Software Requirements Specification Template(SRS)

작성자:	신재철, 정구익, 하현수, 홍상원
생성일자:	2018-03-14
최종 갱신:	2017-03-14
버전:	0.1

목차

1. 개요

여러가지 기업에서 블록체인에 대한 관심이 뜨겁다.

대부분이 여러가지 프로젝트를 POC 로 진행하고 있지만,

수요에 대비해서 블록체인 개발 인력은 터무니 없이 부족하다.

따라서 누구나 편하게 사용할 수 있는 프레임워크 형태의 블록체인 오픈소스를 개발하고자 한다.

1.1 목적

- 단순한 코드 수정만으로 자체 블록체인을 생성할 수 있는 오픈 소스 프레임워크를 구현한다.
- Public Blockchain 에 익명성 프로토콜을 도입하여 트랜잭션 데이터에 대한 보안을 향상시키고, 공개 범위를 제한한다.
- 익명성이 필요한 분야(전자투표, 강의평가 등)에서 블록체인을 통한 정보의 신뢰성과 무결성을 보장하고, 익명성 프로토콜을 통해 개인의 신원 또한 숨길 수 있다.

1.2 관련부서/관계자

Development Team 은 숭실대학교 컴퓨터학부 학부생(4 학년) 2 명, 소프트웨어 학부생(4 학년) 2 명이 팀을 이뤄 구성된다.

또한 본 프로젝트는, 숭실대학교 캡스톤 프로젝트 과목의 지도 교수님의 지도 하에 진행된다.

1.3 개발범위

Transaction

블록체인의 트랜잭션을 담당하는 모듈.

Anonymity Protocol

Ring Signature, Confidence Transaction, Tor, Stealth Addressing 등의 다양한 익명성 프로토콜 개발 및 블록체인 연동.

P2P

블록체인이 동작할 P2P 노드와 서버 구현

RPC

블록체인이 동작할 RPC 서버 구현.

Mining & Consensus

채굴과 컨센서스(POW,POS,DPOS,PBFT)등등의 기능 구현

2. 전체개관

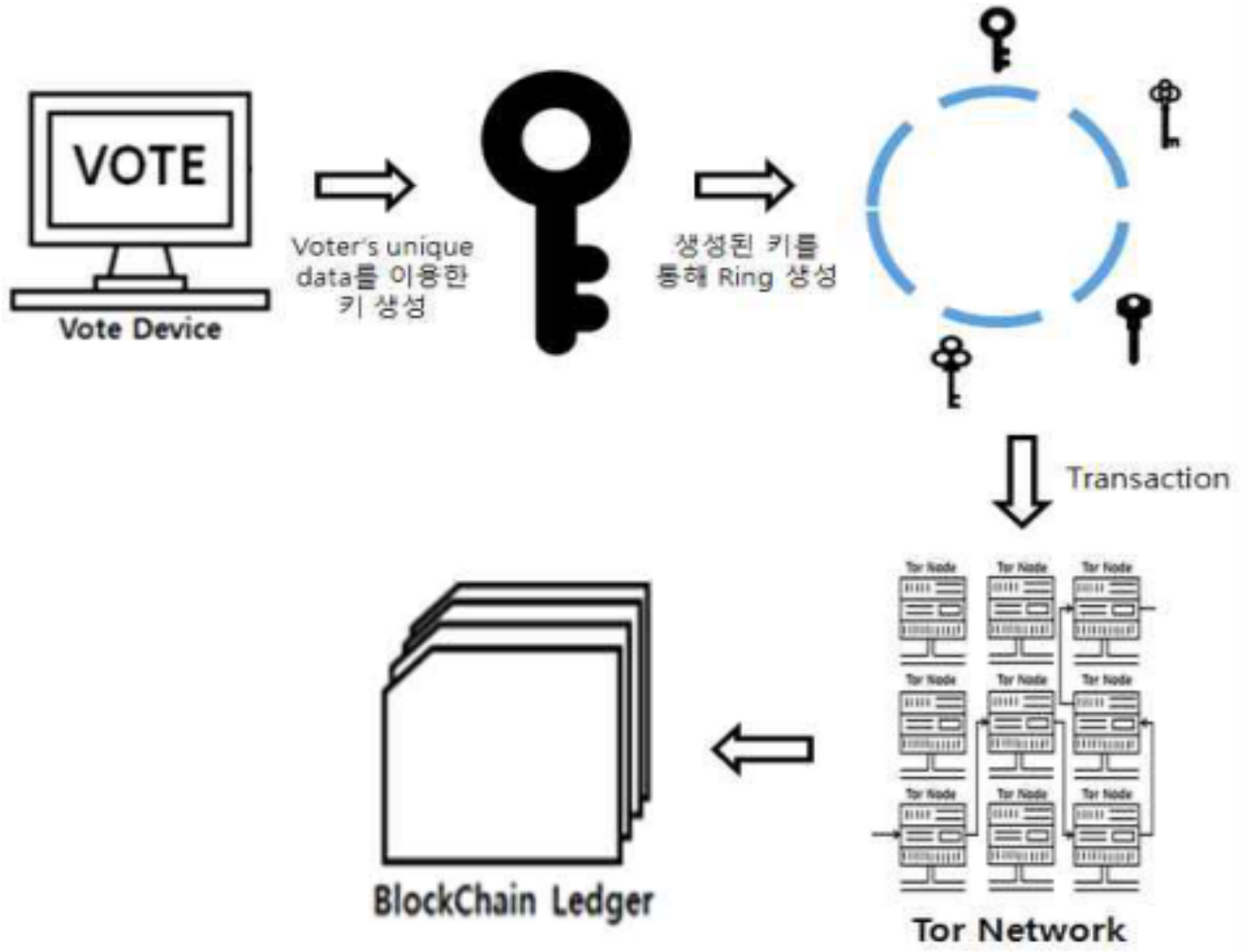
2.1 프로젝트 개요

기존에 존재하던 블록체인 플랫폼은 공개키가 지갑의 형태로 공개 되어있기 때문에 input 과 output 을 통해 해당 transaction 을 주체와 대상을 알아 낼 수 있어 익명성이 보장되어 있지 않다. 이 때문에 선거나 강의평가 등에서 무결성과 투명성을 블록체인을 통해 보장 할 수 있지만, 익명성은 Public Blockchain 의 특성상 보장하기 어려운 것이 현실이다.

이러한 단점을 익명성 프로토콜을 통해 보완하여 좀 더 다양한 분야에서 블록체인이 활용 가능하도록 할 수 있는 블록체인 플랫폼이다.

2.2 Product Function

- TOR 를 통해 패킷 자체를 삼중우회 시킨다.
- 1 개의 개인키에 여러 개의 공개키를 사용하는 Stealth Addressing 기법을 통해 이용자의 신원이 밝혀지지 않도록 한다.
- 여러 개의 트랜잭션의 전자 서명 값을 묶어서 처리하는 Ring Signature 기법을 통해, 트랜잭션 역추적을 통한 신원 조회를 원천 봉쇄한다.
- 소스는 최대한 OOP 를 따라 제작하여 사용자가 단순히 코드를 몇 줄만 바꾸더라도 바로 자체 블록체인을 구현할 수 있도록 코딩한다.
- POW 의 해싱파워를 단순 계산이 아닌 여러 가지 용도(머신 러닝, 수학 문제 해결)로 사용할 수 있도록 한다.(Option)



사용사례 – 전자 투표 예시

2.3 사용자 특성

프레임워크이기 때문에 익명성이 요구되는 블록체인을 이용한 플랫폼을 만들고자 하는 개발자, 기획자가 주로 사용할 것이다.

오픈 소스로서 블록체인을 공부 혹은 개발하고자 하는 사람들에게도 사용될 것이다.

2.4 소프트웨어 운영환경

프로그래밍이 가능하고 컴파일이 가능하다면 어떠한 환경에서도 가능하다.

2.5 디자인과 배포 제약사항

본 프로젝트의 뼈대가 되는 Hyperledger Fabric 과 CryptoNote 의 소스코드는 MIT 라이선스이므로, 명시만 하면 사용해도 문제되지 않는다.

따라서 Hyperledger Fabric 와 CryptoNote 의 주요 소스코드를 발라내어 뼈대를 구상하고, 그 후에 기능을 얹고 기존 코드를 변경하도록 한다.

2.6 가정과 의존성

- 네트워크 상황이 좋지 않아도 서비스는 정상적으로 유지되어야 한다.
- P2P Node 와 Seed Node 는 반드시 항상 동작하는 상태여야 한다.
- 서버의 보안은 잘 유지되어야 한다.
- 실시간으로 블록체인 동기화가 이루어져야 한다.

2.7 데이터 요구사항

- 블록체인의 최신 블록 정보
- 블록체인에 접속한 Whitepeer 와 GrayPeer 및 SeedNode 의 정보
- 트랜잭션 정보
- 사용자들의 전자 서명 정보

2.8 사용 시나리오

전자 투표에서 투표의 무결성을 보장하면서도 비밀투표의 원칙을 만족시킬 수 있다.

익명이 필요하면서도 조작이 되어서는 안되는 대학교 강의평가나 여론조사 플랫폼 등에서 이용될 수 있다.

2.9 타어플과의 차이점

블록체인의 트랜잭션 정보를 필요에 따라서 조회를 막아, 개인의 신원을 보호한다.

제멋대로인 코딩컨벤션으로 짜인 복잡한 오픈소스가 아닌, 누구나 코드를 간단하게 수정하면 사용할 수 있는 블록체인 오픈소스 프레임워크이다.

.