|  |
| --- |
| **1. 주제**  **대중들을 위한 블록체인을 이용한 온라인 투표 시스템**  **가반, 12팀, 20213061** |

|  |  |
| --- | --- |
| **2. 요약**  전자적인 방식을 통해 투표 및 개표를 하여, 사람들이 장소에 연연하지 않고 투표하며, 적은 인력과 비용 투입을 가능하게 하는 방식으로 투표를 하는 데에 목표가 있다. 거기다 블록체인 기술로 보안성을 높여 불법적인 조작을 차단할 수도 있다. | **3. 대표 그림** |

|  |
| --- |
| **4. 서론**  선거는 민주주의의 가장 근간이 되는 행동이라 할 수 있다. 하지만 옛날부터 부패한 정치인들과 공무원들은 불법을 하거나, 조작하기도 했다. 물론 쉽게 할 수 있는 일은 아니지만, 그렇다고 그런 일이 없을 거라고 완전히 배제하고 볼 수도 없다. 따라서, 여러 나라에서 종이투표보다 전자투표를 택하기도 한다. 스위스의 경우 1990년대부터 연구를 시작하여, 2000년대 초반에 지역별로 테스트를 시작하였고 대다수 도시에서 2005년쯤에 상용화가 시작되었다.  하지만, 스위스를 포함하여 초기의 전자투표는 사람들의 신뢰 부족과 기술 부족으로 인한 보안성 부족으로 사람들의 반대가 있어 원활히 발전하지 못하였으며 이는 현재도 마찬가지다. 이 문제를 해결하기 위해 전자투표의 가장 치명적인 단점인 신뢰성과 보안성을 강화하는 블록체인 기술을 전자투표 시스템에 도입하자는 것이다. 이때 말하는 전자투표 방식은 3가지 투표 방식인 PSEV 방식, 키오스크 방식, REV 방식 중에 디지털 TV, 모바일, PC 등을 이용하여 투표하는 REV 방식을 말한다. |

|  |
| --- |
| **5. 본론**      이 시스템이 작동하는 데 필요한 요소들로는 가장 중요한 블록체인 기술, 보안을 위한 SHA-256 암호화, 데이터의 간편하고 확실한 인증을 위한 머클트리 루트, 디지털 서명과 사이드 체인 등이 있다.  블록체인 기술은 데이터를 담고 있는 여러 블록이 신뢰를 검증받아 서로 연결되어 서로 관리하는 기술이다. 이때, 블록체인은 거래를 블록 단위로 해서 데이터 구조에 저장한다. 하나의 블록은 블록헤더와 블록바디로 나뉘는데 이 블록 헤더에 SHA-256 암호화 알고리즘을 이용하여 해시값을 읽고, 머클트리 루트가 포함된다. 투표할 때 기능들을 7가지로 표현하자면 투표 방 추가, 질문 및 항목 입력, 투표 리스트 표시, 신원 인증, 투표 진행, 중복 사용자 체크, 투표 결과 보기가 있다. 이를 투표 등록자와 사용자로 구분하여 순서대로 어떻게 구현되는지 보자.  첫째로, 투표 등록자가 투표 방을 생성한다. 그 후, 투표방안에 추가할 항목을 입력한다. 그렇게 만들어진 항목들을 투표 방 리스트에 표시한다. 이제 사용자가 신원 인증을 하고 리스트를 요청하면 투표 리스트는 블록체인에 리스트를 다시 요청하고 블록체인이 제공하면 리스트를 사용자에게 표시해준다. 사용자가 투표를 완료하면 투표 진행하는 방에 리스트가 사용자가 무엇을 선택했는지 전달하고 투표 진행 방이 블록체인에 방 정보 요청 후 이를 재구성하여 작업을 마친다. 이때, 만약 사용자가 이중 투표를 하면 방 정보를 확인 후 사용을 금지한다. 이후 결과화면을 보여줄 때도 사용자가 요청하면 리스트에서 블록체인에 요청 후 결과화면을 사용자에게 보여준다. |

|  |
| --- |
| **6. 결론**  아직 블록체인 기술 또한 상용화하기에 기술력이 부족하여 해킹당할 위험이 있고 이를 보완하기 위해 사용되는 이더리움 기술 또한 사용 시간이 길어진다는 단점을 해결하지 못하고 있다. 이에 취약한 보안성 문제를 해결하기 위해 더 정교한 블록체인 알고리즘을 연구하고 암호화 기술을 발전시켜 여러 문제를 해결해야 할 것이다. |

**7. 출처**

[1] 허균, 임꺽정, “홍길동의 얼굴 분석,” 한국OOO논문지, 제5권, 제6호, pp. 1-10, 2006.

[2] 박태진. "블록체인을 활용한 온라인 투표 시스템 설계 및 구현." 국내석사학위논문 한양대학교 공학대학원, 2019. 서울

[3] 한영빈 "스위스의 전자투표:도입배경, 현황 및 전망을 중심으로" 유럽연구 26.1 pp.125-151 (2008) : 125.