자체 블록체인 네트워크 구축을 위한 블록체인 코어 프레임워크 구현

The Implement of Blockchain Core Framework for Construct Own Blockchain Network

요 약

블록체인 기술은 일종의 분산 원장 데이터베이스로써, 중앙 서버가 존재하지 않고, 모든 노드가 Peer로 참여하는 퓨어 P2P 방식의 네트워크이다. 모든 네트워크 참여자들이 Consensus 에 참여하여 원장의 위변조를 사전에 방지하고, 네트워크의 신뢰성을 유지할 수 있기 때문에 Decentralized Service라는 특성을 가지고 있다.

이러한 이유 때문에, Decentralize를 필요로 하는 서비스에서 블록체인을 접목시키려는 시도가 늘고 있다. 하지만 서비스와 잘 호환될 수 있는 자체 블록체인 코어를 Zero-Base에서 설계 및 구축하는 것은 많은 시간이 소요되기 때문에 대다수의 업체는 호환성, 속도등의 다양한 문제점을 감안하고, 이미 존재하는 블록체인 프로젝트를 Fork하거나 이더리움, EOS와 같은 플랫폼을 이용한 Dapp을 구축한다.

본 논문에서는 자체 블록체인 코어를 보다 쉽고 효율적으로 구현 할 수 있도록 하는 블록체인 코어 프레임워크를 오픈 소스를 이용하여 구현 및 개발한 내용을 다룬다.

1. 서 론

Decentralize를 필요로 하는 다양한 서비스에서 블록체인을 이용하려는 시도가 늘어나고 실제 제공되는 서비스도 빠른 속도로 증가하고 있다. 하지만 자신이 제공하고자 하는 서비스와 잘 호환될 수 있는 자체 블록체인 코어를 Zero-Base에서 설계 및 구축하는 것은 많은 시간과 노력이 필요하기 때문에 대다수의 업체는 호환성, 속도등의 다양한 문제점을 감안하고, Bitcoin과 같은 이미 존재하는 블록체인 프로젝트를 Fork하여 사용하거나 별도의 코어가 필요한 서비스라 할지라도 Ethereum, EOS와 같은 플랫폼을 이용한 Dapp을 구축하는 경우가 많다.

타 블록체인 프로젝트를 사용하면 수많은 문제가 발생하는데도 불구하고 자체 코어를 개발하지 않는 데에는 여러가지 이유가 있다. 가장 일반적인 코어 개발 방식은 기존의 블록체인 코드를
Fork한 후 구현하는 것이다. 하지만, 기존의 블록체인 프로젝트는 대다수가 하드코딩 되어 있기 때문에 코드 분석이 어렵고 블록체인 코어의 특성상 하드코딩되어 있는 대부분이 해싱 값이기 때문에 더욱 코드 분석의 어려움이 가중된다.

또한 기존 블록체인 프로젝트들은 자체 블록체인 프로젝트에 특화된 코드설계를 갖고 있다는 점이다. 즉 오픈소스
로서의 범용성과 활용성이 떨어진다. 이러한 프로젝트를 Fork하여 사용할 경우 간단한 코드 수정에도 수많은 Code Dependency를 체크해야 하는 문제가 발생하게 된다.

뿐만 아니라 기존 블록체인 프로젝트는 익명성 프로토콜이나 자체 프로젝트에 종속적인 기능이 운영 및 유지 보수 과정에서 추가 구현된다. 하지만 Fork를 통해 자체 블록체인 네트워크를 구축하고자 할 경우 기존 블록체인의 추가 구현된 내용의 대다수가 불필요하다. 이러한 불필요한 기능들은 코드 분석을 어렵게 만들고 Dependency문제를 가중시킨다. 또한 필요하지 않은 기능은 성능의 저하를 야기하게 된다.

위와 같은 문제들로 인해 자체 블록체인 네트워크를 분리시키는 것은 많은 비용이 요구된다. 본 논문에서는 이러한 기존의 문제를 해결하기 위한 프레임워크를 구현 및 개발한 내용을 다룬다.

2. 관련 연구

2.1 Bitcoin

Blockchain Technology는 2008년 Satoshi Nakamoto의 논문 Bitcoin : A Peer to Peer Electronic Cash System[1]에 최초 기술되었으며 Bitcoin은 2009년 개발된 최초의 블록체인 기술을 이용한 Decentralized 암호화폐이다.

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

2.2 Litecoin

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

Open Source로 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 있게되었지만, 큰 틀에서의 변화를 위해서는 기존 코드를 새롭게 고치고 Dependency를 체크하며 수정해야 한다는 점에서 여전히 Bitcoin Fork 방식의 한계점이 존재한다.

2.3 Peercoin

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

Bitcoin에서 합의 알고리즘을 Dependency를 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

Bytecoin[3]은 CryptoNote technology 기반의 최초

3. 구현 내용

4. 결론 및 향후 연구

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