Journal of KIIT. Vol. 23, No. 5, pp. 219-228, May 31, 2025. pISSN 1598-8619, eISSN 2093-7571
http://dx.doi.org/10.14801/jkiit.2025.23.5.219

단일 기관의 의존성을 배제하는 블록체인 기반 설문 조사 시스템 설계

황 교 찬*

Design of a Blockchain-based Survey System Eliminating Dependence on Specific Institutions

Kyo-Chan Hwang*

요 약

기존 설문 조사 시스템은 데이터 조작, 보안 취약성, 개인정보 유출 등의 문제가 제기되며, 단일 기관이 데이터를 관리할 경우 신뢰도가 저하된다. 이러한 문제를 해결하기 위해 블록체인 기술을 활용하여 투명성과 익명성을 보장하려는 시도가 있지만, 블록체인을 통해 데이터의 분산 관리가 가능하더라도, 관리 주체가 단일 기관에 집중되면 개인정보 유출 및 데이터 조작의 위험성을 완전히 배제하기 어렵다. 본 연구는 단일 기관의 종속성을 배제하기 위해 설문 조사 과정을 의뢰, 수행, 신원 인증으로 구분하고, 각 과정을 스마트 컨트랙트(Smart constract)로 설계하였다. 또한, 설문 의뢰 내용과 응답을 NFT로 만들어서 분리된 기관들이 블록체인 내에서 유기적으로 협력할 수 있도록 설계하였다. 이를 통해 단일 기관에 의존하지 않는 신뢰성 높은 설문 조사 방식을 구축하고, 조사 과정 전반의 투명성과 보안을 강화하는 설문 조사 모델을 제시한다.

Abstract

The existing survey system raises problems such as data manipulation, security vulnerability, and personal information leakage, and the reliability decreases when a single institution manages data. In order to solve this problem, there are attempts to ensure transparency and anonymity by utilizing blockchain technology, but even if distributed management of data is possible through blockchain, it is difficult to completely rule out the risk of personal information leakage and data manipulation if the management entity is concentrated in a single institution. In this study, in order to exclude the dependence of a single institution, the survey process was divided into commissioning, performing, and identity authentication, and each process was designed as a smart contract. In addition, by making survey request contents and responses into NFTs, it is designed so that separated institutions can cooperate organically within the blockchain. Through this, we propose a survey model that builds a reliable survey method that does not depend on a single institution and strengthens transparency and security throughout the survey process.

Keywords

blockchain, e-voting, survey, smart contract

* 성신여자대학교 융합보안공학과 겸임교수
- ORCID: https://orcid.org/0000-0002-6953-3169

· Received: Mar. 21, 2025, Revised: Apr. 13, 2025, Accepted: Apr. 16, 2025
· Corresponding Author: Kyo-Chan Hwang
Dept. of Convergence Security Engineering, Sungshin women's University, Korea
Tel.: +82-2-920-7114, Email: eekdro@gmail.com

Ⅰ. 서 론

현대 사회에서 설문 및 여론 조사 그리고 투표는 정책 결정, 시장 조사, 학술 연구 등 다양한 분야에서 핵심적인 구실을 하고 있다. 그러나 기존의 조사 시스템은 데이터 위·변조, 개인정보 유출, 중앙 집중식 관리로 인한 보안 문제 등 여러 한계를 갖고 있다[1]. 특히 설문 조사 기관이 설문 결과에 개입하여 조작할 수 있는 위험에 노출될 수 있다는 것은 신뢰성에 위협이 된다[2].

설문 조사에서 발생할 수 있는 문제들을 해결하기 위하여 투명성, 익명성을 보장하는 블록체인을 도입하기 위한 연구가 다양하게 이루어지고 있다. 블록체인을 활용한 설문 조사는 응답 데이터가 블록체인에 기록됨으로써 위·변조가 불가능하며, 모든 참여자가 결과를 검증할 수 있는 장점이 있다[3][4]. 설문 과정의 위조 및 변조 방지를 위해 중개자의 개입 없이 스마트 컨트랙트(Smart contract)를 활용하여 설문 응답의 기록 및 검증을 자동화할 수 있도록 설계하여 투명성을 높였다[5]. 투명성은 공공기관의 경우 그 중요성은 더욱 커진다. 국민연금의 가입자 의견 수렴과 공공 의사결정을 위해 블록체인 기술을 활용한 투표 시스템을 제안하는 연구도 이루어지고 있다[6]. 또한, 기존 설문 방식보다 처리 시간이 비약적으로 감소하기 때문에 비용 절감 효과도 예상된다[7].

인터넷이 보편화된 시대에서 개인정보 보호는 모든 분야에서 필요성과 중요성이 야기되고 있다. 인터넷 쇼핑의 증가로 운송장에 기재된 개인정보를 악용하는 범죄를 막기 위해 고객의 배송 정보 익명성을 보장하는 스마트 컨트랙트 기반의 배송 추적 방지 모델이 제안되고 있다[8]. 익명성은 설문 조사, 여론 조사, 투표 등 개인의 성향을 묻는 조사에서 특히 중요하다. 조사 대상의 성향이 특정되면 결과 조작과 유사한 효과가 발생할 수 있다. 따라서 블록체인의 투명성을 유지하면서도 익명성을 보장해야 한다[9]. 이러한 문제를 영지식(Zero-know ledge proof), 동형 암호화(Homomorphic encryption) 등의 암호 기술을 적용하여 더욱 높은 수준의 보안성을 강화하여 개인정보의 유출 방지에 대한 신뢰성을 확보하려는 연구가 진행되고 있다[10][11].

블록체인을 조사 시스템에 도입하면서 투명성과 보안이라는 두 가지 핵심 가치를 강화하려는 의미 있는 진전이었다. Follow My Vote, Agora, Voatz, Polyas, Luxoft, Polys 등 여러 기업들은 각기 다른 방식으로 블록체인을 활용해 투표 기록의 불변성과 유권자의 검증 가능성을 확보하고자 했다[12]. 그러나 이러한 기술적 진보에도 불구하고, 이 시스템들은 특정 기관이나 기업의 관리 하에 구축되고 운영되었다는 점에서 탈중앙화라는 블록체인의 본질적 가치에는 미치지 못했다. 이는 유권자가 시스템을 완전히 신뢰하려면 여전히 기관에 대한 신뢰가 전제되어야 한다. 서비스 전체를 단일 기관이 운영할 경우 설문 조작, 특정 성향의 응답자 편향, 개인정보 유출 등 블록체인 기록 전후 단계에서 데이터가 변조될 가능성을 완전히 배제하기 어렵다.

그림 1은 본 연구에서 제안한 설계 모델과 기존 블록체인 조사 서비스 모델을 비교한 이미지이다. 본 연구에서는 단일 기관에 의존하지 않으면서 익명성, 무결성, 투명성을 확보할 수 있는 블록체인 기반 설문 조사 시스템을 설계한다. 이를 위해 조사 과정을 의뢰, 수행, 신원인증으로 구분하고, 각 단계를 스마트 컨트랙트로 설계하였다.

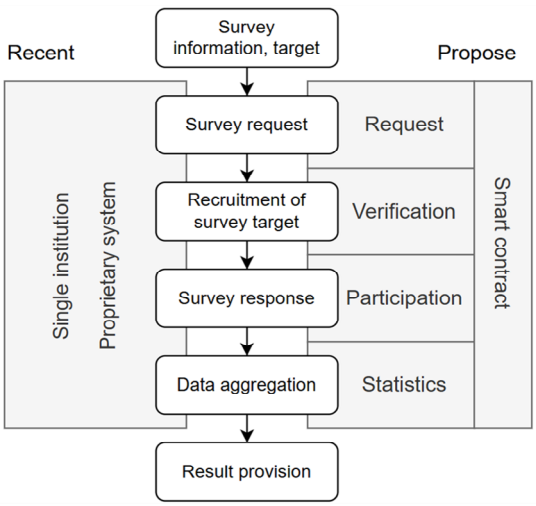

그림 1. 기존 블록체인 기반 조사 서비스와 제안 시스템의 설계 구성 비교

Fig. 1. Design structure comparison between the existing blockchain-based survey service and the proposed system

또한 설문 의뢰 내용과 답변을 NFT(Non-Fungible Token)로 만들어 분리된 기관들이 블록체인 안에서 유기적으로 동작할 수 있도록 설계하였다. 제안 방식은 설문 조사 전 과정을 블록체인에 기록하고, 분산된 기관이 독립적으로 각각의 서비스를 운영할 수 있는 구조를 제공하여 시스템의 신뢰도를 강화하는 시스템 설계 방안을 제안하였다.

II. 시스템 설계 요건

탈중앙화, 익명성, 무결성, 투명성이 보장된 실용적인 설문 조사 시스템의 구축을 위해, 본 연구에서는 다음과 같은 네 가지 핵심 설계 요구사항을 정의하였다.

2.1 단일 기관 의존성 제거

중앙 집중형 설문 조사 시스템은 특정 기관이 데이터를 관리하는 구조로 인해 데이터 조작 및 신뢰성 저하의 위험이 존재한다. 이에 따라 설문 조사 시스템은 단일 기관이나 플랫폼에 종속되지 않고 독립적인 여러 기관에서 함께 운영이 가능한 구조를 갖추어야 한다. 또한 블록체인의 투명성과 무결성을 기반으로 설문 전 과정의 데이터를 각 기관의 의존성 없이 접근이 가능하게 설계되어야 한다.

2.2 신원 인증 및 익명성 보장

중복 응답을 방지하고 데이터 무결성을 유지하기 위해서는 신원 인증이 필수적이지만, 개인정보 유출 위험이 있다. 이를 해결하기 위해 블록체인과 암호화 기술을 활용하여 개인정보를 익명화하고, 탈중앙화 식별자(DID, Decentralized Identifier)를 부여하는 방식을 적용한다. DID기반 인증을 통해 참여자의 익명성과 함께 신뢰성을 확보할 수 있으며, 설문 응답의 정직성을 보장할 수 있다. 또한, 개인정보를 직접 저장하지 않고도 성별, 지역, 연령대 등의 인구통계학적 정보만을 활용하여 요구 조건에 부합하는 참가자를 선별하도록 해야 한다.

2.3 설문 조사 과정의 투명성 보장

기존 설문 조사 과정은 투명성이 결여되어 있어 결과에 대한 신뢰가 부족하다. 이에 따라, 설문 시작부터 설문 참여까지 모든 상황은 블록체인에 기록되어야 하며, 실시간으로 설문 진행 상황을 누구나 확인할 수 있는 구조야 한다. 또한, 설문 조사 내용의 위·변조 여부를 검증할 수 있도록 스마트 컨트랙트를 설계하여, 데이터의 무결성을 보장하는 시스템을 설계해야 한다.

2.4 익명성과 무결성이 보장된 설문 수행 및 보상제공

설문 조사 시스템의 서비스 활성화를 위해서는 설문 참여자에 대한 보상 제도가 필요하다. 이를 위해, 설문의 응답이 제출됨과 동시에 보상 토큰(Token)을 자동으로 지급하는 구조로 설계하여 참여도를 높이는 방안에 대한 설계가 필요하다. 보상 지급 과정에서도 익명성을 보장해야 하며, DID를 적용하여 이중 지급을 방지할 수 있어야 한다.

III. 시스템 구성 요소 설계

3.1 단일 기관의 의존성 제거

단일 기관의 의존성 제거를 위해 Ethereum의 메인넷(Mainnet)을 기반으로 설계하였다. 메인넷에 스마트 컨트랙트를 발행하게 되면 스마트 컨트랙트의 코드는 특정 기업이 만들었다 할지라도 etherscan.io에 소스코드(Source code)를 등록하면 모든 사람이 해당 코드를 확인 할 수 있어 참여자의 신뢰도를 높일 수 있다.

그림 2는 Etherscan에서 스마트 컨트랙트의 소스코드를 볼 수 있는 것을 확인 할 수 있다[13]. 그림 2①은 발행된 스마트 컨트랙트의 주소를 나타내며 그림 2②는 해당 스마트 컨트랙트의 소스코드이다. 발행한 사람이 아니라도 스마트 컨트랙트의 공개된 함수를 직접 실행할 수 있다. 그림 2③처럼 스마트 컨트랙트의 함수 중 하나를 선택해서 인자를 넣고 그림 2④의 'Write' 버튼을 클릭하여 누구나 실행할 수 있다. 그림 2⑤는 스마트 컨트랙트로 구현되어 있는 함수 목록이다.

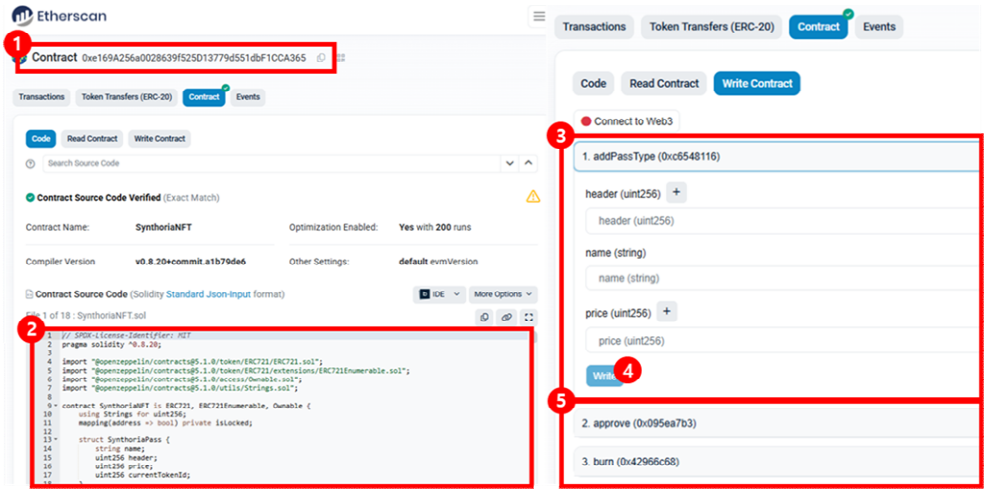

그림 2. Etherscan.io 에서 특정 스마트 컨트랙트의 소스코드 확인 및 함수 실행 웹 화면
Fig. 2. Web page for viewing the source code and executing functions of a specific smart contract on Etherscan.io

단, 'onlyOwner' 키워드를 포함한 함수는 스마트 컨트랙트를 발행한 사람만 호출할 수 있어서 정책적인 기능에 사용할 수 있다. 이처럼 스마트 컨트랙트를 발행하면 누구나 공개된 함수를 실행할 수 있다는 점을 이용하여 설문 의뢰와 수행 기관을 분리할 수 있다.

표 1에 기업이 독립적으로 서비스가 가능한 항목을 기술하였다. 신원 인증(User verification)을 담당하는 기관은 신원을 인증할 수 있는 국가 공인기관, 또는 그에 준하는 신원에 대한 인증이 가능해야 된다. 설문 요청(Survery request)을 담당하는 기관은 신문사, 정부, 기업의 마케팅 부서 등에서 요청한 설문을 블록체인에 기록하는 기관이다. 설문 수행(Survey participate)은 참여자의 설문 응답을 기록하는 역할을 한다. 마지막으로 설문 통계(Statistics)는 설문 상황을 모니터링하고 결과를 제공하는 역할을 한다.

표 1과 같이 분산된 기관별 역할을 스마트 컨트랙트로 구현하여 각자의 역할이 블록체인 안에서 유기적으로 정보를 관리할 수 있도록 설계했다.

설문조사 진행을 위해서는 설문의 내용(Survey information)을 스마트 컨트랙트로 의뢰하게 된다. 설문 수행은 웹(Web) 또는 앱(App)으로 설문 참여자를 모아서 진행한다. 해당 서비스에 설문 참여자가 가입하면 신원 인증을 통해 DID를 발급받고 참여할 수 있는설문을 스마트 컨트랙트에서 얻어오게 된다.

표 1. 독립적 서비스가 가능한 항목
Table 1. Items capable of independent service operation

Survey progress	Shared service agency
User verification	National public institutions capable of authenticating users for DID issuance
Survey request	Institutions that request survey responses
Survey participate	Institutions that collect survey participants and record responses to the survey request
Statistics	Institutions that monitor surveys and responses in real-time to create statistics

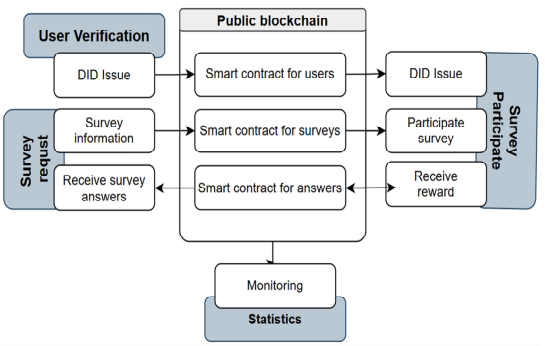

그림 3. 블록체인 스마트 컨트랙트를 기반으로 인증, 설문 의뢰, 수행, 통계 기관을 분리해서 운영할 수 있는 서비스 구성도
Fig. 3. Service architecture diagram for operating verification, survey requests, participation, and statistical institutions separately based on blockchain smart contracts

이후 설문 답변을 스마트 컨트랙트에 전송하면 자신의 블록체인 지갑으로 보상을 받을 수 있게 된다. 이러한 설문 전 과정을 스마트 컨트랙트를 통해 모니터링 할 수 있도록 설문 통계를 구축한다.

본 연구에서는 단일 기관의 의존성 제거를 위해 3개의 스마트 컨트랙트 사용하여 설문 시스템을 설계하고자 한다. 그림 4의 SCU(Smart contract for Users)는 인증기관에서 인증된 개인정보를 단방향 암호화하여 설문 참여자에게 DID 기반의 NFT를 발급하는 기능을 수행한다. SCU의 메타데이터(Metadata)는 3.2절에서 설명한다. SCS(Smart contract for Surveys)는 설문 조사 한 건당 하나의 NFT를 발행하며, NFT의 메타데이터에는 설문의 필수 내용과 참여 조건이 포함된다. SCS의 메타데이터는 3.3절에서 설명한다. SCA(Smart contract for Answers)는 각 설문 조사당 하나씩 발급되며, 설문 참여자가 답변을 제출하면 각각의 고유한 NFT가 발행되는 방식으로 운영된다. SCA의 메타데이터는 3.4절에서 설명한다.

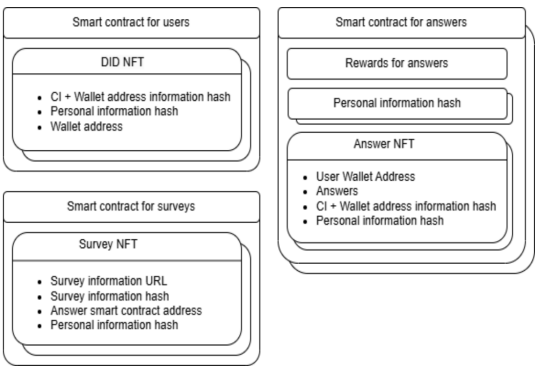

그림 4. 설문조사에 필요한 스마트 컨트랙트 구성
Fig. 4. Smart contract structure required for the survey

단일 기관의 의존성 제거를 위해 스마트 컨트랙트 자체를 업무 단위로 구분하였다. 이를 통해 각 기관에서 참조하거나 관리하는 스마트 컨트랙트를 분리할 수 있다. 이를 통해 Open API를 사용하듯이 설문 과정의 일부를 독자적으로 구축하여 서비스할 수 있다.

3.2 신원 인증 및 익명성 보장

정확한 신원 인증을 위해서는 국가 공인 기관의 인증이 필수적으로 필요하다. 현재 블록체인 거래소는 KYC(Know Your Customer)라는 고객확인제도를 통해 고객의 신원 확인을 의무화하고 있다.

표 2는 국내 블록체인 거래소인 업비트에서 KYC에 대한 요구사항을 기술한 것이다. 개인, 영리법인, 비영리법인, 외국인, 외국단체 등에 따라 신원 확인을 위해 요구하는 내용이 다를 수 있다.

표 2. 블록체인 거래소 업비트에서 KYC 과정에서 확인이 필요한 신원 확인 사항 (출처:업비트)
Table 2. Identity verification details required during the KYC process on the blockchain exchange Upbit

Category	Required Verification Information
Individual	Real name (name, resident registration number), address, contact information
For-profit Corporation	Real name of representative, business type, main office and business location, contact information
Non-profit Corporation & Others	Real name of representative, purpose of establishment, registered office address, contact information
Foreign Individual or Organization	Corresponding items based on the above categories, nationality, and local or office address in Korea

KYC 이후 내외부 시스템에서는 통상적으로 고유식별정보인 CI(Connecting Information)를 통해 신원을 인증하게 된다. 단, CI도 개인정보이기 때문에 본 연구에서는 지갑주소(Wallet address)와 CI를 합한 값을 단방향 암호화해서 개인을 특정할 수 없는 값을 사용하였다. 단방향 암호화를 통해 CI를 역산으로 구하는 것은 불가능하다.

설문을 위해서는 신원 확인뿐만 아니라 지역, 성별, 나이 등 통계를 내기 위한 개인정보(PI, Personal Information)가 필요하다. 그림 5와 같이 성별, 지역, 나이대를 포함한 문자열을 SHA-256으로 단방향 암호화한 결과로 나타낸다. 이렇게 만들어진 Hash 값은 대상을 선별하는 용도로 사용된다.

그림 6에 따라 UKey와 PIH를 메타데이터에 기록하여 NFT를 발행하게 되면 설문자의 신원 정보 없이도 인증된 신원을 갖고 있는 고유한 DID를 얻을 수 있다.

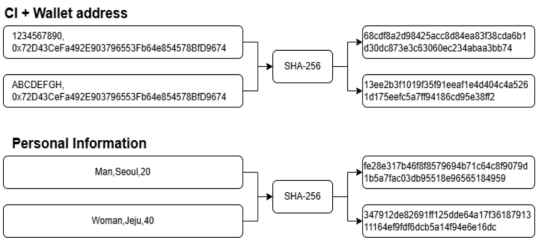

그림 5. 설문에 필요한 개인정보를 단방향 암호화한 결과
Fig. 5. Result of one-way encryption of personal information required for the survey

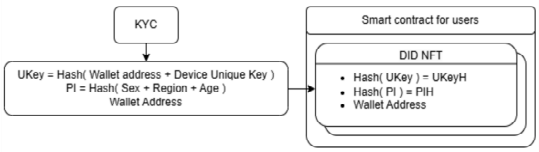

그림 6. 신원 인증 정보 보관 및 DID 발급 흐름도
Fig. 6. Identity verification information storage and DID issuance flowchart

또한 UKey와 PI를 스마트 컨트랙트에 넣기 전에 다시 Hash로 인코딩하여 발행된 NFT의 정보를 갖고 UKey나 PI를 역산할 수 없게 하였다. 스마트 컨트랙트 함수를 실행한 사람의 지갑주소를 알 수 있으므로 실행한 사람의 지갑주소에 DID NFT 보유 여부도 판단할 수 있다. DID NFT를 발급한 지갑주소도 함께 저장하여 지갑주소가 변경되었으면 재발급을 할 수 있게 하여 보안성을 높였다. 스마트 컨트랙트에는 개인정보를 암호화한 결과만을 갖고 있으므로 해당 정보를 통해 인물을 특정할 수 없는 익명성을 보장받게 된다.

사용자의 DID에 대한 신원 검증(Verification of identity)은 그림 7에서 제시한 방법으로 스마트 컨트랙트의 함수 호출을 시도할 수 있다.

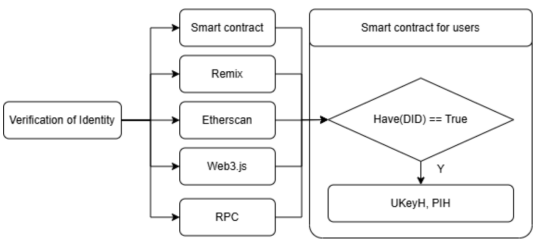

그림 7. 발급된 DID 검증 요청 흐름
Fig. 7. Verification request flow of the issued DID

신원 검증 요청을 하게 되면 스마트 컨트랙트를 실행한 대상자의 지갑주소에 DID NFT 보유를 확인하고 해당 DID NFT의 메타데이터에서 UKeyH와 PIH를 얻어 설문조사에 참여하게 된다.

인증된 신원의 인구통계학적인 정보를 UKeyH, PIH로 분리 후 NFT로 만들어 관리하여 익명성을 보장한 상태에서 설문 대상자를 선별할 수 있다.

3.3 설문 조사 과정의 투명성 보장

설문 과정의 투명성을 위해서는 설문지의 위조와 변조를 검증할 수 있는 구조를 스마트 컨트랙트로 구현해야 한다.

그림 8은 설문 NFT 발급을 위한 과정의 흐름을 나타내고 있다. 설문을 요청하는 기관은 HTML 형태로 설문 문항(Survery information web page)을 만들고 서버에 업로드해야 한다. 이를 통해 특정 URL에서 설문지를 확인할 수 있어야 한다. 설문을 의뢰할 때마다 SCS 안에 Survey NFT를 하나씩 민팅(Minting)한다. NFT의 메타데이터 안에 HTML 소스를 Hash로 변환해서 URL과 함께 보관한다. 이를 통해 등록 이후 설문이 위조 혹은 변조됐는지 Hash와 비교해서 확인할 수 있다. 설문 대상을 선정하여 PIH로 변환해서 메타데이터에 보관함으로써 차후 설문에 참여하고자 하는 사람의 PIH와 대조해서 참여 가능 여부를 판단할 수 있다.

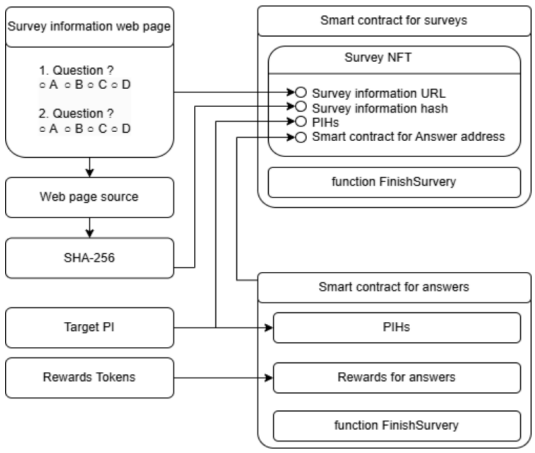

그림 8. 설문 NFT 발급을 위한 과정
Fig. 8. Process for issuing survey NFTs

대상자의 조건이 하나 이상일 경우가 존재할 수 있어 여러 개의 PIH를 보관하여 대조할 수 있게 하였다. 설문에 대한 답변을 보관하는 스마트 컨트랙트는 설문당 하나씩 발행하고 해당 스마트 컨트랙트의 주소를 설문 NFT의 메타데이터에 보관함으로써 결과에 대한 추적을 가능하게 하였다. 보상 토큰(Rewards token)은 차후 설문을 마친 사람에게 자동으로 일정량이 제공된다. 설문조사가 끝났다면 설문 종료 함수(Function FinishSurvery)를 실행하여 더 이상의 답변을 받지 않게 한다. 남은 보상 토큰은 설문 NFT 발행자에게 돌려주게 된다.

설문지의 위변조부터 답변하는 상황까지 전체과정을 블록체인에 기록함으로써 설문 조사 전 과정을 누구나 스마트 컨트랙트로 확인 할 수 있는 투명성을 보장했다. 이를 통해 전체 시스템의 신뢰를 높일 수 있다.

3.4 익명성과 무결성이 보장된 설문 수행 및 보상제공

설문 대상자의 익명성이 보장된 상태에서 이중 참여 방지를 위해 SCS와 SCA에서 SCU의 DID NFT를 검증하는 방식으로 스마트 컨트랙트간 유기적인 연결이 될 수 있게 설계해서 무결성을 보장한다.

그림 9는 설문에 참여하기 위한 전 과정의 흐름을 나타내고 있다. 사용자는 웹 또는 앱을 통해 설문 조사에 참여하게 된다. 설문에 참여하기 위해서는 최초에 한번 KYC를 진행해야 한다. 이 부분은 2.3절에 기술되어 있다. 웹 또는 앱에서 설문 요청 리스트를 요구(Request surveys)하면 SCU에서 사용자의 DID NFT의 메타데이터에서 PIH를 얻어온다. 설문 참여자는 스마트 컨트랙트에 의해 설문에서 요구하는 PIH와 일치하는 목록만 제공받게 된다. 이후 설문에 대한 응답 기록을 SCA에 하게 되면 PIH를 다시 얻어와서 해당 PIH와 같은지 확인한다. 이후 이중 참여 방지를 통한 무결성을 유지하기 위해 UKeyH가 해당 설문에 대해 답변했는지는 발급된 Answer NFT 목록을 확인하여 검사한다.

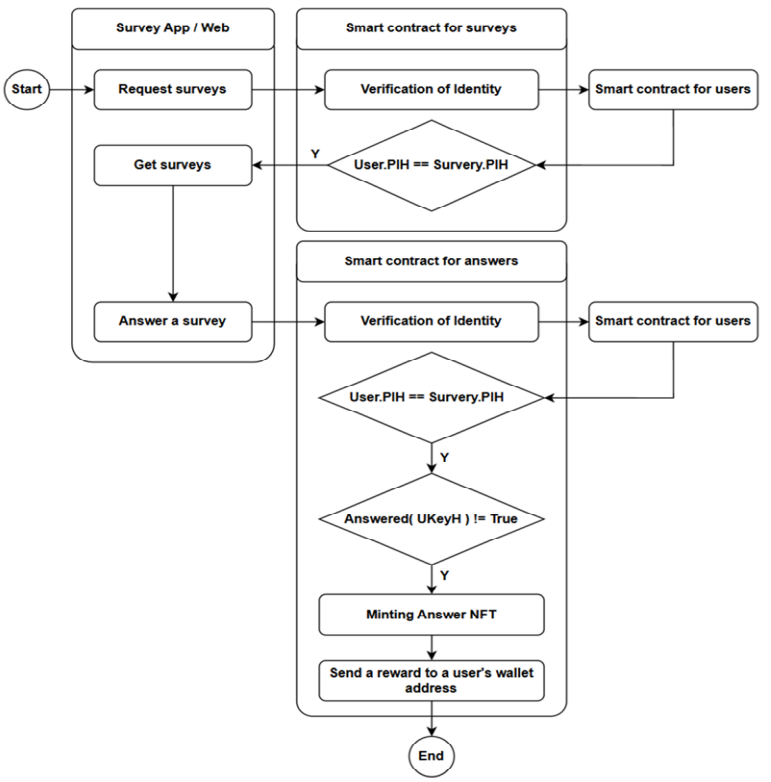

그림 9. 설문 참여 과정 흐름도
Fig. 9. Survey participation process flowchart

신규 답변이라면 Answer NFT를 발급하고 사용자의 지갑 주소로 사전 SCA에 저장해 둔 Token을 제공하게 된다.

위와 같은 설계를 기반으로 설문 조사 시스템을 구축한다면 익명성, 무결성, 투명성을 보장하면서도 단일 기관의 의존성이 제거된 서비스 구축이 가능하다.

Ⅳ. 구 현

연구 모델의 구현 및 모의 실험을 통해 설계의 적합성을 검증하였다. 블록체인에 등록한 스마트 컨트랙트는 그림 7에서 제시한 방법처럼 Web3.js(Ethereum Javascript API)등을 통해 스마트 컨트랙트의 함수를 실행할 수 있다.

그림 10①은 SCU에서 DID NFT를 발행하기 위해 정보를 입력하는 화면이다. 그림 10②는 DID NFT를 관리하는 스마트 컨트랙트가 블록체인에 등록된 화면이다[14]. 해당 링크를 웹브라우저를 통해 접속하면, 그림 2에서 언급했듯이 구현된 소스코드도 확인이 가능하다. 그림 10③는 DID NFT의 정보를 확인하는 SCU의 함수를 실행하여 블록체인에 기록된 DID NFT의 UKey와 PI정보를 보여주는 그림이다.

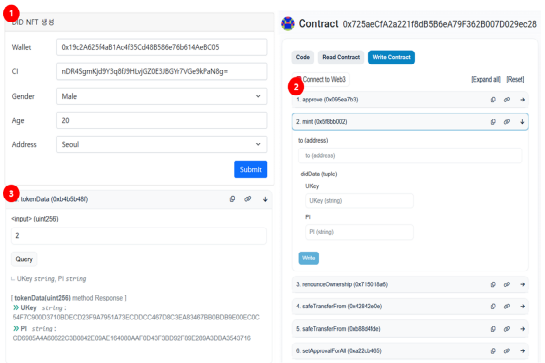

그림 10. SCU 구현 및 DID NFT 발급
Fig. 10. SCU development and DID NFT issuance

그림 11①은 SCS에서 Survey NFT를 발행하기 위해 정보를 입력하는 화면이다. 그림 11②는 Survey NFT를 관리하는 스마트 컨트랙트가 블록체인에 등록된 화면이다[15]. 그림 11③는 Survey NFT의 정보를 확인하는 SCS의 함수를 실행하여 블록체인에 기록된 Survey NFT의 정보를 확인하는 그림이다.

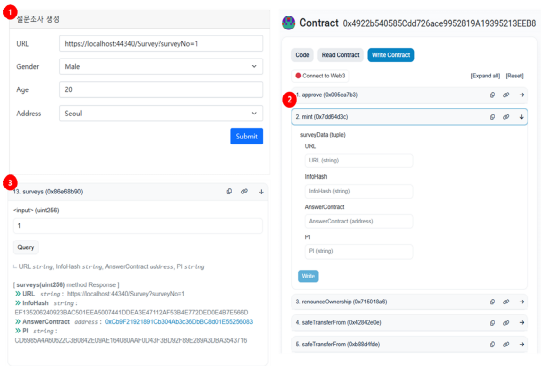

그림 11. SCS 구현 및 Survey NFT 발급
Fig. 11. SCS development and Survey NFT issuance

그림 12①은 SCA에서 참여자에게 제공되는 설문에 대한 답을 입력하는 화면이다. Submit 버튼을 누르면 Answer NFT가 발행된다. 그림 12②는 Answer NFT를 관리하는 스마트 컨트랙트가 블록체인에 등록된 화면이다.[16] 그림 12③는 Answer NFT의 정보를 확인하는 SCS의 함수를 실행하여 블록체인에 기록된 Answer NFT의 정보를 확인하는 그림이다. 그림 12①의 웹에서 입력한 답변이 블록체인에 기록된 것을 그림 12③에서 확인할 수 있다.

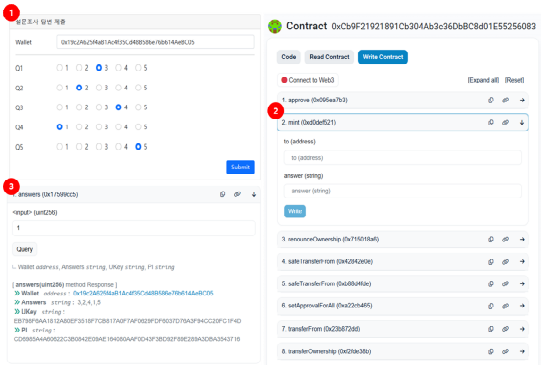

그림 12. SCA 구현 및 Answer NFT 발급
Fig. 12. SCA development and Answer NFT issuance

Ⅴ. 결 과

그림 13는 모의 설문을 진행한 결과를 스마트 컨트랙트에서 읽어와서 가시화 한 것이다.

Survey NFT의 URL을 통해 설문지의 내용을 얻어올 수 있다. URL에 있는 설문지의 소스코드는 Hash로 변환 후 Survey NFT에 기록되어 있다.

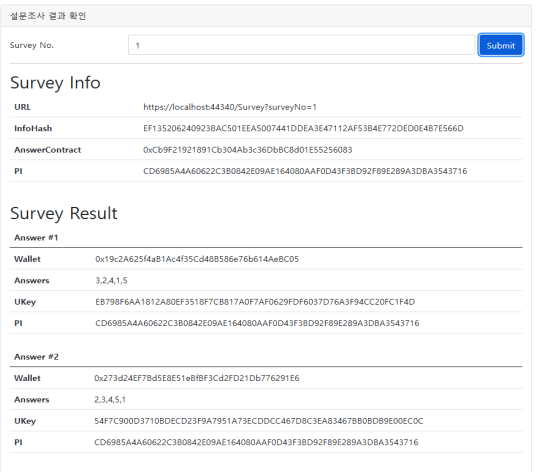

그림 12. 설문 결과
Fig. 12. Survey result

이를 활용하면 Survey NFT를 발행한 이후에 설문지에 대한 위변조가 있었는지 확인이 가능하다. Survey Result는 Survey NFT에 있는 SCU의 주소를 통해 발행된 Answer NFT의 목록을 읽어와서 출력한 것이다. Survey NFT에서 요구한 PI 값만 Answer NFT에 기록된 것을 확인할 수 있다.

설문조사 모델의 입증을 위한 모의 실험으로 표 1에서 제시한 것과 같이 스마트 컨트랙트를 통해 설문 단계를 분리하여 각 기관의 종속성 없이 서비스 구현이 가능함을 확인하였다.

Ⅵ. 결론 및 향후 과제

중앙 집중형 설문 조사 시스템의 한계를 극복하기 위해, 특정 기관에 의존하지 않으면서도 익명성, 무결성, 투명성을 보장하는 블록체인 기반 설문 조사 시스템을 설계하였다. 이를 위해 설문 조사 과정을 의뢰, 수행, 신원 인증의 세 단계로 분리하고, 각 단계를 스마트 컨트랙트로 구현하여 중개자의 개입 없이 유기적인 상호작용이 될 수 있도록 설계하여 시스템의 공정성을 확보하였다. 또한, 설문 의뢰 내용과 응답을 NFT로 만들어 데이터 무결성 및 익명성을 보장하였다.

제안한 모델은 기존 설문 조사 시스템의 단일 기관에 대한 의존성을 배제함으로써 신뢰성과 공정성을 강화하고, 조사 과정의 투명성을 높이는 새로운 패러다임을 제시하고자 한다.

향후 연구에서는 제안된 시스템에 대한 실증 연구로 실제 설문 조사 및 여론조사 환경에서의 적용 가능성을 평가해야 하며, 이를 통해 더욱더 효율적이고 신뢰성 높은 설문 조사 시스템으로 발전할 것으로 기대된다.

References

[1] U Jafar, M. J. A. Aziz, and Z Shukur, "Blockchain for electronic voting system—review and open research challenges", Sensors, Vol. 21, No. 17, pp. 5874, Aug. 2021. https://doi.org/10.3390/s21175874.

[2] E. Akbari, Q. Wu, W. Zhao, H. R. Arabnia, and M. Q. Yang, "From blockchain to internet-based voting", 2017 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA, pp. 218-221, Dec. 2017. https://doi.org/10.1109/CSCI.2017.34.

[3] A. Mukherjee, S. Majumdar, A. K. Kolya, and S. Nandi, "A privacy-preserving blockchain-based E-voting system", arXiv:2307.08412, Jul. 2023. https://doi.org/10.48550/arXiv.2307.08412.

[4] Puneet, A. Chaudhary, N. Chauhan, and A. Kumar, "Decentralized voting platform based on Ethereum blockchain", 2021 international conference on advances in electrical, computing, communication and sustainable technologies (ICAECT), Bhilai, India pp. 1-4, Feb. 2021. https://doi.org/10.1109/ICAECT49130.2021.9392580.

[5] J. Huang, D. He, Y. Chen, M. K. Khan, and M. Luo, "A blockchain-based self-tallying voting protocol with maximum voter privacy", IEEE Transactions on Network Science and Engineering, Vol. 9, No 5, pp. 3808-3820, Jul. 2022. http://doi.org/10.1109/TNSE.2022.3190909.

[6] H. Chung, "Blockchain E-voting System and Governance: The Case of Korean National Pension Service", Society for e-Business Studies, Vol 24,

No. 4, pp. 1-16, Oct. 2019. https://doi.org/10.7838/jsebs.2019.24.4.001.

[7] H. Kim, et al., "An Efficient and Transparent Blockchain-based Electronic Voting and Survey System", Journal of the Korea Society for Simulation, Vol. 30, No. 4, pp. 9-19, Dec. 2021. https://doi.org/10.9709/JKSS.2021.30.4.009.

[8] Y. Kim, Y. Kim, and K. Im, "Delivery tracing protect model based smart contract for guaranteed anonymity", Journal of Industrial Convergence Vol. 16, No. 1, pp. 15-20, Mar. 2018.

[9] R. H. Sahib and E. S. Al-Shamery, "A review on distributed blockchain technology for e-voting systems", Journal of Physics: Conference Series, International Conference of Modern Applications on Information and Communication Technology (ICMAICT), Babylon-Hilla City, Iraq, Vol. 1804, No. 1, pp. 012050, Oct. 2020. https://doi.org/10.1088/1742-6596/1804/1/012050.

[10] C. K. Adiputra, R. Hjort, and H. Sato, "A proposal of blockchain-based electronic voting system", 2018 second world conference on smart trends in systems, security and sustainability (WorldS4), London, UK, pp. 22-27, Oct. 2018. https://doi.org/10.1109/WorldS4.2018.8611593.

[11] M. N. Probor, M. Ahmed, S. B. Kabir, Md. M Fuad, and T. Bushra, "Blockchain based e-voting system with homomorphic encryption and threshold signature", Diss. Brac University, May 2023.

[12] Y. Abuidris, R. Kumar, and W. Wenyong, "A Survey of Blockchain Based on E-voting Systems", Series ACM Other Conferences, pp. 99-104, Xi'an, China, Dec. 2019. https://doi.org/10.1145/3376044.3376060.

[13] Smart contract, https://sepolia.etherscan.io/address/0xe169a256a0028639f525d13779d551dbf1cca365#code [accessed: Mar. 20, 2025]

[14] Smart contract for Users, https://testnet.bscscan.com/address/0x725aeCfA2a221f8dB5B6eA79F362B007D029ec28. [accessed: Apr. 30, 2025]

[15] Smart contract for Surveys, https://testnet.bscscan.com/address/0x4922b540585Cdd726ace9952819A19395213EEB8. [accessed: Apr. 30, 2025]

[16] Smart contract for Answers, https://testnet.bscscan.com/address/0xCb9F21921891Cb304Ab3c36DbBC8d01E55256083. [accessed: Apr. 30, 2025]

저자소개

황 교 찬 (Kyo-Chan Hwang)

2023년 2월 : 상명대학교 스포츠ICT융합(공학박사)
2022년 2월 ~ 현재 : ㈜워크스타일 대표이사
2023년 9월 ~ 현재 : 성신여자대학교 융합보안공학과 겸임교수

관심분야 : 블록체인, eSports, 게임