# 아토믹 스왑 기술 및 동향 연구

*박하영, 최해웅, 이흥노
광주과학기술원 전자전기컴퓨터공학부
e-mail : *mintyoung@gm.gist.ac.kr, haeung@gist.ac.kr, heungno@gist.ac.kr*

## A study on the Atomic Swaps and Trends

*Ha-Young Park, Haeung Choi, Heung-No Lee
School of Electrical Engineering and Computer Science
Gwangju Institute of Science and Technology

## Abstract

Blockchain is a decentralized network that stores and manages data. Users who contribute to the blockchain network can get coins as a reward. To swap various coins, users have been dependent on centralized exchanges. That method has a lot of problems. Thus, decentralized exchange(DEX) is necessary. Atomic swap is the main technique to implement DEX. This paper describes Atomic swap and various implementations.

## I. 서론

블록체인은 데이터를 분산 시켜 저장하고 관리하는 탈중앙화된 네트워크이다. 중앙 서버나 기관이 존재하지 않기 때문에 사용자들이 네트워크를 유지할 필요가 있다. 네트워크를 유지하는데 기여하는 사용자들은 보상으로 코인을 받을 수 있다. 코인들은 블록체인마다 서로 다르기 때문에 다양한 코인들을 교환하기 위해서 기존에는 제삼자인 중앙화된 중개소를 이용하였다. 그러나 이러한 방식은 과정이 복잡하고, 중개소가 해킹에 노출될 위험이 있고, 중개소는 공인 기관이 아니기 때문에 완전한 신뢰성을 보장받을 수 없다는 것과 같은 문제들이 존재한다. 이러한 문제점들을 해결하기 위한 방안으로 탈중앙화된 중개소의 필요성이 대두되었다. 이를 구현하기 위한 기술로 다양한 블록체인 간에 유저들끼리 코인을 직접 교환할 수 있는 아토믹 스왑이 주목을 받게 되었다.

본 논문에서는 아토믹 스왑 기술과 다양한 아토믹 스왑 서비스들의 동향에 대해 조사한 바를 기술함으로써 아토믹 스왑에 대한 이해를 돕는다.

## II. 본론

### 2.1 아토믹 스왑

아토믹 스왑은 2013년 티어 놀란이 아토믹 크로스 체인 트레이딩이란 이름으로 비트코인 토크 포럼에서 처음 제안하였다. [1] 코모도(Komodo)의 창시자인 JL777이 처음으로 개발에 성공하였다. 일반적으로 아토믹 스왑은 다음과 같은 과정을 따른다. 송신자가 코인을 사전에 실행할 내용을 기록하고 특정 조건이 만족되면 그 내용을 자동으로 이행하는 스마트 컨트랙트에 담고 무작위로 선정된 숫자 값 x와 타임락을 이용해 컨트랙트를 잠근다. 타임락은 시간제한을 통해 코인 교환 과정에서 부정이 일어나는 것을 막는다. 스마트 컨트랙트의 주소를 블록체인에 보낸다. 수신자는 송신자의 스마트 컨트랙트에 코인이 보내졌음을 확인하고 송신자와 같은 숫자 x를 사용해 같은

과정을 반복한다. 송신자는 수신자의 컨트랙트에 코인이 보내졌음을 확인하고 x를 이용해 잠금을 풀고 코인을 받는다. 이때 x는 블록체인상에 공개되기 때문에 수신자도 x를 이용해 송신자가 보낸 스마트 컨트랙트를 해제하고 코인을 받을 수 있다.

### 2.2 아토믹 스왑 구현 방법

#### 2.2.1 스마트 컨트랙트(Smart contract)

OP code로 구성되고 스택을 기반으로 작동하는 스크립트 랭귀지(Script Language)는 비트코인에서 스마트 컨트랙트 프로그래밍을 가능하게 한다. 즉 스크립트 랭귀지를 이용해 아토믹 스왑을 하는 스마트 컨트랙트를 작성할 수 있다. 아토믹 스왑은 기존에 작성되어 있는 scriptPubKey 와 HTLC(Hash Time Lock Contract)를 이용하여 이루어진다. 그러나 현재 비트코인은 보안상의 이유로 표준으로 정의된 스크립트만 실행이 가능하게 되어있다. 티어놀란이 제시한 스크립트 언어를 이용한 아토믹 스왑의 과정은 다음과 같다.

1. A가 임의의 숫자 x를 선택한다.
2. A는 x가 공개되고 B의 서명을 받으면 w BTC를 B의 공개키로 보낸다는 트랜잭션 1을 만든다.
3. A는 48시간이 지나면 A의 공개키로 w BTC를 보내는 트랜잭션 2를 만든다.
4. A가 트랜잭션 2를 B에게 보낸다.
5. B가 트랜잭션 2에 서명하고 A에게 돌려준다.
6. A는 트랜잭션 1을 비트코인 네트워크에 보낸다.
7. B는 x가 공개되고 A의 서명을 받으면 v ALT를 A의 공개키로 보내는 트랜잭션 3을 만든다.
8. B는 24시간이 지나면 B의 공개키로 v ALT를 보내는 트랜잭션 4를 만든다.
9. B가 트랜잭션 4를 A에게 보낸다.
10. A가 트랜잭션 4에 서명하고 B에게 돌려준다.
11. B는 트랜잭션 3을 알트코인 네트워크에 보낸다.
12. A는 x를 사용해 트랜잭션 3을 사용하여 v ALT를 받는다.
13. B는 x를 사용해 트랜잭션 1을 사용하여 w BTC를 받는다.

이더리움에서는 솔리디티(Solidity), 바이퍼(Vyper) 등의 튜링 완전 언어로 아토믹 스왑을 하는 스마트 컨트랙트를 작성할 수 있다. 비트코인의 스크립트보다 더 복잡하고 다양한 프로그래밍이 가능하다.

#### 2.2.2 온 체인 과 오프 체인

온 체인은 메인 블록체인에서 코인 교환 트랜잭션이 이루어지는 것을 의미한다. 코모도의 바터 덱스(Barter DEX)가 온 체인 방법을 이용한다. [2] 스마트 주소(Smart address)를 사용하여 비트코인과 이더리움 계열 코인들, 다양한 ERC-20 토큰 등을 교환할 수 있다. 현재는 더 경량화된 버전인 아토믹 덱스(Atomic DEX)로 서비스 중이다. 바터 덱스는 네트워크상의 거래들의 모음을 저장하는 오더 북 방식을 통해 교환을 원하는 사용자와 유동성 공급자(Liquidity provider)를 매칭시킨다. 유동성 공급자는 시장에 가격 안정성을 공급하고 사용자들이 빠르고 효율적인 거래를 하도록 해주고 수수료를 얻는다. 사용자가 교환하고자 하는 UTXO(Unspent Transaction Output)의 양과 일치하는 유동성 공급자의 UTXO가 존재한다면 서로 오더 매칭이 이루어진다. 바터 덱스의 교환 과정은 다음과 같다.

1. A는 두 개의 UTXO를 갖는다. 하나는 프로토콜 수수료 dexfee를 위한 것, 다른 하나는 교환하고자 하는 양에 해당하는 a payment이다.
2. 유동성 공급자인 B도 두 개의 UTXO를 갖는다. 하나는 A가 교환하고자 하는 토큰 양의 112%에 해당하는 b deposit, 다른 하나는 A가 교환을 요청한 토큰의 양과 같은 b payment이다.
3. A가 교환 요청을 하고 dexfee를 노드에 보낸다. 노드는 요청을 받고 네트워크에 전파한다.
4. B가 네트워크에서 A의 요청을 보고 승낙한다. 그리고 b deposit을 BarterDEX에 보낸다.
5. A는 B의 BarterDEX 임시 지갑으로 a payment를 보낸다. B만 개인 키를 사용해 접근할 수 있다. 그러나 거래가 완전히 끝날 때까지 B가 가져갈 수 없다.
6. B가 b payment를 A의 BarterDEX 임시 지갑에 보낸다. A도 개인 키를 사용해 접근할 수 있다.
7. A가 b payment를 A의 스마트 주소로 옮긴다. BarterDEX가 A가 가져감을 확인한다.
8. B가 a payment를 자신의 스마트 주소로 옮긴다. BarterDEX가 B가 가져감을 확인한다.
9. A와 B의 BarterDEX 임시 지갑이 모두 비었음을 확인한 뒤, b deposit을 b에게 돌려주고 스왑 거래를 종료한다.

유니스왑(Uniswap)은 ERC-20 토큰들과 이더를 교환할 수 있는 프로토콜이다. [3] 이더리움을 기반으로 온 체인에서 실행된다. 유니스왑은 오더 북 방식이 아닌 자동화된 마켓 메이커(Automated market maker) 방식을 사용한다. 이는 수학적 공식을 통해 가격을 계산하는 알고리즘이다. 유니스왑에서는 x * y = k 공식으로 가격이 정해진다. x는 한 토큰의 수량, y는 다른 토큰의 수량, k는 상수로 처음 유동성이 공급될 때 정해지고 유동성이 더해지거나 감소할 때 거래 수수료에 의해서 값이 조금씩 변한다. 상대적으로 수량이 적은 토큰의 가격이 비싸지게 된다. 처음으로 유동성이 공급되면 풀(pool)이 만들어지고

토큰이 저장된다. 이 풀을 통해서 교환을 할 수 있다. 유동성 공급에 대한 보상으로 유동성 풀 토큰을 주는데. 거래 시 수취 되는 수수료는 소유한 토큰의 양에 비례하여 유동성 공급자들에게 배분된다.

표 1. 온 체인 아토믹 스왑.

| 서비스 | 블록체인 | 교환 가능 자산 |
|---|---|---|
| BarterDEX | Komodo (KMD) | BTC와 ETH 계열 코인, ERC-20 토큰 |
| Uniswap | Ethereum (ETH) | ETH, ERC-20 토큰 |
| Pancake swap | Binance chain (BNB) | ETH와 BNB, ERC-20와 BEP-20 토큰 |
| Kyber network | Ethereum (ETH) | ETH, ERC-20 토큰 |

오프 체인은 메인 체인 밖에서 거래가 이루어지고 거래의 결과만 메인 체인에 기록하는 방법을 의미한다. 퍼스트 레이어와 대비되는 세컨더리 레이어(Layer2)를 이용한다. 세컨더리 레이어에는 사이드 체인(Side chain), 지불 채널(Payment channel), 롤업(Roll-ups), 플라즈마(Plasma)가 있다.

사이드 체인을 이용하는 방법은 트랜잭션은 다른 블록체인에서 진행하고 트랜잭션의 결괏값만 메인 체인에 기록한다. 트랜잭션이 처리되는 다른 블록체인이 사이드 체인이다. 사이드 체인은 브리지를 통하여 메인 체인과 연결된다. 블록 스트림(Block Stream)의 리퀴덱스(LiquiDEX)는 비트코인의 사이드 체인인 리퀴드(Liquid)를 이용하는 아토믹 스왑 프로토콜이다. [4] 리퀴드는 비트코인과 일대일로 대응되는 L-BTC(Liquid-BTC) 코인을 사용하고 사용자가 자산 토큰을 발행할 수 있다. 리퀴덱스의 아토믹 스왑 과정은 다음과 같다. Maker는 거래를 제안하고 Taker는 거래를 승낙한다.

1. Maker가 x만큼의 A의 UTXO를 y만큼의 B와 교환하고자 한다면 A는 이 UTXO를 사용하여 y만큼의 B를 받는 트랜잭션을 만든다.
2. Maker가 UTXO 인풋에 SIGHASH_SINGLE 또는 SIGHASH_ANYONECANPAY로 서명을 한다. 이는 Maker의 서명을 무효화하지 않고도 Taker가 트랜잭션에 인풋과 아웃풋을 추가할 수 있게 해준다.
3. Maker가 트랜잭션을 리퀴덱스에 게시한다.
4. Taker가 리퀴덱스에서 트랜잭션을 확인하고 몇 가지 검증 과정을 거친다.
5. Taker가 y만큼의 B와 수수료를 트랜잭션에 인풋으로 추가하고 SIGHASH_ALL로 서명한다.
6. Taker가 트랜잭션을 리퀴드 네트워크에 보낸다. 트랜잭션이 블록에 포함되면 스왑이 완료된다.

지불 채널은 블록체인 밖에서 두 당사자끼리 거래를 하는 채널을 열고 지불 상태를 기록한다. 라이트닝 네트워크(Lightning network)는 비트코인의 지불 채널을 직접적으로 연결을 해 주지 않아도 라우팅이 되어 연결되는 라우티드 지불 채널(Routed payment channel)을 구현하는 모델 중의 하나이다. A와 B가 서로 교환을 하고자 하면 A와 B는 중간자인 C와 두 코인의 블록체인 모두 지불 채널로 연결되어 있어야 한다. A가 첫 번째 코인을 C에게 B가 두 번째 코인을 C에게 보내면 C는 첫 번째 코인을 B에게 두 번째 코인을 A에게 보냄으로써 아토믹 스왑이 이루어진다. 라이트닝 랩스(Lightning Labs)의 서브마린 스왑(Submarine swaps)은 라이트닝 네트워크와 온 체인을 혼합해서 사용하는 아토믹 스왑 모델이다. [5] 현재 비트코인과 라이트코인 간의 교환이 가능하다. 라이트닝 네트워크만을 이용한 방법은 교환하고자 하는 코인 모두 라이트닝 네트워크가 가능해야 한다. 그리고 지불 채널을 연결할 때 초기에 설정한 코인이 모두 소모되면 다시 새로운 채널을 열어야 한다. 이는 온 체인에서 이루어지기 때문에 수수료가 든다. 서브마린 스왑은 하나의 코인만 라이트닝 네트워크가 가능해도 거래를 가능하게 하고 코인이 모두 소모되더라도 완전히 새로운 채널을 열지 않고 기존에 존재하는 다른 채널로 라우팅을 해준다. 이더리움의 라우티드 지불채널인 라이덴 네트워크(Raiden network)를 통해서는 ERC-20 토큰의 아토믹 스왑이 가능하다.

롤업은 오프 체인에서 거래 처리가 이루어지고 대량의 거래를 하나의 거래로 모아 그 해시값만 메인 체인에 트랜잭션 데이터로 저장을 한다. 그리고 데이터의 소유권을 보장해 주기 위해서 영지식 증명(Zero Knowledge Proof)이나 사기 증명(Fraud proof) 방법을 사용한다. 영지식 증명을 사용하는 zk-Rollups 기반의 이더리움 프로토콜인 zk-Sync는 ERC-20 토큰과 NFT 스왑 기능을 제공한다. [6] 사기 증명을 사용하는 Optimistic-Rollups 기반의 이더리움 프로토콜 Optimism은 -유니스왑의 테스트 버전이 아-배포되어 ETH, ERC-20 토큰 스왑을 할 수 있다. [7]

## 2.3 한계점

온 체인 방식의 아토믹 스왑은 느린 처리 속도, 높은 수수료, 익명성이 보장되지 않는 등의 메인 체인에서의 문제를 그대로 가지게 된다.

오프 체인 방식의 아토믹 스왑은 처리 속도가 빠르고 낮은 수수료, 익명성 보장의 장점이 있지만, 규모가 큰 트랜잭션의 처리가 불가능하고 사용자가 오프라인 상황에서는 사용이 불가능하다.

표 2. 오프 체인 아토믹 스왑

| 서비스 | Layer2 | 교환 가능 자산 |
|---|---|---|
| LiquiDEX | Bitcoin Side-chain | L-BTC, 사용자 발행 자산 |
| Submarine Swaps | Bitcoin Lightning Network | BTC, LBTC |
| zk-Sync | Ethereum zk-Rollups | ETH, ERC-20 토큰, NFT |
| Optimism | Ehtereum Optimistic-Rollups | ETH, ERC-20 토큰 |

## Ⅲ. 결론

아토믹 스왑은 중앙화된 중개소에서 발생할 수 있는 여러 문제를 해결해 줄 수 있다. 아토믹 스왑을 통해 탈 중앙화된 중개소를 구현한 서비스들도 많이 생겨났다. 그러나 아직 아토믹 스왑은 기술적인 한계점들이 존재한다. 탈중앙화된 금융(DeFi) 시장이 성장하면서 아토믹 스왑의 중요성은 앞으로도 계속해서 커질 것이다. 따라서 아토믹 스왑의 기술적 한계를 개선하기 위한 연구가 필요하다.

## Acknowledgements

이 논문은 2021년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.2021-0-00118, 대규모 노드를 위한 탈중앙화 합의체 구성 기술개발)

## 참고문헌

[1] “Alt chains and atomic transfers”, Bitcoin Forum https://bitcointalk.org/index.php?topic=193281.msg2003765#msg2003765

[2] “Komodo An Advanced Blockchain Technology, Focused on Freedom”, https://cryptorating.eu/whitepapers/Komodo/2018-02-14-Komodo-White-Paper-Full.pdf

[3] “Uniswap v3 Core”, https://uniswap.org/whitepaper-v3.pdf

[4] “LiquiDEX Github”, https://github.com/RCasatta/LiquiDEX

[5] “This Tech Lets You Send Any Cryptocurrency to the Lightning Network”, https://www.coindesk.com/markets/2018/09/08/this-tech-lets-you-send-any-cryptocurrency-to-the-lightning-network/

[6] “Introduction to zkSync for Developers”, https://zksync.io/dev/#overview

[7] A New Way to Scale – Optimized Optimistic Rollup, https://blog.idex.io/all-posts/o2-rollup-overview