1페이지 주제제안서 (제출일 : 2018년 3월 14일)

팀명 : Chainerator	**팀원 : 신재철, 정구익, 하현수, 홍상원**

제목 : Public Anonymity Blockchain Constructor

(익명성이 보장되는 Public Blockchain 기반의 오픈소스 프레임워크)

개요

- Public Blockchain은 일종의 분산 원장 시스템으로서, Cryptocurrency의 트랜잭션의 위변조를 막는 핵심 기술이다. 투명성과 무결성이 보장되는 Public Blockchain의 특성상 조작이 일어나서는 안되는 전자투표나 여론조사, 강의평가 등에 핵심 기술로 이용될 수 있다.

  하지만 Public Blockchain에서 프라이버시 침해 문제는 심각한 문제로 대두되고 있다. Blockchain Wallet의 주소가 공개키 개념으로 완전히 공개되고, 대부분의 Blockchain Monitoring Service에서 해당 주소를 검색하면 모든 트랜잭션 내역을 조회할 수 있기 때문이다.

  이로 인해 Public Blockchain을 이용할 경우, 플랫폼 이용자의 신원이 그대로 노출될 수 있다.

  반면에 Private Blockchain을 이용할 경우, 트랜잭션 내역이 모두 공개되지 않아 익명성은 보장될 수 있지만, 투명성과 무결성이 보장되지 않는다. Blockchain 자체는 신뢰성 네트워크지만, 본인의 트랜잭션이 실제로 잘 전달되었는지 확인할 방법이 없기 때문이다.

  따라서 본 프로젝트에서는 Public Blockchain을 이용하여 투명성과 무결성을 유지하되,

  다양한 Anonymity Protocol을 적용하여 필요에 따라서 참여자들의 신원을 보호할 수 있는 프레임워크를 만드는 것을 목적으로 한다.

- 최근 Blockchain에 뜨거운 관심이 쏟아지면서, 다양한 기업들이 블록체인 POC 프로젝트에 뛰어들고 있다. 하지만, 기업의 개발자 수요에 비해서 블록체인 코어를 제작할 수 있는 개발자는 매우 적어 실제로 기업체에서 자체 블록체인을 구현하는것은 어려운것이 현실이다.

  따라서 본 프로젝트에서는 코드를 간단히 몇 줄 수정함으로써, 자체 블록체인을 생성할 수 있는 프레임워크 를 제작하는 것을 목표로 한다.

장점

- Public Blockchain의 투명성과 무결성은 유지하면서 익명성을 보장할 수 있다.
- 익명성이 보장된 자체 블록체인 플랫폼 제작을 누구나 간단히 할 수 있다.

참고 자료 및 비교 대상

- Satoshi Nakamoto. “Bitcoin: A Peer-to-Peer Electronic Cash System” bitcoin.org, 2009.
- Yoshiharu Akahane, Manabu Aikei., Blockchain SHIKUMI TO RIRON, rictelecom, Oct.2016
- 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
- Verge Foundation,"Verge-Anonymity-Centric-CryptoCurrency "(White paper), Oct, 2017
- Nicolas van Saberhagen, “CryptoNote V2.0”,(White Paper), Oct, 2013

창의성 및 차별화 전략

- Public Blockchain에 Anonymity Protocol을 접목하여 Public 블록체인의 투명성, 무결성을 유지하면서 익명성을 보장할 수 있다.
- 오픈 소스 프레임워크 방식으로 제작하여 누구나 쉽게 코드를 바꿔서 자체 블록체인 네트워크를 생성할 수 있다.
- Consensus Algorithm방식을 POW, POS, DPOS, Hybird POS, PBFT 에서 선택하여 생성할 수 있도록 한다.

결론

- 복잡한 코딩 없이도 익명성이 보장되는 Public Blockchain 플랫폼을 구현 할 수 있는 오픈 소스 프레임 워크를 제공한다.
- 다양한 블록체인 플랫폼을 개발할 수 있도록 Consensus 방식을 사용자가 직접 선택할 수 있도록 구현한다.
- 이를 통해 누구나 쉽게 블록체인을 이용하여 전자 투표나 강의평가등을 진행할 수 있다.