프로젝트 최종보고서

나는 숭실대학교 컴퓨터학부/소프트웨어학부의 일원으로 명예를 지키면서 생활하고 있습니다.

나는 보고서를 작성하면서 다음과 같은 사항을 준수하였음을 엄숙히 서약합니다.

1. 나는 자력으로 보고서를 작성하였습니다.

2. 나는 보고서에서 참조한 문헌의 출처를 밝혔으며 표절하지 않았습니다.

3. 나는 보고서의 내용을 조작하거나 날조하지 않았습니다.

프로젝트 제목	SoongsilCoin
교과목 교수	이상준 교수님
지도 교수	김영종 교수님
프로젝트 팀명	Chainerator (체이너레이터)
프로젝트 구성원	컴퓨터학부 4 학년 신재철(20132142) 컴퓨터학부 4 학년 홍상원(20142577) 소프트웨어학부 4 학년 정구익(20150271) 소프트웨어학부 4 학년 하현수(20150291)
제출일	2018년 6 월 29 일

1. 프로젝트 팀원 소개

<table>
<tr><td rowspan="2">프로젝트명</td><td>영문</td><td colspan="4">SoongsilCoin</td></tr>
<tr><td>국문</td><td colspan="4">숭실코인</td></tr>
<tr><td colspan="2">팀 명</td><td colspan="4">Chainerator</td></tr>
<tr><td colspan="2" rowspan="5">팀 구성</td><td>직 책</td><td>성 명</td><td>학 번</td><td>E-mail</td></tr>
<tr><td>팀 장</td><td>신재철</td><td>20132142</td><td>jcgod413@gmail.com</td></tr>
<tr><td>팀 원</td><td>홍상원</td><td>20142577</td><td>qpakzk@gmail.com</td></tr>
<tr><td>팀 원</td><td>정구익</td><td>20150271</td><td>rndlr96@gmail.com</td></tr>
<tr><td>팀 원</td><td>하현수</td><td>20150291</td><td>dhy03196@gmail.com</td></tr>
<tr><td colspan="2">수행 기간</td><td colspan="4">2018년 3월 ~ 6 월</td></tr>
</table>

1) 신재철(팀장)

- 팀 일정 총괄
- 이더리움 블록체인 확장성 이슈 연구 (“이더리움 블록체인 성능 향상을 위한 기술 동향” 제 2저자)
- SoongsilCoin 개발

2) 홍상원(팀원)

- 이더리움 블록체인 확장성 이슈 연구 (“이더리움 블록체인 성능 향상을 위한 기술 동향” 제 1저자)
- SoongsilCoin 개발

3) 정구익 (팀원)

- 플랙서블 블록체인 프레임워크 연구 (“자체 블록체인 네트워크 구축을 위한 플렉서블 블록체인 프레임워크 구현” 제 2저자)
- Poof-of-Work, Proof-of-Stake 모듈화 연구

4) 하현수 (팀원)

- 플랙서블 블록체인 프레임워크 연구 (“자체 블록체인 네트워크 구축을 위한 플렉서블 블록체인 프레임워크 구현” 제 2저자)
- Poof-of-Work, Proof-of-Stake 모듈화 연구

2. 프로젝트 목적

블록체인(Blockchain)은 신뢰할 수 있는 제 3자 없이도 P2P(Peer-to-Peer) 네트워크에 속한 노드(Node)들이 합의 알고리즘(Consensus Algorithm)에 의해 안전하게 데이터를 통신하고 위변조 없이 영구적으로 데이터를 기록할 수 있는 탈중앙화된 컴퓨팅 시스템이다.

현재 대부분의 서비스들은 서버-클라이언트 구조의 시스템으로 개발, 운영되고 있다. 서버-클라이언트 구조에서는 서버로 데이터가 집중되어 서버를 관리하는 회사들이 데이터를 독점하게 된다. 그리고 해커들이 몇 개의 서버만 공격하면 해킹에 성공할 수 있기 때문에 보안에 취약할 수밖에 없다.

블록체인은 이러한 패러다임을 전환시켰다. 블록체인은 시스템을 탈중앙화하여 모든 노드들이 모든 데이터를 저장하도록 구성하였다. 그리고 블록체인은 과반수의 노드를 해킹하지 않으면 데이터 위변조가 불가능하기 때문에 사실상 해킹이 불가능한, 보안성이 높은 시스템을 구축할 수 있게 한다.

탈중앙화라는 새로운 패러다임 덕분에 블록체인을 활용한 서비스를 개발하려는 움직임을 보이고 있다. 특히 이더리움(Ethereum) 블록체인은 플랫폼을 지향하고 있기 때문에 Turing Complete한 가상 머신인 EVM (Ethereum Virtual Machine) 상에 프로그래밍 가능한 스마트 컨트랙트(Smart Contract)를 개발하여 서비스를 구동시킬 수 있다. 이더리움에서는 다양한 라이브러리, 프레임워크, IDE를 제공하여 서비스(DAPP)를 개발하는데 다양한 지원을 해주고 있다.

그러나 이더리움을 활용하여 서비스를 개발하는 것은 한계가 많다. 이더리움 성능 이슈 뿐만 아니라 범용적인 블록체인 플랫폼을 지향하기 때문에 서비스 목적에 부합하는 블록체인을 지원하는데는 한계가 있다. 여기서 이더리움 성능 이슈(또는 이더리움 확장성 이슈)란 이더리움이 트랜잭션을 처리하는 속도가 너무 느려서 발생하는 문제이다15 ~ 20 TPS). 따라서 이더리움 플랫폼 상에서 많은 서비스를 구동시키기에 사실상 불가능한 상황이다.

이더리움 플랫폼의 범용성 때문에 블록체인 기반 서비스를 개발할 때 서비스의 특수한 요구사항을

블록체인에 반영할 수 없다는 문제점이 있다. 그러나 블록체인 기반 서비스를 개발하기 위해 별도로 서비스에 특화된 블록체인 코어를 개발하기에는 배보다 배꼽이 더 큰 형국이다.

본 프로젝트에서는 서비스에 특화된 블록체인 코어가 필요한 개발자들을 위해 Flexible한 블록체인 코어 프레임워크 개발을 구상하였다. 현재 비트코인, 이더리움 등의 블록체인은 오픈소스로서 누구나 하드 포크를 통해 새로운 블록체인을 개발할 수 있다. 그러나 현재 오픈소스화된 블록체인들은 소스코드 간 dependency가 심해서 서비스 별로 특화된 블록체인 코어를 추려내고 특화된 기능을 추가하기 어려운 상황이다. 따라서 Flexible한 블록체인 코어 프레임워크는 블록체인에서 필요한 최소한의 기능만 모듈화하여 단순한 설정만으로 가장 기본적인 블록체인 코어를 구성할 수 있도록 하는 것을 목표로 하였다.

Chainerator는 본 프로젝트를 개발하려면 블록체인에 대한 많은 조사 및 연구가 필요하다고 판단하였다. 따라서 1년 간 합의 알고리즘 부분을 모듈화하여 합의 알고리즘을 단순한 설정에 의해서 변경시킬 수 있도록 하는 프레임워크 개발을 목표로 잡았다. 그리고 전종종합설계 1에서는 합의 알고리즘에 대한 조사 및 연구를 진행하는 한편, Javascript를 이용하여 경량화된 블록체인인 SoongsilCoin을 개발하는 것을 목표로 하였다. 경량화된 블록체인인 SoongsilCoin 개발을 통해 블록체인 코어의 구조를 파악하여 블록체인 코어 모듈화를 위한 기반을 다질 예정이다.

3. 관련 조사 및 연구

합의 알고리즘

1) PoW

비트코인과 이더리움(Ethash)이 PoW 방식의 Consensus 알고리즘을 사용한다. 작업증명 알고리즘을 사용하는 블록체인의 블록 해시는 Difficulty에 따라 선택된 Target 데이터 규격을 만족해야 한다. 블록해시는 해시 알고리즘에 의해 만들어지기 때문에 Target 데이터를 가지고 입력값을 알아낼 수 없다. 즉, 블록체인의 노드는 조건을 만족하기 위해 Nonce라는 임의의 값을 계속 대입한다. 임의로 대입한 Nonce값이 Target 데이터 조건을 만족하면 블록이 성생되는 것이다. 이러한 작업 방식이 의미없을 수 있지만, 이는 네트워크의 모든 노드가 동시에 블록을 만들 수 없게 하는 것이다.

공격자가 악의적으로 블록체인 상의 거래내역을 조작하고자 한다면 컴퓨팅 파워 중 51%의 지분을 확보해야 하며, 이를 51% Attack이라고 한다. 즉, 공격자는 51% 이상의 컴퓨팅 파워를 확보해야 한다. 하지만 최근, 마이닝 풀들이 연합하여 점점 거대해지면서 얼마전 실제로 중국에서 비트코인 마이닝파워의 51%에 근접한 Mining Pool이 등장했다. 즉, 채굴 중앙화 현상이 일어나 신뢰도가 급격히 떨어지게 된 것이다. 또한, 하지만 비트코인 채굴을 위해서 평균 수천조 번 이상의 시도가 필요하여, 비효율적이고 엄청난 전기를 잡아먹는다. 비트코인의 연간 채굴 에너지 소비량은 전세계 전기 소비량 국가 72위인 시리아보다도 높다는 문제가 있다.

2) PoS

Proof of Stake 즉 지분 증명이라는 개념이다. PoW의 가장 큰 문제인 채굴에 들어가는 많은 비용 및 유지비와 채굴의 독점화로 인한 보안상의 문제를 해결하기 위해 만들어진 방식이다.

네트워크 구성원은 지분을 예치하고 지분에 비례한 블록 생성 권한을 얻는다. 해싱파워 51% 이상을 얻는 것 보다, 코인 지분 51%를 구매하는것이 훨씬 어렵고 비용이 비싸다. 이를 통해 복잡한 채굴 없이도 PoW 방식보다 더욱 Decentralized 된 네트워크를 구성할 수 있다. 하지만, 트랜잭션

발생 빈도가 적은 신생 네트워크는 PoS 보상 수익이 너무 적을 뿐더러, 체인이 나뉘었을 경우, 양쪽 모두에게 투표를 해서 합의 알고리즘을 방해하고 수익을 모두 챙기는 Nothing At Stake등의 문제가 발생한다.

3) DPoS

DPOS는 위임된 지분 증명이란 의미로 위의 POS 방식과는 차이가 있다. POS와는 달리 DPOS는 네트워크를 구성하고 있는 모든 노드들의 투표 결과로 정한 Witness라는 상위노드에게 권한을 위임해 대표(마스터 노드)가 합의하도록 한다. 이는 합의 해야 할 노드가 네트워크를 구성하는 모든 노드가 아닌 마스터 노드이기 때문에 합의 시간과 비용을 줄일 수있다. 따라서 PoW나 PoS 방식보다 더 많은 블록을 생성할 수 있다. 하지만 권한이 소수에게 집중되어 있다는 문제가 있다. 또한, 일반 네트워크 참여자에게는 별도의 보상 모델이 없어서 Witness에게 자신의 지분을 위임할 명분이 없다.

4. 프로젝트 시나리오

SoongsilCoin의 시나리오는 다음과 같다.

- SoongsilCoin은 Proof-of-Work (PoW) 합의 알고리즘 방식의 블록체인이다.
- 각각의 노드들이 최신의 블록체인을 업데이트하고 동기화한다.
- Proof-of-Work 합의 알고리즘 방식에 의해 마이닝에 성공한 블록은 블록체인에 새롭게 연결된다.
- 동시에 두 개 이상의 블록이 생성되어 포크가 발생한 경우 마이닝을 어렵게 한 블록에 우선권을 주어 우선권을 부여받은 블록이 연결된 체인을 메인 체인으로 선택하게 된다.
- 블록체인 노드에서 Wallet을 구현하여 지갑 주소에 대한 잔고 확인이 가능하다. 따라서 송금 시 이중 송금이나 보유액 이상의 송금인 부정 송금을 방지한다.

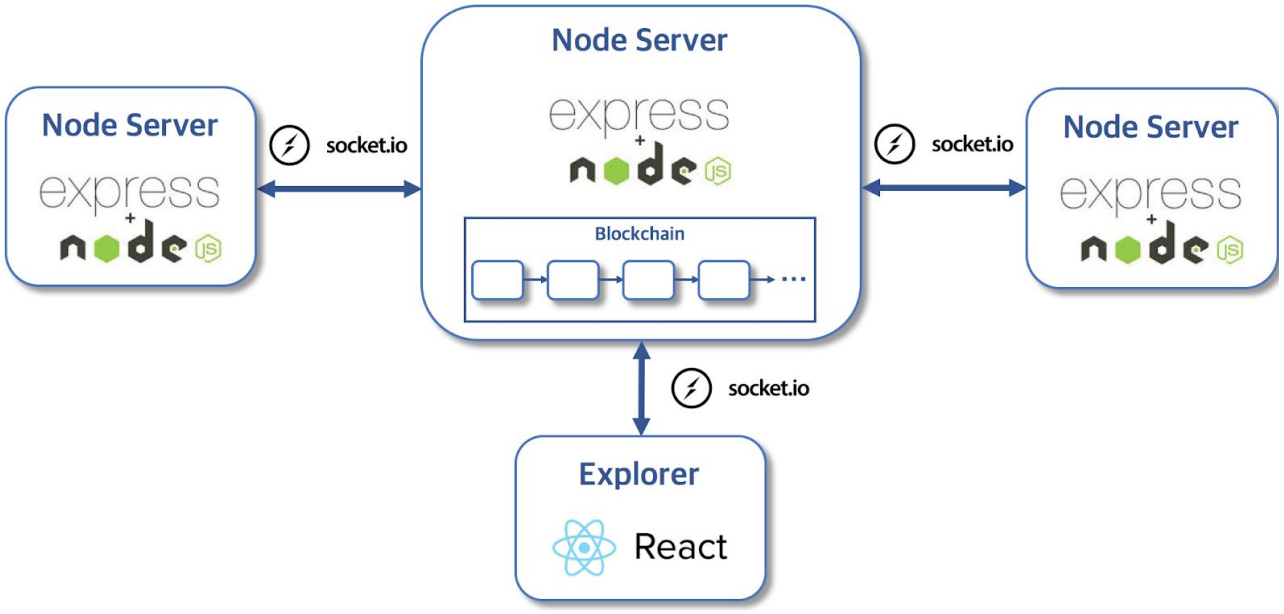
5. 특징 및 차별화

비트코인 코어는 100K 라인이고 과거 버전 바이트코인 코어는 600K 라인으로 매우 무겁다. 그러나 SoongsilCoin에서는 불필요한 소스코드를 제거하고 필수적인 부분만 Javascript를 이용하여 구현하였기 때문에 경량화된 블록체인이라는 점에서 기존 블록체인과 차별성을 갖는다.

6. 프로젝트 개발 범위

1. Node server
2. Consensus algorithm (Mining)
3. Transaction
4. Wallet
5. Explorer

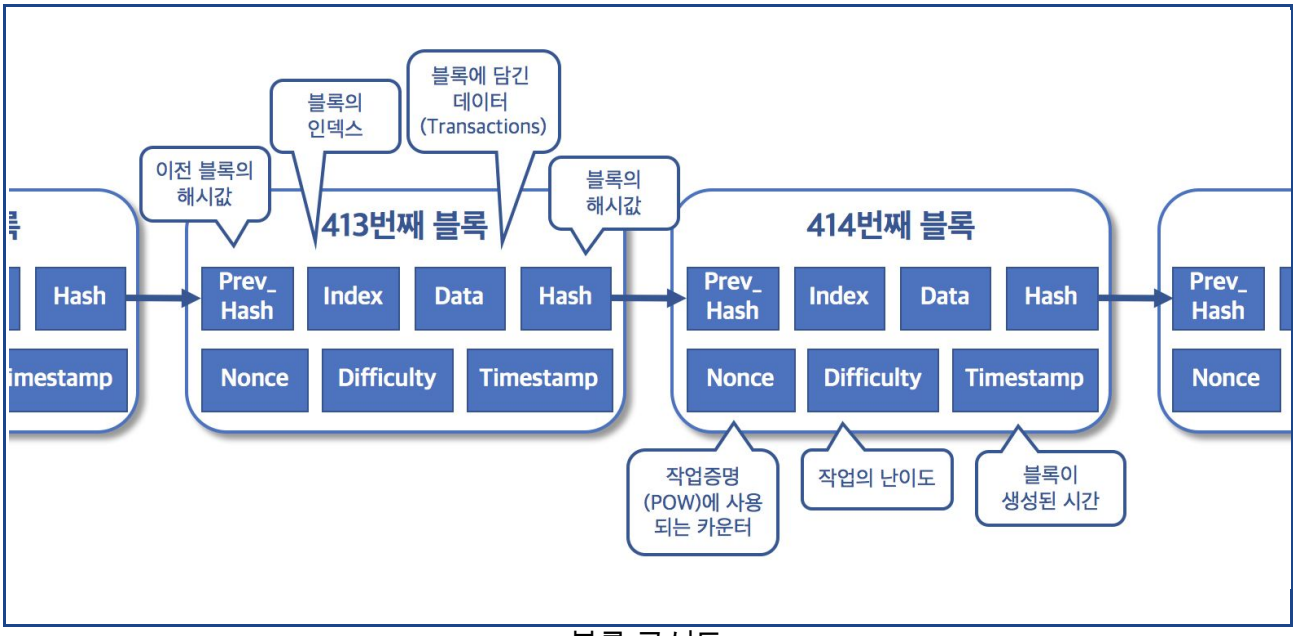
7. 시스템 구성도 - SoongsilCoin



블록체인 시스템 구성도

Node Server들이 P2P 방식으로 서로 연결되어 있고 Explorer를 통해 블록체인의 정보 및 트랜잭션

등을 확인할 수 있다.



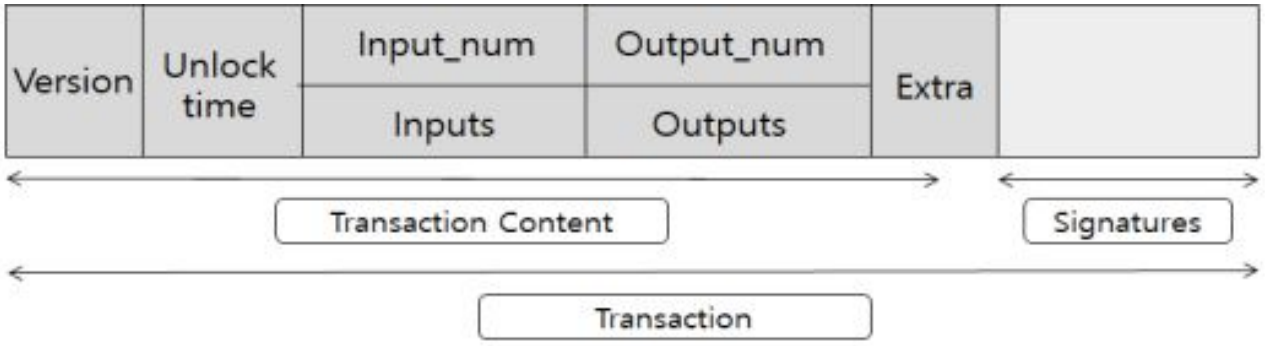
블록 구성도

블록체인에서 블록은 트랜잭션의 집합이다. 블록에는 트랜잭션 뿐만 아니라 블록체인을 구성하기 위한 다양한 요소들이 포함되어 있다.

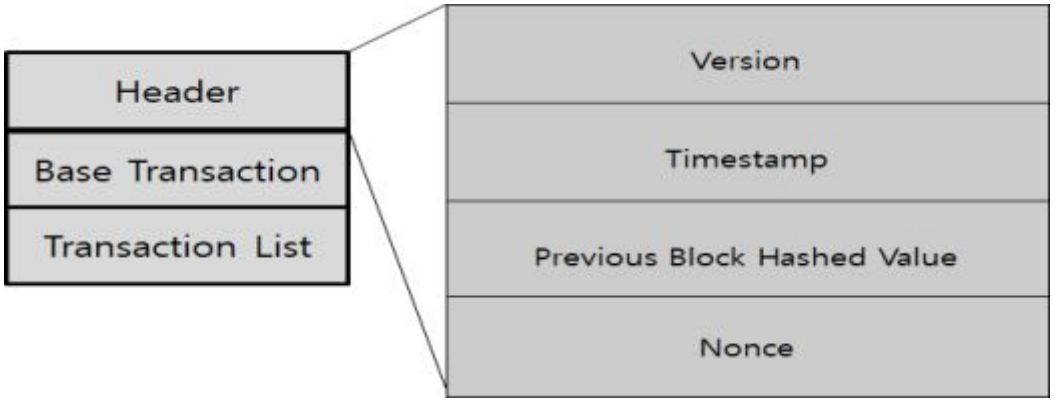
- Prev_Hash : 이전 블록의 해시값이다. 블록들은 이전 블록의 해시값을 저장하는 방식으로 현재 블록과 이전 블록을 연결하여 블록체인을 구성한다.
- Index : 현재 블록 인덱스(또는 높이)를 나타낸다.
- Data : 블록에 담길 데이터인 트랜잭션을 의미한다.
- Hash : 블록의 해시값으로 다음 블록의 이전 블록의 해시값에 저장된다.
- Nonce : POW에서 사용되는 카운터이다.
- Difficulty : 작업 난이도를 나타낸다. 블록이 일정 주기 별로 생성되어야 하므로 일정 주기를 조절하기 위해 작업 난이도를 설정한다.
- Timestamep : 블록이 생성된 시간을 의미한다.

8 . 시스템 구성도 - Flexible Blockchain Core Framework

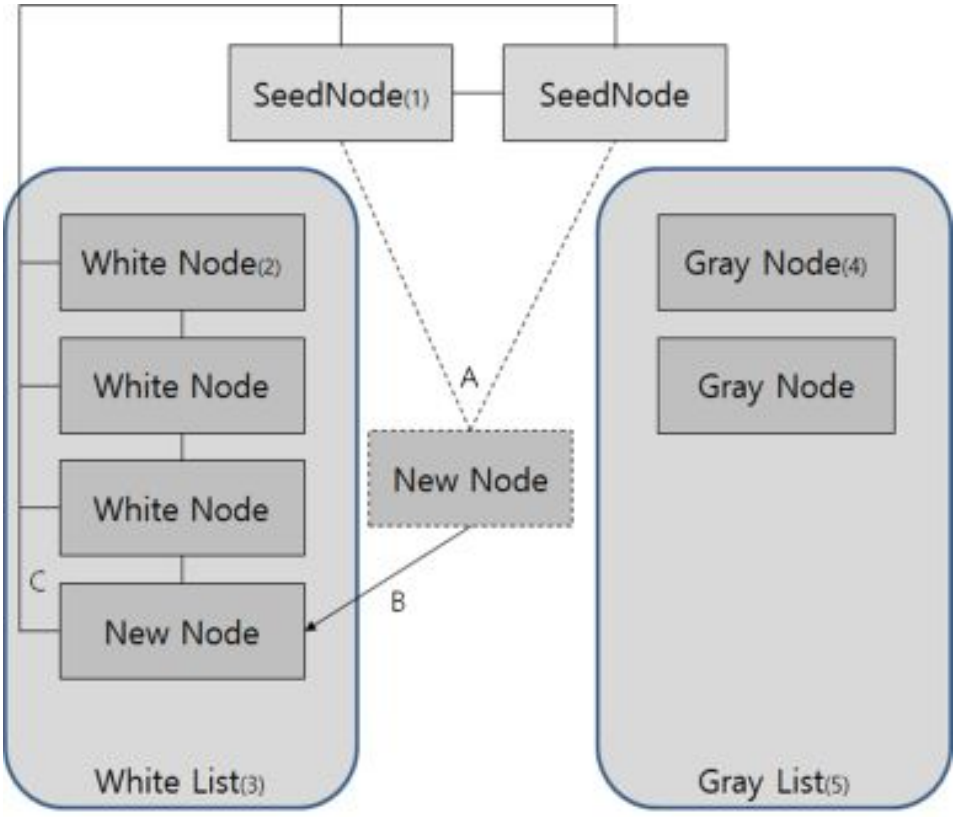
Flexible Blockchain Core Framework 설계는 다음과 같다.



트랜잭션 구조



블록 구조



P2P 네트워크 구조

1) Seed Node

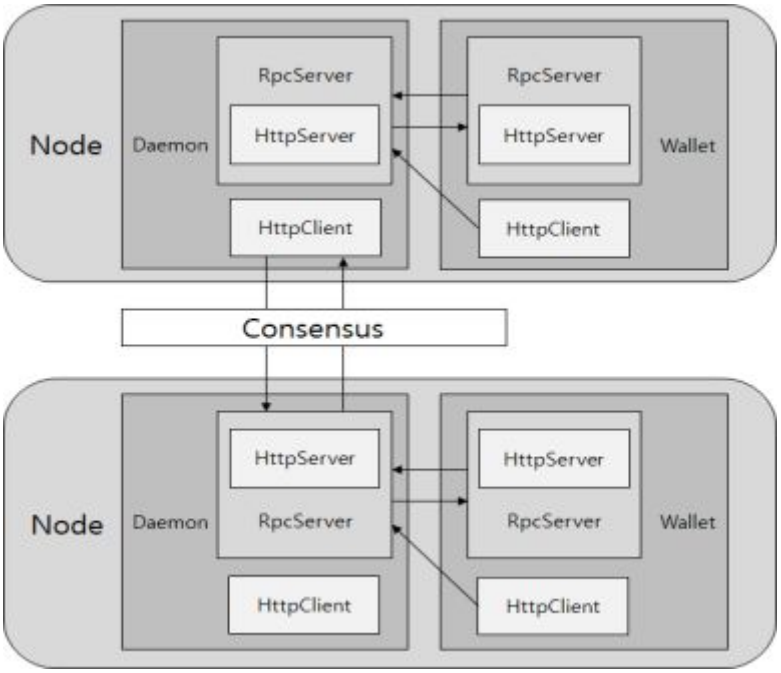
SeedNode는 네트워크에서 첫 번째 노드이다. 다른 노드들이 처음 연결될 때 이 노드에 연결된다.

2) White Node

P2P 네트워크에 연결되어 운영 중인 노드이다.

3) Gray Node

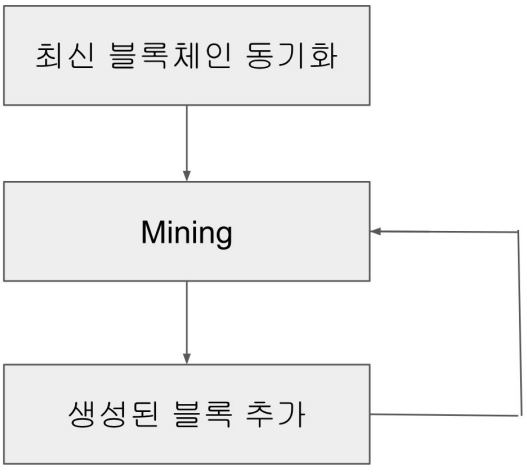
P2P 네트워크에 구성원인 노드이지만 현재 연결되어 있지 않는 노드이다. 노드의 연결이 끊어지는 시점에 White List를 저장한다.



블록체인 네트워크 구조

- 각 노드에는 RPC 서버와 HTTP 서버를 사용하여 외부 노드 및 프로세스와 통신하는 데몬과 월렛이 있다.
- 노드와 프로세스 간에 통신을 할 때 demander는 JSON으로 작성된 신호와 메소드 실행 요청을 요구하고 이에 따라 State 값 또는 JSON 결과를 수신한다.

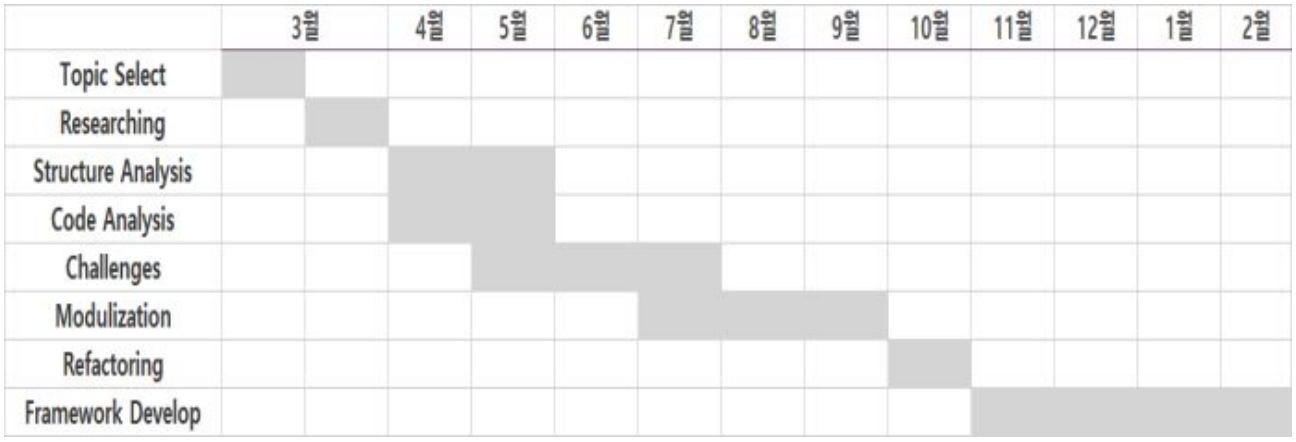
9. Flow Chart



마이너 입장에서 나타낸 Flow Chart이다. 노드가 P2P 네트워크에 참가하면 최신 블록체인으로 동기화하여 저장한다. 마이닝을 통해 다른 노드가 블록을 생성하든, 내가 블록을 생성하든 생성된 블록을 블록체인에 추가하고 다시 새로운 블록 생성을 위해 마이닝을 진행한다.

10. Time Table

Flexible Blockchain Core 개발을 위한 일정을 기준으로 Time Table을 구성하였다.



Time Table에 기반하여 지금까지의 진행 상황은 다음과 같다.

- Topic Select
    - 익명성 프로토콜 기반 퍼블릭 블록체인 개발
    - Flexible Blockchain Core Framework 개발
    - 위 두 가지 프로젝트 주제 중에서 Flexible Blockchain Core Framework를 프로젝트 주제로 선택
- Researching
    - Blockchain Core Framework가 실제로 존재하는지 조사 진행
    - Cryptonote라는 블록체인을 발견하였지만 개발이 중단되었고 명세서가 부실해서 프레임워크로서 제 기능을 하고 있지 못한다는 사실을 발견함
    - Cryptonote를 분석하여 Flexible Blockchain Core Framework를 개발할 것을 목표로

함

- Structure Analysis
    - Flexible Blockchain Core Framework는 블록체인 최소한의 핵심 기능만 추려 이 기능들을 모듈화하여 단순한 설정만으로 기본적인 블록체인 코어를 생성할 수 있도록 지원하는 것을 목표로 함
    - Cryptonote 구조 분석을 통해 위와 같은 목표를 도출함
- Code Analysis
    - Cryptonote 소스코드 분석을 통해 최소 기능을 파악하려고 시도함
    - 그러나 블록체인 소스코드를 완벽히 이해하기에는 아직 블록체인에 대한 지식 베이스가 부족하다고 판단하여 리서치 중심으로 프로젝트 진행 방향을 선회
- Challenges
    - 경량화된 블록체인인 SoongsilCoin을 구현하여 Flexible Blockchain Core Framework 개발을 위한 기반을 다짐

Time Table에 기반하여 앞으로의 계획은 다음과 같다.

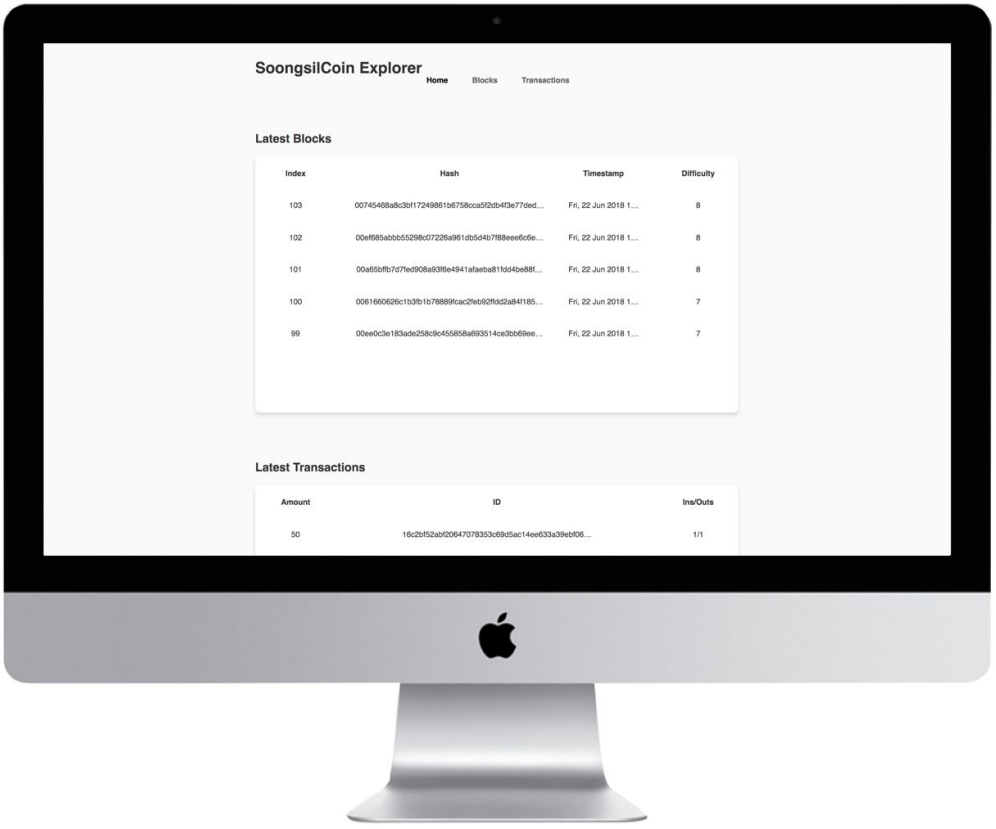
- Challenges
    - SoongsilCoin에서 합의 알고리즘 부분을 모듈화하여 PoW, PoS, DPoS 등으로 선택하여 블록체인을 생성할 수 있도록 개선
- Modulization
    - 지금까지 리서치를 통해 축적해왔던 블록체인에 대한 지식을 바탕으로 Cryptonote를 분석한 뒤 Cryptonote를 하드 포크하여 모듈화 구현 진행
- Refactoring
    - 모듈화 마무리 및 리팩토링
- Framework Develop
    - 설정만으로도 간단하게 블록체인 코어를 생성할 수 있도록 프레임워크 개발
    - 블록체인 코어를 생성하려는 사용자가 편하게 설정할 수 있도록 GUI도 구현

11. 사용기술

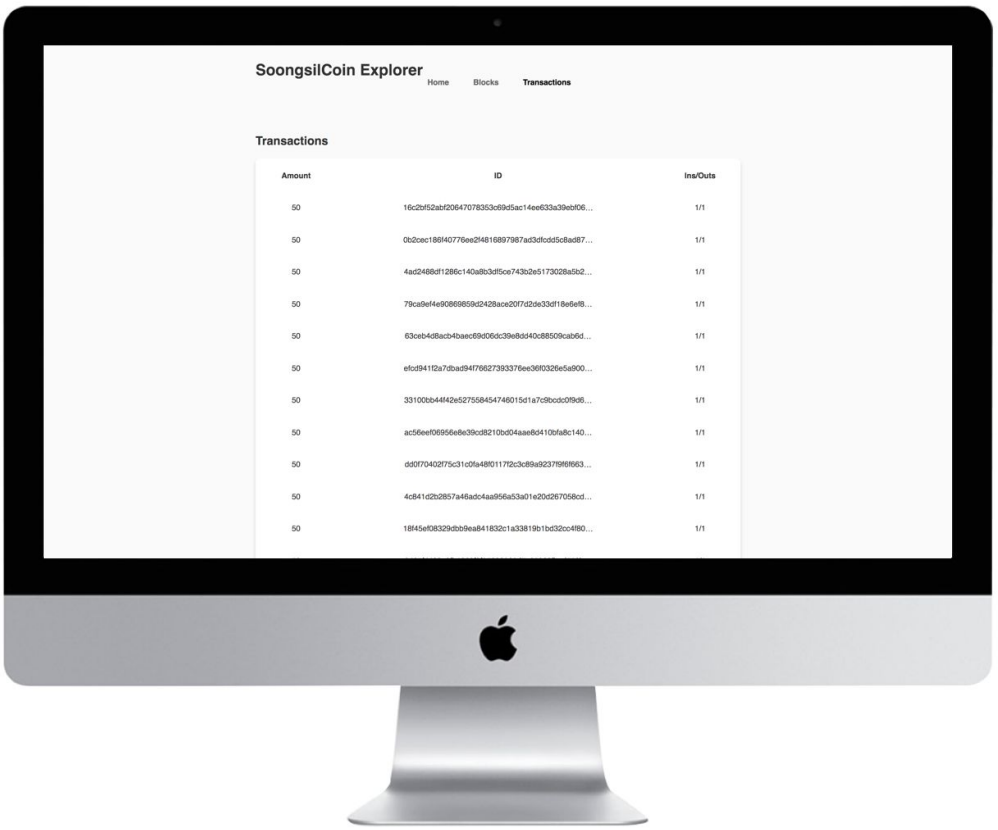
- Development Environment
    - macOS High Sierra (v 10.13.3)
- IDE
    - Visual Studio Code
- Programming Language
    - JavaScript
- Framework
    - Node.js / Express
    - React

12. 실제 화면

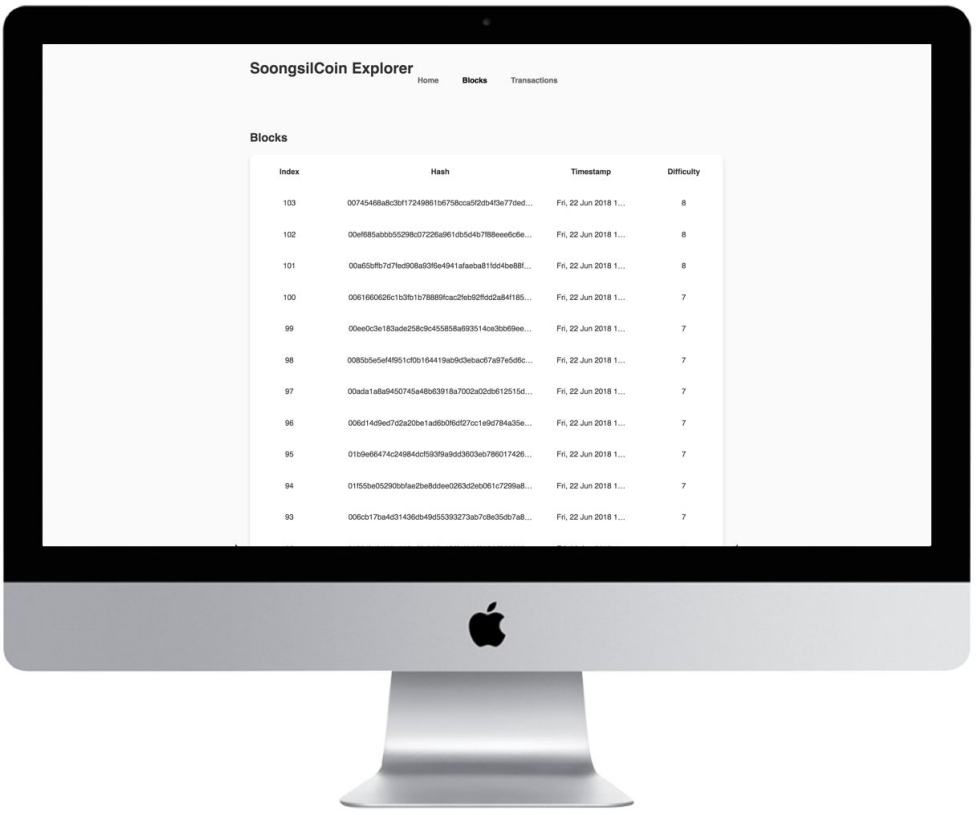
Explorer를 통해 블록체인 및 트랜잭션의 정보를 확인할 수 있다.



최근 블록의 정보 확인


SoongsilCoin Explorer
Home
Blocks
Transactions
Transactions
Amount
ID
Ins/Outs
50
16c2bf52abf20647078353c69d5ac14ee633a39ebf06…
1/1
50
0b2cec186f40776ee2f4816897987ad3dfcdd5c8ad87…
1/1
50
4ad2468df1286c140a8b3df5ce743b2e5173028a5b2…
1/1
50
79ca9ef4e90869859d2428ace20f7d2de33df18e6ef8…
1/1
50
63ceb4d8acb4baec69d06dc39e8dd40c88509cab6d…
1/1
50
efcd9411f2a7dbadf94f76627393376ee36f0326e5a900…
1/1
50
33100bb44f42e527558454746015d1a7c9bcdc0f9d6…
1/1
50
ac56eef06956e6e39cd8210bd04aae6d410bfa8c140…
1/1
50
dd0f70402f75c31c0fa48f0117f2c3c89a9237f5f6f663…
1/1
50
4c841d2b2857a46adc4aa956a53a01e20d267058cd…
1/1
50
18f45ef08329dbb9ea841832c1a33819b1bd32cc4f80…
1/1

트랜잭션의 정보 확인



블록들의 정보 확인

11. 기대효과 및 활용분야

기대효과

- Flexible Blockchain Core Framework 개발을 위한 가장 기본적인 코드 구현 완료
- 기존 비트코인, 이더리움과는 달리 경량화된 소스코드로 구현하여 SoongsilCoin을 통해 블록체인의 핵심 기능을 파악할 수 있음
- 블록체인 코어 자체를 개발해봄으로써 블록체인의 구동 과정을 이해할 수 있음
- Explorer를 통해 블록체인과 관련된 정보를 한눈에 확인할 수 있음
- Cryptonote를 분석하는데 기본적인 이해도를 높임
- Cryptonote를 이용하여 모듈화를 진행하기 전에 경량화된 블록체인에서 합의 알고리즘 모듈화를 진행해봄으로써 모듈화의 실현 가능성을 체크해볼 수 있음

활용분야

- 블록체인 코어를 입문하고자 하는 개발자들에게 좋은 학습 자료로 활용될 수 있음
- 기존 블록체인보다 경량화된 소스코드를 가지고 있기 때문에 다양한 기능을 수행하지는 못하지만 블록체인의 원리를 파악하기 위해 블록체인을 돌려보려고 할 때는 소스코드가 가벼워서 빠르게 다운로드 받아서 실행시켜 볼 수 있음
- JavaScript 기반으로 개발을 하였기 때문에 JavaScript들의 다양한 라이브러리들을 활용하여 SoongsilCoin를 발전시킬 수 있는 가능성을 가지고 있음