Abstract

스마트 컨트랙트를 활용한 탈중앙화된 포럼 어플리케이션 플랫폼

2009 년 1 월에 처음으로 블록이 생성된 비트코인은 전세계적인 화폐혁신을 일으켰다. 블록체인의 최초의 활용이자 동시에 비트코인의 장부로서의 블록체인이 나타나면서 기존의 신뢰하지 못하는 네트워크에서의 신뢰기반에 대한 혁신과 이를 이용한 통화의 혁신을 불러온 첫 번째 사례이다. 이후 꾸준하게 그 활용도를 높여가면서 기술발전이 꾸준히 이루어지고 있다.

비트코인이 블록체인의 가장 기본적인 기능인 통화로서의 안정적인 전송과 보관의 기능에 집중하였다면 2015 년에 첫번째 블록이 생성된 이더리움은 전송의 기능위에 사적 계약이라는 기능을 추가하였다. 사적인 계약을 삼자의 개입 없이 블록체인상에서 체결 가능하게 만든 최초의 스마트 컨트랙트라는 기능을 사용하였다.

비트코인에 이어 블록체인 2.0 으로도 불리는 이더리움은 완벽한 튜링완전(turing-complete) 프로그래밍 언어가 심어진 블록체인이다. 이 프로그래밍 언어는, 정해진 규칙에 따라 사적계약(contracts)을 사용자들이 직접 작성 가능하게 할 수 있게 하였다. 이 계약이라는 것은 말 그대로의 계약서의 계약도 있으나 ERC-20 의 규약을 만족하는 조건에서 "토큰생성"이라는 개념의 계약도 생성이 가능하다. 이더리움의 계약이라는 조건을 이용해서 이더리움 블록체인 네트워크 상의 또 다른 코인의 발행 및 전송을 실행하는 것도 가능하며 무수히 많은 토큰들이 이더리움 플랫폼위에서 작동하고 있다.

이더리움은 끊임없이 발전해나가는 블록체인으로 뛰어난 기능 발전을 보여주고 있다. 하지만 아직 일반인과 각종 어플리케이션 개발자들이 그 기능을 실제로 적용하기에는 많은 한계가 있다. 또한 각종 소셜네트워크, 커뮤니티, 게임사이트에서 자체적인 코인개발 등을 진행하는 것이 매우 복잡한 일이 아닐 수 없다.

이더소셜(ESN)은 ERC-20 스마트 컨트랙트 규약을 준수하는 토큰을 클릭 몇 번으로 생성할 수 있는 매니지먼트 툴과 각종 서비스에 적용하는 API 기능을 제공한다. 이를 이용해 각 사이트 관리자는 독자적인 토큰을 기획, 제작, 생성, 전송, 관리 소멸할 수 있다.

목차

역사(History)

비트코인의 소개

최초의 가상화폐 비트코인은 2008 년 사토시 나카모토 (Satoshi Nakamoto)의 논문 "비트코인 : 개인 간 전자 결제 시스템(Bitcoin: A Peer-to-Peer Electronic Cash System)"에서 처음 제시되었다. 나가모토는 블록체인을 도입하여 코인의 전송과 보관을 구현했다. 블록체인은 앞의 데이터를 수정할 수 없으며, 이중지불의 문제를 방지하므로 금융 거래 원장으로 사용되기에 적합했다. 각 블록에는 계산에 많은 컴퓨팅 파워를 요구하는 해시정보가 기록되기 때문에 위조와 변조가 어렵다. 또 블록에는 시간이 기록되고, 또 직전의 블록을 참조하므로 이를 위변조 하려면 모든 블록을 위변조 해야 하는데, 현실적으로 불가능하다. 양자컴퓨터가 개발되면 비트코인에 심각한 위험이 된다는 주장도 존재하지만, 향후 10 년 후에나 가능한 이야기이며, 적어도 가까운 시일 내에는 충분히 안전한 시스템이다. 현재까지 비트코인은 중앙 관리자가 없음에도 불구하고 2009 년 1 월 9 일의 제네시스 블록이 생성된 후 약 500,000 개의 블록이 생성되는 동안 비트코인 자체에 대한 해킹은 존재하지 않았을 정도로 탄탄한 보안성을 보유하고 있다. 비트코인을 통해 하루 평균 23 만 건의 거래가 진행되고 있으며, 200 조원 이상의 시가총액을 기록했다. 비트코인의 경우 작업증명이라는 과정을 통해 새로운 블록을 만들어낸다. 중앙의 통제나 중개자 없이도 자발적인 채굴자들의 협력으로 최초의 암호화폐가 만들어진 것이다. 현대사회에서 가장 대중적인 결제수단인 신용카드나 해외송금을 하기 위해서는 중앙형 서버가 필수적이었고, 내가 돈을 보낸 것을 증명해 줄 "은행"이나 "카드사"와 같은 신뢰할 수 있는 기관이 필수적이었다. 비트코인은 그러한 제 3 자 없이도 정상적으로 코인을 전송, 보관을 가능하게 했으며, 이는 예전에는 상상할 수 없었던 큰 혁신이었다.

비트코인의 한계

비트코인을 위해 지속적인 코드의 수정을 통해 업그레이드가 진행되었다. 하지만 비트코인이 개발된 지 오랜 시간이 흘렀으며, 최초의 암호화폐인 만큼 분명한 한계를 나타낸다. 비트코인 전송에 걸리는 시간은 10 분 이상이다. 왜냐하면

블록이 10 분에 한 번 생성되기 때문이다. 게다가 1BTC 의 가격이 지나치게 높으므로 실생활에서 결제 수단으로 사용되기가 쉽지 않다. 비트코인은 공개형 블록체인(Public Blockchain)으로, 트랜잭션 목록이 모두 공개된다. 누구에게나 공개되어 투명하고 조작할 수 없지만, 비밀을 숨기지 못한다는 단점이 존재한다. 대량의 BTC 를 보유한 많은 사용자의 경우 자신의 BTC 를 노출하기 싫어할 수도 있다. 또 자신의 송금 내역을 숨기려는 사람들도 존재한다. 이러한 한계성을 극복하기 위하여 제트캐시(Zcash), 모네로(Monero) 등의 익명성 기능을 도입한 코인이 속속 등장했다. 이외에도 중요한 한계는 코인의 송수신 이외의 분야에서는 사용되기 힘들었다는 점이다. 비트코인에서 사용되는 "스크립트(Script)"라는 언어는 반복문 등이 없어서 제한적인 기능만 가능하다. 이러한 한계 극복을 위해 이더리움이 등장했으며, 이더리움을 통해 암호화폐의 송수신뿐 아니라 다른 영역으로의 확장이 가능해졌다.

이더리움의 소개

2014 년에 이더리움의 ICO 가 진행되었으며, 2015 년에 최초 버전이 출시되었다. 이더리움은 블록체인을 이용하여 "스마트 컨트랙트(Smart Contract)"라는 개념을 실제로 구현한 플랫폼이었다. 스마트 컨트랙트란 디지털 명령어로 계약을 작성하면 조건에 따라 계약 내용을 자동으로 실행할 수 있는 개념이다. 이더리움을 이용하면 블록체인을 다양한 분야로 확장하는 분산애플리케이션(DApps)을 이전보다 손쉽게 만들 수 있다. 이더리움의 사용자는 "토큰"을 생성하여 자신이 원하는 용도로 사용할 수 있다. 새로운 토큰을 생성하면, 블록체인이 손쉽게 생성되며 송수신, 지갑, 탐색기 등이 토큰을 만든 사용자에게 제공된다. 토큰과 코인의 가장 큰 차이점은 코인은 자체적인 네트워크를 보유한 반면 토큰은 다른 코인의 네트워크에 더부살이로 만들어지고 운영된다는 점이다. 공통점은 송신 수신이 가능하며, 블록체인에 기록된다는 점이다. 현재 443 개의 토큰이 이더리움 기반에서 만들어졌으며, 코인 종류를 기준으로 토큰 시장의 81%를 점유하고 있다. 이더리움을 활용한 토큰은 중개자 없이 다수의 투자자와의 크라우드펀딩을 가능하게 했으며, 2017 년 6 월에는 블록체인 분야에 ICO 를 통해 투자된 돈이 처음으로 벤처캐피탈을 통해 투자된 금액을 능가할 정도로 ICO 가 활성화되었다. ICO 를 통해 개미투자자는 소액으로는 참가하기 어려웠던 첨단 IT 벤처기업과 프로젝트에 투자하여 수익을

남길 수도 있었다. 한편 아이디어와 기술력이 확보되었으나, 자본이 부족했던 개인, 그룹 등도 새로운 자금조달 수단을 확보한 것이다. 이더리움의 가장 큰 위기는 다오(DAO) 사태였다. 스마트 컨트랙트라는 양날의 검은 범용성을 주었지만, 빠른 개발 속도로 인해 보안성이 낮아졌는데, 이러한 취약점을 이용하여 다오 사태가 발생했고, 이는 이더리움의 하드포크로 이어지고 말았다. 이러한 보안상 취약점은 현재는 상당 부분 보완된 상태이다. 2016 년 다오 사태가 발생한 후 지금까지 이더리움 플랫폼에서 수많은 ICO 가 이루어졌으나 중대한 보안 이슈가 발생하지는 않았다. 따라서 현재의 이더리움 코드는 수 년 이상의 안정화와 테스트를 거쳤으므로, 신뢰할 수 있다.

이더리움의 한계

이더리움의 중요한 문제점은 일반적인 포럼에 이더리움을 직접 도입하기는 어렵다는 점이다. 이더리움을 이용한 보상시스템을 도입하기 위해서는 스마트 컨트랙트 언어인 솔리디티를 능숙하게 다루어야 하며, 블록체인에 대한 이해도가 필요하다. 이더리움에는 API 가 존재하지만, 포럼 사이트에 특화되어 있지는 않다. 따라서 블록체인에 대한 이해도가 낮은 웹개발자의 접근성이 떨어진다. 결국, 이더리움을 포럼에 도입하려면 추가적으로 개발에 따른 시간과 비용이 발생한다. 결국 포럼에 특화된 암호화폐가 필요하다면 이더리움을 이용하여 개발을 진행하는 것과 새로운 코인을 처음부터 개발하는 것과 큰 차이가 없을 수도 있다.

스팀코인의 소개

스팀코인은 '스팀잇'이라는 포럼 전문 코인으로, 2016 년부터 코인의 매매가 시작되었다. 스팀코인의 목표는 포럼에서 사용될 수 있는 코인을 생성하는 것이다. 스팀잇은 개인 블로그와 댓글의 형태로 구성되어 있으며, 이 글에 대해 사용자들이 좋은 평가를 하게 되면 보상을 얻게 되는 시스템이다. 스팀잇을 활발히 이용하는 개인 사용자는 스팀코인을 통해 보상받을 수 있고, 또 보유하는 스팀코인의 가치가 거래소에서 상승하면 보유하는 스팀코인만큼의 추가적인 이득도 얻게 된다. 스팀코인은 포럼 서비스 자체로도 60 만 명 이상의 사용자를

확보할 정도로 성공했다. 스팀잇 포럼에서 사용하는 화폐인 스팀(Steem)의 가격도 2016 년 4 월 런칭 이후 1 년 8 개월 동안 6 배 이상 상승했다.

스팀잇의 한계

하지만 스팀잇은 다양한 문제점을 내포하고 있다. 우선 스팀잇에 업로드된 주제는 상당히 제한적이다. 구글 연관검색어를 통한 검색결과 스팀잇의 연관검색어로 등장하는 사용자의 포스팅은 대부분 코인 또는 투자와 관련된 주제였다. 그 이유는 우선 스팀잇을 처음 사용하는 사용자들이 접근하기 어렵기 때문이다. 반면 암호화폐에 관심이 큰 사람들은 번거롭더라도 스팀잇의 보상을 얻기 위해 적극적으로 가입한다. 또 다른 단점은 한국형 포럼에 특화되지 않았다는 점이다. 한국에서는 블로그보다 게시판을 사용한 포럼이 일반적이다. 하지만 스팀잇은 해외 사이트를 뿌리로 두고 있으며, 따라서 개인 블로그 형식만을 지원한다. 현재의 스팀잇을 그대로 한국형 게시판에 도입하기는 어렵다. 또 다른 문제점은 많은 코인을 보유한 일부의 의견에 따라 대부분의 보상이 결정된다는 점이다. 많은 코인을 보유한 이들은 일명 '고래'라고 불리며, 이들이 1 번 '좋아요'를 누르게 되면 300 달러에 상당하는 코인 보상을 받기도 한다. 구글에 영어로 Steemit 이라는 단어를 입력하면 가장 먼저 등장하는 연관검색어는 haejin 이다. 이 아이디의 소유주가 한국인인지는 확실하지 않지만, 하루에 10 개의 포스트를 남기고 있으며, 각각 300 달러 내외의 이익을 얻고 있다. 결국 하루에 3,000 달러에 해당하는 코인 보상을 얻는 상황이다. 단순한 그림 1 장과 1 줄의 글로 구성된 포스트가 300 달러의 보상금을 받는다는 것은 일반적인 스팀잇 사용자에게는 불가능한 일이었고, 스팀잇 사용자들은 분노의 '비추천'을 남기기 시작했다. 하지만 haejin 은 지금까지도 꾸준한 포스팅을 지속하고 있으며, 일부 사용자들은 "고래 사용자 1 명이 몰아주기를 하고 있다. 스팀잇은 망가지고 있다."라며 우려했다. 또 다른 문제점은 스팀코인의 거래가 시작된 지 벌써 2 년 이나 지났으나 아직 API 가 정식 출시되지는 않았다는 점이다. 게다가 2018 년에 출시될 계획이던 SMT 토큰의 발행도 아직 이루어지지 않았다. SMT 토큰이란 이더리움의 ERC20 토큰과 유사한 것이며, 자신만의 포럼을 위한 토큰을 만드는 기능이다. 결국 현재 스팀코인은 스팀잇 포럼 1 개만을 위한 코인으로 남게 되었다. 요약하면 스팀코인은 암호화폐에 관심 있는 사용자들만의

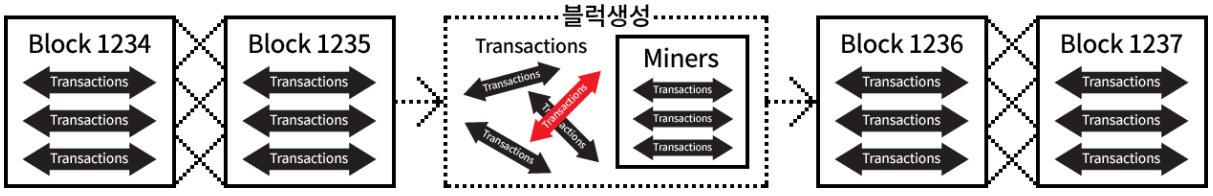
코인이 되었고, 그 중 에서도 스팀 포럼을 사용하는 사람들만을 위한 코인이 된 것이다.

비트코인과 기본 개념

기본 개념의 적립

디지털 통화라는 개념을 완성하기 위해서는 기본적으로 안전한 보관과 이동, 변경되는 내용에 대한 검증이라는 두 가지 목표를 달성해야만 한다. 또한 안전하되 익명성을 갖추어야만 암호화 화폐라 말할 수 있다. 이러한 익명성과 안정성이라는 요건을 충족하기 위해, 공개키 암호화 방식의 소유권 관리 알고리즘 위에 블록체인이라고 부르는 장부의 노드와 작업증명이라는 보안 절차를 걸쳐, 특정집단에 종속되지 않으면서도 단순하면서 완벽한 보안을 구성해 냈다. 참여자는 오로지 "연산능력"이라는 방식으로 이러한 블록체인의 암호해체작업에 참여 하게 되며, 이를 "채굴"이라고 칭하게 된다. 채굴은 블록체인의 기본적인 보안과 트렌젝션의 처리를 담당하면서, 참여자 모두 블록체인의 보상을 받게 되는 독특한 구조를 생성하게 된다. 따라서 채굴자가 없는 블록체인은 (포스방식을 제외한다면) 거래나 이동이 성립되지 않거나 극히 느리게 된다.

채굴



블록체인 구조는 매우 단순하다. '최초의 블록이 정상인가', '이후 생성되는 하나하나의 블록이 정상인가'의 개념으로 존재한다. 우리는 매번 생성되는 블록체인이 정상적으로 생성되는지 감시하면 되고, 이를 끝없이 붙여 나가면, 하나의 블록체인에 이제까지의 모든 소유와 거래를 담을 수 있다.

1. 모두가 합의된 최초의 블록과 이전까지의 블록

2. 각각의 오류 없는 트렌젝션 조합의 검증

3.온전한 블록의 생성

4.적절한 난이도의 검증과 검증의 적합성

채굴자는 기존에 검증이 완성된 블록에서부터 출발하여, 완전하고 안전한 블록을 생성하는데 최선을 다하면 된다. 그는 코인보상을 위하여 기꺼이 본인의 계산능력을 제공하면서 동시에 블록체인의 보안수준을 유지하는 것이다. 블록체인을 해킹하기 위해서는 채굴의 계산능력과 다투어야 한다. 물론 이러한 채굴은 많은 전기소모와 함께 수많은 자원을 소모하고 있다. 이것은 장기적으로 우리가 개선해 나가야 할 부분이지만, 아직까지 가장 효과적인 보안 유지 수단이다. 이더소셜은 GPU 채굴 방식을 따른다.

이더소셜

이더소셜의 목적은 이더리움의 분산 어플리케이션 프로토콜을 활용하여 실제 서비스에 적용되는 API 와 매니지먼트 툴을 만드는 것이다. 이더리움 자체는 튜링 완전 언어를 내장하고 있는 블록체인이라는 필수적이고 근본적인 기반을 제공하는 발전하는 블록체인이지만 다음과 같은 단점이 있어서 실제 서비스에 쉽게 접목하기 쉽지 않다.

1. 개발이 끊임없이 진행되고 있다

    - 개발이 진행되는 것은 좋은 현상이다. 하지만 개발이 끊임없이 진행되기 때문에 그 사이에 이더리움 계정 등에 대한 보안이슈가 발생을 하는 경우가 수 차례 발생을 했다. 이 보안이슈가 확실히 없는 안정적인 버전이 필요하다.

2. 일반 사용자 또는 일반 개발자가 접근하기 쉽지 않다.

- 이더리움 코어의 기능개선위주로 개발이 이루어지기 때문에 사용자 환경에서는 치명적인 단점을 가지고 있다. 그래서 현재로서는 일반 서비스에 접목하는 것이 거의 불가능하다.

3. 네트워크 트래픽이 굉장히 많다.

   - 끊임없는 발전과 여러 가지 테스트들로 네트워크는 항상 붐빈다. 그래서 그 위의 각종 스마트 컨트랙트들이 제대로 전송이 되지 않는 경우가 매우 많다.

4. 수수료가 비싸다.

   - 이더리움 가격 자체가 비싸져서 스마트 컨트랙트를 구현하기 위한 비용이 너무 비싸졌다.

이를 해결하기 위해 이더소셜(Ether Social) 코인은 다음 특징을 가지고 있다.

1. 이더리움의 기능 중에서 Stable 버전의 기능만을 취사선택한다.

   - 안정적인 버전의 우수한 기능만을 취사선택해서 기능을 발전시킨다.

2. 사용이 편리하게 한다.

   - 일반사용자도 쉽게 접근이 가능하도록 GUI 관리툴을 제공한다. 또한 일반 개발자들이 많이 사용하는 언어로 개발하여, API 사용이 편리하도록 하여 실제 각종 서비스에 적용이 가능하도록 한다.

3. ERC-20 의 토큰 기능에 특화 하여 다른 스마트 컨트랙트 기능의 사용을 줄여서 네트워크를 원활하게 한다.

4. 이더리움보다 낮은 가격에 적은 수수료를 사용하여 토큰 관리가 가능하도록 한다.

이더소셜 어카운트

ESN 은 이더소셜의 스마트 컨트랙트를 구동하기 위한 수수료로 트랜잭션 수수료를 지불하는데 사용된다. 계정에는 두 가지 종류가 있는데 개인키에 의해 통제되는 외부 계정과 컨트랙트 코드에 의해 통제되는 컨트랙트 계정이 그것이다. 외부 계정은 아무런 코드도 가지고 있지 않으며, 이 계정에서 메시지를 보내기 위해서는 새로운 트랜잭션을 하나 만들고, 서명을 해야 한다. 컨트랙트 계정은 메시지를 받을 때마다, 자신의 코드를 활성화, 읽기, 내부 저장공간에 기록, 다른 메시지들을 보내거나, 컨트랙트들을 차례로 생성하게 된다.

메시지와 트랜잭션

트랜잭션은 이더소셜의 전송내역을 말하는 것으로 누가 누구에게 무엇을 보내는지에 대한 정보가 들어있다. 이 트랜잭션은 다음을 포함하고 있다.

- 수신자
- 발신자 서명
- 발신자가 보내는 ESN 의 양
- 옵션 데이터
- 허용 계산 횟수
- 계산 수수료

수신자, 발신자, 보내는 양은 대부분의 암호화폐에서 공통으로 사용하는 항목이다. 허용 계산 횟수와 계산 수수료는 이더소셜에서 DDos 공격을 막기 위한 역할을 수행한다. 트랜잭션 전송 시 실수로 무한반복 전송을 실행하거나 또는 악의적으로 무한연산을 하는 경우를 제한하기 위해 트랜잭션 전송시의 코드 실행 시 각 단계별로 ESN 을 수수료로 지불한다. 기본 단위는 1gas 이며 전송이 길거나 복잡한 경우에는 수수료를 더 많이 지불해야 한다. 이렇게 하면 악의적인 공격자가 공격을 하려면 ESN 을 많이 소모해야 하는데, ESN 을 많이 가진

소유자는 악의적인 공격을 할 유인이 적으므로 악의적 공격을 효율적으로 방지할 수 있다.

메세지(Messages)

전송 컨트랙트는 메세지를 이용해 또 다른 컨트랙트를 호출하여 정보를 전달할 수 있다. 즉 스마트 컨트랙트를 메세지를 사용해 전달할 수 있다. 메세지에는 다음 정보들이 들어있다.

- 발신자
- 수신자
- ESN
- 옵션 데이터
- 허용계산횟수

메시지는 외부 계정에 의한 것이 아니라는 것만 제외하면 트랜잭션과 유사하다. 트랜잭션과 마찬가지로, 메세지는 수신자 계정에서 해당 코드를 실행하게 된다. 트랜잭션이나 컨트랙트에 할당된 gas 는 그 트랜잭션과 연관된 모든 실행에 의해 소모된 총 gas 에 적용된다. 예를 들어, 외부 계정 A 가 B 에게 1000 gas 와 함께 트랜잭션을 보내고, B 는 600 gas 를 소모한 뒤 C 에게 메시지를 보내고, C 의 내부 실행에 300 gas 를 소모한 후 반환하면, B 는 gas 가 모두 소모되기 전에 100 gas 를 더 사용할 수 있다.

블록체인과 채굴(Blockchain and Mining)

이더소셜 블록체인은 앞에서 설명한 비트코인 블록체인과 유사하지만 여러 차이점이 있다. 가장 큰 차이점으로는 비트코인과는 달리 이더소셜 블록은 가장 최근의 계정 상태, 블록 넘버, difficulty 를 포함한다는 것이다. 비트코인은 블록에 블록넘버가 없어서 블록번호를 알려면 처음블록부터 카운트를 해야 한다.

기본적인 이더소셜의 블록검증 방법은 다음과 같다.

1. 현재 블록의 존재, 유효성 확인.
2. 현재 블록의 타임스탬프가 이전 블록의 그것보다 크고 현 시점을 기준으로 15 분을 벗어나지 않는지 확인.
3. 블록 넘버, difficulty, 트랜잭션 루트, uncle 루트, gas 제한을 확인.
4. 블록의 작업증명 POW 유효성 확인.
5. S[0] 이 이전 블록의 마지막 상태(state)라고 가정 하자.
6. 트랜잭션 목록의 오류, 소모된 gas 가 GASLIMIT 을 초과하지 않았는지 확인.
7. 채굴자에게 지불된 보상 블록을 검증.

이렇게 정보를 모두 블록에 넣는 방식은 매우 효율적이다. 트리구조로 저장되고 모든 블록 뒤에 트리의 작은 부분만이 변경되기 때문이다. 이더소셜에서는 비트코인과 달리 인접한 두 개의 블록간에는 트리의 대부분의 내용이 같기 때문에 한 번 저장된 데이터가 다음 블록에서 또 한 번 재사용될 있기 때문이다. 머클 트리 개념에 더하여 효율적으로 삽입, 삭제하는 것을 가능하게 하며 계정의 상태변화에 대한 정보가 마지막 블록에 포함되어 있기 때문에, 전체 블록체인 정보를 모두 저장할 필요가 없다.

이렇게 블록 검증을 하면서 동시에 각 트랜잭션의 컨트랙트 코드가 실행되면서 스마트 컨트랙트가 이루어진다.

어플리케이션(Applications)

토큰 시스템(Token Systems)

블록체인토큰시스템(On-blockchain token system)은 미화/금 등과 연동된 하위화폐, 주식과 '스마트자산* (Smart Property: 비트코인의 블록체인 상에서 소유권이 컨트롤/관리되는 자산)' '위조 불가능한(secure unforgeable)' 쿠폰, 그리고 통상적인 가치와 연결되어 있지 않은 기타 토큰시스템 (예, 인센티브 부여를 위한 포인트제도) 등에 이르기까지 다양한 형태의 거래시스템을 네트워크

상에서 구현하게끔 해주는 어플리케이션들을 갖고 있다. 이더소셜에서 토큰시스템은 놀랍도록 쉽게 구현할 수 있다. 토큰시스템을 이해하는 데에 핵심은 아래와 같다.

보상형 커뮤니의 적용 과정

코인의 사업화 과정에서 필요한 것들

이더소셜은 지불형 컨텐츠 포럼을 위해 설계되었으며, 또한 블로그 형태의 컨텐츠 제작자들을 포럼으로 묶는 역할을 하게 된다. 코인은 서버나 DB 인증을 벗어나서 컨텐츠에 대한 클릭형 보상, 추천보상, 직접적인 구매에 모두 적용가능하며, 다양한 포탈에서 활동하던 서로 다른 서버기반의 컨텐츠를 하나로 묶어 낼 수 있다. 수많은 코인들이 각자의 역할을 하나 이상 가지고 출시되곤 한다. 블록체인의 기술과 각종 응용소프트웨어를 활용할 수 있는 백서를 통해서 블록체인이 얼마나 많은 분야에 기여할 수 있는 지 확인할 수 있다. 하지만 수많은 코인 중에서 백서대로 실용화된 코인은 극히 소수에 불과하며, 이는 코인과 블록체인의 상용화에 심대한 의혹을 불러일으키고 있다. 이미 검증된 보안과 전송 기술이 많고, 또한 수많은 응용소프트웨어 및 각종 컨텐츠 유통이 가능함에도 불구하고, 실생활에 적용된 코인이 적은 이유를 고찰해본다.

1. 제일 먼저 블록체인 생태계와 일반적인 컨텐츠/소프트웨어 개발진과의 괴리를 들 수 있다. 아직까지 블록체인은 가상화폐 영역에 속하는 것으로 간주되며, 주로 채굴자나 투자자들의 관심을 받고 있어, 다른 소프트웨어 개발자들의 관심도가 낮은 편이다.

2. 또한 코인에 투자되는 대부분의 ICO 등의 투자금액은 실질적인 응용소프트웨어의 정착보다는 효과적인 마케팅을 통한 코인의 안정적 런칭을 주요한 관심사로 하는 바, 결국 코인을 생성하고 상장을 통해 기존 투자자의 이익에 먼저 초점을 맞추는 경향이 크다.

3. 몇 번의 시도가 있었으나, 블록체인이 여전히 보안을 중심으로한 소유와 이동에 초점이 맞추어져 있다 보니, 다른 기능을 첨부하여 속도의 저하나 네트워크의 리소스를 감소시키는 것에 대하야 반감이 있는 편이다. 이유를

떠나서 코인은 단순한 소유나 거래의 대상이 아니라, 다양한 응용소프트웨어 및 시스템과 거래하여 보다 쓰임새를 확대할 필요가 있다. 이러한 상황에서 계속적인 ICO 와 신규 코인투자의 범람은 자칫 암호화폐 생태계 전체를 투기판으로 만들 우려가 있다. 따라서 실질적인 소프트웨어 결합과 운영의 사례가 필요한 시기이다.

이더소셜은 기존 암호화폐 포럼 땡글을 기반으로 실질적인 포럼 운영에 필요한 모듈을 공급하고, 포럼 운영에 적용된 사례를 수집하는 것에서부터 출발한다. ICO 등의 자금모집 수단을 배제하고 채굴과 코인의 생산/배포에 이르는 전 과정을 투명하게 공개하고, 집단지성과 합의에 의한 방향성을 도출한 결과물이라 할 수 있다.

포럼 활성화를 위한 코인의 특성

포럼 운영자는 기존의 마일리지의 개념에서 보다 확대된 리워드 시스템을 구축할 수 있다. 포럼 내에서는 기존의 포인트나 마일리지로 활용할 수 있으며, 외부의 제휴사나 광고 마케팅에 대한 리워드를 코인으로 대체할 수 있다. 이더소셜이 제공하는 토큰으로 제작된 각 포럼 코인은 기본적으로 자유롭게 배포/상장/거래될 수 있다. 이러한 환금성을 바탕으로 추가적인 확장이 가능하다.

1. 다른 포럼과 광고주에게 직접적인 리워드 제공이 가능하다. 즉 광고주에게 일정량의 코인을 사전배포하고, 광고주가 직접 리워드를 고객에게 제공할 수 있다.

2. P2P 거래나 중고 거래에 적절한 에스크로 서비스 제공이 가능하다. 즉 입금액을 토큰과 함께 제공하여, 거래와 완료됨을 승인함과 함께 현금화 할 수 있으며, 그 토큰 자체를 다시 거래할 수 있다.

3. 특히 게임의 등수 등에 대해 추가적인 리워드가 가능하다. 외부의 게임사와 제휴할 때 토큰을 활용하여 쉽게 포럼 사용자를 게임사에, 혹은 게임사의 사용자들의 활동을 포럼으로 가져올 수 있다.

4. 이러한 기능은 기존의 마일리지나 포인트, 레벨을 수정하지 않고 바로 적용할 수 있다. 땡글의 활용예시처럼 기존의 포인트를 환산해서 지급하고, 활용할 수 있다.

기본적으로 포럼이 코인을 배포하고, 이동하고, 관리하고 싶다면, 지갑과 함께 다양한 코인 컨트롤 부분이 필요하다. 이러한 부분은 기본적으로 이전의 '거래소'가 하던 역할과 비슷하다.

코인을 활용하기 위한 포럼의 필수 요소

1. 사용자는 자신만의 입금용 지갑을 생성할 수 있으며, 해당 지갑을 통해서 외부의 코인이나 토큰을 블록체인 네트워크상에서 받을 수 있다.

2. 포럼은 본인의 핫월렛 하위로 사용자별 입금지갑을 생성할 수 있으며, 외부에서 일시에 들어오는 포럼의 코인을 수령할 수 있다.

3. 사용자가 코인의 거래규약을 생성하고 이를 실행시키도록 하는 행위, 즉 거래소에서는 현금을 동반한 쌍방 거래가 주로 이용되지만, 포럼에서는 추천, 기부, 응모 등의 형태로 각 코인의 주소가 바뀌게 된다.

4. 이러한 것들이 포럼(본 장에서는 거래소)에서 발생할 경우 외부의 블록체인망을 활용하지 않고, 직접 DB 이동하게 된다.

5. 각 사용자는 출금용 지갑을 생성할 수 있으며, 이를 활용하여 외부의 포럼, 개인 지갑, 그리고 상장되어 있는 경우라면 국내외의 거래소로 직접 송금할 수 있다.

6. 포럼 내부에서는 로그인, 댓글 작성, 추천 등의 행위에 따라서 포럼 내부 규약에 따라 관리자가 지급할 수 있다.

7. 각 회원은 다른 회원에게 기부하거나, 댓글에 대한 답례로 코인 지급할 수 있으며, 자신의 활동에 따라 다른 사용자의 코인을 수령할 수 있다.

8. 거래를 위한 증명을 위하여 특정 사용자의 특정 부분의 코인을 잠금 상태로 만들 수 있다. 이러한 잠금 상태(Lock in)는 에스크로 기능뿐만 아니라,

다양한 거래에 대한 증거금 역할, 배팅 프로세스 등으로 활용할 수 있으며, 이후의 액션과 연계하여 실질적인 승인절차와 이어질 수 있다.

9. 즉 조건부 이벤트뿐만 아니라 사용자간의 내기나 배팅에 사용할 수 있으며, 보다 강력한 모듈을 활용하여, 포럼내의 간단한 게임 등에 적용할 수도 있다.

10. 자체적으로 수수료 도입이 가능하도록 기본설계 되어 있다. 포럼의 관리자는 사용자들간의 거래에 일정한 수수료율을 사전에 지정할 수 있으며, 이를 통해 일정부분의 코인 수익을 회수할 수 있다.

11. 이더소셜 및 그 기반의 코인도 블록체인을 활용하기 때문에 포럼 외부와의 입출금시 블록체인 채굴자들을 위한 수수료가 발생하며, 이는 채굴자들의 수익이 된다.

12. 수수료율은 포럼 스스로 결정할 수 있으나, 수수료율이 너무 낮을 경우 다른 블록체인 코인과 마찬가지로 채굴자들에 의해 거절되거나 많은 딜레이를 경험하게 된다. 이는 이더소셜의 회사가 관여하는 바가 아니다.

13. 포럼 내외의 각종이벤트에 현금대신 응모할 수 있으며, 인당 수령제한을 두어 일부 코인 대량 보유자의 횡포를 막을 수도 있다.

14. 특히 추천 등의 사용자 액션에 대한 리워드로 이더소셜 혹은 토큰을 사용을 권장하고 있으며, 실질적인 컨텐츠 생산자가 수익을 발생할 수 있도록 하는 것을 목적으로 하고 있다.

15. 작은 포럼의 자체 코인 개발은 블록체인의 기술뿐만 아니라 채굴에 의한 검증과정에 어려움이 있을 수 있으므로, 이더소셜상의 토큰 발행을 권장한다.

게임 등 보다 다양한 포럼으로의 확장기능

이더소셜은 특히 컨텐츠 리워드형 포럼에 우선 적용할 수 있게 설계되었으며, 향후 게임 포럼과 소셜 네트워크 서비스에 적용하기 위한 모듈을 지속적으로 확장해갈 예정이다.

1. 외부 광고를 이더소셜 혹은 이더소셜을 기반으로한 토큰으로 직접 구입하게 할 수 있다.

2. 이러한 광고 리워드를 컨텐츠 생산자에게 제공할 수 있다.

3. 1 인당 추천이나 기부에 제한을 두는 기능을 제공하여, 보다 민주적인 투표가 가능하도록 도울 수 있다.

4. 블로그와 포럼 내의 포럼 모두에 같은 리워드가 가능하도록 제공한다. (심지어 포럼 외부의 블로그에도 리워드 전송이 가능하다. 이 경우 해당 블로그는 이더소셜 지갑을 가지고 있어야 한다.)

5. 코인 보유량의 순위별 노출, 추천 등의 기능을 제공하지만, 이를 생산자가 직접확인 할 수 없게 하는 것을 권장한다. (포럼 운영자의 권한으로 보유 코인을 노출 할 수 있고, 특정 코인 이상의 회원을 대상으로 마케팅이나 컨텐츠 제공도 가능하도록 지원한다.) 하지만 코인 자체가 외부로의 전송이 허용되는 한, 보안상의 이유로 가급적 노출되지 않도록 해야 한다.

실제 적용을 위해 필요한 API 들

포럼에서 핵심적인 사항들의 기능을 정의하고, 해당 모듈의 구현 방식을 설명한다. 코인을 실제 소프트웨어에 적용하기 위해서는 기본적으로 지갑을 각 회원에 배분하는 시스템을 보유해야 한다. 이러한 장벽은 보안을 시작으로 여러 가지 기존 거래소들이 안고 있던 어려움과 같아진다. 코인이 비록 저작권을 보호하고 유통시키도록 설계되었더라도, 그 사용자가 지갑을 프로그래밍 해야 한다면, 어차피 사용할 수 없는 개념만 존재하게 된다. 이더소셜은 이러한 근본적인 문제를 해결하기 위해서, 응용소프트웨어가 지갑과 코인을 컨트롤 하는 부분에 대해 추가적인 API 를 제공함으로써 솔루션을 제공한다. 초기 API 는 기본적으로 포럼에 한정되며, 이후 블로그와 게임 아이템 거래를 활용하기 위한 API 가 지속적으로 추가될 예정이다.

기본적으로 필요한 API 리스트들

1. 락인

- 정의 : 락인의 기능은 사용자의 코인을 특정기간 동안 혹은 특정 이벤트가 발생하는 시점까지 상태변화를 고정하는 것을 뜻한다.
- 이는 기본적으로 거래등의 이후의 행동을 보장하거나, 에스크로 기능을 제공하기 위해서 설정된다.
- 대부분의 락인은 사용자가 스스로 선택한 액션에 의해 이루어지지만, 일부는 시스템이 자동으로 부여한다.
- 사용자 지정 락인의 종류 : 거래를 위한 준비, 경매, 취소가 가능한 전송
- 시스템 지정의 락인 : 계정의 블록상태, 거래 승인에 대한 준비
- 락인 해제 기법

2. 코인의 생성(포럼에서 사용자에게 배포하는 행위)
   - 정의 : 실제 코인이 생성되는 것이 아니라, 포럼 내부 보유분이 회원에게 배포되는 행위
   - 기본적으로 포럼 내부의 마일리지 시스템이나 포인트와 결합하여 지급됨.
   - 이벤트 참여, 댓글, 추천등을 통해 지속적으로 배포할 수 있도록 한다.
   - 배포하는 API 에는 "악용"의 소지가 가장 많다. 이는 기능적인 해킹 이외에 회원가입의 반복, 추천의 도움 등이 지속적으로 발생한다. 만약 API 적용에 적절한 캡을 생성하지 못할 경우, 매우 치명적인 문제를 야기하고, 밤새 보유 코인이 증발하고, 포럼 내 인플레이션이 급증할 수 있음을 명심해야 한다.
   - 수동 배포를 지원한다. 코인의 자동 배포가 가능하지만, 수동배포를 통해 전체적인 총량을 관리해야 한다.

3. 일방적인 제공

- 정의 : 사용자가 다른 사용자 혹은 객체(기업회원 등)에게 코인을 포럼 내에서 전송하는 행위
- 유료추천이나 이벤트 응모, 기부 등으로 활용한다.
- 거래로 보이지만 일방적인 제공으로 처리하는 경우는 추후 확정되지 않은 약속(언젠가 소설이 발간되면 받기로 하는 등의), 공개 등 받을 수 없는 것들은 일방적인 제공으로 처리한다.
- 일방적인 제공은 지갑을 통해 외부로 빠져나가는 '지갑출금'과 구별된다.

4. 쌍방 거래
   - 정의 : 사용자간에 코인을 포함하여 거래하는 행위
   - 포럼은 거래소가 아니므로, 자주 발생하지는 않지만 중고거래나 디지털 컨텐츠 거래로 작용할 수 있다.
   - 매우 한정적인 API 가 제공될 예정이다. 이 부분을 광범위하게 사용하기 위해서는 보다 수준높은 프로그래머와 함께 개발을 진행하길 권장한다. 기본 제공 API 는 이런 상업적 목적 전체를 포함하지 않으며, 이러한 상업적 사용은 보다 광범위한 보안적 이슈와 책임 소재를 포함한다. 기본 API 는 서비스 자체를 보증하지 않으며, 이러한 부분은 각 포럼의 책임하에 추가적인 프로그램 작업을 해야 한다.

5. 지갑 입출금 주소의 생성
   - 정의 : 개별 사용자의 코인을 받기 위한 포럼의 지갑 주소 생성 및 관리
   - 코인의 지갑은 비록 "토큰"형태라 하더라도 개인 지갑을 생성하고 관리할 수 있다. 하지만 포럼 회원이 지갑을 굳이 가지고 있을 필요도 없으며, 이는 불필요한 낭비에 가깝다. 포럼은 각 회원별 입출금이 가능한 지갑의 주소를 생성하고 관리해줌으로써, 외부의 코인을 쉽게 받거나 보낼 수 있게 해준다.

- 입출금과 실제 내부의 보유 코인에 대한 밸런스 관리가 매우 중요하다. 이는 별도의 API 가 제공되기 어려운 항목이기도 할 뿐 아니라, 포럼 정책에 매우 밀접한 관계가 있다. 이러한 부분은 지갑 부분의 밸런스를 기반으로 포럼의 다른 파트의 밸런스를 잘 맞추거나, 임의의 밸런스 조정계정을 생성하여 조정해야 한다.

- 실제 입금과 출금을 위한 블록체인상의 문제(현재 승인의 단계, 블록체인 내부 거래정보의 열람)는 가급적 이더소셜에서 제공하거나, 외부 개발자들의 탐색툴을 활용하도록 한다.

보상형 컨텐츠 포럼의 개발계획

현재 포럼의 일반적 형태

1. 땡글은 토론이 중심이 되는 포럼의 형태이다. 따라서 본문의 컨텐츠 생산에 따른 부담이 적고, 댓글이나 다른 사용자의 참여로 보다 좋은 컨텐츠가 완성된다. 하나의 컨텐츠는 생산 이후 토론과 검증, 각 진영별 입장에 따라 의견이 갈리고, 이 모든 과정 전체가 좋은 정보와 컨텐츠가 된다.

- 게시판 형태이므로, 컨텐츠는 작성자가 아니라 포럼에 종속되며 별다른 수익이 제공되진 않는다.

- 필연적으로 지지와 비난, 검증을 거친다.

- 유명한 필자라 하더라도, 필자중심의 검색보다는 일반적인 추천된 게시글에 의지한다.

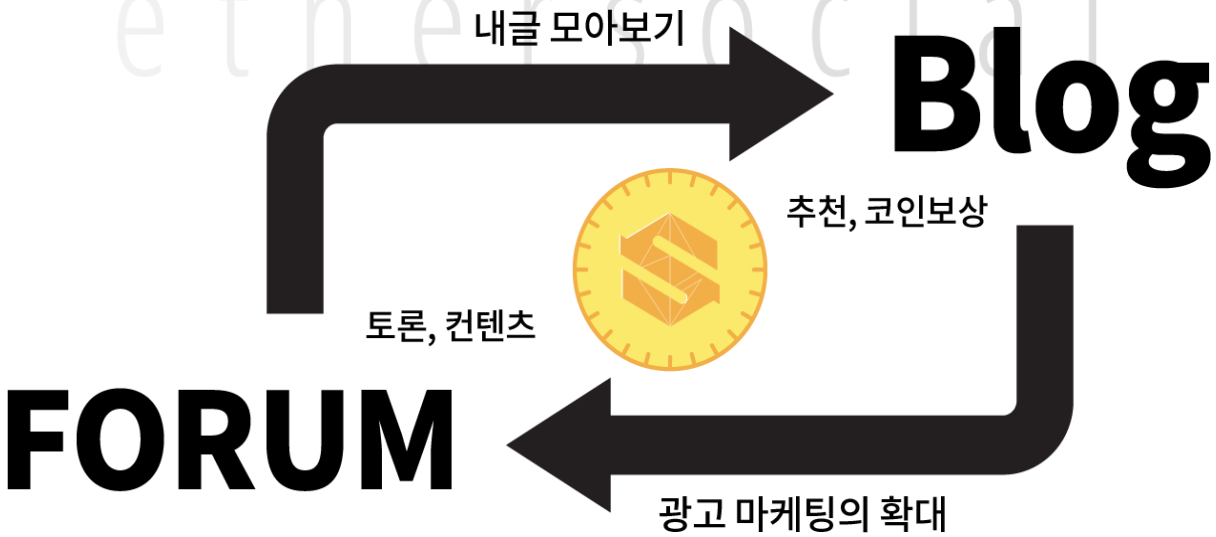
- 게시판은 평준화 되어 있으므로, 지속적인 관리가 필요하다. 평등한 포럼이 꼭 좋은 것은 아니다. 다양한 신규 진입자와 부적절한 게시글의 관리가 필수적이다.

2. 개인의 블로그 형태의 포럼. 개인의 창작물 제작이 가능하고, 블로그를 장기 연재할 수 있으므로 높은 수준의 컨텐츠 제작 및 제공에 유리하다. 다만 자신을 많이 홍보 및 노출시켜야 하는데 어려움이 있어 부익부 빈익빈 현상이

가중된다. 개인별 서비스이므로 광고비나 제휴비 등의 실질적 매출이나 수익을 발생 시킬 수 있다. 이러한 동기부여는 창작자에게 늘 큰 도움이 된다.

- 블로그 형태는 창작자의 능력에 비례하는 문제가 있지만, 훨씬 훌륭하고 다양한 연출과 표현이 가능하다.
- 따라서 창작에 대한 노력이 많이 필요하고, 품질의 차이가 엄청나게 벌어진다.
- 광고 등의 수익모델을 다양하게 펼칠 수 있으며, 많은 팔로워나 이웃을 지속적으로 확대하여 안정적인 컨텐츠 제공처를 확보하고 결과적으로 수익을 증대시킬 수 있다.
- 저작권이 분명하다.
- 컨텐츠의 정리 및 분류가 분명하고 쉬운 편이다.

개발 방향



게시판 형태의 토론형 포럼과 블로그의 장점을 혼합하고, 수입배분과 컨텐츠 활성화에 코인을 매개로 하여 보다 적극적으로 개입할 수 있도록 한다. 이를 위해서 일반적인 창작자도 응용이 가능한 이더소셜 코인의 응용소프트웨어 API 를 활용한다.

1. 게시판의 본인의 게시물을 블로그 형태로 그룹핑할 수 있도록 한다.
    - 기본적으로 토론과 검증이 되는 게시판, 포럼의 형태를 유지한다.
    - 본인의 게시물을 그룹핑해서 블로그화 하거나, 링크될 수 있도록 하고, 이를 분류하여 정리할 수 있도록 한다.
    - 해당 본문의 광고나 클릭에 대한 정보를 공유할 수 있도록 한다.
2. 코인을 활용한 '비용지불형 추천'과 민주적 추천을 모두 허용하고, 직접적인 수익이 발생할 수 있도록 한다.
    - 광고비나 추천 등에 이더소셜을 활용하여, 창작자에게 직접적인 보상이 지불되도록 한다.
    - 광고주는 코인을 구매하여 보다 향상된 필터를 활용하여 충전해 둘 수 있도록 한다.
    - 본문과 댓글 모두에 "비용지불형 추천"을 활용하여, 독자가 창작자에게 보상할 수 있도록 한다.
    - 추천 등에 일인당 한도 설정이 가능하도록 하여, 필요 시 민주적 순위 결정이 가능하도록 한다.

적극적 수익배분

이더소셜을 활용할 경우, 우리가 제작하는 포럼에서 뿐만 아니라, 외부의 제휴사이트나 개인적인 홈페이지에서도 우리의 지갑을 통해 광고비를 받거나, 기부를 받을 수 있다. 기존 컨텐츠를 활용해서 추가적인 수익을 만들고 자신의 블로그를 새로운 포럼에 입점시키는 효과를 누릴 수도 있다.

2018 년 4/4 분기 신규 보상형 컨텐츠 포럼 업데이트를 목표로 하고 있다.

이더소셜 개발자들을 위한 보상 프로그램

보상 프로그램의 범위

이더소셜은 탄생부터 포럼의 집단지성을 기반으로 생성되었으며, 개발진 이외에 보다 광범위한 참여자들의 기여로 탄생되었다. 따라서 코인의 배포과정서부터 이러한 개발에 참여한 개발자, 마케팅 도움뿐만 아니라, 블록체인 및 암호화폐의 개선과 발전에 기여한 다양한 종사자들에 대한 보상프로그램을 포함하고 있다. 반드시 이더소셜의 개선일 필요는 없으며, 또한 땡글이나 우리 개발을 위한 깃허브 이외의 활동을 포함한다. 채굴을 위한 하드웨어 혹은 관리 소프트웨어, 기존 코인의 실질적인 활용을 위한 제안들을 포함하며, 수익의 유무와 상관없다. 다만 이러한 보상 프로그램은 ICO 를 위한 신종 코인 개발은 제외하였다. ICO 자체는 아직은 수익화 모델에 더 가깝기 때문이며, 추후 변경될 가능성은 있다. 보상 프로그램 범위에 대한 상세한 기준은 아래와 같다.

1. 이더소셜의 개발 기여자
    - o 이더소셜의 깃허브에 직접적인 소스의 개발, 수정, 안정화 작업에 기여
    - o 프로그램이 아닌 위키의 내용에 대한 추가, 수정 보완에 기여
    - o 각 국가별 언어 및 정책적 개선방향에 대한 기여
    - o 이더소셜의 실질적 활용에 대한 국내외 업무제휴에 기여
    - o 개인 기여도 평가 알고리즘 개발에 기여
2. 채굴 시스템의 개선자
    - o 국내외 이더소셜 채굴풀 개발 및 유지 관리에 기여
3. 코인의 응용소프트웨어 개발자
    - o 포럼, 소셜 네트워크 서비스, 게임 및 Media 관련 이더소셜 기반의 DApp 개발에 기여

- 응용소프트웨어의 개발 및 개선을 위한 API 개발에 기여

4. 마케팅 및 소셜 네트워크 서비스를 활용하여 암호화폐의 개발뿐만 아니라 이미지의 개선에 힘쓴 자

   - 질적, 양적 컨텐츠를 제공하여 이더소셜 마케팅 및 활성화에 기여

5. 정책의 입안 혹은 방향성에 대한 고찰에 기여한자

6. 새로운 개념과 가능성에 대해 기여한자

   - 이더소셜의 기술적, 활용적 확장성에 대한 기여

보상프로그램 운영

이더소셜의 도전과제는 공정하게 기여도를 평가하여 보상을 지급하는 것이다. 추가적인 기여와 보상에 대해 이더소셜의 개발 포럼에서 지속적으로 논의할 예정이며, 이러한 논의 결과는 지속적으로 반영될 예정이다. 세부적인 지원 플랜은 아래와 같다.

1. 개인별 기부 활성화 방안

   - 컨텐츠 제작자 혹은 프로그래머, 마케팅 담당자는 이더소셜 제작자 포럼에 등록하고 기부를 위한 익명의 계정을 생성할 수 있다.

   - 이 계정은 개인정보가 노출되지 않으며, 이더소셜의 주소를 내부에 포함하고 있다.

   - 이곳에 등록된 계정에 누구라도 기부를 하게 되면, 이더소셜 운영진이 해당 기부액과 동일하게 추가로 기부하게 된다.

   - 물론, 1 인 기부의 한도가 있으며, 한 명의 과도한 기부로 인해 운영 기금이 고갈되는 것을 방지하고, 보다 공정한 집행이 가능하도록 조정될 예정이다.

- o 이더소셜이 제공하는 모듈은 기부의 안정성을 높이고, 해당 기부에 상당하는 액수를 추가로 제공하여 컨텐츠 제공자의 이익에 부합하도록 설계되었다.

- o 기부자에 기부액에 상응하는 혜택을 지급하여 개인별 기부를 활성화할 예정이다.

2. 투표에 의한 기여도 순위에 대한 보상 플랜

- o o 개인 기여도에 대한 보상은 사실상 객관화가 불가능하기 때문에 정기적 혹은 비정기적으로 투표를 진행하여 집단지성을 반영한 순위를 공개 및 보상을 진행한다.

- o o 매월 혹은 비정기적으로 이더소셜 홈페이지를 통해 추천을 받아 대상 리스트를 선정한다.

- o o 선정된 인원의 실질적인 활동 및 도움 내용을 공개, 온라인 투표를 진행한다.

로드맵

* 2017 년 12 월 26 일 최초의 ESN 채굴

* 2018 년 01 월 15 일 포럼 '땡글'회원 중 선정을 통한 베타테스트 진행

* 2018 년 1 월 넷째주 포럼 '땡글'에 코인 5 백만개 배정(향후 10 년간 진행 예정)

* 2018 년 1 월 넷째주 ESN 코인 채굴풀 오픈

* 2018 년 1 월 넷째주 '땡글' 회원대상 일괄 코인 배포방향 공지

(기존 회원 등급과 활동지수 반영) * 2018 년 1 월 넷째주 이더소셜 코인 정식 런칭 (공식 출시)

* 2018 년 02 월 '땡글' 회원 대상 추가 코인 배포

* 2018 년 02 월 ESN 공식 백서 릴리즈

* 2018 년 03 월 ESN 기반의 타 포럼 공동개발 발표 (타 포럼 토큰 개발 기술지원)

* 2018 년 04 월 외부 포럼용 API 공식 발표 (땡글 적용 사례등)

* 2018 년 04 월 마이닝 컨퍼런스를 통한 밋업개최

* 2018 년 3/4 분기 해외 포럼용 코인 런칭

* 2018 년 3/4 분기 해외 거래소 ESN 상장

* 2018 년 4/4 분기 국내외 2~3 개 내외의 외부포럼 코인 출시

* 2018 년 4/4 분기 포럼+코인의 통합 운영툴 출시

* 2018 년 4/4 분기 "컨텐츠 보상형 포럼" 해외 런칭

그 밖의 이슈들

엉클블록의 도입

이더소셜은 다음과 같은 이유로 엉클블록을 도입한다.

이더소셜은 비트코인의 10 분에 비해 블록생성주기가 매우 짧다. 이로 인해 보안성 저하라는 문제가 생기는데 그 이유는 다음과 같다. 채굴자 A 가 블록을 생성했다고 가정해보자. A 는 블록을 생성하고 그 블록을 네트워크에 전파한다. 그런데 아직 A 의 블록이 채굴자 B 에 도달하지 않은 그 시간에 채굴자 B 가 블록을 생성할 수도 있다. 이더소셜은 블록에 블록번호가 들어가기 때문에 채굴자 A 의 블록과 채굴자 B 의 블록은 같은 블록번호를 가지게 된다. 이 경우 비트코인에서는 채굴자 A 의 블록만 인정되고 채굴자 B 의 블록은 버려지게 되는데 이는 채굴자 B 의 자원이 낭비가 되고 네트워크 보안에도 기여를 하지 못하게 되는 결과를 초래한다.

게다가 중앙집중화(centralization) 이슈도 있다; 만일 채굴자 A 가 30%의 해시파워를, 그리고 B 가 10%의 해시파워를 가지고 있다면, A 가 스테일 블록을 생산할 위험성은 매번 70%가 될 것이고(왜냐하면 다른 30%의 경우에는 A 가 마지막 블록을 만들게 되었고, 따라서 즉각적으로 채굴데이터를 가지게 되기 때문이다), 반면 B 는 매번 90%의 경우에 스테일 블록을 생산하게 될 위험성을 가지고 있다. 따라서 만일 블록 주기가 스테일 비율이 높은 것에 필요한 만큼 충분히 짧다면, A 는 단순히 크기가 크다라는 사실 자체만으로 훨씬 더 높은

효율성을 가지게 된다. 이러한 두 가지 효과가 결합되어서, 블록주기가 짧은 블록체인에서는, 높은 해시파워 점유율을 가진 단일한 풀이 채굴과정에 대한 사실상의 통제권을 가지게 될 가능성이 매우 높아진다.

그래서 단순히 가장 긴 체인의 블록에만 보상을 하는 것이 아니라 거의 동시에 만들어졌지만 두번째로 만들어진, 해시가 약간 낮은 블록에도 채굴 보상을 지급한다. 하위 블록에 대해서는 삼촌뻘의 블록이어서 삼촌 이라는 뜻의 엉클블록이라고 한다. 이 엉클블록도 기존 보상의 87.5%를 받게 되며, 그 엉클블록을 포함하고 있는 사촌뻘의 블록이 나머지 12.5%를 받는다. 하지만 전송수수료는 엉클블록에 주어지지 않는다.

이더소셜의 엉클블록은 최대 7 세대까지만 엉클블록의 보상을 제공한다. 그 이유는, 첫째, 무제한으로 하게 되면 무수히 많은 엉클이 기하급수적으로 늘어나면서 계산이 매우 복잡해진다. 둘째, 무제한으로 엉클보상을 하면 채굴자들이 메인에 대해서 채굴을 하는 것이 아니라 의도적으로 엉클블록에서 채굴을 진행할 수 있게 되기 때문이다.

수수료

블록체인에 포함되는 모든 트랜잭션은 그 트랜잭션을 다운로드하고 검증하기 위해서는 컴퓨팅 자원이 필요하기 때문에 이를 사용하는 비용, 전송수수료를 지불해야 한다. 전송수수료가 없다면 무수히 많은 트랜잭션을 남발하여 컴퓨팅 자원이 소모되고 의미 있는 전송이 제대로 이루어지지 않는 문제점이 생기므로 전송수수료는 반드시 필요하다. 마찬가지로 ERC-20 토큰의 전송을 위해서도 토큰 전송의 남용을 방지하기 위해 전송수수료를 지불해야 한다. 비트코인 채굴에서는 전송자가 자발적으로 수수료를 책정하고 시장경쟁원리에 따라 높은 수수료부터 채굴이 가능하게 되기 때문에 수요, 공급의 원리에 따라 수수료와 채굴의 블록생성이 결정된다.

하지만 여기에는 문제가 있는데, 트랜잭션을 처리해서 블록을 만들 때 이익을 극대화하려는 채굴자들은 항상 존재한다는 것이다. 그래서 다음과 같은 문제점이 발생할 수 있다.

첫째, 블록을 생성하려면 많은 트랜잭션을 검증하고 블록을 생성하는 해시를 만들어야 하는데 트랜잭션을 검증하는 만큼 시간이 소모되면서 블록의 생성시기라 늦어질 확률이 커져서 채굴자가 수익을 얻지 못할 수 있다. 그리고 늦는 만큼 다음 블록 생성 준비시간이 짧아져 블록을 생성활 확률은 더욱 낮아진다. 둘째, 채굴자들은 검증에 시간이 적게 걸리고 수수료 수익을 극대화할 수 있는 트랜잭션만 포함하려 한다.

이런 이유로 합리적인 수수료체계가 존재하지 않는다면 이더소셜 및 ERC-20 토큰의 트랜잭션의 전송이 제대로 이루어지지 않는 문제점이 생길 수 있다.

통화 그리고 발행(Currency and Issuance)

이더소셜 네트워크는 그 안에서 자체적으로 통용되는, 'ESN'이라는 화폐를 가지고 있다. ESN 은 여러 가상자산들간의 효율적인 교환을 가능하게 하는 매개물의 역할을 하며, 또한 트랜잭션 수수료(transaction fee)를 지불하기 위한 방법을 제공한다. 사용자의 편의와 향후 있을 지 모르는 논쟁을 예방하는 차원에서, ESN 의 각 단위에 대한 명칭은 다음과 같이 미리 정해졌다. (비트코인 명칭과 관련하여 벌어지는 논쟁 참조)

- 1: wei
- 10^{12}: szabo
- 10^{15}: finney
- 10^{18}: ESN

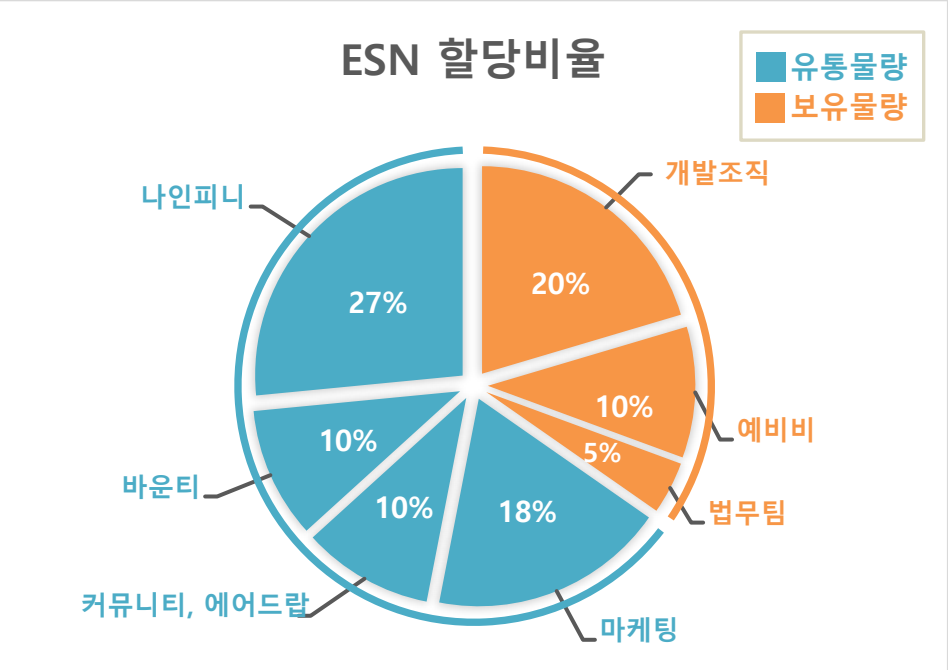
위 명칭들은, 미화 명칭인 "달러"와 "센트" 또는 비트코인의 "BTC"와 "사토시" 등의 확장개념으로 생각하면 이해하는데 도움이 될 것이다. 나머지 명칭들은, 지금 당장은 클라이언트에 포함시키지 않는다

화폐발행 모델:

• 이더소셜 조직을 금전적으로 지원하고 개발에 필요한 비용을 모아 개발자를 위한 월급과 보상, 그리고 여러 가지의 이더소셜 관련 영리와 비영리프로젝트를 위한 투자금으로 사용된다.

※ ESN 할당비율

[총 발행량 100%] = [보유물량 35%] + [유통물량 65%]



• 이더소셜이 외부 공개되기 이전에 확보된 초기 이더소셜 물량은 개발조직(Geminis)에서 보유했으며, 총 발행량은 4,900 만 ESN 의 규모였다. 이 금액은 크게 보유물량과 유통물량으로 배분되는데, 보유물량은 개발조직 내부에서 장기적으로 보관하는 ESN 이며, 유통물량은 적극적으로 외부에 유통하는 물량으로 일반 사용자들에게 유통된다.

※ 보유물량

• 보유물량은 총 발행량의 35%인 1,700 만 ESN 이며, 개발조직을 위한 비용, 예비 비용, 법적 비용으로 각각 사용된다. 개발조직을 위한 비용이란 ESN 코어 및 생태계의 개발과 유지를 위한 비용으로 개발팀이 직접적으로 활용할

수 있는 부분으로 1,000 만 ESN 이 배분되었다. 이는 총 물량 대비 20%에 해당한다.

- 보유물량 중에서 예비비는 500 만 ESN 으로, 전체 물량의 10%를 차지한다. 예비비용은 장기적으로 매도하지 않은 상태로 보유할 예정이며, 돌발상황이 발생할 경우 사용될 수 있다. 이외에도 법무비용 200 만 ESN 은 전체 물량의 5%로 법률자문 등의 비용으로 사용될 예정이다.

※ **유통물량**

- 유통물량의 발행량은 전체의 65%인 3,200 만 ESN 으로, 마케팅, 바운티 이벤트 등을 통해 외부에 적극적으로 유통된다. 마케팅은 전체의 18%인 900 만 ESN 으로 ESN 의 적극적 광고 및 홍보 등의 마케팅 비용으로 활용된다. 커뮤니티, 에어드랍에는 10%인 500 만 ESN 이 배분되어 더욱 많은 사용자가 ESN 을 이용할 수 있도록 한다.

- 바운티는 특정 미션을 수행하거나 개발 및 디자인 등에 기여한 사용자에게 제공하는 ESN 으로, 10%인 500 만 ESN 이 배분되어 ESN 의 개발과 확산을 장려한다. 나인피니에는 총 물량의 27%인 1,300 만 ESN 이 배분되어 이더리움을 통해 교환이 가능하다. 또 나인피니는 ESN 의 해외 진출을 위한 에이전트 역할을 수행한다.

※ **초기발행 이후의 ESN 발행량**

- 채굴시점 이후로 최초 1 년간은 18,709,078 ESN, 그 이후로는 매년 총 15,626,576 ESN 을 채굴자에게 신규 발행한다.

- 이 후 블록 난이도와 채굴난이도에 따라 채굴되는 양은 점차로 감소할 수 있다.

- 채굴 난이도와 전용 채굴기의 사용여부에 따라 채굴 알고리즘은 개발진에 의해 임의로 변경될 수 있다.

'커뮤니티, 에어드랍(땡글)'의 정당성에 대해서는 다음과 같이 설명할 수 있다. 예를 들어 10 년간 매년 일정하게 이더소셜을 분배하여 이더소셜의 사용자층을 늘리는데 기여할 수 있다. 일정비율은 포럼의 회원 기여도에 따라 분배되고 일정비율은 특정 이벤트를 통해 분배 될 수도 있다. 또는 타 포럼 또는 사이트에서 이더소셜 토큰을 사용하기 위한 기본 자산으로서 필요 시에 분배를 할 수도 있다. 만일 이러한 보유금이 없다면 이더소셜을 쉽게 얻지 못하여 이더소셜의 사용자층이 좁아질 수 밖에 없게 된다.

'이더소셜 개발조직(Geminis)의 분배'의 정당성에 대해서는 다음과 같이 설명할 수 있다. 블록체인의 개발 및 각종 API 개발 및 유지보수에는 많은 개발인력, 기획, 마케팅 인력이 필요하다. 이 조직을 운용하기 위해서는 비용이 필요하기 때문에 이 비용을 충당하기 위해 개발조직에 이더소셜을 분배해야 한다. 최소 '장기보유금'의 정당성에 대해서는 다음과 같이 설명할 수 있다. 이 장기보유금은 최소 1 년간(혹은 그 이상) 시장에 유통되는 유통량이 아니다. 최초 1 년동안 채굴보상량은 18,709,078 ESN 으로 다른 여타 암호화폐에 비해 최초 발행량 대비 채굴량의 비율이 월등히 높다. 하지만 최초 발행량만을 무리하게 높인다면 널리 사용되는 암호화폐가 되지 못하는 문제점이 생기므로 최초 발행량을 이더리움 대비 절반 이하로 낮추면서도 또한 그 비율을 너무 낮게 하지는 않는 방법으로 최소 1 년간 유통을 금지한다.

** 비교

* 이더리움 최초 발행량 72,002,436 ETH, 최초 1 년간 채굴보상량 15,626,576 ETH

* 이더소셜 최초 발행량 49,922,490 ESN, 최초 1 년간 채굴보상량 18,709,078 ESN . 이후 1 년간 채굴보상량 15,626,576ESN

정해진 양의 ESN 을 영구적으로 신규 발행하는 방법은 비트코인이 겪고 있는 '부의 집중현상'을 완화시킬 수 있다. 또한 현재 또는 미래의 참여자들이 계속해서 이더소셜을 시장이 아닌 채굴을 통해 얻을 수 있는 기회를 제공한다. 또한 이더리움보다 초기 채굴량을 늘려 300,000 블록까지는 9 ESN, 그 이후로는 5ESN 을 채굴보상량으로 정한다.

채굴 중앙집중화(Mining Centralization)

비트코인 채굴 방식은, 목표 값보다 낮은 값이 나올 때까지, 블록헤더에 대한 sha256 해싱 작업을 무한정 반복하는 것이다. 하지만 해당 방식에는 두 가지 약점이 존재한다.

첫번째는 현재 채굴참여에 대한 장벽이 매우 높아졌다는 것이다. 현재 채굴은 ASIC 에 의해 완전히 잠식되었다. 이러한 ASIC 채굴기는 일반 GPU 채굴기 등에 비해 수천배 이상의 효율을 가지기 때문에 GPU 를 통한 채굴은 경쟁력에서 밀려 효용을 잃게 되었다. 과거의 채굴행위가 분권화되어 있었다면, 지금은 ASIC 에 의한 집중화가 심화되고 있다.

두번째는 채굴방식이다. 이전처럼 여러 지역에서 여러 참여자가 블록생성에 참여하는 것이 아니라, 중앙집중화된 채굴풀(Mining pool)이 제공하는 블록헤더(block header)에 의존하여 채굴에 참여한다는 점이다. 이로 인한 부작용이 상당한데, 현재 기준으로는, 3 개 채굴풀들이 개인들의 컴퓨팅파워를 인계 받아서 무려 50%에 육박하는 해시를 간접적으로 통제하고 있다. 물론 해당 풀의 점유율이 50%를 넘어가기 전에 개인들이 다른 소규모 풀들로 이동을 할 수 있기 때문에, 풀들이 마음대로 자원을 남용할 수는 없겠지만, 이는 여전히 큰 문제이다.

이더소셜의 채굴 방식은 조금 다르다. 각 채굴자가 상태정보(the state)에서 무작위의 정보를 가져와서, 무작위로 선택 된 최근 몇 개의 블록내역을 해싱 작업하고 결과값을 내놓는 것이다. 이렇게 하게 되면 두가지 이점이 있다.

첫번째는 이더리움 계약이 모든 종류의 컴퓨터 계산방식을 포괄할 수 있다는 점이다. 따라서 자연히 ASIC 도 모든 계산방식에 적합하게 설계되어야 하는데, 이렇게 되면 결국 ASIC 이라기 보다는 일종의 고성능 CPU 가 되는 셈이다. 즉 현실적으로 ASIC(주문형 전용반도체) 자체가 무용지물이 된다.

두번째로, 채굴자들은 작업 시 전체 블록체인을 다운 받아 모든 이체내역을 검증해야 한다는 점이다. 이렇게 되면 중앙집중화 된 대형 풀이 필요 없게 된다. 물론 대형풀 자체는 신규블록생성 보상을 균일하게 참여자들에게 배분해 주는 효과가 있긴 하지만, 그러한 효과는 P2P 형식의 풀(pool)을 통해서도 충분히

구현이 가능하다. 굳이 중앙집중형 풀(centralized pool) 방식을 사용할 필요가 없다.

하지만 어느 시기가 오면 이더리움 채굴 전용 ASIC 이 나올 수도 있다. 이 시기에 ASIC 이 사용하기 어려운 새로운 해시 알고리즘을 적용하셔 분산화된 채굴을 가능하도록 해야 한다.

결론

이더소셜은 스마트 컨트랙트를 기반으로 하는 범용 ERC-20 규약을 준수하는 토큰 매니지먼트 툴과 각종 서비스에 손쉽게 접목할 수 있는 API 를 제공한다. 이더소셜은 매우 범용적인 프로그래밍 언어를 통해 '블록체인상 에스크로나 인출한도설정, 금전계약, 등의 고급 기능'을 제공하는 어플리케이션들을 다양한 서비스에서 쉽게 사용할 수 있게 만드는 관리자 매니지먼트 툴을 제공한다. 튜링완전언어를 통해 이론적으로 거의 모든 형태의 이체방식이나 어플리케이션을 만들어낼 수 있도록 지원한다. 이를 통해 일선 포럼 운영자나 계정이 존재하는 모든 서비스의 관리자가 쉽게 이런 서비스를 보편적으로 사용할 수 있게 한다.

Refernce

1. Bitcoin Whitepaper https://bitcoin.org/bitcoin.pdf

2. Ethereum Whitepaper https://github.com/ethereum/wiki/wiki/White-Paper

3. Steem Whitepaper https://steem.io/SteemWhitePaper.pdf