

공유 마켓 서비스를 위한 Private Blockchain Network 구축

박민영, 송유빈, 최환석, 이우섭
한밭대학교

ginibang10@gmail.com, youbinscon@naver.com, hkrock7904@gmail.com, wsrhee@hanbat.ac.kr

Implementation of private blockchain network for sharing market service

Park Min Young, Song You Bin, Choi Hoan Suk, Rhee Woo Seop
Hanbat National University

요 약

블록체인 기술은 네트워크에서 일어나는 거래정보를 합의 알고리즘을 통해 네트워크 참여자들이 공유하는 분산 원장 기술로 투명성과 신뢰성을 확보할 수 있다. 인터넷이 보편화 되면서 사이버 거래가 증가했고, 사이버 거래 사기 또한 증가했다. 이러한 위험을 줄이기 위해 본 논문은 블록체인 기술을 적용하여 공유 마켓 서비스를 제안하고 이를 구현하기 위해 이더리움 기반의 Private Blockchain Network 을 구축해본다.

I. 서 론

최근 다양한 분야에서 블록체인 연구가 진행되고 있다. 블록체인 기술은 네트워크에서 일어나는 거래정보를 합의 알고리즘을 통해 네트워크 참여자들이 공유하는 분산 원장 기술이다[1].

인터넷이 보편화 되면서, 사이버 거래가 증가하고 있다. 사이버 거래는 시공간의 제약이 없는 장점이 있으나, 사기를 예방하기 힘들어 매년 사기 피해가 증가하고 있다[2]. 이에 블록체인 기술은 모든 데이터를 공유하기 때문에 투명성을 확보할 수 있어 사기 피해를 줄일 수 있다. 하지만 블록체인 기술은 기존의 데이터베이스에 비해 느린 거래 처리 속도와 저장 공간 부족의 문제[1]가 있다. 따라서 본 논문에서는 블록체인의 장점을 활용함과 동시에 저장 공간 부족 문제를 해결하기 위해 이더리움의 Private Blockchain Network 와 데이터베이스를 함께 사용한다.

Private Blockchain 은 Public Blockchain 과 달리 미리 정해진 조직이나 개인들만 참여할 수 있기 때문에 Public Blockchain 에 비해 빠른 처리속도와 블록생성을 지원할 수 있고[3], 다양한 서비스를 연구할 때 테스트 넷으로도 사용된다. 본 논문에서는 공유마켓 서비스를 위한 이더리움 기반 Private Blockchain Network 구축에 대해 설명하고자 한다.

II. 공유마켓 서비스를 위한 이더리움 기반 Private Blockchain Network 구축

본 논문에서 설명할 이더리움 기반 Private Blockchain Network 구성은 그림 1 과 같다. 결과적으로 독립적인 3 대의 PC 에서 4 개의 노드를 생성한 뒤 노드들을 연결하여 네트워크를 구축한다. 세부적으로 단계를 나누면 (1) Private Network 를 구성하기 위한 노드를 생성한 뒤, (2) 부트 노드에 피어 노드 2 개를 연결해 Private Network 를 구축한다. 마지막으로 (3) 부트 노드를 제외한 피어 노드에서 마이너 노드를 지정한 뒤, 노드 하나를 추가 생성해 연결한다.

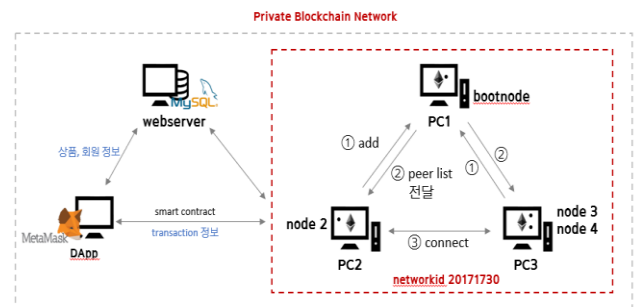


그림 1. Private Blockchain Network 구성도

2.1 Network 구성을 위한 부트 노드 및 피어 노드 생성

블록체인은 거래에 참여하는 개개인의 서버들이 모여 네트워크를 유지 및 관리한다. 이때 이 개개인의 서버, 즉 참여자를 노드라고 한다. 이는 참여 형태에 따라 공개적인 Public Network 와 비공개인 Private Network 로 나뉠 수 있다. 블록체인은 P2P 망으로 중앙 집권적인 망이 아니기 때문에 피어 노드가 네트워크에 연결되면 다른 노드를 탐색하고, 하나 이상의 부트스트랩 노드에 접속하여 연결된 노드의 목록을 받아 해당 노드들과 연결한다. 부트스트랩 노드는 블록체인 정보를 저장하지 않고 네트워크상의 피어 노드들을 찾는데 사용되는 노드로, 일정 시간 동안 연결되어 있는 노드의 목록을 유지하다 새로운 피어 노드에게 노드의 목록을 전달한다. 부트스트랩 노드는 피어 노드가 많은 규모의 네트워크에서 사용하며 작은 규모의 경우 Geth 클라이언트가 부트스트랩 노드 역할을 한다[4].

이더리움 기반 Private Network 를 구축하기 위해서는 기본적으로 최초의 블록인 제네시스 블록을 설정하기 위한 네트워크 설정 내용을 포함하고 있는 제네시스 파일과 사용자 정의 Network id, 부트스트랩 노드가 필요하다. 이때 특정 Private Network 를 구성하는 모든 노드의 제네시스 파일과 Network id 가 동일해야 하며, 동일한 부트 노드를 통해 연결되어야 한다.

첫번째 노드인 부트 노드 생성 과정은 3 단계로 나뉜다. 첫 번째로 제네시스 설정 파일을 작성하고, 두 번째로 제네시스 파일을 이용하여 최초 블록을 생성한 뒤, 사용자가 지정한 Network id 에 접속한다. 마지막으로 Account 를 생성한 뒤, 초기 Ether 를 할당해 주기 위해 제네시스 파일의 alloc 부분을 수정하고 제네시스 블록을 다시 생성한다. 제네시스 설정 파일은 그림 2 와 같으며, 피어 노드들은 수정된 제네시스 설정 파일을 이용해 마지막 단계를 제외하고 생성해 준다.

```

1 {
2   "config": {
3     "chainId": 20171730,
4     "homesteadBlock": 0,
5     "eip155Block": 0,
6     "eip158Block": 0,
7     "ethash": {}
8   },
9   "gasLimit": "0x47b760",
10  "difficulty": "0x80000",
11  "alloc": {
12    "0x579bbab2391c1f3399dc0ffbe9422a6d8e04e33": {"balance": "1000000000000000000"},
13    "0xa15eca297247dccb5c63127b97254f21488e489e": {"balance": "2000000000000000000"}
14  }
15 }

```

그림 2. 네트워크 생성을 위한 제네시스 설정 파일

2.2 부트 노드와 피어 노드 연결 및 네트워크 구축

부트 노드와 2 개의 피어 노드를 생성한 후, 부트 노드에 피어 노드를 연결해 주기 위해 부트 노드의 enode URL 을 확인한다. admin.nodeInfo.enode 명령을 사용해 부트 노드의 enode 를 확인한 뒤, 피어 노드에서 Geth 를 구동시키고 addPeer 로 부트 노드와 P2P 연결을 한다. 연결 명령은 admin.addPeer("부트 노드 enode") 이다. 여기까지 진행할 경우 연결 상태는 그림 3 과 같다.

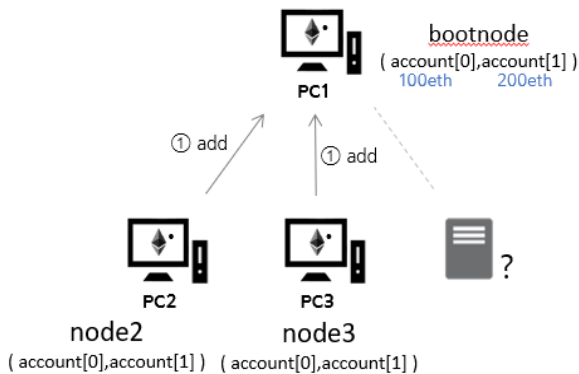


그림 3. 피어 노드와 부트 노드 연결

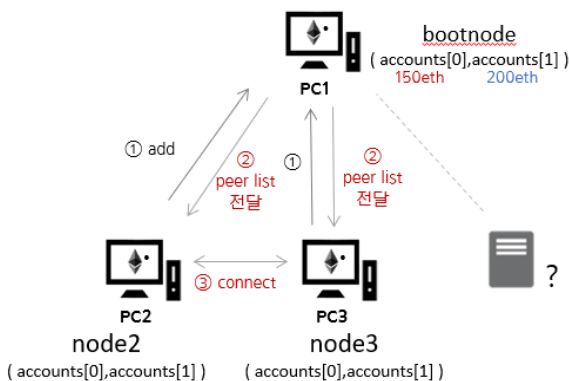


그림 4. 부트 노드를 통한 피어 노드들의 연결

현재 부트 노드와 각각의 피어 노드들이 P2P 연결이 되어있기 때문에, 피어 노드는 부트 노드를 제외한 다른

노드의 존재를 확인할 수 없다. 따라서 부트 노드에서 채굴을 해주어야 한다. 부트 노드가 채굴을 시작하면 연결 목록이 전달되며, 부트 노드를 제외한 노드끼리 연결이 된다. 여기까지 진행할 경우 연결 상태는 그림 4 와 같다. 즉, 서로 다른 3 대의 PC 에서 3 개의 노드로 송금이 가능한 Private Network 구축이 되었다.

2.3 마이너 노드 지정 및 피어 노드 추가

부트 노드에서의 채굴을 멈춘 뒤, 연결된 node3 에서 채굴을 시작해 마이너 노드로 지정한다. 그 뒤, PC3 에서 새로운 노드인 node4 를 생성해 부트 노드에 연결해준다. 이 때 같은 호스트에서 여러 노드를 구현할 경우 port 번호를 달리하고, IPC-RPC 를 disable 시켜준다. 부트 노드가 추가적으로 채굴을 하지 않더라도 연결된 노드 중 마이너 노드가 있다면 연결되어 있는 노드에게 리스트 전달을 요청해 모든 노드가 새로운 노드의 존재를 확인한다. 연결과정은 그림 5 와 같다.

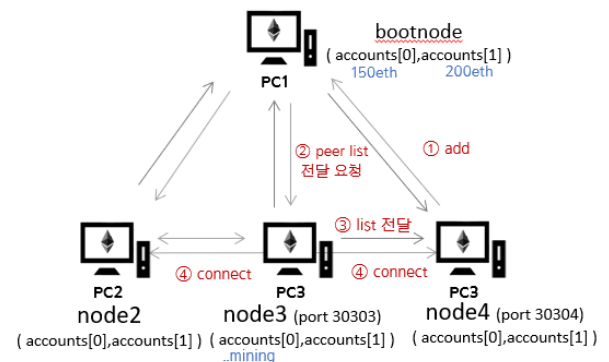


그림 5. 마이너 노드 지정 및 피어 노드 추가

III. 결론

본 논문에서는 공유 마켓 서비스 구현을 위한 이더리움 기반 Private Blockchain Network 구축에 대해 설명하였다. 구축된 네트워크는 3 대의 독립적인 PC 를 기반으로 4 개의 노드가 연결되어 있다. 이는 공유마켓 서비스의 거래정보를 분산 저장하여 안전한 관리를 제공한다. 현재 이더리움 네트워크는 완전하게 작동하고 있지만, Private Blockchain 의 용도는 한정적이며, 여러 분야로 확산 적용화 되지는 않았다. 따라서 향후 Private Blockchain 을 테스트 넷 역할에서 벗어나, 그 이상으로 다양한 분야에 활용하기 위한 저장 공간 한계 및 확장성 문제를 해결하기 위한 연구가 지속적으로 필요한 실정이다.

참 고 문 헌

- [1] 김정숙, "산업 생태계의 혁신을 선도할 블록체인 기술의 미래전망," 한국콘텐츠학회논문지, vol. 18, no. 6, pp. 324-332, Jun. 2018.
- [2] 정진효, 이창무, "인터넷 직거래 사기의 실태 및 보안대책," 한국전자거래학회지, vol. 20, no. 2, pp. 141-153, May 2015.
- [3] 김광훈, "블록체인 기술의 이해 및 적용 현황," 대한산업공학회 ie 매거진, vol. 25, no.1, pp. 13-19, Mar. 2018.
- [4] 박재현, 오재훈, 박혜영, "코어 이더리움 프로그래밍 (블록체인, 이더리움 핵심에서 암호화폐 구축을 위한 스마트 컨트랙트 개발까지),"제이펍, Apr. 2018.