Public Blockchain 기반의 익명성 전자투표 블록체인 플랫폼 모델

Anonymity Electronic Voting Blockchain Platform Model Based on Public Blockchain

저자 (Authors)

하현수, 이선준, 정구익, 신용구, 김명호, 김영종
Hyunsoo Ha, SunJun Lee, Guik Jung, YongGu Shin, MyungHo Kim , YoungJong Kim

출처 (Source)

한국정보과학회 학술발표논문집 , 2017.12, 1176-1178 (3 pages)

발행처 (Publisher)

한국정보과학회
KOREA INFORMATION SCIENCE SOCIETY

URL

http://www.dbpia.co.kr/Article/NODE07322432

APA Style

하현수, 이선준, 정구익, 신용구, 김명호, 김영종 (2017). Public Blockchain 기반의 익명성 전자투표 블록체인 플랫폼 모델. 한국정보과학회 학술발표논문집, 1176-1178.

Public Blockchain 기반의 익명성 전자투표 블록체인 플랫폼 모델

하현수[O1] 이선준[2] 정구익[2] 신용구[2] 김명호[2] 김영종[2]
[1,2]숭실대학교 소프트웨어 학부
dhy03196@naver.com, starj1024@gmail.com, rndlr96@gmail.com, tls09611@naver.com,
kmh@su.ac.kr, youngjong@ssu.ac.kr

Anonymity Electronic Voting Blockchain Platform Model Based on Public Blockchain

Hyunsoo Ha[O1] SunJun Lee[2] Guik Jung[2] YongGu Shin[2] MyungHo Kim[2] YoungJong Kim[2]
[1,2]School of Software, Soongsil University

요 약

블록체인 서버는 분산 원장 간의 합의 알고리즘을 통해 정보의 위·변조를 방지하고, 이용자가 자신의 트랜잭션을 직접 확인할 수 있다는 장점이 있다. 이러한 이유로 블록체인은 신뢰성이 중요시되는 전자 투표 플랫폼의 핵심 기술로서 평가받는다. 이중 제출 방지 기능을 통해서 이중 투표의 문제를 해결하고, 투표 결과의 위변조를 컨센서스 알고리즘을 통해 해결할 수 있기 때문이다. 또한 Public Blockchain을 이용할 경우, 트랜잭션의 결과를 모두 직접 확인할 수 있기 때문에, 직접 자신의 투표 결과가 잘 반영되었는지 확인할 수 있어 신뢰성을 향상시킬 수 있다. 그러나 Public Blockchain은 트랜잭션을 모두 직접 확인할 수 있기 때문에 유권자가 어떤 후보자에게 투표하였는가에 대한 내용까지도 유출될 수 있다는 한계점이 존재한다. 또한 개인에 대한 신변이 패킷 역추적을 통해 네트워크 계층에서도 유출될 수 있어 기존의 Public Blockchain 전자 투표 플랫폼은 익명성을 보장할 수 없게 된다. 본 논문에서는 Tor(The Onion Routing)을 통하여 패킷 역추적을 막고, Ring Signature와 Stealth Addressing 기법을 사용하여 기존 블록체인 전자 투표 플랫폼의 문제점인 유권자의 익명성을 안전하게 보장할 수 있는 블록체인 전자 투표 플랫폼 구현 방식을 제안한다.

1. 서 론

블록체인은 다양한 컨센서스(Consensus) 알고리즘을 통해서 신뢰성이 보장된 네트워크로 활용되고 있으며, 공개적으로 트랜잭션 조회가 가능하고, 위변조할 수 없다는 점에서 비트코인, 이더리움 등의 각종 암호 화폐(CryptoCurrency) 거래에 사용되고 있다. 뿐만 아니라, 최근에는 다양한 분야에 블록체인을 적용하려는 시도가 나타나고 있는데 대표적인 사례가 블록체인을 이용한 전자 투표 시스템이다[1].

전자투표는 기본적으로 지켜야 할 요구사항이 있다[2]. 전자투표에서 가장 중요시되는 두 가지 요구사항은 개표 과정이 완전하게 이뤄져야 한다는 완전성, 자신의 투표가 결과에 잘 반영되었는지를 살필 수 있어야 하는 검증성(투명성)이 있다. 블록체인의 특성은 전자 투표의 요구사항과 잘 부합하기 때문에, 블록체인은 전자투표 플랫폼 네트워크의 신흥 강자로 주목받고 있다.

블록체인을 이용한 전자 투표 플랫폼은 크게 두 가지로 구분되는데, 확실한 Privacy 보장이 가능하지만, 개표 결과를 직접 조회할 수 없으며 중앙 기관이 관여하도록 설계된 Private Blockchain을 사용하는 방식과 중앙 기관이 관여하지 않는 탈중화 방식(Decentralized)의 퓨어 P2P 네트워크를 구성하여, 네트워크 참여자 전원이 블록체인의 모든 트랜잭션 내역을 열람할 수 있도록 설계된 Public Blockchain을 사용하는 방식이 있다[3].

Private Blockchain의 경우 트랜잭션 내역은 중앙 기관만 열람할 수 있기 때문에, 투표자가 어떤 후보에게 투표하였는지에 대한 정보를 중앙 기관 외의 이용자에게는 숨길 수 있다. 이를 통해 비밀 투표의 원칙을 일정 수준 보장할 수 있다. 그러나 유권자는 실시간으로 개표되는 전자 투표용지의 수를 조회할 수 없고 중앙 기관이 발표하는 개표 결과만을 통해서 투표 결과를 알 수 있기 때문에 투표 결과를 완벽히 신뢰할 수 없다. 즉 투표 시스템의 익명성은 일정 수준 보장될 수 있지만, 검증성과 완전성을 만족시키지 못해 실제 전자투표에 사용되기 어렵다.

Public Blockchain을 이용할 경우에는 이와 반대로 중앙 기관의 개입 없이 전자 투표 플랫폼을 구성할 수 있지만 모든 트랜잭션 내역이 공개되어 트랜잭션의 주체가 되는 유권자의 신원이 드러날 수 있고, 해당 유권자가 어떤 후보자에게 투표했는지 드러날 수 있다. 그러나 트랜잭션 내용이 모두 공개되면 개표 상황을 실시간으로 투명하게 볼 수 있어 부정 개표의 가능성을 배제할 수 있다. 즉 투표 시스템의 완전성과 검증성을 확실히 보장할 수 있지만, 익명성을 보장할 수 없다. 대부분의 Public Blockchain 전자투표 플랫폼은 익명성을 보장하지 못해서 적용되지 못하고 있다.

즉 종합적으로 봤을 때, 가장 이상적인 블록체인 전자투표 플랫폼을 위해서는 Public Blockchain을 이용하여 트랜잭션 투명한 투표를 진행하되, 블록체인과 함께 각종 익명성 프로토콜을 사용하여 투표자의 신원을 보호하고, 비밀 투표의 원칙을 보장하는 플랫폼을 만들어 <표 1>의 조건을 만족하도록 한다.

본 논문에서는 블록체인의 분산 원장 노드를 Tor 방식을 사용하여 블록체인 망이 아닌 물리적 네트워크 레이어에서 패킷 역추적을 방지하면서 블록체인 망에서는 Ring Signature 방식을 통해서 트랜잭션 송신자(투표자)의 신원을 역추적할 수 없도록 묶어 전송한 후, 전자 투표용지의 목적지인 수신자(후보자)

의 Blockchain Address를 Stealth Addressing을 통해 은닉시키는 방식의 블록체인 전자 투표 플랫폼 구현 방식을 제안한다.

< 표 1. 제안 플랫폼이 만족해야하는 조건 >

	Public Blockchain 전자투표	Private Blockchain 전자투표	Public Blockchain 기반의 익명성 전자투표 블록체인 플랫폼
익명성 보장	X	△	O
실시간 개표 확인	O	X	O
위조 및 변조	X	X	X
본인 트랜잭션 확인	O	O	O

2. 관련 연구

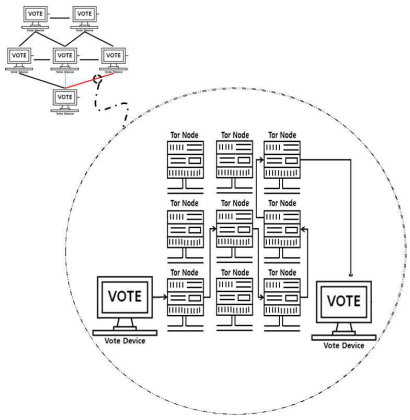
2.1 블록체인

블록체인은 P2P 방식으로 이루어진 분산 원장 기반의 공공 거래 장부로서, 각각의 분산 노드가 서로의 장부를 대조하며 조작된 내용을 수정하는 합의(Consensus) 알고리즘을 통해서 실시간으로 위·변조를 방지한다. 만약 특정 노드가 해킹당해 정보가 위·변조되었다고 하더라도, 다른 분산노드와의 합의 과정에서 위·변조된 정보는 합의 알고리즘에 의해서 자동으로 수정되므로, 위변조를 위해서는 블록체인 노드의 51% 이상을 점거해야만 한다. 이는 현실적으로 매우 어려운 일이므로, 블록체인은 사실상 해킹이 불가능한 구조라고 할 수 있다. 암 최근엔 Linux 재단과 IBM이 금융적 측면이 아닌 분산 원장 기술에 중점을 두고 다양한 산업 분야에 블록체인을 접목하기 위한 시도가 진행 중이다.

2.2 Tor

TOR(The Onion Routing)는 <그림 2>와 같은 구조로 되어 있다. 일반적인 라우팅과 달리 네트워크 패킷을 전송할 때 중간에 다수의 TOR 노드를 거치게 하는 우회 방식으로 패킷의 근원지와 도착지를 파악할 수 없게 하는 익명성 기법이다[4].

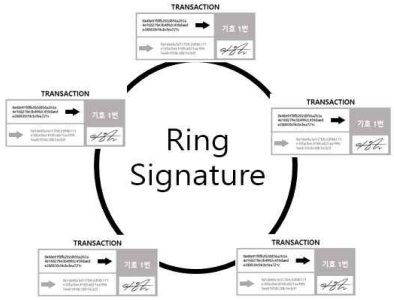
Tor노드는 전 세계적으로 퍼져있기 때문에 역추적을 통해 패킷의 근원지를 찾기 위해서는 사실상 전 세계의 Tor노드를 점거하여야 하므로, 현실적으로 역추적은 불가능하다.



< 그림 2. Tor 기법 구조 >

2.3 Ring Signature

<그림 3>의 구조를 가지는 Ring Signature는 전자 서명의 익명화 방식의 일종으로 이전 트랜잭션에서 임의로 그룹에 필요한 Dummy 참여자를 선정하여 그룹을 구성하고 그룹원 각각의 전자 서명(signature)을 묶어 링 형태의 서명을 만드는 방식이다[5]. 이렇게 생성된 링 서명은 트랜잭션에 사용되어 링-서명 구성원 중 누구의 트랜잭션인지 알 수 없도록 하여 트랜잭션의 송신자(Sender)를 특정할 수 없도록 한다.



< 그림 3. Ring Signature 구조 >

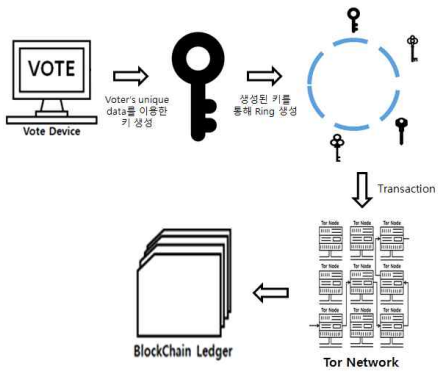
2.4 Stealth Address

Stealth addressing은 ECC(Elliptic Curve Cryptography) 와 DH(Diffle Hellman)를 결합한 ECDH 방식의 암호화 기법을 사용하여 트랜잭션(Transaction)의 수신자(receiver)를 알 수 없도록 하는 블록체인의 트랜잭션 익명화 기술이다. 이를 통해 트랜잭션의 주체를 제외한 다른 사람들은 절대로 해당 트랜잭션의 목적지를 알 수가 없다.

해싱(Hasing) 방식을 통해서 암호화된 목적지를 복호화할 수 있는 것은 오직 트랜잭션의 수신자 측의 개인키(Private Key) 뿐이기 때문이다[6].

3. 제안 방식

3.1 제안 플랫폼 도식도



< 그림 4. 투표 플랫폼 도식도 >

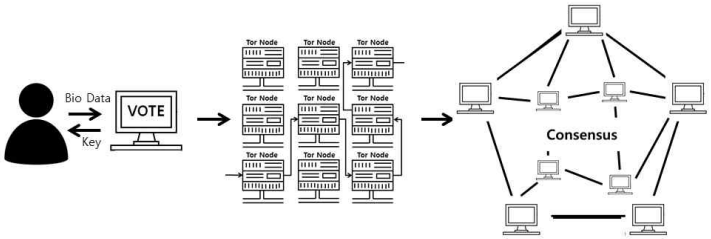
제안된 구조<그림 4>에서 단말기는 투표자의 생체인증을 바탕으로 생성된 Unique Data를 이용하여 전자 서명에 사용될 Key를 생성한다. 그 후, 유권자가 전자투표를 진행하게 되면, 투표 정보를 담은 트랜잭션이 생성된다. 트랜잭션의 내역이 공개되는 Public Blockchain의 특성에 의해서 투표자는 자신의 트랜잭션 내역을 조회하고, 개표 결과를 실시간으로 블록체인망을 통해서 조회할 수 있다. 하지만, Public Blockchain을 이용할 경우, 자신의 트랜잭션 정보가 공개되어 유권자가 어떤 후보에게 투표하였는지가 노출될 수 있다.

제안하는 방식에서는, Stealth Address 기법을 사용하여 트랜잭션의 목적지인 후보자(Receiver) 측의 주소를 감춘다. 그 후에 트랜잭션의 전자 서명을 링 형태로 융합시키는 Ring Signature 기법을 통해서 해당 트랜잭션의 투표자(Sender)가 누구인지 특정 지을 수 없도록 하여 투표자 측의 주소를 역추적 할 수 없

는 상태(Untraceable)로 만든다. 이를 통해서 블록체인 망에서의 완벽한 익명성을 보장하면서도 개표의 투명성과 완전성을 보장할 수 있다.

3.2 물리적 우회 방식 구조도

블록체인에서의 익명성은 다양한 익명성 프로토콜을 통해서 보장할 수 있지만, 네트워크 계층(Network Layer)에서의 물리적인 익명성도 중요하다. 따라서 제안하는 방식에서는 Tor(The Onion Routing)를 통해서 물리적인 익명성 또한 보장할 수 있다.

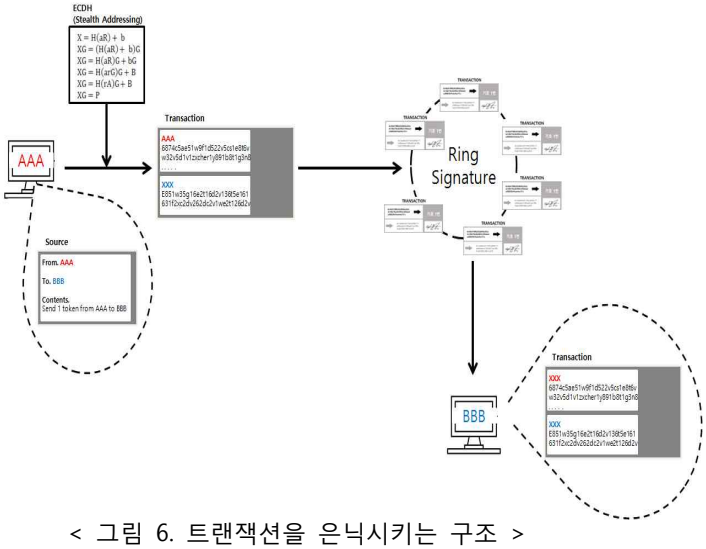


< 그림 5. 네트워크 계층에서의 우회 구조 제안 >

블록체인 망은 분산노드로 이루어져 있고, 브로드캐스팅(Broadcasting)방식을 통해서 장부를 공유한다.

<그림 5>에서 확인할 수 있는 제안 구조에서는 패킷 근원지의 IP주소와 정보를 숨기기 위해서 투표 단말기와 블록체인 노드의 연결 중간에 TOR 노드를 섞어서 패킷을 우회 전송시키는 Tor 기법을 사용한다. 이를 통해 블록체인망 뿐만 아니라 네트워크 계층에서의 익명성 또한 보장할 수 있다.

3.3 트랜잭션 은닉 방법



< 그림 6. 트랜잭션을 은닉시키는 구조 >

제안된 트랜잭션 구조 <그림 6>은 기존 구조와 달리 일반적인 공개키로 해싱(Hasing)하는 방식을 채택하지 않았다. 그 대신 ECDH(Elliptic Curve + Diffie-Hellman) 암호학 기법을 통해 해싱 한다. ECDH 암호학 기법을 사용할 경우, 공개키를 해싱하는데에 사용된 개인키를 가지고 있는 트랜잭션의 수신자(Receiver) 외에는 해당하는 트랜잭션을 조회하여도, 암호화된 목적지 주소의 해싱 값은 알 수 있지만, 그 Hash 값이 어떤 대상을 가리키고 있는지 복호화하여 확인할 수 없다. 즉 투표에서 어떤 후보자에게 해당 트랜잭션이 투표를 진행하는지를 은닉시킨다. 그 후 이렇게 만들어진 트랜잭션들은 더미로 사용되는 다른 트랜잭션들과 함께 Ring 형태로 묶어 전송한다. 이때 더미로 사용되는 트랜잭션은 이전에 사용되었던 트랜잭션 중 임의의 값을 사용한다. Ring형태로 전송된 transaction 은 송신자를 특정할 수 없게 해주며, 수신자 측에서는 더미 트랜잭션들을 Hash를 복호화 하는 과정과, consensus 알고리즘을 통한 이중제출방지를 통해 Valid 트랜잭션을 색출하여, 이를 원장에 기록하고 진행하게 된다. Ring Signature를 통해서 유권자(송신자)의 신원을 익명화 시킬 수 있다. 따라서 제안하는 방식에서는 Public Blockchain의 투명성과 검증성을 보장하면서도, Private Blockchain 이상의 익명성을 제공할 수 있다.

4. 결론 및 향후 연구

본 논문에서는 익명성과 검증성을 모두 보장하는 전자 투표 블록체인 플랫폼에 대한 구현 방법을 제안하였다. 기존의 블록체인 투표 플랫폼은 Public Blockchain을 이용하여 트랜잭션 내역을 공개하여 투명성은 보장하였지만, 익명성을 보장하지 못한다는 한계를 가지고 있었다. 본 논문에서는 Public Blockchain과 Stealth Addressing 그리고 Ring Signature를 결합함으로써 익명성과 투명성을 모두 보장할 수 있는 블록체인 플랫폼을 제안하였다.

향후 연구방향으로는 다양한 암호학 기법을 사용함으로써 발생하는 트랜잭션의 오버헤드를 줄여 퍼포먼스를 향상시키고, 보다 적은 비용을 소비하면서 익명성과 투명성 모두를 보장할 수 있는 암호학 기법을 구현하고, 향상 시킬 것이다.

5. 참고 문헌

[1]Satoshi Nakamoto. "Bitcoin: A Peer-to-Peer Electronic Cash System" bitcoin.org, 2009.

[2]허원근, 김희선, 김광조. "전자선거 프로토콜의 요구사항 연구,"『정보보호학회지』, v.10, no.1, 63-69, 2000.

[3]Yoshiharu Akahane, Manabu Aikei., Blockchain SHIKUMI TO RIRON, rictelecom, Oct.2016

[4]Robert Koch, Mario Golling, and Gabl Dreo Rodosek. "How Anonymous Is the Tor Network? A Long-Term Black-Box Investigation", Computer,vol.49,no.,pp.42-49, Mar.2016

[5]Adam Bender, Jonathan Katz, Ruggero Morselli. "Ring Signatures : Stronger Definitions, and Constructions without Random Oracles", Theory of Cryptography, Third Theory of Cryptography Conference, TCC 2006, New York, NY, USA, March, 2006

[6]Verge Foundation,"Verge-Anonymity-Centric-CryptoCurrency "(White paper), Oct, 2017