

# 비트코인 트랜잭션 시각화

AJOU 2021-1  
SOFTCON



팀 명 TxSpider

팀 원 송영훈, 고창빈, 공윤환, 이현석

지도교수 손태식

멘 토 삼성전자 인정식 수석연구원

## 개발 동기 및 목적

최근 몇년간 비트코인은 사람들의 관심을 받아온 주제 중 하나다. 특히 올해 들어 비트코인 가격이 급등하면서 많은 사람이 비트코인에 관심을 갖고 투자를 하면서 비트코인의 시가총액은 1조 달러를 넘기도 했다. 하지만 이렇게 거래도 늘어나면서 자연스럽게 불법적인 거래 또한 증가하였는데, 지난 4월에는 하루 24조 가량의 거래가 불법적인 거래로 추정된다는 자료가 발표되기도 했다. 또 실제로 여러 범죄 사건에서 비트코인, 이더리움 등을 이용해서 불법 자금을 세탁해온 것은 어제 오늘의 일이 아니다.

이러한 불법 자금 세탁이나 탈세 등의 자금을 추적하는 것에는 트랜잭션의 시각화가 필수적이다. 트랜잭션이 전부 공개가 되어 있는 하지만 시각화를 하지 않는 이상 그 상관 관계를 파악하는 것은 거의 불가능에 가깝기 때문이다. 이더리움 같은 경우는 일반 사용자가 접근 가능한 트랜잭션 시각화 툴이 존재한다. 하지만 비트코인의 경우에는 일반 대중이 접근 가능한 시각화 툴이 존재하지 않는다. 그리고 이더리움, 비트코인 모두 전문적인 시각화 툴은 모두 일반 대중의 접근이 불가능하고 오직 수사 용도로만 사용된다.

블록체인과 비트코인 등의 관심이 늘어난 지금 우리는 일반 대중에게도 비트코인 트랜잭션을 분석할 도구의 필요성이 늘어날 것이라고 생각했다. 그리고 현재 '일반 대중이 접근 할 수 있는 비트코인 트랜잭션 시각화 툴'이 없다는 것에서 착안하여, 트랜잭션을 트리의 형태로 시각화 하는 툴을 만들게 되었다.

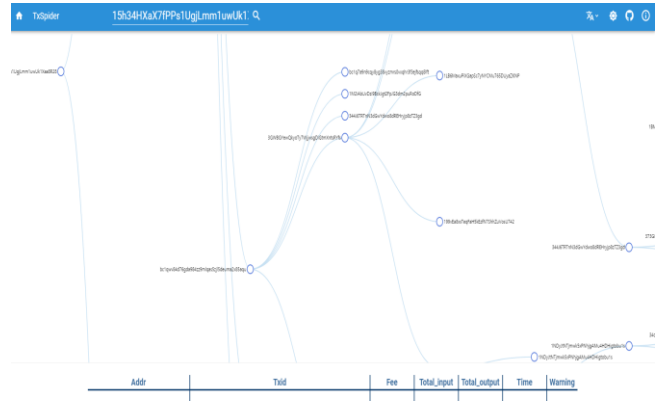
자연스럽게, 우리의 목적은 트랜잭션을 시각화 하고, 각 노드의 정보를 출력해주는 기능을 구현하는 것이며, 관련 논문들을 참고해서 의심 노드를 탐지하고 출력해주는 기능을 구현하였다. 우리가 제공하는 시각화는 너무 지나치게 시각화를 하여 직관적인 이해를 방해하지 않도록 하였고, 전체적인 포맷은 수사기관에서 사용하는 것으로 알려진 형태를 참고하여 개발하였다. 우리의 툴을 통해서 일반 대중도 비트코인 트랜잭션의 흐름과 그에 따른 분석에 도움이 될 것으로 기대한다.

## 주요 기술

'TxSpider'의 주요 기술은 총 네 가지로 나눌 수 있다.

- TX 파싱 및 Wallet Address - Transaction 매칭  
RPC를 통해 획득한 transaction들을 이용하여 올바른 Wallet Address와 매칭 시켜주는 기능이다.
- 트리 형태로 데이터 가공  
백엔드에서 담당하는 기능으로써 Wallet Address - Transaction 매칭 데이터를 시각화하기 위해서는 트리 형태로 가공된 데이터가 필요하기에 이에 맞는 기능을 구현하였다.
- 트랜잭션 시각화  
이 기능은 말 그대로 사용자가 입력한 주소에 관련된 트랜잭션들을 트리 형태로 보여주는 것이다. 기존에 제공되고 있는 텍스트 형식의 트랜잭션 정보는 직관적으로 파악할 수 없는 구조였으나, 우리 'TxSpider'는 이 트랜잭션에 대한 정보를 직관적으로 파악할 수 있게 해준다.
- 노드 정보 제공  
이 기능은 사용자가 노드에 대한 정보를 알고 싶을 경우 노드를 더블 클릭 시 해당 노드에 대한 정보(Txid, Fee, Total\_input, Total\_output, Time, Warning)를 출력해 주는 기능이다.

## 개발 내용



TxSpider 검색 화면

사용자는 지갑 주소를 통해 검색을 할 수 있다. 검색한 주소와 연관된 트랜잭션들을 최대 depth 9까지 시각화하여 렌더링하고 줌인, 줌아웃, 폴드, 패닝 기능을 제공한다. 또한 각 노드별 상세 정보를 조회할 수 있으며 각각 클립보드에 저장할 수 있다.

각 노드는 최대 5개의 엣지를 가지며 거래량과 엣지수를 토대로 전체 트랜잭션 데이터 중 이상 거래가 의심되는지 알려준다.

## 결과 및 분석

우리는 비트코인 트랜잭션 시각화 도구 'TxSpider'를 구현하였고, 개발 동기 및 목적에서 제시한 것 처럼 트랜잭션의 시각화, 각 노드의 정보 출력, 의심 노드 탐지 등의 기능을 모두 구현하였다. 그리고 우리의 서비스를 오픈 소스로 제공함으로써 일반에 공개함과 동시에 오류의 탐지 유연한 성장을 가능케 하였다.

우리는 이 서비스의 효용 및 가치를 다음과 같이 판단하였다. 우선 가상화폐(특히 비트코인)의 흐름에 대한 이해를 상승시켜 줄 것이다. 여러 논문들을 종합해 본 결과 거래의 목적에 따라 트랜잭션을 시각화 했을 때 나타나는 형태가 다르다고 알려져 있다. 일반 대중, 연구자는 실제 트랜잭션을 시각화 하면서 이러한 흐름에 대한 이해를 더 명확히 할 수 있을 것이다.

다음으로 기존 서비스보다 훨씬 더 간편한 자동화와 시각화를 제공한다. 기존 서비스에서는 노드를 마우스로 하나씩 끌어가면서 시각화를 하는 등, 너무 시각적인 측면에만 초점을 맞춰서 유의미한 결과를 얻기 힘들었는데, 우리의 서비스는 지갑 주소를 기반으로 관련 트랜잭션을 출력해주기 때문에 훨씬 편하고 자동화 수준도 높다고 할 수 있다.

마지막으로 의심 노드에 대한 출력을 해줌으로써 일반 대중과 연구자들에게 의심 노드에 탐지에 대한 감각과 패턴을 느낄 수 있게 하였다.

아쉬운 점도 있었다. 서버의 성능이 충분치 못해서 depth를 제한할 수 밖에 없었고, 의심 노드를 출력하는 알고리즘을 더욱 정교하게 계산하여 도출하려고 했지만 이 역시 서버의 성능 문제 등에 부딪혀서 더 발전시키지 못했다. 하지만 우리의 서비스를 오픈소스로 제공한 만큼 이 컨셉에서 나아가면 더욱 정교한 툴이 될 것이다.

