랜섬웨어와 비트코인

BoB7기 취약점분석 정성조

# Bitcoin: A Peer-to-Peer Electronic Cash System Summary

(<https://bitcoin.org/bitcoin.pdf>)

인터넷에서의 상거래는 제 3자를 신용기관으로 하는 전자지불 방식에 전적으로 의존한다. 제 3자가 있기 때문에 거래를 취소하려고 할 때 중재 비용이 발생하고 최소 거래금액을 제한하고, 이는 결국 더 많은 비용을 발생시킨다. 이는 신용 기관이 존재하지 않는 암호 화폐를 이용하여 해결할 수 있다.

소유자들은 전까지의 거래 내역에 다음 소유자의 공개키를 덧붙인 뒤 비밀키로 암호화하여 디지털 서명을 한다.

이중지불을 막기 위한 공통적인 해법은 신용할 수 있는 중앙 기관을 도입하는 것이다. 중앙 기관에 모든 거래 내역이 걸쳐가도록 하는 것이다. 하지만 이는 제 3자를 만들어낸다.

중앙 기관을 도입하지 않고도 이런 방법을 가능하게 하기 위해서는, 모든 거래가 공개적으로 알려져야 하고 시간 순서에 따라 단일한 거래내역으로 수용하는 시스템이 필요하다.

타임스탬프 서버는 시간 내역이 기록된 항목들의 블록의 해시값과 전 블록의 해시값을 통해 해시를 만들어 발행하는 역할을 한다.

타임스탬프 서버를 구현하기 위해서는 작업증명 시스템이 필요하다. 작업증명은 다수의 0비트들로 시작되는 암호화 해시값을 찾는 과정이 포함되어 있다. 이는 0비트의 요구 개수에 따라 지수적으로 증가한다. Nonce값을 1씩 증가시키며 찾기 때문이다. 하나의 블록을 변경하기 위해서는 그 블록을 포함한 다음 모든 블록들에 대해 작업 증명 과정을 다시 수행해야 한다.

네트워크는 새로운 거래 내역이 모든 노드에 알려지고 작업 증명이 성공적이라면 모든 노드에게 블록을 전송하고 수신한 노드가 사용되지 않은 노드라면 승인한다. 그 후 수신한 노드의 해시 값을 이용하여 다음 노드를 만든다.

# 랜섬웨어 감염자에게 돈을 받아야 한다. 어떻게 받아야 안잡힐까?

현금으로 받는다, 계좌이체로 받는다 등의 여러가지 방법이 있겠지만 신원이 노출된다. 나는 이에 대한 방법으로 “비트코인”이라는 전자 화폐를 이용할 것이다.

# Why bitcoin?

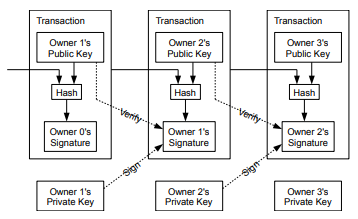


그림 1. 트랜잭션 (출처: <https://bitcoin.org/bitcoin.pdf>)

비트코인의 트랜잭션은 위와 같은 과정을 통해 진행된다. A가 B에게 50BTC를 전송하는 상황을 예로 들어보자. A는 먼저 트랜잭션 블록을 만든다. 해당 블록에는 이전 거래 내역을 가지고 있는 해시값과 받는 주소(B) 받는 금액(50BTC), 고유 일련번호가 저장되어 있다. 그 후 A의 비밀키로 전자 서명을 한 후 블록체인 네트워크에 브로드캐스트 한다. 작업 증명 과정에서 nonce 값을 증가시키며 target을 만족하는 해시값을 구한다면 모든 블록에 해당 블록이 저장된다. 이를 수신한 노드들은 해시 값을 비교하여 소비되지 않은 블록인지 확인한다. 해당 블록이 만들어지고, B는 A의 블록을 받고 A의 공개키로 서명을 본 후, A가 맞다는 것을 확인하고 A블록의 해시값을 이용하여 블록을 만든다.

먼저, 트랜잭션 과정을 보면 개인정보는 들어가 있지 않으며 주소 값을 통하여 통신한다. 이 주소 값은 랜덤으로 생성되기 때문에 개인정보가 아니다. 하지만 사용자가 제품이나 서비스를 제공받기 위해서는 신원을 제공해야 하기 때문에 계속해서 같은 주소를 사용하는 것보다는 계속해서 다른 주소를 써주는 것이 익명성을 보장하는데 도움이 된다.

모든 비트코인 거래는 공개되며 해시값을 통해 추적이 가능하다. 그렇기 때문에 자금 추적을 피하기 위해 지캐시나 모네로 코인이 존재한다. 지캐시는 제로 knowledge 이론을 사용하기 때문에 추적이 불가능한 암호 화폐이다. 이를 통해 거래소(빗썸)에서 현금화 인출을 시도할 것이다.