가상화폐 범죄의
시작과 끝

Patrick Kim, Uppsala Security

'어둠의 화폐' 비트코인이 'n번방' 판 키웠다

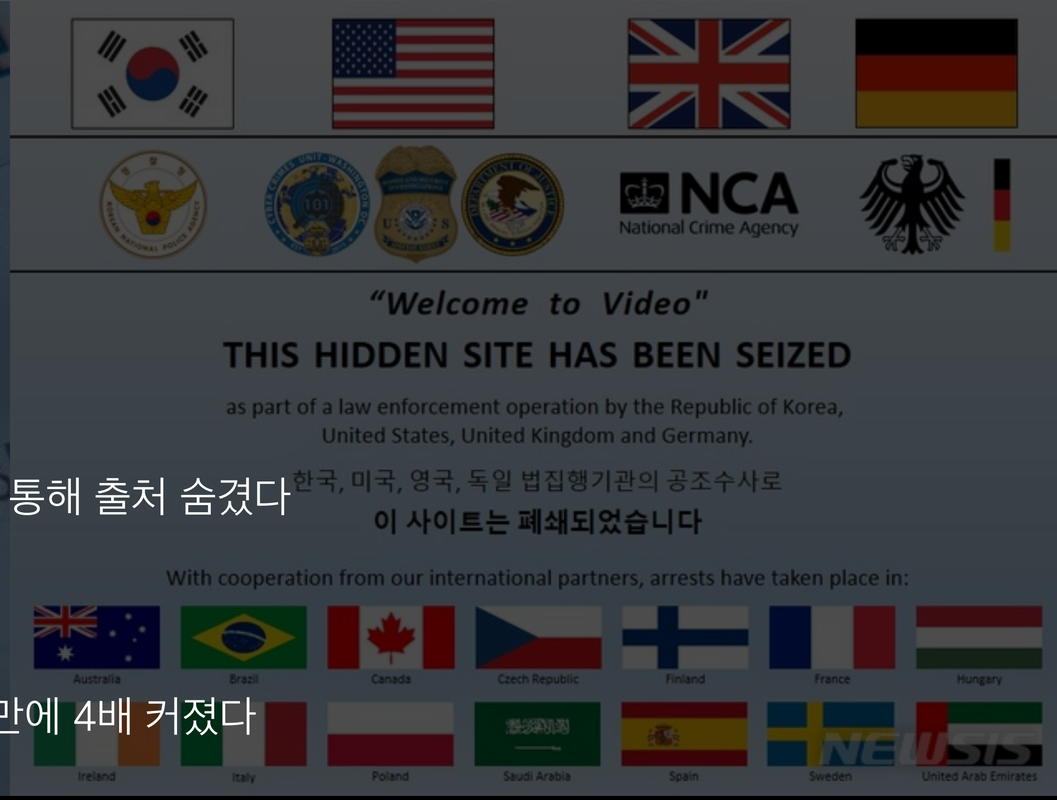
동아일보

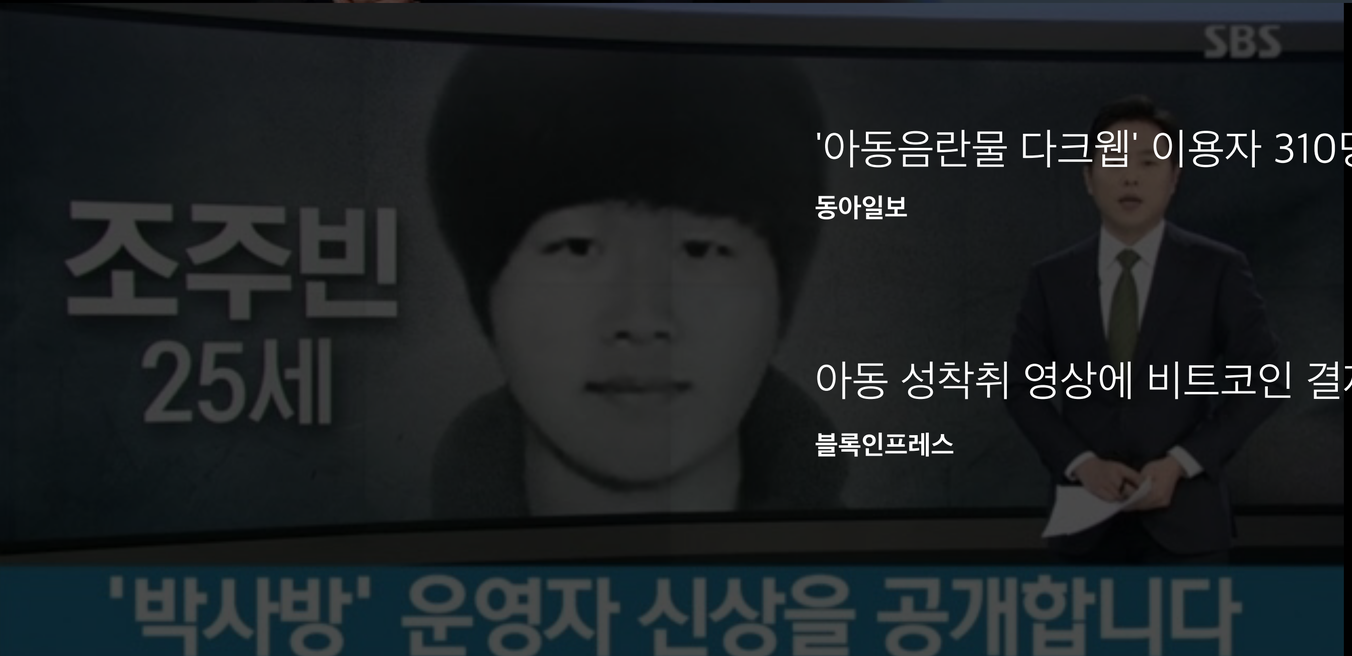
조주빈 '입장료' 비트코인, 전문 믹싱서비스 통해 출처 숨겼다

코인데스크코리아

‘검은 코인’이 쌓은 범죄도시…다크웹, 1년 만에 4배 커졌다

서울신문



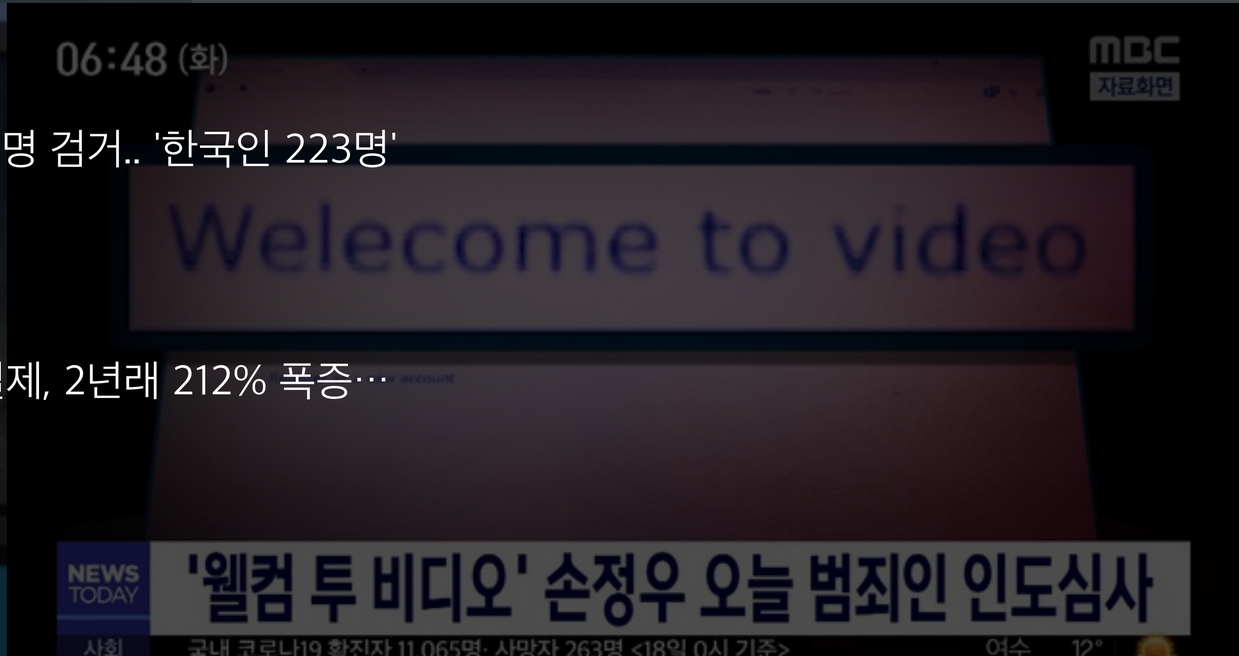


'아동음란물 다크웹' 이용자 310명 검거.. '한국인 223명'

동아일보

아동 성착취 영상에 비트코인 결제, 2년래 212% 폭증…

블록인프레스



"It's totally anonymous,"

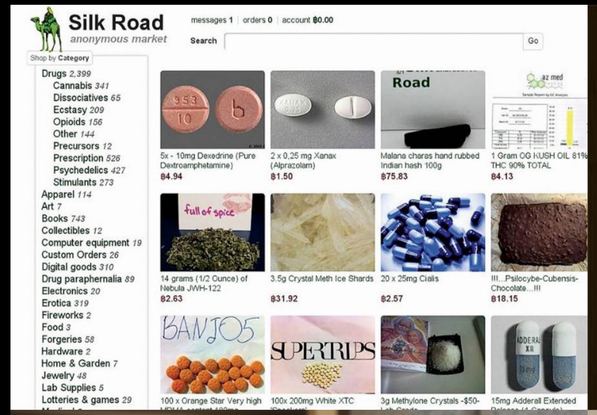
완벽한 익명성이다.

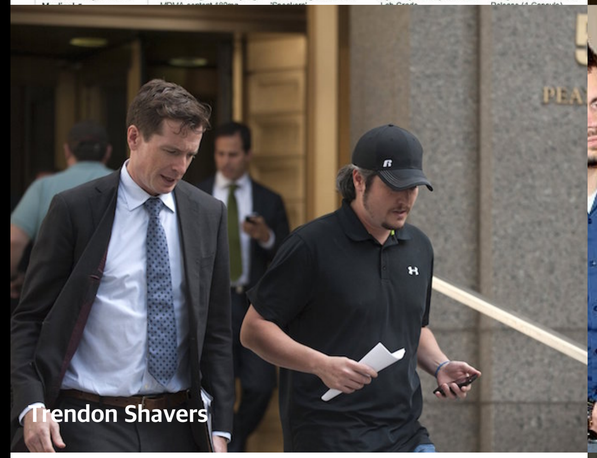
"The FBI does not have a prayer of a chance of finding out who is who."

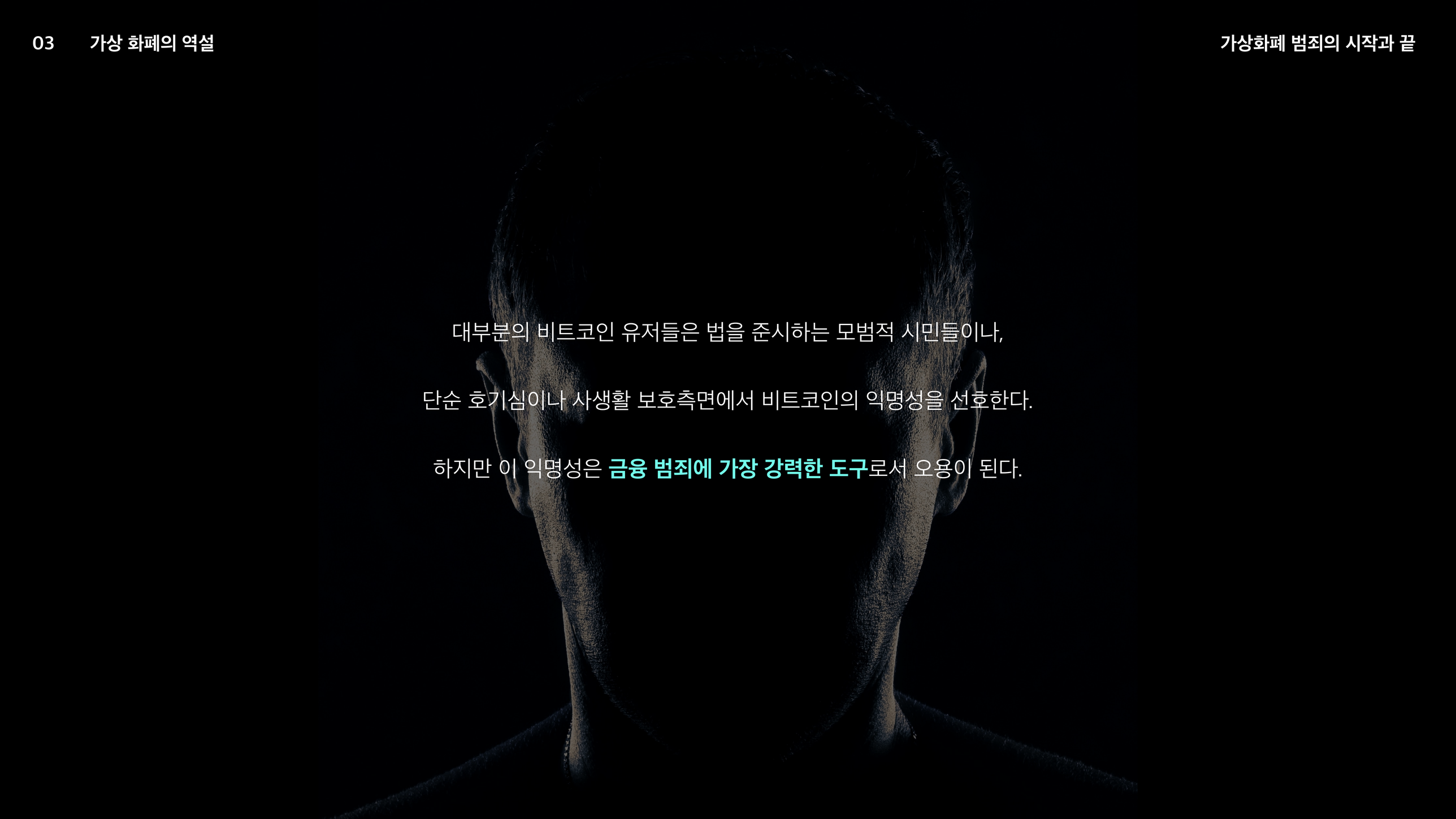
FBI는 누가 누군지 알아낼 방법이 없다.

2013년 bitcoin forum, 익명 유저의 코멘트 중

- 2013년 7월 FBI 의 비트코인을 교환 매개체로 하는 익명 마켓 플레이스 **실크로드** 서버에 접속 성공
- 10월 서버 압수, 미국 국적의 운영자 **Ross Ulbricht** 의 체포
- 2015년 2월 1 billion 이 넘는 불법 마약등의 거래 혐의로 종신형 선고
- 2015년 9월 미국 국적의 **Trendon Shavers** $150 million 이상의 다단계 사기 혐의로 체포 **(최초의 증권법 위반 비트코인 사기 케이스)**
- 2015년 3월 체코 국적의 **Tomáš Jiříkovský** 체포, $40 million 이상의 자금 세탁을 비트코인을 이용한 혐의
- 2014년 Mt. Gox 해킹 사건의 책임에 대한 혐의로 **Mark Karpelès** 체포
  (당시 390 millon 이 넘는 비트코인 해킹 피해에 대한 조작 혐의)



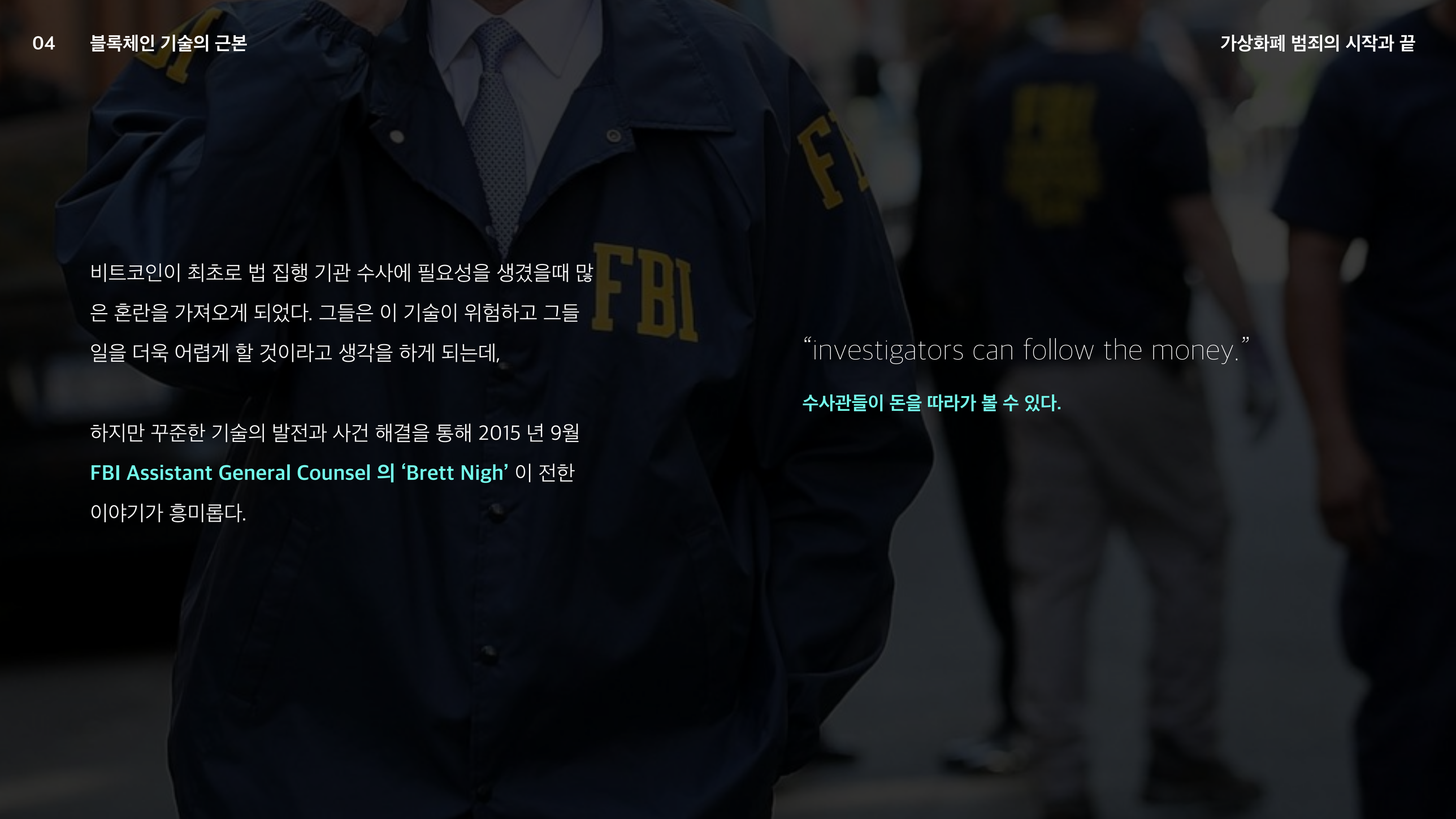




대부분의 비트코인 유저들은 법을 준시하는 모범적 시민들이나,

단순 호기심이나 사생활 보호측면에서 비트코인의 익명성을 선호한다.

하지만 이 익명성은 **금융 범죄에 가장 강력한 도구**로서 오용이 된다.



비트코인이 최초로 법 집행 기관 수사에 필요성을 생겼을때 많은 혼란을 가져오게 되었다. 그들은 이 기술이 위험하고 그들 일을 더욱 어렵게 할 것이라고 생각을 하게 되는데,

하지만 꾸준한 기술의 발전과 사건 해결을 통해 2015 년 9월 **FBI Assistant General Counsel 의 'Brett Nigh'** 이 전한 이야기가 흥미롭다.

"investigators can follow the money."

수사관들이 돈을 따라가 볼 수 있다.

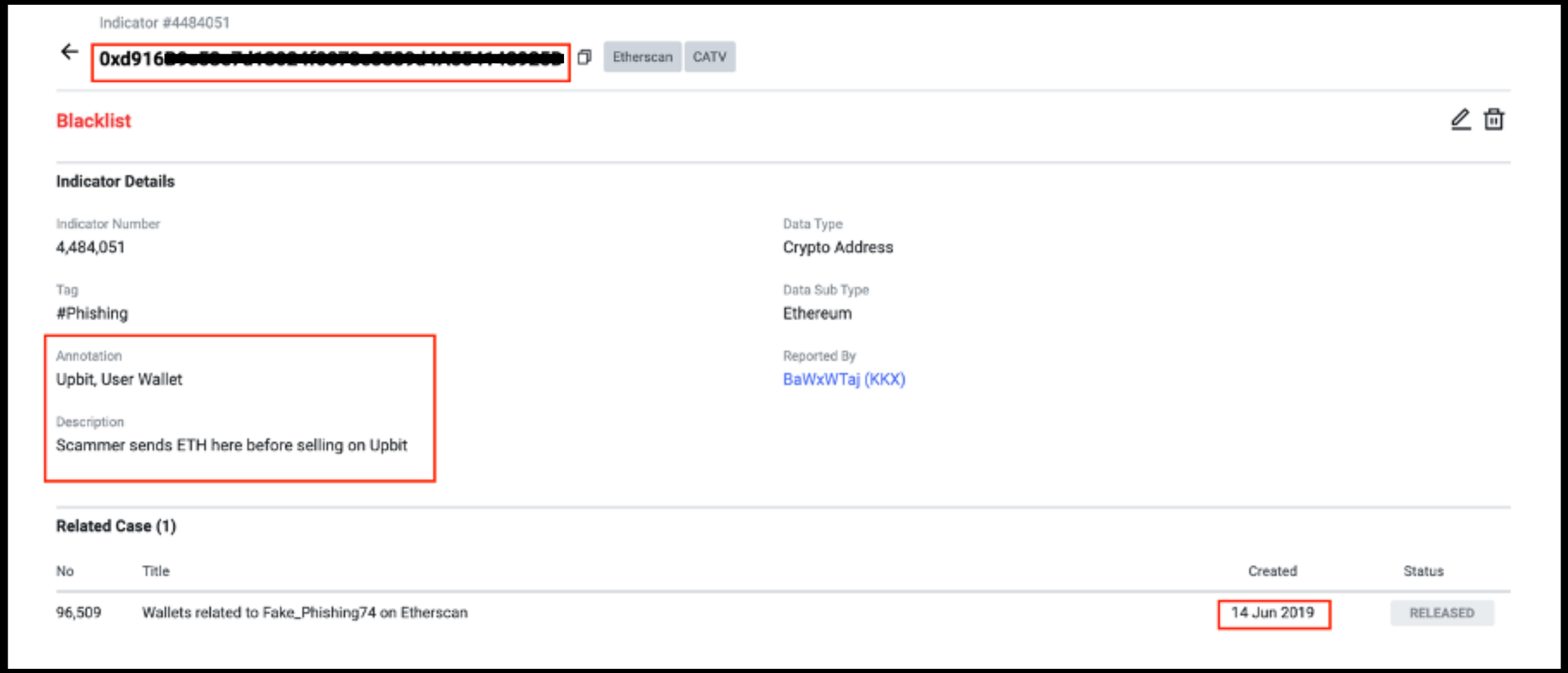
수사관의 관점에서만 본다면 비트코인은 큰 장점을 가질수 있다.
만약 길거리의 마약상을 체포하고 현금을 압수 한다면 이것은 하나의 범죄만 입증된 상황이다.

하지만 만약에 암호화폐 범죄자들의 경우 그들의 기록을 통해 범죄 전체에 대한 기록을 찾아 볼수가 있는데 **이는 하나의 “범죄 장부” 를 발견하는 것이나 마찬 가지다.**

N번방, 웰컴투비디오 등의 사건을 통해 정확한 사례를 설명 해볼수 있다.

해당 사건들은 성착취물소비자, 운영자 들이 비트코인 , 이더리움, 모네로 등을 통하여 익명 거래를 진행했으나 성착취물 소비자가 구매를 하기 위해 사용한 거래소, 그리고 운영자들이 현금화를 하기 위해서 사용한 거래소들의 기록이 남겨져 있어 **그들의 신원을 밝혀 냄에 큰 도움이 된다.**

수사 측면에서 공개된 범죄 장부의 개념으로 생각해 본다면 이러한 사례들도 발견 된다. 아래는 블록체인 공공 위협 플랫폼 “센티넬 프로토콜"에 기 등록된 주소이다. 2019년 6월 14일 에 이미 사기 기록을 가진 트랜잭션이 업비트의 개인 주소로 연속 발생 된 내용이다.



해당 사기 기록은 Jaxx 라는 지갑 유저가 973 개의 이더리움을 해킹에 의해 탈취 당한 기록이다.

Jaxx mobile hacked.. 973 eth gone. AMA

I have no idea what happened and I'm still in shock, but I had 973 eth and 7000+ golem in Jaxx mobile ... I logged in to check on it and it's all gone.

Here is all I have...

The transaction itself..
https://etherscan.io/tx/0x911ee7a8fae17dd77cdaccd66c65b58a2bd479d78d3a836ea96f307d5c03cdb8

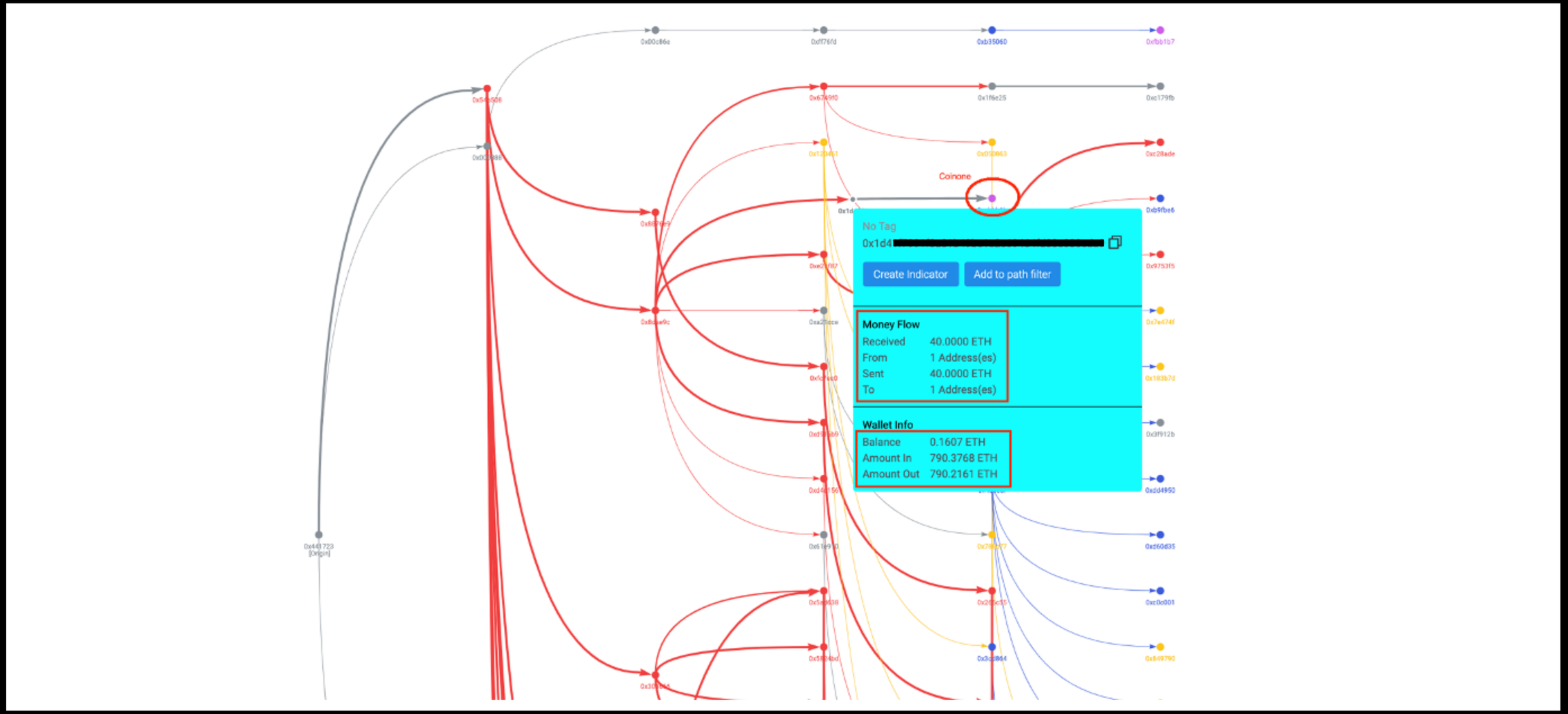
The address and the last transaction s:
https://etherscan.io/address/0x54a508ff8da468cbdbe9a68550ec5ef745c08126

I'm still very gutted right now and emotional, but if I can help other from this happening then I will try.

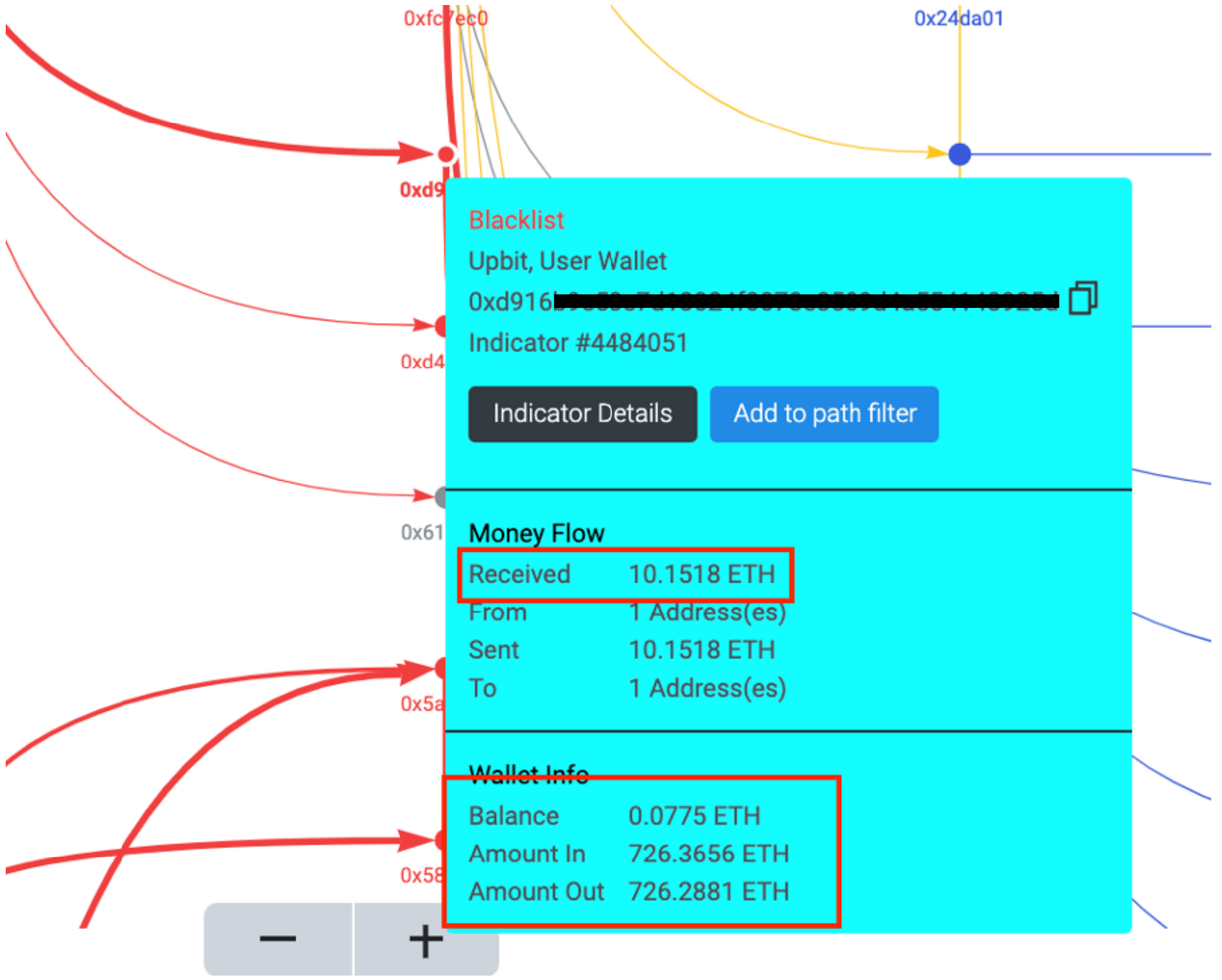
Please be gentle.

973 개의 이더를 해킹한 해당 해커의 지갑은 2018년 당시 코인원, 업비트, 바이낸스 , 비트렉스, 비트파이넥스 다양한 자금 세탁을 하였다.

그중 국내 거래소인 코인원에는 2018년 7월 17일 이더리움 40개를 보냈으며 (총 125개의 트랜잭션을 통하여)

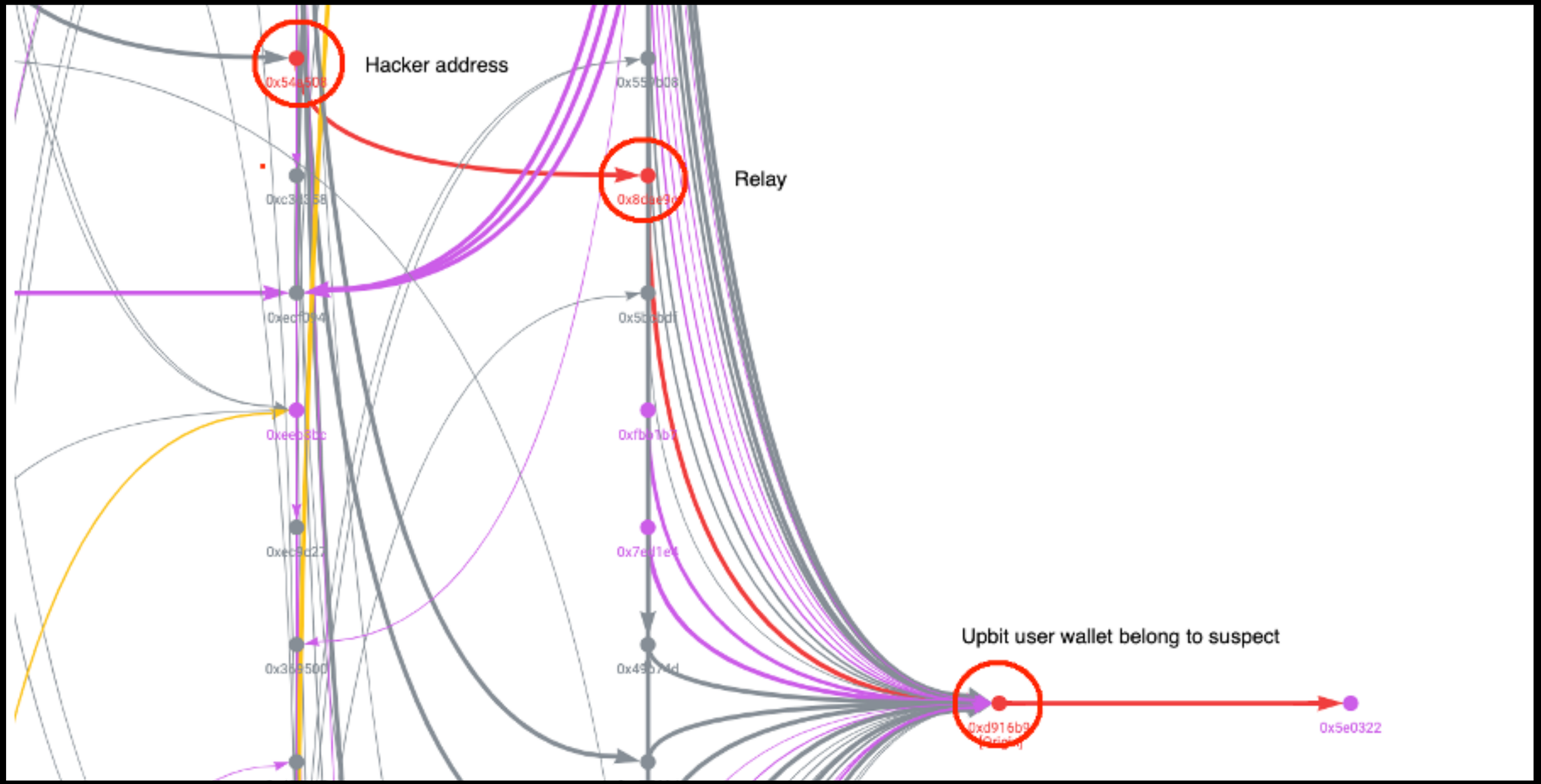


2018년 8월 6일 업비트로 이더리움 10개를 입금 하였다.



이 해커의 불법 자금 10개가 세탁된 이력을 가진 업비트의 개인 지갑이

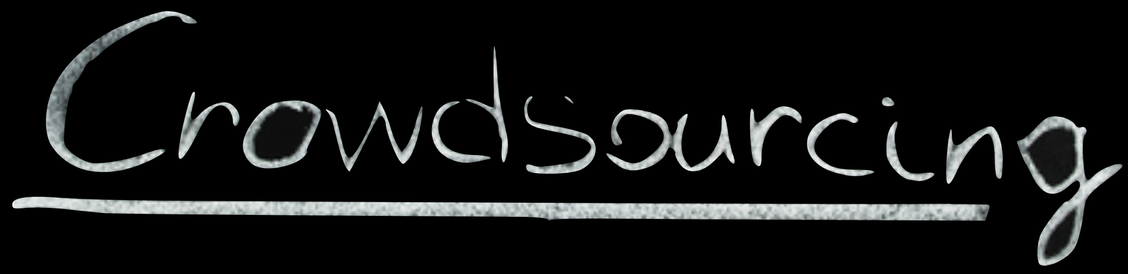
바로 **N번방의 현금화 자금 세탁**에 사용된 거래소 지갑 중 하나이다.


Hacker address
Relay
Upbit user wallet belong to suspect
0x5e0322

익명성을 쉽게 사용할 수 있다는 편의성이 가상 화폐 범죄를 증가시켰으나 블록체인 기술 자체의 근본적인 투명성은 범죄자가 보호받을 수 없는 강력한 증적 데이터를 입증한다. 공공의 데이터, 특히 위협 데이터는 다수의 참여로 인해 더욱 더 강력한 보호막을 형성할 수 있다.

사기, 자금세탁 , 해킹등의 가상 화폐 범죄 데이터는 온라인상에 주홍글씨로 남게 되지만 **이에 대한 강력한 단서를 제공할 수 있는 것**은 소수의 전문 보안인, 회사가 아닌 **가상화폐 일반 유저** 들이다.

따라서 정교하며 지능적인 가상화폐 금융 범죄는 **전세계 민간인 참여형 플랫폼 (크라우드 소싱)의 형태로서 발전 한다면 기술의 특성을 지렛대 삼아 효과적인 대응책으로 고려 될수가 있다.**



감사합니다.