한 번에 끝내는
블록체인 개발 A to Z

Chapter 1

Blockchain 1.0 - Bitcoin

Chapter 1

Blockchain 1.0 - Bitcoin

Bitcoin의 익명성

제한적인 익명성

❶ PKI를 이용한 익명성

Bitcoin의 익명성은 신원인증 없이 PKI를 이용해서만 거래를 하여, 사용자의 실제 신원을 숨기는 익명성을 제공한다.

❷ Key 재사용 제한

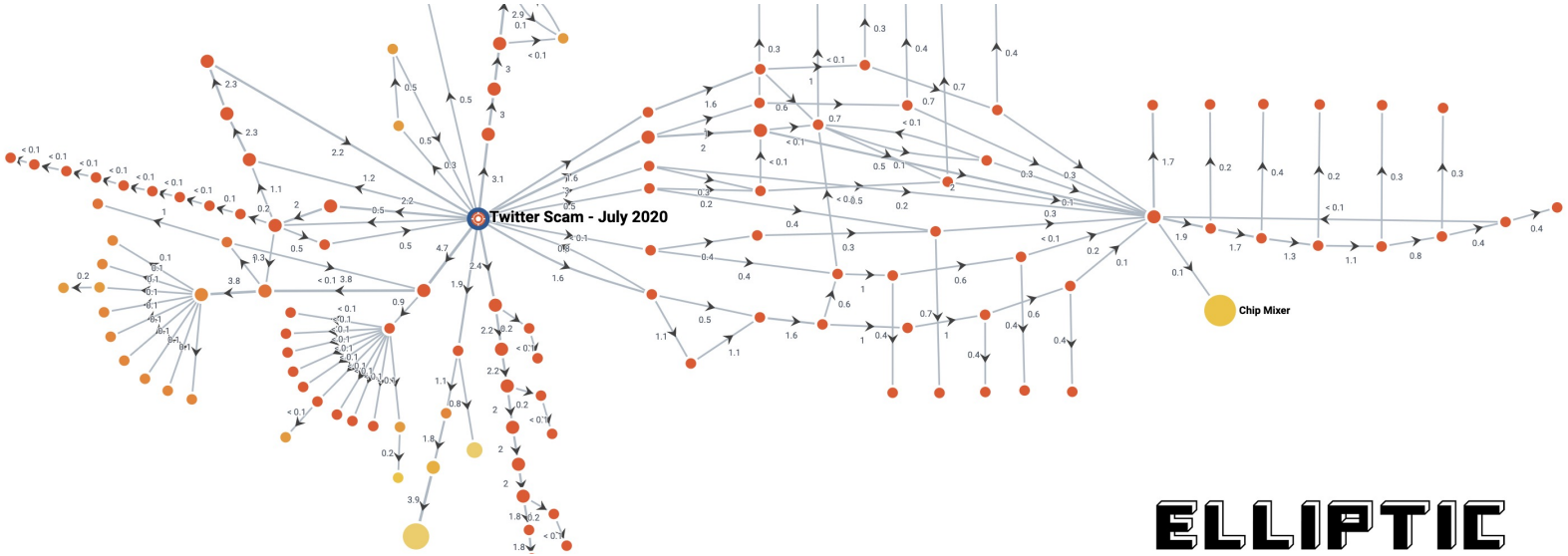
Bitcoin 공식 문서에서는 사용자의 익명성을 제한하기 위해서 Key(주소) 사용을 한번만으로 제한할 것을 권장하고 있다.

❸ Mixer

CoinJoin과 같은 코인 Mixer 기능을 통해 다른 사용자와의 거래에 나의 거래를 숨길 수 있는 기능을 제공하고 있다.

모든 기록이 공개된 Blockchain

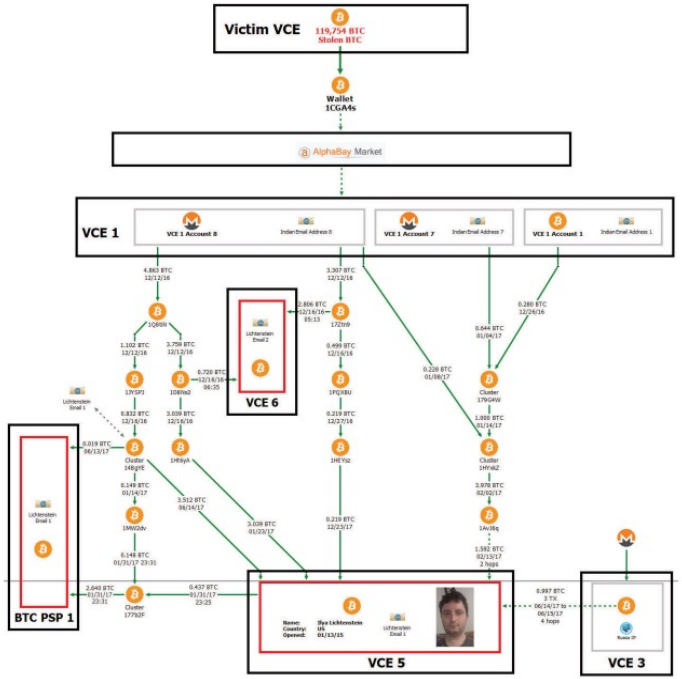
Bitcoin의 가장 큰 장점은 모든 거래 기록이 공개되어 있다는 점이다. 따라서 특정 시점부터 시작된 거래는 UTXO의 연결성에 따라서 거래를 따라갈 수 있다는 점이다. 사용자가 결국 fiat money로 환전할 때 신원이 공개 될 수 밖에 없다.



(출처 : elliptic 공식사이트)

Bitfinex
해킹 자금 회수

- 2017년 최대 거래소 중 하나인 Bitfinex에서 119,754 BTC가 해킹되었다.
- 현재금액으로 약 5조원 상당의 큰 피해금이었다. 하지만 FBI와 추적기관들의 노력으로 세탁업자 2명이 체포되고 훔친 자금 대부분은 국가에 귀속되었다. 이들은 세탁과정에서 세탁한 금액을 세탁소와 Uber등 본인의 신원이 들어날 수 있는 곳에서 사용하며 Bitcoin의 추적 결과와 신원 매핑을 통하여 검거될 수 있었다.



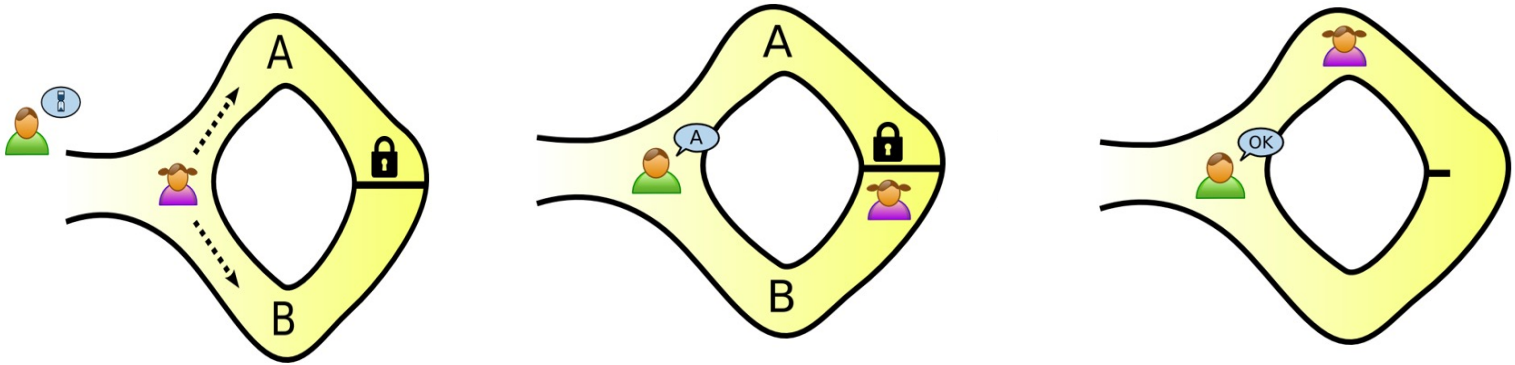
(출처 : USA 법무부)

Bitcoin Mixer(Tumbler)

- Bitcoin의 신원을 숨기는 방법 중 대표적인 것은 Exchange, Gambling Site를 통하거나 Mixer를 사용하는 것이다.
- Exchange, Gambling Site를 통한 세탁의 목적은 하나의 주소에 모든 사용자들의 거래를 Mixing 시키는 것이다.(offchain)
- On chain 상에서 Mixing 하는 방법은 그레고리 맥스웰이 제안한 CoinJoin과 같은 방법이 있다. Coinjoin은 여러 사용자의 input과 output을 하나의 거래로 만드는 것이다.
- Dash 라는 블록체인 플랫폼이 Coinjoin 기술을 통해서 익명성을 보장한다.
- Bitcoin Wallet 중에는 Wasabi Wallet이 Coinjoin을 지원한다.

ZKP

Zero Knowledge Proof(ZKP)은 대표적으로 블록체인에서 사용하는 Privacy 보호 기술로 Zcash 플랫폼에서 사용중이다.
나의 신원(서명과 공개키)를 공개하지 않고 나의 거래라는 것을 증명하는 기술이다.



(출처 : Wikipedia.org)

Travel Rule

Travel Rule 이란 중앙화 거래소에서 입금된 거래는 자금 세탁의 위험성이 있기 때문에, 거래소에서 사용자의 입출금을 실명으로 관리하는 것이다. 금융실명제와 동일한 효과를 볼 수 있다.

사용자는 Travel Rule로 인해서 특정 금액 이상의 입출금 발생시 상대방의 신원정보를 함께 등록하여야 출금이 가능하다.