 구조와 도전적 문제 (challenge)의 중요성을 살펴보았다. 도전적 문제가 없으면 Schnorr 인증 프로토콜이 건실성을 만족하지 못하였다. 그리고 도전적 문제는 증명자가 아닌 검증자가 대화의 형태로 제출하였다: 증명자가 먼저 무작위 값을 제출한 후, 검증자가 이어서 도전적 문제를 제출하였다. 이렇게 하지 않으면 거짓 증명자가 도전적 문제를 자신에게 유리하게 조작할 수 있게 되어 거짓 증명이 쉬워지기 때문이었다. 즉, 도전적 문제의 공정성이 훼손되면 프로토콜의 건실성이 위협받는다.

NIZK의 한 예인 Fiat-Shamir heuristic가 적용된 Schnorr 인증 프로토콜은 random oracle이라는 랜덤 프로그램의 존재를 가정한다. 증명자가 random oracle로부터 무작위 값을 수여받아 검증자의 도전적 문제를 대체한다. Random oracle은 매번 다른 무작위 값을 생성하여야 하며, 생성된 무작위 값이 random oracle에 의한 값이라는 것을 누구나 확인 할 수 있어야 한다. 다시 말해, 증명자가 도전적 문제를 정직한 과정을 거쳐 생성하였다는 것을 누구나 검증할 수 있어야 한다.

Random oracle로써 hash 함수가 사용 될 수도 있다[8]. Hash 함수는 입력값이 변함에 따라 출력값이 무작위처럼 변하는 특성이 있으며, 입력값을 알면 누구나 같은 출력값을 재생산 해볼 수 있다. 즉, 도전적 문제가 공정하게 생성된 것이 맞는지 누구나 검증 할 수 있다.

본론으로 돌아와, Fiat-Shamir heuristic에서는 도전적 문제를 검증자가 아닌 random oracle이 선택한다. Schnorr 프로토콜에 Fiat-Shamir heuristic을 적용하면 다음과 같다. 증명자는 공개 된 값 y, g, p에 대해 $y \equiv g^x \bmod p$를 만족하는 비공개 값 x를 알고 있음을 검증자에게 증명하는 상황이다.

1. 증명자는 하나의 (비공개) 무작위 값 v $(0 \le v < p-1)$로 $t=g^v \bmod p$를 계산하여 검증자에게 보낸다.2. 도전적 문제: 검증자는 하나의 무작위 값 c $(0 < c < p-1)$를 증명자에게 보낸다.
3. 증명자는 $r=v-cx \bmod (p-1)$를 계산하여 검증자에게 보낸다.
4. 검증자는 $t \equiv g^r y^c \bmod p$임을 확인한다.

[프로토콜2] Fiat-Shamir heuristic이 적용된 Schnorr 프로토콜

프로토콜 1과 프로토콜 2를 비교해 보면, 증명자와 검증자 간의 대화(conversation)과정이 사라진 대신, 증명자가 검증자에게 최종 제출할 증거가 추가되었다. 구체적으로, 대화형 방식에서는 두 개의 값 r과 t를 검증자에게 제출하였으나, 비대화형 방식에서는 r과 t, 그리고 c까지 총 세 개의 값을 제출한다.

결과적으로, 비대화형 Schnorr 인증 프로토콜은 대화과정을 제거한 대신 증거의 길이가 더 길다. 다행히 Schnorr 프로토콜은 증명해야 할 명제가 단순하여 증거의 길이의 증가폭이 크지 않다. 반면 최근 연구되는 NIZK 프로토콜은 일반적인 연산이 포함된 복잡한 명제를 지원한다. NIZK의 증거는 명제가 복잡해질수록 길이가 더욱 길어질 수 있으며, 증거의 길이가 길어지면 다양한 분야로의 응용이 제한이 될 수 있다. 이러한 이유로 최근의 영지식 증명 연구자들은 증거의 길이를 효율적인 수준으로 줄이는 zk-SNARK를 연구하고 있다.

3 zk-SNARK

NIZK에 덧붙여 더욱 발전된 형태의 영지식 증명의 정의들이 최근 연구되고 있다. 그 중 하나인 zk-SNARK (zero-knowledge succint non-interactive argument of knowledge)는 NIZK에서에서 간결성(succintness)이 추가된 정의이다. zk-SNARK로 분류될 수 있는 영지식 증명 프로토콜중 하나로 Jens Groth가 2016년 제안한 Groth16[9]이 있다. Groth16은 2013년 B. Parno에 의해 제안된 zk-SNARK 프로토콜인 Pinocchio[10]의 원리를 따르고 일부 성능을 개선한 프로토콜이다. 이 외에도 2020년 영국의 Aztec 그룹에서 발표된 PlonK[11]도 원리가 비슷한 점이 많다. 이러한 zk-SNARK 연구들의 주요 관심사는 증명과정이 더 빠르고, 증거의 크기가 더 작으며, 검증과정이 더 빠른 프로토콜을 설계하는 것이다. 더욱 다양한 zk-SNARK 연구 동향은 [12]에 소개되어 있다.

영지식 증명의 간결성은 증거의 간결함, 즉 증명과정에 의해 산출되는 증거 데이터의 물리적 크기가 작음을 의미한다. 일반적으로 증거의 크기는 증명해야 할 명제의 복잡도에 따라 커진다. 연구자 그룹에 따라 다르지만, 간결성이 추가된 영지식 증명 프로토콜이 지향하는 목표는 증거의 크기가 명제의 복잡도에 관계없이 고정되어 있거나, 혹은 명제의 크기가 명제의 복잡도와 유사 선형적 관계에 있는 프로토콜이다.

증거의 크기가 간결할 때의 이점은 검증자가 검증을 빠르게 끝낼 수 있다는 것이다. 증거의 크기가

제1장 블록체인 전문가 기고문

작기 때문에 검증자가 증거의 오류를 검사하기 위해 소요해야하는 필요 계산량도 작아지게 된다. 이뿐만 아니라, 증거의 간결성은 증거를 기록해야 할 서버의 용량이 한정 된 경우에도 유용하다. 그러한 서버의 한 예시가 블록체인인데, 블록체인의 블록의 크기는 제한적이다. 따라서 증거의 크기가 크면 하나의 블록에 기록될 수 있는 증거의 수가 줄어든다. 이는 시간당 블록체인을 사용할 수 있는 사용자의 수가 제한되는 것과 같다. 즉, 블록체인의 확장성(scalibility)이 줄어드는 것이다. 반대로, 증거의 크기가 작아질수록 같은 시간동안 더 많은 사용자가 블록체인을 사용 할 수 있게 되며, 따라서 블록체인의 확장성이 우수해진다.

III 온라인 투표 시스템

3장에서는 투표의 원칙을 정의한다. 이후 온라인 투표 시스템들을 소개하며 투표의 원칙에 의거하여 분석한다.

1 온라인 투표 시스템

온라인 투표 시스템은 공동체 구성원들이 직접적인 대면 없이 의사를 전달하고 결정할 수 있도록 해주는 시스템이다. 이는 대표적인 대면 (오프라인) 투표시스템인 선거와 대조적이다. 선거와 같은 기존 대면 투표시스템은 완벽하지는 않지만 표 1의 원칙들이 잘 지켜질 수 있도록 체계화 되어있다. 그러나 대면 투표시스템은 시간과 공간의 제약을 크게 받으며, 이로 인해 발생하는 인적, 물적 자원의 소요 또한 상당하다. 이에 반해 온라인 투표시스템은 경제적이며 언제, 어디서든 의사표현을 할 수 있다는 장점이 있지만, 표 1의 원칙을 지키기 어렵다는 단점이 있었다. 일반적인 투표 시스템이 지녀야 할 투표의 원칙은 아래 표 1과 같이 나열할 수 있다.

투표 원칙	내 용
정확성	모든 정당한 유효투표는 투표결과에 정확히 집계됨
확인성	투표결과 위조방지를 위한 투표결과 검증수단이 필요
완전성	부정 투표자에 의한 방해 차단, 부정투표는 미 집계
단일성	투표권이 없는 유권자의 투표참여 불가
합법성	정당한 투표자는 오직 1회만 참여 가능
기밀성	투표자와 투표결과의 비밀관계 보장
공정성	투표 중의 집계결과가 남은 투표에 영향을 주지 않음

[표1] 투표 시스템의 원칙 (출처: 중앙선거관리위원회)

온라인 투표 시스템에서는 모든 과정에서의 산출물이 데이터로써 저장된다. 만약 데이터가 중앙 서버에 저장된다면, 데이터의 위변조가 가능하기 때문에 기술의 도움을 받을 필요가 있다. 이때 도움이 될 수 있는 기술 중 하나가 블록체인이다. 구체적으로, 투표의 원칙 중 정확성과 확인성, 완전성은 블록체인 기술로 해결 될 수 있다. 블록체인의 의의가 위변조가 불가능하고 누구나 검증 가능한 분산 서버를 만드는 것이기 때문이다.

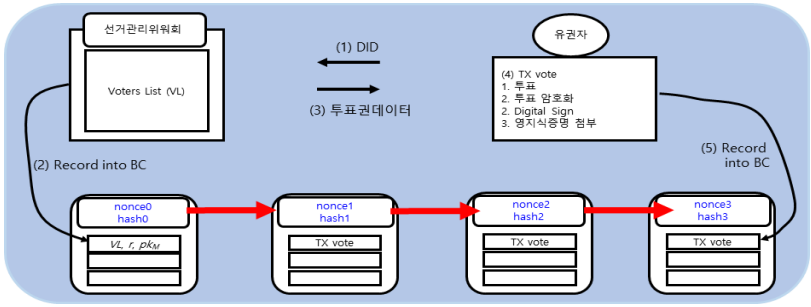
한편 온라인 투표의 단일성과 합법성은 digital identity (DID)와 public key infrastructure (PKI)기술의 도움을 받아 만족시킬 수 있다. DID는 사용자가 자신이 신뢰받을 수 있는 개인 혹은 기관, 장치라는 정보가 기록된 디지털 데이터이다. 그리고 PKI는 public-key encryption 기술을 활용해 증서를 발급하는 기반 시설(infrastructure)이다. PKI를 이용하여 DID를 네트워크상에서 안전하게 전송 할 수 있다. 일반적인 대면방식의 선거에서는 선거위원이 투표자의 신원을 확인한 후 투표권을 배부한다. 만약 온라인 투표라면, 신원확인에 필요한 신분증을 공인인증서와 같은 DID로 대체 할 수 있다. 문제는 온라인 투표권인데, 만약 투표권이 항상 변하지 않는 어떤 디지털 데이터라면, 복제되어 악용될 수 있다. 그러므로 투표권은 투표자의 DID에 따라 변하는 데이터여야 한다. 이렇게 DID를 기반으로 투표권을 생성할 수 있는 기술의 예가 PKI이다. 중앙 선거관리 위원회가 PKI를 통해 사용자의 DID를 넘겨받은 후 고유의 투표권 데이터를 다시 사용자에게 배포 할 수 있다. 이후 투표 결과를 검표할 때는 투표권 데이터가 중앙 선거관리 위원회에 의해 배포된 투표권이 맞는지 확인할 수 있다. 즉, DID와 투표권 데이터간의 1대1 대응이 되도록 하는 것이다. 만약 DID와 사용자 개인 간의 완벽한 1대1 대응이 보장된다면, 단일성과 합법성이 만족 될 수 있다. 그러나 검표과정에서 어떤 DID가 어떤 의사결정을 하였는지가 중앙 선거관리 위원회에 공개되기 때문에, 기밀성을 만족시키지는 못한다.

온라인 투표 시스템의 한 예는 2016년 개발된 FollowMyVote[13]이다. FollowMyVote는 블록체인에 기반하였으며, 모든 투표 절차에서 대면 과정이 전혀 포함되지 않는다. 기밀성 보장을 위해 두 쌍의 공개 키와 비공개 키를 사용하였으며, 한 쌍은 본인 인증에, 그리고 나머지 한 쌍은 투표권 발급에 사용하였다. 투표자 인증과 투표권 발급은 선정된 중앙 관리자가 수행한다. 이러한 노력에도 불구하고 FollowMyVote는 여전히 기밀성이 보장되었다고 할 수 없다. 중앙 관리자가 투표자의 암호화 키와 투표권에 관한 모든 정보를 갖고 있기 때문에, 모든 투표결과가 중앙 관리자에게 노출될 수밖에 없다.

영지식 증명은 온라인 투표 시스템이 기밀성을 만족하도록 해주는 도구가 될 수 있다. 예를 들어, 어떤 투표자가 있고 그 투표자의 DID를 x, 그리고 x에 의해 생성된 투표권 데이터를 $s(x)$라 하자. 그리고 투표권 데이터를 확인 (verification)하는 함수를 f라 하자. 즉, s가 x로부터 생성된 것이라면 $f(x,s)=1$이며, 그렇지 않다면 $f(x,s)=0$이다. 이제 투표자가 증명해야 할 명제 S는 "$f(x,s)=1$"이며, 여기서 공개되지 않아야 할 비공개정보는 x이다. 영지식 증명 프로토콜에 의해 투표자는 명제 S를 스스로 자가 검증한 후 그 증거파일 π를 생성하여 투표결과와 함께 투표함에 기록한다. 이후 검표과정에서는 π에 문제가 없는지를 확인한다. 만약 증거파일 π에 문제가 없다면, 영지식 증명의 정의에 의해 해당 투표는 정당한 투표권자에 의한 투표임을 수학적으로 보장받게 되며 (단일성 만족), DID를 유출하지 않았기 때문에 투표자와 투표결과간의 비밀관계도 보장받게 된다 (기밀성 만족)

제1장 블록체인 전문가 기고문

2 영지식증명 기반 온라인 투표 시스템



[그림1] 영지식 증명이 적용된 블록체인기반 온라인 투표시스템 (참조 [14])

그림 1은 한양대학교와 국민대학교가 2018년 공개 출원하고 2020년 등록된 특허 "비밀 선거가 보장된 블록체인 기반의 전자 투표를 수행하는 단말 장치 및 서버와 전자 투표 방법[14]"의 대표도해를 간략하게 나타낸 그림이다. 그림 1의 온라인투표 시스템에서, 투표자(유권자)의 DID는 pk_{ID}이다. 모든 유권자의 pk_{ID} 즉 Voters List(VL)를 갖고 있는 선거관리 위원회가 투표자의 DID를 확인 한 후 투표자에게 투표권 데이터 $\sigma_{pk_{ID}}$와 $vkey_M$ 를 준다. 투표권 데이터는 투표자의 DID에 따라 변한다. 투표자가 투표권을 보유한 자인지를 확인하도록 설계된 함수는 $member(\ )$와 $verify(\ )$이다. 함수 $member$는 투표자의 DID가 투표대상이 맞는지 (유권자 리스트에 포함되어 있는지)를 확인하는 함수이고, 함수 $verify$는 투표권 데이터가 투표자의 DID로부터 올바르게 생성된 데이터인지를 확인하는 함수이다.

만약 영지식증명이 적용되지 않은 투표시스템이라면, 두 함수 $member$와 $verify$는 검표과정에서 검표자 (선거관리 위원회)가 수행해야 할 함수이다. 반면 그림 1과 같이 영지식 증명이 적용된 투표 시스템에서는 두 함수를 투표자가 스스로 수행하여 자가 검증한다. 그 후 자가 검증을 잘 수행하였다는 증거 데이터 영지식증명 π 를 자신의 투표 결과와 함께 블록체인에 기록한다. 투표가 끝난 후, 검표자는 영지식증명 π에 오류가 없는지 확인함으로써 정당한 투표권자에 의한 투표임을 확인한다.

그림 1과 같은 투표 시스템은 온라인 투표의 실현 가능성을 제고 하였으나, 두 가지의 이유에 의해 아직 완벽하다고 할 수는 없다.

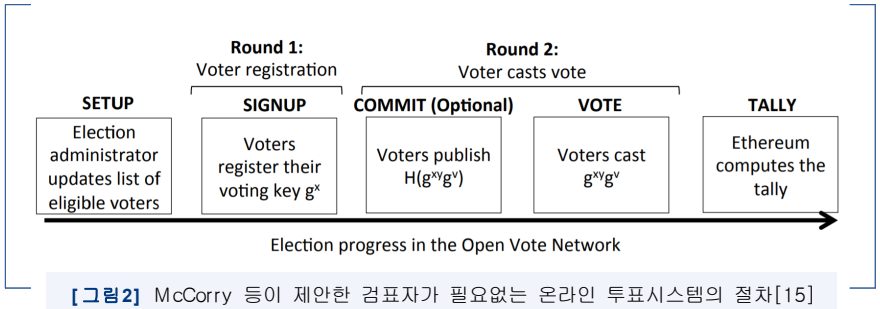
첫째로, 한 명의 투표자가 다수의 투표권 데이터를 확보 할 가능성에 관한 대처가 논의되지 않았다.

둘째로, 투표 시스템이 선거관리 위원회라는 신뢰받는 제 3자(trusted third-party)에 의존하고 있다.

믿음을 기반으로 동작하는 선거관리 위원회가 타락하면 부정투표가 가능할 수 있다. 예를 들어 선거관리 위원회는 투표자들의 DID들과 그에 대응하는 투표권 데이터들을 모두 보관하고 있을 수 있다. 투표 결과에 투표자의 DID가 기록되지 않아 기밀성은 보장받지만, 선거관리 위원회가 타인의 투표권을 부정 사용 할 가능성을 배제할 수 없다.

3 신뢰받는 제 3자에 의존하지 않는 온라인 투표시스템

2017년 저자 McCorry 등은 검표자가 필요 없는 온라인 투표 시스템을 제안하였다[15]. 그림 2는 이 투표 시스템의 대표도해이다. 이 시스템의 핵심 기술은 영지식 증명과 그룹 암호화[16]이다. 영지식 증명은 투표자가 자신의 투표권을 스스로 발급 할 수 있도록 하는데 사용되었으며, 투표권이 올바른 과정을 거쳐 생성되었음에 관한 증거만이 블록체인에 기록된다. 영지식 증명 프로토콜로써 Fiat-Shamir heuristic이 적용된 Schnorr 프로토콜을 사용하였다. 한편 그룹 암호화란, 정해진 수의 투표자 그룹의 각 투표자가 자신의 투표를 공개 키로 암호화 하면, 후에 검표 시 개별 투표 내용의 복호 없이도 모든 투표자의 투표를 합산 할 수 있게 하는 암호화 기술이다. 그룹 암호화는 검표자가 필요 없도록 해준다. 결과적으로 영지식 증명과 그룹 암호화의 도움으로 기밀성이 만족되었으며 투표과정에서 제 3자의 개입이 없다. 이 뿐만 아니라 투표가 모두 완료 된 후 검표가 가능하기 때문에 투표의 공정성 또한 만족된다. 그러나 투표자 인증시에 개인 인증 수단이 논의되지 않았기 때문에, 한 명의 투표자가 다수의 표를 행사 할 수 있을 가능성에 대한 대처가 부족하다.



[그림2] McCorry 등이 제안한 검표자가 필요없는 온라인 투표시스템의 절차[15]

IV 결 론

이 글에서는 영지식 증명 프로토콜의 한 예인 Schnorr 인증 프로토콜과 Fiat-Shamir heuristic과 이들이 블록체인과 함께 활용 될 수 있는 온라인 투표 시스템을 소개하였다. 블록체인의 데이터

제1장 블록체인 전문가 기고문

불변성과 투명성은 온라인 투표 시스템이 투표의 원칙 중 정확성과 확인성, 완전성을 충족하도록 도움을 줄 수 있었다. 그리고 영지식 증명의 익명성은 PKI와 같은 암호화 기술과 함께 사용되어 온라인 투표 시스템이 투표의 원칙 중 단일성과 합법성, 그리고 기밀성을 충족하도록 도움을 줄 수 있었다. 이러한 블록체인과 영지식 증명의 장점을 활용하여, 제안된 온라인 투표 시스템들은 모두 투표의 원칙을 만족하도록 목표하였다.

그러나 소개된 온라인 투표 시스템들은 아직 완벽하지는 않았다. 시스템에 소요된 기술인 블록체인과 영지식 증명, 그리고 암호화 기법은 투표의 7원칙 모두를 만족 시킬 수 있도록 정의되었지만, 그것들의 집합체인 온라인 투표 시스템은 7원칙 모두를 만족하지 못하였다. 결과적으로, 소요기술들을 상호보완적으로 사용하지 못하였다는 의미이다. 예를 들어 그림 1의 온라인 투표 시스템은 영지식 증명이 익명성을 유지한 투표자 인증 수단으로 사용되었으나, 결과적으로 신뢰받는 제 3자에 의존하기 때문에 제 3자가 투표자 인증 기록을 악용 할 수 있었다. 또한 그림 2의 투표시스템은 신뢰받는 제 3자를 제거함으로 인해 1인 1투표의 원칙, 즉 합법성을 만족시키는 방안은 논의되지 못하였다.

현재의 온라인 투표 시스템이 아직 완벽하다고 말 할 수는 없으나, 소요되는 기술들인 블록체인과 영지식 증명, 그리고 암호화 기법들은 투표의 7원칙을 모두 지니고 있다. 이 글에서 소개된 온라인 투표 시스템들은 완전한 투표 시스템의 실현 가능성을 보여주었다. 영지식 증명이 적용된 또다른 투표 시스템이 스위스의 업체 Luxoft와 스위스 루체른 대학의 공동연구로 2018년에 개발되었으며, 스위스 Zug시의 주관 하에 72명의 시민을 대상으로 시범투표가 시행되기도 하였다 [17]. 온라인 투표 시스템은 더욱 개선 될 수 있으며, 소요기술들을 상호 보완적으로 융합 할 방안을 마련하는 것이 주요 관건이다.

참고문헌 (Reference)

[1] S. Park, H. Choi, and H.-N. Lee, "Time-variant proof-of-work using error-correction codes," arXiv:2006.12306, 2020.
[2] H. Jung and H.-N. Lee, "ECCPoW: Error-correction code based proof-of-work for ASIC resistance", Symmetry, June 2020.
[3] S. Goldwasser, S. Micali, and C. Rackoff, "The knowledge of complexity of interactive proof systems," SIAM J. Comput., Feb. 1989.
[4] E. B. Sasson, et. al., "Zerocash: Decentralized anonymous payments from Bitcoin", May 2014. Online available: http://zerocash-project.org/media/pdf/zerocash-extended-20140518.pdf
[5] C. P. Schnorr, "Efficient identification and signatures for smart cards," in CRYPTO '89, 1990.
[6] A. Fiat and A. Shamir, "How to prove yourself: Practical solutions to identification and signature problems," in CRYPTO' 86, 1987.
[7] I. Damg˚ard, "On Σ-protocols," CPT, 2010.
[8] M. Bellare and P. Rogaway. "Random Oracles are Practical: A Paradigm for Designing Efficient Protocols," ACM Press, pp. 62-73, 1995.
[9] J. Groth, "On the size of pairing-based non-interactive arguments," EUROCRYPT 2016, pp. 305-326, 2016.
[10] B. Parno, et. al, "Pinocchio: nearly practical verifiable computation," IEEE Symposium on Security and Privacy 2013, pp. 238-252, 2013.
[11] A. Gabizon, et. al., "PLONK: Permutations over Lagrange-bases for Oecumenical Noninteractive arguments of Knowledge," Mathematics, Computer Science IACR Cryptol. ePrint Arch., 2019.
[12] 오현옥,"영지식 증명 연구 동향", IITP 주간 기술 동향, 2020.
[13] Followmyvote, "Blockchain voting: The end-to-end process," 2016. Online available: https://followmyvote.com/blockchain-voting-the-end-to-end-process/.
[14] 한양대학교 산학협력단, 국민대학교 산학협력단, "비밀 선거가 보장된 블록 체인 기반의 전자 투표를 수행하는 단말 장치 및 서버와, 전자 투표 방법," 대한민국 특허, 등록번호: 1021446140000, 2020.
[15] P. McCorry, S. F. Shahandashti, and F. Hao, "A smart contract for boardroom voting with maximum voter privacy," in IACR Cryptology ePrint Archive, 2017.
[16] F. Hao, P. Y. Ryan, and P. Zielinski, "Anonymous voting by two-round public discussion," IET Information Security, 2010.
[17] Lucerene University of Applied Sciences and Arts, "Evaluation of the blockchain vote in the city of Zug," 2018. Online available: https://www.stadtzug.ch/_docn/1938568/eVoting_Final_Report_ENG.pdf