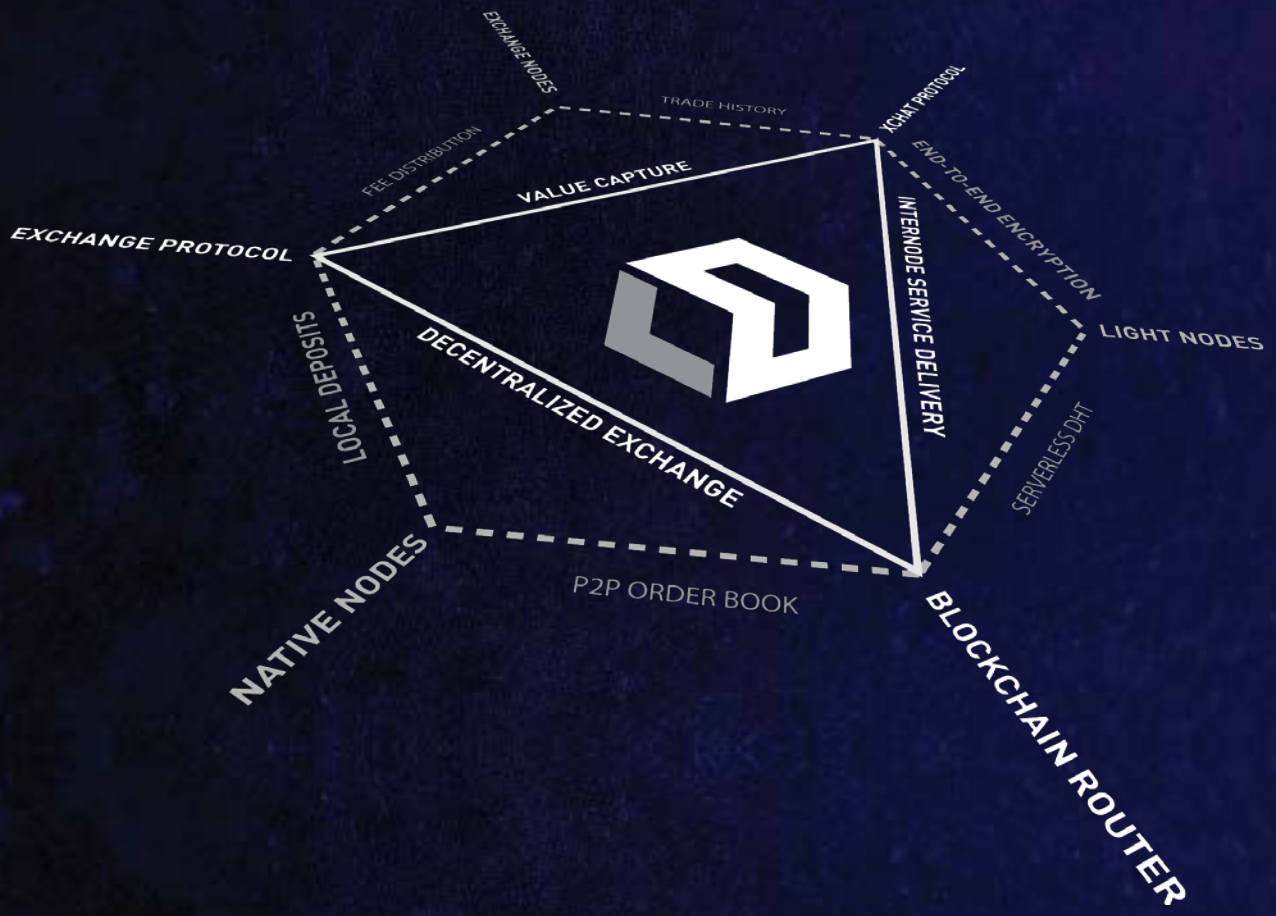


블록넷

디자인 설명서

알린 컬윅과 덴 멧칼프

알렉스 코크와 블록넷 팀원들과 함께

목차

Version control

날짜	버젼 컨트롤	제작자	관련 글
2016-08-27	0.1	알린 컬윅	컨셉위주의 기존 밑 그림
2017-05-18	0.2	알린 컬윅	최초 초기 글
2017-10-26	0.3	알린 컬윅	더 확실한 컨셉을 위한 강화된 구조
2018-01-20	0.4	알린 컬윅	저 등급의 표기 제거 후 주요 부분 부각
2018-03-07	0.5	알린 컬윅	블록체인 라우팅을 위한 디자인 위치 합작; 서비스노드에 다시쓰기와 정리정돈.
2018-03-09	0.6	알린 컬윅	서비스 노드 재료 초기 완성; 주문 시스템 프로토콜 및그림, 주문관련 섹션 추가 매칭 시스템, 주문내역 초기 프로토콜 및그림
2018-03-11	0.7	알린 컬윅	레지스트리 서비스 섹션 추가; 다수의 소규모 조정
2018-03-11	0.8	한니 아부	그림 관련 오류 및 복사과정의 오류 수정
2018-03-12	0.9	알렉스 코크	인터 체인 건축 구조를 위한 몇몇의 추가
2018-03-15	1.0	알린 컬윅	첫번째 최종 공개버젼 완성

소개글

이 소개글은 읽는이가 누구건 블록체인이 무엇인지 기본적인 이해를 돕고자 하는 취지에 쓰여졌습니다. 블록넷의 디자인과 구조는 도표와 인터체인 서비스의 단계적인 설명을 통해 최대한 비전문적인 방식으로 소개되었으며 이는 인터체인 서비스 구조를 잠재적 소비자들에게 이해시키는데에 본사가 제공해야할 최소한의 의무라 생각합니다. 이 문서는 인터체인 서비스가 무엇인지를 논함으로 시작하지만, 점차적으로 이상적인 인터체인 서비스가 무엇일지, 더 나아가 블록넷이 왜 이상적인 인터체인 서비스인지에 대해 논하게 될 것입니다.

이 문서가 쓰여진 이유

본사는 본사의 목적과 취지가 다양한 시각에서 교류되고 영감을 받는 것보다 더 나은 디자인 솔루션은 없다고 믿습니다. 본사는 더 많은 사람들이 본사가 제공한 코드를 사용, 관여하길 바라며, 외부에 공개되지 않고 본사 내부에서만 공유되는 비밀이 없어야 한다고 믿습니다. 이 혁신적인 구조적 프로젝트에는 본사가 제공한 기술을 바탕으로 많은 사람들이 적극적으로 관여해야한다는 사실을 믿어 의심치 않습니다.

몇몇의 사람들은 본사가 개발한 기술과 경험이 다른 경쟁사에게 아무런 제제 없이 도용되는것에 우려했습니다. 특히나 본사의 기술은 시장에 처음 제공되는 완전히 새로운 혁신적인 디자인, 기술이기 때문입니다. 하지만 본사가 고심끝에 내린 결론은 공개하자는 방향이었고, 이는 본사가 개발한 기술과 경험에 대한 확고한 믿음을 바탕으로 내려진 결론이었습니다. 본사는 가상화폐와 이를 보유하고 있는 투자자들과의 관계를 나누는것은 불가능하다가 결론내렸고, 본사가 제공한 가상화폐에 부여되어있는 투자대 기회비용 (risk-reward ratio) 을 통해 잠재적인 경쟁사들에 대한 우려를 잠식할 수 있었습니다.

환영합니다

블록넷은 이 문서에서는 임의상 “본사” 라고 지칭되었지만, 이때까지 존재했던 회사라는 개념과는 많이 다릅니다. 블록넷에는 소속된 직원, 임원이 존재하지 않으며, 개념상 “회사” 보다는 “구조”에 가깝습니다. 누구들 블록넷의 구조의 일원이 될 수 있고, 이 기회는 누구에게나 제공됩니다.

이 문서는 아직 완결된 최종문서가 아님을 알려드립니다. 블록넷은 최종적인 디자인이 없습니다. 왜냐하면 블록넷은 프로젝트의 진행에 따라 지속적으로 개발과 보완을 반복하여 계속 더 나은 방향으로 나아갈 것이기 때문입니다. 본사는 모든 이들의 의견을 존중하여 발전하겠습니다.

블록넷의 코드는 공개되어 있으며, 누구든 블록넷 프로젝트에 참여하실 수 있습니다.

블록넷과 같은 혁신적인 프로젝트는 더 많은 사람들의 관점과 능력이 관여될 때 더 나은 디자인과 결과물이 창조된다고 본사는 믿습니다.
블록넷에 질문이 있으시면, contact@blocknet.co 으로 이메일을 보내주세요.

감사합니다.

기회

블록넷에 대하여

블록넷은 다가오는 “인터블록체인 시대”를 맞이하여, 가상화폐의 탈 중앙화 (decentralized)와 가상화폐 스스로의 가치를 창조함을 접목하여 만들어진 “토큰 경제 생태계” 구조 입니다. 이 새로운 생태계가 더 보편화 되는 시기는 셀수 없이 많은 가상화폐들이 자유자재로 상호간 거래가 되는 시점이 될 것이며, 이는 스마트 컨트렉트 (smart-contracts) 와 “dapps” 기술이 보편화 되는 시점일 것 입니다. 이 문서가 쓰여지는 현 시점에, 블록넷은 위의 기술 분야에서 압도적인 리더로써 시장을 이끌고 있습니다.

본사의 판단에 가상화폐는 미래 사회의 다양한 분야에 적용되어 화폐로서의 역할을 해내겠지만, 크게 서비스 소프트웨어 분야 (software-as-a-service) 와 일상적 블록체인 사용 (practical blockchain usability) 로 나눠질 것이라 예측합니다.

서비스 소프트웨어 분야 (SaaS) 에서의 가상 화폐 경제 생태계는 기존 정부 위주의 화폐 정책과 비교해 크게 두 부분에서 앞선다고 결론 내릴 수 있습니다. 첫째, 디지털 서비스 거래 부분에서 더 제제 없고 자연스러운 거래가 가능하고, 둘째로는 블록체인 기술을 화폐에 접합하여 더 안전하고 탈 중앙적인, 이상적인 화폐로서의 가치를 지닙니다.

이미 현 시점에는 수 백, 수천의 다양한 종류의 가상화폐들이 존재합니다. 블록 체인 기술의 관점으로 본다면, 우리는 이 모든 다양한 가상화폐들을 서로 직거래가 가능하게 하여 편리함을 극대화 할 필요성이 있습니다. 모든 가상화폐들 간의 직거래가 자유롭게 이루어 지지않는한, 각각의 가상화폐들은 매우 제한적인 상품들만 거래 할 수 있는 상황이 벌어지고, 더 나아가 블록체인 기술의 가장 큰 장점중 하나라고 꼽을 수 있는 탈중앙화를 포기해야 하는 상황을 맞이 하게 됩니다.

블록넷은 “인터넷 블록체인 토큰 생태계”를 구축함에 따라, 현존하는 모든 가상화폐들간에 직거래를 활성화 하여 화폐로서의 기능을 막힘없이 수행할 수 있도록 할 것입니다. 이는 블록넷이 다가오는 미래 가상 화폐 경제 사회에서 리더로서의 역할을 수행하게 만들 것 입니다.

기존 가상화폐에 대한 불만 – 그리고 블록넷

인터넷을 기반으로 한 기존의 서비스는 필연적으로 기술이나 보안의 결함을 피할 수 없습니다. 더 나아가, 기존 서비스의 중앙화된 개인 정보 수집으로 인한 불안감을 소비자 입장에서 떨쳐내기 어렵습니다. 이와는 다르게 블록체인 기술은 모든 정보가 아무도 알 수 없는 암호화된 코드로 변환되어 중앙화하는 정보 수집에 대한 소비자의 무조건적인 신뢰 자체를 요구하지 않습니다. 각각의 블록체인 사용자들은 그 스스로가 시스템의 일부분이 되어 암호의 일부분으로서의 역할을 수행하게 되므로, 이는 타 회사나 개인과의 거래에 절대적으로 필요한 “신뢰”에 대한 걱정을 덜게 합니다. 이와 같은 새로운 시스템을 바탕으로, 블록체인은 다양한 형태의 사업에 더 뛰어난 가격 경쟁성, 더 나은 브랜드의 가치, 그리고 무엇보다 절대적인 정보 보안을 확실히 보장하게 됩니다.

위에 언급된 엄청난 가능성을 보유하고 있음에도 불구하고, 아직까지 블록체인 기술을 그 잠재적 가능성을 다 발휘하지 못하고 있으며 이는 아직까지 다양한 가상화폐들이 각각 서로 자유롭게 직접적으로 거래할 수 없기 때문입니다. 이미 현 시점에 수천종류의 가상화폐들이 존재하고 있지만, 이 모든 화폐들은 아직 각각

제한된 환경에서 제한된 품목 또는 개인간에 거래에만 활성화 되어 있습니다. 오래전 인터넷이 활성화 되기전 오피스 또는 제한된 구역에서 LAN 으로만 연결되어 있던 환경이 인터넷의 보급을 통해 Facebook, Google 같은 대 기업을 창조하고 끊어져 있던 곳곳의 점들을 이어 하나로 통합했듯이, 블록넷은 점점이 흩어져 있는 수천개의 가상화폐를 하나로 있는 연결통로가 될 것입니다.

블록넷의 솔루션 (Solution)

블록넷은 토큰 생태계를 근본으로 이루어졌고, 이를 통해 모든 가상화폐와 다양한 블록체인간에 직거래가 가능하도록 기획되었습니다. 블록넷의 특징들은 다음과 같습니다:

- 어떤 종류의 디지털 서비스라도, 어떤 종류의 블록체인 이라도 상호간 거래를 자유롭게 할 수 있습니다.
- 어떠한 블록체인 서비스라도 더 이상 제한된 "엡코인"으로서의 기능이 아닌 "프로토컬 서비스" 로서의 기능 수행이 가능해짐으로, 처음 블록 체인이 제작될 당시 목표한 가상 화폐로서의 기능을 넘어서 더 넓은 시장 (모든 다른 dapp) 에서 가상 화폐로서의 역할을 수행합니다. 이로서 그 가상화폐의 잠재적 가치 및 수익 창출은 기존의 목표를 넘어설 수 있습니다.
- 한정적인 "dapp" 내부에서만 통용되는 가상 화폐가 아닌 "프로토콜 토큰" 으로서의 역할을 수행함에 따라, 기술적으로 잠재성이 제한되어 있던 단점을 극복 할 수 있습니다. 추가적으로, 다양한 서비스 코드들을 상호 교환하여 서로 배우고 보완해 나갈 수 있으므로, 코드의 반복성이나 불 필요하게 복잡한 코드를 줄임으로서 개발 인건비를 줄이며, 완성된 서비스를 제한적인 한개의 블록체인 시장이 아닌 *현존하는 모든 가상화폐* 블록체인 시장에 공개할 수 있습니다.
- 현재까지 존재했던 어려운 코드 생성 방식이 아닌 체인간 상호 서비스를 통해 더 간단한 방식을 도입했습니다. 어플리케이션 제작이 아닌 어플리케이션 코드만 적용하면 되므로, 코드를 새로 제작하거나 "방탄보안" 을 위해 힘쓰지 않아도 되어 더 쉽습니다.
- 각각의 dapp 의 기존 큰 틀 구조를 유지하되 그 위에 각각 가상화폐가 상호 통용하는 추가적 구조를 건설함에 따라, 전체적으로 더 간단한 구조를 유지하여 오류수정 (버그) 이나 업그레이드를 더 쉽게 할 수 있습니다.
- 현재 심각한 걱정거리인 "어느 블록체인을 선택하여 프로젝트를 진행할 것인가" 라는 문제를 사전에 제거할 수 있습니다.
- 토큰에 주어진 근본 가치를 바탕으로, 가상 화폐들간에 거래가 제한없는 가상화폐를 주조할 수 있게됩니다.
- 가상화폐를 바탕으로 여지껏 존재하지 않았던 완전히 새로운 사업이 가능해 집니다. 예를 들자면, 사업체들은 "무료보다 나은 정도의" 모델을 바탕으로 가치를 창출해 낼 수 있습니다. 사업체가 주조한 화폐정책을 바탕으로 ICOs, transaction fees, deflationary economics, block rewards, and superblock self-funding system 등을 통해 수익 창출이 가능해 집니다.

블록넷은 위에 언급된 장점들을 혁신적인 구조와 접근 방식을 통해 이루어 냈으며, 이에 관한 추가적인 설명들이 이 문서에 다뤄졌습니다.

디자인

디자인의 목표

블록넷은 아래와 같은 디자인 목표를 가지고 개발되었으며, 가장 먼저 언급된 특징이 더 중요하게 부각되어 디자인 되었습니다.

1. 상호 직접 직거래 가능 여부

블록넷은 무엇보다 가장 중요하게 모든 가상화폐간 직접 거래를 가능하게 하는 구조로 디자인 되었습니다. 블록넷은 현존하는 거의 전부의 가상화폐들 간의 직접 거래가 가능합니다. 추가적으로, 본사가 개발한 토큰 경제 생태계를 바탕으로 하여 기존의 서버를 근본으로 한 서비스에서도 가상화폐간 직접 거래가 가능하게 하였습니다.

2. 탈 중앙화 가상화폐

탈 중앙화라 함은 필수적으로, *어떠한 하나의 국가, 개인, 또는 회사도 다른 국가, 개인 또는 회사가 보유한 가상화폐에 직접적인 영향력을 끼칠수 없는 시스템* 을 의미합니다. 이미 대중화된 탈 중앙화를 시도한 가상화폐인 비트코인의 예를 들어 설명하자면, 기존 국가에서 발행된 화폐와는 다르게 아무도 그 가치를 조종할 수 없으며, 거래를 제제할수 없고, 거래의 기록을 찾아 볼 수 없으며, 추가적인 화폐 주조를 할 수 없습니다.

위와 같은 특성에도 불구하고 비트코인은 완벽한 탈 중앙화를 실현하지 못하였고, 이로 인해 가상화폐의 추가적인 잠재성이 억제되고 있습니다. 비트코인은 탈 중앙화된 서비스들에게 완벽한 탈 중앙성을 제공하지 못하고 있으며, 비트코인이 제공할 수 있는 서비스들은 다음과 같은 이유들로서 그 가치가 많이 떨어진다 할 수 있습니다. 첫째, 어플리케이션 제작 API 생태계에 이 정도의 탈 중앙화는 이미 존재하고 있습니다. 둘째, 탈 중앙화로 이룰 수 있어야 할 투자자에 대한 이자의 개념이 이미 상실되어 버렸습니다. 예를 들자면, 만약 거래를 하려고 하는 사람이 비트코인을 중앙화되어 있는 거래소를 통하여 구매 한다면, 가상 화폐의 최대 장점인 “신뢰”가 필요없는 시스템이 이미 무너집니다. 왜냐하면 가상화폐를 구매하는 사람 입장에서는 거래소를 절대적으로 무조건적인 신뢰를 해야만이 구매를 할 수 있기 때문입니다. 이외에 은행 수수료, 신용카드 수수료, 중개 수수료 등 다양한 추가적 수수료를 지불해야 합니다. 그러므로, 진정한 탈 중앙화 기술을 이룩해 내어 그 잠재성을 최대화 하기 위해서는, “*탈중앙화된 경제 생태계*” 가 필수적이며, 이는 위에서 언급된 비트코인의 단점들을 보완하고 진정한 의미의 탈 중앙화된 가상화폐 경제를 이룩할 수 있을 것입니다.

3. 보안

탈중앙화된 가상화폐 주조 서비스는 특성상 기존의 서비스 방식에 비해 더 고강도의 보안을 요구합니다. 왜냐하면 첫째, 유저의 기기에 의존해서 처리되는 방식과 달리 네트워크를 기반으로 하고 있으므로 오프라인 상태로 만들 수 없기 때문입니다. 둘째로, 보안에 이상이 생겨서 어떠한 방식으로라도 가상화폐가 강제적으로 빼앗기는 경우가 생긴다면, 탈 중앙화식으로 설계된 구조가 단점이 되어 어디에도 책임을 물을수 없고 중앙화식으로 설계된 가상화폐 구조에서 최소한의

대처를 할 수 있는것과는 달리 아무런 대책도 없이 속수무책으로 당하게 되어, 가상 화폐로서의 가치가 폭락하기 때문입니다. 위와 같은 상황을 방지하고자, 블록넷은 현존하는 어떠한 보안보다 더 정교한 고강도의 보안 시스템을 유지합니다.

4. 신뢰가 필요없는 서비스 전달 방식

탈중앙화 시스템을 성공함으로서 이룰 수 있는 가장 이상적인 결과중 하나는 두 개체가 거래함에 있어 상호간 사전에 이루어야 할 신뢰 구축과정이 불 필요해 진다는 점 입니다. 비트코인을 예로 들어 설명하자면, 거래를 하려고 하는 사람은 중간 업자가 양심적으로 자신의 돈을 보내는지, 정확한 양을 보내는지, 받아야 하는 금액을 거래처로 부터 받았는지에 대한 걱정으로 부터 해방될 수 있습니다. 이를 가능하게 하는 것은 중간 업자가 아예 없다는 점 뿐만 아니라, 양측 모두 독립적으로 거래 내역을 원할 때에 어디에서나 확인 가능하다는 점 또한 큰 부분에 기여하고 있습니다.
블록넷이 추구하고 있는 모든 가상화폐간에 직접거래에서도 위에 언급된 신뢰가 필요없는 서비스 전달방식은 필수 조건입니다. 블록넷은 모든 가상화폐간의 직접 거래를 최소한의 불편함으로 자유스럽게 가능하게 하되, 거래에 임하는 양측의 신뢰성을 고려하지 않고도 안전하고 보안이 보장되는 거래 환경을 제공할 것입니다.

5. 코딩이 필요없는 간단한 연동

가상화폐간 직접거래를 최대화함과 동시에 일어날 수 있는 모든 문제를 최소화하기 위해서는, 블록넷이 제공하는 토큰 경제 생태계에 접속하는 모든 이에게 간단한 연동 방식을 제공해야 합니다. 블록넷의 시스템에 영향력을 행사 할 수 있는 몇몇의 제 3개인 또는 기업에게는 코딩이 요구될 수도 있지만, 블록넷을 사용하는 대 다수의 일반 유저들에게는 코딩이 요구되어선 안될 것입니다.

6. 탈 중앙화된 연동

블록넷의 토큰 경제 생태계가 인터넷 형식의 생태계를 구축하여 최대한의 보안과 편리성을 제공하기 위해서는, 블록넷에 유저들이 연동할때 어떠한 중앙화된 매개체도 거치지 않아야 하며, 이 매개체에는 제작자인 본사도 포함됩니다. 블록넷을 이용하여 어떠한 서비스 또는 상품을 거래 할때, 잠재적인 소비자들은 다음과 같은 과정을 거치지 않아야 합니다. 첫째, 블록넷의 블록체인을 필수적으로 사용할 필요는 없어야 합니다. 둘째, 서비스 또는 블록체인 종류 사용에 제한이 없어야 합니다. 셋째, 어떠한 중앙화된 매개체 또는 중앙화된 거래 효과를 거치지 않아야 합니다. 여기서 사용된 “중앙화”는 다양하게 적용 가능하며, 예를 들자면 어떠한 중앙화된 업체를 거친다거나 중앙화된 네트워크를 통해 일처리가 이루어 지는 것들 등 매우 넓은 적용이 가능합니다. 본사는 이를 “인터체인 중앙화”라고 명시 하겠습니다.

제 3개인 또는 기업을 거쳐 블록넷의 토큰 경제 생태계에 입문하게 되는 몇몇의 경우에는 “인터체인 중앙화”가 이루어 질 수도 있지만, 블록넷을 사용하는 대 다수의 일반 유저들에게는 적용되지 않을 것 입니다.

7. 결합성

블록넷은 수 많은 중소 인터체인 서비스들이 구상중인 것과 비슷하게 결합성과 모듈성을 추구해야

할 것입니다. 결합성과 모듈성이라 함은 구상이나 상황에 맞추어 유연하게 변화할 수 있음을 의미합니다. 특히나 중소 서비스 디자인의 가장 중요한 점은 유연하게 변화하여 언제나 블록넷에 속한 모두의 이익을 추구하여 "정체된 단일집단"의 발생을 방지하는 것입니다. 이와 같이 블록넷에 속한 전체의 이익을 추구하여 토큰 경제 생태계가 퇴화하지 않고 유지되게 합니다.

8. 화폐 주조 가능성

위에서 강조되었던 유연한 결합성을 적용하여 블록넷은 기존의 가상화폐들과는 다른 특징인 "자체 화폐 주조성"을 추가 하였습니다. 본사는 기존 가상화폐 모델에 이 특징을 추가함으로서, 블록넷을 보유하고 있는 모든이들에게 잠재적인 수익을 보장합니다.

더 나아가, 이렇게 투자자들에게 주어지는 수익은 신뢰성 보장이 필요없는 가상화폐 인센티브로써 안정성이 보장되며 이를 통하여 화폐 자체의 가치를 보장받습니다. "자체 화폐 주조성"을 통해 새로 주조된 가상 화폐는 두 가지 조건이 만족될 때 그 가치를 보장받습니다. 첫째, 다른 사람들이 그 화폐를 구매할 이유가 있어야하며, 둘째로 구매의사가 있는 사람들이 무료로 획득할 수 있는 방법이 없어야 합니다.

블록넷은 실현 가능하고 사용자들에게 무료로 제공되는 주요 서비스를 바탕으로 안전성과 보안을 바탕으로 한 가상 화폐 주조를 해야할 것입니다.

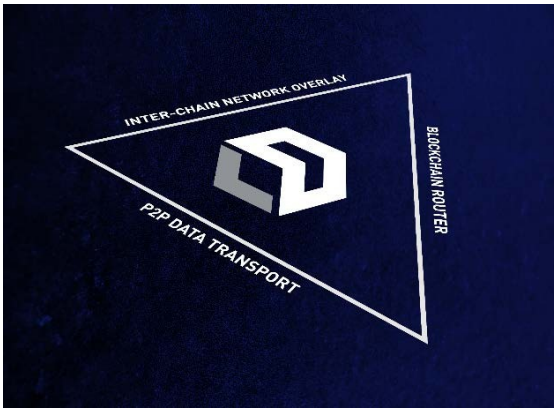
9. 유동성과 최소한의 흔적

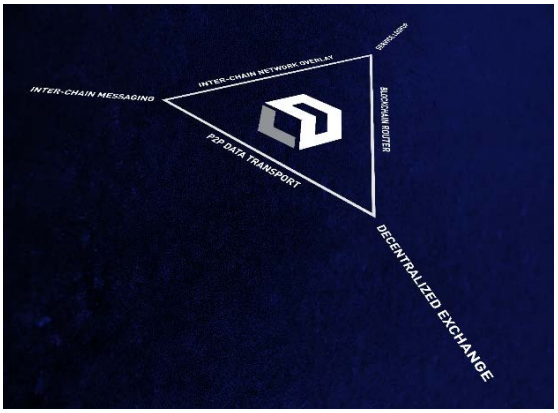
토큰을 근본으로 한 생태계는 경제 분야에만 국한되지 않고 더 다양한 분야에 접목 가능하며 이에 예를 들자면 보험, 의료분야, 도소매 유통업, 농업, 자동차 내부 컴퓨터와 보안업체등에서 영향력을 행사할 수 있습니다. 이와 관련한 자세한 자료는 2015년 2월달에 제안된 블록넷 사업 계획서를 참조하시거나 contact@blocknet.co로 연락하시길 바랍니다. 위에서 언급한 다양한 분야에서 영향력을 행사하기 위해서는 필수적으로 사용자들의 내역에 대한 흔적 추적이 최소한으로 이루어져야 하며, 단 하나의 블록체인이라도 이 흔적을 추적할 수 있어서는 안됩니다. 위에 분야에 블록넷이 적용되기 위해서는 IoT 서비스에 대한 어떠한 해킹이나 공격으로부터 완벽한 보안 보장이 이루어져야하며, 이는 향후 블록넷에게 가장 중요한 사업적 목표로서 다루어 져야 할 사항일 것입니다. 블록넷은 인터체인 서비스간에 직접 거래가 이루어질때 남는 흔적을 최소화 해야 할 것이며, 어떠한 거래도 블록넷 전체가 아닌 지방 블록체인 (blockchain locally)에 인터넷 호스팅 서비스를 근거해서는 안 될 것입니다.

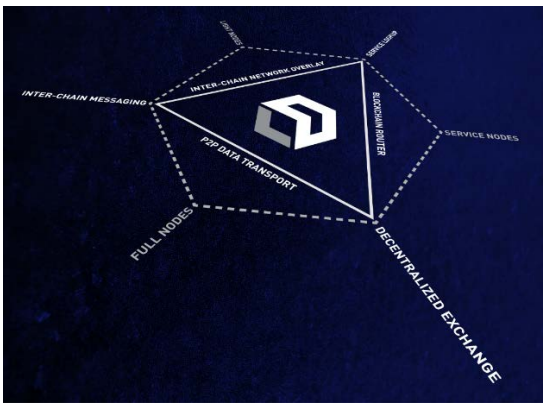
건축 구조

블록체인 간에 직접 거래 연결 목적을 달성하기 위해서는 3가지의 요소들이 연동되어야 하며, 이를 바탕으로 블록체인 서비스들과 블록체인 요소들이 결합하여 3가지의 주요 서비스를 제공합니다. 토큰 경제 생태계를 바탕으로 어플리케이션들 간에 직접 연결이 달성되어 무제한의 블록체인 서비스들이 직접적으로 연결되는 환경을 조성하게 됩니다.

이 영역에 대해 배울 기회가 없었던 읽는이들을 위해서 도표와 그림을 사용하여 이해하기 쉽게 풀어 서비스들과 이를 이루는 요소들과의 관계를 설명할 것입니다. 아래에 소개되는 그림들을 참조해 주세요:







건축 구조를 이루는 요소들에 대해 먼저 설명하고 서비스에 대해 설명 드리겠습니다. 이에 앞서서, 인터체인 건축구조에 대한 기본적인 자연환경에 대해 간단히 설명드리겠습니다.

인터체인 건축구조란 무엇인가?

보통의 경우, 인터블록체인 건축구조는 언제나 적어도 2가지 이상의 블록체인 네트워크들을 토대로 상호 연결하여 기능합니다. 블록체인 네트워크는 탈 중앙화 되어있으므로 상호 연결되는 요소들은 보통의 경우 중앙화된 장소에 보관되지 않습니다. 블록체인들 간의 상호 연결을 유지하기 위해, 서비스 제공자들은 각각 블록체인 네트워크의 가장자리에 부분적으로 관여하여 정보 교류를 실행합니다. 아래의 그림을 참조해 주세요.

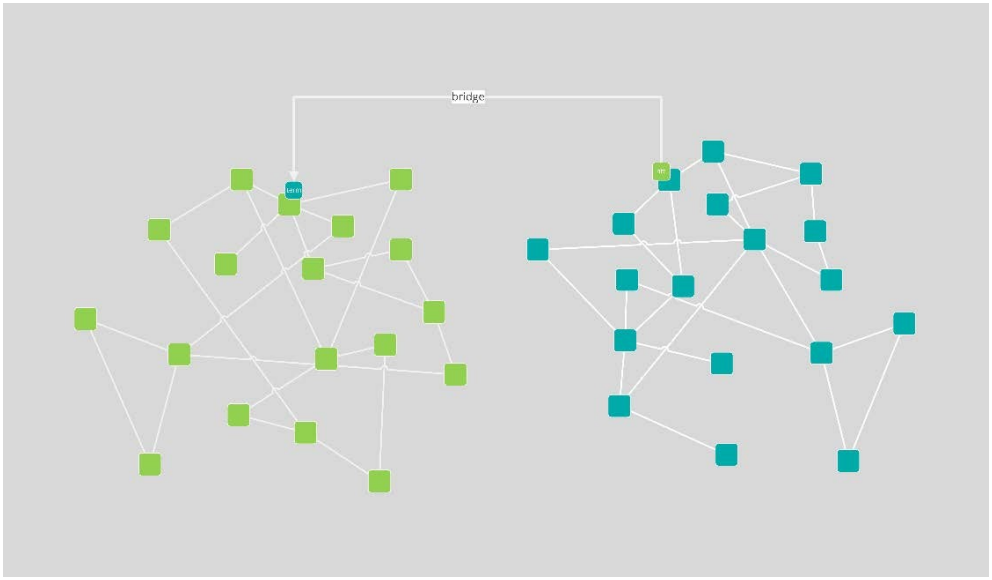


그림 1.
중간과정을 거치지 않고 각각의 블록체인 네트워크를 잇는 이상적인 p2p 네트워크 서비스 모델

이제껏 진행 되었던 다양한 프로젝트들은 다음과 같은 솔루션들을 제공하였습니다:

- 고전 기술: 중앙화된 중간과정 (예: Poloniex.com 폴로닉스)
- 최대 관여자: 탈 중앙화된 네트워크를 제공하지만 중앙화된 중간과정 (예: Bitcoin 비트코인)
- 소유주의 코드 (proprietary code): (예: 월렛, 스마트 컨트렉트, 볼트온 월렛) 부분적으로 블록체인간 상호 연결을 해냈지만 같은 코드를 쓰는 경우에만 가능한 경우 (예: BTCrelay)
- 벽에 둘러쌓인 정원 (walled gardens): 몇몇 임의로 설정된 블록체인들 간에만 인터 체인 프로토콜이 가능하며, 제작자들을 이미 설계된 위에서 제작하게 유도함 (예: 아이온 Aion)

위에 열거된 어떠한 인터체인 기술들도 포괄적이며 탈 중앙화된 두가지 특징을 공존시키는 시스템을 구축하지 못했습니다. 이는 위에 열거된 인터체인 기술들이 현재 존재하는 블록체인을 조건없이 포함하는 서비스를 공급하는데 실패했거나 탈 중앙화를 완벽히 시행하여 각각의 서비스들에게 독립적인 서비스 공급을 원활히 하는데 실패했습니다.

블록넷이 추구하는 디자인 목적은 포괄성과 탈 중앙성 두가지를 충족시키는 디자인입니다. 이 두가지는 블록넷이 추구하는 “최우선 원칙”이며 이는 인터체인 기술 그 자체의 자연 스러움을 유지시키는데 꼭 필요할 것입니다.

1. 분산된 네트워크 건축 구조

첫째로, 어떠한 인터체인이라도 연동된 요소들의 네트워크 가장자리에 상주해야 한다는 것은 확실하며, 이로써 블록체인 네트워크나 소비자 서비스에 대한 확실한 분산된 서비스를 보장 받습니다. 추가적으로, 서비스를 제공하는 인터체인 요소들 마저도 그들 스스로의 네트워크의 가장자리에서만 상주함으로서 중앙화된 결정을 방지하여, 중간업체로서의 중앙화 되는 과정을 막는 역할을 합니다.

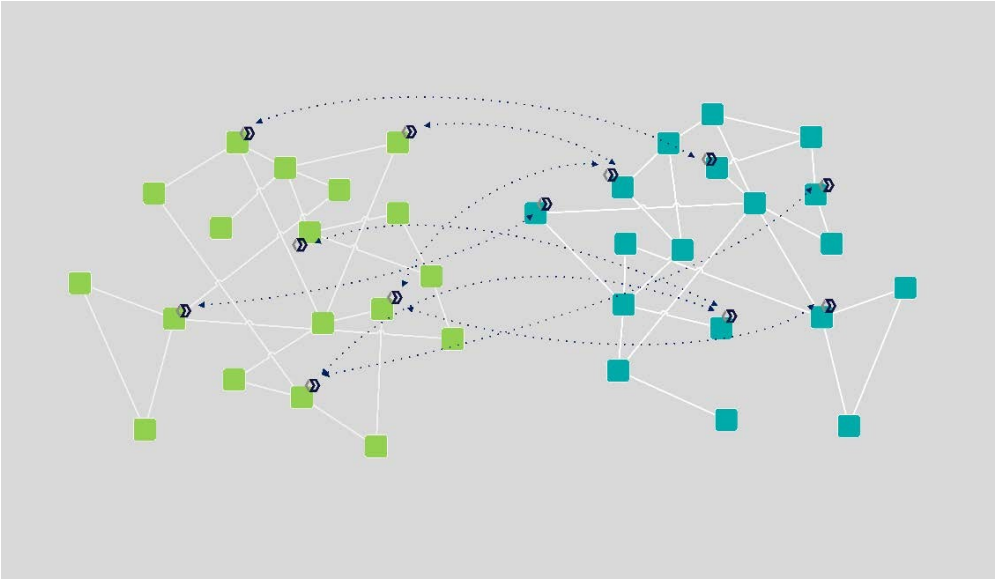


그림 2.
적절한 인터체인 서비스는 사용되는 네트워크와 사용하는 네트워크 둘다의 가장자리 에서만 상주해야합니다.

2. 탈 중앙화된 결정

둘째로, 인터체인 서비스를 구매 또는 매매 하는 행위는 제 3자의 영향을 전혀 받지 않고 독립적으로 이루어 질 수 있어야합니다. 건축 구조적으로만 설명하자면 (프로토콜 디자인의 관점), 이를 해결할 수 있는 가장 직접적이고 안전한 방법은 인터체인 서비스 구조를 이루는 네트워크 제공자와 소비자가 같은 로컬 머신 (same local machine)에 존재하는 것 입니다. 이것의 필요성의 정도는 (인터체인 서비스 발자취에 대한 영향력) 최대치의 노드 (node)가 요구될 지, SPV 노드 (node)를 사용할 지, 그냥 거래내역에 서명을 할지, 아니면 최소한, 블록체인 웹사이트 또는 다른 중앙화된 오라클 (oracle) 보안 어플리케이션을 사용할 지 차이가 있습니다. 후자의 경우에는 “인터 체인”에 적용되기에는 매우 제한적이라고 판단됩니다.

엄밀히 말하자면, 지방 건축 구조 (local architecture)의 최대 범위 요구사항에 대하여 분명히 밝혀져야 합니다. 제한된 몇몇의 경우를 제외한 모든 경우에, 각각의 결정권에 탈 중앙화된 관점에서 참여하기 위해서는 서비스 제공자와 소비자 네트워크 둘다의 직접적인 참여를 요구합니다.

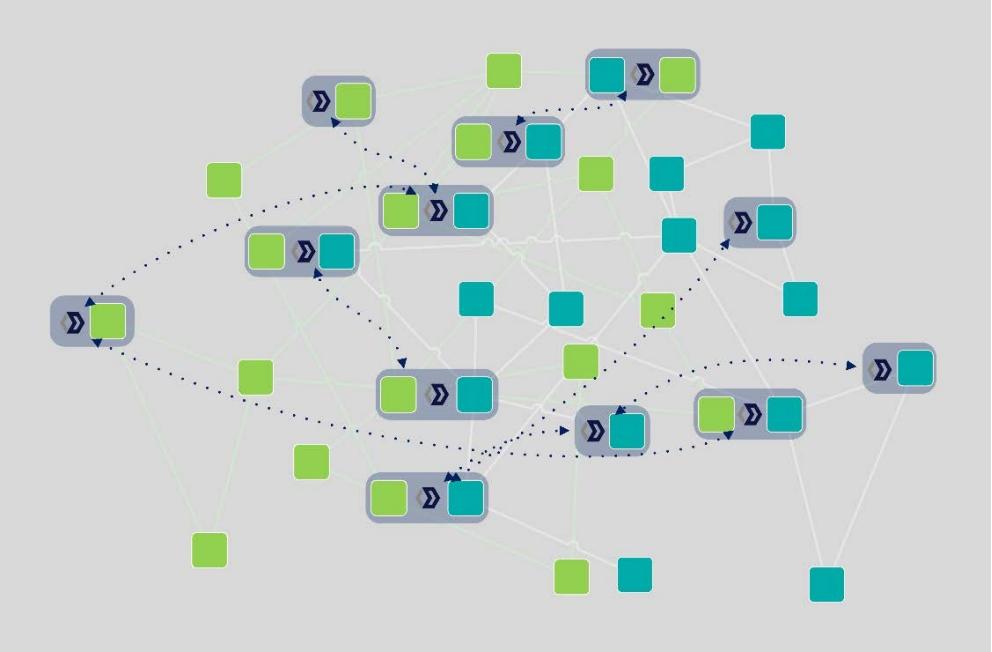


그림 3.
탈중앙화된 사회기반시설 인터체인

파란 부분은 다양한 소비층, 서비스 제공자, 인터체인 노드들의 조합을 의미합니다. (파란 부분 밖의 노드들은 인터체인 서비스를 제공하지 않습니다.)

3. 잠금없는 블록체인

모든 인터체인 서비스는 수 많은 형태의 체인중 하나의 노드를 근본으로 하여 전달되어야 하지만 특정한 인터체인 건축 구조물에서만 작동하게 제한 되어서는 안됩니다. 왜냐하면 서비스가 특정 블록체인에서만 작동하도록 제한되어 버린다면 그저 한낮 클라이언트 서버 모델로 전락하기 때문입니다. 하지만 안타깝게도 현재 보편화된 중앙 어플리케이션 건축물은 위와 같이 중앙화, 제한된 건축 구조물을 사용합니다. 예를 들자면, *블록스트림의 사이트체인 구현 모델*은 사실상 모든 유저들이 비트코인 블록체인과 연동해야만 모든 종류의 체인 서비스를 소비할 수 있기를 요구합니다. 본사는 이 위험요소를 "인터체인 중앙화" 라고 명명했습니다. 이를 피하기 위해서는 토큰 경제 생태계를 유지할 수 있는 진정한 블록체인을 통해 모든 블록체인의 모든 서비스라도 소비될 수 있는 단일화된 시장을 탄생시켜야 합니다.

이 부자연스러운 체인의 개념은 엡발자취 (app footprint) 연동 요구사항을 최소화 하게 하는 동기를 부여합니다. 예를 들어 만약 본사가 블록넷을 사용하는 모든 소비자들에게 블록넷의 블록체인을 서비스 제공자의 블록체인과 별도로 설치할 것을 추가적으로 요구한다면, 블록넷의 대중성과 편리성은 매우 제한됨과 동시에 사용자들이 느끼는 불편함도 굉장히 높아질 것 입니다.

인터체인 건축 구조물 디자인은 이러한 측면을 적극 반영하되 화폐로서의 순수 기능인 서비스의 교환을 수행하고자 한다면 다음과 같은 문제점들을 극복해야 할 것입니다. 첫째, 네트워크 상의 일대일 거래 (peer-to-peer network) 에서는 상호간 신뢰가 전무하므로 서비스 제공과 화폐의 지불이 동시에 묶음으로 이루어 져야 합니다. 둘째로, 매우 높은 품질과 안전이 보장된 고성능의 코딩을 통하여 탈 중앙화된 거래를 이루어 지게 해야하며, 이를 통한 기본적인 거래 방식은 하나의 노드에서 사용하는 고유의 토큰과 다른 노드에서 사용하는 또 다른 고유의 토큰이 상호 교환 될 수 있는 시스템이 구축되어야 합니다. 하지만 각각 다른 종류의 고유 토큰들 간의 거래를 성사 시키기 위해서 하나 이상의 블록체인을 다운로드하고 유지시키며 사용해야한다면, 이러한 거래 시스템이 대중화되고 널리 퍼지기를 기대하는 것은 어려울 것입니다. 그러므로, 블록넷은 이런 방식을 피해야 합니다.

요약

위에서 언급한 사항들을 통해 다음과 같은 블록넷 디자인 요소들의 3가지 원칙들을 정리할 수 있습니다:

1. 인터체인 건축 구조물 서비스는 모든 서비스 제공자와 서비스 소비자 네트워크의 가장자리에서 실행되어야 하며, 이는 블록넷 자체에도 적용된다.
2. 개발 건축구조 상으로만 본다면, 탈 중앙화된 서비스는 같은 로컬 기계 (same local machine)에서 서비스 제공과 서비스 소비에 필요한 요소들이 실행될 때 가장 쉽게 달성될 수 있다.
3. 인터체인 사회기반 구조물 서비스들은 연동될 때 필요한 요구사항과 발자취 (footprint)를 최소화해야 한다

주요 요소들 (Core Components)

블록넷은 인터체인 서비스 건축 구조물의 목적을 달성시키는 3가지의 근본 주요 요소들이 있으며, 이는 다음과 같습니다:

- **XBridge**, an inter-chain network overlay (엑스브리지: 인터체인 네트워크 오버레이)
- **XName**, a block chain router (엑스네임: 블록체인 라우터)
- **XChat**, a p2p data transport (엑스챗: 피투피 데이터 트렌스포트)

위 세가지가 "주요 3대 요소"로 꼽힌 이유는 다른 모든 인터체인 상호운용 솔루션들 또한 이 세가지 없이는 완성될 수 없기 때문입니다. 모든 솔루션들은 노드들간에 네트워킹이 필요하고, 라우터 서비스를 노드들이 찾을 수 있게 해야 하며, 적당한 노드를 피투피 연결을 시키는 프로토콜이 필요하기 때문입니다.

이 글을 읽는 독자들에게 블록넷의 난해한 요소들과 서비스들을 이해하고 시각화하기 쉽게 하기 위해서 곳곳에 도표를 소개할 것 입니다. 아래의 도표에 블록넷을 이루는 3대 주요 요소들을 표현 했습니다.

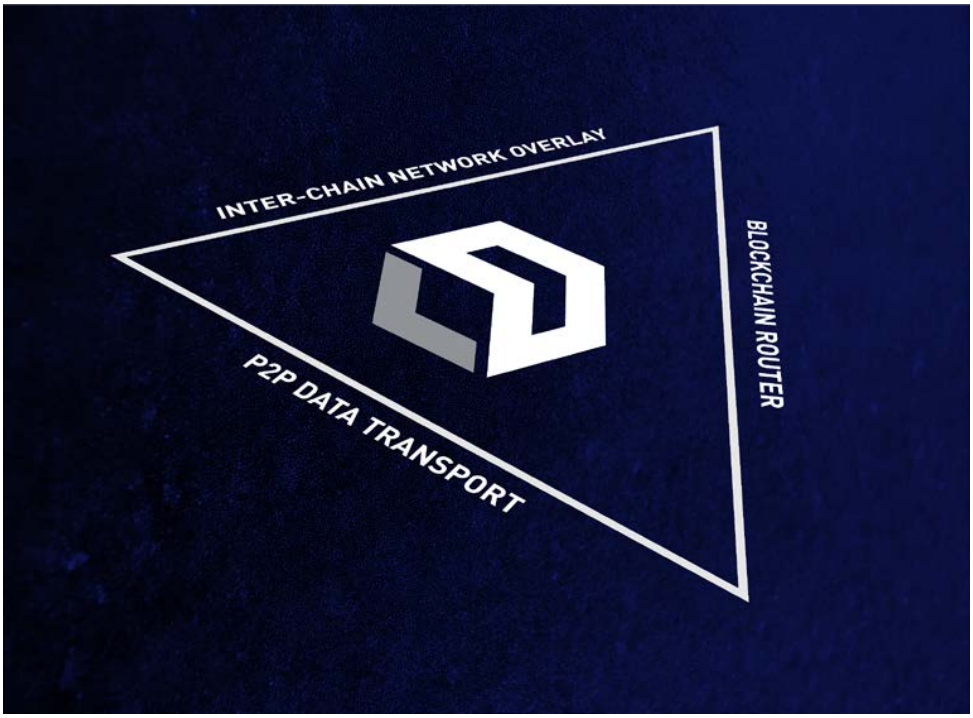


그림 4.
첫번째 신판: 블록넷의 3대 주요 요소들.
이 요소들은 인터체인 서비스를 유지하는 기본 골격으로서 각 면을 이룹니다. 그림속 삼각형의 면은 끝 점에서 만나고, 이는 3가지 주요 요소들이 상호 보완하여 완벽함을 추구하는 블록넷의 원칙을 표현 하였습니다.

엑스브리지 (XBridge): 인터체인 네트워크 오버레이

블록넷의 엑스브리지는 서버가 필요없는 DHT를 근본으로한 일대일 네트워크 (peer-to-peer network) 입니다. 노드는 주어진 로컬 기계를 바탕으로 다른 네트워크에 속한 노드와 연동하여, 우리의 네트워크를 인터체인 네트워크 오버레이로 만듭니다. 이로서 블록체인 네트워크의 속성에 상관없이 노드들간의 찾아보기 (lookup), 위치추적 (location), 방송하기 (broadcast) 등을 가능하게 합니다.

문맥 도표

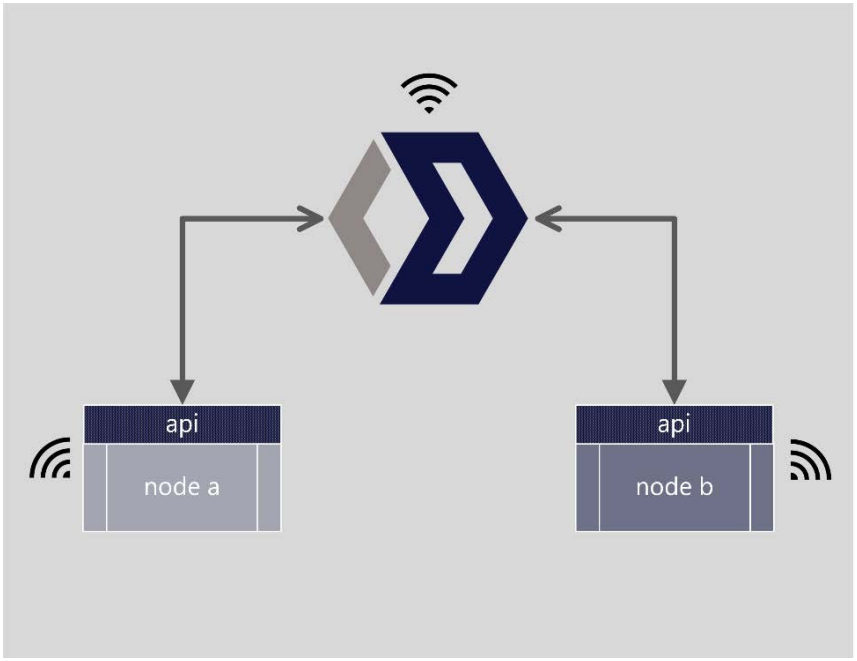


그림 5.
로컬 기계의 네트워크 구성 요소들

전문 기술 관련 문서는 “기술 설명서” 란을 참조해 주세요.

완성 및 구현

현재: 네트워크 오버레이 코드가 XBridgep2p.exe 와 블록넷 지갑 (Blocknet wallet) 둘다에 구현 되어 있습니다. 아직 화폐 주조는 이행되지 않았습니다.

미래: 비록 주 서비스들을 시행하기 위해 독립적인 어플리케이션으로 출시되지 않고 다른 요소들과 상호 운용하게 될 것임에도 불구하고, 이것은 코드베이스로 모듈화 될 것입니다.

엑스네임 (XName): 블록체인 라우터 (Blockchain Router)

인터체인 서비스 생태계는 정확한 블록체인에게 올바른 정보 전달 (라우팅 메세지 routing message) 을 성공적으로 하는 것이 요구되고 블록넷은 인터체인 주소 시스템으로 이것을 달성할 것 입니다. 블록체인 라우팅은 아직 개발 초기 단계이며 가상 화폐 커뮤니티에서 아직 더 폭 넓은 탐험과 동의를 요구 함에도 불구하고, 근본적으로 라우팅 데이터를 레지스트리에 기록하고 찾아보는 기능을 위해서는 블록체인의 Uport's MNID와 같은 인터체인 표준을 지정하는 것이 요구됩니다. 가장 중요한 질문은 라우팅 결과의 최선 가격대 진실성 비율입니다. 예를들자면, 서비스 제공자들은 레지스트리가 아예 없는 서비스를 통해 최대의 이익을 얻을 수 있으므로, 서비스에 대한 지불과 이행 바로 이전에 어느 정도의 찾아 보기 기능의 실패를 용인할 수 있고, 이는 찾아보기 기능 이후에 정직하지 않을 가능성을 제거함으로써 가능합니다. 아마도 몇몇의 서비스들은 대체 방법으로서 아주 신뢰할 만한 찾아보기 결과를 요구함과 동시에 적은 비용을 지불할 것 입니다. 엑스네임은 레지스트리 서비스 디자인에 구속 받지 않는 접근 방식으로 개발하여, 최종적인 솔루션은 필요하다면 다양한 연동자들의 필요함을 충족시켜야 하며 이는 치열한 레지스트리 서비스 시장의 출현 가능성을 포함합니다.

이와 같이 합당한 라우터의 디자인의 방향성은 체인아이디 레지스트리 서비스 찾아보기 (lookup) 기능을 포함한 라우팅 데이터를 레지스트리 서비스에 저장함에 있어 필요한 신뢰의 정도를 최소화 함과 동시에 이에 필요한 비용을 최소화 하는 방향이 되어야 합니다. 이를 위해 엑스네임의 기능은 API의 레지스트리 서비스를 호출하고 서비스 전달이 완료된 후 이 라우팅 결과 기록을 로컬 또는 캐치 메모리에 저장하여야 합니다. 초기 출시 전에 순환성 개선 (순환성 개선이란 서비스를 찾아보기 전에 레지스트리 서비스부터 찾아 보는 것) 을 위해서는 노드들은 다음 중 하나의 방법으로 스스로 부트스트랩 (bootstrap) 할 수 있습니다. 첫째, 믿을만한 레지스트리임을 입증할 수 있게 하드코드 체인 아이디 (hardcoded chainId) 를 물어볼 수 있습니다. 둘째, 그들의 피어 (peers)를 엑스브리지 전용의 겟레지스트리서비스 콜 (getRegistryService call) 에 문의한 후 각각의 레지스트리 서비스 리턴을 문의함 으로써 각각의 서비스가 레지스트리 서비스들과 (다른 인터체인 서비스들과) 신뢰 구축을 위해 필요했던 신뢰 보증관계를 개발할 수 있습니다. 인터체인 서비스 찾아보기 (lookup) 와 하는 방법에 대해서 질문이 있으시면, 서비스룩업 (Service Lookup) 섹션과 레지스트리 서비스 (Registry Service) 섹션을 참조해 주십시오.

기술관련 문서는 기술관련 설명서 (Technical Specification) 섹션을 참조해 주십시오.

구현 방법

현재: 블록체인 라우터가 XBridgep2p.exe와 블록넷 지갑 (Blocknet Wallet) 두 곳 모두에 다른 주요 서비스들과 함께 구현되어 있습니다.

이후 계획: 주요 서비스들을 효과적으로 전달하기 위해 이 요소는 다른 요소들과 언제나 상호 운용되어, 따로 배치될 필요가 없을 것 입니다. 하지만, 블록체인 라우팅 주조 과정 렌더링 (render) 이 충분히 진전된 이후에는 독립적으로 배치되야 할 수도 있으며, 이는 화폐 주조성 그 자체가 서비스 운용 비용을 반영할 수 있으므로, 라우팅 서버들 간의 경쟁을 가능하게 하고 서비스의 기술적 진전을 보상화 하기 위해서 입니다. 만약 주조가 된다면, 라우터의 요소는 추가적으로 다른 요소들과 그들 스스로의 블록체인 네트워크를 연동해야 할 수도 있습니다.

엑스칫 (XChat): 개인에서 개인으로 데이터 전송

디지털 서비스를 전달하기 위해서는 메세지를 보내고, 받고, 지불하는 수단이 필요합니다. 이를 위해 블록넷은 엑스칫을 사용합니다. 엑스칫은 암호화된 개인과 개인간의 메세지 전달 모듈이며, 개인간의 메세지들은 물론 그룹간의 메세지도 기능에 포함됩니다. (브로드케스트 메세지는 이미 엑스브리지에서 지원하고 있습니다)

디지털 서비스 전달을 위한 교류 요구사항 정도는 서비스의 형태에 따라 차이가 있습니다. 사생활 보호, 인터넷 접속 속도, 인터넷 라텐시 (latency), 인터넷의 안정성, 중간 매개체의 유무 등등이 모두 이 차이에 포함되며, 이 모든 것들이 몇몇의 데이터 전송 기술에 의해 완성됩니다. 현재 아직 미완성 단계임에도 불과하고, 블록넷은 사생활 보호, 속도, 개인간의 솔루션 등에서 매우 우수하여 충분한 성능을 보여주고 있습니다.

기술관련 문서는 기술 설명서 섹션을 참조해 주시기 바랍니다.

구현 방법

현재: 데이터 전송은 XBridgep2p.exe 와 블록넷 지갑 (Blocknet Wallet) 두 곳 모두에서 주요 서비스들과 함께 구현되었습니다.

차후계획: 코드베이스 (codebase)로 모듈화 (modularized)될 수 있으며, 만약 독립적인 어플레케이션으로서 화폐화가 이루어 진다면 그리 출시될 수 있습니다.

주요 서비스들

화폐 주조 가능한 인터체인 서비스들은 세 가지의 주요 기반 서비스들이 요구되며, 이는 다음과 같습니다:

- **서비스 찾기 (lookup):** 서비스를 판매 또는 구매하기 위해서 대상을 찾는 기능
- **인터체인 메세징 (messaging):** 디지털 서비스를 전달하는 방법
- **탈 중앙화된 교환 (Decentralized exchange):** 서비스 전달을 현금화 하는 수단

위의 서비스들은 주요 요소들이 조화롭게 어우러져 제공되며, 이는 아래 제공된 도표의 삼각형 끝부분 각진곳에 위치되어 시각적으로 이해를 도울 수 있습니다.

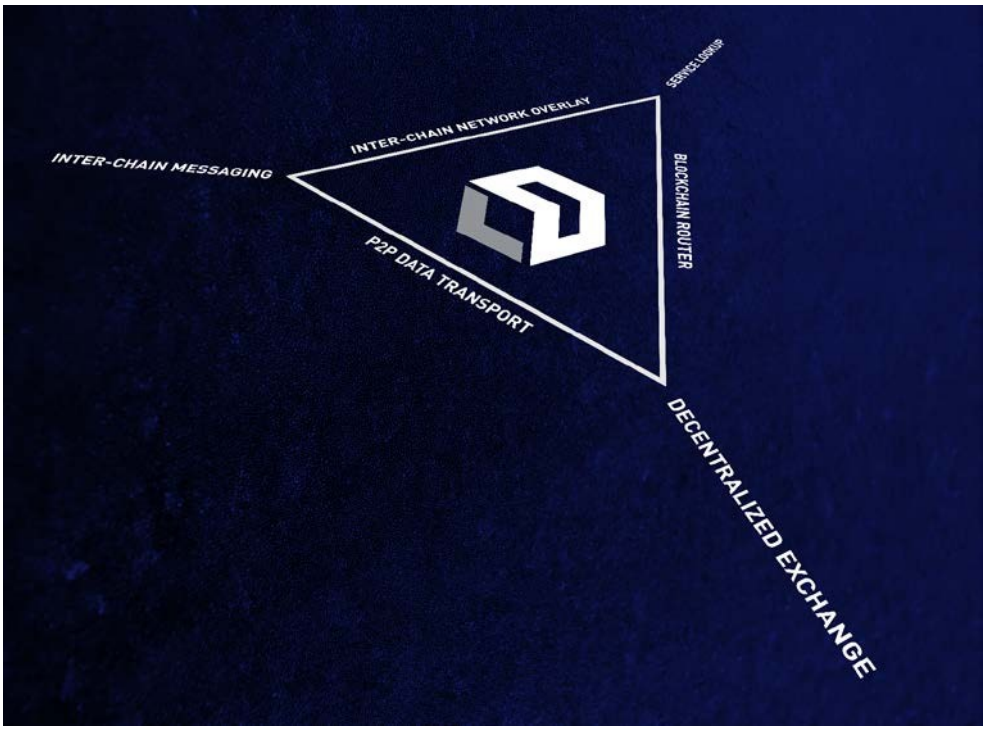


그림 5.
두번째 신판: 블록넷의
세 가지 주요 서비스와
요소들
삼각형의 끝 부분 각은
면들이 만나는 부분으로,
서비스들이 이곳에
배치되어 주요 요소들을
조화롭게 어우르는 형태를
시각화 하였습니다.

서비스 찾기

인터체인 서비스 찾기는 엑스브리지, 엑스 네임, 엑스챗 요소들을 조화롭게 어울러 블록넷의 **레지스트리에 있는 어떠한 인터체인 서비스들이라도** 찾을 수 있게 합니다. 이는 블록넷이 완성되어 감에 따라 추상적으로 변하여 허울뿐인 API 가 될 수도 있습니다.
기존의 인터넷과 같이, 상호 운영하기 위해서는 유저 및 단체들 간에 검색기능과 위치하기 기능이 필요합니다. 그러므로, 아날로그식의 DNS (Domain Name System) 이 요구됩니다. 하지만 기존의 인터넷 방식인 하나의 IP주소를 중심으로 서버들이 연개되는 것 과는 다르게, 서비스들은 네크워크에 있는 아무 노드에 의해 개인에서 개인으로 전달되어, 서비스가 신청될 때 주어진 블록체인 네트워크에 속한 노드중 *아무거나* 하나만 요구됩니다. 이런 이유로, “체인 코드”들이 최우선적 요구사항이며, 다른 것들은 이차원적인 요구사항들 입니다.

보통의 경우에는 서비스들이 특정한 노드로만 전달 된다고 가정합니다.

개인에서 개인간의 네트워크 레지스트리 서비스에서 꼽히는 특징 중 하나는 *누구나* 서비스를 제공할 수 있다는 사실입니다. 기존의 경우 보통 대 다수의 서비스 제공자들은 신뢰성이 보장되었지만, 개인에서 개인간의 서비스에서는 나쁜 의도를 가진 아무나 신뢰성이 보장되지 않고 서비스 제공이 가능합니다. 디자인 전략에 따라 서비스 찾기로 얻어지는 결과의 정보 신뢰성이 보장되지 않는다면 찾기 과정 이후에 서비스의 온전성이 보장되어야 합니다. 또는, 서비스 찾기 과정이 효과적으로 암호화 되어 데이터 결과물의 신뢰성을 보장하고 결과로 찾아지는 노드들이 어떤 악의적 의도를 가지고 있는가와는 상관없이 안전성과 신뢰성이 보장되어야 합니다. 블록넷의 디자인은 레지스트리 디자인이 어떤 형식으로 짜여져 있던지 와는 무관하게 실행할 수 있도록 디자인 되었습니다.

메세지 보내기 과정

이제까지 쓰여지던 디자인으로 예를 들자면, 다음과 같은 전형적인 서비스 찾기 과정을 거쳐야 합니다:

1. 엑스브리지를 통해 상대를 찾습니다
2. 엑스네임으로 서비스 체인아이디와 서비스리스트를 얻습니다
3. 엑스브리지를 통해 상대를 요청하여 체인 아이디로 지정된 상대의 체인을 찾습니다
4. 엑스쳇으로 전환하여 상대가 제공하는 서비스들의 리스트를 얻습니다
5. 서비스를 신청합니다 (동시에 서비스의 신뢰성을 입증받습니다)

최신 디자인이라고 가정한다면, 서비스 찾기는 평범하게 블록체인 공통의 알고리즘을 사용하여 완료되며 (블록넷 프로젝트에 특별히 추가되지 않았습니다) 노드가 서비스를 로컬 호스트하기 위해서는 블록체인의 체인 아이디 데이터를 얻어서 간단히 무료로 요청할 수 있습니다. 하지만 이 방법은 유저들에게 많은 양의 저장소와 오랜 시간을 부과하게 되므로 블록넷의 보편적인 방법으로 기대되지 않습니다. 기존의 비트코인 설명서 (Bitcoin Whitepaper)에서 설명이 되었듯 유저들이 서비스 레지스트레 블록체인을 유지하는 SPV 노드들에서는 이 방법이 사용 되었을 수도 있습니다. 더 큰 확장성과 작은 엡 흔적을 위해서는 지금 이 순간에도 대체 가능한 시스템이 개발되고 있습니다. 디자인 패턴을 위해서는 **거래 내역 섹션**과 **레지스트리 서비스 섹션**을 참조해 주십시오.

맥락 도표

위에 설명된 과정들을 아래 그림 구조에 대입시켜 보았습니다:

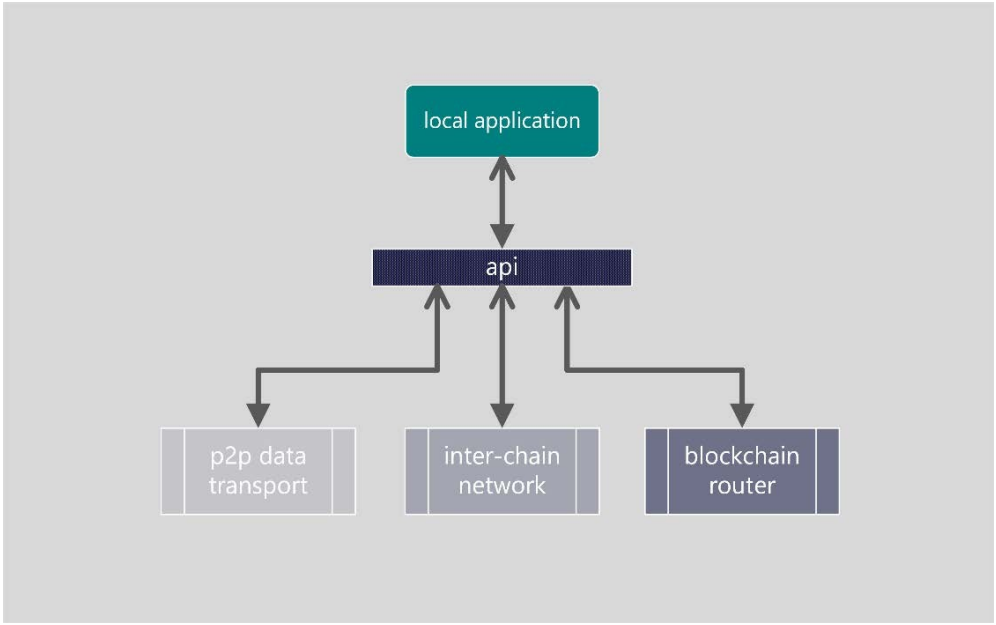


그림 6.

맥락 도표는 로컬 머신이 사용하는 찾아보기 기능에 사용되는 주요 요소들의 관계를 표현하였습니다. 기술관련 문서는 기술설명서 섹션을 참조하여 주십시오.

기술관련 문서는 기술설명서 섹션을 참조하여 주십시오.

구현 방법

현재: 서비스 찾기 기능은 XBridgep2p.exe 또는 블록넷 지갑 (Blocknet Wallet) 에서 구현되도록 하였습니다. 블록넷의 현재 개발 상황에서 구현된 유일한 어플리케이션은 탈 중앙화된 거래 (decentralized exchange)이며, 이를 위해서는 노드들은 단지 실시간 통화 가치를 근거로 한 교환을 위한 과정을 거쳐야 합니다. 보통의 목적으로 한 서비스 찾기 기능은 현재 개발 중에 있습니다.

차후 계획: 블록체인 경제 생태계에 적합한 보통 목적의 서비스 찾기 기능이 개발 중에 있습니다. 더 나아가, 유저들의 더 나은 인터페이스와 편리성을 추구하기 위해 서비스 찾기 기능이 API façade 에 내장될 수 있습니다. 이것이 모든 주요 서비스들에 공통적으로 연동되는 하나의 façade 인지 아니면 서비스 찾기 기능만을 위한 façade 인지 여부와는 상관 없이 유저들의 요구사항, 시간 절약, 그리고 완성도를 고려하여 개발 될 것입니다.

인터체인 메세지 보내기

인터체인 메세지 보내기는 엑스브리지와 엑스쳇을 조화롭게 연결하여 제작 되었으며, 서비스 제공자와 서비스 소비자가 서로를 만나고, 연락하며 서비스가 전달되는 중요한 요소입니다.
이 요소는 유저들이 적극적으로 서비스를 찾는다는 가정하에 설계 되었으며, 서비스 제공자들은 언제나 지속적으로 찾아 질 수 있도록 설계 되었습니다.

공공의 개인에서 개인으로의 네트워크에서는 스스로 서비스 제공자이던 서비스 소비자라고 밝히는 모든이들이 좋은 의도를 가지고 있다고 가정하기 어렵습니다. 그러므로, 상호간 거래가 이루어 지기 전에 서비스 제공자는 서비스 소비자가 돈을 지불할 것 이라는 확신이 있어야 하며, 서비스 소비자는 서비스 제공자가 자신에게 원하는 서비스를 제공할 것이라는 확신이 있어야 합니다. 다른 말로 하자면, 모든 서비스 거래는 *신뢰성 여부와는 상관 없이 즉각적으로 atomically 이루어 져야 합니다.*

이를 달성하기 위해 본사는 “Zero-knowledge Proof System”을 사용 하였습니다. BIP-0199에서 주석하였듯, “다양한 zero-knowledge proving system이 존재하며 이는 hash preimage 의 가치있는 정보를 보장해 줄 수 있다. 예를 들어, zero-knowledge proof 는 hash preimage 가 스도쿠 퍼즐의 해답을 위한 암호 해독의 열쇠로 사용될 것이라는 확신을 줄 수 있다. (pay-to-sudoku 프로토콜의 예 참조.)” 쉽게 정리 하자면, 간단한 디지털 서명 행위만으로 서비스 제공자의 개인적인 열쇠 (key) 가 공개되지 않게 하면서 소비자 스스로 자신의 신원을 서비스 제공자에게 입증할 수 있습니다. 실제적인 신원 입증 과정은 서비스들 간에 구현의 차이가 있을 수 있고, 이 모든 과정은 “신뢰성이 필요없는” 서비스 전달 방식을 실현 하기 위해 필요한 것입니다.

Atomicity 는 탈 중앙화된 거래를 통해 이루어 졌으며, 이어지는 섹션을 참조 바랍니다.

메세지 보내기 과정

인터체인 메세지 보내기의 보편적인 과정은 다음과 같습니다:

1. 서비스를 네트워크 오버레이에서 찾고 서비스를 요청합니다.
2. 엑스쳇에서 서비스 제공자는 페이로드의 합법성을 위해 zero-knowledge proof 에 필요한 것들을 제공합니다. (간단한 예를 위해서는 거래 내역 섹션을 참조해 주세요)
3. 서비스 소비자가 서비스를 수락합니다

4. 서비스 제공자가 탈 중앙화된 거래 서비스를 통해 서비스를 전달합니다

엡 흔적 (footprints)를 최소화 하고 간단한 거래를 위해서, 인터체인 메세지 보내기는 다른 API façade를 요구할 수 있습니다. 이것이 적절하게 사용된 경우는 무료 서비스, 또는 체인 찾아보기가 hardcoded 된 탈 중앙화된 쳇 엡 (chat app) 입니다.

도표 정황

아래의 도표에 위의 내용을 담아 보았습니다.

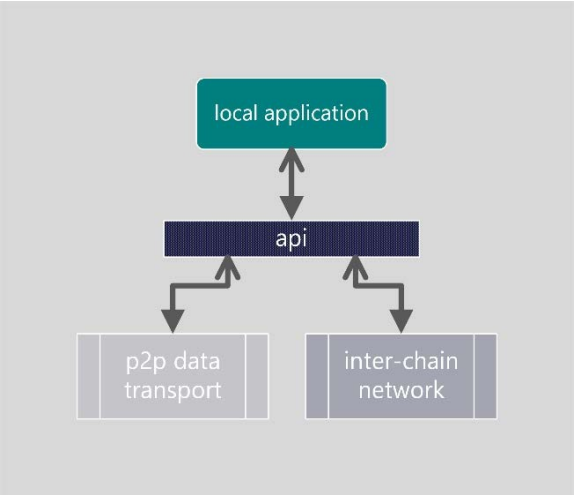


그림 7

주요 요소들의 관계도와 로컬 머신의 인터체인 메세지 보내기 서비스를 연결하여 도표에 표현해 보았습니다.

구현 방법

현재: 개발자들이 엑스쳇에 어플리케이션을 내장하거나 네트워크 오버레이를 활용할수 있으며 이를 엑스브리지만의 독립적인 어플리케이션을 통하거나 블록넷 지갑 (Blocknet Wallet)에 내장한 형태로 구현 할 수 있습니다.

차후 계획: 요소들은 API들에 적히거나 모듈화되어야 하며, 추가적으로 API façade 를 잠재적으로 추상화하거나 두가지 이상의 요소들을 접목시켜 확실한 서비스를 제공합니다.

탈 중앙화된 거래

탈 중앙화된 거래는 다른 화폐나 서비스로 교환할 때 신뢰가 필요 없이 일시적으로 거래 됨을 의미합니다. 이것은 엑스브리지와 엑스쳇의 조화로운 상호 실행으로 가능하며 노엘 티어난의 아토믹 거래 프로토콜의 구현 방법을 통하여 적어도 두 가지의 지갑들 또는 블록체인 노드를 요구합니다. 이 프로토콜은 자본이 사용될 때 드러나게 실패 할 수 없는, 자본을 사용하는 데에 요구되는 비밀이 만들어 지는 지식을 활용합니다. 그러므로, 만약 제작자가 상대 측의 자본을 쓴다면, 상대측 또한 제작자의 자본을 사용할 수 있는 비밀을 얻을 수 있게됩니다.

참조: 탈중앙화된 거래 서비스는 탈중앙화된 거래 어플리케이션과는 다릅니다. Block DX는 이 서비스를 블록체인 서비스들에 추가적으로 사용합니다.

초기 개발 모델

프로토콜의 첫 번째 버전에서는 malleability-based extortion attack 에 취약한 모습을 보였고, 이후에 이를 보완하여 Bitcoin-and-clones 생태계에서 opcode인 OP_CHECKLOCKTIMEVERIFY를 공개 하였습니다. 케이쿠로가와 (Kay Kurokawa)의 프로젝트 블로그에 차후 디자인 활용도에 대해 자세히 다루었습니다. 마침내, 가상화폐의 아토믹 스왑 (atomic swaps) 과 토큰들과 다른 디지털 페이로드 (digital payload) 들을 지원하기 위해 본사는 이 프로토콜을 암호 해독의 키로 사용하거나 해쉬 기능을 안전하게 하기 위해 비밀로써 추가 하였습니다. 이로써, 비밀을 밝히는 행위는 즉각적으로 전에 암호화 되었던 상품들을 소비하거나 몇몇의 진실을 요구하는데 입증하는 목적으로 사용될 수 있습니다. 이것은 전 섹션에서 열거되었던 zero-knowledge proofs 을 사용하는것과 접목되어 소비자들이 디지털 상품들을 받기전에 미리 신뢰성을 확보하여 *신뢰가 필요없는 서비스와 상품들의 화폐화된 소비를 활성화 할 것입니다.* 아래에 이를 위한 평범한 서비스 프로토콜을 소개 하였습니다.

프로토콜 순서

개념상으로 프로토콜의 순서는 다음과 같습니다:

1. 서비스 제공자는 디지털 상품을 위한 열쇠 (디지털 서명 또는 진실성 여부 입증을 위한 해쉬 파일) 을 만들거나 코인 거래를 위한 무작위의 숫자를 만들어서 프로토콜의 비밀로서 사용합니다.
2. 서비스 제공자는 “bail-in” 거래내역을 “이 거래내역은 소비자가 비밀을 제공하거나 서비스 제공자와 소비자 둘다 거래에 서명한다면 소비자가 사용할 수 있다.” 와 같은 계약을 근거하여 만든다. (만약 코인이 아닌 디지털 상품이 제공된다면 거래 수수료를 부담할 네트워크 비용 코인만 필요합니다.)
3. 서비스 제공자는 부차적인 대비장치로서 “환불” 거래를 “현재로 부터 X 양의 시간이 지난 후 베일-인(bail-in) 거래의 양 만큼 서비스 제공자의 주소로 보낸다” 는 법칙하에 만든다.
4. 서비스 제공자는 서비스 소비자에게 서비스 소비자와 서비스 제공자 양측 모두 동의, 서명할 경우 되돌릴 수 있는 베일-인 (bail-in) 거래를 위한 두번째 요구사항을 충족 시키기 위하여 환불 거래 서명을 요청한다.
5. 소비자는 환불 거래에 서명하고 서비스 제공자에게 돌려 준다.

a. 참조: 이것으로 서비스 제공자는 소비자가 거래를 취소하거나 거래가 완료되는 데 필요한 조건을 불충족 시켰을 경우, 만약 서비스 제공자 소유의 코인이 있었다면 일정 시간 내에 소유권을 되 찾을 수 있습니다.

6. 서비스 제공자는 거래 내역을 공개합니다.

a. 참조: 소비자가 비밀을 주었다면 이제 이 거래를 “소비” 할 수 있습니다.

7. 소비자는 순서 2 에서 언급된 방법으로 개인 소유 블록체인에 있는 코인을 위해 “베일-인 (bail-in)” 거래를 만듭니다.

a. 참조: 이 단계에는 서비스 제공자가 비밀을 소유하고 있으며, 이 거래가 소비되기 위해서는 서비스 제공자가 소유한 비밀이 풀리는 것이 요구됩니다.

8. 순서 3 에서 언급된 방법으로 소비자가 스스로의 “환불” 거래를 만듭니다.
9. 순서 4 에서 언급된 방법으로 소비자는 서비스 제공자에게 환불 거래에 대한 서명을 요청합니다.
10. 서비스 제공자는 환불 거래에 서명하고 소비자에게 환불합니다.

a. 참조: 이로서 서비스 제공자가 현금화 하기 실패한 소비자 소유였던 코인은 소비자에게 돌아가며, 소비자는 서비스 제공자가 소유하고 있던 비밀을 풀수 없으므로 서비스 제공자의 서비스를 소비하거나 거래를 통한 코인을 획득할 수 없습니다.

11. 소비자는 베일-인 (bail-in) 거래 내역을 공개합니다.

a. 참조: 서비스 제공자는 이제 소비자의 비밀을 풀었으므로 소비자의 코인을 사용할 수 있습니다.

b. 참조: 소비자의 코인을 사용함 으로서 서비스 제공자는 비밀을 공개적으로 밝히게 되며, 소비자는 서비스를 이제 사용할 수 있습니다.
c. 참조: 만약 서비스 제공자가 거래를 취소하기를 원한다면, 순서 3 에서 일정 시간을 기다린 후 환불 거래를 공개할 수 있습니다.
12. 서비스 제공자는 소비자의 거래 내역을 소비하여 비밀을 풉니다.
a. 참조: 만약 서비스 제공자가 베일-인 (bail-in) 거래를 소비하는데 실패한다면, 소비자는 환불 거래를 공개할 수 있고 일정 시간이 지난 후 코인을 되 돌려 받을 수 있습니다.
b. 참조: 서비스 제공자는 소비자의 베일-인 (bail-in) 거래를 거래 내역에 계약되어진 일정 시간 내에 반드시 소비해야 하며, 이를 어길 경우 소비자는 자유롭게 환불을 받을 수 있습니다.
13. 소비자는 서비스 제공자의 베일-인 (bail-in) 거래를 소비하거나, 파일을 암호화 하거나, 사실을 확인하기 위해 비밀을 사용합니다.
a. 참조: 코인 거래의 경우, 소비자는 서비스 제공자의 거래 내역을 환불 거래 계약에 명시되 있는 일정 시간내에 반드시 소비해야 하며, 이를 어길 경우 서비스 제공자는 자유롭게 환불 받을 수 있습니다.

위의 프로토콜은 서비스 노드들이 그들에게 의존하고 있는 SPV 노드들과 “가벼운” 클라이언트들이 거래를 공개하여 메세지를 확실하게 업데이트 하도록 아토믹 스왑의 상태에 대해 업데이트 한 추가적인 부수적 과정들을 포함할 수 있습니다.

메세지 보내기 과정

블록넷의 요소들에서 구현되었듯, 탈 중앙화된 거래는 보통 다음과 같은 과정으로 실현됩니다:

1. 인터체인 메세지 보내기 섹션에서 언급된 방법으로 소비자가 서비스를 수락한 후, 서비스 제공자는 프로토콜 순서 1-3 을 거치고 난 후 엑스칫을 통하여 순서 4 를 실행합니다.
2. 소비자가 엑스칫을 통해 순서 5 를 실행합니다.
3. 서비스 제공자가 원래 사용하던 블록체인 네트워크를 통해 프로토콜 순서 6 을 실행합니다.
4. 소비자는 프로토콜 순서 7-8 을 실행한 후 엑스칫을 통해 순서 9 를 실행합니다.
5. 서비스 제공자는 프로토콜 순서 10 을 엑스칫을 통해 실행합니다.
6. 소비자와 서비스 제공자는 프로토콜 순서 11-13 을 각자 애초에 사용하던 블록체인 네트워크를 사용하여 실행합니다.

이 모든 과정들은 오로지 탈 중앙화된 거래 서비스만을 염두하고 있습니다. 탈 중앙화된 거래를 위한 어플리케이션인 Block DX 는 거래용 어플리 케이션으로서의 기능을 수행하고자 다른 대 다수의 어플리케이션과 같이 몇몇의 추가적인 (부수적인) 서비스들, 특히나 오더 브로드케스트 (order broadcast), 오더 매칭 (order matching), 안티스팸 메쥬어 (anti-spam measures), 안티도스 메쥬어 (anti-DOS measures)와 거래 수수료 수집용 서비스를 요구합니다.

도표 정황

위에서 언급된 과정들이 로컬 머신과 요소들간의 관계도를 아래의 그림에 정리 하였습니다.

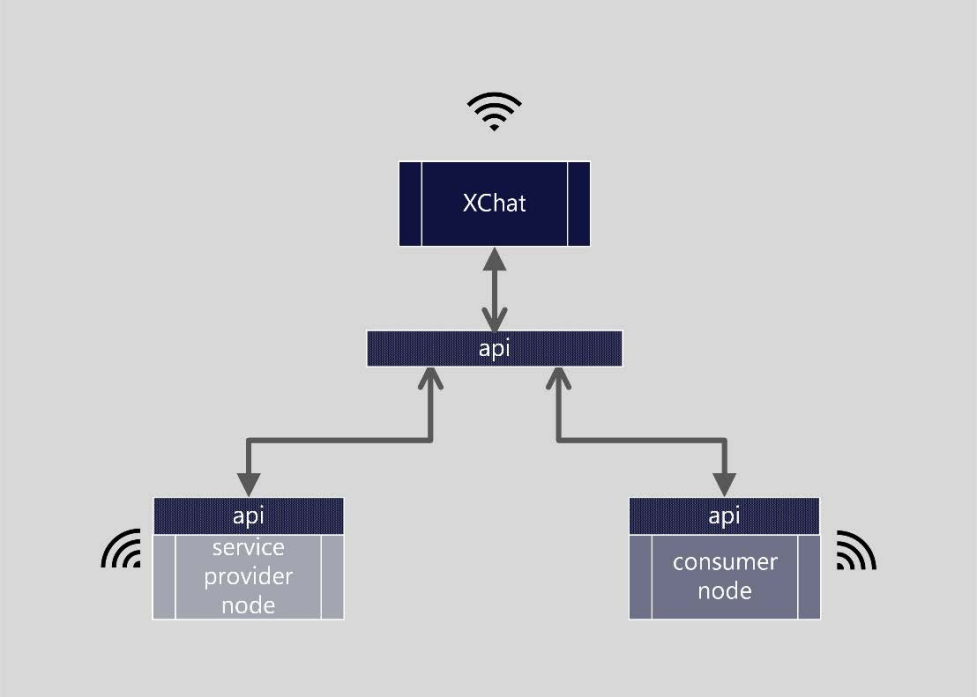


그림 8

로컬 머신에 포함된 요소들의 관계도와 그로 인한 탈 중앙화 거래 서비스의 관계를 그림으로 표현 하였습니다.

구현 방법

현재: 탈 중앙화된 거래 서비스는 블록넷 지갑 (Blocknet Wallet)과 XBridgep2p.exe 에 독립적으로 내장되어 있습니다 (하지만, 개발은 총 프로젝트 개발 후기에 재개될 것 입니다). 탈 중앙화 된 거래 어플리케이션을 동시에 보조하는 API는 이미 준비 되었습니다.

차후 계획: 블록 DX 가 소비하는 서비스는 다양한 블록 체인 서비스들과는 따로 나뉘어져 취급 되어야 하며, 엑스칫과 블록체인 서비스를 조화롭게 운용하고자 API façade가 개발되었습니다.

블록넷 요소들

주어진 로컬 머신에 위의 섹션들에 언급된 세가지 주요 서비스들이 각자와 상호 운용 될 수 있으며, 그렇지 않은 경우의 몇몇 블록 체인들에서는 아래의 요소 종류들의 조합을 통해 실행 될 수 있습니다:

1. 풀 노드 (full nodes): “보통의” 최대 기능의 노드들과 지갑들 (wallets)
2. 라이트 노드 (light nodes): SPV 노드들 몇몇의 간단화된 노드들 (예: 거래 내역에 필요한 서명)
3. 서비스 노드: 보통 블록체인 워크에 특정한 서비스를 제공하고자 특별한 기능을 보유한 노드들

이러한 요소 종류들은 보통 블록넷에 의해 관리되거나 만들어 지지 않은, 외부 회사 또는 개인이 블록넷에 통합된 제 3기업 또는 개인입니다. 그럼에도 불구하고 그들은 자발적으로 그들만의 요소, 고유의 블록체인들을 복사하여 블록넷에 접목, 연동 시킴으로서 블록넷이 이룩할 수 없는 상호 운용성등 블록넷에 필요한 기능들을 제공합니다. 이 방식은 블록넷의 입장으로서는 절대로 옹호 할 수 없는 비효율 적인 접근 방식이지만, 이 모든것이 제 3자에 의해 자발적으로 이루어 지기에 가능합니다.

세 가지 주요 요소들과 서비스들, 다른 추가적인 노드 종류 소비형태 또는 인터체인 서비스 전달하기 등을 보기 쉽게 그림으로 아래에 정리 하였습니다:

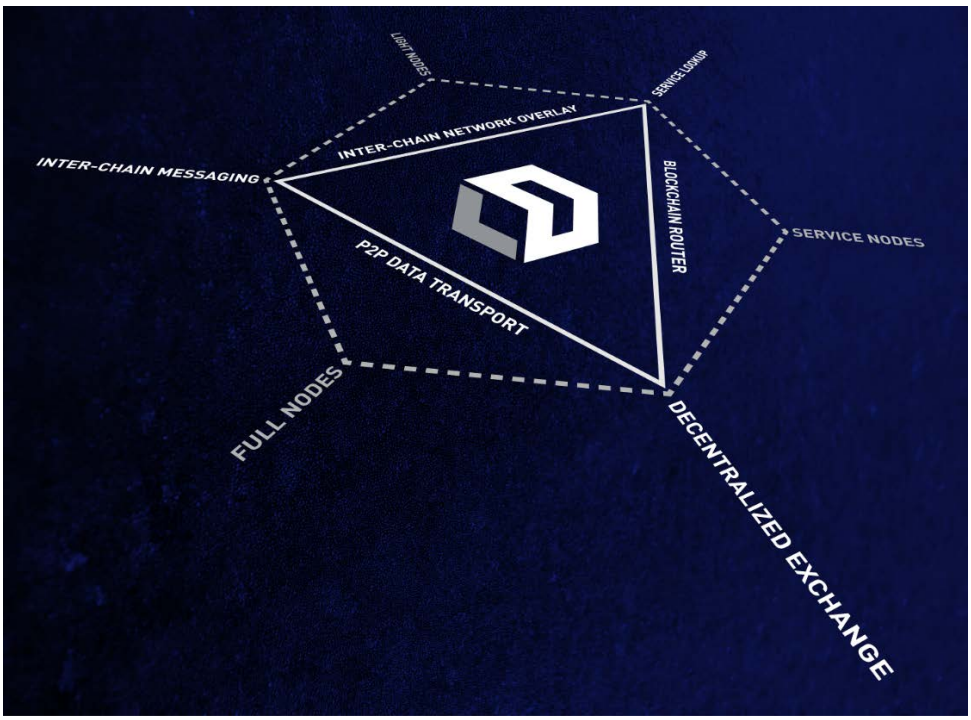


그림 9.

세번째 신판: 세 가지 주요 서비스, 요소들과 블록체인 요소들의 관계도
블록 체인 요소들은 주요 서비스들을 소비하므로, 이들의 관계도는 삼각형의 끝 부분 각진곳에 위치하고 있습니다.

블록체인 서비스들

블록체인 서비스들은 특정 경우에 주요 서비스들의 기존 목적을 돕는 보조자 역할을 합니다. 블록넷에 생성될 수 있는 인터 체인 서비스들의 한도 숫자가 존재하지 않으므로, 제 3자가 건설할 수 있는 블록 체인 서비스들의 숫자 또한 제한받지 않습니다.

블록 DX는 블록넷의 첫 번째 인터 체인 dapp이며 몇몇 블록체인 서비스들을 필요로 합니다. 이것에 대해 문서화하고 블록체인 서비스의 특징을 삽화화 하려면 이 것에 대해 짚고 넘어 가지 않을 수 없습니다.

블록 DX 블록체인 서비스들에 관한 개요

거래 기능을 수행하자면 계약 당사자들간의 아토믹 스웝 (atomic swap) 관련 몇몇 서비스들이 요구됩니다. 사실상 중앙화 또는 탈 중앙화된 모든 거래 목적 서비스는 아래와 같은 네 가지의 주요 기능들을 충족시켜야 합니다:

- 자본 저장기능
- 공개적인 주문기능
- 공개적인 주문 매칭기능
- 거래 마무리

블록 DX는 탈 중앙화된 거래 시스템 이므로, 넓은 관점에서 볼때 탈 중앙화를 적절히 이루었다고 평가 되는 완전히 공개된 코드 베이스 소스 (codebase sourse) 유지하기나 누구라도 코인 종류를 등록할 수 있는등의 기능과는 별도로 위에서 언급된 네 가지 모든 기능들이 전부 탈 중앙화를 이루어 추가되어야 합니다. 아토믹 스왑을 통하여, **탈 중앙화된 거래 서비스는** 자본 저장기능과 거래 마무리 기능 둘 다 *선천적으로* 탈 중앙화 됩니다. 하지만, 아토믹 스왑은 스스로 거래의 양을 정하지 않는 관계로 공개적인 주문이나 주문 매칭은 추가적으로 탈 중앙화 되어야 합니다. 이러한 기능들이 블록 체인 서비스들에 의해 보조될 것이며, 이는 아래와 같습니다:

- 공개적인 주문은 서비스 찾기 기능을 레버레징 (leveraging)하여 탈 중앙화를 이루며, 이 모든 과정은 완전히 개인과 개인간에 이루어 집니다.
- 주문 매칭 기능은 각각 거래자들의 로컬 dapp 을 통하여 이루어 지며, 이 모든 과정은 블록넷의 주요 요소들과 각각 블록체인 요소들과의 조화로운 운영을 통하여 완성됩니다.

공개적 주문하기 기능과 주문 매칭 기능의 근본적인 디자인은 다른 모든 개인과 개인간 거래 시스템과 같이 DOS (denial-of-service) 공격에 취약합니다. 비트코인이 이러한 비잔틴 제네랄의 문제 (Byzantine Generals Problem) 를 풀고 전산적 현금 시스템을 구축하고자 선택한 아날로그적 방법으로 내린 결론은, 운용 가능한 솔루션은 주문 예약이 된 서비스들의 질을 보장해야 합니다. 둘째로, 토큰 경제 생태계 디자인의 중요한 고려 요소중 하나는 만약 사업 모델들이 암호 경제화되지 않았다면 아예 적용이 안되는 것인데 탈 중앙화된 생태계 환경에서 어떻게 서비스가 현금화 되는지를 고려 해야 합니다. 앞으로 다루어질 내용들은 이러한 문제들의 논의 및 소개글이며, 이 문제에 대해 블록넷이 제시한 해결책들입니다.

탈 중앙화된 주문 예약

참조: 앞으로 자세히 다루어지는 섹션들은 블록넷의 후보 주문 시스템입니다. 여러 시스템들이 고려되고 있지만, 이 새롭고 익숙하지 않은 탈 중앙화된 주문 시스템 디자인 공간에 대한 여러가지 의견이나 소견들은

듣고자 현재로서 가장 유력한 후보 시스템이 소개 되었습니다.

주문 예약은 전형적인 주식 거래 방식과 같이 한 거래자가 유동자산을 매매 또는 입찰하는 과정입니다. 주문 예약을 통해 매매 또는 입찰이 이루어 질 경우 이를 되 돌릴수 없습니다. 탈 중앙화된 시스템에서의 주문 예약은 공적으로 거래를 알리는 알림처의 역할도 수행하게 되었고, 누구나 주문을 매매 또는 입찰할 수 있으며 이를 관여하여 조종할 수 있는 중앙화된 악한 의도를 가진 제 3자는 존재하지 않습니다.

이와 같은 탈 중앙화된 주문 예약 서비스는 두 가지를 조건을 충족 시켜야 합니다. 첫째, 악한 의도를 가진 사기성 주문이 올라오는 것을 막아 진짜 거래 목적을 가지고 올라오는 "좋은" 주문들만 최종적으로 올라오게 해야 합니다. 둘째, 만약 주문이 매칭되었을 경우, 주문에 관여된 양 측은 무조건적으로 거래를 수행하게 해야 합니다. 이를 위해서는 주문-DOS를 방지해야만 합니다. 하지만 놀랍게도 블록체인은 두 가지의 이유로 인해 주문 예약을 위해 *적합하지 않은* 기술입니다. 첫째 이유는 주문 예약은 엄청나게 빠른 속도를 요구하여 사용자들에게 실시간 거래를 가능하게 해야 하지만, 블록 체인은 여러 검증 과정을 거쳐야 하는 관계로 이를 충족시킬 수 없습니다. 둘째로, 블록체인은 코인을 채굴하거나 진실을 밝혀서 모아야 하는 특성때문에 다음 블록을 체굴하게 되는 사람에게 잠재적으로 주문 매칭이 이루어 지는데에 더 유리한 주문 정보를 제공하게 됩니다. 그러므로, 탈 중앙화된 주문 예약 과정을 성공적으로 충족시키기 위해서는 별도의 시스템이 필요합니다.

주문 예약에 관해 마지막으로 언급하고 싶은 특성은, *주문 매칭은 미래 거래 행위에 대한 책무 이므로*, 매칭 과정이나 공적인 주문 과정에서 자산이 보내져 사기 당할 가능성을 줄이므로 직접적으로 자산이 보내지거나 지불하는 방식에 비해 훨씬 적은 사기 가능성을 가지고 있습니다. 이로서 블록체인 사용에서 나타날 수 있는 시스템 오작동에 의한 벌금에 대한 부담이 아예 없으므로 주문 시스템 디자인에서 확실한 우위를 점하게 하는 요소라고 판단됩니다. 시스템은 약간의 비 신뢰성은 용인하며 정상 기능을 수행할 수 있습니다. 이와 같이, *최소한의 기본* 디자인 요구사항은 각 개인의 행동의 정도와 상관없는 어떠한 불법행위라도 방지할 수 있어야 합니다. 이에 대해 자세히 언급하자면 블록넷의 솔루션이 갖추어야 할 사항들은 아래와 같이 정리됩니다:

a) 거래에 사용된 코인이 소비 가능하도록 UTXO 인증을 갖춥니다.
b) 정직한 거래자들에게 최소한의 영향을 끼치며 스팸 행위를 극도로 어렵게 하는 해쉬캐쉬 형태의 거래 수수료를 통해 스팸 주문들을 방지합니다.
c) (b)와 같은 방식으로 DOS 주문들도 방지합니다.
d) 서비스 노드들간의 경제적 결탁을 수지타산이 맞지 않게 하여 방지합니다. (**서비스 노드들의 특수성** 참조)
e) 여러 당사자들간에 하나의 주문을 소비하는 것을 가능하게 하고, 환불된 금액이 소비 가능해 지기 전까지 주문 전체가 하나의 당사자에 의해 취소되게 되는 일이 없도록 부분적 주문 매칭을 지원합니다. 이것은 반대 측이 높은 가치를 지닌 하나의 거래를 버릴 때 발생하는 기회 비용을 피하고자 여러 주문에 다양한 가격대로 나누어 버리는 거래 전략을 보조할 수 있습니다.

탈 중앙화된 주문은 도대체 어떨까요? –자주 통치권-

탈 중앙화된 거래에서 거래하는 사람들 간의 자주 통치권을 유지하기 위해 본사는 주문들과 주문양에 관해 탈 중앙화를 유지합니다. 탈 중앙화는 아직 잘 알려지지 않은 개념으로서 자주 "분포" 의 개념과 섞여서 같은 의미로 혼동되곤 합니다. 비탈릭 부테린 (Vitalik Buterin) 이 확실히 설명하였듯, 탈 중앙화에 가장 중요한 요소는 "규제"입니다. 탈 중앙화된 시스템에서는 공유되는 자원에 관련된 것 이외에는 그 누구도 "규제" 당하지 않으며 모든 개인이나 단체가 동등한 취급을 받습니다. "분포" 에서는 이와는 다르게 누군가가 규제하여 몇몇의 단체들이 결과물을 나누거나 각자의 역할을 수행합니다. 결론적으로, 분배 형태가 될지 탈 중앙화된 규제 형태가 될지는 단체들간의 엄격한 동의와 의견 일치를 통해서 결정 됩니다. 하지만 이것이 탈 중앙화된 비트코인이 어떤 거래 내역이 진짜인지, 또는 결과물이 네트워크의 가장자리에 분포되는지에 대해

동의하는 것을 필요로 하지 않는다는 것을 의미하는 것은 아닙니다. 이러한 요소들이 필요하긴 하지만 비트코인을 탈 중앙화 하는데 충분한 것은 아닙니다.

탈 중앙화된 화폐는 과거에 겪어 보았던 자주 통치권을 행사하는 탈 중앙화된 주문들과 유사하며, 이에는 같은점과 다른점이 있습니다. 같은 점에는 첫째, 비트코인을 보유한 누구건 제 3자의 규제없이 코인을 보낼수 있으며, 오더북 (order book) 에 누구건 자산을 추가하거나 자산을 뺄 수 있습니다. 둘째, 비트코인 사용자들은 코인이 어떤 시간에 누구에게로 보내 졌는지 입증할 수 있고 이와 거래하는 측은 이 주문들의 유효함과 주문 허락 메세지를 스스로 확인 할 수 있습니다. 하지만 다른 점도 존재하며 하나의 예로 주문들은 코인을 보내는 것을 의무화 하여, 미래의 거래 상대측은 이 것을 소비하는것을 의무화 하여 매칭 과정에 관여하게 됩니다. 매칭과정이 주문 허락 메세지에 공동으로 서명하는 것을 의무화 하고 이 주문이 매칭되는데에 다른 어떤 추가 독립체들을 필요로 하지 않으므로, 네트워크에 속한 개인들은 일치되는 알고리즘 (예:결과물의 증거) 을 요구받지 않고 각자의 순수 자주 통치권에 근거하여 주문들의 상황에 대해 알아낼 수 있습니다.

본사는 완전한 자주 통치권 주문 시스템 디자인을 추구하며 세개의 단체들과 연관되어 있습니다. 아래의 피상적 전체 요약은 이에 대한 설명이 추가됨에 따라 더 자세히 다루어 질 것입니다:

- 주문이 공개화 되기 이전에, 시장을 만든이가 개인적으로 주문과 스팸 방지 비용 내역을 서비스 노드에게 보내고 이는 나중에 공개화 되며 만약 이것이 악용되었을 경우 이 코인들을 네트워크 비용으로 소비하게 되어 시장을 만든이에게 피해를 줍니다. 비용 거래내역이 비준되고 난 이후 서비스 노드는 주문에 서명하고 시장을 만든 이는 이것을 주문을 비준하는데에 사용합니다.
- 주문이 공개화될 때, 거래자들은 주문이 진짜 코인을 근거로 이루어 지는지, 서비스 노드에 의해 서명되었는지, 거래 비용은 지불되었는지를 스스로 확인할 수 있습니다.
- 한명 또는 여럿의 거래자들이 주문을 수락하려고 시도할 때, 시장을 만든이는 이 요청들 가운데 (보통의 경우 첫 번째 요청을 수락합니다) 자신이 원하는 거래 상대를 정할 수 있습니다.
- 거래 상대가 결정되면 시장을 만든이는 거래 상대가 거래를 DOS 할지 걱정하게 되므로 서비스 노드가 거래 비용을 지불했는지 확인하고자 기다릴 것입니다.
- 서비스 노드가 서명 수락 메시지를 공개화 하면, 주문은 공개 예약 리스트에서 사라지며 이는 전체 마켓 업데이트 될 것입니다.

이와 같이, 블록 DX의 주문 예약 기능은 탈 중앙화된 형태의 머신입니다. 아래의 도표에 이 고도의 머신을 표현해 보았습니다 (이 섹션은 도표에 자세히 소개되었습니다):

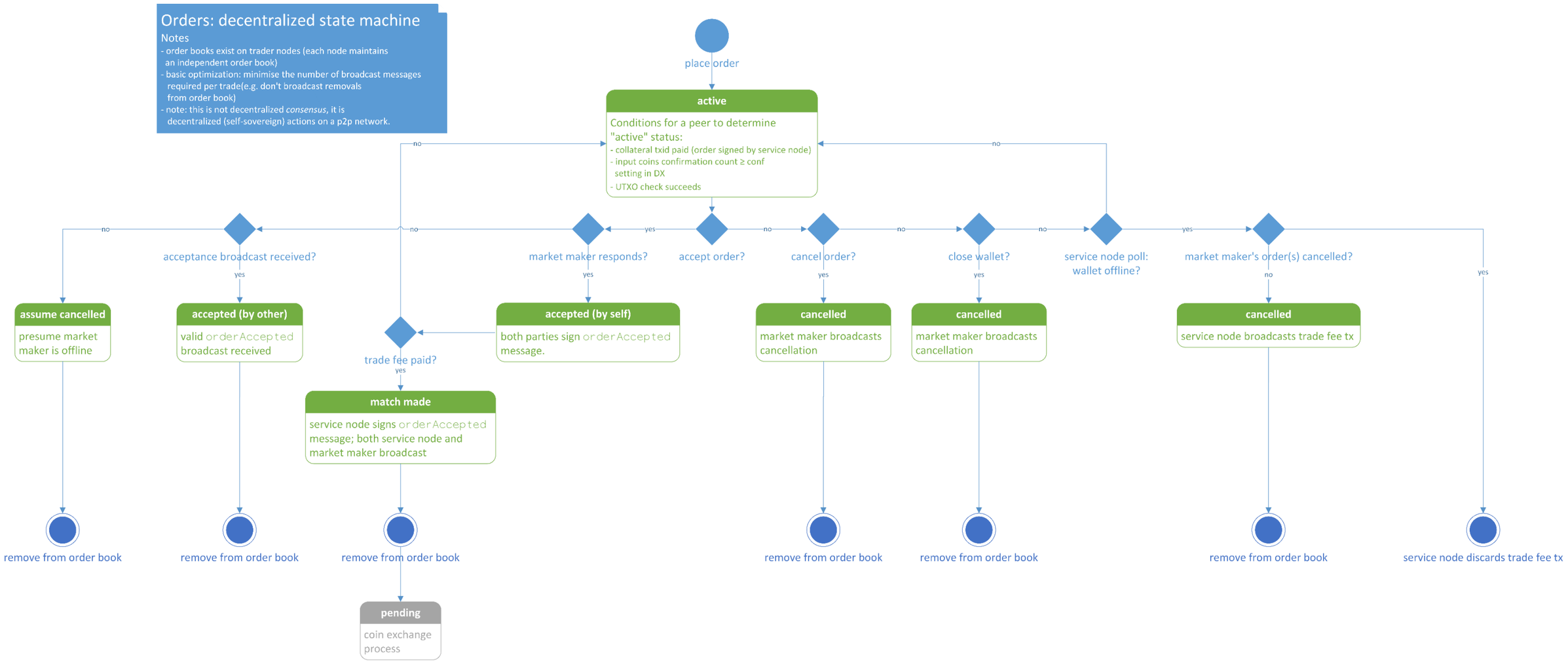


Figure 10
Decentralized state machine for orders

서비스 노드들의 역할 분담

블록넷의 명령 체계는 놀랍게도 단순한 양자간 거래가 아닌 삼자간 거래 시스템을 도입했습니다. 하지만 사용자들이 이 효과의 결과를 경험하게 될 때는 수수료를 부담하게 될 때입니다. 예를 들자면, 사용자가 주문 신청을 하기 전에 소액의 거래 수수료를 부담하도록 간단한 탈중앙화된 수수료 솔루션을 도입할 수도 있지만, 이 경우 주문이 취소되거나 구매자가 주문을 취소하는 경우 조차도 수수료를 부담하게 됩니다. 이 부당함을 방지하려면 제 삼자 체계를 도입하여 사용자가 거래가 이루어 지지 않거나 구매자가 주문을 취소한 경우에 수수료를 부담하지 않도록 하게 함과 동시에 주문을 올리기 전에 수수료를 부담하도록 하는 체계를 갖추어야 합니다. 이것은 현금화 신청, 자산의 현금화, 거래 상대방의 수수료 부담 유무 확인, 거래 수수료를 얻는데에 (1) 거래 수수료 내역을 악용화 하고자 공개하는데에 대한 유혹을 없애고 (2) 거래가 수락되지 않는 한 거래 수수료를 부당하게 갈취하지 않고자 이로 인해 얻어지는 인센티브를 나눈데에 따른 결과입니다. 다시 한번 강조하지만, 무엇보다 가장 중요한것은 자주 통치권으로서 이는 각각 개인 또는 단체의 인센티브들이 특정한 방법으로 나누어 지도록 조정되어 처리될 때 유지될 수 있습니다. 이것은 굉장히 복잡한 시스템이므로 간단화하여 이해를 돕기 위해서는 여러 부분으로 나뉘어져 한번에 하나씩만 다루어 보아야 합니다. 우선 현 상황에서는 구매자가 주문을 수락하기 전에 취소할 때 서비스 노드들이 부담하게 되는 거래 수수료에 대해 취할 수 있는 행동을 다룰 것 입니다. (주문 시스템에 속한 정확한 역할, 순서에 대해서는 아래에 위치한 **자세한 스케치 프로토콜**을 참조해 주세요)

서비스 노드들의 특별한 기능들

구매자가 거래를 수락하기 전에 취소할 때, 수락은 하되 부당한 거래 수수료는 방지하고자 (안티 스팸이나 안티 도스 비용) 서비스 노드들이 취할 수 있는 믿을 만한 몇몇의 새로운 기능들이 돕고자 추가 되었고 이는 아래와 같습니다.

1. 쉽게 구분 가능하며 제한된 횟수

거래 상대방이 안티 스팸이나 안티 도스에 대한 척도로 거래 수수료를 의지하고 있는 관계로 수수료가 부담되었지는 여부는 쉽게 구분할 수 있게 되어야 합니다. 이를 가능하게 하려면 서비스 노드에 의해 서명된 주문들과 (주문 수락 메세지들도) 다른 노드들이 서명한 것들을 구분할 수 있는 기능이 꼭 필요합니다. 이를 가능하게 하기 위해 본사는 서비스 노드들이 5000 블록 (BLOCK)을 필수적으로 보유하기를 요구합니다. 이렇게 할 경우, 모든 사용자들은 5000 블록 (BLOCK) UTXOS를 블록체인에서 찾아 쉽게 서비스 노드 목록을 고를 수 있습니다. 만약 한 주소가 5000 BLOCK을 보유하고 주문의 서명을 인증하면, 서비스 노드에 의해 서명된 것입니다.

2. 사기 행위에 대한 비싼 댓가

서비스 노드들은 블록 보상 (Block Rewards)와 거래 수수료를 얻기 위해서는 최소한 1000 블록 (BLOCK)을 보유 해야만 합니다. 만약 서비스 노드들이 사용자가 주문을 합버적으로 취소했을 때에 수수료를 공개화 하는 사기 행위를 할 경우, 거래자는 네트워크에 서비스 노드가 부정행위를 했다는 블랙 리스트 신청을 할 수 있습니다. 서비스 노드가 블랙 리스트에서 지워지기 위해서는 BLOCK이 새 주소로 옮겨가야 하며, 서비스 노드는 1000 BLOCK을 기다리는 동안 매우 많은 양의 거래 수수료와 블록 보상을 잃게 될 것입니다.

3. 사기 행위로 얻을 수 있는 이익 방지

사기 행위를 함으로서 많은 것을 잃게 되는 것과는 별도로, 서비스 노드는 위법적으로 거래 수수료를 소비함으로서 직접적으로건 간접적으로건 수익을 창출할 수 없습니다. 왜냐하면 모든 거래 수수료는 예측할 수 없는 확률로 다음 위닝 스테이커 (winning staker) 에게 보상되기 때문입니다. 이로 인해 서비스 노드들은

사기 행위로서 얻을 수 있는 수익이 없으므로, 동기 부여가 이루어 지지 않습니다.

4. 블록넷과 상호 운용되는 가상화폐들과 토큰들에 대한 보조

주문과 주문 수락 메세지에 대한 입증을 위해서, 서비스 노드들은 주문을 감당할 수 있는 코인이나 자본이 있는지를 입증해야 합니다. 이를 위해서 블록넷과 상호 운용되는 각각의 블록 체인 노드 지갑 (node wallets)을 유지하기를 요구합니다. 이 요구사항은 SPV와 라이트 노드들 (light nodes)들이 필요한 데에 서비스 노드들이 메세지와 거래 내역을 전달하고자 갖추어야 합니다.

5. 부당한 내부거래 방지

서비스 노드를 소유하고 있는 사람이 어떤 특정 거래자 (예를 들자면 자신이 소유한 거래 노드) 에게 특혜를 주고자 서명 또는 주문 수락 메세지를 연기한다면, 어떤 사람 이라도 다른 서비스 노드가 제공하는 동일한 서비스의 주문에 서명할 수 있으므로 서비스 노드가 특정인에게 특혜를 제공하는 것은 가능하지 않습니다.

위의 예에 따른 결과로, 거래자들은 (a) 서비스 노드들의 증언을 믿을 "좋은 이유" 가 있으며, (b) 만약 서비스 노드의 불 공정한 행위로 손해가 발생 했을 때, 손해 본 거래 수수료에 상충 또는 그 이상 가는 피해를 서비스 노드에게 가할 수 있는 능력이 부여되며, (c) 위에서 살펴 보았 듯, 주문 과정에서 거래자들이 잠재적으로 노출되는 낮은 위험성과 높은 확실성을 얻고자 하는데에 따른 심각한 실적 피해는 주문들에 대한 높은 확실성을 보증하지 않습니다.

주문 시스템 프로토콜

앞에서 언급한 탈 중앙화된 주문 예약에 관한 특성과 현실이 맞는다고 가정한다면, 아래에 쓰여질 프로토콜 스케치는 이것의 자연스러운 솔루션입니다. 아래에 제시된 솔루션은 현재 진행형으로 블록넷에 의해 적극적으로 연구되고 있으므로 변화가 있을 수 있음을 참조해 주십시요.

1) 만든이가 거래 수수료를 준비합니다
a) 만든이가 xLTC 를 yBTC 로 사기를 원합니다
b) 만든이가 tx 비용 (BLOCK 으로 지불 가능)을 계산합니다: y* 0.05%/가격 (BLOCK)
i) 참조: 블록의 가격은 주문이 들어가는 그 순간에 시장에서 구매하는 평균 블록 가격입니다.
ii) 참조: 블록은 주문이 들어가기 이전에 이미 구매 되어야 하며 (거래 속도를 위해서), 예: DX 엡을 시작할 때 – 다만, 엡의 블록 소유량이 예를 들어 1 블록 이하로 내려갈 때만 적용되며, 과정 (a)에서 언급 되었듯 간단히 소비되는 블록의 양을 계산할 수 있습니다.
c) 만든이가 tx 스팸비용을 만들되 공개화 하지는 않으며, 사기성 주문을 방지하기 위해 거래를 만든이에게 거래 수수료가 부담됩니다:
i) 블록 tx
ii) 추가적인 0.05%의 거래 수수료 네트워크 비용
iii) 만든이의 주소로써의 결과물
2) 만든이가 주문을 올립니다
a) 만든이가 xLTC 를 yBTC 로 구매 하기 위해 주문을 만듭니다. Fields:
i) y 의 가치
ii) x 의 가치
iii) 주문거래를 위한 BTC 주소
iv) 코인을 받기위한 LTC 주소
v) 자세한 만든이의 엑스칫 정보 (주소, 공개키)
vi) [다른 유용한 정보: 유통기한 등등]
vii) tx 스팸 비용의 txid

b) 만든이가 주문과 tx 스팸비용을 엑스칫을 통해서 서비스 노드에게 보냅니다.
c) 서비스 노드가 주문에 대한 비용을 인증합니다
i) tx 스팸비용 of txid 는 주문의 tx 스팸비용 txid field 와 동일합니다.
ii) Tx 스팸비용 네트워크 비용은 y 의 0.05% 입니다.
(1) 참조: 서비스 드는 블록의 가격을 반드시 DX 에 확인하여 정확한 비용을 계산해야 합니다. 실시간으로 변동할 수 있으므로, 정확한 비용의 15% 범위 내로 보유하고 있기를 권장합니다.
iii) tx 스팸비용 블록 주소는 비용을 지불하기에 충분한 블록을 보유합니다.
iv) 멤풀 (mempool)에 속한 어떤 txs 도 같은 주소의 블록을 소비할 수 없습니다.
d) 서비스 노드가 주문에 서명합니다.
e) 서비스 노드와 만든이 둘 다 주문과 서명을 공개화 합니다.
f) 서비스 노드는 메모리에 속한 tx 스팸비용을 갖고 있되 당장 공개화 하지 않습니다.
3) 구매자가 거래 수수료를 준비합니다.
a) 구매자가 xLTC 로 yBTC 를 사기를 원합니다.
i) 참조: UX 관점에서 볼때, 구매자는 시장가 또는 특정 제한가로 다른 수량을 구매 할 확률이 높으므로, 양측의 요구에 매치되는 프로토콜로 전량 또는 부분 수량이 거래되는 시나리오를 가정합니다.
b) 구매자가 tx 비용을 계산합니다 (블록으로 지불 가능): x * 0.2% / 블록 가격
i) 참조: 블록 가격은 거래 채결 당시 블록 시장 평균 가격입니다.
ii) 참조: 블록은 거래 이행 이전에 미리 보유하고 있어야 합니다 (매끄러운 속도 진행을 위해서) 예시: DX 엡 실행 이전 – 예를 들어 1 블록 이하로 보유 블록이 떨어질 경우, 위에 언급된 과정 (a) 를 통해 간단히 소비되는 블록의 양을 계싼합니다.
c) 구매자가 txDOS 수수료를 만들되 아직 공개화 하지는 않습니다.
i) 블록 tx 을
ii) 정확한 0.2%의 거래 수수료 네트워크 비용으로
iii) 구매자의 주소처럼 결과물을 만듭니다.
4) 구매자가 주문을 수락합니다.
a) 구매자가 주문 수락 메세지를 엑스칫을 통해 만든 이에게 보냅니다. Fields:
i) 주문의 LTC 자본 주소
ii) 코인을 받게되는 BTC 주소
iii) tx DOS 수수료의 txid
iv) BTC 주소를 위해 개인열쇠를 통한 서명하기
b) 만든이가 수락 메세지를 입증합니다.
i) 만든이의 BTC 주소에 만든이의 개인열쇠에 대답한 인증에 서명하기
ii) BTC 주소에 충분한 잔금여부 확인
iii) 어떠한 멤풀 (mempool)에 속한 txs 도 BTC 주소에서 소비할 수 없습니다.
(1) 신뢰 참조: 만든이가 수락 메세지를 입증할 수 있다고 하더라도, tx DOS 수수료가 서비스 노드에 의해 입증되기 전까지는 구매자가 스왑을 무료로 DOS 할 수 있기 때문에 이 이상 거래가 진행되어서는 안됩니다.
c) 만든이가 주문 수락 메세지에 서명합니다.
d) 서비스 노드가 주문 수락 메세지를 입증합니다:
(1) 신뢰 참조: 만든이는 서비스 노드가 하기 이전에 수락 메세지를 반드시 입증해야 하거나, 그렇지 않다면 서비스 노드는 (a) 거래 상대가 찾아지기 이전에 특정 가격에 상대가 구매하려고 하는 의사를 사전에 알게 되거나 (b) 누구든 수락 메세지를 다른이에게 보내는데 입증할 수 있는 이점을 얻거나 (c) 수락 메세지를 임의의 기준을 정하여 막거나 걸러낼 수 있습니다.
ii) tx DOS 수수료의 txid가 수락 메세지 tx DOS 수수료 txid field 와 동일합니다.
iii) tx DOS 수수료 네트워크 비용은 x 의 0.2% 입니다.

(1) 참조: 서비스 노드는 정확한 비용을 계산하기 위해서 블록의 가격을 DX 에서 확인해야 하며, 실시간 가격 조정을 대비하여 정확한 가격의 15% 정도의 유동성을 고려합니다.
iv) tx DOS 수수료 블록 주소는 비용을 감당할 수 있는 충분한 양의 블록을 소유합니다.
v) 멤풀 (mempool) 에 속한 어떠한 txs 도 같은 블록 주소에서 소비할 수 없습니다.
e) 서비스 노드는 수락 메세지에 서명합니다.
f) 서비스 노드와 구매자 양 측다 수락 메세지를 공개화 합니다.
g) 각각의 거래자의 주문 예약 메세지를 분석하여 만든이와 서비스 노드 양 측다 서명함에 따라 주문 현황이 “거래 이전” 에서 “거래 완료”로 바뀌고 주문이 예약 리스트에서 사라집니다.
5) 베일-인 (bail-in) tx 설정으로 진행됩니다.
a) 아토믹 거래 프로토콜에서 언급 되었 듯 진행 됩니다.

거래 수수료 내역을 공개화 하기 위한 조건

아래와 같은 상황에는 서비스 노드가 거래 수수료 내역을 공개 할 수 없습니다:
- 주문 유통기한이 지난 경우
- 아무도 거래를 수락하지 않았는데 지불하는 사람이 엡을 닫은 경우
- 거래가 수락되기 이전에 주문을 취소한 경우 (과정 4f 참조)
- 거래 상대가 베일-인 (bail-in) 거래 내역을 공개화하는데 실패할 경우

주문 매칭 시스템

블록넷은 탈 중앙화된 시스템을 위하여 (a) 기존의 주문 형태의 거래 (시장가, 제한가 등등)을 기본적인 자산 소비형태의 이벤트로 변환하였으며 (b) 일정 가격에 일정량의 한가지 종류의 코인이 인정량의 다른 한가지의 코인과 매칭 되도록 하였습니다. 위에서 소개된, 양 측이 각각 스스로 구매자 또는 만든이로서의 역할을 수행하고자 위에서 소개된 탈 중앙화된 주문 형태의 기계를 사용할때, 주문 매칭은 만든이로부터 자산의 유동성을 소비하는 것을 구매자가 요청하는 것을 포함하며, 만약 제한된 주문의 경우에는 정해진 최소한의 제한선 보다 적은 수의 주문 존재 여부가 거래자의 만든이 또는 구매자로서의 역할을 결정합니다.

시장 주문의 습성은 다음과 같습니다: 예약되어 있는 주문들을 소비하고, 가장 좋은 가격의 주문부터 일차적으로 거래되며, 시장 주문이 완전히 소비되기 까지 그 다음으로 좋은 가격 순으로 거래가 진행됩니다. 만약 시장 주문이 예약 되어 있던 모든 주문들을 거래 했음에도 불구하고도 아직 주문했던 양을 다 완료하지 못할 경우에는 거래되지 않은 남은 주문을 취소합니다.

제한 주문의 습성은 다음과 같습니다: 만약 팔고자 하는 주문의 가격이 더 낮을 경우 (또는 사고자 하는 주문의 가격이 더 높을 경우), 주문 예약 리스트에 있는 제일 높은 (또는 낮은) 순으로 거래가 진행됩니다.

UTXO 를 근본으로 한 가상 화폐 환전에서의 문제를 최소화 하기위해서 (기다림을 최소화하기 위해서는) 엑스브리지는 자동적으로 거래 지갑 (trading wallets)의 코인을 나누어진 주소로 소액 또는 제한된 금액으로 분할하며 이는 거래 반대측 과의 혼동을 최소화합니다. 추가적으로, 최소한의 거래 크기는 각 주소에 부과되는 금액의 양과 일치하여 이로서 악용적인 금액 변화를 방지합니다.

거래 내역 서비스

다른 코인들 간에 거래 내역은 투자 관련 전문 분석을 목적으로 한 차트 제작에 필수적인 도구이며, 이는 많은 투자자들에게 시장에 대한 전반적 이해를 도움으로서 더 나은 투자 결정을 내릴 수 있도록 합니다. 거래 내역 분석 차트의 가장 중요한 부분은 진실됨 이며, 만약 자료가 거짓을 바탕으로 제작되었다면 이를 토대로 특정 투자자가 다른 투자자를 상대로 한 거래에서 엄청난 이점을 얻을 수 있기 때문입니다. 그러므로, 거래 내역은 블록넷 서비스의 일 부분으로서 모든 투자자들에게 공정하고 동등하게 제공 되어 "신뢰성 여부가 필요없는" 정보 서비스가 되어야 할 것 입니다.

솔루션은 대표적인 아이디어를 내세우고자 세세한 기계적 솔루션임을 거부하고 간단함을 추구하여 이상적인 방향을 제시했습니다. 완성화된 솔루션 제품은 최대한 간단 명료하고 (거래 내역 데이터를 아토믹 스웝 atomic swap 내역에 내포하지 않음으로서), 대신에 예를 들자면 방탄화 (bulletproofs)와 같이 세련된 zero-knowledge proof scheme을 적용하였습니다.
"신뢰가 필요없는" 데이터 세트는 (a) 신뢰할 수 있는 거래 내역 데이터를 저장 할 수 있는 도구이자 (b) 신뢰할 수 있는 저장된 거래 내역을 불러올 수 있는 도구 이여야 합니다. 솔루션이란 다음과 같습니다.

거래 내역 블록체인이 생성되어 다른 블록체인들과 거래된 내역을 적합한 노드들이 공통된 거래 내역 데이터로 완수할 수 있어야 합니다. 보통의 데이터는 다음의 요소들을 내포합니다:

- 코인 A
- 코인 B
- 코인 A 의 양
- 코인 B 의 양
- 코인 A 대 코인 B 의 가격 비율
- 첫번째 베일-인 tx 가 소모된 시간

완수되는 데이터는 소비자가 데이터를 다양한 형태로 불러내는 데 충분하여야 합니다. 트레이드뷰 차트 (TradingView Charts)를 예로 들자면, 아래와 같은 데이터들이 요구됩니다:

- 봉 (candle)의 기간
- 봉 (candle)의 시작 시간
- 장이 열릴때의 가격
- 장이 끝날때의 가격
- 최고가
- 최저가
- 등등등

데이터 완수하기

거래 데이터를 완수하려면 거래 내역 블록체인을 보유한 노드들이 반드시 "데이터 점검하기"를 요청해야 합니다.

- 코인 A
- 코인 B
- 체인 A 에 관한 소비 베일인 거래의 txid
- 체인 B 에 관한 소비 베일인 거래의 txid (만약 없다면 빈칸으로 체크)
- 시장 생성을 위한 거래 수수료 소비 내역의 txid
- 시장 테이커를 위한 거래 수수료 소비 내역의 txid
- 모든 내역의 타임 스템프

- “데이터 점검하기”가 요청된 내역의 타임 스템프

노드에 의해 요청된 데이터 점검하기는 차후 네트워크에 의해 거래에 활용되는 블록체인 코인을 찾아보는 확인과정을 거친후 블록체인 코인을 위한 점검 결과가 공식화 됩니다. 노드들은 주어진 거래를 처음으로 검증하여 요청한 노드를 구별하여 네트워크에서 반복적으로 같은 형태의 활동이 수행됨을 방지하며, 처음 요청한 노드가 아닌 다른 노드들에 의해서 검증 및 요청된 데이터를 제거합니다.

데이터 복구 방법

거래 내역 데이터를 복구하는 데에는 다양한 방법이 존재합니다. 거래하는 사람들은 아래와 같은 방법들을 사용할 수 있습니다:

- 거래 내역 블록체인은 다운로드 하여 무료로 데이터를 복구 할 수 있습니다.
- 로컬 메모리에 이루어진 모든 거래 내역을 저장할 수 있습니다. 이를 위해서는 블록 DX 가 지속적으로 실행되고 있어야 합니다. (실행시, 차트를 실시간으로 업데이트 해야만 유용할 것 입니다)
- 비용을 지불한 후, 거래 내역 체인에 관여된 노드에게서 거래 내역을 요청 할 수 있습니다.
  특정 코인의 경우
  특정 시간 구간

거래 내역 데이터의 제공

거래 내역을 거래자에게 제공하기 위해서는, 거래 내역 블록체인 노드들은 아래의 정보를 반드시 공개 해야만 합니다:

- 특정 거래자가 특정 시간 구간에 거래한 코인 A, 코인 B 와 거래 수수료에 관한 모든 txids 해쉬
- 모든 노드들의 주소

이 데이터를 토대로 특정 거래자는 많은 노드들이 제공한 거래 내역 블록체인 데이터의 신뢰성의 “simple zero-knowledge proof” (위에 언급 참조) 을 구축하며, 제공된 해쉬들의 동일성을 검사할 수 있습니다. 만약 동일성 결과가 긍정적 이라면, 노드들이 서로를 무조건 적으로 신뢰해야 할 이유가 없음에 따라 악용될 데이터의 가능성의 폭이 크게 줄어 듬으로, 이를 토대로 하여 데이터의 신뢰성을 나름 보장 받을 수 있습니다. 만약 거래자가 데이터의 더 확실한 신뢰성을 보장받기를 원한다면, 다른 노드들로 부터 거래 내역을 제공받거나 스스로 블록체인을 다운로드할 수 있습니다. 노드들은 각자 서로 거래자들에게 제공 해야하는 책임을 확인할 수 있고 블록 체인에서 확인될 수 있는 불공정한 행동의 증거 공개적으로 서로에게 제출할 수 있는 권한을 가짐으로써 불법 행위를 통하여 불 공정한 행동을 하는 노드를 견제, 신고할 수 있습니다.

만약 거래자가 거래 내역을 제공할 노드의 정보에 만족할 경우, 그 노드는 거래자에 의해 해쉬 제공자로 선택되어 아래와 같은 아토믹 스왑을 시작할 수 있습니다:

- 오로지 소비만 가능한 베일 인 거래
- 노드가 제공한 주소에 한해 사용가능한 개인용 열쇠와
- 제공된 해쉬에 국한하여 반응하는 거래 내역 데이터
- (다르게 표현하자면, 아토믹 스왑에서 비밀 역할을 수행하는 거래 내역 데이터)

이와 같이, 만약 거래 내역 노드가 베일인 거래 내역을 소비한다면, 이는 거래 내역 데이터를 공개하며, 거래자는 이를 제공받습니다. 이와 동시에, 거래 내역 데이터는 거래자가 지불하지 않을경우 공개되지 않습니다.

현재 (그리고 간단한) 기술은 아래와 같은 가치를 갖고 있습니다:

- 요청된 데이터셋의 크기는 거래 형태에 속하는 비밀의 최대 길이에 제한됩니다. 거래 내역 노드들은 거래자들이 장기간에 걸친 거래 데이터를 원할 경우 적어도 하나 이상의 요청을 필수화함 으로서 수익을 낼 수 있습니다.
- 데이터셋 당 지불해야하는 수수료는 거래량에 따라 매 순간 조절되며, 이는 요구되는 시간당 더 큰 용량이 주어진 최대 크기의 데이터셋에 요구되는 시간을 줄어들게 합니다.
- 거래 내역 데이터에 미미한 불확실성이 의도적으로 포함되며 이는 요청된 거래 내역 데이터가 만약 다른 거래자들에 의해 가로채 져서 거래 내역 노드가 이를 공개화 하는것을 방지하기 위함입니다. 왜냐하면 데이터 셋이 거래를 묶거나 시간 구간을 포함하지 않음으로서, 가로채진 데이터가 유용하게 사용되지 않고 만약 사용하고자 한다면 이는 매우 비싸고 복잡할 것이기 때문입니다.
- 큰 불확실성을 포함하는 거래 내역 데이터가 엑스칫을 통해서 암호화되어 보내지며, 아토믹 스왑에 포함된 비밀이 데이터 암호화를 푸는 열쇠 역할을 수행합니다. 하지만 이를 위해서는 이 스케치에서 언급된 zero-knowledge proof 보다 더 세련된 것이 필요합니다. (위를 참조하세요).

레지스트리 서비스

위에서 언급된 거래 내역 서비스는 보통의 경우 인터 체인 서비스의 실행 가능한 레지스트리 서비스를 제공하기 위해 나타납니다. 직감적으로, 코인을 위한 거래가 아닌 디지털 상품을 위한 거래에서도 블록 체인 라우팅 (Blockchain Routing)의 결과와 찾기 단계를 바뀌지 않고 유지됩니다. 이와 별도로 거래 내역 노드들은 추가적으로 블록체인 거래 기록에서 가장 최근에 나타나는 체인아이디를 걸러내어 이 체인아이디 결과물 목록들과 서비스 아이디에 연관된 것들을 함께 묶습니다. 이후 이 목록은 거래 내역 대신에 전달되어 차후 실행되는 섹션 프로토콜에서 사용됩니다.

프로젝트의 단계

1. 단일화된 클라이언트/노드

- 블록체인 라우터
- 엑스쳇 프로토콜
- 서비스 현금화 방법
- 거래 수수료 등분 방법

2. 탈 중앙화된 dapp 교환

- 프론트엔드 UI
- 시장, 제한가, 요구가 주문
- 주문 예약
- 주문 내역
- 사용자의 예약된 주문
- 트레이딩뷰 차트 연동
- 각각 유저들의 어카운트 API 에 부여된 자격 사용
- 셋업 위저드: 자동화된 지갑 API 와 차트 API 배열
- 리스크 관리 (확인 가능한 숫자)
- 주문 예약 거르기
- 유저가 주문을 더 빠르게 할 수 있게 함
- 주문 변화 다루기:
- 허가된 주문; 주문 변화가 취소됨
- 변화된 주문은 x 분 동안 소비가 가능하지 않습니다.
- 이후 적합한 리스크 계층으로 들어갑니다.
- 주문이 속하는 리스크 계층은 자동적으로 코인의 나이를 업데이트 합니다.

제 2단계

1. 엑스브리지 p2p 를 모듈화 합니다.

- 블록체인 라우터 모듈
- 엑스쳇 모듈
- 코인 거래 모듈
- 탈 중앙화된 교환 클라이언트

2. 모든 모듈화된 요소들을 위한 API

3. 교환 프로토콜을 보조하기 위한 데이터 페이로드

4. 교환 프로토콜과 엑스쳇 간 이동가능한 프로토컬을 통한 쉬운 상호운용성 (사용자의 Dapp 을 통한 조절)

제 3단계

1. 더 많은 주문 형태를 위한 보조: 트레일링 스톱 (trailing stop), OCO
2. 앱을 닫은 이후에도 주문을 유지할 수 있는 보조성 (주문이 블록체인에 속합니다)

제 4단계

1. 프로토콜 증진: 스왑을 위한 파생시장 (p2p margin lending)
2. 프로토콜 증진: 포괄적인 파생시장들

기술 설명서

더 쉬운 기술 유지와 하나뿐인 진실성을 내포한 낮은 등급의 문서화된 주문을 위해서, 이 섹션은 GitHub 섹션으로 옮겨졌습니다.

메세지 순서들

https://github.com/BlocknetDX/blocknet-docs 를 참조해 주세요.

API 참고 목록

https://github.com/BlocknetDX/BlockDX/blob/master/doc/dx/dxpi.md 를 참조해 주세요.

사용하기- 케이스들

이미 실존하지 않는 생태계의 구축물들을 상상하는 것은 꽤나 어렵습니다. “이것은 무엇을 위한것인가?” 는 가장 흔한 디자인의 관점에 맞추어진 질문이며, 이에 적절한 해답은 “토큰 경제 생태계로 인해 이익을 얻는 모든 것” 이라고 대 부분의 경우 대답할 수 있습니다. 덜 추상적인 관점의 해답은 아래에 언급된 블록넷의 짧은 목록들에 의해 대답될 수 있습니다.

1. 탈 중앙화된 교환

탈 중앙화된 가상화폐를 근본으로 한 경제 생태계는 블록넷의 주요 서비스이며, 이를 토대로 다른 서비스들을 현금화 할 수 있습니다.
이것은 쉽게 사용 가능한 dapp UI 내에 속하며, 탈 중앙화된 거래 기술을 정말로 필요로 하는 가상화폐 커뮤니티는 블록넷의 첫 번째 소비자 상품이기도 합니다.
중앙화된 가상화폐 교환은 1/16의 비트코인이 사기, 해킹, 실수, 도둑질 등으로 훔쳐지는 결과를 낳았습니다. 그러므로, 사용 가능한 탈 중앙화된 교환은 더 안전하고 확실한 코인과 토큰의 교환을 이끌어 내는 역할을 수행할 것 입니다.

2. 블록체인 라우터

인터 체인 트레픽은 목표로 한 장소로 정확히 인도되기 위해서 반드시 라우터를 사용해야 하므로, 블록체인 라우터는 블록넷의 또 다른 주요 서비스입니다. 이 말을 다르게 말하자면 이 분야는 소비 가능한 가치있는 서비스이며, 어떠한 노드라도 이 서비스를 전달하거나 소비하는 인터 체인 서비스를 요구합니다. 블록넷의 초기 라우터인 엑스브리지는 현재 무료로 서비스되고 있으며, 향후에도 이와 같이 운영될 수도 있습니다.

3. 인터 체인 메세지 보내기

체팅 엡으로 사용될 것 인지 데이터 전송에 사용될 지 상관 없이 인터 체인 메세지 보내기는 토크 경제 생태계에 대체 불가능한 필수 서비스입니다. 탈 중앙화된 교환과 블록체인 라우팅과 함께, 이 두가지 요소들은 블록넷의 주요 서비스이며, “엑스쳇”이라고 불리웁니다. 이 것은 처음부터 끝까지 전부 암호화 되어, 개인에서 개인으로 전달되므로 디지털 상품 및 메세지 전달에 매우 높은 안전성을 보장할 수 있습니다. 이는 현재 무료 서비스로서, (현재에는) 엑스브리지와 함께 페키지화 되어 블록체인 라우터 서비스를 책임지고 있습니다.

4. 모바일 엡 멀티 체인 활용하기

작은 발자취를 남기는 모바일 엡은 대 다수의 경우 단 하나의 SPV 노드와 기존에 사용하던 블록체인 토큰을 사용합니다. 이는 아래와 같이 표현 가능합니다,

- 코인이 아닌 서비스를 소비할 것이며,
- 다양하게 소비되는 블록체인 서비스들은 블록넷의 요소들을 활용하며,
- 엡이 서비스를 요청할 때, 서비스는 “비밀”을 만들고 이는 동시에 디지털 상품의 암호를 푸는 열쇠로서 역할하며,
- 서비스는 엡을 사용 가능하게 하는 데이터를 보내며, 이는 상품이 진품임을 보증하는 zero-knowledge proof 를 만들고자 사용되며,
- 이는 아토믹 스왑에서 베일-인 거래 내역을 만들며,
- 서비스가 원할 경우 차후 거래에서 다른 코인으로 베일인 거래 내역을 소비할 수 있으며,
- 따라서 엡은 비밀을 받아서 서비스를 소비할 수 있습니다.

5. 완벽에 가까운 코인 믹서

Z Cash, Z Coin 또는 Monero 같은 사유 재산 형태의 화폐는 엑스브리지를 통해서 연동되며, 어떠한 화폐라도 자동화된 거래로 사유 재산 형태의 화폐와 고유 화폐를 반복적으로 교환 할 수 있습니다. 탈 중앙화된 교환이 유저의 데이터를 통한 제 3자의 신뢰성 여부를 요구 하지 않음에 따라 아토믹 스왑이 위조성 여부에 따른 위험에 노출되어 있지 않기 때문에, 거의 완벽에 가까운 다양한 화폐가 섞일 수 있는 개인 서비스가 완성 될 수 있습니다.

6. 탈 중앙화된 마켓 시장 엡

마켓 시장 엡은 보통의 경우 아래와 같은 서비스들을 요구합니다. (a) 소비자들의 입소문과 정보, (b) 지불 과정 및 방법, (c) 이미지 저장하기, (d) 상품 리스트하기 입니다. 소규모 서비스 제공자들의 구조는 위에 언급된 이유들을 따르기를 권하며, 이로 인해 다양한 종류의 블록 체인들을 활용할 수 있는 장점을 갖게 됩니다. 그러므로, 하나의 체인은 암호화된 소비자의 정보를 저장할 수 있게되며 (목록 13을 참조해 주세요), 엑스 브리지를 통해서 어떠한 형태의 가상화폐도 수용할 수 있게되며, 서버에 이미지를 저장 가능하며, 상품 리스트 만들기와 UI 요소들을 제 3의 체인을 사용하고 in-wallet code를 통하여 사용할 수 있습니다. 이로 인한 결과는 측정 가능하여, 서비스들을 버그를 수정하거나, 업그레이드 하거나, 더 나아가 아예 덮어씌우는 것도 쉽게 가능합니다.

7. 이더리움 (Ethereum) 스마트 계약을 위한 원료 교환인 (Fuel-converter)

탈 중앙화된 거래를 사용하여, 어떠한 이더리움 (Ethereum)의 계약이라도 다른 코인들의 “가스”에 의해 충전될 수 있습니다.

8. 진정한 탈 중앙화된 안정적인 코인

안정적인 코인이라 하기 위해서는 탈 중앙화된 교환에 관련한 거래 기록들이 체인 내에게 유지되어야 합니다. 이와 같이, 참된 데이터세트를 입증하기 위한 목적으로 코인이 주조되었는지 또는 채취되었는지 (또는 얼려졌는지 녹여졌는지) 여부를 확인 할 수 있습니다.

9. 개인 소유의 ID 와 개인 정보 관리

개인 정보 서비스에 관련된 암호화된 개인 데이터는 블록체인에 내장되어 기록되며, 사용자의 허락 여부에 따라 폐지 가능한 시스템이 구축되어야 합니다. 사용자들은 이로 인해 개인 정보에 대한 스스로의 권리를 얻게 됩니다. 이 관점에서 본다면, 이 기술은 한 개인의 블록체인을 사용자 로그인을 요구하는 아무 웹사이트나 엡에 연동하거나, 자발적으로 자신의 정보를 소규모의 보상을 주는 광고회에서 판매 하거나, 여권이나 신원조회 시스템을 위해 사용될 수 있습니다. 비트네이션 (Bitnation) 이나 마이크로 소프트의 코코 프레임 워크 (Microsoft’s Coco Framework) 현재 이 방면에서 미래를 보장받는 위치에 있는 신규 기술들입니다.

10.서플라이 체인 2.0 솔루션

블록넷 구조는 “서플라이 체인 2.0” 의 뼈대를 이루는데 적합한 역할을 수행합니다. 많은 단체들은 다른 블록체인들의 상호 수행성을 필요로 하며, 블록넷의 서비스를 찾게 될 수 있습니다. 멀티체인 엡들은 이로 인해 Bill of Lading 과 같이 데이터들을 보내거나 Bill of Material 과 같이 상품 제작 데이터 보유 현황, 또는 financial dat등의 여부와는 상관없이 다양한 체인들에게서 데이터를 읽을 수 있습니다. 다양한 자료들과 데이터를 비교하여, 회사들이 위조 청구서나 위조 자격증을 사용하여 중간 업자들에게서 부당한 이윤을 취하는 것을 제한 할 수 있습니다.

11.IoT 건축구조

몇몇의 지속되는IoT 보안관련 문제는 블록체인 기술을 이용하여 해결 가능하며, 이 후에 블록넷에 상주하는 몇 천가지의 다른 블록 체인들간에 상호 운용이 가능합니다. 이는 다양한 주요 주조기회를 많은 이들에게 제공합니다: 예를 들자면, SPV 지갑을 이용하여 몇몇의 체인들을 하나의 거래로 배칭하는 것이 가능합니다.

이렇게 흐른 데이터는 토큰화될 수 있으며, 노드들은 회사의 거대 데이터 (big data) 패턴 구축에 관여하여 인센티브를 받을 수 있습니다.

12.In-App 광고 서비스

모바일 앱은 블록넷의 서비스로서 사용자들에게 광고를 제공하고 토큰을 얻어 수익을 창출할 수 있습니다. 앱은 무료로 사용자들에게 제공될 수 있지만, 이렇게 얻어진 토큰들은 앱을 위한 인터 체인 서비스를 강화하거나 현금화 하여 서비스 제공자들에게 수익을 안겨줄 수 있습니다.

13.탈 중앙화된 P2P 저장 솔루션

Storj와 같이 블록체인은 근본으로 한 저장 솔루션은 인터 체인 서비스 전달을 통해 사용자의 수를 토대로 하여 서비스 제공자들에게 수익을 안겨줄 수 있습니다.

14.허락이 필요없는 ICO 플렛폼

탈 중앙화된 교환을 통해 누구건 토큰을 판매 할 수 있으며, 이는 다른 허가가 필요 없는 행위입니다.

15.예산관리 분배를 위한 사업을 위한 도구

암호화된 프로젝트는 보통의 경우 전체 시장에 의해 예산이 정해지는 거대 대중 토대 사업의 예(ICO)를 겨냥하여 발매됩니다. 하지만, 실제적인 회사 잔고는 가상 화폐의 가격 변동에 따라 실시간으로 변합니다. 블록넷을 사용하여, 개발자들은 다양한 체인들 사이에 퍼져있는 계좌들과 토큰들은 손 쉽게 관리할 수 있습니다. 더 나아가, 스마트 거래를 사용한다면, 다른 코인들을 통해 이루어지는 투자나 지출을 관리하고, 프로젝트에 해당하는 사업 계획은 암호화되어 완벽한 투명성을 유지하며 자동화 되어 계약이 체결될 수 있습니다.

16.회사들 간의 ERP, CRM, PLS 시스템 연동

블록넷의 간단한 API 토대 연동하기는 ORACLE이나 SAP과 같이 직접적 또는 간접적으로 컨소시엄 타입과 사유 블록체인간에 상호 실행성을 가능하게 합니다.

17.가치있는 인터넷을 위한 사회 구축망

블록넷의 인터 체인 사회 구축망은 시간이 지남에 따라 더욱 향상되어 진실되며, 투명하고, 공정성이 유지되는 “가치의 인터넷” 을 만드는 역할을 할 것입니다. 시간이 지남에 따라, 회사를 대표하는 총괄자들이 블록체인을 토대로 하여 거래하게 됨에 따라, 블록체인들은 해당 네트워크에서 진정한 가치를 관리하는 시스템으로 자리잡게 될 것입니다. 이는 전체 경제 시스템의 가치를 잇고 더 나은 미래로 도약하는 힘있는 주요 기술로써 자리잡음하게 할 것입니다