숭실대학교 Soongsil University

설계보고서 제출서약서

나는 숭실대학교 컴퓨터학부의 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.

교 과 목	전공종합설계 1
프로젝트 명	Chainerator
교과목 교수	이상준 교수님
제 출 인	컴퓨터학부 4 학년 신재철(20132142) 컴퓨터학부 4 학년 홍상원(20142577) 소프트웨어학부 4 학년 정구익(20150271) 소프트웨어학부 4 학년 하현수(20150291)
제 출 일	2018년 4 월 10 일 (화)

A Table of Content

1. 프로젝트 소개

블록체인은 중앙 서버 없이 모든 노드가 피어(Peer)로 참여하는 퓨어 P2P 네트워크 기반의 분산 원장 기술이다. 모든 노드가 합의를 기반으로 참여하게 되어 원장의 위·변조를 사전에 방지할 수 있고, 중앙화된 서버가 존재하지 않기 때문에 탈중앙화(Decentralization)라는 특성을 가지고 있다.

이러한 특성 때문에, 다양한 서비스에 블록체인을 접목하려는 시도가 늘고 있다. 다양한 서비스들의 각 목적에 맞는 블록체인을 처음부터 설계 및 구축하는 것은 많은 시간이 소요되기 때문에 대다수 업체는 기존 프로젝트를 수정하여 자체 블록체인을 구축한다. 그렇지만 기존 블록체인의 경우 블록생성시간, 블록사이즈 등의 블록체인 속성값들이 코드 전역에 분산되어 있을뿐더러 수정을 고려하지 않고 고정되어 있어 수정 시 코드 의존성 등의 문제가 발생할 수 있기 때문에 효율적인 개발이 어렵다. 또한, P2P 네트워크의 구조를 피어에게 알려주는 역할을 하는 Seednode의 주소값이 고정되어 있어 블록체인의 속성값을 바꾸더라도 자체 네트워크로 분리시키기 어렵다.

위와 같은 문제를 해결하기 위해서 기존 블록체인 코드를 기능 단위로 모듈화하고, 블록체인 속성값들을 설정 파일 한곳으로 통합시켜 보다 효율적인 수정을 할 수 있도록 하고, Seednode의 주소값 또한 수정 가능할 수 있도록 한다.

2. 기존시스템 분석

- Bitcoin

Bitcoin은 2008년 사토시 나카모토의 논문 “Bitcoin : A Peer to Peer Electronic Cash System”에 최초 기술됐던 블록체인 기술을 이용하여 2009년 개발된 최초의 암호화폐이다. 오픈 소스로 공개되어 있지만, 상수와 변수값의 수정이 제한되어 있어 수정 시 Assert에 의해 컴파일 에러가 발생하기 때문에 유연한 수정이 어렵다. 또한, 모듈화가 잘 되어있지 않아 소스코드 분석에 시간이 오래 걸린다는 단점이 있지만 그럼에도 불구하고 가장 많은 블록체인들의 모체가 되었다.

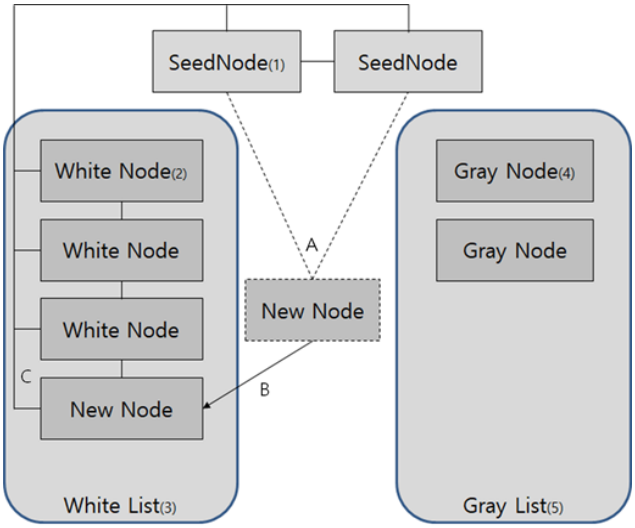
- Litecoin

Litecoin은 MIT의 Charlie Lee가 개발한 Bitcoin 기반의 암호화폐로 해싱함수를 SHA-256에서 Scrypt로 바꾸고, 블록사이즈와 최대 발행 수량을 늘린 블록체인 프로젝트이다. 블록체인 속성값 수정을 위해 Bitcoin의 Assert문장을 제거하여 최대 발행량, 해싱 방식, 블록사이즈, 블록 생성 시간 등의 블록체인 속성값을 비교적 플렉서블하게 수정 할 수 있게 되었다는 의의가 있다.
하지만 모듈화가 충분히 진행되지 않아 컨센서스 방식과 같은 큰 틀에서의 변화를 위해서는 기존 소스 코드를 새롭게 고치고 의존성을 검사하며 수정해야 한다는 점에서 여전히 Bitcoin 기반 방식의 한계점이 존재한다.

- Bytecoin

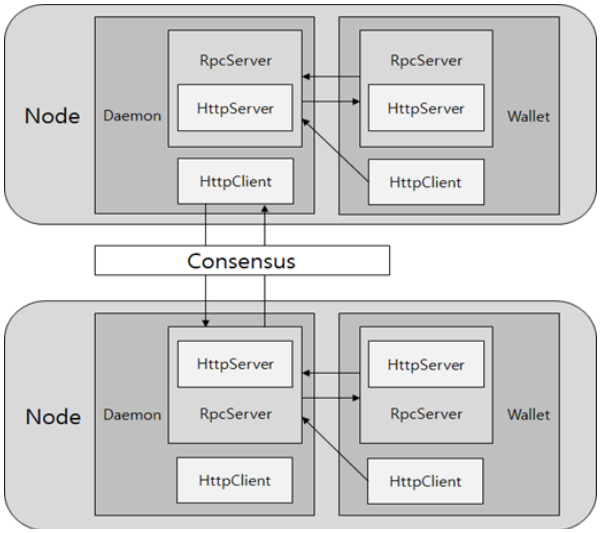
Bytecoin은 Cryptonote 기술 기반의 최초 익명성 코인으로 Cryptonight 알고리즘을 사용하였으며 링 서명을 이용하여 익명성과 정보 보호를 강조하며 등장하였다. Bitcoin 기반 블록체인과 전혀 관련이 없는 최초의 독립 블록체인이기도 하다. Cryptonote라고 하는 자체 블록체인 코어 기술을 통해 만들어졌으며, 비교적 쉽게 블록체인 속성값을 수정할 수 있지만 소스코드 길이가 Bitcoin보다 훨씬 방대하고 모듈화가 진행되지 않아 소스 분석이 아주 복잡하며, 블록체인의 속성값 변경은 간단하더라도 자체 블록체인의 P2P 네트워크를 분리해내는 것이 어렵다
는 단점이 있다.

3. 《Chainerator》 구상도



< P2P Network >

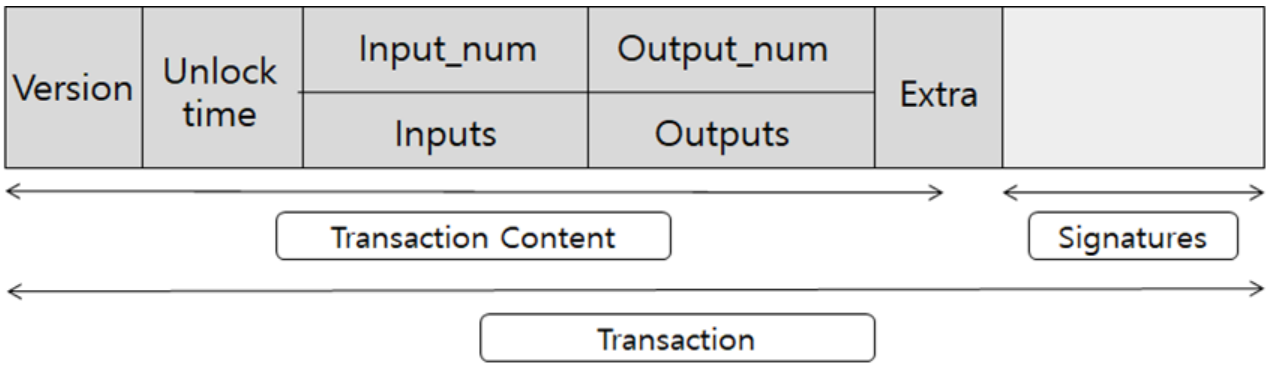
- Seednode는 네트워크의 첫 번째 노드이며 다른 노드들은 처음 연결 시 해당 노드에 먼저 연결되어 현재 네트워크에 참여하고 있는 노드들의 항목을 받아 항목의 노드들과 연결된다.
- White Node는 현재 네트워크에 P2P연결되어 현재 동작 중인 노드를 의미하며 의들의 집합을 White List라고 한다. White List는 새로운 노드가 연결될 때 Seednode에서 전달되는 정보이다.
- Gray Node는 블록체인 네트워크에 참여하였지만, 현재는 연결이 종료된 노드를 의미하며 각 Gray Node는 종료 당시의 White List를 갖고 있다. 또한 이들의 집합을 Gray List라 한다.



< Blockchain Network >

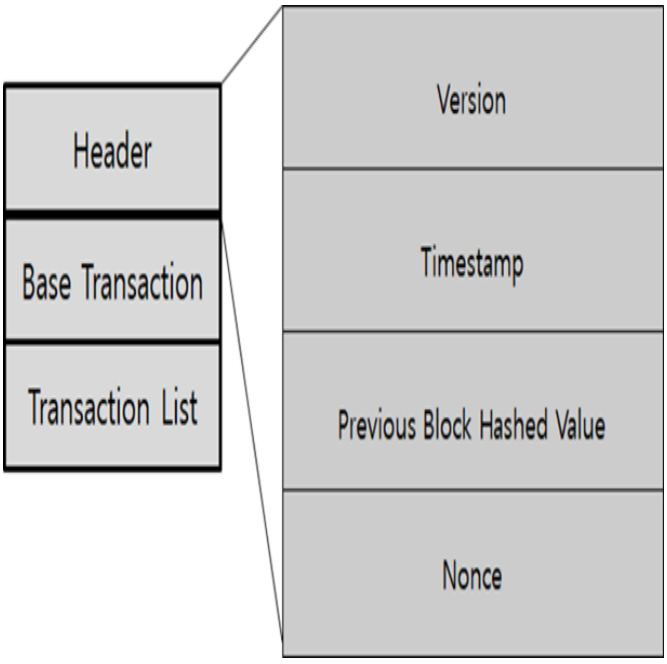
- P2P 네트워크를 구성하는 각 노드내에는 데몬과 지갑 프로세스가 동작하고 있으며 RPC 서버와 HTTP 서버를 사용하여 외부 노드 및 다른 프로세스와 통신을 진행한다.
- 위와 같은 통신 방식을 통해 동기화 과정 및 합의 알고리즘에 의한 합의를 통한 블록 생성 등의 과정을 진행하게 된다.

4. 《Chainerator》 설계



< 트랜잭션 설계 >

트랜잭션 설계 구조는 위와 같으며, 비트코인의 트랜잭션 구조를 참고하여 가장 일반적으로 사용되는 구조로 설계하여 호환성을 높였다. UnlockTime에는 UNIX의 시간정보인 Timestamp를 기록하며, Inputs에는 트랜잭션 소유권에 대한 키 정보와 Block Height가, Outputs에는 전송될 코인의 수량과 송금 주소정보가 저장된다.

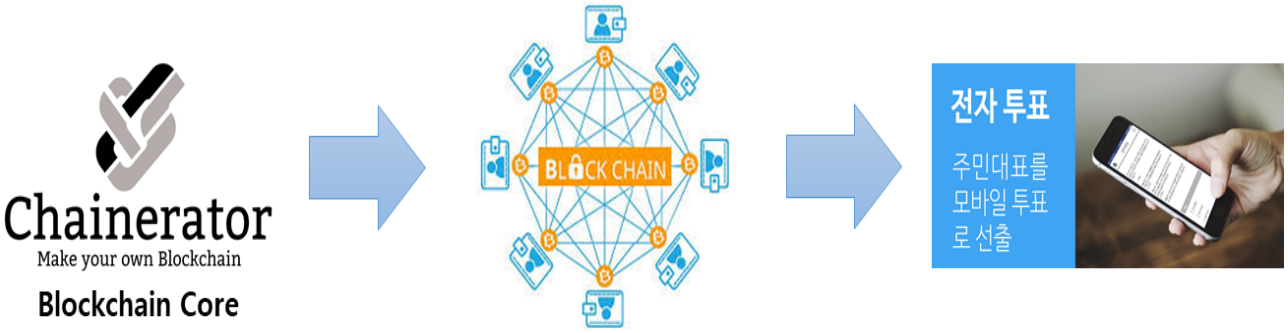


< 블록 구조 설계 >

- 블록헤더는 버전과 UNIX기반의 Timestamp, 이전 블록의 해시값, 작업증명을 위한 Nonce로 구성되어 있으며 이러한 값들을 통해 위·변조를 파악할 수 있다.
- Base Transaction은 채굴 보상을 받을 계정을 식별하기 위한 블록에 생성된 최초 트랜잭션인 블록 생성 트랜잭션 정보를 저장하고 있다.
- Transaction List는 해당 블록에 포함된 트랜잭션들의 TxHash값이 리스트 형태로 각각 저장된다.

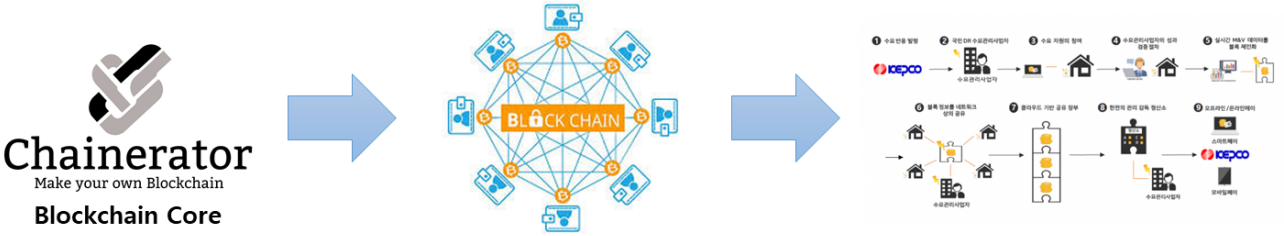
5. 《Chainerator》 시나리오

Chainerator를 이용한 블록체인 전자 투표 플랫폼 개발



Chainerator를 이용한 블록체인 무역 플랫폼 개발

Chainerator를 이용한 블록체인 에너지 거래 플랫폼 개발



6. 《Chainerator》기반의 SoongSilCoin 구현

6-1. 프로젝트 시나리오

- 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.

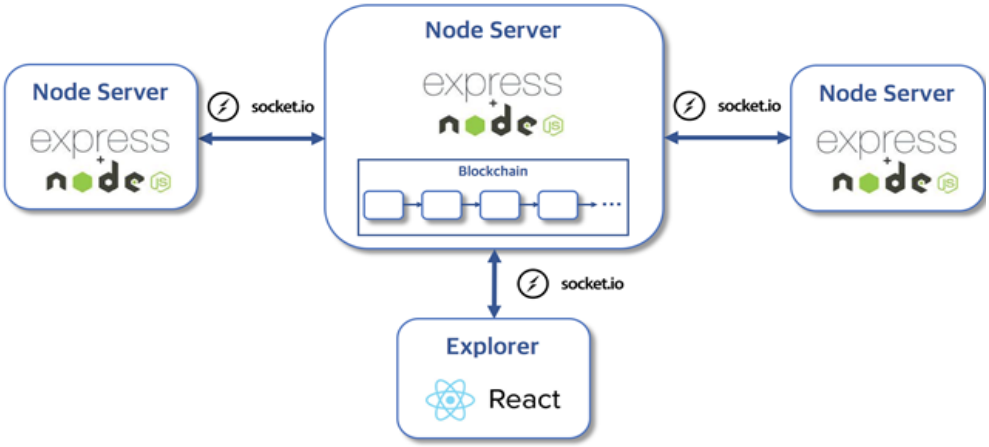
6-2. 특징 및 차별화

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.

6-3. 프로젝트 개발 범위

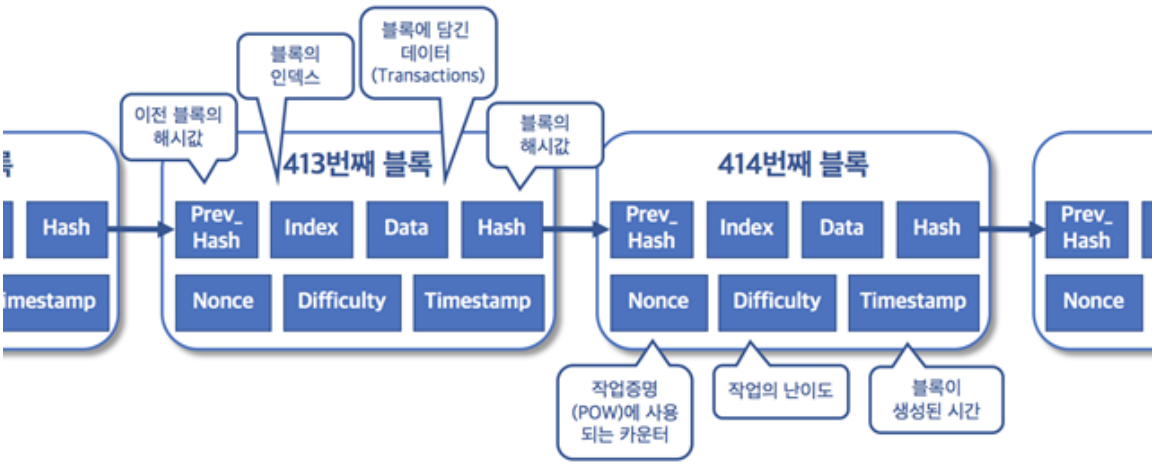
- Node server
- Consensus algorithm (Mining)
- Transaction
- Wallet
- Explorer

6-4. 시스템 구성도



< 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.
- Timestamp : 블록이 생성된 시간을 의미한다.

7. 관련연구

- P2P Network (Peer - to - Peer Network)

동등 계층간 통신망라고도 불리는 P2P는 비교적 소수의 서버에 집중하기보다는 망구성에 참여하는 기계들의 계산과 대역폭 성능에 의존하여 구성되는 통신망이다. P2P 통신망은 일반적으로 노드들을 규모가 큰 애드혹으로 서로 연결하는 경우 이용된다. 이런 통신망은 여러 가지로 쓸모가 있는데, 오디오나 비디오, 데이터 등 임의의 디지털 형식 파일의 공유는 매우 보편적이다. 또한, 인터넷 전화(VoIP)같은 실시간 데이터 등도 P2P 기술을 통해 서로 전달될 수 있다.

- Blockchain

관리 대상 데이터를 '블록'이라고 하는 소규모 데이터들이 P2P 방식을 기반으로 생성된 체인 형태의 연결고리 기반 분산 데이터 저장환경에 저장되어 누구라도 임의로 수정할 수 없고 누구나 변경의 결과를 열람할 수 있는 분산 컴퓨팅 기술 기반의 데이터 위변조 방지 기술이다. 이는 근본적으로 분산 데이터 저장기술의 한 형태로, 지속적으로 변경되는 데이터를 모든 참여 노드에 기록한 변경 리스트로서 분산 노드의 운영자에 의한 임의 조작이 불가능하도록 고안되었다. 잘 알려진 블록체인의 응용 사례는 의 거래과정을 기록하는 탈중앙화된 전자장부로서 이 있다. 이 거래 기록은 의무적으로 되고 블록체인 소프트웨어를 실행하는 컴퓨터상에서 운영된다. 비트코인을 비롯한 대부분의 암호화폐들이 형태에 기반하고 있다.

- RPC (Remote Procedure Call)

별도의 원격 제어를 위한 코딩 없이 다른 주소 공간에서 함수나 프로시저를 실행할 수 있게하는 프로세스 간 통신 기술이다. 다시 말해, 원격 프로시저 호출을 이용하면 프로그래머는 함수가 실행 프로그램에 로컬 위치에 있든 원격 위치에 있든 동일한 코드를 이용할 수 있다.

- POW (Proof Of Work)

블록체인의 대표적인 합의 알고리즘으로, 채굴기를 사용하여 특정 Nonce값을 찾아 블록을 생성하고 보상을 받아가는 형태이다. 해시파워를 51% 이상을 차지할 경우, 51% Attack을 통해 블록체인의 신뢰성을 무너뜨릴 수 있다는 취약점이 존재한다.

- POS (Proof Of Stake)

채굴방식을 사용하지 않는 지분증명이라는 합의 알고리즘으로, 네트워크 참여자가 자신의 블록체인 코인 지분을 위임함으로써 투표권을 가지게되고, 블록 생성에 대한 검증을 투표로 진행한다. 하지만 네트워크 참여자들이 자신의 이익을 최대화 시키기 위해서 여러 블록후보에 분배하여 투표하는 Nothing At Stake 문제로 인해 네트워크 신뢰성이 떨어질 수 있다.

8. 기대효과 및 활용분야

기대효과

- 코드 의존성과 같은 문제를 생각하지 않고 복잡한 코딩 없이 Public Blockchain 플랫폼을 구현할 수 있다.
- 모듈화 시켰기 때문에 코드를 이해하는 데에 어려움이 크게 줄 것이고 이해도 또한 증가할 것이다.
- Consensus 방식을 모듈화 하기 때문에 POW, POS등의 합의 알고리즘에 상관없이 다양한 블록체인 플랫폼을 개발할 수 있다.
- 불필요한 기능 및 블록체인을 위한 기능외에 서비스를 위한 기능을 제거하기 때문에 순수한 블록체인 코어로만 구성되기 때문에 블록체인 코어 학습을 위해 사용이 가능하다.

활용분야

- **전자 투표**

  블록체인의 투명성과 위변조가 불가능하다는 특성을 활용하여 전자투표 시스템에 적용시킬 수 있다. 블록체인을 사용함으로써, 신뢰성이 보장되는 전자투표를 진행할 수 있으며, 이용자들은 자신의 투표가 정상적으로 반영되었는지 확인할 수 있고, 개표 또한 간편히 진행할 수 있다.

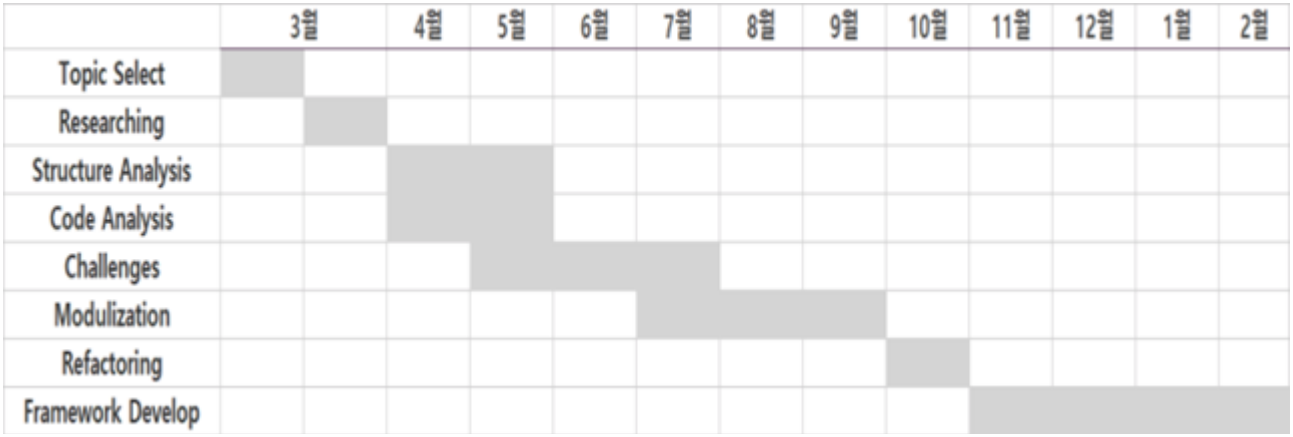
- **무역**

  블록체인의 분산원장을 활용하여 무역 인프라에 적용할 경우, 중간 과정을 블록체인을 통해 간소화함으로써, 중간과정에서 생성되는 선하증권, 운송장 등의 무역관련서류들을 보다 효율적으로 관리할 수 있고 비용적 절감효과도 얻을 수 있으며, 값비싼 송금수수료 없이 대금을 지불할 수 있다.

- **에너지 거래**

  전기등의 에너지를 블록체인을 활용하여 개인과 개인이 P2P로 사고팔 수 있다. 이 또한 중간과정이 사라지므로 비용적 절감효과를 가질 수 있고, 한전등의 중앙기관을 거치지 않아 개인이 P2P로 보다 저렴한 가격에 에너지를 거래할 수 있다.

9. 개발로드맵



- 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
  - Cryptonote를 분석하여 Flexible Blockchain Core Framework를 개발할 것을 목표

- Structure Analysis
  - Flexible Blockchain Core Framework는 블록체인 최소한의 핵심 기능만 추려 이 기능들을 모듈화하여 단순한 설정만으로 기본적인 블록체인 코어를 생성할 수 있도록 지원하는 것을 목표

- Code Analysis
  - Cryptonote 소스코드 분석을 통해 최소 기능을 파악

- Challenges
  - Flexible Blockchain Core Framework를 기반으로 하여 경량화된 블록체인인 SoongsilCoin을 구현

10. Reference

1. Satoshi Nakamoto, &Bitcoin A Peer-to-Peer Electronic Cash System,& bitcoin.org, 2009
2. Nicolas van Saberhagen. &CryptoNote v 2.0& (White Paper),& cryptonote.org, 2013
3. https://ko.wikipedia.org/wiki/P2P
4. https://ko.wikipedia.org/wiki/Blockchain
5. https://ko.wikipedia.org/wiki/RPC