KIPS Trans. Comp. and Comm. Sys.
Vol.12, No.8 pp.253~262
ISSN: 2287-5891 (Print), ISSN 2734-049X (Online)

https://doi.org/10.3745/KTCCS.2023.12.8.253

A Hybrid Blockchain-Based E-Voting System with BaaS

Kang Myung Joe† · Kim Mi Hui††

ABSTRACT

E-voting is a concept that includes actions such as kiosk voting at a designated place and internet voting at an unspecified place, and has emerged to alleviate the problem of consuming a lot of resources and costs when conducting offline voting. Using E-voting has many advantages over existing voting systems, such as increased efficiency in voting and ballot counting, reduced costs, increased voting rate, and reduced errors. However, centralized E-voting has not received attention in public elections and voting on corporate agendas because the results of voting cannot be trusted due to concerns about data forgery and modulation and hacking by others. In order to solve this problem, recently, by designing an E-voting system using blockchain, research has been actively conducted to supplement concepts lacking in existing E-voting, such as increasing the reliability of voting information and securing transparency. In this paper, we proposed an electronic voting system that introduced hybrid blockchain that uses public and private blockchains in convergence. A hybrid blockchain can solve the problem of slow transaction processing speed, expensive fee by using a private blockchain, and can supplement for the lack of transparency and data integrity of transactions through a public blockchain. In addition, the proposed system is implemented as BaaS to ensure the ease of type conversion and scalability of blockchain and to provide powerful computing power. BaaS is an abbreviation of Blockchain as a Service, which is one of the cloud computing technologies and means a service that provides a blockchain platform ans software through the internet. In this paper, in order to evaluate the feasibility, the proposed system and domestic and foreign electronic voting-related studies are compared and analyzed in terms of blockchain type, anonymity, verification process, smart contract, performance, and scalability.

Keywords : Hybrid-Blockchain, BaaS(Blockchain as a Service), E-Voting, Smart Contract

BaaS를 이용한 하이브리드 블록체인 기반 전자투표 시스템

강 명 조† · 김 미 희††

요 약

전자투표는 정해진 장소에서의 키오스크 투표, 정해지지 않은 장소에서의 인터넷 투표 등의 행위를 포함한 개념으로, 오프라인 투표 수행 시 많은 자원과 비용이 소모되는 문제를 완화하기 위해 등장했다. 전자투표를 사용하면 투표 및 개표 업무의 효율성 증대, 비용 감소, 투표율 상승, 오류 감소 등 기존 투표시스템에 비해 많은 이점을 가진다. 하지만 중앙집중식 전자투표는 타인에 의한 데이터 위·변조 및 해킹 우려로 투표 결과를 신뢰할 수 없어 공적 선거 및 기업 안건 투표에 주목받지 못했다. 이를 해결하기 위해 최근에는 블록체인 기술을 활용한 전자투표 시스템을 설계하여 투표정보의 신뢰성 증가, 투명성 확보 등 기존의 전자투표에서 부족한 개념을 보완하는 연구가 활발히 진행되어왔다. 본 논문에서는 퍼블릭 블록체인과 프라이빗 블록체인을 융합하여 사용하는 하이브리드 블록체인 기술을 도입한 전자투표 시스템을 제안하였다. 하이브리드 블록체인은 프라이빗 블록체인을 이용해 느린 트랜잭션 처리 속도와 수수료 문제를 해결하고, 퍼블릭 블록체인을 통해 거래의 투명성과 데이터 무결성 부족 문제를 보완할 수 있다. 또한, 설계한 시스템을 BaaS로 구현하여 블록체인의 타입 변환 용이성 및 확장성을 확보하고 강력한 연산력을 제공할 수 있도록 한다. BaaS란, Blockchain as a Service의 약어로 클라우드 컴퓨팅 기술 중 하나이며 인터넷을 통해 블록체인 플랫폼 및 소프트웨어를 제공하는 서비스를 의미한다. 본 논문에서는 타당성을 평가하기 위해 제안시스템과 국내외에서 진행한 전자투표 관련 연구를 블록체인 타입, 익명성, 검증 프로세스, 스마트 계약, 성능, 확장성 측면에서 비교 분석한다.

키워드 : 하이브리드 블록체인, 서비스형 블록체인, 전자투표, 스마트 계약

1. 서 론

현재 우리나라는 대통령선거, 국회의원 선거 등 대다수의 투표는 오프라인을 통해 진행하고 있다. 다만, 이러한 오프라인 투표는 투표용지의 준비, 투표소의 준비 및 투표 관리자, 개표 결과 도출 등 많은 자원이 소모되며 선거 후 사용하지

※ 이 논문은 2018년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No.2018R1A2B6009620).
† 준 회 원 : 한경국립대학교 컴퓨터응용수학부 석사과정
†† 종신회원 : 한경국립대학교 컴퓨터응용수학부 교수
Manuscript Received : January 27, 2023
First Revision : March 20, 2023
Accepted : March 28, 2023
* Corresponding Author : Kim Mi Hui(mhkim@hknu.ac.kr)

않은 용품들은 재활용이 힘들어 폐기 처분하고 있는 문제가 있다. 또한, 노약자나 장애가 있는 사람들은 한정된 시간 및 보행의 불편함, 인지 부족 등으로 투표에 참여하지 못하는 경우가 있어 전반적인 투표율의 감소를 확인할 수 있다. 이러한 문제를 해결하기 위해 많은 국가에서는 오프라인 투표가 아닌 전자투표 시스템을 도입하기 위한 다양한 연구를 진행하고 있다[1]. 전자투표의 개념은 2000년대 이전에도 제안되었지만, 해킹으로 인해 투표 데이터의 무결성이 확보되지 않거나 익명성 확보 불가 등 자신의 투표정보가 위・변조될 수 있다는 우려로 인해 실질적인 적용이 어려운 상황이었다. 하지만 2000년대 이후 블록체인 기술 개념이 등장하며 전자투표에서 확보하지 못했던 공정성 및 익명성을 확보할 수 있도록 하는 연구가 활발히 진행되었다[2]. 블록체인이란 P2P 환경에서 분산 데이터베이스의 한 형태로 데이터를 중앙서버 한 곳에 저장하는 것이 아닌 블록체인 네트워크로 연결된 여러 컴퓨터에 기록 및 관리하는 기술을 의미한다[3]. 블록체인 환경에서 데이터의 위・변조를 수행하기 위해서는 네트워크 내 존재하는 모든 노드의 내용을 수정해야 하기에 실질적으로 불가능하며 하나의 블록이 수정되면 이후의 블록에 포함된 해시 정보가 모두 변조되므로 해킹의 공격을 빠르게 파악할 수 있어 안전하다. 또한, 모든 거래정보가 투명하게 공개되어 네트워크에 참여한 모두가 내용을 확인할 수 있어 투명성을 확보할 수 있다. 블록체인을 이용한 전자투표 시스템을 도입하면, 기존의 전자투표의 단점을 보완할 수 있다. 전자투표에 블록체인을 도입한 대표적인 예시로 스페인의 한 정당 포데모스(Podemos)는 직접 민주주의를 추구하는 방식으로 블록체인 기반의 투표 '아고라 보팅'을 실행하여 온라인을 통한 정당 투표의 참여를 가능하게 했다[4]. 호주의 '플럭스(Flux)'는 블록체인 기반의 전자투표로 당원의 의사결정을 손쉽게 해 정치 참여를 증가시켰다. 국내에도 정당의 경선, 아파트 동대표 선거 등에 활용하기 위한 블록체인 투표시스템을 구상한 다양한 연구가 진행되었다[5].

본 논문에서는 오프라인 투표의 환경문제 및 투표 환경 개선, 노약자나 장애인의 접근성 개선을 성취할 수 있는 원격 투표시스템, 원격 투표 키오스크 등을 통한 참여율 개선 등을 위해 하이브리드 블록체인 기반 전자투표 시스템을 제안한다. 하이브리드 블록체인은 클라우드 서비스로 제공하며 투표자를 인증하기 위한 인증 블록체인, 투표 집계를 위한 집계 블록체인으로 구성한다. 블록체인 간 통신은 스마트 계약을 이용해 수행하여 불필요한 연산을 최소화한다.

본 논문의 구성은 다음과 같다. 2장에서는 본 논문에서 제안하는 시스템에 대한 배경지식을 서술하며, 3장에서는 제안 시스템 및 구성요소 등을 서술한다. 4장은 제안시스템과 기존 연구를 몇몇 기준에 따라 비교하고 논의하며, 5장에서는 연구의 의의와 앞으로의 연구 방향성을 제시한다.

2. 배경 지식

2.1 하이브리드 블록체인과 BaaS

하이브리드 블록체인은 블록체인 구조 중 블록 내용이 제3자에게 모두 공개되는 퍼블릭 블록체인과 기업 및 특정 단체에서 운영하는 프라이빗 블록체인을 연결하여 사용하는 구조를 뜻한다.

Fig. 1은 블록체인의 유형에 따른 퍼블릭, 하이브리드, 프라이빗 블록체인을 나타낸다. 하이브리드 블록체인의 경우 개념적으로 일부 노드는 퍼블릭으로, 일부 노드는 프라이빗하게 운영할 수 있다. 이는 퍼블릭 블록체인에서의 느린 성능 및 익명성 불만족, 높은 수수료 등의 문제점과 프라이빗 블록체인에서의 투명성 불만족 및 보안성 약화 등의 문제점을 해결하면서 두 블록체인의 주요 특성은 모두 만족할 수 있도록 설계되었다. 트랜잭션을 처리하기 위한 채굴 과정은 프라이빗 블록체인에 속해있는 특정 노드를 선정해 퍼블릭 블록체인에서의 트랜잭션 처리를 보완하며, 검증이 필요한 프로세스는 퍼블릭 블록체인에서 처리함으로써 투명성을 제공할 수 있다. 설계된 구조 중 블록체인에 접근하기 위해서는 조직이 정해둔 규칙을 만족하거나, 조직으로부터 접근을 인가받아야 한다. 이러한 특성을 이용해 하이브리드 블록체인에서는 사용자들의 개인정보, 민감정보 등을 외부로부터 보호하고, 외부 공격자의 접근을 차단하여 51% 공격, 계정 탈취 등의 가능성을 배제할 수 있다. 하지만 2가지 블록체인을 동시에 사용하기 때문에 시스템의 세부 설계 및 통신 과정이 기존 블록체인 네트워크 구성보다 복잡한 단점이 있다[6].

하이브리드 블록체인은 인터넷으로 블록체인 플랫폼 및 소프트웨어를 제공하는 클라우드 서비스인 BaaS(Blockchain as a Service)로 이용했을 때 유용하게 사용될 수 있다. BaaS는 클라우드 서비스를 이용해 인프라, 플랫폼, 소프트웨어 등을 제공하는 개념을 블록체인에 접목한 서비스로, 주로 블록체인 플랫폼 및 블록체인 소프트웨어를 제공한다. BaaS

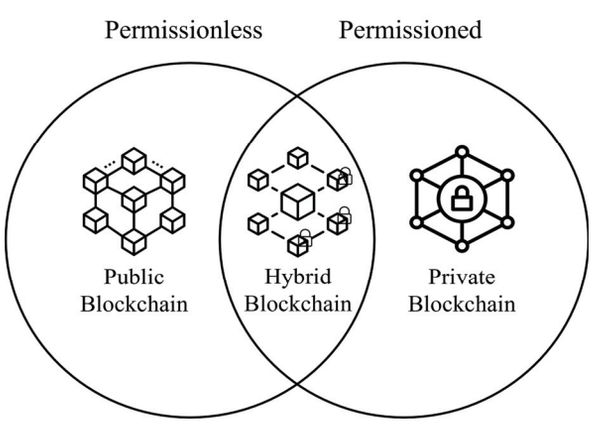

Fig. 1. Type of Blockchain Network

를 이용하면 네트워크 구성 및 변경이 자유로운 클라우드의 특성을 통해 블록체인 타입의 변환이 자유로워 구성하고자 하는 시스템에 맞게 퍼블릭/프라이빗/하이브리드 블록체인을 구성할 수 있다. BaaS는 기존 클라우드 서비스의 장점인 운영 비용 감소, 강력한 접근 제어, 확장성 확보 및 유연성 제공 등의 특성을 이용한 시스템 구성이 가능하다. 또한, 개발 과정의 초기 설정 및 네트워크 구성은 클릭 몇 번으로 클라우드 서비스 제공자가 대신 구현하기 때문에, 개발 비용 및 기간이 감소하며 노드 간 통신에 암호화를 제공하여 신뢰성을 보장할 수 있다. 현재 BaaS는 클라우드 서비스를 제공하는 IBM, Microsoft, Amazon 등 세계 유명 IT 기업, 국내의 KT, 두나무 등의 기업에서 제공하고 있으며 지속적인 연구, 개발 중이다[7].

2.2 전자투표

전자투표란, 일반적으로 투표소에 방문하여 표를 행사하는 기존의 투표가 아닌, 정해진 장소 혹은 정해진 장소 외의 공간에서 인터넷 네트워크를 통해 표를 행사하는 방식이다. 정해진 장소에서의 전자투표는 투표권을 가진 투표자가 투표소나 주민센터 등에 방문하여 투표를 위한 키오스크, 터치스크린, 전자투표기 등에 마우스를 이용, 터치 등의 방식을 이용해 투표권을 행사한다. 정해지지 않은 장소에서의 전자투표는 투표권을 가진 투표자가 네트워크를 통해 자신의 스마트폰이나 PC로 투표권을 행사한다. 일부 국가에서는 전자투표를 도입함으로써 공정성 및 효율성 제고, 선거에 필요한 비용 및 시간 절약, 투표 참여율 상승, 개표 오류율 감소, 무효표 비율 감소 등의 많은 긍정적인 효과를 확인했다. 대표적으로 에스토니아는 감소하는 투표율 제고, 선거 결과의 정당성 확보를 위해 블록체인 기반 대규모 전자투표를 투표소 및 원격으로 수행했고, 지금까지 11번의 전자투표를 문제없이 수행하며. 국민의 약 절반이 전자투표를 이용해 투표한다. 또한, 국가가 아닌 기업이나 학교와 같은 단체에서는 주로 투표용지의 제조, 운반, 집계 등의 과정을 간소화하기 위해 전자투표를 사용한다[8-10]. 전자투표에 참여하는 엔티티는 투표자, 등록 기관, 집계 기관이 있다. 투표자는 투표를 위한 권리를 가진 자를 의미하며, 등록 기관은 투표를 개설하고, 투표자 인증, 안건 및 후보자를 등록하는 기관, 집계 기관은 투표자가 행사한 투표 값을 집계한다. 투표는 등록 기관에 의해 허용된 투표자만 참여할 수 있어야 하며, 1번만 행할 수 있어야 한다. 또한, 투표자가 행사한 투표 값의 집계에 있어 외부로부터 보호되어야 하며, 투표자의 신분이 외부에 노출되지 않도록 시스템을 구성해야 한다[11,12].

2.3 스마트 계약

2000년대 블록체인 기술의 등장으로 주목받기 시작한 스마트 계약은 닉 스자보에 의해 1994년에 제안되었다[13]. 이는 계약 조건을 일종의 소스 코드로 정의하고 조건이 충족되면 즉시 계약이 실행되는 전자거래 시스템을 의미한다. 계약 과정에 있어 별도의 중개 과정이 필요하지 않고 발행된 계약의 조건 수정이 어려워 중개 수수료를 절약하고 계약과정에서 발생할 수 있는 분쟁을 최소화한다. 스마트 계약은 주로 이더리움[14] 기반 플랫폼에서 사용되며, 튜링 완전 언어인 솔리디티[15] 프로그래밍 언어를 이용해 계약을 정의한다.

2.4 기존 연구

연구 [16]은 메시지 원문을 제공하지 않은 채 서명자에게 서명받는 기술인 은닉서명과 N명으로 구성된 투표자 그룹의 대상자들을 유추할 수 없도록 하는 투표자 믹스, 그러한 그룹들의 서버를 혼합하는 서버 혼합 믹스를 활용한 하이브리드 믹스 방식을 사용하여 투표자의 신원을 보호하는 블록체인 기반 익명 전자투표 시스템을 제안했다. 다만 이러한 방식은 일정 인원이 모인 후에 투표를 진행할 수 있다는 문제점을 가진다.

연구 [17]은 주민등록번호와 지문 정보에 동형암호기법을 활용한 암호화를 통해 복호화 없이 투표자의 신원을 확인한 후 안건-표본번호로 구분된 코인(투표권)을 발행해 노드에 코인을 보내는 방식으로 투표를 진행하는 투표시스템을 제안했다. 이때 동형암호기법은 투표권자의 익명성을 보장해주며, 투표권자 인증 후 투표를 수행할 수 있도록 하는 역할이다. 투표 결과는 타임스탬프로 기록을 남겨 모두가 확인할 수 있게 했으며, 투표의 집계 결과는 선택지 노드별 잔액 확인을 통해 확인할 수 있다. 투표시스템은 컨소시엄 블록체인을 적용하여 퍼블릭 블록체인으로 투표시스템을 구성했을 때 발생할 수 있는 합의 문제를 보완하기 위해 순환순서 합의 모형을 제시하였다. 이는 블록의 생성 권한을 신뢰할 수 있는 집단에 균형 있게 나누어 한 집단이 투표를 독점할 수 없는 공정한 투표를 유도하는 방식이다.

연구 [2]는 이더리움 솔리디티 언어 기반 스마트 계약을 이용해 탈중앙화 투표시스템을 제안했다. 제안시스템은 사용자를 구분하기 위해 16진수 형태의 주소 계좌를 생성한 후 중복 투표를 방지하기 위해 해당 주소의 사용자가 투표 시 투표 유/무를 참/거짓으로 저장하여 투표했음을 기록한다. 이후 투표 값의 집계는 스마트 계약 기반으로 이루어지며, 후보자의 성명을 입력하는 함수를 사용해 사용자별 투표 집계 여부를 확인할 수 있다. 다만 솔리디티 기반의 스마트 계약은 배포 이후 수정이 어려워 유지보수 측면에 어려움이 있다는 단점을 가지고 있다.

연구 [18]은 퍼블릭 블록체인을 기반으로 한 투표시스템을 제안했으며, 유권자들의 투표 환경을 감독하기 위해 POA 합의 알고리즘을 사용하는 블록체인을 구성했다. 제안한 블록체인 투표시스템에는 각 투표 지역을 나타내는 District Node와 BootNode가 존재한다. Distric Node에 속한 선거

관리자가 선거 생성 시 스마트 계약이 발행되어 투표용지를 배부하며 해당 투표 데이터를 검증한다. BootNode는 각 지역 노드가 서로 통신할 수 있도록 하며, 정적 IP에서 실행해 District Node가 다른 노드들을 더 빠르게 찾을 수 있도록 한다. 투표시스템에서 투표 과정은 각 유권자가 확인하기 위해 각자에게 트랜잭션 ID를 할당하여 투표하게 되는데, 이를 각 District Node의 다른 노드가 동의할 시에만 다음 체인에 추가하게 된다. 이를 통해 각 유권자의 개인정보보호 및 보안 및 투명성 요구 사항을 충족할 수 있다.

연구 [19]는 대시 코인의 마스터 노드의 개념을 응용해 투표자의 익명성을 보장하는 블록체인 투표시스템을 제안했다. 해당 시스템의 투표 서비스 구조는 먼저 선거관리위원회는 유권자, 후보자, 투표 기간 등에 대한 정보를 블록체인에 저장한다. 이후 투표 기간에는 유권자에 대한 정보를 확인하고 해당 유권자가 확인되면 투표용지인 ERC20과 유사한 토큰을 분배한다. 원하는 후보자에게 해당 토큰을 전송하는 투표의 단계를 거치게 되면 투표 종료 후 이를 집계하게 된다. 이때 투표자의 익명성을 보장하기 위해서 대시 코인의 마스터 노드를 사용했다. 유권자들은 투표 후 각 단계에서 랜덤한 마스터 노드에 해당 정보를 암호화하여 전송하고 해당 마스터 노드를 1차적으로 믹싱한다. 이렇게 생성된 마스터 노드들을 다른 마스터 노드에 전송하여 반복하여 믹싱한다. 이러한 과정을 체인믹싱이라고 한다. 체인믹싱이 완료되면 해당 정보를 후보자 계좌에 전송하여 투표의 결과를 확인할 수 있게 된다.

3. 제안시스템

Fig. 2는 본 논문에서 제안하고 있는 기법의 표면적인 흐름을 나타낸다. 투표 이벤트가 발생한 상태에서 투표자가 인증 블록체인(Fig. 2. Auth Blockchain)에 키를 요구하면, 인증 블록체인은 키 생성 스마트 계약을 통해 키 생성 트랜잭션을 수행하여 투표자의 개인정보 및 요청 시각을 기반으로 키를 생성한 뒤 투표자에게 건네준다. 건네준 키는 이후 투표자의 표를 검증할 때 사용한다. 임시 키를 받은 투표자는 [키, 투표 값]의 파라미터를 이용한 투표 스마트 계약을 발행하여 투표를 진행하며, 키 암호화 트랜잭션에서 투표 값을 투표자의 개인키로 전자서명하고 키값은 집계 블록체인(Fig. 2. Tally Blockchain)의 투표 관리 노드의 공개키로 암호화를 수행한다. 그 후 투표 값 전달 트랜잭션을 통해 집계 블록체인에 값을 전달하며, 투표 스마트 계약으로부터 값을 받은 집계 블록체인의 투표 관리 노드는 임시 키 검증 스마트 계약을 발행하여 키 해시 트랜잭션으로 사용자가 전달한 키의 해시값을 구하고 키 검증 트랜잭션을 통해 인증 블록체인이 저장한 해시값과 비교하여 검증 후, 검증이 성공적으로 끝난 경우에만 투표 집계를 진행한다.

Fig. 3은 클라우드 서비스 BaaS를 이용해 인증 블록체인과 집계 블록체인을 구성하고, 설계한 시스템에서 사용하는 스마트 계약 구조를 나타낸다. 본 논문에서 제안한 기법은 하이브리드 블록체인 구조를 사용해 퍼블릭 블록체인의 느린 트랜잭션 처리 속도와 비싼 수수료 문제를 해결하고 프라이빗 블록체인의 투명성과 데이터 무결성 부족 문제를 보완한

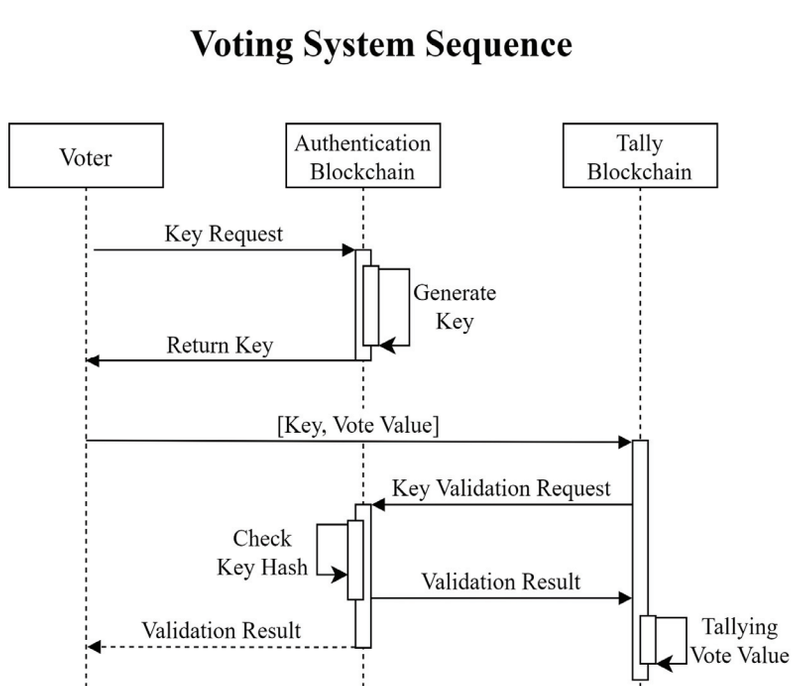

Fig. 2. Sequence of Voting System

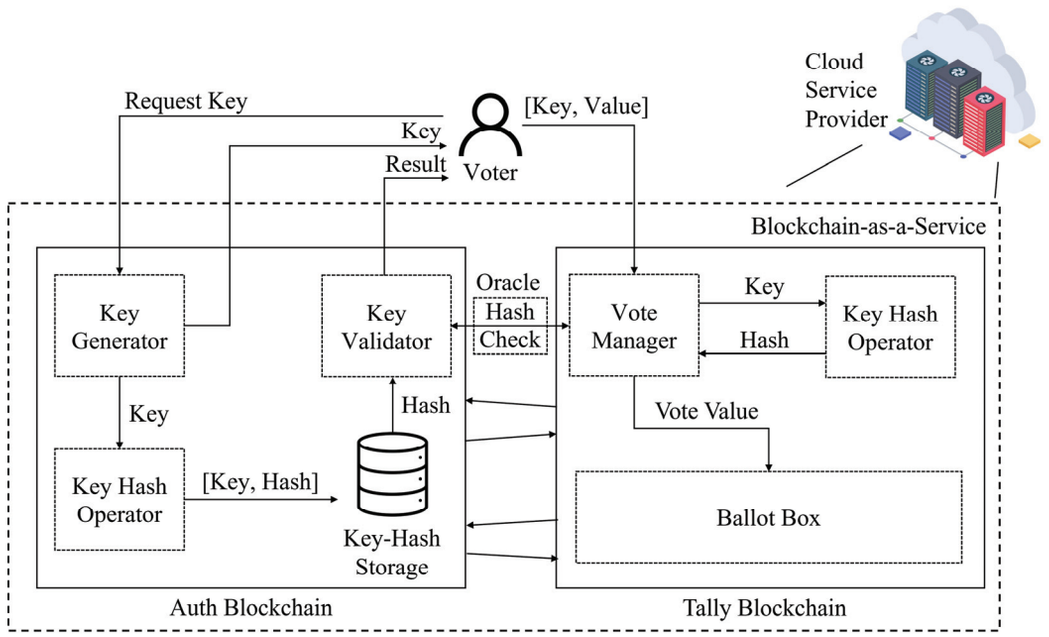

Fig. 3. Structure of Proposed System

다. 프라이빗 블록체인에 참여하는 노드는 누구나 신뢰할 수 있는 주체로 선정하며 클라우드 시스템에서 스마트 계약, 트랜잭션을 처리할 수 있는 채굴 노드를 다수 지정하여 대규모 투표 상황에서도 빠른 일 처리가 가능하게 한다. 또한, 퍼블릭 블록체인과 통신하는 투표자의 스마트 계약, 인증 블록체인의 스마트 계약은 외부에 불필요한 정보의 유출이 없도록 데이터를 암호화하거나 은닉할 수 있도록 한다. 두 가지 형태의 블록체인을 사용하면서, 각 블록체인이 다루는 데이터를 분리하여 기밀성을 보장한다. 인증 블록체인의 경우 투표자에게 임시 키를 발급해주지만 이후 과정에서 투표자가 어떤 투표 값을 실행했는지 알 수 없다. 집계 블록체인의 경우 투표자로부터 임시 키값과 투표 값을 받아 집계를 수행하지만, 임시 키로부터 특정 투표자를 생각할 수 없다. 또한, 모든 과정은 스마트 계약과 해시 추출, 암호화 및 전자서명을 통해 처리되므로 데이터의 무결성 및 정당성을 보장할 수 있다.

제안시스템은 투표자(Fig. 3. Voter), 인증 블록체인(Fig. 3. Auth Blockchain), 집계 블록체인(Fig. 3. Tally Blockchain)으로 구성되며 인증 블록체인은 프라이빗 블록체인, 집계 블록체인은 퍼블릭 블록체인으로 한 하이브리드 블록체인 기반 시스템을 구성한다. 투표자는 투표 행위의 주체로, 인증 블록체인에 자신을 인증하고 투표를 위한 임시 키(ID)를 발급받은 뒤 이를 이용해 투표한다. 해당 키를 기반으로 추후 자신의 표가 방해와 조작 없이 수행되었는지 확인할 수 있다. 인증 블록체인은 투표를 운영하는 주체로 키 생성 노드(Fig. 3. Key Generator), 키 검증 노드(Fig. 3. Key Validator), 키 해시 노드(Fig. 3. Key Hash Operator), 키 해시 저장소(Fig. 3. Key Hash Storage)로 구성된다. 각 노드는 데이터 전송과정의 암호화 및 전자서명을 위해 자신만의 공개키, 비밀키를 갖는다. 키 생성 노드는 투표자의 정보가 포함된 키 생성 요청을 통해 인증과정을 거쳐 키를 생성하기 때문에 인증 정보를 가진 국가 기관, 기업 내 인사팀 등이 될 수 있으며, 투표자가 투표 권한이 존재하는지 확인하고, 투표 임시 키를 생성해 전달한다. 임시 키는 투표 기간에만 사용할 수 있는 일종의 주소이며 인증 블록체인에서 키 풀을 구성하여 관리한다. 키 검증 노드는 투표 블록체인의 투표 관리 노드(Fig. 3. Vote Manager)로부터 투표자 검증 요청이 온 경우 키-해시 저장소(Fig. 3. Key-Hash Storage)로부터 해시값을 받아 검증을 수행하고, 결과를 투표자에게 알려주어 투표 행위가 정상적으로 수행되었음을 알 수 있도록 한다. 집계 블록체인은 투표 관리 노드, 키 해시 노드, 투표함으로 구성된다. 투표 관리 노드는 투표자의 투표 값이 유효한 투표인지 검증하는 과정을 거쳐 투표 집계를 수행하는 주체로 선거운영위원회, 기업 내 의사결정지원팀, 정당 등이 될 수 있으며 사전에 공고된 후보 혹은 안건에 따라 투표 값을 집계한다. 이는 투표자가 투표를 수행했을 때 투표자의 투표 권한을 인증 블록체인에 저장되어있는 해시값을 오라클 서비스를 통해 확인하여 정상적인 투표자인 경우에만 투표함에 집계를 수행할 수 있도록 한다. 오라클 서비스는 서로 다른 블록체인 네트워크 사이에서의 통신 및 상호작용을 가능하게 하는 크로스 체인 플랫폼으로, 스마트 계약 간의 데이터 처리도 가능하도록 도와주며 외부 이벤트를 불러오는 역할도 한다. 대표적인 오라클 서비스 제공자로는 체인링크[20]가 있다. 인증 블

록체인과 집계 블록체인에 존재하는 키 해시 노드는 동일한 기능을 수행하며, 키를 입력으로 받아 keccak256 해시 함수를 이용해 해시 문자열을 추출하는 역할을 한다.

시스템에서 인증 블록체인은 프라이빗 블록체인으로, 하이퍼레저 패브릭[21] 블록체인을 구성하며 집계 블록체인은 퍼블릭 블록체인으로 이더리움의 확장성 문제를 해결하기 위해 등장한 폴리곤(Polygon)[22] 블록체인을 구성한다. 폴리곤 블록체인은 이더리움 EVM(Ethereum Virtual Machine)을 일부 수정하여 구성한 블록체인으로, 이더리움과 비교해 높은 트랜잭션 처리량, 낮은 트랜잭션 수수료 등을 갖는 퍼블릭 블록체인이며 이더리움의 프로그래밍 언어인 솔리디티를 사용하여 DAPP(Decentralized Application) 및 스마트 계약을 개발할 수 있다. 두 블록체인 모두 오라클 서비스를 사용한 상호작용이 가능하며 하이퍼레저 패브릭은 ECC (Elliptic Curve Cryptography) 기반 공개키 암호 기능을 이용해 암호화를 진행하고 폴리곤은 솔리디티의 crypto 라이브러리 혹은 오픈제플린(OpenZeppelin) 라이브러리[23]를 이용해 암호화를 진행한다.

3.1 투표 스마트 계약

투표 스마트 계약에는 키 암호화 트랜잭션, 투표 값 전송 트랜잭션이 존재하며, 투표자가 수행한다.

1) 키 암호화 트랜잭션

집계 블록체인은 제3 자의 열람이 가능한 퍼블릭 블록체인 형태로 구성함으로, 투표자가 투표 스마트 계약을 통해 투표 값을 건네줄 때 투표자의 정보가 노출될 수 있다. 또한, 투표 값을 전달하는 과정에서 중간자 공격 등으로 투표 값이 변경될 수 있다. 이를 방지하기 위해 투표 값을 투표자의 개인키로 전자 서명하고, 인증 블록체인의 키 생성 노드로부터 발급받은 임시 키를 집계 블록체인의 투표 관리 노드의 공개키를 이용해 암호화한다. 이는 투표 값이 중간자 공격 등으로부터 값이 변경되지 않았음을 증명하여 퍼블릭 블록체인인 집계 블록체인과의 통신 과정에서 키가 노출되지 않도록 하기 위함이다.

3.2 임시 키 발급 스마트 계약

임시 키 발급 스마트 계약에는 키 생성 트랜잭션이 존재하며, 인증 블록체인에서 수행한다.

1) 키 생성 트랜잭션

인증 블록체인의 키 생성 노드(Fig. 3. Key Generator)가 투표자로부터 키 생성 요청을 받고 키를 전달하기 위해 키를 생성하는 트랜잭션으로, 투표자가 전달한 개인정보와 시각을 이용해 생성한다. 생성한 키는 투표 기간에만 사용할 수 있는 임시 키이며, 발급한 키를 키 생성 노드의 개인키로 전자 서명한 후, 투표자의 공개키로 암호화하여 투표자에게 전달한다. 전달한 키는 키 해시 노드에서 keccack256 해시 함수를 이용해 해시 문자열을 추출하고 자신의 개인키로 해시값을 전자서명 후 키 해시 저장소(Fig. 3. Key-Hash Storage)의 공개키로 암호화해 [키, 암호화 문자열]의 형태로 저장한다. 이는 이후 임시 키 검증 스마트 계약에서 투표자의 투표 권한 확인을 위해 넘겨받은 키의 검증을 수행하기 위함이다.

2) 키 전송 트랜잭션

인증 블록체인의 키 생성 노드가 투표자로부터 키 생성 요청을 확인하고 키를 생성한 후 투표자에게 전달하기 위해 수행하는 트랜잭션으로, 발급한 키에 개인키로 전자서명 후 투표자의 공개키로 암호화를 수행해 전송한다.

3.3 임시 키 검증 스마트 계약

임시 키 검증 스마트 계약에는 키 해시 트랜잭션과 키 검증 트랜잭션이 존재하며, 집계 블록체인과 인증 블록체인이 수행한다.

1) 키 해시 트랜잭션

집계 블록체인의 투표 관리 노드는 투표자가 투표 스마트 계약을 수행하여 전달한 키를 자신의 개인키로 복호화 후, 키 해시 노드로 전달한다. 키 해시 노드는 keccak256 해시 함수를 이용하여 해시 문자열을 추출한다. 다른 여타 트랜잭션과 마찬가지로 집계 블록체인을 통해 외부로 정보가 노출되지 않도록 한다.

2) 키 검증 트랜잭션

키 검증 트랜잭션은 집계 블록체인이 키 해시 트랜잭션을 수행한 후 추출한 해시 문자열을 이용하여 사용자가 투표 값과 함께 전달한 키가 유효한지 확인하기 위한 과정으로 인증 블록체인의 임시 키 발급 스마트 계약에서 추출한 해시 문자열을 집계 블록체인의 키 해시 트랜잭션에서 추출한 해시값을 비교해 두 값이 같은 경우에만 투표 집계 스마트 계약을 발행할 수 있도록 한다. 이 과정을 통해 투표 권한을 가진 투표자만 투표에 참여할 수 있도록 할 수 있으며, 검증이 성공적으로 수행되면 결과를 투표자에게도 전송해 자신의 투표가 정상적으로 수행되었음을 알 수 있게 한다.

3.4 투표 집계 스마트 계약

투표 집계 스마트 계약에는 투표 값 저장 트랜잭션이 존재하며 집계 블록체인의 투표 관리 노드가 수행한다.

1) 투표 값 저장 트랜잭션

투표 값 저장 트랜잭션은 투표자의 투표 값이 가리키는 후

보 혹은 안건의 득표 값에 1을 더하는 연산을 수행한다. 트랜잭션은 퍼블릭 블록체인에서 이루어지는 연산이지만 실시간 진행 상황 파악 및 연산의 단순화를 위해 암호화는 진행하지 않는다. 투표 집계 스마트 계약이 수행되는 조건은 임시 키 검증 스마트 계약의 키 검증 트랜잭션 완료이므로, 검증에 성공하는 경우 투표 값 저장 트랜잭션을 수행하고 그렇지 못한 경우에는 저장하지 않는다.

3.5 전자서명 및 암호화

제안시스템에서의 통신은 각 노드의 개인키를 사용해 송신자를 인증하기 위한 전자서명과 기밀성 유지를 위해 수신자의 공개키를 통한 암호화를 진행한다.

1) 노드의 공개키 및 개인키

Table 1은 제안시스템에서 암호화 및 전자서명에 사용되는 공개키 및 개인키를 나타낸다.

Table 1. Keys for Encryption and Signature

Symbol	Meaning
$AuthPub_{g,v,h,s}$	Node's Public Key in Auth Blockchain
$TallyPub_{m,h}$	Node's Public Key in Tally Blockchain
$AuthPriv_{g,v,h,s}$	Node's Private Key in Auth Blockchain
$TallyPriv_{m,h}$	Node's Private Key in Tally Blockchain
CipherText = $En(msg,\ pubkey)$	Message Encryption using Public Key
PlainText = $De(CipherText,\ privkey)$	Message Decryption using Private Key
$Sign(msg,\ privkey)$ = (r, s)	Signature on Message using Private Key

인증 블록체인 및 집계 블록체인에 속해있는 노드 중 투표함을 제외하고 인증 블록체인에서는 키 생성기, 키 검증기, 키 해시 연산기, 키 해시 저장소는 각자의 공개키 및 개인키를 가지며 집계 블록체인에서는 투표 관리기, 키 해시 연산기가 가진다.

- $AuthPub$: 인증 블록체인 속 노드의 공개키
- $AuthPriv$: 인증 블록체인 속 노드의 개인키

인증 블록체인 속 노드 키워드
g : Key Generator
v : Key Validator
h : Hash Operator
s : Key Hash Storage

- $TallyPub$: 집계 블록체인 속 노드의 공개키
- $TallyPriv$: 집계 블록체인 속 노드의 개인키

집계 블록체인 속 노드 키워드
m : Vote Manager
h : Hash Operator

2) 메시지 전자서명 및 암호화

전자서명은 메시지를 송신하는 송신자가 메세지를 전달하는 도중 제3 자로부터 방해받지 않고 잘 전송했음을 증명하는 방법으로, 노드의 개인키를 이용해 메세지에 서명함으로써 사용한다. 암호화는 두 노드의 통신에서 외부에서 데이터를 훔쳐보는 행위나 유출되었을 때 내용을 알아볼 수 없도록 수신자의 공개키를 이용해 메시지를 암호화한다. 제안시스템의 경우 전자서명에는 ECDSA를, 암호화에는 ECC를 사용한다.

ECC는 3차 방정식으로 표현되는 유한체 상의 타원 곡선을 사용하는 암호화 기법으로, 소수체나 장 유한체 상에서 정의된다. 대표적인 공개키 암호화 알고리즘인 RSA(Rivest, Shamir, Adleman)보다 작은 키를 사용하며 더 빠른 암호화가 가능하다. 개인키는 난수 생성기를 이용해 소수를 사용하며, 공개키는 미리 정해놓은 G(x, y)를 n번 더하는 연산으로 도출한다.

ECDSA는 전자서명 기법인 DSA(Digital Signature Algorithm)의 변형으로, 타원곡선 기술을 사용해 전자서명을 수행하는 알고리즘이다. 이는 타원 곡선에 위치한 점의 스칼라 곱을 기반으로 수행한다. ECDSA에서 개인키는 정수 하나를 랜덤하게 선택하고 공개키는 개인키를 정해진 생성자 값에 곱해 선택한다.

인증 블록체인에서는 ECC 및 ECDSA를 사용하기 위해 Node.js, Java, Python과 같은 언어에서 제공하는 Fabric SDK의 cryptoSuite 라이브러리를 이용하며 집계 블록체인에서는 오픈제플린 라이브러리, secp256k1 곡선, keccak 256 해시 함수 등을 이용한다.

4. 비 교

4장 비교에서는 2장에서 나열한 기존 연구들과 제안시스템의 비교를 위해 몇 가지 특성을 기준으로 표를 작성하고, 논의한다.

4.1 블록체인 타입

블록체인 기술을 이용한 시스템을 운영하려면 블록체인 타입을 잘 선택해야 한다. 블록체인은 타입에 따라 퍼블릭, 프라이빗, 컨소시엄, 하이브리드로 구분할 수 있으며 타입마다 장단점이 존재한다. [16]의 연구에서는 블록체인 구성에 구체적인 언급이 없었고, [17]은 신뢰할 수 있는 기관들을 이용해 컨소시엄 블록체인을 구성하여 프라이빗 블록체인에서 확장성을 추가할 수 있었다. [2]는 퍼블릭 블록체인을 구성하여 탈중앙화 및 투명성 확보에 중점을 두었고, [19]의 연구는 프라이빗 블록체인으로 구성하여 운영하는 투표시스템의 데이터가 외부에 노출되지 않는 것에 중점을 두었다. 본 논문에서 제안한 시스템은 퍼블릭 블록체인과 프라이빗 블록체인을 함께 사용한 하이브리드 블록체인으로, 각 블록체인의 단점을 서로의 장점으로 상쇄할 수 있는 특성을 가진다. 모든 거래의 공개/비공개 유무를 정할 수 있어, 운영하고자 하는 시스템에 맞게 활용할 수 있다.

4.2 익명성

익명성은 온라인 투표의 주요 속성으로 특정 투표의 주체를 알 수 없게 하는 속성이다. Table 2에 나열한 시스템 중 [2]의 연구만 고려하지 않았으며 나머지 4개의 연구는 모두 고려함을 확인했다. [16]는 투표자 믹스와 서버 믹스를 함께 사용하는 하이브리드 믹스를 도입하여 익명성을 만족했고, [17]은 컨소시엄 블록체인을 기반으로 구성한 시스템의 특성을 이용해 익명성을 보장한다. [19]는 블록체인 네트워크에 포함된 모든 블록의 정보를 가지고 있는 마스터 노드를 이용한 믹싱 과정을 이용해 익명성을 보장했지만, 연산이 복잡하고 속도가 느린 단점이 있다. 제안시스템은 프라이빗 블록체인을 이용해 외부에 불필요한 데이터의 노출을 최소화했으며, 실질적인 투표 행위가 수행되는 블록체인과의 통신에서 임시 키를 사용하여 자신의 정체를 숨길 수 있도록 한다.

Table 2. Comparison with other systems

	[16]	[17]	[2]	[19]	Proposed
Blockchain Type	-	Consortium	Public	Public	Hybrid
Anonymity	O	O	X	O	O
Validation Process	O	X	X	X	O
Smart Contract	-	X	O	O	O
Performance	-	High	Low	Low	High
Scalability	-	O	-	-	O

- : No mention in the paper

4.3 검증 프로세스

온라인 투표에서의 검증은 투표자의 투표 행위가 정상적인 행위인지 판단하는 과정이다. [17], [2], [19]는 이를 위한 별도의 프로세스가 존재하지 않았다. [16]은 하이브리드 믹스를 구성하는 서버 믹스에 검증 프로세스가 존재하며 검증이 성공한 경우에만 트랜잭션을 생성하도록 구성했다. 제안시스템은 투표자가 사용한 임시 키가 실제로 투표 권한이 있어 발행된 것인지 확인하기 위해 암호화를 진행한 키의 해시값을 추출해 검증한다.

4.4 스마트 계약

투표시스템은 시작부터 끝까지 사람의 개입과 방해 없이 수행되어야 한다. 이를 잘 구현하기 위해 스마트 계약의 사용은 투표시스템에서 매우 중요하다. 다만 [16]의 연구에서는 스마트 계약을 언급하지 않았고, [17]의 연구에서는 스마트 계약을 언급했지만, 설계 및 수행하지 않았다. [2]의 연구에서는 스마트 계약을 이용했지만, 투표의 기본 기능만 구현된 스마트 계약이기에 아쉬운 부분이 있다. [19]의 연구는 트랜잭션 암호화 및 마스터 노드를 이용한 믹싱 과정 전체에서 스마트 계약을 사용했다. 제안시스템의 경우 투표를 위한 ID 요청 과정을 제외하고 모두 스마트 계약을 이용해 수행할 수 있도록 설계했다.

4.5 성능

블록체인에서 성능은 트랜잭션 처리 속도로 비교할 수 있는데, 자명하게도 퍼블릭 블록체인을 제외한 프라이빗, 컨소시엄, 하이브리드 블록체인의 처리 성능은 대부분 비슷하다. 기존 연구 중 퍼블릭 블록체인을 기반으로 사용한 [2]와[19]에서는 느린 성능을 보이며, [16], [17], 제안시스템은 빠른 처리 성능을 확보할 수 있다. 또한, [24]의 연구에서 BaaS 기반 시스템이 일반적인 시스템과 비교해 스마트 계약 배포에는 약 3.75%, 트랜잭션 처리에는 약 4.6%의 가스 사용량의 감소를 확인했다. 이는 BaaS를 사용하는 제안시스템이 일반적인 하이브리드 시스템보다 더 좋은 성능을 기대할 수 있도록 한다.

4.6 확장성

블록체인에서 확장성을 고려하려면, 기존 퍼블릭, 프라이빗 타입의 블록체인 구성보다 컨소시엄, 하이브리드 블록체인이 더 유리하다. 기존 연구 중 컨소시엄 블록체인을 구성한 [17]의 연구에서 간접적인 확장성만 언급했으며, 다른 연구들에서는 확인할 수 없었다. 제안시스템은 하이브리드 블록체인을 사용함과 동시에 클라우드 서비스로 블록체인을 제공하는 BaaS를 도입하여 강력한 컴퓨팅 연산을 기반으로 한 확장성을 보장할 수 있다.

5. 결 론

종이를 이용한 투표시스템은 환경문제 및 막대한 운영 비용 문제로 해결 방안을 탐구하고 있다. 이를 해결하기 위해 제안된 개념이 전자투표이며, 전자투표란 종이를 사용하지 않고 온라인에서 투표를 수행할 수 있는 시스템을 의미한다. 하지만 중앙집중식으로 운영되는 전자투표의 경우 투표가 조작되거나 방해받아 투표의 의미가 없어질 위험이 존재했으며, 이를 해결하는 방안으로 블록체인을 활용한 투표시스템이 등장했다.

본 논문에서는 하이브리드 블록체인과 BaaS를 이용한 투표시스템을 제안했다. 제안한 시스템은 기존 블록체인 기반 투표시스템과 달리 BaaS를 사용해 확장성을 확보할 수 있으며, 투표 성향, 규모, 종류에 따라 자유롭게 유형을 변경할 수 있는 장점이 있다. 또한 하이브리드 블록체인 구성을 사용하여 사용자의 인증 정보를 취급하는 블록체인과 투표 값을 취급하는 블록체인을 구분하여 익명성, 검증성, 기밀성 등을 확보했고 모든 연산 및 데이터의 흐름은 스마트 계약을 기반으로 수행되어 무결성을 확보했다. 다만, 다수의 스마트 계약을 유지보수 함에 있어 복잡한 점이 있다.

향후 연구에는 BaaS를 이용한 하이브리드 블록체인 구성에 있어 유지보수에 효율적인 스마트 계약 구조를 연구하고 하이브리드 블록체인 플랫폼을 고안한다. 또한, 하이브리드 블록체인 구조에서 다른 타입의 블록체인이 통신할 때 외부로부터 데이터를 보호할 수 있는 기법을 연구할 예정이다.

References

[1] W. R. Jeon, Y. H. Lee, and D. H. Won, “Current status and prospects of the electronic voting system,” *Korea Institute of Information Security and Cryptology*, Vol.21, pp.83-92, 2011.

[2] C. J. Kim, “An online voting system based on ethereum block-chain for enhancing reliability,” *Journal of Korea Academia-Industrial cooperation Society*, Vol.19, No.4, pp.563-570, 2018.

[3] H. S. Kim and H. J. Kwon, “Blockchain utilization in the insurance industry: Inspection and response,” Korea Insurance Research Institute, 2018.

[4] G. J. Song, “The socio-political possibility and prospects of blockchain,” Center for Digital Social Science, 2022.

[5] S. P. Hong, G. S. Min, and H. L. Kim “A study on the applicability of online voting system using blockchain method,” Korean Society for Internet Information, 2017.

[6] L. J. Yan and L. D. Wang, “A hybrid blockchain model for trusted data of supply chain finance,” Wireless Personal Communications, pp.1-25, 2021.

[7] J. Song, P. Zhang, M. Alkubati, Y. Bao, and G. Yu, “Research advances on blockchain-as-a-service: Architectures, applications and challenges,” Digital Communications and Networks, 2021.

[8] S. R. Kim, “Introduction of blockchain-based electronic voting in the metaverse era and how to secure election credibility,” *Korea Low Association*, Vol.22, No.2, pp.85-115, 2022.

[9] J. W. Moon, “How to introduce electronic voting within constitutional limits,” *Korea Comparative Public Law Association(KCPLA)*, Vol.22, No.1, pp.157-182, 2021.

[10] E. Y. Moon, “Review of the principle of election - Focusing on the Estonia e-voting case,” *National Information society Agency(NIA)*, Vol.29, No.4, pp.67-90. 2022.

[11] E. Abu-Shanab, M. Knight, and H. Refai, “E-voting systems: A tool for e-democracy,” *Management Research and Practice*, Vol.2, No.3, pp.264-274, 2010.

[12] O. Cetinkaya and D. Cetinkaya, “Verification and validation issues in electronic voting,” *Electronic Journal of E-government*, Vol.5, No.2, pp.117-126, 2007.

[13] N. Szabo, “Formalizing and securing relationships on public networks,” First Monday, 1997.

[14] Ethereum [Internet], https://ethereum.org/

[15] Solidity [Internet], https://soliditylang.org/

[16] Y. H. Lee, “A Blockchain-based anonymous electronic voting system,” *Journal of Information Technology and Architecture*, Vol.18, No.2, pp.199-204, 2021.

[17] H. J. Chung, “Blockchain e-voting system and governance: The case of Korean national pension service,” *The Journal of Society for e-Business Studies*, Vol.24, No.4, pp.1-16, 2019.

[18] F. Þ. Hjálmarsson, G. K. Hreiðarsson, M. Hamdaqa, and G. Hjálmtýsson, “Blockchain-based e-voting system,” *11th International Conference on Cloud Computing*, 2018.

[19] J. H. Cho, L. S. Lee, and C. H. Choi, “Anonymous block-chain voting model using the master node network,” *Journal of the Korea Academia-Industrial Cooperation Society*, Vol.22, No.5, pp.394-402, 2021.

[20] Chainlink [Internet], https://chain.link/

[21] Hyperledger Fabric [Internet], https://www.hyperledger.org/use/fabric

[22] Polygon [Internet], https://polygon.technology/

[23] OpenZeppelin, [Internet], https://www.openzeppelin.com/

[24] M. J. Kang and M. H. Kim, “A study on non-fungible token platform for usability and privacy improvement,” *KIPS Transactions on Computer and Communication Systems*, Vol.11, No.11, pp.403-410, 2022.

강 명 조

https://orcid.org/0000-0002-0691-2970
e-mail : rkdaudwh13@hknu.ac.kr
2021년 한경국립대학교 컴퓨터응용수학부 (학사)
2022년 한경국립대학교 컴퓨터응용수학부 석사과정
관심분야 : 네트워크 보안, 블록체인, 머신러닝

김 미 희

https://orcid.org/0000-0002-4896-7400
e-mail : mhkim@hknu.ac.kr
1997년 이화여자대학교 전자계산학과(학사)
1999년 이화여자대학교 컴퓨터학과(석사)
1999년 ~ 2003년 한국전자통신연구원 연구원
2007년 이화여자대학교 컴퓨터학과(박사)
2007년 ~ 2009년 이화여자대학교 컴퓨터학과 전임강사
2009년 ~ 2010년 노스캐롤라이나주립대학교 연구원
2011년 ~ 현 재 한경국립대학교 컴퓨터응용수학부 교수
관심분야 : 네트워크 성능 분석 및 보안, 무선네트워크 보안, 침입대응, 크라우드센싱, 블록체인