

**1인 1표 가중치 전자투표 SDK 개발**

* **SDK를 활용한 예시 dApp**

|  |  |  |
| --- | --- | --- |
| 과목명 | Ethereum Dapp 개발과 성능 시험 | |
| 담 당 | 이 춘 화 교수님 | |
| 제출일 | 2023년 10월 20일 | |
| 공과대학 | 컴퓨터소〮프트웨어학부 | |
| 4 학년 | 2015000346 | 2020019152 |
| 이 름 | 우수몽 | 정지나 |

****

**개요**

전통적인 투표 시스템에서는 투표자들의 의사를 동등하게 취급하는 것이 일반적입니다. 그러나 어떤 문제의 경우 특정 의견이나 주제를 다른 것보다 더 중요하게 여기는 가중치 투표가 필요할 수 있습니다. 이에 따라 1인 1표 무기명 투표 SDK를 활용하여 가중치 투표 시스템을 개발하고자 하는 것이 본 연구의 주요 동기입니다.

연구의 주요 목표는 다양한 의견이나 주제에 대해 공정한 가중치를 부여하여 더 중요한 투표를 가능하게 하는 가중치 투표 시스템을 구축하는 것입니다. 이를 통해 다양한 시민들의 의견이 공정하게 반영될 수 있는 투표 시스템의 필요성을 강조하고자 합니다. 이러한 목표는 민주주의의 핵심 원리에 부합하는 효과적인 의사결정 방식을 개발하는 데 있어서 중요한 의의를 가지고 있습니다.

1인 1표 무기명 투표 SDK를 활용하여 가중치 투표를 지원하는 블록체인 기반의 dApp을 개발할 계획입니다. 이를 통해 투표자들은 각 투표 항목에 대해 부여하는 상대적인 가중치를 관리할 수 있으며, 이러한 가중치가 투표 결과에 어떻게 반영되는지에 대한 연구를 수행할 예정입니다. 이러한 방법론의 채택은 다양한 의견과 이해관계자들 간에 공정한 의사소통을 촉진하며, 의사결정의 투명성과 정확성을 강화하는 데 일조할 것으로 기대됩니다.

이 연구를 통해 다양한 의견이나 주제에 대한 공정한 가중치 부여가 가능해지면서, 투표 결과의 다양성과 정확성을 보다 향상시킬 수 있을 것으로 기대됩니다. 이는 사회적 참여의 다양성을 존중하고, 민주주의 프로세스를 보다 포괄적이고 효과적으로 이끌어 나갈 수 있는 중요한 기반을 마련할 것입니다.

본 연구는 가중치 투표 시스템의 보안과 공정성을 중점적으로 다루고자 합니다. 그러나 개인 정보 보호와 투표 결과의 신뢰성에 대한 일부 한계를 인식하고 있으며, 이러한 한계를 극복하기 위한 보완 방안을 적극적으로 모색할 것입니다. 이를 통해 안전하고 투명한 가중치 투표 시스템의 개발에 기여할 수 있을 것입니다.

**목차**

**논문 개요**

**제1 장 서론**

1. **연구배경 및 목적**

**제2 장 관련 연구**

1. **전자투표(E-voting)**
2. **블록체인**
3. **동형암호화**
4. **영지식증명**
5. **Oracle - chainlink**

**제3 장 선행 연구 및 요구 사항 분석**

1. **선행연구**
2. **요구사항 분석**

**제4 장 시스템 설계 및 구현**

1. **시스템 설계**
2. **시스템 구현**

**제5 장 결론 및 제언**

**참고문헌**

**제1 장 서론**

**1. 연구배경 및 목적**

최근의 글로벌 상황 변화와 함께, 코로나-19 팬데믹은 전 세계적으로 대면 투표 시스템에 막대한 영향을 미쳤습니다. 이로 인해 투표 접근성과 안전성에 대한 우려가 더욱 부각되었습니다. 특히 대규모 유권자들이 모여 투표하는 것이 어려운 상황에서, 안전한 대안이 되는 전자 투표 시스템의 필요성은 더욱 중요해졌습니다.

한편, 기존의 전자 투표 시스템은 보안 취약성과 조작 가능성으로 인해 많은 논란을 빚고 있습니다. 특히 인터넷 망을 통해 관리되는 기존 시스템은 외부 공격에 취약하고, 투표 과정에 조작이 가능한 위험이 따르는 것으로 알려져 있습니다. 이에 따라 기존의 투표 시스템은 투표의 공정성과 안전성을 동시에 보장하기 어려운 문제를 안고 있습니다.

본 연구는 이러한 문제를 해결하기 위해 블록체인 기술의 특성을 활용하여 전자 투표 시스템을 개발하고자 합니다. 블록체인의 불변성과 투명성은 투표 과정의 신뢰성을 보장하는 데 있어서 중요한 장점으로 작용할 것으로 기대됩니다. 또한, 이더리움 기반의 블록체인을 활용하여 solidity 언어를 이용한 smart contract 코딩을 가능하게 하는 SDK의 개발은 전자 투표 시스템을 보다 접근하기 쉽고 안전하게 할 수 있는 획기적인 방안입니다.

이에 따라 본 연구의 목적은 블록체인 기술을 활용하여 전자 투표 시스템을 개선하고, 보다 투명하고 안전한 투표 환경을 조성하는 것입니다. 또한, SDK의 개발을 통해 일반 개발자들도 쉽게 전자 투표 시스템을 구현할 수 있도록 지원함으로써, 전자 투표 시스템의 보급과 발전에 기여할 것으로 기대합니다. 이를 통해 민주주의 원칙을 보다 강화하고, 투표 과정의 신뢰성을 증진할 수 있는 전자 투표 시스템을 설계하고자 합니다.

전자투표는 선거 과정을 전자화 하여 투표의 편리성을 높이고, 대면 투표의 어려움을 극복하는 시스템입니다. 이러한 시스템은 일반적으로 물리적 투표소에 방문하지 않고도 투표를 진행할 수 있으며, 이는 유권자들에게 편의성을 제공하여 참여율을 높일 수 있는 장점이 있습니다. 이러한 유용성에도 불구하고, 기존의 전자 투표 시스템은 여전히 안전성과 신뢰성에 관한 문제를 안고 있습니다. 이러한 문제점을 극복하기 위해 블록체인 기술의 도입이 필요하다고 볼 수 있습니다.

**제2 장 관련 연구**

**1. 전자투표(E-voting)**

선거는 민주주의의 근본으로, 국가 및 사회의 방향을 결정하는 중요한 과정입니다. 그러나 종이 투표 시스템은 왜곡 및 조작 가능성으로 인해 신뢰할 수 없는 측면이 있었습니다. 2004년 우크라이나 대통령 선거 및 2019년 볼리비아 대통령 선거 부정 의혹과 같은 사례가 종이 투표의 취약점을 드러내었습니다. 이러한 문제점을 해결하기 위해 전자 투표 시스템이 주목받고 있습니다.

전자 투표 시스템은 다양한 형태로 구현될 수 있습니다. PSEV(Poll Site E-Voting)은 전자 투표 기기를 사용하여 투표소와 개표소를 공공망으로 연결하는 방식으로, 외부 침입의 가능성은 있으나 공공망이라는 특성으로 인해 통제가 가능합니다. 키오스크 방식은 학교나 공공장소 등에 설치되는 전자 투표기기를 통해 투표를 진행하는 방식으로, 관리자가 없는 환경에서 전자적 인증장치를 사용하여 투표가 이루어집니다. REV(Remote Electronic Voting)은 모바일 기기나 PC를 사용하여 투표를 하는 방식으로, 기술적 위험이 높고 선거 관리자의 개입이 없는 자유로운 투표가 가능하지만 비밀 투표의 침해 가능성이 존재합니다.

전자 투표의 발전은 효율성과 신뢰성을 증가시키는 데 도움이 되었습니다. 이러한 시스템은 전 세계적으로 정부 및 국제 기구에서 적극적으로 채택되고 있으며, 기존의 문제점을 극복하기 위해 계속해서 발전하고 있습니다. 전자 투표 시스템은 민주주의를 강화하고, 투표 과정의 투명성과 신뢰성을 보장하는 데에 큰 기여를 하고 있습니다.

**2. 블록체인**

블록체인은 해싱과 암호화 기술을 통해 정보를 블록 단위로 저장하고, 이를 체인 형태로 연결하는 분산 원장 기술입니다. 이 기술은 블록들이 시간순서대로 유지되며, 각 블록은 자신의 이전 블록을 해시 함수를 이용하여 참조합니다. 이러한 특성으로 인해 블록체인은 데이터의 무결성과 보안을 보장하며, 중앙 관리자 없이도 신뢰할 수 있는 거래와 데이터 교환을 가능하게 합니다. 이러한 특징으로 블록체인은 다양한 분야에서 중요한 역할을 수행하고 있습니다.

블록체인은 불변성과 투명성이라는 특성을 갖습니다. 기록된 정보는 변경이 불가능하며, 정해진 규칙에 의해 상태가 변경됩니다. 또한 기록의 내역이 블록에 공개되어 있어 누구나 정보의 진실여부를 확인할 수 있습니다. 이러한 특성 덕분에 블록체인은 신뢰에 큰 비용이 들지 않아도 정보의 진실성을 보장할 수 있습니다.

따라서 블록체인 기술을 활용하면, 기존에는 신뢰 문제로 인해 어려웠던 여러 서비스들을 구현할 수 있게 됩니다. 이러한 잠재력을 활용하면 혁신적인 서비스의 제공이 가능해질 것입니다.

스마트 컨트랙트는 특정 주소에 배포된 트랜잭션으로 실행 가능한 코드입니다. 이 코드는 함수와 상태로 구성되어 있으며, 이들은 블록체인에 영구적으로 저장됩니다. 함수는 상태를 변경하는 함수와 상태를 변경하지 않는 함수로 분류됩니다. 사용자가 스마트 컨트랙트 함수를 실행하거나 상태를 읽을 때는 해당 스마트 컨트랙트의 주소가 필요합니다. 스마트 컨트랙트는 트랜잭션을 통해 실행되며, 해당 트랜잭션의 결과는 스마트 컨트랙트에 반영됩니다. 이를 통해 블록체인 환경에서 분산 애플리케이션을 실행하고 관리할 수 있습니다.

Solidity는 이더리움과 클레이튼 등에서 사용되는 스마트 컨트랙트 언어입니다. 일반적인 프로그래밍 언어와 유사한 문법을 가지고 있지만 몇 가지 제약이 있습니다. 예를 들어, 포인터 개념이 없어서 재귀적인 타입 선언이 불가능하며, 대신 블록체인의 주소 개념이 사용됩니다. Solidity는 분산 애플리케이션(DApp) 및 스마트 컨트랙트를 개발하는 데 사용되며, 이를 통해 보안 및 투명성을 보장하는 탈중앙화된 애플리케이션을 구축할 수 있습니다.

**3. 동형암호화**

동형 암호화는 암호화된 데이터를 해독하지 않고 처리하는 기술로, 블록체인 분야에서는 주로 개인 정보 보호를 위해 활용됩니다. 특정 사용자만이 거래 데이터와 계약 상태를 볼 수 있는 스마트 컨트랙트를 만드는 데 사용됩니다. 이를 통해 블록체인 상에서 개인 정보 보호를 구현할 수 있습니다. 암호화된 트랜잭션 데이터와 상태값은 해독할 수 없으므로 외부의 민감한 정보가 노출되지 않습니다.

최근 기술 발전으로 인해 동형 암호화의 실용성이 향상되었습니다. 이러한 기술은 블록체인 분야에서 다양한 방식으로 활용됩니다. 신뢰할 수 없는 bridge 구현, 블라인드 경매, 비밀 투표 등 다양한 응용이 가능합니다.

기술적 과제와 해결책

권한 설정: 중앙 집중식 암호 해독 키 없이 선택적으로 상태를 해독하는 방법으로, Threshold FHE로 private key를 보호합니다. 그러나 이 방법은 고정된 수의 검증자가 있어야 한다는 제약이 있습니다.

결합성: 사생활을 침해하지 않고 스마트 컨트랙트를 구성하는 방법으로, 입력값에 대한 영지식 증명을 활용할 수 있습니다.

성능: 블록 크기를 작게 유지하면서 처리량을 늘리는 방법으로 Tranciphering, FHE-rollups, FHE 하드웨어 가속기 등의 기술을 활용합니다.

**4. 영지식증명**

영지식증명(Zero-Knowledge Proof)은 암호학과 컴퓨터 과학 분야에서 중요한 개념으로, 증명자가 어떤 명제가 참임을 증명할 수 있는 동시에 그 명제가 참이라는 사실 외에는 어떠한 추가 정보도 제공하지 않는 방법을 말합니다. 이러한 방식은 증명의 유효성을 검증할 수 있는 존재성 증명을 수행하면서도 프라이버시와 보안을 보장하는 중요한 수단이 됩니다.

영지식증명은 보안 프로토콜에서 중요한 역할을 하며, 완전성(Completeness), 건실성(Soundness), 그리고 영지식성(Zero-Knowledge)이라는 세 가지 중요한 특성을 가지고 있습니다. 완전성은 유효한 증명이 항상 검증자를 납득시키는 성질을 나타내며, 건실성은 거짓인 명제에 대해서는 거의 항상 정직한 증명자가 검증자를 납득시키지 않는 성질을 나타냅니다. 마지막으로 영지식성은 올바른 증명이라도 제3자가 증명과정을 통해 얻을 수 있는 정보가 없음을 의미합니다.

이러한 영지식증명은 블록체인 기술과 밀접한 연관이 있으며, 분산 원장 기술의 신뢰성과 프라이버시 보호를 강화하는 데에 활용됩니다. 블록체인에서 영지식증명은 트랜잭션의 유효성을 증명함으로써 개인정보 유출 등의 문제를 방지하고, 투명성을 유지하면서도 정보의 보안을 보장하는 역할을 합니다.

또한 영지식증명은 다양한 분야에 활용되고 있으며, 블록체인 외에도 보안 프로토콜, 암호화 통신, 인증 시스템 등 다양한 분야에서 활발하게 연구되고 적용되고 있습니다. 그 결과로 영지식증명은 정보 보안 및 프라이버시 보호를 위한 중요한 도구로 각광받고 있습니다.

영지식증명(Zero-Knowledge Proof)은 임의의 관계 R(Relation)에 대한 입력(instance)와 비밀정보(witness)가 해당 입력이 관계에 속하는 비밀정보를 가진다는 명제를 만족하는 상황에서, 증명자와 검증자 사이에서 세 가지 중요한 특성을 갖춰야 합니다.

첫째, 완전성(Completeness)은 유효한 입력과 비밀정보를 가진 정직한 증명자가 항상 검증자를 납득시킨다는 성질을 의미합니다. 둘째, 건실성(Soundness)은 어떤 명제가 거짓이라면 정직한 검증자를 납득시킬 확률이 거의 없음을 나타냅니다. 마지막으로 영지식성(Zero-Knowledge)은 올바른 증명에도 불구하고 검증자가 추가 정보를 얻지 못함을 의미합니다.

또한, 영지식증명은 증명의 크기가 관계의 복잡도와 무관하게 상수로 고정되거나 선형 이하의 크기를 가지며, 이로 인해 검증자가 증명을 빠르게 검증할 수 있는 장점을 갖고 있습니다. 이는 증명 검증에 필요한 시간이 실제 수행에 비해 효율적이기 때문에 검증자의 계산량이 감소한다는 의미를 포함합니다.

**5. Oracle - chainlink**

스마트 컨트랙트는 외부에서 발생하는 정보를 지속적으로 관찰하거나 어떤 사건이 발생했을 때 스스로 결과값을 입력할 수 없는 제약이 있습니다. 이러한 제약으로 인해 외부 정보에 기반한 판단이나 결정을 내리는 데 제한이 있습니다. 스마트 컨트랙트가 외부 환경과 상호작용하기 위해서는 외부에서 발생한 사건을 관찰하고, 이를 스마트 컨트랙트의 입력값으로 전달해주는 주체가 필요한데, 이를 위한 주체가 오라클(Oracle)입니다. 이로써 스마트 컨트랙트는 외부 환경과의 연결성을 확보하며 보다 다양한 상황에서의 응용이 가능해집니다.

Chainlink는 블록체인과 외부 데이터 소스 간의 상호 연결성을 제공하는 오픈 소스 플랫폼으로, 신뢰할 수 있는 외부 데이터 및 API로 상호 작용할 수 있는 분산형 Oracle 네트워크를 구축하고 운영합니다. 이를 통해 스마트 컨트랙트가 외부 실제 데이터를 활용하여 의사 결정을 내릴 수 있습니다. Chainlink는 안전성, 확장성, 그리고 신뢰성을 보장하며 다양한 블록체인 플랫폼과 호환되어 전 세계의 데이터 및 서비스 제공 업체가 블록체인 생태계에 참여할 수 있도록 촉진합니다. 이러한 특징으로 인해 Chainlink는 블록체인 기반 애플리케이션과 서비스가 외부 신뢰할 수 있는 데이터를 활용할 수 있도록 지원합니다.

Chainlink의 종류

Pre-Built Chainlink Oracles: 사전에 구축된 Chainlink Oracles는 기존에 사용되었던 데이터 소스 및 API에 대한 연결을 제공합니다. 주가, 날씨, 이벤트 데이터 등 다양한 외부 데이터를 제공할 수 있습니다.

Decentralized Chainlink Oracles: 분산형 Chainlink Oracles는 여러 참여자가 집합적으로 데이터를 제공하고 검증하는 방식으로 작동합니다. 이는 데이터의 신뢰성과 보안성을 높이는 데 도움이 됩니다.

Custom Chainlink Oracles: 사용자 정의 Chainlink Oracles는 특정한 사용자 요구에 맞춰 개발된 오라클로, 사용자가 자체적으로 데이터 소스를 설정하고 조작할 수 있습니다.

External Adapters: External Adapters는 Chainlink에서 외부 시스템과 상호 작용하기 위해 사용되는 플러그인 모듈입니다. 다양한 데이터 소스와 상호 작용하여 스마트 컨트랙트에 데이터를 제공하는 데 활용됩니다.

이러한 다양한 종류의 Chainlink는 스마트 컨트랙트가 다양한 환경에서 외부 데이터를 활용하여 보다 유연하고 효과적으로 동작할 수 있도록 지원합니다.

**제3 장 선행 연구 및 요구 사항 분석**

**1. 선행연구**

**- [Blockchain for Electronic Voting System—Review and Open Research Challenges - Uzma Jafar (31 August 2021)]**

블록체인을 활용한 투표 시스템은 현실적인 도전과제를 안고 있다. 이러한 도전 과제들은 투표 과정의 공정성, 익명성, 그리고 유효성에 관한 문제를 다루고 있다. 먼저, 자격 증명 문제는 기존의 식별 시스템을 활용하는 것이 일반적인 접근 방법이며, 별도의 자격 증명 시스템 구축은 복잡성을 증가시킬 수 있다.

재투표 방지와 유권자 익명성의 상충 관계는 블록체인 기반 투표 시스템에서 흔히 발생하는 문제 중 하나이다. 이를 해결하기 위해서는 절충안을 도입하여 특정 측면을 어느 정도 포기할 필요가 있다. 투표자의 개인 정보 보호 문제는 블라인드 서명, 동형 암호화, 그리고 혼합 네트워크와 같은 암호 기술들을 활용하여 처리된다.

공정성은 중간 결과를 얻는 사람이 없어야 하며, 투표 결과의 집계는 투표가 완전히 마무리된 후에 이루어져야 한다. 이를 위해 신뢰할 수 있는 딜러가 생성된 키를 분할하여 여러 키 소유자에게 배포하는 비밀 공유 방법이 사용될 수 있다. 또한, 제로 지식 증명을 활용하여 투표의 유효성을 보장하고, 투표 과정의 건전성과 완전성을 유지할 수 있다.

최적의 해결책을 찾는 것은 여전히 과제가 되고 있으며, 각 문제는 단일적인 해결책이 아닌 다양한 기술과의 절충으로 해결될 수 있는 것으로 보인다. 현재까지는 완벽하게 이러한 문제들을 해결하는 투표 시스템은 존재하지 않으며, 현실적인 제약 조건과의 균형을 맞추는 것이 중요하다.

- **[영지식 증명 이해와 블록체인 활용 - 대한전자공학회 2022.12 한양대]**

블록체인과 영지식 증명은 현대 사회에서 핵심적인 보안 및 개인정보 보호 문제를 해결하기 위한 중요한 기술로 인정받고 있다. 이 두 기술은 각자의 독특한 기능을 제공하며, 상호 보완적으로 작용함으로써 혁신적인 보안 솔루션을 제공할 수 있다. 영지식 증명은 완전성, 건실성, 그리고 영지식성이라는 핵심적인 특성을 가지며, 이를 통해 효과적인 보안을 제공할 수 있다. 그러나 특정 영지식 증명 기법은 신뢰 기관의 의존성이나 큰 증명 크기 등의 제약 사항을 갖고 있어, 보다 효율적인 구현을 위해 다양한 기술적 접근 방법이 연구되고 있다.

논문은 다양한 영지식 증명 기법에 대한 조사 결과를 제시하고 있다. QAP(Quadratic Arithmetic Program) 기반 영지식 증명은 SRS(Structured Reference String) 생성 과정에서의 위조 가능성 등의 단점을 갖고 있으며, 이를 극복하기 위해 유니버셜 영지식 증명과 신뢰 가정이 없는 영지식 증명 등이 제시되고 있다. 특히, 신뢰 가정이 없는 영지식 증명은 Bulletproofs나 GKR15와 같은 기법을 활용하여 보다 빠른 증명 및 검증 시간을 제공한다.

이러한 영지식 증명 기법은 블록체인 기술과의 결합을 통해 다양한 분야에서 유용하게 활용될 수 있다. 예를 들어, Zcash는 영지식 증명을 사용하여 프라이버시 보호 기능을 제공하고 있으며, 이러한 기술의 활용은 이더리움과 같은 다른 블록체인 플랫폼에서도 적용 가능하다. 또한, 영지식 증명은 확장성 문제를 해결하기 위한 방안으로도 활용될 수 있다. 블록체인의 확장성 문제는 블록체인의 처리량을 증가시키기 위한 다양한 기술적 접근 방법을 제시하고 있으며, 이러한 확장성 문제를 해결함에 있어서 영지식 증명은 중요한 역할을 수행할 수 있다.

이러한 내용을 통해 논문은 영지식 증명 기법과 블록체인 기술의 융합이 현대 사회에서의 보안 및 프라이버시 보호 문제를 해결하는 데에 어떤 역할을 할 수 있는지에 대해 탐구하고 있다. 해당 논문은 이러한 중요한 주제를 더 깊이 있게 탐구함으로써 학계와 산업계에서의 영지식 증명과 블록체인 기술의 활용에 대한 이해를 촉진하고 있다.

**- [프라이빗 블록체인 기반 전자투표 시스템 설계 및 구현 - 서강대 김권섭]**

"프라이빗 블록체인 기반 전자투표 시스템 설계 및 구현" 논문은 민주주의의 핵심인 선거 시스템을 전자화하는 데에 대한 필요성과 함께, 이러한 과정에서 발생하는 보안 및 무결성 문제를 해결하기 위한 방안을 다루고 있습니다. 이러한 논문은 기존 전자 투표 시스템에서 발생하는 다양한 문제점을 블록체인 기술을 활용하여 극복하는 방식에 초점을 맞추고 있습니다. 특히, 이 논문은 프라이빗 블록체인을 사용하여 투표의 합법성과 비밀성을 보장하는 설계를 제안하고 있습니다.

이 논문은 선행 연구와 배경지식을 토대로 전자 투표 시스템의 주요 유형과 관련 기술적 배경에 대해 깊이 있게 논의하고 있습니다. 전자 투표 시스템의 유형에 대한 설명과 함께, 공개키 암호화 및 RSA 암호화와 같은 암호화 기법에 대한 이해를 바탕으로 블록체인을 이용한 안전한 투표 시스템을 구축하는 방법을 상세히 설명하고 있습니다.

또한, 이 논문은 전자투표 시스템의 구현 과정을 자세히 설명하고 있습니다. 논문은 프라이빗 블록체인 기술을 적용하여 투표의 무결성을 보장하는 방안을 제시하고 있으며, 구현 과정에서 이더리움 네트워크 및 JAVA의 RSA 암호화 라이브러리를 활용하는 등 다양한 기술적인 측면을 다루고 있습니다.

이러한 연구 결과는 전자 투표 시스템의 보안성을 향상시키는 실용적인 접근 방법을 제시하고 있습니다. 이 논문은 민주주의를 위협하는 문제를 해결하기 위한 구체적이고 현실적인 방법을 제시하고 있어, 전 세계적으로 전자 투표 시스템을 보다 안전하고 신뢰할 수 있는 방식으로 발전시키는 데에 기여할 것으로 기대됩니다.

**2. 요구 사항 분석**

**확보하고자 하는 것**

1. 신뢰성

* 올바른 유저가 표를 받아야 함(부정선거 및 표 탈취가 불가능함)
* 투표 결과가 조작되지 않아야 함
* 선거기관으로부터 인증을 받은 투표권은 제 3자에 의해 위조가 불가능해야 한다.

1. 익명성

* 누가 누구에게 투표했는지 몰라야 함
* 투표가 마감되기 전까지 투표의 진행 과정 및 현재 투표 결과를 알 수 없어야 함

**요구사항**

* 정확성(Accuracy)  
  시스템이 투표용지를 수정, 삭제할 수 없고, 유효한 투표용지가 투표 기록에올바로 집계되며, 유효하지 않는 투표용지가 투표 기록에 집계되지 않아야 한다, 즉 집계결과가 정확해야 한다.
* 비밀성(Privacy)  
  시스템이 투표권을 행사하는 투표자에게 연결되어있지 않고, 어떠한 방법으로도 투표자가 누구에게 투표를 했는지를 증명할 수 없어야 한다. 또한 투표자와 투표자 자신이 투표한 내용은 해당 투표자만이 알 수 있어야 한다.
* 위조 불가능성(Unforgeability)  
  선거기관으로부터 인증을 받은 투표권은 제3 자에 의해 위조가 불가능해야 한다.
* 단일성(Singularity)  
  합법적인 투표자는 단지 한 번의 투표권만 행사 할 수 있어야 한다.
* 합법성(Eligibility)　  
  합법적인 절차를 통하여 투표권을 얻은 사람만이 투표에 참여할 수 있다.
* 공정성(Fairness)  
  투표 진행 과정에서 다른 사람의 투표권 행사에 의해 자신의 투표권 행사가전체 투표에 영향을 줄 수 없어야 한다. 즉 전체 투표에 영향을 줄 수 있는중간 투표 결과를 알 수 없어야 한다.
* 확인성(Verfiability)  
  투표자가 올바르게 자신의 투표용지가 집계되었는지를 확인 할 수 있어야 한다.
* 투표권 매매방지(Untradability)  
  투표권을 타인에게 매매할 수 없으며, 매매에 따른 결과는 투표권을 소유하는 인증된 투표자만이 알 수 있어야 한다.
* 완전성(Completeness)  
  투표자들이나 집계자의 부정에 의해 투표 시스템의 모든 투표 진행이 중단되거나 불완전한 결과를 초래하지 않아야 한다.

**구성요소**

* 투표ID 발급 contract(신원확인)
* 투표 기록 contract(실제 유저들이 투표)
* 검증 contract(신뢰성 상승)

**고려 사항**

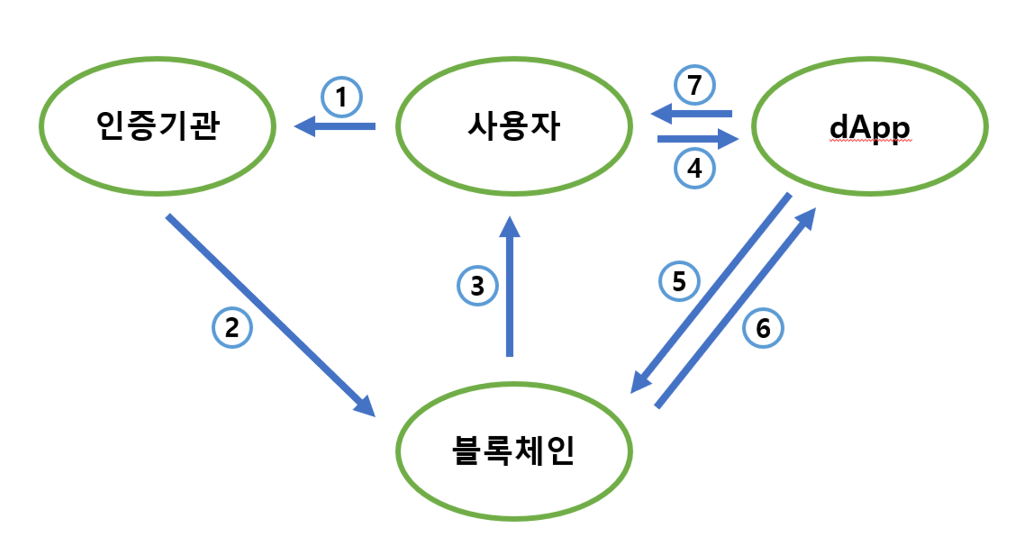
개발자의 임의적인 맞춤화가 제한되는 영역을 명확히 설정해야 합니다.

(다만, 제한이 지나치게 많아지면 활용 가능성이 감소할 수 있으므로 적절한 균형을 유지해야 합니다.)

**제4 장 시스템 설계 및 구현**

**1. 시스템 설계**

**<초기설계 동작과정>**



1 : 인증기관은 공개키 암호화 방법으로 투표 ID 암호화에 사용할 공개키, 개인키를 생성하고, 생성한 공개키는 블록체인에 등록한다.

- ①, ②, ③ : 유권자는 인증기관을 통해 신원인증을 받아서 투표자 인증을 완료하고①, 인증기관은 유권자에게 표에 해당하는 코인을 전송한다.② ③

- 신원인증 시스템[on-chain] | 투표 시스템[on-chain] 이 분리되어야 한다.

- 신원인증 시스템 작동 시나리오

: 유저가 토큰 발급 시스템에 접속 → 외부 라이브러리를 통해 유저 인증 → 토큰 발급 시스템은 외부 라이브러리로부터 결과값을 oracle을 통해 받아서, 해당 유저가 유효한지를 확인 → 유효하다면 토큰 전송

3 : 인증기관은 랜덤 투표ID N개를 생성하고(투표 토큰 N개를 생성), 각각을 인증기관의 개인키로 암호화하여 투표자에게 전송한다.(각각 토큰을 후보자에게 전송.)

- 랜덤 투표 ID는 방법이 여러 가지가 있을 수 있는데, 어느 쪽이 보안에 문제가 없을지 조사가 필요하다.

- `\*\*선정\*\*` case a) 투표ID(private key)를 화면상에 표시하고, 유저가 이를 복사해서 투표 dApp에 붙여넣기해서 로그인하는 방법

- ~~case b) 투표ID를 직접 유저 지갑에 전송하는 방법~~

(private key를 NFT 형태로 지갑에 넣어준다고 보면 된다. 기존 방식에 비해 UX가 크게 개선되고, 확실히 참신하다는 장점이 있다. 다만, 구현 난이도가 올라가는데, 실제 구현 난이도를 측정하기 어렵다는 단점이 있다.)

~~4: (기존 : N개의 랜덤 투표 ID를 받은 투표자는 웹(Web)에서 정수를 입력하여 투표ID를 선택한다(N개의 토큰을 부여 받은 사용자는, dApp에서 후보자를 선택한다.). 투표자가 입력한 정수 N번째의 해당하는 투표 ID가 선택되며 투표 ID 선택이 완료된다.(후보자 지갑에 토큰 각각 전송?))~~

- 4, 5 : 투표 DApp으로 투표자는 투표를 진행한다. 투표자는 DApp과 지갑을 연결하고, 토큰의 보유 여부를 통해 투표권이 있는 정당한 투표자인지 확인한다. 정상적인 코인을 보유하고 있음이 확인되면 코인을 기반으로 투표를 진행된다.(4) 투표를 완료하면 투표 결과는 프라이빗 블록체인에 트랜잭션으로 전달되며 검증 이후 등록된다.(5)

- 선택 완료 시 유저가 선택한 결과값을 암호화한 데이터는 IPFS를 활용해서, 블록체인 서버에 저장된다.

- 6 : 블록체인으로부터 투표등록결과를 받은 투표자는 검증자(검증자가 우리한테 어디있나요?)에게 투표완료결과를 전송한다. ⇒ ()

- 7 : 투표자는 투표자의 공개키로 블록체인에 등록된 투표 결과를 검색하고, 투표 결과가 정상적으로 반영되었는지 확인한다. 검증자는 프라이빗 블록체인에 등록된 투표 결과를 인증기관의 공개키로 투표 ID를 복호화하여 투표권한이 있는 투표자가 투표했는지 검증, 확인한다. 투표 결과가 모두 확인되면 블록체인에 등록된 투표 결과로 투표 결과를 집계하고 투표가 최종 종료된다.

**<최종설계 동작과정>**

- 1 : 운영자는 공개키 암호화 방법으로 투표 ID 암호화에 사용할 공개키, 개인키를 생성하고, 생성한 공개키는 검증자 컨트랙트에 등록하고, 개인키는 투표ID 발급 컨트랙트에 private로 등록한다.

- 2 : 유권자는 투표ID 발급 컨트랙트를 통해 신원인증을 받아서 투표자 인증을 완료한다.

- 투표ID 발급 컨트랙트의 종류에 따라 신원인증이 달라진다. (PASS / MetaMask / None)

- 3 : 투표ID 발급 컨트랙트는 UUID 버전1 기반의 랜덤 투표ID N개를 생성하고, 각각을 컨트랙트가 들고 있는 개인키로 암호화한다. 이후, dApp에서 랜덤 함수를 통해 1~N까지의 정수 중 하나를 선택하면, 투표ID 발급 컨트랙트가 선택한 정수 번째에 해당하는 암호화된 투표ID를 투표자에게 보낸다.

- 의문점 : 투표ID가 굳이 여러개를 주고, 그 중 1개를 선택하게 하는 이유는?

⇒ UUID 국제 표준이기 때문

- UUID란? 🔽

- 네트워크상에서 서로 모르는 개체들을 식별하고 구별하기 위해서는 각각의 고유한 이름이 필요하다. 같은 이름을 갖는 개체가 존재한다면 구별이 불가능해지기 때문에, 이름은 고유성이 매우 중요하다. 고유성을 완벽하게 보장하려면중앙관리 시스템에서 일련번호를 부여해주면 간단하지만 동시다발적이고 독립적으로 개발되고 있는 시스템들의 경우 중앙 관리 시스템은 불가능하다. 개발주체가 스스로 이름을 짓도록 하되, 고유성을 충족할 수 있는 방법이 UUID(Universally Unique IDentifier)이며 국제기구에서 표준으로 정하고 있다

- 의문점 : 투표ID가 중복될수 있는가?

⇒ 랜덤 ID 구현 시 시간 파라미터가 들어가 있어서 중복될 일이 거의 없다.

- 4 : 투표자는 투표 dApp으로 투표를 진행한다. 투표자는 투표ID 발급 컨트랙트로부터 받은 투표 ID를 dApp에 입력하면, 검증 컨트랙트는 투표권이 있는 정당한 투표자인지 확인한다. 이후 정상적인 투표ID으로 확인되면 투표를 진행된다.

- 투표자 한 명당 투표ID를 하나만 받을 수 있으며, 투표ID는 투표자 한 명이 받을 수 있는 투표권 모음에 대응된다. (예를 들어 투표권 6장을 주는 투표라면, 투표ID 1개당 투표권 6장이 나온다고 보면 된다.)

- 투표권을 확인하는 방법 : 투표자가 입력한 투표 ID를 검증 컨트랙트가 들고 있는 공개키로 해독 가능한지를 확인한다.

(근데 이게 맞는지 확인은 해봐야 할 듯. 잠만 이 과정이 아래에 있는데?)

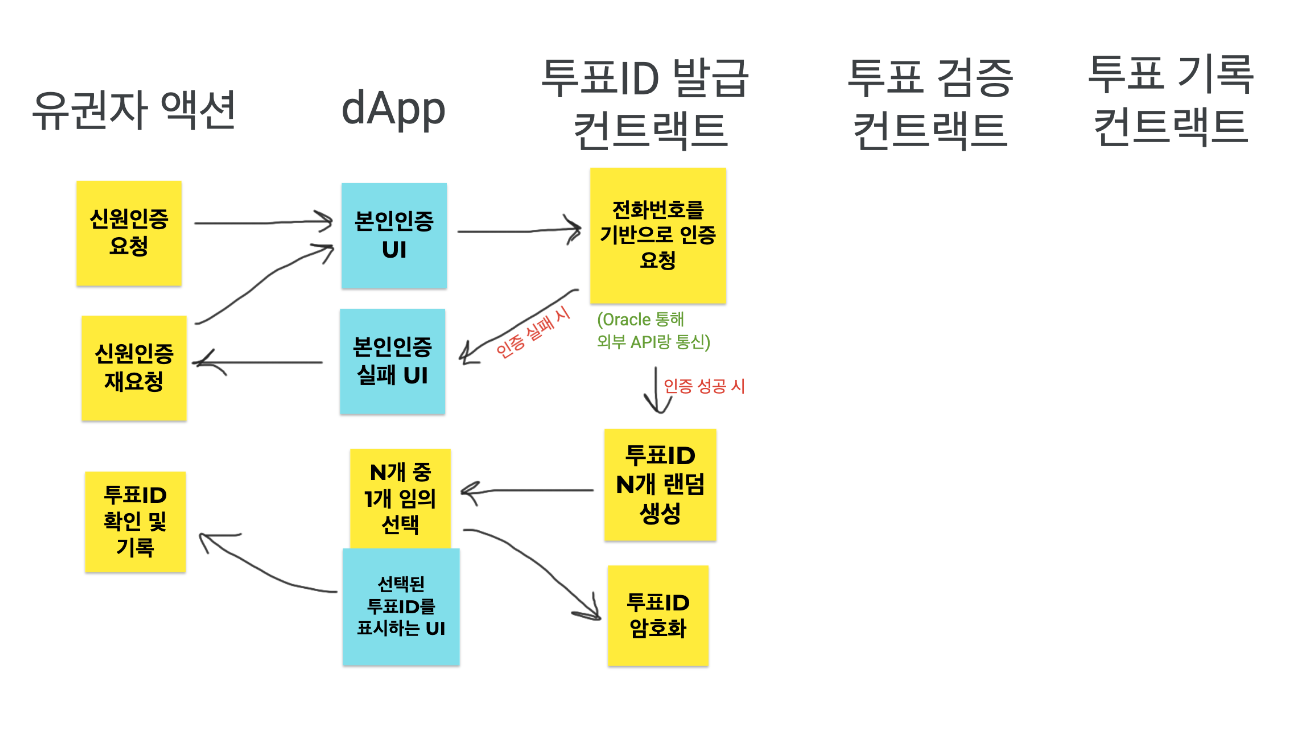
- 5 : 투표자가 투표를 완료(투표종료)하면 그 결과는 투표 컨트랙트에 전달되고, 검증 컨트랙트는 투표 컨트랙트에 등록된 투표 결과 중 투표 ID를 공개키로 복호화하여 투표권한이 있는 투표자가 투표했는지 검증, 확인한다. 문제가 없으면 투표자가 제출한 값을 투표 컨트랙트에 반영한다.

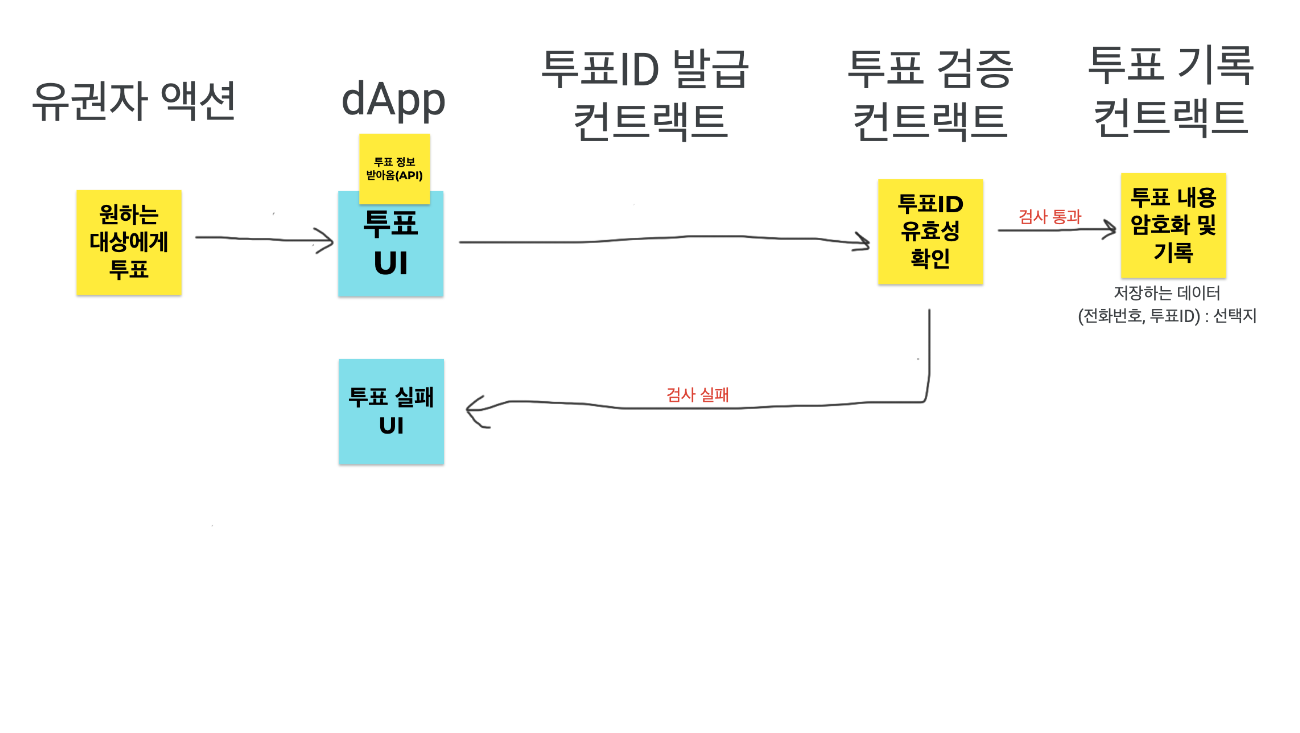
- 이 시점에서는 연산을 하지 않기 때문에, 투표자들은 중간 집계 결과를 알 수 없다.

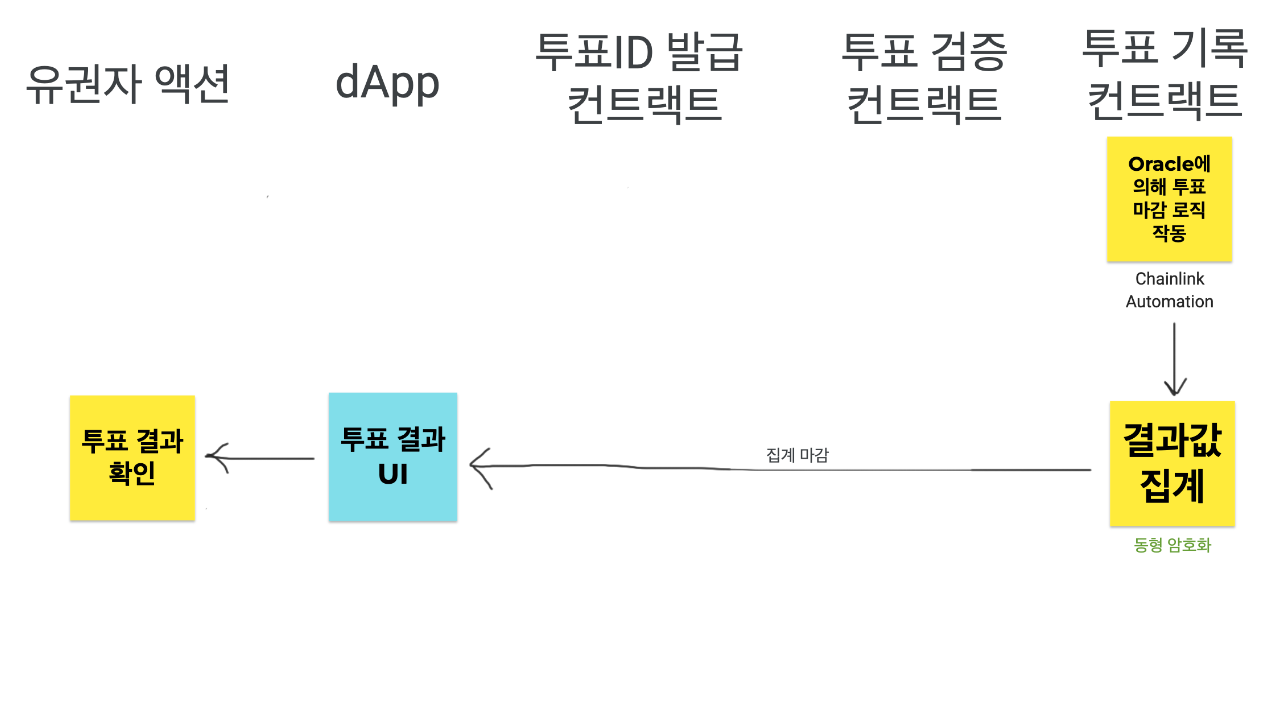
- 6 : 투표 기간이 끝나면, 투표자들이 등록한 표를 바탕으로 투표 결과를 집계하고 투표자들에게 결과를 알려준다.

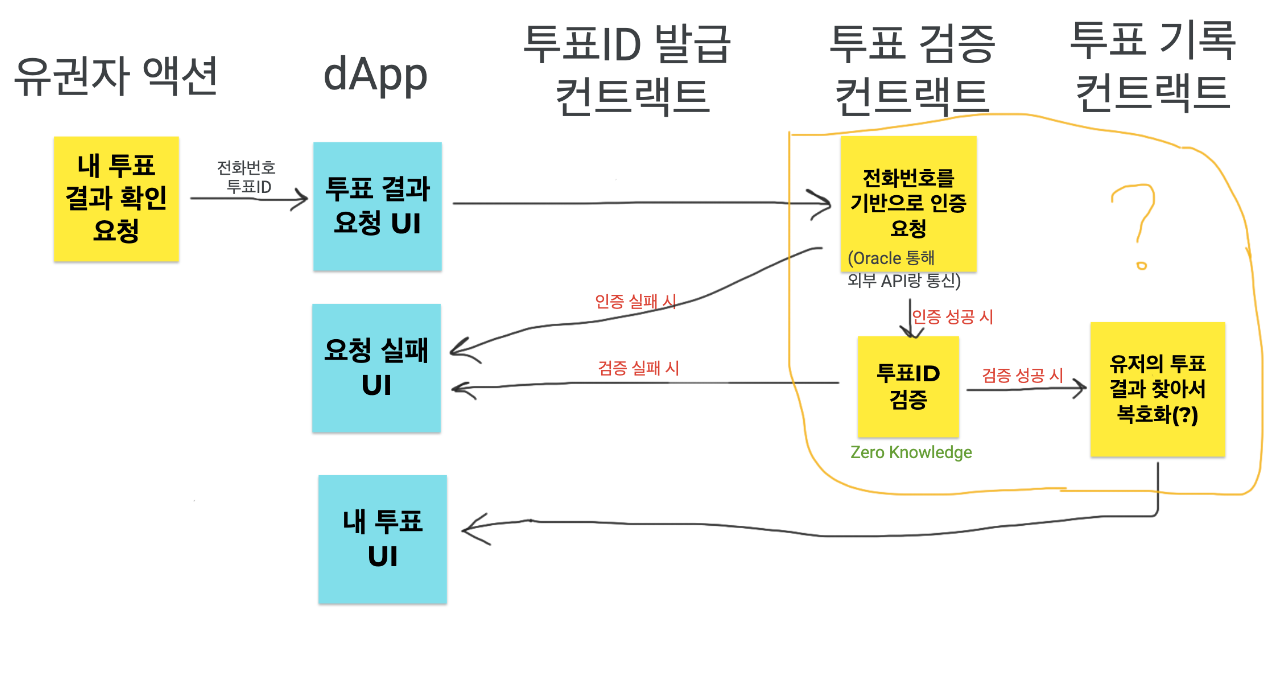
- (6 이후 : 만약 투표자가 원한다면, 투표자는 본인의 개인키로 블록체인에 등록된 투표 결과를 검색하고, 투표 결과가 정상적으로 반영되었는지 확인할 수 있다.)

**<유권자가 투표 하는 시나리오 Flowchart>**









**<기능 명세>**

1. 기능 명세 작성

(\*\*편집 가능\*\*/ \*\*편집 불능\*\*)

투표ID 발급 컨트랙트(신원 확인)(투표 아이디 발급하는 몇가지 메쏘드 중 택1의 기회(3개면 충분할 듯?))

\*\*편집 가능\*\* 개인 키 등록

\*\*편집 불능\*\* 신원 인증을 받아 유권자 인증 (메서드를 개발자가 선택)

\*\*편집 가능\*\*투표 대상(whitelist) 저장

\*\*편집 가능\*\* 투표 ID N개 생성 + 개인키로 암호화 (개발자는 N에 해당하는 값 지정 가능)

\*\*편집 불능\*\* N번째 투표 ID 전송

투표 기록 컨트랙트(실제 유저들이 투표)

\*\*편집 가능\*\* 투표 ID 공개키 복호화

\*\*편집 가능\*\* 투표권 몇 개 부여 + 선택지 + 투표 기한 + 투표 관련 정보 제공(contract or DB)

\*\*편집 가능\*\* 투표자들의 표 집계 및 결과 전달

검증 컨트랙트

\*\*편집 가능공개키(유저가 직접 등록)\*\*

\*\*편집 불능\*\* 투표 검증 기능(시스템 내부에서 동작하며 외부로 노출되지 않음)

**2. 시스템 구현**

**프로젝트의 역할 분담**

**개별 임무 분담**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **번호** | **학과** | **학번** | **학년** | **이름** | **담당업무** |
| 1 | 컴퓨터소프트웨어 | 2020019152 | 4 | 정지나 | 컨트랙트 개발, 설계, 보고서 |
| 2 | 컴퓨터소프트웨어 | 2015000346 | 4 | 우수몽 | 컨트랙트 개발, FE BE 개발 |

**개발 일정**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **구분** | **추진내용** | **수행기간** | | | | | | | | | | | |
| **1월** | **2월** | **3월** | **4월** | **5월** | **6월** | **7월** | **8월** | **9월** | **10월** | **11월** | **12월** |
| 계획 | 시장 분석 및 주제 선정 |  |  |  |  |  |  |  |  |  |  |  |  |
| 분석 | 스마트 컨트랙트 기술의 이해 |  |  |  |  |  |  |  |  |  |  |  |  |
| 설계 | 라이브러리 및 기술 선택 |  |  |  |  |  |  |  |  |  |  |  |  |
| flow chart 설계 |  |  |  |  |  |  |  |  |  |  |  |  |
| 개발 | FE BE 개발 |  |  |  |  |  |  |  |  |  |  |  |  |
| smart contract 개발 |  |  |  |  |  |  |  |  |  |  |  |  |
| 테스트 | web3 연결 및 컨트랙트 작동 확인 |  |  |  |  |  |  |  |  |  |  |  |  |
| 논문작성 | 결과보소서 작성 및 작업물 정리 |  |  |  |  |  |  |  |  |  |  |  |  |
| 종료 | 발표 및 작업물 제출 |  |  |  |  |  |  |  |  |  |  |  |  |

**사용기술**

이 연구에서는 다양한 혁신적인 기술과 프레임워크를 사용하여 안전하고 효율적인 전자 투표 시스템을 설계하고 구현했습니다. 그 중 일부 기술은 다음과 같습니다.

Chainlink: Chainlink는 블록체인과 외부 데이터 소스 간의 연결을 제공하여 신뢰할 수 있는 데이터를 블록체인으로 가져올 수 있도록 하는 오픈 소스 프레임워크입니다. 이를 통해 전자 투표 시스템은 외부 데이터를 활용하여 보다 정확하고 신뢰할 수 있는 투표 결과를 보장할 수 있습니다.

Web 3 서비스: Web 3 서비스는 사용자의 데이터 및 디지털 자산에 대한 투명성, 보안 및 소유권을 강화하기 위한 웹 기술의 집합입니다. 이를 통해 전자 투표 시스템은 보다 안전하고 신뢰할 수 있는 투표 환경을 제공할 수 있으며, 사용자의 개인 정보 보호를 강화할 수 있습니다.

동형암호 기법 - Paillier 암호화: Paillier 암호화는 동형 암호 기술의 일종으로, 투표 데이터를 보호하고 블록체인 네트워크 상에서 안전하게 전송하면서도 데이터의 기밀성을 유지할 수 있습니다. 이를 통해 전자 투표 시스템은 투표 데이터의 안전성과 개인 정보 보호를 보장할 수 있습니다.

이러한 기술들의 융합은 전자 투표 시스템의 보안성과 신뢰성을 강화하는 데에 기여했습니다. 사용자의 투표 데이터와 신원 정보를 보호하고 외부 데이터 소스와의 안전한 연결을 통해 정확하고 신뢰할 수 있는 투표 결과를 제공하는 것이 이 연구의 주요 목표였습니다.

**제5 장 결론 및 제언**

위 프로젝트를 통해 얻은 결론과 기대효과는 다음과 같습니다:

- 보안 강화: 전자투표 시스템에 블록체인과 암호화 기술을 통합하여 투표 과정의 보안을 강화할 수 있습니다. 이를 통해 투표 결과의 무결성과 신뢰성을 보장할 수 있습니다.

- 투표 과정의 투명성 향상: 블록체인을 통해 투표 과정의 투명성을 높일 수 있습니다. 이는 투표에 참여하는 모든 개별 참여자들이 투표 과정과 결과를 실시간으로 확인할 수 있음을 의미합니다.

- 프라이버시 보호 강화: 암호화 기술과 블록체인을 활용하여 투표자의 프라이버시를 보호할 수 있습니다. 이는 투표자의 투표 의사가 공개되지 않도록 보장하며, 동시에 투표의 무결성을 유지합니다.

- 신속하고 효율적인 투표 집계: 블록체인 기술을 활용하면 투표 결과의 신속한 집계가 가능해집니다. 이는 전통적인 투표 방식에 비해 투표 결과를 더욱 효율적으로 처리할 수 있음을 의미합니다.

- 데이터 무결성과 불변성 보장: 블록체인의 분산원장 기술을 통해 투표 데이터의 불변성과 무결성을 보장할 수 있습니다. 이는 투표 기록이 변조되지 않고 신뢰할 수 있는 데이터로 유지됨을 의미합니다.

이러한 결론과 기대효과를 통해 전자투표 시스템의 신뢰성을 향상시킬 수 있으며, 민주주의 프로세스를 강화하고 민중의 신뢰를 얻을 수 있습니다.

이 프로젝트를 통해서 앞으로 고려해볼 사항입니다.

- 추가 보안 연구 및 테스트: 시스템의 안전성을 강화하기 위해 암호화 기술과 블록체인의 적용 범위를 확장하고, 이를 확인하기 위한 철저한 테스트가 필요합니다.

- 사용자 경험 개선을 위한 UI/UX 디자인 개선: 사용자 편의성을 높이기 위해 직관적이고 친숙한 UI/UX 디자인을 채택하여 사용자들이 쉽게 시스템을 사용할 수 있도록 해야 합니다.

- 확장성을 고려한 시스템 설계: 대규모 선거나 다양한 유형의 선거를 위해 시스템을 확장 가능하도록 설계해야 합니다. 이는 시스템의 유연성을 높이고 다양한 환경에 적응할 수 있도록 하는 데 도움이 될 것입니다.

- 사용자 교육 및 훈련 강화: 시스템 사용자들에게 적절한 교육과 훈련을 제공하여 시스템을 올바르게 이용할 수 있도록 해야 합니다. 이는 시스템 사용의 효율성과 정확성을 높일 수 있습니다.

정부 및 국제 기관과의 협력 강화: 전자투표 시스템을 보다 넓은 범위에서 적용하기 위해 정부 및 국제 기관과의 협력을 강화해야 합니다. 이는 시스템의 신뢰성을 높이고 국제적인 표준과 규제를 준수하는 데 도움이 될 것입니다.

**참고 자료**

- https://github.com/a16z/cicada : 프라이버시를 보장하는 블록체인상의 투표 프로토콜.\*\*\*\*

- [homomorphic time-lock puzzles](https://eprint.iacr.org/2019/635.pdf) 알고리즘

- Foundery(스마트 컨트랙트 개발 도구 체인)를 필요로 한다.

- https://github.com/ScopeLift/flexible-voting : DAO(탈중앙화 자율 조직) 거버넌스를 위한 강력한 구성요소

- 정확히는 OpenZeppelin DAO Governor의 확장으로, 새로운 투표 패턴을 거버넌스에 제공한다.

- 특정 안건에 대해 찬성/반대/기권의 세 가지로 투표할 수 있다.

- 비밀/비공개 투표 및 더 저렴한 보조 서명 기반 투표를 제공한다.

- 단점 :

- https://github.com/devanoneth/ERC4626Votes

- ~~https://github.com/yearn/veYFI (이거 투표 관련이 아닌듯? Voting YFI라고는 되어 있는데 설명은 투표랑 거리가 멀다.)~

[Code Snippet 성격이 강한 것들]

- https://github.com/oo-00/Votium (이건 그냥 예제같은 느낌인듯)

- https://github.com/D3LAB-DAO/Governor-C :

- https://github.com/TheBojda/zktree-vote :

- https://github.com/trizin/homomorphic-voting-on-evm-with-zkp

\*\*\*\*: [ECC(Eliptic Curve Cryptography, 타원 곡선 암호학)](https://www.crocus.co.kr/1226) + [ElGamel 암호화 체계](https://yjshin.tistory.com/364) + ZKP(분리형 차움-페데르센 영지식 증명)

- 두 개의 공개키 암호화 체계에 동형 암호화를 적용했고, 거기에 프라이버시의 구현을 위해 ZKP까지 사용했다.

- https://github.com/kalidao/ERC1155V

- https://github.com/makerdao/vote-proxy

- https://github.com/z0r0z/veSUSHI

https://www.mdpi.com/1424-8220/21/17/5874