OmiseGo
Decentralized Exchange and Payments Platform
탈중앙화된 교환과 결제 플랫폼

Joseph Poon & OmniseGO 팀
joseph@lightning.network omg@omise.co

번역: Blockchain Partners Korea

2017 년 06 월 17 일

초록

OmiseGo 는 탈중앙화된 거래, 유동성 공급자 제도, 정보교환 메세징 네트워크, 그리고 자산이 뒷받침 되는 블록체인 게이트웨이를 구축하고 있습니다. Omisego 는 어떤 한 개인이나 단체에 소유되지 않습니다. OmiseGo 는 참여하는 모든 사람들의 활동을 보증해주는 개방된 분산 네트워크입니다. OmiseGo 는 지분증명 (POS) 방식의 블록체인을 통해 참여자간의 시장 활동을 실행할 수 있는 프로토콜 토큰 메커니즘을 사용합니다. 이러한 고성능 분산 네트워크는 명목담보 (fiat-backed) 발행자들로부터 as-set classes 들간의 거래를 가능하게 하여 온전히 탈중앙화된 블록체인 토큰들 (ERC-20 스타일 토큰들과 기존 암호화화폐간들) 과 교환을 시행할 수 있게 합니다. 다른 대부분의 탈중앙화된 거래 플렛폼들과는 달리 이러한 방식을 통해 다른 블록체인과 여러 블록체인들간에 신뢰할 수 있는 게이트웨이 토큰 없이도 분산된 거래를 할 수 있게 됩니다. 이로서 시장은 분산을 최소화시키고 시장의 투명성을 높여 보증을 할 수 있게 될 수 있습니다. 스마트 컨트렉트 (계약서), 주문서 매칭시 정확한 시장 행동을 시행시키는 프로토콜 토큰의 사용, 이더리움과 연결된 외부적으로 강화된 새로운 청산 (clearinghouse) 활동, 그리고 과거 거래 데이터를 사용하기 위해 이더리움 스마트 컨트렉트를 사용하는 약속에 의해 달성할 수 있습니다.

1. OmniseGo 소개와 문제 정의

블록체인의 주된 역할은 네트워크에 참여하는 사람들이 다자간 동의를 할 때 발생하는 조정 문제를 해결하는 것입니다. 투명성, 보증 그리고 집행을 보장함으로서 전에는 불가능했던 다자간의 합의를 가능하게 할 수 있습니다. 모든 사람들에게 운영의 투명성이 보장되고 상당한 노력없이는 매커니즘이 변경되지 않을거라는 확신이 생길 때 참여자들은 더 조직화할 의지가 생기게 됩니다. 참여자들은 어떤 한 개인이나 단체가 본인에게 사업 방식이나 정보의 비대칭성을 악용하여 비용을 착취하기 더 힘들어지게 된다는 것에 더 큰 보장을 얻을 수 있습니다. 다른 말로 하자면, 어떤 비즈니스 과정이나 매커니즘이 다른 한 개인이나 단체에게 소속되지 않을 때, 사람들은 그 시스템을 더 사용하고 싶어합니다.

결제기관과 게이트웨이, 그리고 국가기관들 사이에서는 근본적인 조정 문제가 있습니다. 예를 들어, 어떤 은행 고객이 다른 네트워크의 상인에게 결제를 한다는 가정을 해보겠습니다. 전통적으로 각 국가기관과 결제 네트워크들간에 호환될 수 있는 결제 시스템을 구축하는기 위해서는 상당한 노력을 필요로 했습니다. 이는 보통 중앙 당사자의 청산이나 당방/타방 계정을 통한 메세징 네트워크를 구축한 거래를 관리할 수 있는 청산소를 만듬으로서 가능하였습니다. 예시로 Fedwire, CHIPS, SWIFT, 고객 카드결제 네트워크, NSCC/DTCC, OCC, 그리고 ACH 같은 곳이 있습니다. 이러한 네트워크들은 지역별/나라별 결제, 해외 결제, 신용, 지분/자산간 거래, 그리고 다른 파생상품등의 처리와 같은 각기 다른 역할과 기능들이 있습니다. 이러한 중앙화 네트워크는 그 네트워크 소유자가 임의적으로 매커니즘을 변경하는것을 가능하게 하여 정보비용 및 실사, 그리고 모든 참여자들의 계약적인 실행 등의 이유로 상당한 거래 비용을 발생시켰습니다.

저희는 새로운 플랫폼을 사용한 혁신적인 디지털 결제 (Venmo 와 Alipay 같은) 시장이 현재 폭팔적으로 증가하고 있다고 믿습니다. 이러한 네트워크는 다른 네트워크로 전환할 때 간접비용이 많이 들기 때문에 서로 다른 네트워크로 전환하는 것에 대해 상당한 반감이 들 수 있습니다. 계약 당사자들은 당방/타방 계정이 서로간에 맞춤형 계약을 요구하기 때문에 중앙 청산기관을 사용하기 꺼려합니다. 더 큰 네트워크들은 자신들의 네트워크의 미치는 영향을 보호하려는 성향이 크지만, 저희는 전자지갑 서비스들이 다자간 참여자들 사이에서 조정역할을 잘 할 수 있다고 기대합니다. 이러한 중간급 참여자들은 네트워크 내에서 사용하기에 충분한 네트워크 영향을 받기 위해서 가치이동을 할 수 있게 됩니다. 이러한 구조는 네트워크 효과가 네트워크 자체에 새겨질 수 있게 할 수 있고, 새로생기는 전자지갑 참여자들에게 높은 네트워크 사용성을 즉시 제공할 수 있게 됩니다.

블록체인을 통해 전 세계 사업의 흐름은 한개의 중앙화된 기업이었던 시스템에서 탈중앙화된 컴퓨팅 네트워크로 바뀐 사회가 될 수 있습니다 [1][2] OmiseGO (OMG) 는 시장 유동성의 탈중앙화, 주문기록 매칭과 처리, 청산관리, 그리고 확장의 고도화가 가능한 결제

네트워크로서 새로 등장하고 있는 전자지갑 결제 네트워크의 결제문제를 해결하기 위해 나온 솔루션입니다.

기존 한개의 기업에게 집중되어있던 사업 과정을 바꾸어 탈중앙화되고 고성능이며 공개된 네트워크에서 전자지갑간의 거래를 가능하게 할 수 있습니다.

2. 디자인적 접근

최종적으로 필요한 것은 자산담보 (fiat-backed) 가치를 가지고 있는 전자지갑의 탈중앙화된 플랫폼 매커니즘을 구축하는 것입니다. 전자지갑의 자산화된 (fiat) 토큰을 통해 최대 효율을 낼 수 있는 교환/중개 수단으로 탈중앙화화되고 공개된 이더리움 [3][4] 체인 (또는 다른 탈중앙화된 암호화화폐) 을 사용할 수 있게 될 것입니다. 저희는 탈중앙화된 암호화화폐들 사이에서 위 사실이 여러 전자지갑 플랫폼의 장터로 역할을 하기에 훨씬 더 많은 활동과 가치를 부여할 수 있을 거라고 믿습니다.

탈중앙화된 네트워크에서 전자지갑간의 교환이 가능하게 하는것이 주된 역할이듯, OmiseGO 블록체인 원장 (ledger) 은 각 전자지갑 서비스 (또는 어떤 사용자/노드들) 마다 일정수준의 자금을 가지고 있어야 합니다. 이 원장 (ledger) 은 다양한 자산/상품들에 대해 자산을 보유할 수 있어야 합니다. 하지만 단순히 원장 (ledger) 을 가지고 있는것은 교환이 성사되는데 부족합니다. 매커니즘 자체 또한 이런 자산/상품을 거래할 수 있도록 허용해 주어야 합니다.

교환이 가능하기 위해서는 공개된 공공 시장에서 한 주문이 여러곳에 들어가야 합니다. 그러기 위해서는 탈중앙화된 주문기록 (orderbook) 과 거래 엔진을 필요로 합니다. 거래 엔진은 OMG 블록체인 내에 구축이 되고, 주문은 공개되어 매칭된 주문이 충분한 인증 횟수를 충족했을 때 각 블록의 일부로서 거래가 수행됩니다. 이렇게 진행된 거래는 특정 한 당사자나 기관의 탈중앙화된 거래방식데 의존되지 않고 거래 당사자의 전자지갑 플랫폼 사이에서 직접 환산이 됩니다.

하지만 전자지갑간의 직접적인 토큰거래는 막대한 볼륨을 필요로하기 때문에 바람직하지 않을 수 있습니다. 암호화폐를 어떤 한곳에 선호도를 가지지 않고 유동시장에 사용하는것이 필요할 수 있습니다. 이더리움을 스마트 컨트렉트 [5] 에 연결시킴으로서 (또는 비트코인같은 코인을 청산소에 연결시킴으로서),이더를 OMG 체인의 활동에 고정시켜 이더나 다른 암호화화폐를 전자지갑에서 작업이 일어나며 유동적 시장을 생성할 수 있습니다. 아주 작은 스프레드 (spreads) 만을 요구하는 활동은 전자지갑 토큰의 교환을 통합하게 됩니다. 하지만, 프로그램적인 판단과 관련된 조정/신용의 이유로 탈중앙화된 토큰을 사용할 강력한 동기부여가 생깁니다. 전자지갑 토큰은 필요하다면 다른 전자지갑 토큰을 통해 교환할 수도

있습니다. 하지만 스마트 컨트렉트 활동의 단기간적인 교환 비율의 움직임에 영향을 주지 않는 활동은 대부분 이더리움으로 이루어질 것입니다 (e.g. HTLC 청산소, 유동성 제공, 그리고 OMG 체인 실행) 암호화화폐를 전자지갑 플랫폼의 보조기능으로 사용함으로서 전자지갑간의 교환활동을 안정적으로 실행할 수 있는 플랫폼이 될 수 있습니다.

이는 묶인 자금에 유동성이 더 필요하게끔 만들고 작은 금액의 교환 활동을 할 때 OmiseGO 의 탈중앙화된 거래방식은 적합하지 않을 수 있습니다 (e.g. 예를들어 높은 볼륨의 마이크로페이먼트)

두개의 각기 다른 전자지갑끼리의 결제가 탈중앙화된 거래소에서 거래가 되어야 하는것만은 아닙니다. 전자지갑은 다른 전자지갑의 토큰 일부를 본인 지갑에 남겨두어 자주 보내지는 곳으로의 송금을 미리 준비할거라는 예상치가 있습니다. 경량 네트워크 (Lightning Network) [6] 와 같은 구축은 전자지갑이 빠른 결제를 촉진시키기 위해 금액을 들고있을 때는 체인 밖에서 결제가 이루어질수 있게 합니다. 이렇게 실행이 된다면 비트코인 [7] 과 이더리움 [8] 을 통한 결제를 전자지갑 잔고를 확인하기 위해 OMG 체인에 쉽게 저장할 수 있게 됩니다.

결론적으로 OmiseGO 블록체인 구조는 온전히 믿을 수 있는 구조 안에서 전자지갑간의 교환이 가능해지고, 탈장앙화된 거래를 지원하며 이더리움과 같은 암호화화폐의 매칭, 주문기록, 그리고 청산소 기능을 할 수 있습니다.

2.1. 탈중앙화된 유동성 허브 (Hub) 채널들

이러한 구축방식은 탈중앙화된 유동성 풀 (pool) 이 생성될 수 있게 하여 비트코인같은 (또한 어떤 면에서는 이더리움까지) 다양한 암호와화폐의 결제 채널로서 사용될 수 있게 합니다.

블록체인의 개별 토큰 결제는 노드들 (nodes) 을 검증/채굴할때 (POW) 연산 부담을 줄이기 위해 기존 체인에 영향을 주지 않는 기존 블록체인 활동을 배분해 줄 필요가 있습니다. 그래서 경량 네트워크 활동 (또는 채널을 사용해 비슷한 구조를 성립) 을 하는것이 필요합니다. 하지만 경량 네트워크는 네트워크 영향과 자금에 대한 상당한 압박을 받고 있고 단일 신용 기관에 중앙화된 유동성 풀 (pool) 이 들어가는것을 막는게 좋습니다. 탈중앙화된 청산소를 사용하는 것과 같은 매커니즘으로 저희는 한명의 개인/기관에 소유되지 않고 더 복잡한 스마트 컨트렉트 (e.g. 이더리움, ERC-20 호환 가능한 토큰등) 경량 네트워크 허브를 만들 수 있게 됩니다. 간단한 스마트 컨트렉트를 사용하는 화폐는 네트워크 (ex. 비트코인 네트워크) 상의 어떤 노드로도 OMG 체인 풀을 통해 어떠한 참여자에게로라도 연결시켜 주는 게이트웨이 역할을 할 수 있게 됩니다. 이렇게 되면 OmiseGO 체인은 탈중앙화 방식을 장려하면서 많은 활성화된 체인 (on-chain) 활동을 수용할 수 있게 합니다.

저희는 유동성 중앙화된 기존 네트워크의 효과가 탈중앙화 기반의 체인과 결정론/알려진 합의 규칙에 의해 완화될 수 있다고 생각합니다.

특히 이더리움의 경우에는 (그리고 다른 모든 기능이 있는 스마트 컨트렉트 블록체인들), 모든 참여자들이 이더리움 스마트 컨트렉트에 채널을 설정해 한개의 풀 (pool) 을 운영할 수 있게 합니다. OMG 의 체인을 보면 참여자들의 잔고를 확인할 수 있습니다. 이는 참가자들이 이 네트워크에 OMG 체인의 합의된 법칙에 따라 유동성을 공급할 수 있게 합니다. 이러한 자금은 결국 OMG 체인에서 어떠한 유동적 활동을 위해 사용될 수 있습니다.

3. 블록체인의 개요와 매커니즘에 대해서

위에 얘기한 매커니즘을 실행하기 위해서는 엄청난 상태량을 포함한 많은 활동이 필요하지만 현재 이더리움 메인 채널에서 이러한 많은 활동이 일어나기에는 적합하지 않습니다. 하지만 이러한 네트워크 구조는 개방된 이더리움 체인과 OMG 체인에 의해 제공된 컨트렉트를 실행하는 연결고리가 될 수 있을 것입니다.

저희는 대부분 이더리움 기반으로 된, 그리고 다른 블록체인과 연결되어 여러 토큰과 자산들과의 거래가 가능해지는 블록체인을 만들고 있습니다. 한개의 체인만을 본다면, OMG 체인 자체의 활동에 계약 상태가 보증이 되는 확장이 가능한 형태의 블록체인을 만들고 있다고 할 수 있습니다. 다른 체인에서의 활동은 OMG 체인에서의 비트코인 릴레이 (Relay) [9]와 비슷한 (하지만 구축방법은 다른) 다른 체인 내부의 커밋 증명을 활용하여 이더리움에 커밋하는 방법으로 연결할 수 있습니다. OMG 체인은 모든 참여자들의 유효성을 검증합니다 (다른 체인에서의 활동을 포함한). 다른말로 OMG 토큰은 계산활동과 실행의 역할을 제공하고 있습니다. 토큰 자체는 블록체인내의 활동에 대한 담보역할을 하여, 부적절한 활동을 할 시에 OMG 체인 내에서 그 토큰/담보는 소멸됩니다. 시행이 중요시되는 체인을 만듬으로서 저희는 고성능 활동에 최적화된 합의 규칙으로 이루어진 시스템을 만들 수 있습니다.

이러한 디자인은 빠른 실행과 청산이 가능하게 합니다. 미래에 있을 반복작업은 OMG 체인의 분산을 포함할 수 있지만, 최초 반복작업은 블록의 번식을 위해 높은 처리량을 포함할 것입니다.

OMG 토큰을 구매하는것은 이 체인의 합의된 규칙에 따른 해당 블록체인을 검증할 수 있는 권한을 사는 것입니다. 이 네트워크를 사용할 때 드는 결제, 교환, 거래, 그리고 청산소 사용 (이 외 관련 비용) 등과 같은 거래 비용은 컨트렉트 상태를 연결시켜주는 인증 담당자에게 지급됩니다.

이 토큰은 사용자들에게 인증을 해줄 의무와 그 비용에 대해 네트워크상에서 받게되는 수수료로 가치가 생기게 됩니다. 토큰은 저비용 공격을 막고 이러한 네트워크를 시행하기 위해서는 가치가 있어야 합니다.

제 삼자에게 인증 권한을 허용하는것이 저희의 나아갈 방향일 수도 있고 재위임이 필요하기 전에 한정된 양은 잘릴 수도 있습니다. (보안 모델링을 위한 정확한 매커니즘은 아직 미정입니다)

이는 고성능 시스템으로 디자인될 것이기 때문에 증명연결 (linked-via-proof) 방식의 블록체인 구조 설계가 필요합니다. 저희는 이 시스템이 매우 높은 볼륨의 거래량을 소화할 수 있을거라고 예상하고 마지막 단계만 이더리움을 통해 이루어질 것입니다. 청산기능과 결제는 OmiseGO 블록체인 내에서 처리됩니다. POS (Proof-of-stake) 네트워크를 통해 합의 규칙이 실행될 것입니다. 이 네트워크의 합의 규칙의 일부로, 모든 OMG (Omise GO) 인증은 이더리움 네트워크에서도 병렬적 인증이 필요합니다. 이더리움과 ERC-20 호환 가능한 보증과 인출같은 기능들은 근 미래에 이더리움에서 사용할 BLS 서명 제도 (또는 대안으로 Schnorr) 를 사용할 것이라고 추정됩니다. 암호화화폐 세계에서 이러한 토큰들은 통제되지 않고 스마트 컨트렉트에 귀속됩니다. (Ripple 같이 검증된 게이트웨이를 필요로 하는 다른 거래 플랫폼과는 다르게) 또한 중앙화된 인증기관에 의존하지 않습니다. (e.g. Ripple)

OMG 블록체인은 이더리움 체인에서 일어나는 주문을 연결해주고 주문의 실행을 관리합니다. OMG 에서의 활동은 원조 이더리움 스마트 컨트렉트를 통해 이더리움 체인에서 실행될 수 있다는 검증 역할을 합니다. 비트코인이나 비트코인과 유사한 시스템에서 저희는 라이트닝 네트워크의 청산소 네트워크를 통한 거래를 가능하게 합니다.

이 블록체인은 커밋된 증명(committed proofs)을 통해 이 네트워크에서의 활동을 실행합니다. 이더리움 네트워크만큼 활성화되지는 않지만, 풀 노드 (full-node) 인증을 하지 않아도 OMG 체인을 통해 거의 즉각적인 청산과 결제가 이루어질 수 있게 합니다. 블록체인 재배열을 허용하지 않는 노드들에 대해서는 이후에 일부 인증만 할 예정입니다; SPA 인증방식의 재배열을 지원하는 블록체인은 보안의 이유로 이 네트워크에서 허용이 안될 예정입니다.

보안 특징에 대한 더 자세한 합의 매커니즘에 대한 설명은 다가오는 2017 년 여름에 Exonumia Labs Inc. (현재 진행중) 의 Joseph Poon 에 의해 제공될 예정입니다. 이 문서는 (그리고 후에 시행되어 사용될 OmiseGO) 미래에 생길 여러 오픈 소스 블록체인 토큰 프로토골 프로젝트에 유용하게 쓰일 수 있을 것입니다. 또한 분배된 데이터 처리, 그리고 교환식 블록체인의 금전적 활동에 대해 다가올 체인 구조에도 좋은 구조를 만드는데 도움이 될 것입니다. 저희는 OmiseGO 와 분배된 거래방식이 전체 프로토콜 토큰 생태계에

생명력을 불어넣을 수 있는 기술과 기반의 기초가 될 수 있게 만들 수 있기를 바랍니다. OmiseGO 의 최초 버전은 텐더민트(Tendermint) 동의 방식을 사용할 수 있습니다.

3.1. 경량 클라이언트 검증 (Light Client Validation)

OmiseGO 가 많은 거래량을 소화할 수 있는 고성능 네트워크로 구축되어 있지만, 부분 인증을 하거나 외부 스마트 계약의 실행을 위해서는 경량 클라이언트 증명방식을 할 수 있어야 됩니다.

각 블록마다 머클 트리(merkle tree)의 커밋된 거래들과 최신 블록 상태에 커밋이 포함될 것입니다. 현재 상태를 알려면 최근 생성된 블록이나 그 사이에 생성된 아무 블록 중 어떤 노드를 다운받으면 됩니다.

최근 생성된 블록에는 최근 상태에 대한 트리 (tree) 가 들어있기 때문에 클라이언트에서는 전체 체인을 다운받지 않아도 최근 커밋 상태에 대해 볼 수 있게 됩니다. 이것은 재정렬과 hlating 공격을 반대하는 금전적 동기부여가 충분히 있기 때문에 가능합니다; OMG 체인은 결합된 증명을 통해 블록이 재정렬되는것에 강력하게 부동기부여를 하지만 블록 확인에 대한 확신을 하지 않습니다. SPV 비트코인 검증 실행방식과 유사하게 검열 위험성에 대해 풀 노트에게 주는 어느정도의 신뢰가 있습니다만; 커밋된 블룸 맵(bloom map)이 거래 볼륨을 고려했을때 탈중앙화된 거래소에 적합하다고하기 힘들다고 예상합니다. 경량 클라이언트는 풀 노드 (full node)의 일부 데이터의 일부 데이터나 다른 어떤 거래가 일어나기에 충분한 검증이 되었음을 보증해줄 수 있습니다. OMG 체인의 스마트 계약서의 구조상 클라이언트가 이더리움 체인에서도 활동을 검증하는것을 매우 권장합니다.

4. 전자지갑

OmiseGo 는 결제 기능을 제공합니다, 하지만 OmiseGo 의 전자지갑 결제 기능은 (EPP) 다른 전자지갑 제공자들과 비교했을 때 앞선다고 말할 수 없습니다. 지갑 연동과 같은 경우 단순히 하나의 EPP 문제는 아니며 여러 다른 전자지갑 제공자 (EPP)들로부터 나오는 공통적인 문제라 생각됩니다. 그럼에도 불구하고 전자지갑들 사이에서의 거래는 필수이고 결제는 블록체인을 통해 이루어지게 됩니다. 그리고 바로 이 블록체인을 통해 전자지갑 제공자들은 OmiseGo 내에서 토큰을 발급할 수 있습니다. 이를 통해 토큰은 플랫폼 안에서 화폐나 로열티 포인트 등과 같은 자산으로 인정 받을 수 있습니다. OmiseGo 는 누구나 자산을 만들 수 있는 시스템이지만 발행 및 감사에 대한 책임은 사용자나 제공자들에게 있습니다. 이는 보안 키를 갖고 있는 발행 스크립트 (Script)를 생성함으로써 가능합니다. 또 다른 방법은 이더리움을 통해 ERO-20 토큰을 발급하여 스마트 컨트렉트 내부에서 잠근 장치를 한 후

이를 OmiseGo 에서 처리하는 것입니다. 이 방법은 이미 OmiseGo 에서 운영되고 있는 ERC-20 토근들과 (REP, GNT 등) 흡사한 접근입니다.

보편적으로 전자지갑 제공자들은 사용자들을 편의를 위해 그들을 대신하여 자금을 보관하고 있다고 알려져 있습니다. 이는 현재의 코인베이스나 많은 중앙 집권화 거래소들의 암호화 가상화폐 지갑들과 비슷합니다. 이를 통해 전자지갑 제공장들은 (EPP) 블록체인을 거치지 않고 그들의 자체 네트워크 안에서 수수료없이 거래를 할 수 있습니다. 하지만 OmiseGo 안에서는 EPP 에서 바로 출금하거나 발행된 토큰을 (화폐자산) 거래하는 것이 가능합니다 (단, EPP 계정에서 발생하지 않은 거래에 대해서는 수수료가 발생할 수 있습니다). 이는 즉 분산화 된 거래이며, 자체 네트워크 안에서 수수료 비용을 원치 않는 EPP 들의 욕구 또한 충족 시켜줍니다. EPP 는 다른 가상화폐 지갑과 비슷한 중앙 집권화 소프트웨어를 제공할 수 있으며 이를 통해 분배 시간을 단축할 수 있습니다. 또한 오직 네트워크를 통한 결제만 EPP 의 인프라를 통해 이루어 집니다. 3 자들도 향후에는 EPP 잔고를 보관할 수 있는 분산화 된 지갑을 생성할 수 있습니다.

블록체인의 일부분을 전자지갑 플랫폼으로 구축한다면, OMG 블록체인에서 분산화 된 화폐기반 토큰이나 프로토콜 토큰을 직접 거래 할 수 있습니다.

4.1 전자지갑의 규정

규정에 따라 발급자의 인증서가 필요한 토큰들의 거래는 제한 적일 수 있습니다. 전자지갑 제공자들은 (EPP) 인증서에 서명하기 전에 본인 인증 절차가 필요 할 수 있습니다. 제한 사항에는 인증된 보유자 거래 및 토큰 유동성 관리 등이 포함되어 있습니다 (계정당 거래 제한과 발행된 토큰의 최대 잔고 금액 제한). 제한 사항이 표기되지 않은 토큰이나 분산화 된 암호화 화폐 관해서는 해당 규정이 적용되지 않습니다. 발급된 토큰의 자격 및 규정에 관련한 사항들에 대해서 전자지갑 제공자들 (EPP)는 책임을 다해야 합니다.

5. 분산화 거래

전자지갑 플랫폼의 핵심 요소는 바로 분산화 된 거래입니다. 분산화 거래는 EPP 로부터 발행된 토큰뿐만이 아닌 분산화 된 가상화폐 간의 거래에도 적용됩니다.

분산화 거래는 토큰들의 가치가 다르고 거래 시 초래할 수 있는 위험과 비용이 다르기 때문에 전자지갑 간의 교환에 최적화 되어 있습니다. 전자지갑 A 와 B 는 동일하게 지원을 받더라도 다른 지갑임에는 분명합니다. 따라서 아주 작은 거래 차이가 있더라도 유동성 있는 시장 운영이 필요합니다.

분산화 거래는 매번 거래가 일어날 때 마다 일괄적으로 처리됩니다. 거래는 특정 블록 안에서 구매되거나 주문이 완료 될 때까지 열어 놓을 수 있습니다. 이러한 구성은 분산화 된 네트워크에서 더 높은 신뢰와 성능을 제공할 수 있습니다. 주문은 장부에 기록 되지만 처리 속도는 EMV 카드 단말기와 견줄 정도로 빠릅니다. 속도가 느린 거래의 경우, EPP 들은 빠른 속도의 지원을 원하는 다른 EPP 들의 잔고를 보관할 의무가 있으며 (마진율이 높을 수 있음) 이는 분산화 거래를 이용한 소량 또는 대량 구매를 통해 이루어 질 수 있습니다.

신속하게 많은 주문을 처리하는 것이 가장 좋겠지만 분산화 된 네트워크 안에서 이를 실행하기 위해서는 장벽들이 존재합니다. 같은 시점에서 주문이 발생되게 끔 하는 기능이 필요합니다. 한 개의 "엔진"에서 주문이 발생되지 않는다면, Sybil 공격이나 Single Party 만을 신뢰해야 하는 가능성이 생기게 됩니다. 만약 누군가가 주문을 하고 이에 대한 처리가 여러 곳에서 일어나게 된다면 거짓 주문이 발생할 수 있게 되고 쉽게 네트워크를 조정하거나 마치 자신이 실행하는 것처럼 조작할 수 있습니다. 이 네트워크의 목표는 가치가 높은 거래소 및 안정적인 플랫폼이 되는 것입니다. (높은 용량과 가치가 떨어지는 네트워크는 지양합니다)

신속하게 처리를 하는 다른 방법은 외부에 있는 중앙화 장소를 이용하는 것입니다, 하지만 이는 단독 개체에서만 신뢰를 쌓습니다. 거래 유동성이 (지급 중앙화 보다 훨씬 강화된) 점차 중앙화 되면서 현재의 가상화폐 거래소가 갖고 있는 신뢰 및 연결 문제들이 발생됩니다 (단, 통제는 받지 않습니다). 그러나 이 형태는 신뢰를 쌓은 단독 벤더 (Vendor)에서만의 거래를 원치 않는 사용자들이 겪고 있는 문제를 해결해 주지 않습니다. OmiseGo 의 분산화 거래 목적은 투명하고 누구나 인지 할 수 있는 처리 기능을 갖추는 것입니다. 우리는 신뢰가 있고 통제에서 자유로운 처리 기능이 분산화 된 엔진을 보안하는 방법이라 생각합니다. 그리고 OmiseGo 또한 다가올 미래에 이러한 플랫폼들을 지원할 것입니다. 발전된 분산화 거래는 스마트 컨트렉트를 분산화 오라클로 사용하는 자유로운 처리 환경에서의 장점을 지니고 있습니다.

이 분산화 거래는 주문이 POS 네트워크를 통해 전송되는 경우 고성능을 발휘하도록 설계 되었습니다. 자격을 갖춘 사용자가 블록을 통해 주문을 확인하면 해당 주문은 장부에 기록되게 됩니다. 일괄 시점의 장부는 해당 시점까지 처리되지 않은 모든 누적 주문의 집계입니다 (따라서 장부와 일치하는 주문들이 존재 합니다). 초기 구성의 주문은 투명성이 포함되지만 블라인드 주문이 발생할 경우 fauxcoin 과 같은 형태의 구축이 가능하고 더 이상 주문이 받아들여지지 않게 됩니다. 그리고 주문을 실행 한 사용자에게 블라인드 키가 주어지며 일정 시간이 지난 후 처리가 되게 됩니다. 최초의 버전은 완벽히 투명한 시스템을 사용할 것입니다 (일괄 처리 방식은 반대되는 행위를 일부 완화할 것입니다).

결과적으로 "단일 엔진" 즉 분산화 된 POS 거래를 통해 실행되는 투명성과 보장성을 갖춘 시스템이 탄생하게 됩니다.

5.1 이더리움 거래

OMG 는 최대한의 효율성과 보안을 위해 이더리움 블록체인의 풀노드(fullnode)에 관한 유효성 검사를 필요로 하고 있고 따라서 OMG 체인의 상태에 따라 자금 잠금 장치가 가능한 스마트 컨트렉트를 생성할 수 있습니다. 이러한 자금은 이제 담보로 잠겨져 있으며 자금의 움직임은 OMG 체인에 의해 실행됩니다. 주문이 실행되면 이더리움 블록체인에서 자금의 잠금을 해지할 수 있는 증거가 제공됩니다.

조만간 이더리움에서 Schor 또는 BLS 서명 방식이 가능할 수 있습니다. 이체는 OMG 체인의 실행을 추적하며 이더리움 체인으로 지불이 되기 전 일정 수준 이상의 승인을 필요로 합니다. OMG 체인의 실행은 이더리움 체인의 결제를 집행합니다. 대립적이지 않은 환경에서는 사용자가 증명 없이 바로 지불을 할 수 있는 (Lightning) 형태의 구현이 가능합니다. 또한 특정 블록의 수가 만들어진 후 결제에 대한 논란이 없을 경우에는 증명이나 계산이 필요 없게 됩니다. 지불한 금액이 OMG 체인에 명시된 바와 일치하지 않을 경우 누구든지 증거를 제시할 수 있으며 송금인의 잔액은 삭감됩니다. 이는 이더리움 블록체인에서의 계산 및 지속 시간의 효율성을 높일 수 있습니다.

OMG 체인의 형태는 이더리움, 이더리움 계열의 체인 및 스마트 컨트렉트를 담보로 하는 ERC-20 와 유사한 이더리움 기반 토큰들의 거래를 위한 것입니다.

5.2 다른 프로젝트와의 비교

거래는 금융의 본질적인 측면입니다. 따라서 암호화 화폐 거래소를 구축하는 다른 수많은 시도들이 있었던 사실은 결코 놀라운 일이 아닙니다.

폴로닉스와 (Poloniex) 같은 완벽한 통제에 의한 중앙 집권 암호화 화폐 거래소들은 높은 성능을 지니고 있는 반면, 단일 기관에 모든 신뢰 및 거래의 정당성을 의존해야 하는 문제가 있습니다.

리플과 (Ripple, XRP) 같은 네트워크는 합의에 도달하기 위해 신뢰를 쌓은 인증자에게만 의존하고 이는 변경 불가한 게임의 법칙입니다. 또한 리플의 거래 기능은 리플의 자체 플랫폼에서 발행된 자산에 의존하고 있습니다 (통제와 관련해 심각한 문제들이 있습니다). 분산화 된 거래소는 발행된 게이트웨이 없이는 비트코인이나 이더리움을 거래할 수 없습니다.

EVM 스마트 컨트렉트를 사용하는 많은 분산화 거래 플랫폼들은 체인상에서 직접 작업을 수행하거나 (오직 이더리움 네트워크 안에서 모든 것을 처리하고 브록체인 간의 작업은 허용하지 않습니다) 단일 엔진을 사용하지 않고 체인 밖에서 작업을 수행합니다. OMG

체인은 원천 암호화 화폐에 대한 통제를 받지 않고 체인간의 거래를 수행할 수 있도록 설계 되었습니다 (예: ETH-BTC).

새로운 네트워크들은 코스모스(Cosmos)와 같은 분산화 거래의 기능을 제공할 수 있습니다. 하지만 이러한 네트워크들은 아직 완전히 구현되지 않았으므로 평가나 비교를 하기에는 다소 이르다고 말할 수 있습니다.

5.3 비트코인 청산소 (Clearinghouse)

한편, 비트코인 및 비트코인 유사 시스템의 경우, BTC 와 다른 유사 블록체인의 거래 뿐만 아니라 청산소를 통해 외부에 담보된 자산을 사용할 수 있는 시스템을 만드는 것이 가능합니다.

기본적으로 이 구조는 비트코인 같은 블록체인들과 분산화된 거래가 이루어질 수 있도록 청산소가 OMG 체인에 의해 보증되고 실행되는 활동을 통해 오라클(Oracle)처럼 운영하도록 합니다. 이 시스템은 외부 거래 실행 엔진에 근거하여 신속한 분산화 거래 실행을 주도한 Tier Nolan 의 작업을 기반으로 하였습니다.

청산소는 비트코인 블록체인에서 결제가 발생하는 것을 보장하기 위해 사용됩니다. 우리는 비트코인 채굴자들이 외부 시스템을 공격하기 위해 합의된 내용에 적합하지 않으나 SPV 증명 방식에서는 유효한 블록을 생산함으로써 얻을 수 있는 적대적 보상의 발생을 방지하기 위해 SPV 증명 대신 청산소를 (Clearinghouse) 사용합니다 (개인이 소유한 블록체인을 공격하는 것은 큰 비용이 들지만 외부 시스템을 공격하는 것은 그렇지 않습니다).

비트코인 유사 시스템에서 OmiseGo 는 유동성 고정(예: 목격자 격리) 또는 투명한 주소에서만 사용할 수 있는 P2SH/BIP-66/CLTV/CSV 조합을 필요로 합니다.

현재로서는 비트코인으로 복합적인 형태의 계약 실행이 가능하지 않기 때문에 청산소가 필요합니다. 청산소는 역상(preimage)과 해쉬(Hash) 생성을 통해 비트코인 (또는 이 와 유사한 체인) 체인에서의 활동을 드러내는 데 책임이 있습니다. 해쉬는 청산소가 담당하고 있는 활동에 충실하며 밀접하게 관련되었습니다. 만약 부정확한 역상(preimage)을 보내거나 OMG 체인에 역상을 전송하는 것을 거부한다면 누구든지 부정행위의 증거로 제공할 수 있으며 청산소 잔액이 삭감 당할 수 있습니다.

청산소는 비트코인 측의 자금 뿐만 아니라 OMG 체인에 담보된 자금도 보유하고 있을 것을 필요로 한다는 점을 염두에 두시기 바랍니다. 담보된 금액은 자금이 청산되고 비트코인 쪽에서 안정화가 되기 전까지 지속될 것이기 때문에 이상적으로 극히 큰 금액의 자금을 필요로 하지 않습니다.

청산소는 라이트닝채널을 (초고속 채널) 운영하지만 채널 내 청산소 본인의 자금 외에도 OMG 체인에서 이동할 것으로 예상되는 다수의 ETH 형태의 자금까지 보유하고 있습니다. (예: 환율변동에 대한 책임을 지기 위해 그들이 담당하는 자금 순환의 3 배).

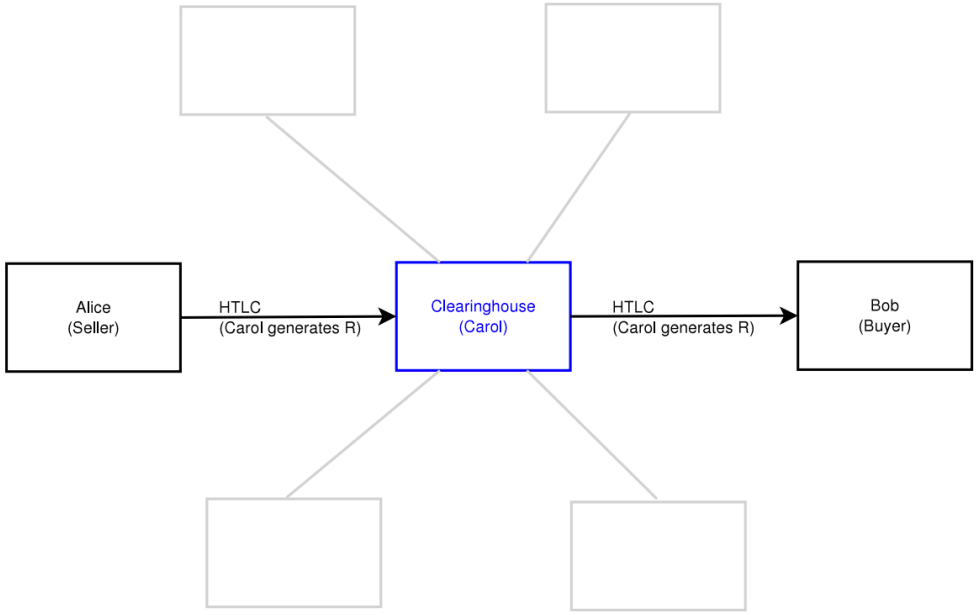

그림 1: Alice 와 Bob 은 비트코인 블록체인에서 Carol 이라는 청산소(Clearinghouse)와 라이트닝 네트워크 채널을 가지고 있습니다. 결제 역상 R 은 Carol 에 의해 생성되고 역상 전송은 OmiseGO 체인에서 보증된 커밋먼트(commitment)에 의해 진행됩니다.

Alice 는 비트코인을 팔기 원하고 Bob 은 비트코인을 사려고 하며 두 사람 모두 Carol the Clearinghouse(청산소)에 채널을 가지고 있다고 가정해봅시다. Alice, Bob, Carol the Clearinghouse 는 모두 OMG 체인을 사용하며, 모두의 동의 하에 Carol 을 청산 중개인으로 지정하였습니다. 양측이 모두 동의하고 거래 참여자 간 합의된 청산소를 통해서만 발생하는 경우, 다수의 청산소를 통해 이체 작업을 진행할 수 있다는 점을 참고하시기 바랍니다. Carol the Clearinghouse 는 OMG 체인 합의 규정과 스마트 컨트랙트에 의해 정해진 스마트 컨트랙트에 자금을 이더리움으로 보관합니다. Carol 은 자기 고유의 해쉬 H 서명이 완료된 증거를 제공합니다(이 시점에서는 Carol 본인만 알고 있는 역상 R 에 의해 생성됩니다). Carol 은 본인이 책임지고 있는 BTC 상응 값을 가진 해시 H 와 사인(signature)을 제공합니다. 이 해시 H 와 사인은 OMG 체인에서 증거로 사용될 수 있습니다. (Carol 이 불완전할 경우, 이더리움 스마트 컨태랙트도 증거로 사용될 수 있습니다).

Alice 가 비트코인을 팔고 원할 때, Carol 이 제공한 H 값이 전송됨에 따라 HTLC (Hash Time Lock Contract)를 지불합니다. 비슷한 방식으로 Bob 이 비트코인을 받기 원할 때도 Carol 이 제공한 H 값이 전송됨에 따라 HTLC 를 보냅니다.

이 H 값들은 OMG 체인에서 특정 사람들에 의해 구성되고 이제 이 자금은 분산화 거래를 가능하게 합니다.

OMG 분산화 거래에서 실제 거래가 실행될 때, (예. Alice 가 ETH 을 사기 위해 BTC 를 팔고 Bob 이 ETH 를 팔아서 BTC 를 사는 것) 이 거래는 바로 OMG 체인 내에서 청산됩니다. 이제 모두가 거래 실행에 대한 책임과 의무를 가지게 됩니다.

Carol 은 Alice 와 Bob 이 OMG 체인에서 거래를 실행할 때 발생하는 H 에 대한 R 역상을 전송할 의무가 있습니다. Bob 은 이 정보를 사용하여 비트코인 체인에서 자금을 인출할 수 있고 Carol 은 Alice 로 부터 자금을 받을 수 있는 권리를 가지게 되었습니다.

만약 Carol 이 정해진 시간 내에 OMG 체인에 R 역상을 전송하는 것을 거부할 경우, 그녀의 자금은 삭감되고 ETH 는 Alice 그리고/또는 Bob 에게 넘겨집니다. (Carol 에게는 환율 변동을 줄이기 위한 벌금과 잘못에 대한 불이익이 주어집니다.)

만약 Carol 이 R 값을 잘못 전송할 경우, 불특정 타인에 의해 OMG 체인에 증거가 제공될 수 있고 Carol 은 벌금을 물게 됩니다. 그리고 자금은 H 값과 함께 잠긴 청산소 거래 계약을 가지고 있는 당사자에게 주어집니다.

청산소가 Alice, Bob 과 같은 참가자와 직결되어 있어야 하는 것은 아니며 참가자들은 연결된 네트워크를 통해 지불할 수 있습니다. 그렇기 때문에 자금 효율성을 최대화 할 수 있습니다. 청산소는 모든 관련 활동에 있어 청산소를 사용할 때 마다 수수료를 청구할 수 있습니다. 청산소의 결제 실행 능력에 대한 믿음은 있지만 관련 활동에 있어서는 최소한의 신뢰만 존재한합니. (청산소의 활동은 OMG 체인에 담보되어 있기 때문).

추가로 이 시스템 구조는 외부와의 결합을 통한 신속한 HTLC 실행에 유리하며 분 단위의 놀랍도록 빠른 시간제한 만료의 지불방식을 구축하는 방법이 될 수 있습니다. 비트코인을 보관하기 위한 청산소는 필요하지 않으며 청산소에 의해 보증된 정보만 전달 받게 됩니다. 이 구조에 대한 자세한 설명은 별도의 문서에서 다루어질 예정입니다.

OMG 체인이 재배열(reogrgs)을 강도 높게 막기 때문에 가능한 것임을 기억하시기 바랍니다. 최종 결과는 비트코인 외부에서 분산화된 거래를 진행할 수 있는 능력입니다. 우리는 이 시스템이 새로운 구조라고 믿고 있습니다. 비트코인 네트워크에서 참가자들의 활동은 비트코인에서 경제적인 보상을 받으며 운영되는 청산소를 통해 외부의 분산화된 거래에 의해

실행됩니다. 외부 조건에 따라 진행된 역상 전달은 비트코인이 프로토콜 토큰 블록체인의 거래에서 비트코인이 사용될 수 있게 합니다

5.4 스마트 컨트렉트 데이터 피드 (Smart Contract Data Feed)

최근 거래의 가중 평균 가격은 (VWAP) OMG 블록체인에서 합의된 규칙으로서 주기적으로 계산되고 공개됩니다. 이는 외부 계약들이 거래 가격과 거래량의 Merkle-tree SPV 증명 방법을 이용할 수 있게끔 허락합니다. 이를 통해 스마트 컨테렉트 안에서의 더 나은 실행 가능성을 기대할 수 있습니다.

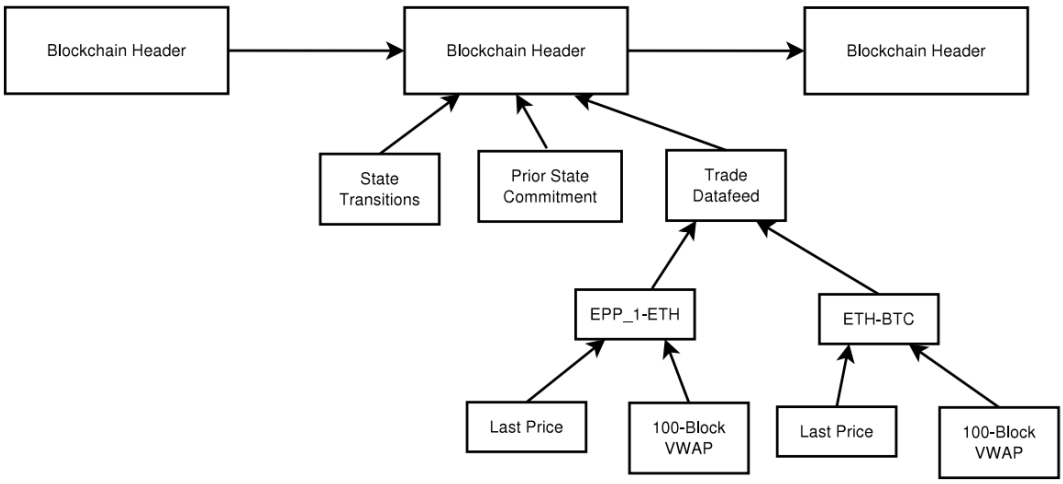

그림 2: 데이터 피드에 대한 주기적인 처리는 OmiseGo 의 블록체인에서 실행됩니다. 이는 블록체인 헤더 (header)의 머클 루트(merkle root)를 통해 외부 인증이 가능합니다. 거래 데이터 피드는 최근 거래 가격, 거래량, 그리고 여러 VWAP 조건들을 포함하고 있습니다.

모든 거래소의 핵심 기능은 주문을 관리하고 실행하는 것뿐만이 아닌 3 자 시스템의 체계를 갖는 것입니다. 이는 3 자 시스템이 해당 정보를 이용하고 사용자들이 단일 체계에서 활동 할 수 있도록 허락해 줍니다. 모든 스마트 컨트렉트는 거래 가격 매커니즘의 기본 사항입니다. 따라서, 해당 시스템에 접근성을 지니고 있다는 것은 거래소를 외부 컨트렉트에서 데이터 체계로서 이용하는 사용자들에게 더 큰 보장과 투명성을 허락한다는 의미입니다. 이를 통해 스마트 컨트렉트의 사용자들은 분산화 된 거래소에 접근 권한을 가질 수 있고 계약을 체결할 수 있습니다. 만약 사용자가 OmiseGo 체인의 가격 오라클 피드를 스마트 컨트렉트에 대한 기본 가격 정책으로 이용한다면 사용자는 OMG 체인에 주문을 함으로서 실행 가능성을 더 크게 높일 수 있습니다. 이로 인해 더 훌륭한 스마트 컨트렉트의 성향을 지닌 OMG 체인 네트워크의 효과가 생성됩니다.

6.라이트닝 (Lightning) 유동성 제공자

자본 유동성의 네트워크 효과를 둘러싼 중앙 집권화 압력은 근복적인 문제입니다. 많은 사람들은 라이트닝 네트워크가 초과 추가 이윤 추출이 (rent extraction) 가능한 소수의 노드들을 중앙화 시킬 수 있다는 잠재성에 대해 우려를 표하고 있습니다. 라이트닝 네트워크는 이러한 형태의 유동성을 갖춘 노드의 초과 추가 이윤 추출을 (rent extraction) 회피하도록 설계되었지만 사실 이렇게 잘 연결된 노드들은 큰 장점을 가지고 있습니다. 위에서 설명한 청산소와 유사하게 하나의 노드가 OMG 체인에서 실행을 보증할 수 있게끔 하는 매커니즘의 설계가 가능하며 이를 통해 OMG 체인은 훌륭한 유동성을 지닌 단일의 라이트닝 허브로서의 역할을 할 수 있습니다.

이더리움나 이더리움과 흡사한 채널들의 경우에는 스마트 컨트렉트에서 바로 실행할 수 있습니다. 비트코인 채널에서도 가능하지만 사용자의 실행은 OMG 체인의 ETH 담보에 의해 시행됩니다. 결제는 OMG 체인의 사용자에게 지불되고 그 밖의 실행들은 체인의 약관에 따라 처리 됩니다.

OMG 플랫폼이 완성되기 전에 이러한 시스템에 너무 많은 자본이 몰리는 것의 방지를 위한 제한이 필요합니다. 이는 청산소 및 분산화 거래의 자금 가용성에 대해 거대한 유동성의 기회를 마련할 것입니다.

7.OmiseGo 토큰에 대한 경제적 시사점

거래 수수료는 OmiseGo 체인에서 발생됩니다. 사용자들은 블록체인에서 발생하는 실행에 대한 유효성을 검사한 대가로 수입을 가져갑니다. 결제 및 거래 수수료는 네트워크에서의 실행과 정당한 활동에 대한 보상을 위해 사용됩니다. 담보에는 비용이 청구 됩니다, 예) 청산소처럼 해당 네트워크에서 타인을 대신해 담보를 해주는 경우 수수료르 부과할 수 있습니다.

8. 한계점

이런 네트워크는 개방된 네트워크입니다. 결국 이 네트워크가 개방되기 위해서는 비록 맹목적인 약정/입찰이 되더라도 정확한 거래 활동이 탈중앙화된 거래 방식으로 진행되는 것이 필요합니다. SNARKS 를 통해 새로운 암호화화폐를 만들 수 있지만 높은 거래량을 소화하는 거래 네트워크를 만들기 위해서는 현재 방식은 너무 느릴 뿐더러 많은 자원의 소비가 필요합니다. 저희는 현재 성능과 스피드를 최적화시키고 있습니다. 이 네트워크는

태생적으로 익명의 네트워크입니다 (발급이 된 토큰들은 AML/KYC 구조를 가질 수 있습니다)

다른 체인의 SPV 인증은 재배열을 인정하지 않는 블록체인에 사용하기에 불안정하다고 생각이 됩니다. 재배열을 허용하는 체인들은 풀 노드 인증이나 HTLC-청산소 구축이 필요합니다. 이더리움이 더욱 신뢰할 수 있고 finality (현재 지분증명 (Proof-of Stake) 연구)를 기반으로 할 것이라는 전제조건을 갖고 있습니다.

이러한 기술들은 새롭고 아직 검증되지 않은 기술입니다. 저희는 악조건인 환경이지만 최대한의 보안 구축을 하는데 최선을 다하고 있습니다. 이 매커니즘에 실제 사람이 사용하는 행동패턴에 맞게 보안 모델을 구축하고 있습니다. 체인들간에 상호작용할 때 에러가 나면 되돌리기 힘들기 때문에 탈중앙화된 블록체인간의 활동시 발생하는 이 체인에서 한번의 거래를 위해 최소한의 필요조건들만을 구축해야 합니다. 최초 버전은 이러한 악조건 환경에서 견고할 수 있습니다. 그리고 저희는 소프트웨어가 시간이 지나면서 여러 공격 (특히 DOS (Denial of Service) 공격) 에 대응할 수 있게 발전될때까지 최소 거래를 추천드립니다. 이렇게 구축한 디자인이 실제로 어떻게 적용될지는 알기 힘듭니다.

이 네트워크에 참여하는 사람들이 장기적으로 어떤 가치를 얻을 수 있을지는 아직은 불명확합니다. 경쟁자들의 영향이 있을 수도 있고 아직 기술적으로 탐구되고 있는 분야이기에 보증자로서 참여하는 것에 대한 어떤 (금전적인) 보증은 없을수도 있습니다.

승인이 난 이체 (지급 전) 의 총합은 검증된 총 금액의 합보다는 낮아야만 합니다. 추가 금액을 결합하는것은 가능하지만 토큰들의 총 가치가 충분히 높다면 그럴 필요가 없을 수 있습니다. 시스템 고유의 실행 매커니즘을 위해 추가 모델링은 필요합니다.

이 비전을 실행하는것은 최종적으로 OmniseGo 팀의 역할입니다. OmniseGo 팀이 아닌 저자들은 원칙적으로는 기술적인 가이드라인이나 아키텍처만을 제공할 책임이 있습니다.

9. 결론

전자지갑 플렛폼이 유명세를 타면서 폐쇄적으로 갇혀있는 형태의 네트워크는 문제가 되고 있습니다. 이러한 상황은 여러종류의 토큰들이 탈중앙화된 네트워크에서 서로 교환되고 다른 가상화폐들과 교잡호환성을 할 수 있는 특이한 기회를 만들어내고 있습니다.

탈중앙화되고 교환 가능한 네트워크를 만들기 위해서는 단순히 결제와 발행된 토큰들이 잘 교환되는 블록체인의 구축뿐만이 아니라 이러한 활동을 지지할 수 있는 탈중앙화된 거래소가 필요하고 잘 작동되는 유동성 풀 (pool) 들에 대한 동기부여를 할 수 있어야 합니다.

결국 발행된 토큰은 점점 더 점근적으로 탈중앙화에 가까와져 (사용자 소유 키를 포함해) 개인의 에이전시 (agency) 를 최대화할 것입니다. 이것은 결제 교환 비즈니스의 투명성을 통해서만이 아니라 한개의 신용 기관의 비즈니스 절차 소유권을 없애므로서 달성될 수 있습니다. OmiseGo 는 개인이나 발행자들 같은 주주들이 사회의 금융 매커니즘에 훨신 큰 확신을 갖게 할 것입니다.

10. 감사의 말

이 글에 도움을 주신 Piotr Dobaczewski 에게, 그리고 의견과 피드백을 주신 Rick Dudley 와 Vitalik Buterin 에게 감사말씀을 올립니다.

11. 라이센스

참고문헌

[1] Fred Erhsam.	Blockchain	Tokens and the dawn of the De-	
centralized	Business	Model.	https://blog.coinbase.com/

app-coins-and-the-dawn-of-the-decentralized-business-model-8b8c951e734f.

2. [2] Fred Erhsam. Tokens, Why How. https://www.youtube.com/watch?v=rktHO5R8Y9c.
2. [3] Ethereum. Ethereum. https://ethereum.org.
2. [4] Gavin Wood. ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER. http://szabo.best.vwh.net/formalize.html, Feb 2015.
2. [5] Nick Szabo. Formalizing and Securing Relationships on Public Networks. http:// szabo.best.vwh.net/formalize.html, Sep 1997.
2. [6] Joseph Poon and Tadge Dryja. Lightning Network. https://lightning.network/ lightning-network-paper.pdf, Mar 2015.
2. [7] Satoshi Nakamoto. Bitcoin: A Peer-to-peer Electronic Cash System. https:// bitcoin.org/bitcoin.pdf, Oct 2008.

2. [8] Raiden. Raiden Network. https://raiden.network/.
2. [9] Joseph Chow. BTC Relay. http://btcrelay.org/.
2. [10] Bitcoin Wiki. Using external state. https://en.bitcoin.it/wiki/Contract# Example_4:_Using_external_state.
2. [11] Tier Nolan. Re: Alt chains and atomic transfers. https://bitcointalk.org/index. php?topic=193281.msg2224949#msg2224949.
2. [12] Ilja Gerhardt and Timo Hanke. Homomorphic Payment Addresses and the Pay-to-Contract Protocol. http://arxiv.org/abs/1212.3257, Dec 2012.