인터넷 커뮤니티 선거에 적합한 스마트계약 기반 투표 모델

윤성현*
백석대학교 ICT학부 교수

The Smart Contract based Voting Model for Internet Community Election

Sunghyun Yun*
Professor, Division of ICT, Baekseok University

요 약 인터넷 투표는 유권자의 위치에 관계없이 투표할 수 있으므로 유권자의 투표 참여율을 높이고 선거에 사용되는 경제적 비용을 줄일 수 있다. 단점은 모든 구성원들이 선거 관리를 위한 인터넷 서버를 전적으로 신뢰해야 한다는 것이다. 만약 선거 관리 서버가 특정 후보자와 공모한다면, 다른 후보자들은 부정 선거임을 증명할 수 없다. 더불어 인터넷 투표와 관련된 대부분의 연구는 유권자가 사는 나라와 지역에 제약을 받는다. 유투브 채널과 같은 인터넷 커뮤니티 구성원들을 대상으로 하는 투표 방법으로는 적합하지 않다. 인터넷 커뮤니티는 구성원이 사는 지역과 나라에 제약이 없기 때문에 새로운 투표 모델의 개발이 필요하다. 본 논문에서는 블록체인 네트워크에서 사용할 수 있는 스마트계약 기반의 인터넷 투표 모델을 제안한다. 제안한 스마트계약 모델은 후보자 등록, 유권자 등록, 투표 및 개표 단계로 구성된다. 유권자 등록 및 투표 단계에서 유권자의 익명성이 보장되고 개표 단계에서 후보자들에 의하여 선거의 공정성이 보장된다.

주제어 : 블록체인, 투표, 스마트계약, 에스엔에스, 공정성

Abstract As Internet voting can take place regardless of a voter's location, the participation rate of the voters would be increased and economic costs will be reduced. But the drawback of it is that all participants have to trust the election management server. If the server colludes with the specific candidate, the other candidates cannot prove rigged election. In addition, majority of researches on Internet voting are mainly focused on the voting restricted by the region and the country. Thus, it's not appropriate for the election in Internet community such as YouTube channels. As the Internet community is composed of members from all around the world, the new type of voting model is needed. In this study, we propose the smart contract based Internet voting model applicable on the blockchain network. The proposed smart contract model consists of candidate registration, voter registration, voting and counting stages. In the proposed model, anonymity of the voter is assured in the voter registration and voting stages, and all candidates can confirm the fairness of the election in the counting stage.

Key Words : Blockchain, Voting, Smart Contract, SNS, Fairness

이 논문은 2018년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(2018R1D1A3B07050180)
*교신저자 : 윤성현(shcrpt@gmail.com)
접수일 2019년 9월 13일 수정일 2019년 11월 28일 심사완료일 2019년 12월 12일

1. 서론

투표는 민주주의 사회에서 다수의 의견을 수렴하는 가장 중요한 사회적 행위이며, 유권자의 익명성과 선거의 공정성이 반드시 보장되어야 한다. 지방선거, 국회의원 선거와 같은 기존의 오프라인 선거는 투표소 설치, 투표용지 제작 및 배송, 선거관리인단 구성 등 막대한 비용이 소모된다. 인터넷 투표는 장소 제약이 없고 전자적으로 투표가 이루어지기 때문에 선거 관리에 소요되는 비용을 줄일 수 있으며 유권자들의 투표 참여율을 높일 수 있다[1].

선거의 공정성은 유권자 및 후보자가 투표 결과에 대해서 부인할 수 없는 것을 의미한다. 기존의 인터넷 전자투표 모델에서 유권자 등록, 투표 및 개표 관리는 선거관리 서버에서 이루어진다. 선거관리 서버를 신뢰할 수 있으면 선거의 공정성이 보장된다. 현행 오프라인 선거와 마찬가지로 유권자들은 본인의 투표가 선거 결과에 반영되었는지 확인할 수 없다. 단점은 서버 관리자가 특정 후보와 공모하여 투표결과를 조작해도 다른 후보자들은 이를 알 수 없다는 것이다[2].

최근, 카카오톡, 라인, 유투브 등과 같은 인터넷 커뮤니티 중심의 SNS 서비스가 광범위하게 보급되고 있다. 이러한 서비스의 특징은 가입자가 특정 국가와 지역에 국한되지 않는다는 것이다. 인터넷 커뮤니티는 정부와 같은 특정 기관의 감독을 받지 않으며 자발적으로 만들어지고 유포된다[3]. 따라서, 기존의 인터넷 투표 모델은 인터넷 커뮤니티를 위한 모델로는 적합하지 않다. 신뢰할 수 있는 감독 기관 없이 커뮤니티 구성원들의 합의에 의해서 공정한 투표를 할 수 있는 새로운 투표 모델의 개발이 필수적이다.

본 연구에서는 스마트계약 기반의 인터넷 투표 모델을 제안한다. 제안한 투표 모델은 유권자 등록, 후보자 등록, 투표 및 개표 단계로 구성되며, 인터넷 커뮤니티 임원 선출을 위한 용도로 적용될 수 있다.

유권자 등록과 투표는 서로 독립적으로 진행되어야 누가 누구에게 투표했는지 유추할 수 없다. 본 논문에서는 유권자 주소와 투표 주소를 분리하여 투표 단계에서는 공인된 투표 주소로만 투표할 수 있도록 한다. 은닉 서명 기법을 적용하여 유권자의 투표 주소를 등록함으로써, 투표 단계에서 누구의 투표 주소인지 알 수 없다.

선거의 공정성은 이해 당사자인 후보자들이 투표 결과를 인정하면 보장된다. 본 논문에서 스마트계약은 RSA 다중키 암호에 사용될 키를 생성하여 각 후보자에게 선거용 개인키를 배포하고 공통 공개키는 상태로 저장한다. 각 유권자는 후보자를 기명한 투표지를 공통 공개키로 암호화하여 스마트계약으로 전송한다. 개표 단계에서 암호화된 투표권은 후보자 모두가 참여하여 복호화해야 복원된다. 따라서 선거에 참여한 후보자들은 선거결과에 대해서 부인할 수 없다. 더불어 개표 결과는 블록체인에 저장되기 때문에 유권자들은 자신들이 사용한 익명 주소를 이용하여 개별적으로 확인할 수 있다.

2. 관련연구

블록체인은 분산 장부로 P2P 방식의 블록체인 네트워크에 참여하는 모든 노드들이 동일한 장부를 공유한다. 채굴자들은 트랜잭션들로 구성된 블록을 만들고, 합의 알고리즘에 따라서 선택된 블록을 블록체인에 연결한다. 비트코인에 사용되는 PoW(Proof of Work) 합의 알고리즘은 제일 먼저 해쉬값을 찾은 채굴자의 블록을 블록체인에 연결할 블록으로 선택한다. 모든 구성원들이 동일한 블록체인을 공유하기 때문에, 피어 노드는 블록체인에 저장된 트랜잭션을 조작할 수 없다[4].

비트코인, 이더리움과 같은 퍼블릭 블록체인에서는 누구나 자발적으로 블록체인 네트워크의 노드가 될 수 있다. 인터넷 커뮤니티 가입도 자발적으로 이루어진다는 점에서 블록체인 노드와 유사한 속성을 갖는다. 따라서 블록체인은 인터넷 커뮤니티 기반의 다양한 서비스로 응용이 가능하다[5].

스마트계약은 이더리움 네트워크에서 실행되는 컴퓨터 프로그램이다. 이더리움 노드는 스마트계약 코드를 컴파일하여 바이트코드를 만들고 이를 포함한 트랜잭션을 발행하여 블록체인에 저장한다. 블록체인에 등록된 스마트계약은 이더리움 가상 머신 EVM이 설치되어 있는 노드에서 실행된다[6, 7].

전자투표에 대한 연구는 크게 부분 전자투표와 인터넷 투표로 구분된다. 부분 전자투표는 기존의 오프라인 선거 절차의 일부를 전자화한 것이다. 예를 들면 유권자 등록 및 투표소에서의 신분 확인은 기존의 절차를 따르고 투표소에서의 기표 및 개표는 전자화 하는 방식이다. 투표지를 이용한 투표는 증거가 남지만 전자식으로 투표할 경우에는 시비가 발생하여도 물리적 증거가 남지 않는다[8].

인터넷 투표는 선거의 전 과정을 전자화한 것이다. 모든 유권자는 PC 또는 스마트폰을 이용하여 장소에 제약

없이 투표할 수 있다. 선거관리 서버는 유권자 등록, 투표, 개표 단계를 관리하는데, 선거의 공정성을 위해서 후보자와 유권자들은 선거관리 서버를 전적으로 신뢰해야 한다. 그렇지 않으면 선거관리 서버와 특정 후보자가 공모할 수 있고, 이 경우에 다른 후보자들 및 유권자들은 공모 사실을 알 수 없게 된다[1, 2, 9].

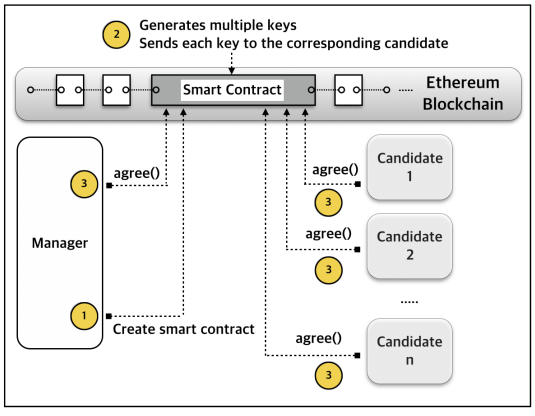
인터넷 투표와 관련된 대부분의 연구들은 정부 감독하에 실시되는 국회의원선거, 지방 선거 등과 같은 대규모 선거의 전자화에 초점을 맞추고 있다[10]. 따라서, 선거에 참여하는 유권자들의 소속은 나라와 지역에 한정된다.

카카오톡, 라인, 유투브 등과 같은 인터넷 커뮤니티 서비스는 구성원들의 참여가 자발적이고 지역에 제한받지 않는 특징이 있다. 기존의 인터넷 투표는 유권자의 주거지역에 제약이 있고 선거관리 서버를 전적으로 신뢰해야만 선거의 공정성을 보장받을 수 있다. 블록체인은 구성원들의 자발적 참여로 신뢰할 수 있는 데이터를 만들어 내기 때문에 인터넷 커뮤니티 선거를 위한 기반으로 적합하다.

3. 제안한 모델

제안한 투표 모델은 스마트계약 생성, 유권자 등록, 투표자 등록, 투표 및 개표 단계로 구성된다.

3.1 스마트계약 생성



[Fig. 1] Smart Contract Generation & Candidates Agreement

그림 1은 인터넷 커뮤니티 리더를 뽑기 위한 스마트계약을 생성하고 후보자들이 이 계약에 합의하는 절차를 보여준다. 스마트계약 트랜잭션은 블록체인 네트워크로 전송되고 채굴자는 해당 트랜잭션을 블록에 포함하여 블록체인에 저장한다.

스마트계약은 블록체인 네트워크에서 실행되는 프로그램으로 상태와 함수로 구성된다. 상태는 계약에 필요한 데이터로 그 값이 변경될 때마다 트랜잭션을 발행하여 블록체인에 저장한다. 함수는 계약 수행을 위해서 사용되는 컴퓨터 프로그램이다.

제안한 모델에서는 투표에 사용되는 익명 주소, 투표지, 후보자 기호, 후보자 공통 공개키, 개표 결과를 스마트계약의 상태로 저장한다. 투표 함수는 유권자가 호출하고 개표 함수는 후보자가 호출한다. 스마트계약 생성 시 실행되는 생성자 함수는 각 후보자에게 전송할 개인키와 공통 공개키를 생성한다[11, 12]. 공통 공개키는 상태로 저장한다.

가정 1. p와 q는 매우 큰 소수로 두 수의 곱으로 만들어지는 합성수 n이 공개되어도 p, q를 소인수분해하는 것은 계산상 불가능하다[13, 14].

$$n = p \times q$$

가정 2. 가정 1의 n은 RSA 다중암호의 법이고 $\phi(n)$은 오일러 파이 함수 값이다. RSA 다중암호의 개인키 sk_i 및 공개키 pk는 다음 조건을 만족한다. ($i = [1 \ .. \ t]$)

$$sk_1 \times sk_2 \times \ ... \ \times sk_t \times pk \equiv 1 \bmod \phi(n)$$

$$GCD(sk1 \times sk_2 \times \ ... \ \times sk_t \ , \ \phi(n)) = 1$$

가정 3. 인터넷 커뮤니티의 유권자 수는 m명, 선거에 참여하는 후보자 수는 t명이라고 가정한다.

유권자	후보자
$V_i \ (i = [1 \ .. \ m])$	$C_i \ (i = [1 \ .. \ t])$
skv_i: V_i의 개인키	skc_i: C_i의 개인키
pkv_i: V_i의 공개키	pkc_i: C_i의 공개키

가정 4. 스마트계약의 주소, RSA 암호의 법, 개인키 및 공개키는 다음과 같이 가정한다. 개인키 및 공개키는 생성자 함수에 의해서 자동으로 생성된다.

CA: 스마트계약 주소

n_{CA}: 스마트계약의 RSA 법

sk_{CA}: 스마트계약의 RSA 개인키

pk_{CA}: 스마트계약의 RSA 공개키

3.2 유권자 등록 및 은닉 주소 생성

유권자는 스마트계약의 register 함수를 호출하여 투표에 사용할 은닉 주소를 생성한다.

· register() : 유권자 주소를 확인하여 이전에 등록된 주소가 아니면 유권자가 전송한 은닉 주소를 서명하여 상태로 저장한다.

```
struct Voter {
    address vAddr; // 유권자 주소
    address bAddr; // 은닉 주소
    bytes32  vsigBaddr; // 유권자 서명
    bytes32  csigBaddr; // 스마트계약 서명
}
```

· 유권자 정보를 저장하기 위한 구조체는 유권자 주소, 은닉 주소, 유권자 서명, 스마트계약의 서명으로 구성된다.

단계 1: V_i는 커뮤니티 선거에 사용할 익명 주소를 생성한다. h는 해쉬함수이고, $nonce$는 V_i가 생성한 패스프레이즈이다.

$$pAddr_i = h(nonce)$$

단계 2: V_i는 n_{CA}와 서로소인 난수 k를 선택한다.

$$GCD(k, n_{CA}) = 1, \quad k < n_{CA}$$

단계 3: V_i는 다음과 같이 익명 주소를 은닉한다.

$$bAddr_i \equiv pAddr_i \times k^{pk_{CA}} \bmod n_{CA}$$

단계 4: V_i는 은닉 주소 $bAddr_i$에 서명한다.

단계 5: V_i는 register 함수를 호출하여 $bAddr_i$와 V_i의 서명을 스마트계약으로 전송한다.

단계 6: register 함수는 $bAddr_i$에 대한 V_i의 서명을 검증한다. 검증에 성공하면 단계 7로, 그렇지 않으면 트랜잭션을 롤백 한다.

단계 7: register 함수는 스마트계약의 개인키로 $bAddr_i$를 다음과 같이 서명하고 상태로 저장한다.

$$csigBaddr_i \equiv bAddr_i^{sk_{CA}} \bmod n_{CA}$$

단계 8: V_i는 스마트계약의 상태로 저장된 $csigBaddr_i$를 다운로드하고 다음과 같이 은닉 값을 해제한다. $csigPaddr_i$는 단계 1에서 생성한 익명 주소 $pAddr_i$에 대한 스마트계약의 서명이다.

$$csigPaddr_i \equiv csigBaddr_i \times k^{-1} \bmod n_{CA}$$

단계 9: V_i는 단계 8에서 추출한 서명이 $pAddr_i$에 대한 스마트계약의 서명이 맞는지 검증한다. 검증에 성공하면 $pAddr_i$를 투표 단계에서 사용한다. 그렇지 않으면 트랜잭션을 롤백 한다.

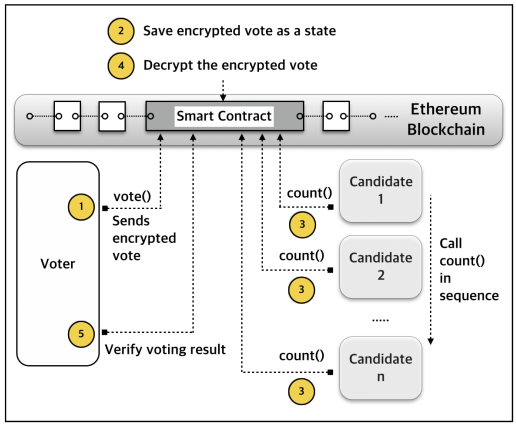
3.3 투표 단계

그림 2는 제안한 모델의 투표 및 개표 단계를 보여준다. 유권자는 익명 주소에서 vote 함수를 호출하여 투표한다.

· vote() : 유권자는 익명 주소에서 스마트계약의 vote 함수를 호출하여 후보자들의 공통 공개키로 암호화된 투표지를 전송한다. vote 함수는 익명 주소를 검증하고 암호화된 투표지를 상태로 저장한다.

```
struct EncryptedVote {
    address pAddr; // 유권자의 익명주소
    bytes32  csigPaddr; // 스마트계약의 서명
    bytes32  encCnum; // 암호화된 투표지
}
```

· 암호화된 투표지를 저장하기 위한 EncryptedVote 구조체는 유권자의 익명 주소, 스마트계약의 서명, 암호화된 투표지로 구성된다.



[Fig. 2] Voting & Counting Stages

단계 1: V_i는 후보자를 기명한 투표지를 스마트계약에 저장된 공통 공개키로 암호화한다.

$$encCnum_i = cNum_i^{pk} \bmod n$$

단계 2: V_i는 스마트계약의 vote 함수를 호출하여 $\{encCnum_i\, pAddr_i,\ csigPaddr\}$를 스마트계약으로 전송한다.

단계 3: vote 함수는 V_i가 보낸 $\{encCnum_i pAddr_i, csigPaddr\}$를 스마트계약의 상태로 저장한다.

3.4 개표 단계

그림 2에서 후보자들은 순차적으로 count 함수를 호

출하여 암호화된 투표지를 복호화 하고 그 결과를 상태로 저장한다. 모든 후보자들이 count 함수를 호출해야만 투표지가 복원된다.

```
struct Vote {
    address pAddr; // 유권자의 익명주소
    bytes32 csigPaddr; // 스마트계약의 서명
    uint cNum; // 유권자의 투표지
}
```

· 개표 결과를 저장하기 위한 Vote 구조체는 유권자의 익명 주소, 스마트계약의 서명, 후보자가 기명된 투표지로 구성된다.

단계 1: 투표가 종료되면 후보자들은 스마트계약의 count 함수를 호출하여 개표를 진행한다.

단계 2: 후보자는 순차적으로 스마트계약에 저장된 암호화된 투표지를 복호화 한다. 마지막 후보자가 스마트계약의 count 함수를 호출하면 다음과 같이 투표지가 복원된다.

$$cNum_i \equiv encCnum_i^{sk_1 \times sk_2 \times ... \times sk_t} \bmod n$$

단계 3: count 함수는 투표 결과를 스마트계약의 상태로 저장한다.

단계 4: 각 투표자는 자신의 투표가 개표 결과에 반영되었는지 검증한다.

4. 안전성 분석

제안한 투표 모델이 유권자의 익명성과 선거의 공정성을 만족하는지 분석한다.

정리 1. 유권자는 익명 주소로 투표를 하기 때문에 개표 결과로부터 유권자의 주소를 유추할 수 없다.

(증명) $vAddr_i$는 V_i가 커뮤니티 멤버로 사용하는 주소이다. V_i는 투표를 위해서 익명 주소 $pAddr_i$를 생성한다. V_i는 $pAddr_i$를 투표에 사용할 수 있도록 스마트계약의 서명을 받아야 한다. 유권자의 익명성을 보장하기 위해서는 $vAddr_i$와 $pAddr_i$ 간에 연관이 없어야 한다. 따라서 Chaum의 은닉 서명 기법을 적용하여 $pAddr_i$를 $bAddr_i$로 은닉 한다[12, 15]. 개표 단계에서 공개된 $pAddr_i$로부터 $bAddr_i$를 추출하려면 유권자가 등록 단계에서 생성한 k 값을 알아야 한다. k는 유권자가 생성한 난수 값이기 때문에 $pAddr_i$로부터 $bAddr_i$를 유추할 수 없다. 따라서 유권자를 제외한 제 3자는 $bAddr_i$를 모르기 때문에 $vAddr_i$를 유추할 수 없다. Q.E.D.

정리 2. 후보자들은 특정 후보를 선출하기 위하여 서로 공모할 수 없고 개표 결과에 대해서 부인할 수 없다.

(증명) 유권자의 투표지는 후보자들의 공통 공개키로 암호화되고 개표 단계에서 모든 후보자들이 참여해야만 복호화가 가능하다. 특정 후보자들이 공모하더라도 복호화 단계에서 나머지 후보자들의 개인키를 모르면 암호화된 투표지를 복원할 수 없다. RSA에서 공개키로부터 개인키를 유추하는 것은 계산상 불가능하다 [13, 14]. 더불어 블록체인에 저장된 개표 결과는 누구도 조작할 수 없다[4, 5]. 따라서 후보자들은 공모할 수 없고 개표 결과의 공정성을 부인할 수 없다.

5. 결론

본 논문에서는 인터넷 커뮤니티 선거에 적합한 스마트계약 기반의 투표 모델을 제안하였다. 제안한 모델은 유권자 등록, 투표 및 개표 단계로 구성된다. 유권자는 스마트계약이 서명한 공인된 익명 주소로 투표에 참여하기 때문에 누가 누구에게 투표했는지 알 수 없다. 유권자는 후보자를 기명한 투표지를 공통 공개키를 이용하여 암호화한다. 암호화된 투표지는 모든 후보자들이 참여하여 순차적으로 복호화해야 복원될 수 있다. 따라서, 선거 결과에 대해서 후보자들은 부인할 수 없다. 개표 결과는 유권자의 익명주소와 함께 스마트계약에 저장된다. 모든 유권자들은 자신의 투표가 선거 결과에 반영되었는지 개별적으로 확인할 수 있다.

REFERENCES

[1] S.H.Yun, "Research Trends and Requirements Analysis for Mobile Electronic Voting," Review of Korean Society for Internet Information, Vol.13, No.1, pp.9-20, 2012.

[2] D.Chaum, "Secret-Ballot Receipts: True Voter-Verifiable Elections," IEEE S&P Magazine, pp.38-47, 2004.

[3] J.H.Han and O.J.Cho, "Platform business Eco-model evolution: case study on KakaoTalk in Korea," Journal of Open Innovation, DOI:10.1186/s40852-015-0006-8, 2015.

[4] A.M.Antonopoulos, Mastering Bitcoin 2nd Edition, O'Reilly, 2017.

[5] Melanie Swan, Blockchain, O'Reilly, 2015.

[6] R.Modi, Solidity Programming Essentials, Packet Publishing, 2018.

[7] Ethereum Foundation, https://ethereum.org/, 2019.

[8] D.Evans and N.Paul, "Election Security: Perception and Reality," IEEE S&P Magazine, pp.24-31, 2004.

[9] J.Tepandi, S.Vassiljev, and I.Tsahhirov, "Wireless PKI Security and Mobile Voting," IEEE Computer, Vol.43, No.6, pp.54-60. 2010.

[10] A.Fujioka, T.Okamoto, and K.Ohta, "A Practical Secret Voting Scheme for Large Scale Elections," In Advances in Cryptology, Proceedings of AUSCRYPT'92. 1992.

[11] C.Boyd, "A New Multiple Key Cipher and an Improved Voting Scheme," In Advances in Cryptology, Proceedings of EUROCRYPT'89, LNCS 434, pp.617-625, 1990.

[12] B.Schneier, Applied Cryptography, Wiley, 1996.

[13] R.L.Rivest, A.Shamir, and L.Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Communications of the ACM, Vol.21, No.2, 1978.

[14] D.M.Burton, Elementary Number Theory, McGraw-Hill, 2010.

[15] P.Horster, M.Michels, and H.Petersen, "Blind Multisignature Schemes and Their Relevance for Electronic Voting," Proceedings of COMPSAC'95, pp.149-155, 1995.

윤 성 현(Yun Sunghyun) **[종신회원]**

- 1997년 2월 : 고려대학교 일반대학원 컴퓨터학과 (이학박사)
- 1998년 3월 ~ 2002년 2월 : LG 전자 선임연구원
- 2002년 3월 ~ 현재 : 백석대학교 ICT학부 부교수

〈관심분야〉
블록체인, 사물인터넷, DRM, 정보보호