프로젝트 최종요약보고서

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>

2. 프로젝트 목적

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. 프로젝트 시나리오

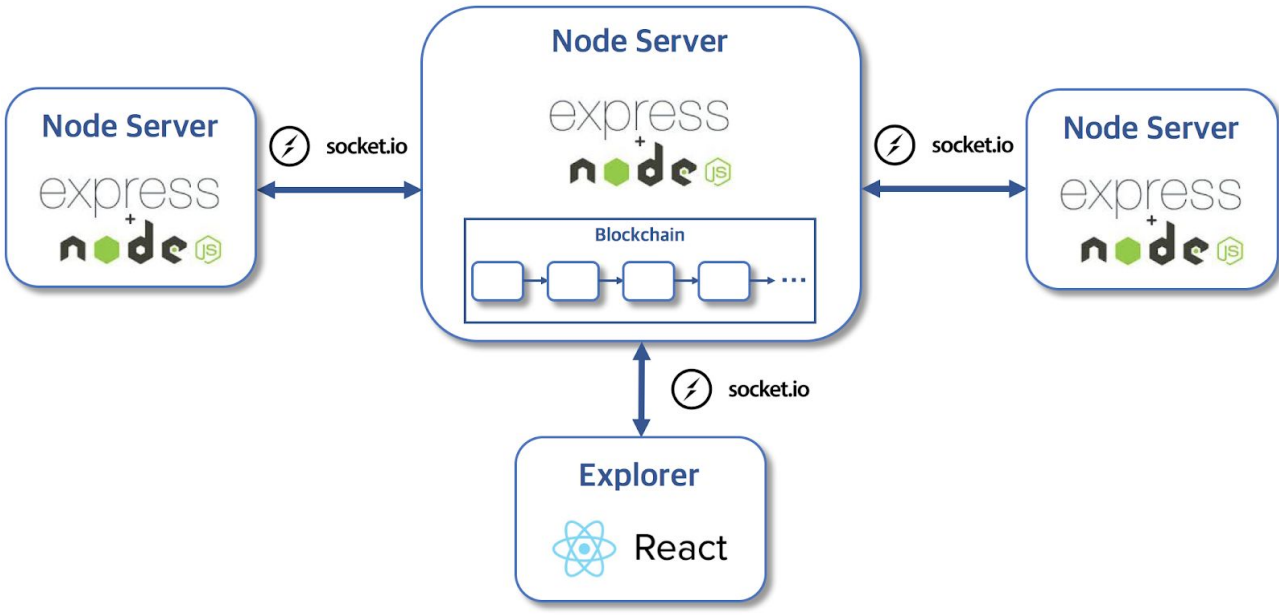
SoongsilCoin의 시나리오는 다음과 같다.

- 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.

4. 프로젝트 개발 범위

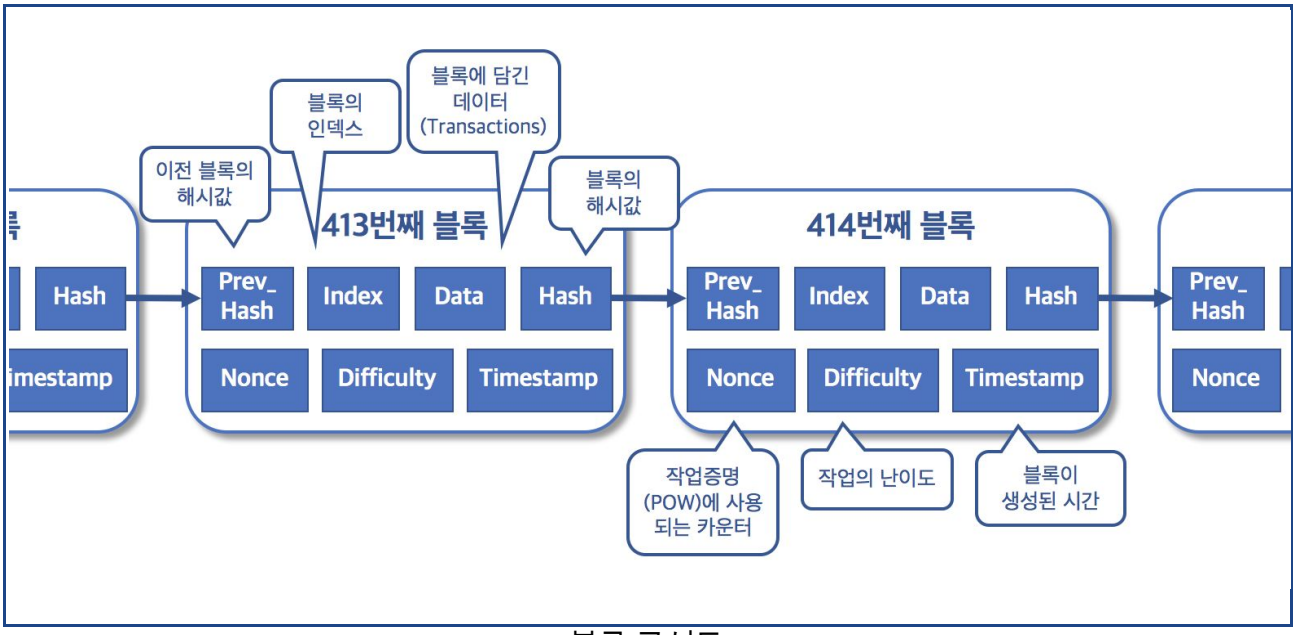
1. Node server
2. Consensus algorithm (Mining)
3. Transaction
4. Wallet
5. Explorer

5. 시스템 구성도 - SoongsilCoin



블록체인 시스템 구성도

Node Server들이 P2P 방식으로 서로 연결되어 있고 Explorer를 통해 블록체인의 정보 및 트랜잭션 등을 확인할 수 있다.

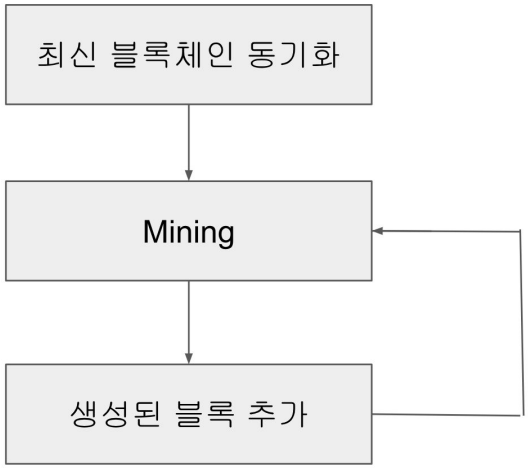


블록 구성도

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.

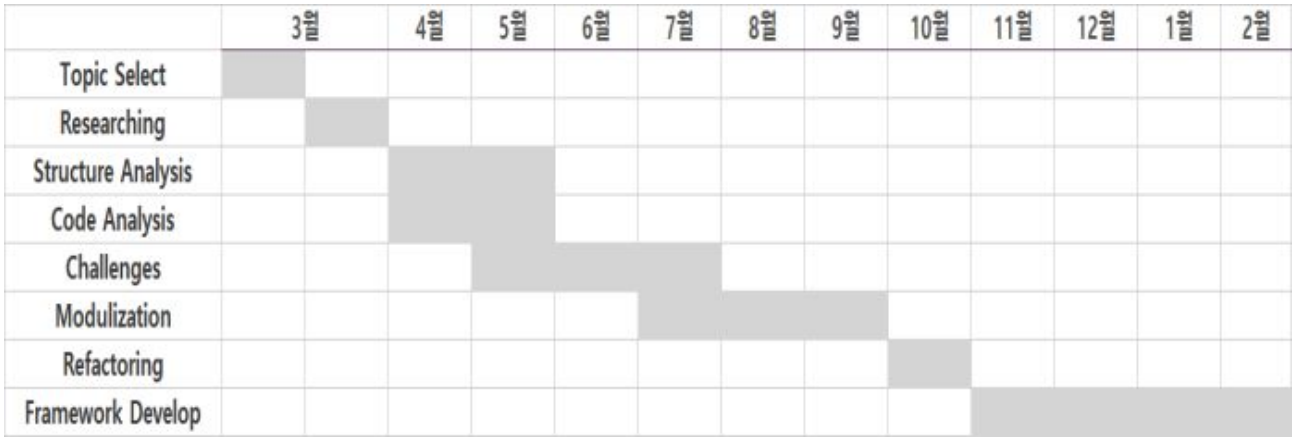
6. Flow Chart



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.

7. Time Table

Flexible Blockchain Core 개발을 위한 일정을 기준으로 Time Table을 구성하였다.

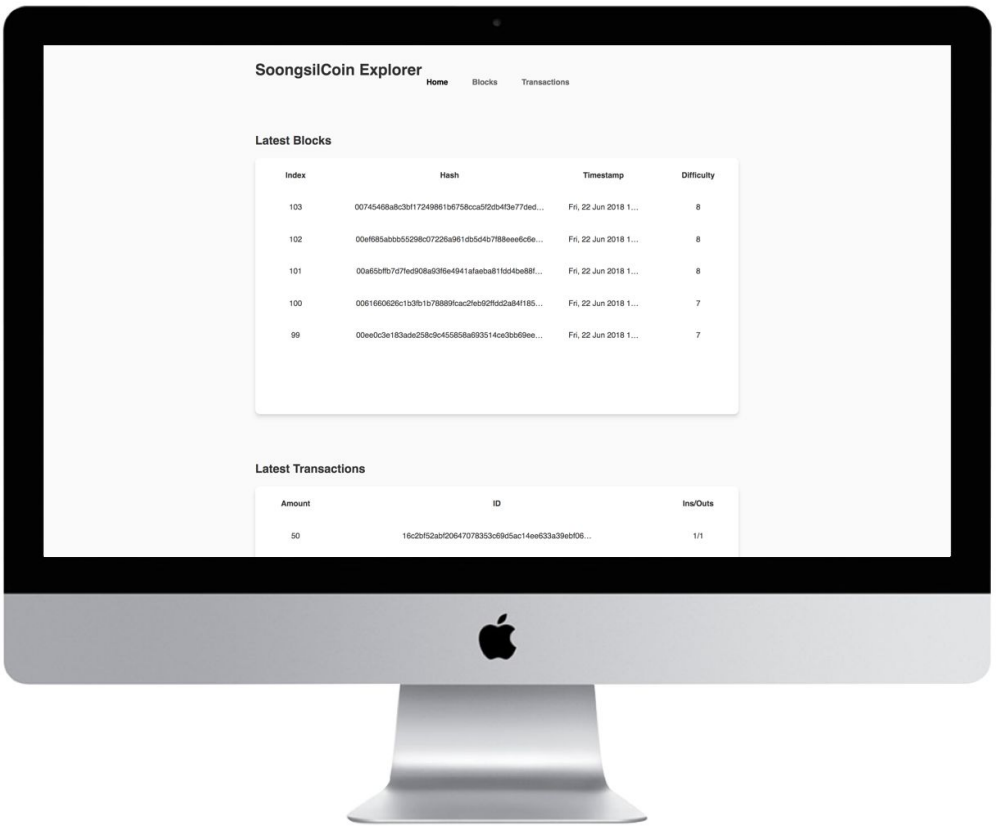


8. 사용기술

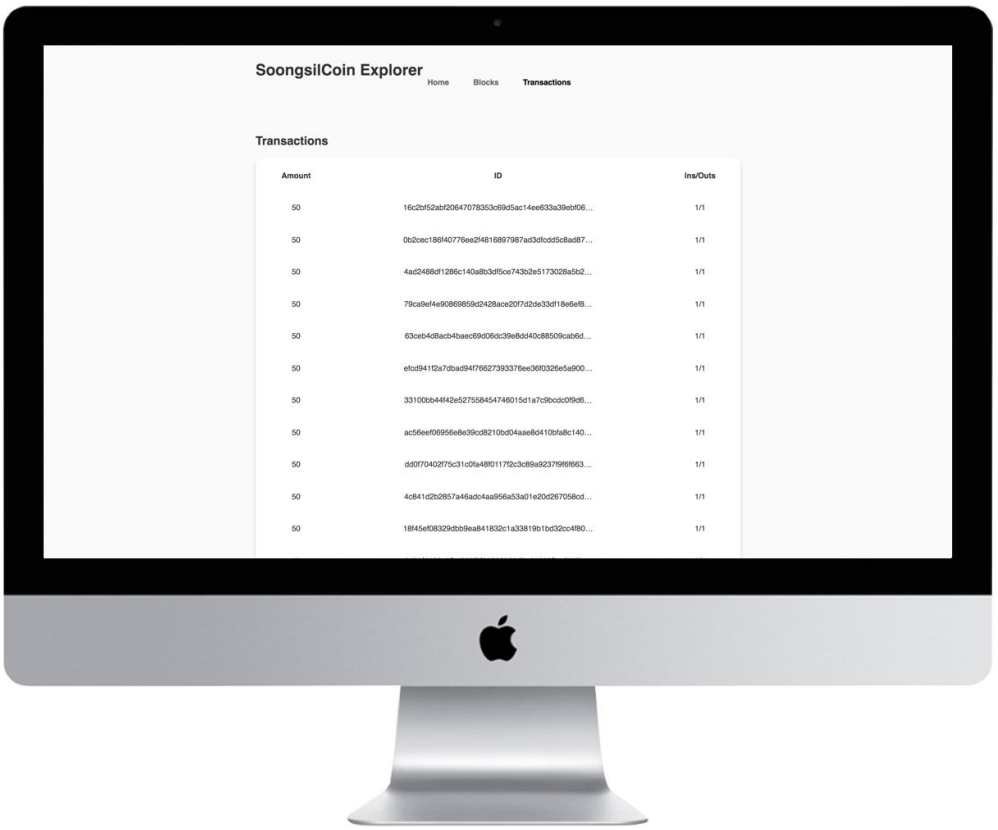
- Development Environment
    - macOS High Sierra (v 10.13.3)
- IDE
    - Visual Studio Code
- Programming Language
    - JavaScript
- Framework
    - Node.js / Express
    - React

9. 실제 화면

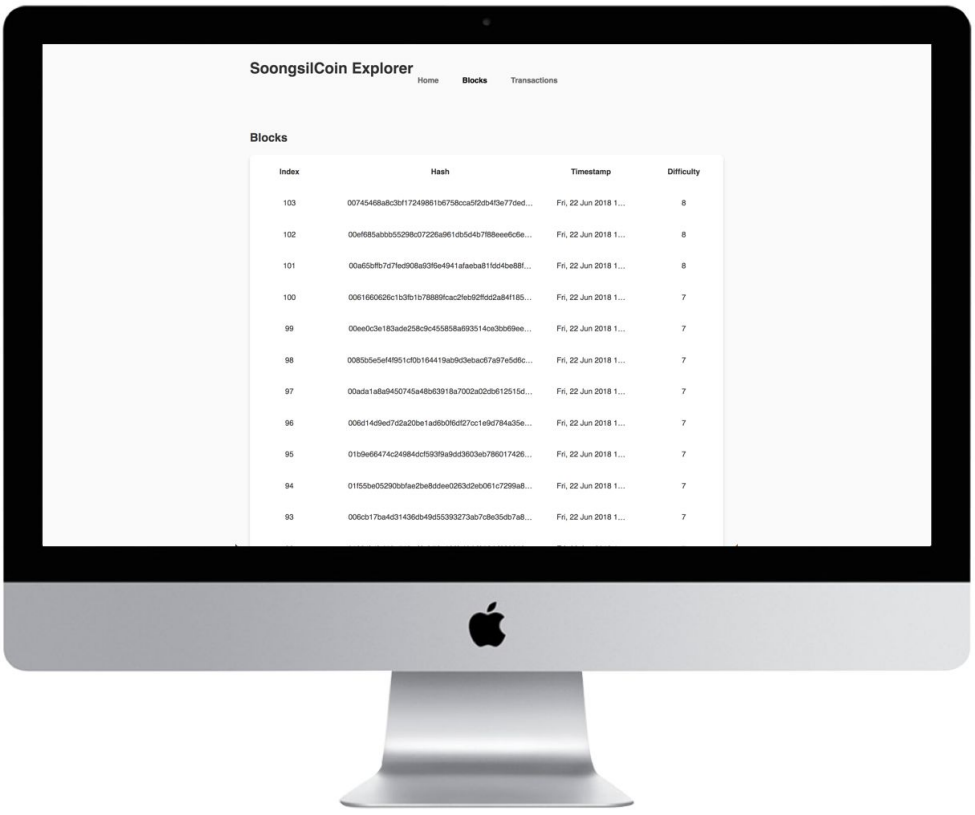
Explorer를 통해 블록체인 및 트랜잭션의 정보를 확인할 수 있다.


SoongsilCoin Explorer
Home
Blocks
Transactions
Latest Blocks
Index
Hash
Timestamp
Difficulty
103
00745468a8c3bf17249861b6758cca5f2db4f3e77ded...
Fri, 22 Jun 2018 1...
8
102
00ef685abbb55298c07226a961db5d4b7f88eee6c6e...
Fri, 22 Jun 2018 1...
8
101
00a65bffb7d7fed908a93f6e4941afaeba81fdd4be88f...
Fri, 22 Jun 2018 1...
8
100
0061660626c1b3fb1b78889fcac2feb92ffdd2a84f185...
Fri, 22 Jun 2018 1...
7
99
00ee0c3e183ade258c9c455858a693514ce3bb69ee...
Fri, 22 Jun 2018 1...
7
Latest Transactions
Amount
ID
Ins/Outs
50
16c2bf52abf20647078353c69d5ac14ee633a39ebf06...
1/1

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


SoongsilCoin Explorer
Home
Blocks
Transactions
Blocks
Index
Hash
Timestamp
Difficulty
103
00745468a8c3bf17249861b6758cca5f2db4f3e77ded...
Fri, 22 Jun 2018 1...
8
102
00ef685abbb55298c07226a961db5d4b7f88eee6c6e...
Fri, 22 Jun 2018 1...
8
101
00a65bffb7d7fed908a93f6e4941afaeba81fdd4be88f...
Fri, 22 Jun 2018 1...
8
100
0061660626c1b3fb1b78889fcac2feb92ffdd2a84f185...
Fri, 22 Jun 2018 1...
7
99
00ee0c3e183ade258c9c455858a693514ce3bb69ee...
Fri, 22 Jun 2018 1...
7
98
0085b5e5ef4f951cf0b164419ab9d3ebac67a97e5d6c...
Fri, 22 Jun 2018 1...
7
97
00ada1a8a9450745a48b63918a7002a02db612515d...
Fri, 22 Jun 2018 1...
7
96
006d14d9ed7d2a20be1ad6b0f6df27cc1e9d784a35e...
Fri, 22 Jun 2018 1...
7
95
01b9e66474c24984dcf593f9a9dd3603eb786017426...
Fri, 22 Jun 2018 1...
7
94
01f55be05290bbfae2be8ddee0263d2eb061c7299a8...
Fri, 22 Jun 2018 1...
7
93
006cb17ba4d31436db49d55393273ab7c8e35db7a8...
Fri, 22 Jun 2018 1...
7

블록들의 정보 확인