자체 블록체인 네트워크 구축을 위한 블록체인 코어 프레임워크(BSF) 구현

The Implement of Blockchain Separation Framework(BSF) for Construct Own Blockchain Network

요 약

블록체인 기술은 블록데이터를 기반으로 하는 체인 형태의 연결고리 기반의 분산 저장기술로, 중앙 서버 없이 모든 노드가 피어(Peer)로 참여하는 퓨어 P2P 방식의 네트워크이다. 모든 노드가 합의를 기반으로 참여하게 되어 원장의 위·변조를 사전에 방지하고, 네트워크의 신뢰성을 유지할 수 있기 때문에 탈중앙화(Decentralization) 라는 특성을 가지고 있다.

이러한 이유 때문에, 탈중앙화(Decentralization)를 필요로 하는 서비스에 블록체인을 접목시키려는 시도가 늘고 있다. 하지만 해당 서비스의 목적에 맞는 자체 블록체인 코어를 처음부터 설계 및 구축하는 것은 많은 시간이 소요되기 때문에 대다수의 업체는 호환성, 속도 등의 다양한 문제점을 감안하고, 이미 존재하는 이더리움, EOS와 같은 플랫폼을 이용하여 Dapp을 구축한다.

본 논문에서는 목적에 맞는 효율적인 블록체인 코어를 오픈소스 기반으로, 보다 쉽고 효율적으로 구현 할 수 있도록 하는 블록체인 코어 프레임워크의 구현 및 개발 방법에 대한 내용을 다룬다.

1. 서 론

블록체인 기술은 블록데이터를 기반으로 하는 체인 형태의 연결고리 기반의 분산 저장기술로, 중앙 서버 없이 모든 노드가 피어(Peer)로 참여하는 퓨어 P2P 방식의 네트워크이다. 모든 노드가 합의를 기반으로 참여하게 되어 원장의 위·변조를 사전에 방지하고, 네트워크의 신뢰성을 유지할 수 있기 때문에 탈중앙화(Decentralization) 라는 특성을 가지고 있다.

이러한 이유 때문에, 탈중앙화(Decentralization)를 필요로 하는 서비스에 블록체인을 접목시키려는 시도가 늘고 있다. 하지만 해당 서비스의 목적에 맞는 자체 블록체인 코어를 처음부터 설계 및 구축하는 것은 많은 시간이 소요되기 때문에 대다수의 업체는 호환성, 속도 등의 다양한 문제점을 감안하고, 이미 존재하는 이더리움, EOS와 같은 플랫폼을 이용하여 Dapp을 구축한다.

본 논문에서는 목적에 맞는 효율적인 블록체인 코어를 오픈소스 기반으로, 보다 쉽고 효율적으로 구현 할 수 있도록 하는 블록체인 코어 프레임워크의 구현 및 개발 방법에 대한 내용을 다룬다.

2. 관련 연구

2.1 Bitcoin

Bitcoin은 2008년 사토시 나카모토의 논문 Bitcoin : A Peer to Peer Electronic Cash System에 최초 기술됐던 블록체인 기술을 이용하여 2009년 개발된 최초의 암호화폐이다[1].

오픈 소스로 공개되어 있지만 대다수의 상수와 변수 값이 하드코딩되어 있고 코드를 변경하였을 경우 Assert에 의해 컴파일시에 에러가 발생하는 등 오픈 소스의 특성인 범용성과 확장성을 갖추고 있지 않다.

2.2 Litecoin

Litecoin은 MIT의 Charlie Lee가 개발한 비트코인 포크 기반의 암호화폐로 해싱함수를 SHA-256에서 Scrypt로 바꾸고, 블록체인 블록사이즈를 4MB로 늘렸으며 최대 발행 수량을 늘린 블록체인 프로젝트이다. 자체 블록체인 서비스 구현을 위해 비트코인의 Assert 문장과 Bitcoin 종속적인 코드를 모두 제거하여 비교적 코드 수정이 간단하다.

오픈 소스로 공개되어 있고, 비트코인 종속성을 제거하였기 때문에 코드 수정이 비교적 간편해 가장 많은 블록체인 프로젝트의 모체가 되었다.

비록 Assert문을 제거하여 최대 발행량, 네트워크 주소, 해싱 방식, 블록사이즈, 블록 생성 시간등의 하드코딩된 블록체인 인자를 바꿀 수는 있게 되었지만, 큰 틀에서의 변화를 위해서는 기존 코드를 새롭게 고치고 의존성을 검사하며 수정해야 한다는 점에서 여전히 Bitcoin 포크 방식의 한계점이 존재한다.

2.3 Peercoin

Peercoin은 Bitcoin을 모체로 하며 기존 Bitcoin의 합의 알고리즘인 작업증명(proof-of-work)을 지분증명(proof-of-stake)으로 변경하였다[2]. 지분증명 방식 기반의 블록체인 프로젝트들의 모체가 되고 있으며 Bitcoin 포크 프로젝트 중 최초로 가장 많은 부분에서 변화가 나타난 프로젝트이다.

Bitcoin에서 합의 알고리즘을 의존성을 모두 고려하면서 Bitcoin의 코드를 수정하여 구현하였지만 결국 Bitcoin이 아닐 뿐, Peercoin에 종속되어있기 때문에 Bitcoin의 문제점으로 언급했던 오픈소스로서의 확장성과 범용성 문제를 여전히 해결하지 못했다.

2.4 Bytecoin

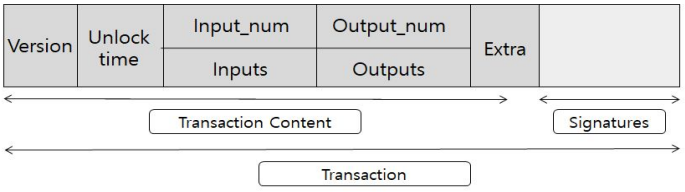
Bytecoin은 CryptoNote 기술 기반의 최초 익명성 코인으로 Cryptonight 알고리즘을 사용하였으며 링 서명은 이용하여 익명성과 정보 보호를 강조하며 등장하였다[3]. Bitcoin과 Bitcoin을 포크한 프로젝트와 전혀 관련이 없는 최초의 독립

블록체인이기도 하다. CryptoNote라고 하는 자체 블록체인 코어 기술을 통해 만들어졌으며, 기존 하드코딩방식이 아닌 확장성과 범용성을 고려한 프로젝트다. 비교적 쉽게 인자를 수정할 수 있지만 소스코드 길이가 비트코인보다 훨씬 방대하며, 자체 블록체인 네트워크를 분리해내는 것이 어렵다는 단점이 있다.

3. BSF(Blockchain Separation Framework)

BSF는 Bitcoin 포크 방식의 종속성 문제를 해결하고 보다 간단히 자체 블록체인 네트워크를 구현할 수 있는 프레임워크이다.

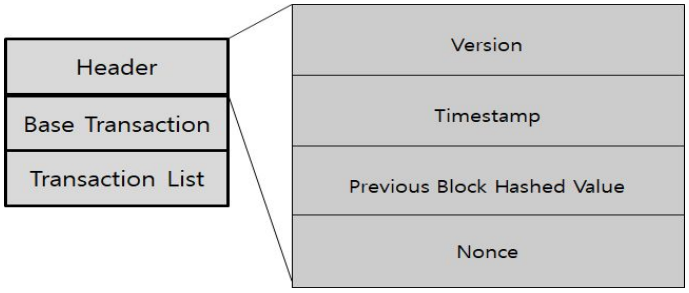
3.1. 트랜잭션 설계 구조



<그림 1 트랜잭션 설계 구조>

BSF의 트랜잭션 설계 구조는 **<그림 1>**과 같으며, 필요에 따라서 타입이나 용도는 이용자가 수정할 수 있도록 구현하였으며 기본적으로 UnlockTime에는 UNIX 기반의 타임스탬프를 기록하며, Inputs에는 트랜잭션 소유권에 대한 키 정보와 Block Height가, Outputs에는 전송될 코인의 수량과 목적 주소정보가 저장된다.

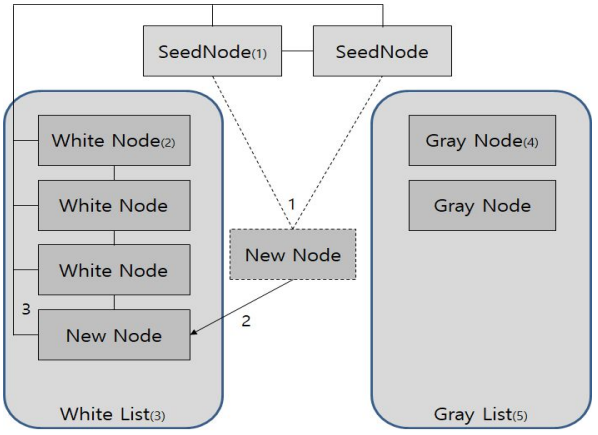
3.2 블록 설계 구조



<그림 2 블록 설계 구조>

블록은 상기 **<그림 2>**와 같이 블록 헤더 + Base Transaction + Transaction List로 구성하였다. 블록헤더는 Version과 UNIX 기반의 Timestamp,이전 블록의 해싱값, 작업증명을 위한 Nonce로 구성되어 있으며 이러한 값들을 통해 위·변조를 파악할 수 있다. Base Transaction은 해당 블록에 생성된 최초 트랜잭션, 즉 Block Creation Transaction 정보를 저장한다. 이를 통해 채굴 보상을 받을 사람을 식별 할 수 있다.
Transaction List에는 해당 블록에 포함된 트랜잭션들의 TxHash 값이 리스트형태로 저장된다.

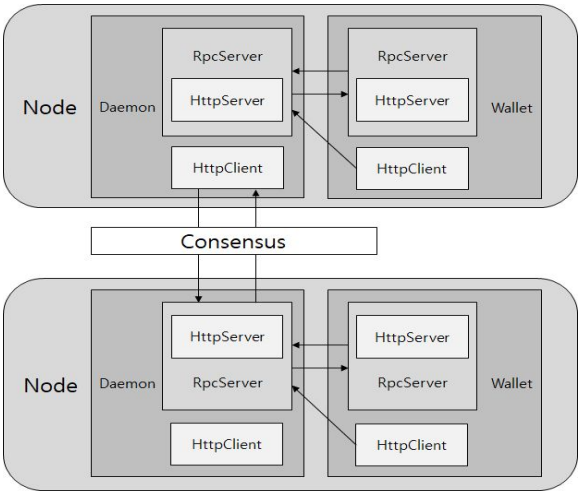
3.3 P2P 네트워크 설계 구조 및 구현



<그림 3 P2P 네트워크 설계 구조 및 구현>

<그림 3>은 BSF의 P2P 네트워크 개발 구조이다.
(1)SeedNode로 네트워크의 첫번째 노드이며 다른 노드들은 처음 연결시 해당 노드에 먼저 연결되어 현재 네트워크에 참여하고 있는 노드들의 항목을 받아 항목의 노드들과 연결된다. (2)White Node는 현재 네트워크에 참여 P2P연결되어 있는 노드를 의미하며 (3)White List는 White Node들의 집합이며 새로운 노드가 연결될 때 SeedNode에서 전달되는 요소이다. (4)Gray Node는 블록체인 네트워크에 참여하였지만 현재는 연결이 종료된 노드를 의미하며 각 Gray Node는 종료 당시의 White List를 갖고 있다. (5) Gray List는 연결이 종료된 노드인 Gray Node들의 집합이다.
1번 동작은 새로운 노드가 블록체인 네트워크에 참여하고자 할 때 모든 SeedNode와 연결되어 현재 참여자 노드 항목인 White List를 받아오는 동작이다. 2번 동작은 White List에 새로운 노드가 추가되는 동작이다. 3번 동작은 White List에 있는 모든 노드들과 연결되는 동작이다.
이런한 방식의 설계를 통해, SeedNode의 변경만을 통해 손쉽게 분리된 P2P 네트워크를 구성할 수 있다,

3.4 블록체인 네트워크 설계 구조



<그림 4 블록체인 네트워크 설계 구조>

<그림 4>는 BSF를 구성하는 P2P노드의 구조와 통신 방식 모델이다.
노드 내에서는 데몬과 지갑이 동작하고 있으며 통신을 위해서 RPC 서버와 HTTP 서버가 실행된다. RPC 서버는 HTTP 서버를 동작시켜 외부 노드 및 프로세스와 통신을 진행한다.
RPC 메소드는 오픈소스로 공개되어 있는 Bytecoin의 JSON_API를 이용하여 구현하였다[4][5]. 지갑과 데몬은 RPC 서버와 HTTP 클라이언트간의 통신을 하게 되는데, 요청측에서

JSON방식으로 작성된 시그널과 메소드 실행 요청을 전달하고 그에 따른 State값 또는 반환 JSON 값을 리턴하는 방식으로 구현되었다.

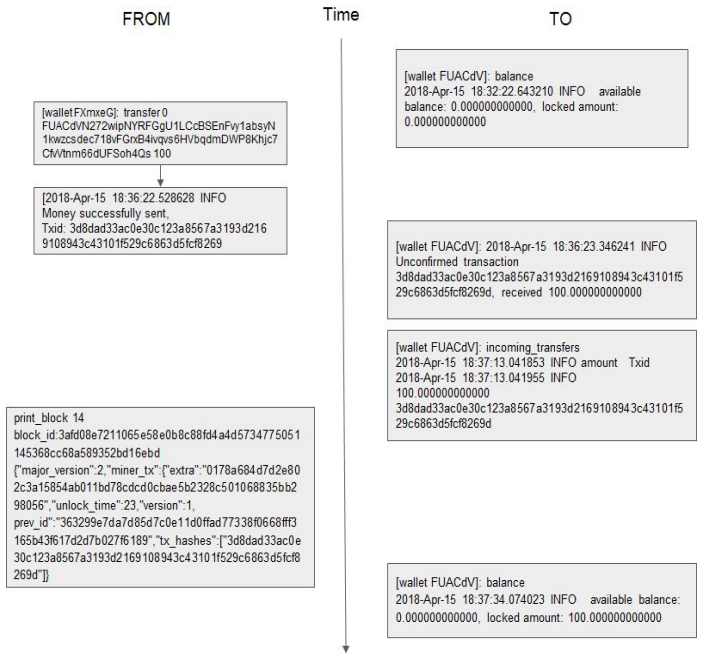
합의 방식은 작업증명(Proof of Work)를 사용한다. 작업증명 방식은 컴퓨터의 연산력을 바탕으로 합의를 진행하는 방식으로 새로운 블록을 블록체인 네트워크에 추가하기 위해서는 채굴 난이도에 따른 특정 규격을 만족시키는 Nonce값과 그 해싱값을 구해야 한다. 본 프레임워크에서는 임의의 Nonce값을 해시함수에 넣고 채굴 난이도에 따른 숫자보다 작은 값인지 확인한다. 만약 채굴 난이도에 따른 인자 값보다 작은 값의 Nonce를 구하게 된다면 블록을 생성하고 채굴 보상을 받고, 아니라면 또다른 임의의 Nonce값을 대입하며 블록 해시 값을 찾도록 구현되었다.

마지막으로 노드들 사이의 통신으로는 동기화과정, 합의에 의한 채굴 블록 생성 등에 사용되는데 이는 데몬에 의해 실행된 HTTP 클라이언트가 요청을 보내오면 HTTP 서버에서 요청을 수신하고 RPC 서버 에서 요청에 해당하는 기능을 수행한다. 수행한 결과는 HTTP 서버에 JSON형태로 전달되어 HTTP 클라이언트에 전달되게 된다.

3.5 자체 블록체인 구현 및 분리 실험

본 논문에서 개발한 BSF를 통해 독자적인 P2P 네트워크 분리를 통한 블록체인 구현이 가능한지, 해당 프레임워크의 SeedNode IP를 Google Cloud 인스턴스의 IP로 바꾼 뒤, 자체 코인을 발행, 작업증명 및 정상적으로 송금 트랜잭션이 작동하는지를 실험한 과정이다.

3.5.1 송금 트랜잭션 진행 과정



<그림 5 송금 트랜잭션 진행 과정>

<그림 5>는 BSF를 이용하여 구현된 자체 블록체인에서 자체 코인을 송금하는 프로세스를 나타내고 있다.

처음엔 잔고가 0이었던 지갑에 트랜잭션을 통해 성공적으로 코인이 송금되어 100코인이 증가한 것을 확인할 수 있다.

3.5.2 트랜잭션 결과


```
{
  'jsonrpc' : '2.0',
  'id' : 'transfer' ,
  'result' : {
    'transaction' : {
          'fee' : 10,
          'extra' : '0178a684d7d2e802c3a15854ab011bd78...',
          'timestamp' : 0,
          'blockIndex' : 13,
          'state' : 0,
          'transactionHash' : '3d8dad33ac0...',
          'amount' : -110,
          'unlockTime' : 0,
          'transfers' :
          {
              'amount' : 100,
              'type' : 0,
              'address' : 'FUACdVN272wipNYR..."
          }
          'paymentId' :,
          'isBase' : False
    }
  }
```


<그림 6 트랜잭션 결과>

<그림 6>은 실제 트랜잭션의 결과로 나온 JSON 값이다. 자체 블록체인에서 성공적으로 RPC를 통해 송금이 진행되었고 자체 네트워크가 분리되었다는 것을 확인할 수 있다. 복잡한 과정 없이도 인자값 변경 만으로 블록체인 네트워크가 독립적으로 분리된 것이다.

4. 결론 및 향후 연구

관련 연구에 기술되어 있는 Bytecoin의 CryptoNote 기술과 JSON RPC API등을 활용하여 RPC서버를 구축하였고, 이를 바탕으로 동작하는 블록체인 프레임워크를 구현하였다. 기존 프로젝트에선 곳곳에 흩어져있던 블록체인의 블록 생성 속도, 블록 사이즈등의 인자 값들을 설정파일로 따로 모아두는 방식으로 개발하여 인자 변경이 보다 간편하며, SeedNode 를 통한 P2P 네트워크 구성 방식을 통해 단순히 SeedNode의 IP 변경을 통한 간편한 네트워크 분리방식이 도입된 범용적인 블록체인 코어 프레임워크(BSF)를 개발하였고 이를 포크함으로서 독립적인 블록체인 네트워크를 손 쉽게 구현할 수 있었다.

향후 연구방향으로는 본 프레임워크의 성능을 향상시키고 유동적인 수정이 가능하도록 코드를 리팩토링하여 보다 뛰어난 확장성과 범용성을 가지는 오픈 소스로서의 블록체인 코어 프레임워크를 구현하는 것을 목표로 한다.

5. 참고 문헌

[1] Satoshi Nakamoto. “Bitcoin A Peer-to-Peer Electronic Cash System” bitcoin.org, 2009

[2] Sunny King. “PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake”, August, 2012

[3] Nicolas van Saberhagen. “CryptoNote v 2.0” (White Paper), October, 2013

[4] Bytecoin. “Bytecoin RPC Wallet JSON RPC API” https://wiki.bytecoin.org/wiki/Bytecoin_RPC_Wallet_JSON_RPC_API, 2012

[5] Bytecoin. “Daemon JSON RPC API” https://wiki.bytecoin.org/wiki/Daemon_JSON_RPC_API , 2012