How to interchain between different blockchains

아주대학교 소프트웨어학과 김용현

2020-02-28

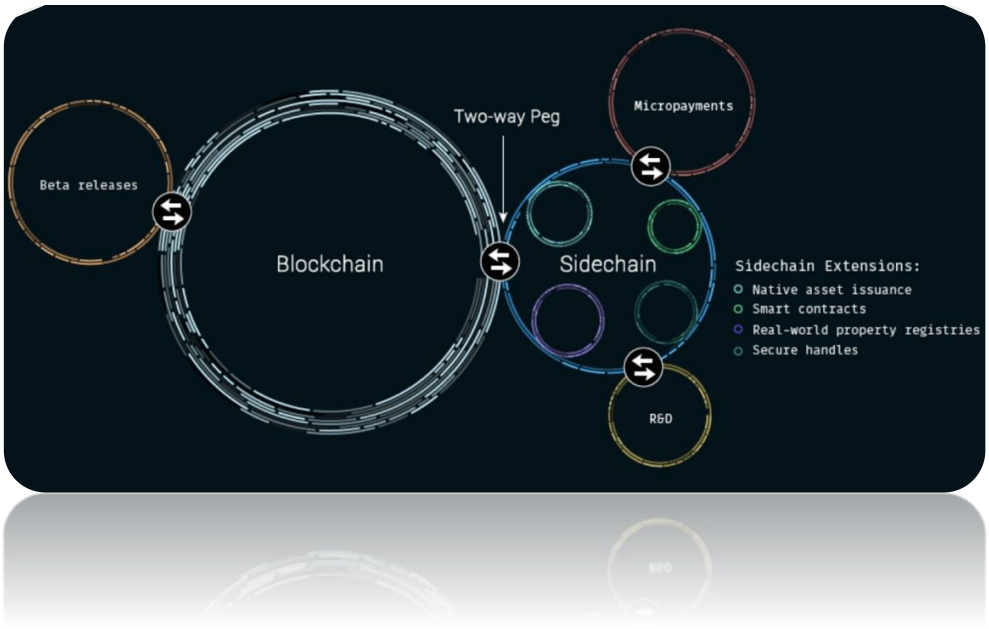
Table of Contents

1. Introduction

2009년 처음으로 블록체인 기술을 토대로 최초의 비트코인이 생성된 이래로, 현재까지 5154 종류의 암호화폐[1]가 유통되고 있다. 이렇게 다양한 암호화폐가 존재하지만 이들이 서로 다른 블록체인 네트워크를 사용할 경우 제3자의 도움 없이 직접적으로 주고받을 수 있는 방법이 아직까지 존재하지 않는다. 따라서 이를 해결할 방법으로 서로 다른 블록체인들을 연결하는 인터체인에 대해 알아보고 이에 대한 이론적 배경과 실제 존재하는 기술들에 대해 알아볼 것이다.

2. Definition

인터체인(interchain)이란 서로 다른 블록체인 간의 연결을 시켜주는 방법으로 각각의 트랜잭션을 교환하는 기술이다. 인터체인을 통해 A라는 암호화폐로만 구매할 수 있는 제품이나 서비스를 인터체인으로 연결된 B라는 다른 암호화폐로도 구매할 수 있게 해 암호화폐간의 거래를 자유롭게 한다. 비트코인의 경우 TPS(Transaction Per Second) 속도가 일정하게 유지되는 본질적 문제를 사이드 체인의 추가 후 인터체인을 통해 TPS 속도를 증가시켜 블록체인 확장성 향상의 대안이 될 수 있다. 또한 블록체인 네트워크 내 전체 노드의 승인이 있어야 블록체인 업데이트가 가능한 부분에 있어 사이드 체인 생성을 통해 전체 노드를 업데이트 하지 않고 필요 부분만 진행할 수 있으며, 체인 결함이 있을 시 원래 네트워크의 피해를 최소화할 수 있어 메인 체인의 변동성을 낮게 유지할 수 있다.



[그림 1] Concept of Two Way Pegging between Main chain & Sidechain

[1] CoinMarketCap, 2020, *Cryptocurrencies*, https://coinmarketcap.com/

3. Concepts

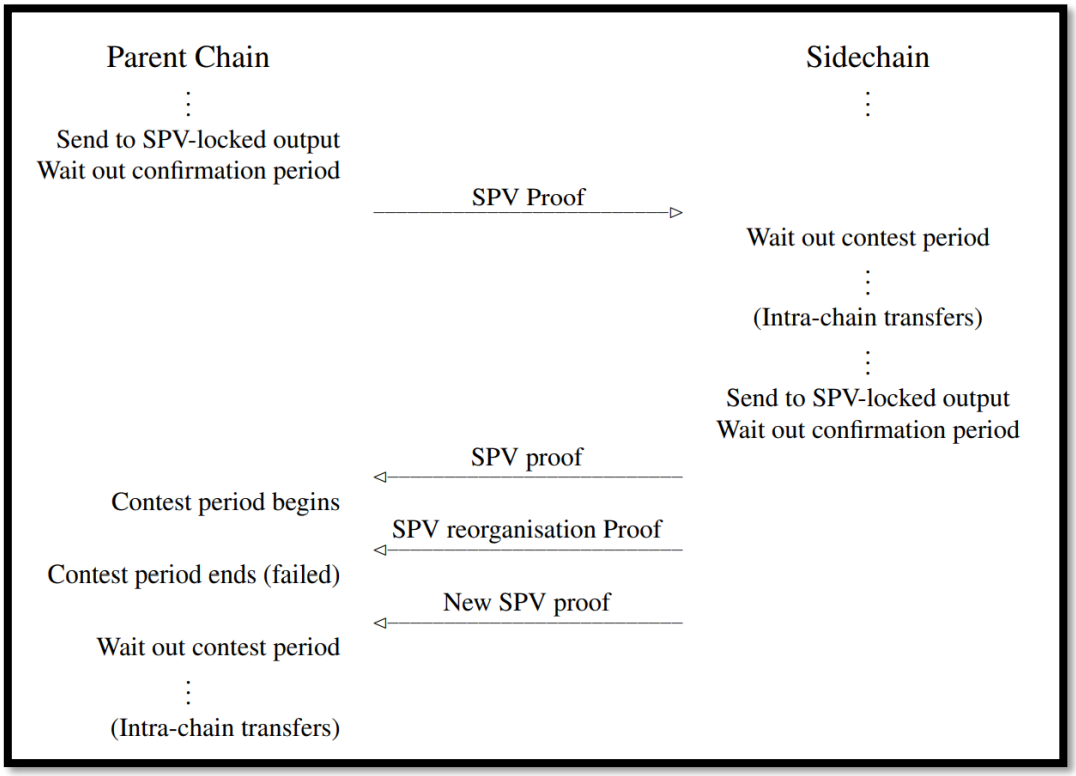
3. Concepts에서는 인터체인 기술에 대한 이론적 배경들이 무엇이 있는지 알아볼 것이며 이에 대한 진행 과정과 한계점에 대해 알아보며 끝으로 실제로 구현되어 있는 기술이 무엇이 있는지 알아볼 것이다.

3.1 Two Way Pegging

Two Way Pegging이란 메인 체인에서 메인 토큰을 동결(Peg)하고 이를 사이드 체인에게 증명(Proof of freeze)해 동일한 가치의 사이드 토큰을 발행하는 기술로 메인 체인이 동결한 자산을 증명할 때 체인의 헤더만 저장해 트랜잭션을 검증할 수 있는 방법인 SPV(Simplified Payment Verification) Proof를 통해 사이드 체인이 증명하게 된다. 이를 수행하기 위해선 두 체인은 다음 기능을 가지고 있어야 한다.

- SPV를 통해 상대 체인의 트랜잭션 검증 가능
- 상대 체인의 Reorg 관찰 가능 및 reorganization proof[2]를 통한 토큰 전송 되돌리기

다음은 Two Way Pegging의 전체 과정이다.



[그림 2] Two Way Pegging Protocol

[2] reorganization proof: contest period 중 체인 내에서 SPV-locked 트랜잭션에 포함되지 않은 블록이 있는지 검증하는 작업. 만약 발견했을 경우, 토큰 교환을 무효 처리한다

1) 메인 체인은 confirmation period[3] 동안 SPV-locked 트랜잭션 생성

2) 메인 체인은 confirmation period 이후 사이드 체인으로 트랜잭션 전달

3) 사이드 체인은 contest period[4]가 끝날 때까지 기다림 (∵ Reorg)

4) 사이드 체인은 트랜잭션에 대해 SPV Proof 진행

5.1) 트랜잭션 유효성이 검증된 경우, 사이드 토큰 생성 혹은 이전에 동결된 사이드 토큰 활성화

5.2) Reorg가 일어났을 경우, 사이드 체인은 reorganization proof 진행. 이후 3)으로 이동

Two Way Pegging은 SPV를 이용한 검증과 confirmation, contest period를 통해 DoS 공격과 Reorg에 대한 대책이 있어 이론적으로 인터체인이 가능한 것처럼 보이지만 실제 구현에 있어서 여러 문제들이 존재한다. 다음은 Two Way Pegging의 널리 알려진 한계점이다.

- Two Way Pegging을 제시한 논문[5]에서는 confirmation, contest period의 기간으로 최소 1, 2일의 시간을 갖기를 권장한다. 따라서 하나의 트랜잭션을 검증하는데 있어 최소 2일 이상이 소요된다. 그러므로 개인간 거래에 있어 적합하지 않다.
- 사이드 체인이 메인 체인의 자산을 일부 보관하는 용도로 사용될 경우, 상대적으로 메인 체인보다 경제 규모(시가 총액)가 작으므로 메인 체인 쪽으로 자산이 쏠리는 뱅크런(Bank run)이 일어날 수 있다.
- 동결된 토큰(pegged token)은 Reorg나 여러가지 이유로 인해 가치가 변경될 수 있다. 따라서 사용자는 동결되지 않은 토큰을 더 선호할 수 있다.
- 교환 비율을 정하는 방법에 따라서 토큰의 총량이 변할 수 있다. 특히 Two Way Pegging의 경우 자산 이동 자체에 대한 방법이므로 이에 대한 방어책은 존재하지 않는다.
- 만약 두 체인이 같은 블록체인 프로토콜을 사용하지 않을 경우, 각 블록체인 안에 상대 블록체인의 트랜잭션을 검증할 수 있는 기능을 추가해줘야 한다. 즉 이 방법을 통해 인터체인을 할 경우 블록체인이 추가될 때마다 그 블록체인에 대한 SPV 검증 기능이 기존 블록체인에 추가되어야 한다. 하지만 블록체인 특성상 업데이트 시 전체 노드의 승인을 받아야 하므로 검증 기능을 추가하는 것은 사실상 불가능하다.

위와 같은 한계점으로 인하여 Two Way Pegging은 이론상으로만 남아있으며 실제로 구현된 기능은 아직까지 존재하지 않고 Relayer와 같은 다른 방법으로 응용되고 있다.

---

[3] confirmation period: 상위 체인에 대해 확인하는 기간. 토큰이 상대 체인으로 전달되기 전에 진행된다.

[4] contest period: 새롭게 전송된 토큰이 상대 체인에서 쓰지 않는 기간.

[5] Adam Back, 2014, "3.2 Symmetric two-way peg", *Enabling Blockchain Innovation with Pegged Sidechains*

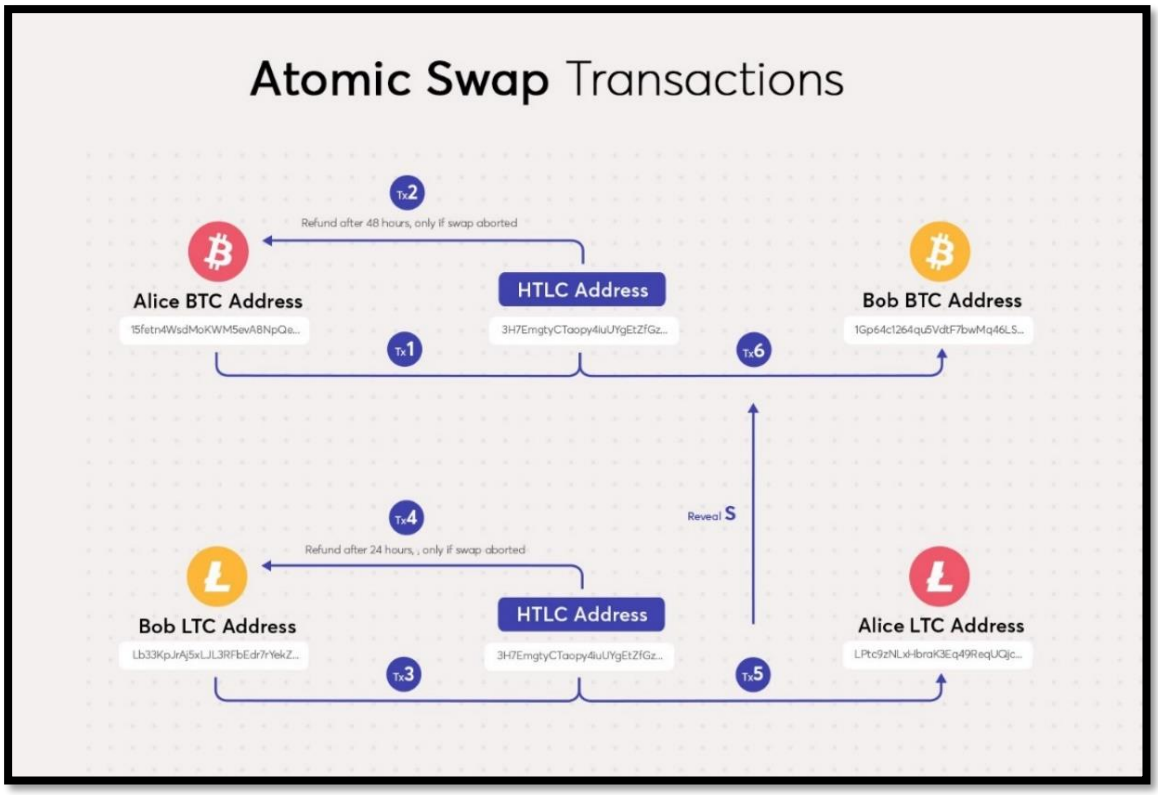
3.2 Atomic Swap

Atomic Swap이란 상호 신뢰 없이 서로 다른 블록체인간 자산 교환을 하는 방법으로 자산 전달이 목적인 Two Way Pegging과 달리 이는 자산 교환에 초점을 두고 있다. 이를 위해 사용자가 보낼 토큰을 HTLC[6]에 저장하고 각 체인마다 토큰 전송용, 거래 취소용, 토큰 교환용 트랜잭션을 생성해 한번 교환 시 총 6개의 트랜잭션을 사용한다.

다음은 Atomic Swap을 사용하기 위한 두 체인의 필요조건이다.

- PoW 기반의 동일한 해시 알고리즘 사용 (BTC의 경우 SHA-256 사용)
- HTLC와 프로그램 작동이 가능한 기능 호환
- 온체인(두 블록체인 네트워크 중 하나) 또는 오프체인(Secondary Layer[7])에서 진행

다음은 BTC과 LTC 사이의 Atomic Swap 전체 과정이다. (α BTC ⇔ β LTC)



[그림 3] Atomic Swap Protocol

1) Alice는 개인키 x 에 대한 HTLC (BTC_contract) 생성 후 α BTC 입금

---

[6] HTLC(Hashed Time Lock Contract): 계약을 일정 시간까지 제한한 타임락(timelock)과 일정한 해시 값이 제시돼야 계약이 성사되는 해시락(hashlock)이 결합된 계약이다.

[7] Secondary Layer(Layer 2): 기존 블록체인 시스템 위에 구축된 보조 프레임워크나 프로토콜. 주요 목표는 메인 암호화폐 네트워크의 TPS 확장 문제를 해결하는데 사용

2) Alice는 개인키 x 와 Bob의 전자서명 입력 시
BTC_contract의 BTC를 Bob의 BTC 지갑으로 보내는 트랜잭션 생성 → **TX1**

3) Alice는 Bob이 48시간 내 TX1을 활성화하지 않을 경우
BTC_contract의 BTC를 Alice의 BTC 지갑으로 보내는 트랜잭션 생성 → **TX2**

4) Alice는 Bob에게 개인키 x 를 암호화한 해시 ***H(x)***를 Bob에게 공유

5) Bob은 해시 ***H(x)***를 통해 또 다른 HTLC(LTC_contract) 생성 후 β LTC 입금

6) Bob는 개인키 x 와 Alice의 전자서명 입력 시
LTC_contract의 LTC를 Alice의 LTC 지갑으로 보내는 트랜잭션 생성 → **TX3**

7) Bob는 Alice가 24시간 내 TX3을 활성화하지 않을 경우
LTC_contract의 LTC를 Bob의 LTC 지갑으로 보내는 트랜잭션 생성 → **TX4**

8) Alice는 24시간 내 개인키 x 를 통해 TX3 활성화 → **TX5**
이 과정에서 Alice는 Bob에게 개인키 ***x*** 공개

9) Bob은 48시간 내 공개된 개인키 x 를 통해 TX1 활성화 → **TX6**

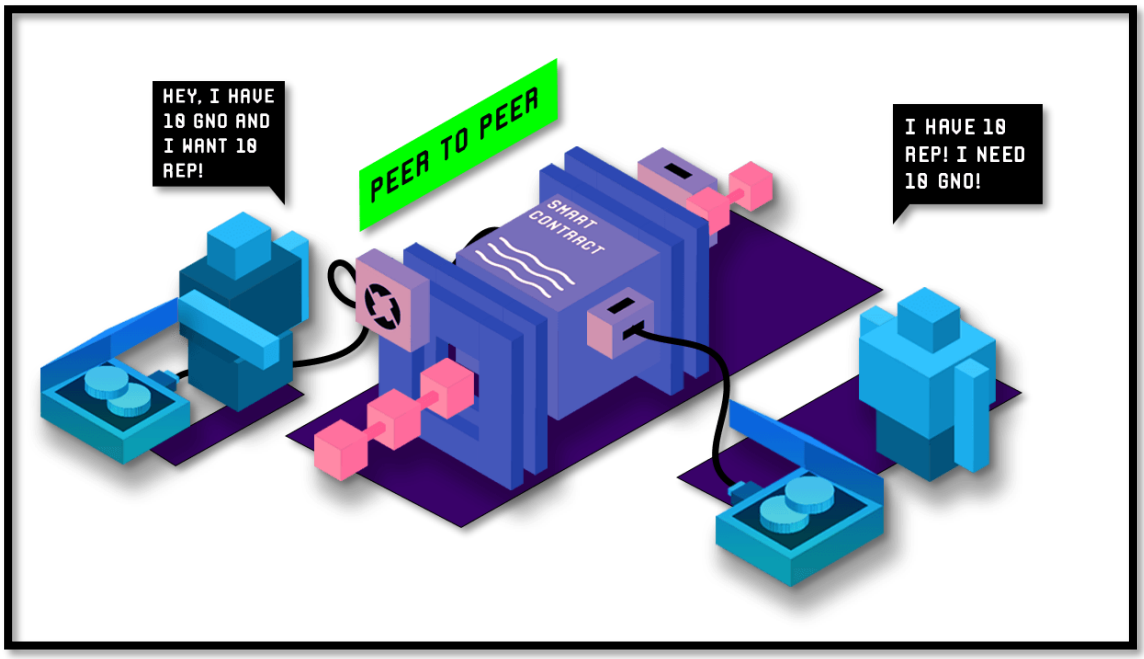
Atomic Swap은 위의 방법처럼 HTLC를 사용할 경우 거래소와 같은 제3자의 도움을 받지 않고 거래를 할 수 있으므로 거래 수수료가 매우 낮거나 존재하지 않아 운용 비용이 저렴하며 거래자 간 신뢰성 있는 교환이 가능하다. 하지만 완벽해 보이는 Atomic Swap 기법에도 한계가 존재한다.

- 두 체인이 동일한 해시 알고리즘을 사용하지 않을 경우 교환이 불가능하다.
- 토큰을 교환하는데 있어 6개의 트랜잭션을 생성해야 하고 타임락으로 인해 최대 48시간의 시간이 소요된다. 따라서 잦은 거래가 필요한 사람에게는 적절하지 않은 방법이다.
- 온체인에서 교환 시 Atomic Swap 거래 내역이 블록체인 탐색기를 통해 빠르게 추적될 수 있고 해당 주소들을 쉽게 연결할 수 있다. 따라서 거래 시 제3자가 개입할 수 있는 여지가 있다.

아직까지 이러한 한계점이 남아있지만 Liquality$_{(atomic\ swaps\ for\ BTC\ and\ ETH)}$, Komodo$_{(Atomic\ DEX)}$ 등 다양한 분야에서 Atomic Swap을 사용한 기술들이 나오고 있으며 계속해서 이를 보완해 나가고 있다.

3.3 Relayer

Relayer(또는 중계자)란 블록체인간 서로 다른 네트워크를 사용해 거래가 불가능할 경우, 거래자의 블록 헤더와 같은 블록 정보를 통해 거래를 중계하는 방법으로 중계자가 주기적으로 블록 헤더를 저장해 SPV client의 역할을 하며 거래자가 자신이 입금한 토큰을 상대 거래자에게 증명할 수 있게 하는 것이 이 방법의 핵심이다. 또한 Relayer는 체인 외부에 있는 주체로 Two Way Pegging과 달리 블록체인 자체를 업데이트 하지 않아도 구애를 받지 않고 사용할 수 있다.



[그림 4] Relayer Plan

다음은 ETH과 BTC 사이의 Relayer 전체 과정이다. (α ETH ⇔ β BTC)

1) Seller는 스마트 컨트랙트(contract_ETH) 생성 후 α ETH 입금
2) Buyer는 Seller에게 β BTC 입금
3) Buyer는 Relayer를 통해 BTC 입금 사실을 증명
4) Relayer는 contract_ETH의 ETH을 Buyer에게 보냄

Relayer는 전체 과정이 간단한 만큼 허술한 부분이 많이 존재한다.

- 거래 실패 시 다시 토큰을 되돌릴 수 있는 방법이 존재하지 않는다.
- 체인 외부에 있는 주체로 탈중앙화적이지 않다. 때문에 중개자 수가 적을 경우 거래자에게 높은 수수료를 부과할 수 있다.
- 중계자가 주기적으로 블록 헤더를 Relay에 저장해야 하지만 해당 블록이 선택되지 않을 경

우 중계자는 수수료를 받을 수 없어 실효성에 문제가 있다.

- Relayer 방식은 아직까지 단방향 통신만 가능하다. 주로 이더리움의 스마트 컨트랙트를 이용한 거래 방식으로 인해 이더리움 네트워크가 아닌 블록체인 간의 거래가 불가능하다.

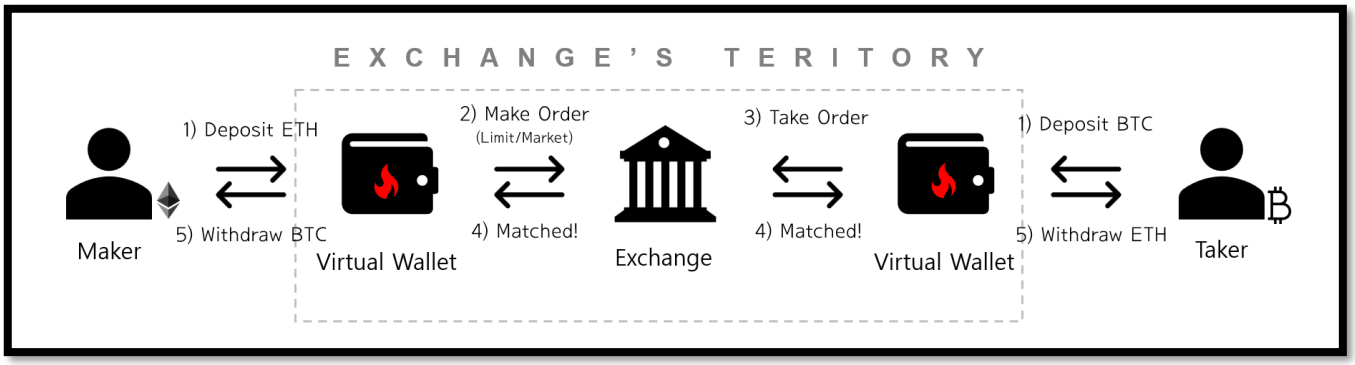
이러한 문제점에도 불구하고 BTC Relay(Bitcoin → Ethereum), RADAR Relay(Ethereum ↔ ERC20 token) 등 실제 구현된 기술들이 존재한다. 이 중 BTC Relay는 **4.1 BTC Relay**에서 자세히 알아보겠다.

3.4 Exchange

Exchange(이하 거래소)란 암호화폐 거래소 내 상장된 토큰(이하 코인)들을 거래해주는 중개소로 기존 주식의 증권거래소와 같이 거래 생성자(Maker), 거래 선택자(Taker), 중개자(Exchange)로 구성되어 있다. 거래소 특징으로는 각 코인마다 거래소 소유의 Hot Wallet[8]이 있으며 거래소 고객이 이 지갑에 입금 후 실제 블록체인 네트워크를 통해 거래가 이루어지는 것이 아닌 거래소 서버 DB 상으로 코인 매매가 이루어진다. 따라서 거래소는 다음과 같은 조건을 만족해야 한다.

- 거래하고자 하는 코인이 거래소에 상장되어야 함
- 각 코인마다 거래를 할 수 있는 HTS(Home Trading System)와 매매체결 시스템 보유

다음은 거래소에서 암호화폐간 거래의 전체 과정이다.



[그림 5] Exchange Overall Structure

1) Maker와 Taker는 Exchange 소유의 가상 지갑에 각자 코인을 예금
2) Exchange는 입금을 확인하고 그 금액만큼 서버 DB에 있는 Maker, Taker의 데이터 변경
3) Maker는 Exchange의 HTS를 통해 BTC 주문

[8] Hot Wallet: 인터넷에 연결되어 있는 암호화폐 지갑으로 실시간으로 거래를 주고받을 수 있다. 하지만 항상 온라인에 연결되어 있어 보안상 안전하지 않다. 반대어로 오프라인 상태로 존재하는 Cold Wallet이 있다.

4) Taker는 HTS에 있는 BTC 주문 중 하나를 선택

5) Exchange는 주문 중 조건이 맞는 것끼리 연결

6) 거래 성사 시 각자의 가상 지갑에 해당 코인이 입금
(단, 서버 DB 상에서만 거래가 이루어지고 블록체인 네트워크에 기록되지 않음)

7) Maker와 Taker는 가상 지갑의 코인을 자기 지갑으로 인출
(블록체인 네트워크에 기록)

2020년 기준으로 암호화폐 거래소는 2만개를 돌파했다.[9] 이렇게 대부분의 사람들이 다양한 블록체인을 거래하는데 있어 거래소를 사용하고 있지만 2019년 한 해의 거래소 해킹으로 인한 피해액은 약 45.2억 달러[10]로 그 금액이 매우 높은 만큼 보안에 있어 취약하다. 다음은 거래소의 대표적인 문제점 및 취약점이다.

- 암호화폐 거래 시 실제 블록체인 네트워크 장부상에 기록되는 것이 아니므로 거래소가 임의의 코인을 상장하고 매물이 있는 것처럼 속일 수 있다.
- 암호화폐 특성상 소수점 처리가 평균 5자리까지 하게 된다. 이때 결제가 같이 일어날 경우 환율 차로 인해 거래소가 손해를 볼 수 있다.
- 주가 조작 방법의 일환인 Pump and Dump[11]에 있어 취약하다.
- 탈중앙화 되지 않은 거래 모델로 인해 해커들로부터 주 공격 대상이다. 주로 서버 DB나 거래소 admin의 Hot Wallet 해킹을 통해 고객들의 암호화폐가 안전하지 않다.
- 실시간으로 고객들의 예금 및 인출을 위해 거래소 내 암호화폐는 어쩔 수 없이 Hot Wallet에 보유하게 된다. 만약 해커들로부터 거래소 지갑의 개인키(private key)를 해킹 당할 경우 매우 큰 피해를 입을 수 있다.
- 거래소가 해킹을 당해 암호화폐를 잃어버렸을 경우 어떠한 보험이나 법적으로 구속되어 있는 것이 없으므로 이 손실은 거래소가 직접 메꿔야 한다.

이와 같은 문제들이 존재함에도 불구하고 현재까지 블록체인 코인들의 많은 거래량과 빠른 속도를 제공해줄 수 있는 방법으로 거래소 이외의 방법이 제시되지 않아 아직까지 블록체인을 인터체인하는 방법으로 가장 많이 사용되고 있다. 다음 **4.2 Peatio Exchange**에서 암호화폐 거래소 오픈소스인 Peatio에 대해 자세히 알아보겠다.

---

[9] CoinMarketCap, 2020, *Markets,* https://coinmarketcap.com/exchanges/binance/

[10] Reuters, 2020, *Cryptocurrency crime losses more than double to $4.5 billion in 2019,* https://www.reuters.com/article/us-crypto-currencies-crime/cryptocurrency-crime-losses-more-than-double-to-4-5-billion-in-2019-report-finds-idUSKBN2051VT

[11] Pump and Dump: 저렴한 가격으로 구매한 주식을 더 높은 가격에 판매하기 위해 주식 가격을 인위적으로 부풀려 이후 다시 파는 행위

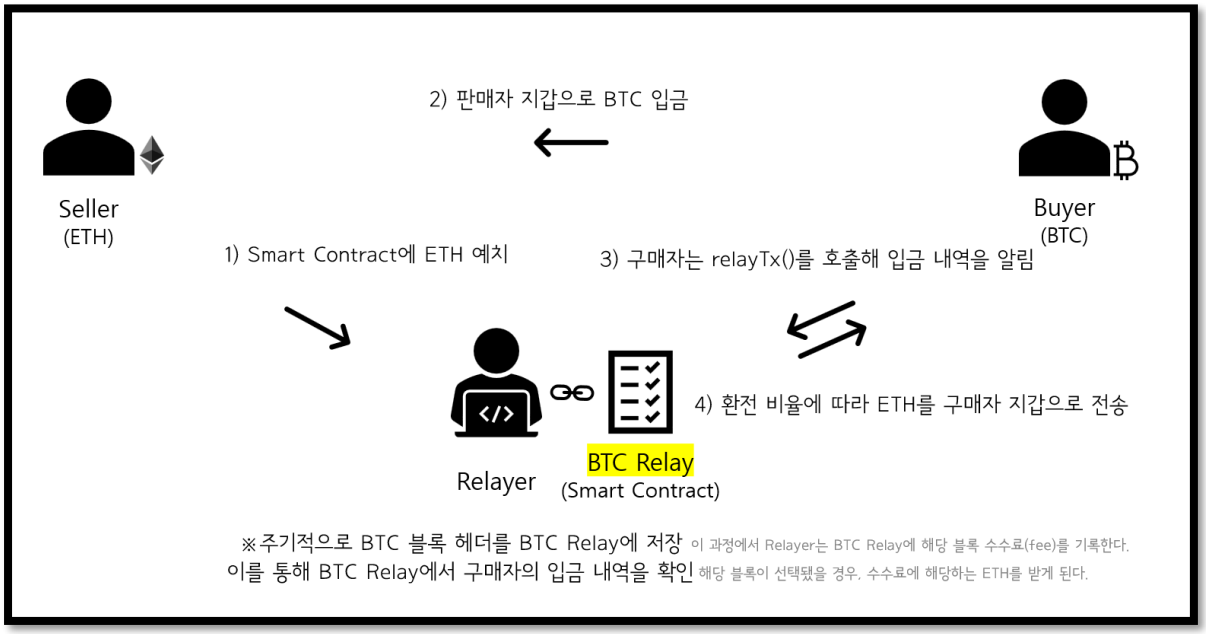
4. Methods

4. Methods에서는 지금까지 알아본 인터체인 개념들 중 실제 개발된 기술들에 대해서 알아보고 각 방법들의 특징과 취약점에 대해 알아보겠다.

4.1 BTC Relay

BTC Relay는 Relayer 개념을 이용해 비트코인과 이더리움을 교환하는 방식으로 중계자가 SPV client 역할을 하는 BTC Relay에 주기적으로 비트코인의 블록 헤더를 저장해 구매자가 판매자에게 비트코인 입금 사실을 증명할 시 BTC Relay를 사용하면서 거래를 진행된다.

BTC Relay의 설치 및 전체 거래 과정은 각주[12]와 [그림 6]을 참고 바람



[그림 6] BTC Relay Overall Structure

BTC Relay의 특징으로는 다음과 같다.

- 오직 단방향 통신(BTC를 통해 ETH DApp 이용)만 거래 가능해 반대 방향으로는 거래가 불가능하다.
- 특정 중계자가 저장한 블록의 소유권을 블록 수수료의 2배에 해당하는 금액을 지불을 함으로써 다른 중계자가 가져올 수 있다. 이를 통해 중계자들 사이에서 인센티브를 통한 수수료 경쟁을 통해 간접적으로 탈중앙성을 띄게 한다

[12] BTC Relay, 2017, https://github.com/ethereum/btcrelay

- SPV Proof 시 스마트 컨트랙트 혹은 블록체인 밖에서 수행 가능하다. 단, 스마트 컨트랙트에서 실행 시 완전히 신뢰 가능하지만 비용(gas)이 많이 들며 블록체인 밖에서 실행 시 비용이 적게 들지만 중앙화 이슈가 존재한다.
- 거래가 성사되지 않았을 때 수수료 처리 및 토큰 반환에 있어 아직 불완전한 부분이 존재한다.
- BTC 블록 헤더를 가져오는 Fullnode는 오직 한군데(blockchain.info)에서 가져온다. 따라서 해당 사이트의 문제가 생겼을 시 SPV Proof에 차질이 생길 수 있다.
- BTC Relay의 대부분 함수들은 기존 중계자의 블록 수수료를 지불한 후 진행하게 된다. 이를 통해 중계자가 저장한 블록 헤더에 포함된 수수료가 최소 1번 이상 보상받게 한다. 하지만 만약 수수료를 비정상적으로 높게 책정하게 될 경우 BTC Relay의 모든 기능을 수행할 수 없게 되므로 큰 문제가 된다. 또한 해커가 코드 우회를 통해 수수료 지불을 하지 않고 대부분의 기능을 수행할 수 있다.

위와 같이 중계자의 수수료 처리 및 인센티브 문제와 이더리움 가스 가격의 상승, Cryptokitties congestion[13] 등으로 인해 중계자가 지속적으로 유지하는데 있어 어려움이 있다. 현재 BTC Relay의 오픈 소스는 2017년 10월을 마지막으로 업데이트가 이뤄지고 있지 않다.

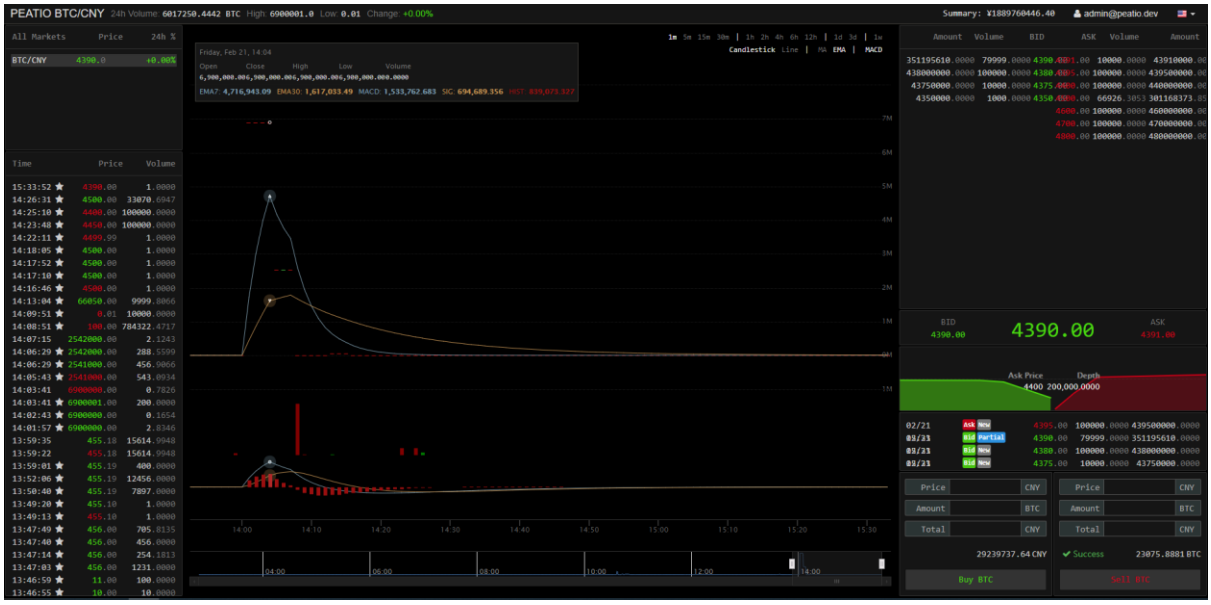
4.2 Peatio Exchange

Peatio Exchange는 암호화폐 거래소 오픈 소스로 암호화폐와 법정화폐간 거래를 해줄 수 있는 거래소 플랫폼이다. 기본적으로 비트코인(BTC)과 위안(CTY)이 등록되어 있으며 다른 암호화폐 추가 시 암호화폐간 거래가 가능하다. 거래소 고객들이 암호화폐 거래를 하기 위해 먼저 거래소에서 제공하는 Hot Wallet에 암호화폐를 입금 후 Peatio에서 제공하는 HTS를 통해 거래를 할 수 있다. 이는 실제 블록체인 네트워크 상에서 이뤄지는 입금/송금 형태가 아닌 거래소 서버 DB에서 일어나는 데이터 교환이다. 실제 고객 지갑으로 들어오기 위해선 거래 이후 Hot Wallet으로부터 인출을 진행해야 한다.

Peatio Exchange의 설치 및 전체 거래 과정은 각주[14]와 [그림 5]을 참고 바람

[13] Cryptokitties congestion: 크립토키티(Cryptokitties, 이더리움 ERC-721 토큰 방식의 디앱(DApp)으로 제작된 게임)에서 트래픽이 몰려 이더리움 네트워크 과부하로 인해 서비스가 지연되고 토큰을 매매할 수 없는 상황을 일컫는 말

[14] Peatio, 2015, *setup_local_ubuntu*, https://github.com/oohyun15/peatio/blob/master/doc/setup-local-ubuntu.md



[그림 7] Peatio Exchange HTS

Peatio Exchange의 경우 보안상 이슈가 되는 부분이 존재한다.

- 서드파티 앱인 Weibo를 통한 로그인에 있어 큰 결함이 존재한다. 만약 Peatio 계정이 Weibo와 연결되어 있을 경우 해커는 피싱 사이트를 통해 valid code를 유출시킬 수 있어 이를 통해 피해자 계정에 로그인이 가능하다. 또한 연결되지 않은 경우에는 해커의 Weibo 계정을 강제적으로 피해자 Peatio 계정에 연결시킬 수 있다.

- 거래소에서 거래를 하기 위해선 반드시 2FA(Two Factor Authenticator)를 거쳐야 한다. Peatio 에서 제공하는 방법은 총 2가지로 SMS, Google Authenticator 방식이 있지만 SMS의 경우 cURL을 통해 SMS update 함수를 호출할 시 커맨드 라인에 바로 OTP이 노출되게 된다. 또한 Google Authenticator의 경우 brute force attack을 통해 최대 3일 내로 해킹이 가능해[15] 2FA 보안에 있어 추가적인 보안 방법이 요구된다.

- Peatio Exchange는 admin 계정을 통해 화폐 입금을 확인 후 일일이 DB에 적용하는 방식이다. 따라서 admin 계정 해킹 시 비정상적인 화폐가 거래소 내에 유입될 수 있어 주의가 요망된다.

이러한 문제점이 대두되지만 오픈 소스 특성상 내부 코드들을 수정해 충분히 대책을 마련할 수 있으며 지금까지 다양한 기업에서 이러한 문제점을 수정하고 거래소를 출시하고 있다.

[15] 6 digit OTP for Two Factor Auth (2FA) is brute-forceable in 3 days: https://lukeplant.me.uk/blog/posts/6-digit-otp-for-two-factor-auth-is-brute-forceable-in-3-days

5. Conclusion

아직까지 서로 다른 블록체인 네트워크의 블록체인들을 탈중앙적이면서 빠른 거래 속도를 보장하는 교환 방법은 오직 이론상으로만 존재한다. 많은 블록체인 개발자들은 이것을 현실화하기위해 머리를 맞대며 고민하고 있지만 지금까진 암호화폐 거래소를 이용하는 방법이 가장 현실적인 방법이다. 서로 다른 체인간 직접적으로 인터체인이 어려운 근본적인 이유는 블록체인이 교환하려는 블록체인 네트워크에서 가치를 증명하는 것이 매우 힘들기 때문이다.

세간에서 블록체인 1세대를 암호화폐 역할을 하는 비트코인, 블록체인 2세대를 스마트 컨트랙트 기능을 추가한 이더리움으로 정의한다. 앞으로 3세대는 TCP/IP와 같이 인터체인 문제를 해결한 블록체인 전송 프로토콜을 통합시킨 블록체인이 되지 않을까 예상한다.

6. References

- Blockstream, *Enabling Blockchain Innovations with Pegged Sidechains,* 2014
  https://blockstream.com/sidechains.pdf
- Sakurity, *Security report for Peatio exchange*, 2015
  https://sakurity.com/peatio.pdf
- Ethereum*, BTC Relay Documentation Release 1.0*, 2016
  https://buildmedia.readthedocs.org/media/pdf/btc-relay/latest/btc-relay.pdf
- Martin Holst Swende, *Hacking on BTC Relay*, 2016
  https://swende.se/blog/BTCRelay-Auditing.html#
- Ethereum, *BTC Relay GitHub*, 2018
  https://github.com/ethereum/btcrelay
- Decipher Media, *블록체인 확장성 솔루션 시리즈:: Interchain solution*, 2018-2019
  https://medium.com/decipher-media/archive
- Jake Frankenfield, *Bitcoin Exchange*, 2019-2020
  https://www.investopedia.com/terms/b/bitcoin-exchange.asp
- Binance Academy, atomic Swaps Explained
  https://www.binance.vision/blockchain/atomic-swaps-explained