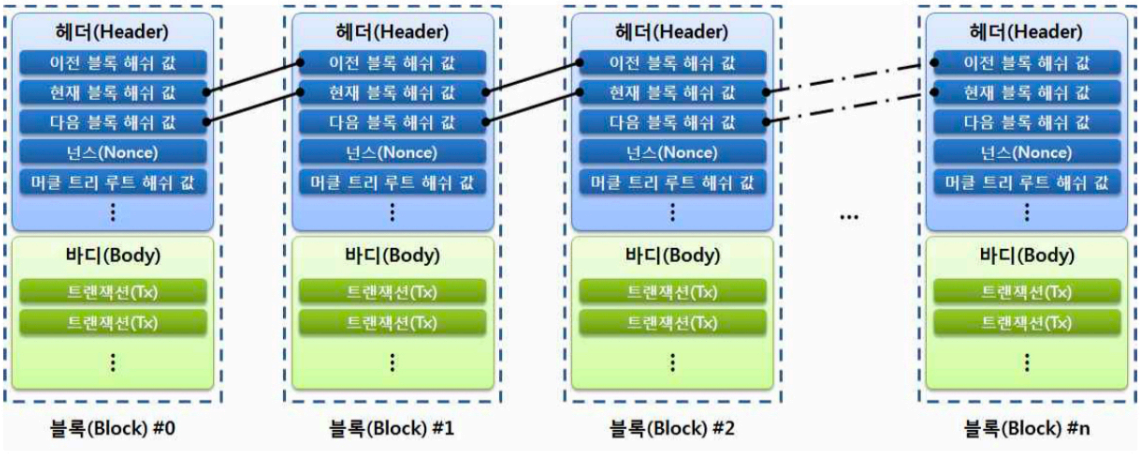
Bitcoin

취약점트랙-김학진

1. 비트코인 사용 이유

비트코인(Bitcoin)은 2009년 나카모토 사토시(Nakamoto Satoshi)가 제안한 전자 화폐로, 통화의 발행과 관리를 수행하는 중앙 기관이 존재하지 않는 구조를 가지고 있다. 대신, 비트코인의 거래는 P2P 분산 네트워크 기반 타임스탬프 서버에 의해 이루어지며, 공개키 암호 방식 기반으로 거래를 수행한다. 이전까지는 온라인상의 자금 거래에 항상 제3자(금융기관)의 신용을 바탕으로 한 개입이 필요했지만 비트코인은 이 과정을 불필요하게 만들었다. 비트코인은 시스템상에서 발생하는 모든 거래를 하나의 공개 장부에 기록하고, 장부는 분산되어 저장된다. 이 단일 장부를 '블록체인(block chain)'이라 한다. 새로운 거래가 발생하면 그 거래에 사용된 비트코인이 예전에 사용된 적이 있었는지 검증된다. 수만 명의 자발적 검증인(채굴자) 및 이용자들로 구성된 지구적 규모의 P2P 네트워크가 스스로 금융기관의 역할을 하게 되는 것이다.

< 블록체인 연결 구조 >



비트코인은 비트코인 주소에 등록된다. 비트코인 주소를 만드는 것은 임의의 유효한 개인키를 선택하고 해당 비트코인 주소를 계산하는 것이다. 하지만 역으로 계산은 수학적으로 불가능하기 때문에 사용자가 개인키를 손상시키지 않고 타인에게 비트코인 주소를 공개할 수 있습니다. 또한 유효한 개인키의 수가 너무 많아서 이미 누군가 사용중인 키 쌍을 계산하고 자금을 확보할 가능성이 매우 낮다. 각 블록은 헤더와 바디로 구성된 구조체로 헤더에는 이전, 현재 블록의 해시 값, 넌스(Nonce) 등을 포함하고 있으며, 블록 검색 시 데이터 베이스 인덱스 방식으로 데이터 값을 찾는다.

비트코인은 독립적인 글로벌 단일 화폐시스템이기 때문에 네트워크 상에서 이루어지는 거래는 페이팔이나 인터넷뱅킹과 달러 등으로 표시되지 않는다. 전 세계 어디서나 비트코인(BTC)을 화폐단위로 거래가 이뤄지고 금액이 표시된다. 이 화폐의 가치는 금 또는 국가 화폐에 비롯되는게 아니라 사람들이 부여한 가치만큼 평가되는 것이다. 비트코인은 인플레이션을 방지하기 위해 통화 발행을

2,100만개로 제한하였으면 비트코인에 대한 달러의 가치는 수요와 공급에 의해 공개 시장에서 결정된다.

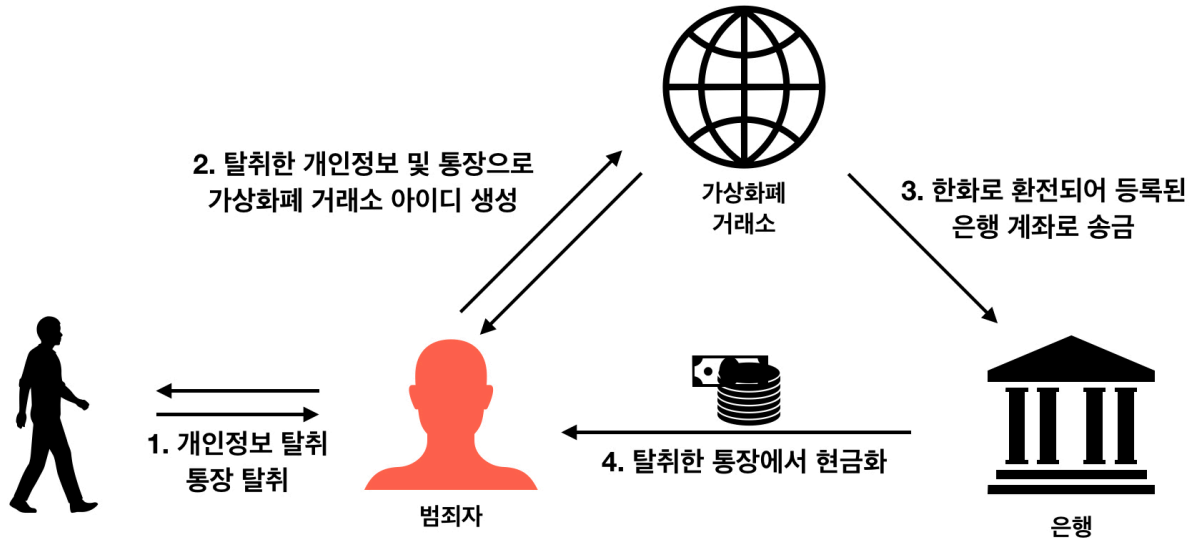
비트코인은 익명성이 보장된다. 즉, 자금이 실제 개인정보에 묶여 있지 않고, 오로지 비트코인 주소와 연결되어 있다.

이처럼 비트코인은 전 국 어디서나 거래가 가능하고, 제3이 신용기관 없이 P2P분산 네트워크를 이용하며 해당 비트코인 주소의 개인정보가 포함되지 않아 누구나 쉽게 사용할 수 있는 가상화폐이기 때문에 메리트가 있다.

2. 불법 비트코인 현금화 시나리오

만약 불법적인 특정 행위를 통해 비트코인을 습득하였다면, 현금화 시키는 방법에는 어떠한 것들이 있을까? 비트코인 기술만을 살펴보면 비트코인의 주소에는 어떠한 개인정보(주민번호, 이름, 주소 등...)도 들어가 있지 않다. 하지만, 우리는 이러한 비트코인을 보다 쉽게 사용하고, 거래하기 위해 '가상화폐 거래소'라는 제3의 서비스를 이용하게 된다. 자신의 비트코인을 쉽게 거래 하기 위해 해당 거래소의 가입을 해야 하며 이때 결국 자신의 개인정보가 들어가게 된다. 또, 해당 거래소의 자신의 계좌를 등록하는 과정에서 본인 인증 과정이 있다. 또한 해당 아이디에 자신의 비트코인 주소를 입력하거나, 해당 거래소에서 비트코인 주소를 발급받게 되므로 비트코인 주소로 추적 가능하다. 따라서 거래소 이용이 필수적이라면, 다른 방법을 이용하여 추적을 회피하여야 한다.

1) 대포 비트코인 주소



오프라인 상에서 일어나는 범죄 행위들을 살펴보면 대포통장을 이용하여 경찰의 추적을 회피하는 일들이 많다. 이를 가상화폐에도 적용시키면 어떨까? 본인의 경험으로 네이버 '중고나라'라는 카페에서 중고 물품을 구매 하기 위해 대상자에게 소정의 금액을 입금시켰지만, 물품을 받지 못했다. 경찰에 신고하여 조사한 결과 범죄자는 대포 통장을 사용 하고 있었다. 해당 대포 통장은 노숙자들에게 소정에 돈을 지불하는 대신 노숙자의 통장과 통장 비밀번호를 구매하여 만들어진 통장이었다. 당장 먹고 사는것이 시급한 노숙자들의 심리를 이용한 범죄였다. 즉, 다른 사람의 명의로 된 통장을 사용하기 때문에 추적에 어려움이 생기게 된다. 이를 적용하여 일련의 금액을 지불하고 다른 사람의 명의로 가상화폐 거래소의 아이디를 만들고, 대포통장을 활용하여 현금화 시킬 수 있다. 이런 메커

니즘을 단일화 하지 않고, 중간 단계에 또 다른 대포 비트코인 주소 등을 얽히고 얽히게 만들면 더욱 추적가능성이 줄어들지 않을까 생각한다.

2) 타 가상화폐 이용

가상화폐 거래소에는 비트코인 뿐만 아니라 리플, 비트코인캐시, 이더리움 등.. 수많은 가상화폐들을 취급하고 있다. 가상화폐간의 환전을 굉장히 쉽게 이루어 질 수 있는데, 여기서 환전이 일어나게 되면 비트코인의 특성에서 환전되는 가상화폐의 특성으로 변환된다고 할 수 있다. 예를들어 비트코인을 대시코인으로 환전한다고 할때, 비트코인은 블록체인에 사용 기록, 보낸 기록, 수량 등의 모든 정보를 등록하는 반면, 대시코인은 마스터노드를 통해 프라이빗센드(PrivateSend) 기술이 적용되어 있다. 프라이빗센드 기술이란 수신자와 발신자 및 거래 정보를 모호하게 하여 익명성을 강화하는 기술이다. 이렇게 비트코인의 특성에서 대시코인의 특성으로 변화되면서 그 과정에서 익명성이 강화되는 효과를 볼 수 있다. 이처럼 특성이 다른 가상화폐들로 환전하는 작업을 수차례 거치고, 가상화폐거래소 또한 한 나라에 국한되지 않고 해외 여러 거래소를 거치면서 환전이 이루어지면 추적이 어렵지 않을까 생각한다.

이처럼 오프라인 상에서의 추적을 피하기 위한 범죄행위들을 복합적으로 조합하여 범죄가 일어나게 되면 단순히 온라인 상에서의 추적으로 끝나는 것이 아니라 온오프라인 전반에 걸쳐 합동적으로 조사가 이루어져야 하기 때문에 추적을 매우 까다롭고 어렵게 만들 수 있다고 생각된다.

3. 비트코인 추적 가능성

선진국에서는 블록체인을 분석하여 비트코인 거래를 시각화해 보여주는 기술들이 개발되고 있다. 체이널리시스(Chainalysis), 코인애널리틱스(Coinanalytics), 블록시어(Blockseer), 엘립틱&스코어체인(Elliptic&Scorechain)등이 있다. 앞서 말한것처럼 비트코인은 블록체인 안에 사용 기록, 보낸 기록, 수량 등의 모든 정보를 등록하게 된다. 체인널리시스의 리액터는 비트코인 지갑 주소를 기반으로 한 입출금 거래내역 분석 솔류션으로서, 지갑 주소를 넣으면 자동으로 해당 지갑의 모든 거래내역 로그를 손쉽게 분석할 수 있다. 하지만 이것 만으로 현실세계와 연결되지 않는다. 체인널리시스의 올리세 델로르토(Ulisse Dellorto)은 "비트코인이 모든 거래내역을 갖고 있지만 현실세계의 정체성과 연결되어 있지 않으며, 실제 엔티티(Entity) 참조가 없다"고 설명했다. 하지만 모든 가상화폐 거래소와 정보 공유, 오픈소스를 이용하여 웹에서 정보를 스크랩, 전문분석가 팀이 거래내용을 분석 등 3가지 전략을 이용하면 비트코인 거래내역과 현실 세계의 엔티티 정보를 분석할 수 있다고 한다.

Reference

[1] Nakamoto Satoshi, “Bitcoin: A Peer-to-Peer Electronic Cash System”, http://www.bitcoin.org, 2008.

[2] 비트코인 (위키피디아), http://en.wikipedia.org/wiki/Bitcoin, 2018. 07. 13. 확인

[3] 금융보안원 보안연구부 보안기술팀, "블록체인 및 비트코인 보안 기술", 2015.11.23

[4] 대시(Dash) - TokenPost ,https://tokenpost.kr/terms/11141, 2018. 07. 13. 확인

[5] 보안뉴스, "가상화폐 산업 지각변동... 비트코인 추적 가능해졌따", http://www.boannews.com/media/view.asp?idx=66953, 2018. 02. 21