정 보 보 호 학 회 지
제26권 제2호, 2016. 4

비트코인의 신뢰구조와 이중지불의 위협

이 혁 준*, 이 수 미*

요 약

비트코인(Bitcoin)은 P2P 네트워크상에 존재하는 실물 없는 화폐이다. 비트코인의 특징은 발행 기관의 통제가 없는 분산 구조를 형성하고 네트워크가 연결된 곳 어디에서나 거래가 이루어질 수 있도록 신뢰성을 부여하고 있다는 것이다. 이러한 특징의 비트코인은 최초 등장 이래 하루 평균 약 21만 건, 1억 7천만 달러가 거래되는 규모로 성장했다. 화폐로서의 가치가 증가함에 따라 부당 이득을 취하려는 위협 또한 증가하게 될 것이다. 대표적으로 비트코인을 위협하는 행위로는 이중 지불, 부정 인출 등을 그 사례로 볼 수 있다. 하지만 아직까지 성장 단계에 있는 비트코인을 대상으로 발생될 수 있는 위협에 대한 인지는 부족한 실정이다. 이에 본 논문에서는 비트코인 신뢰 구조를 살펴보고 이를 기반으로 발생할 수 있는 다양한 위협들을 분석하고 대응방향을 제시하고자 한다.

Ⅰ. 서 론

비트코인은 2009년 1월 사토시 나카모토에 의해 최초로 채굴된 이후 거래량이 지속적으로 증가하면서 가상화폐분야에서 선도 기술로 대두되었다. 2016년 3월 현재, 일평균 약 21만 건, 금액으로는 약 1억 7천만 달러의 거래량을 보이고 있다. 기존 통화의 중앙 집중화 구조와 달리 분산화 구조로 이루어진 비트코인은 분산화 구조를 기반으로 안전성, 투명성 등의 신뢰기능을 제공한다. 이러한 비트코인의 신뢰구조는 블록체인이라는 기술에 기반하고 있는데 블록체인은 공개된 거래 장부의 집합으로 장부 간의 연결고리(chain)가 신뢰성의 근간을 마련해 준다. 즉 블록체인 기술은 네트워크상에서 발생된 비트코인의 거래내역(거래장부)을 고리로 연결하고 연결고리 중간에 거래내역 삭제, 삽입 등이 발생되지 않도록 암호학적 방식을 제공하여 비트코인 거래에 대한 신뢰성을 제공하고 있다.

블록체인 기술은 비트코인에서 시작해 해외 송금, P2P 대출, 거래 인증, 주식 거래 등 핀테크 기술과 융합해 다양한 분야에 활용되고 있는데 그 사례로 미국의 나스닥은 비상장 기업들의 주식 거래를 위한 플랫폼인 링크에 사설(private) 블록체인을 도입하여 체인닷컴(chain.com) 등 비상장기업 6개社의 주식을 대상으로 전자 증권 발행 서비스를 실시한 바 있다〔4〕.

비트코인은 비트코인 거래소를 통해 원화를 비트코인으로 환전하거나 비트코인을 원화로 환전할 수 있다. 국내에서는 코빗, 빗썸, 코인플러그, 코인이즈 등의 비트코인 거래소가 운영 중이다. 거래소를 통해 얻은 비트코인은 송금 받는 사람(수신자)의 주소만 알면 전 세계 누구에게나 송금할 수 있으며 해당국 거래소에서 해당국 통화로 환전이 가능하다. 세계적으로 유로(EUR), 미국 달러(USD), 중국 위안(CNY) 등을 포함한 20종 이상의 화폐에 대한 거래가 제공되고 있다. 이처럼 글로벌 화폐로서 가치가 있는 비트코인의 성장에 따라 다양한 방식으로 부당 이익을 취하려는 시도 또한 증가될 것으로 예상된다.

일반적으로 비트코인에 대한 위협으로는 암호학적 절차를 우회하기 위해 기밀정보인 개인키를 탈취하여 부정인출을 시도하거나 사용한 비트코인을 재사용하는 이중 지불(Double spending) 위협이 대표적이다. 그 사례로 거래소를 공격해 개인키를 탈취하고 비트코인을 부정 인출하는 사례가 이미 여러 차례 발생해 왔다[5]. 위협 중 특히 이중 지불은 분산화라는 비트코인 구조적 특징에 기인한 위협으로 다양한 방식이 존재할 수 있다. 본 논문에서는 비트코인의 구조적 특징을 기반으로 이중 지불 방식을 예측하고 대응방향을 제시하고자 한다.

* 금융보안원 보안연구부 핀테크보안팀 (hjlee@fsec.or.kr)

Ⅱ. 비트코인의 주요 거래절차

실물 화폐 거래의 경우 화폐를 주고받음으로써 거래가 이루어지는데 반해, 가상화폐인 비트코인은 화폐를 주고받은 기록인 거래내역을 비트코인 거래장부 (블록체인)에 기록함으로써 거래가 이루어진다 [1]. 비트코인 거래에 필요한 지갑 프로그램 설치부터 거래내역이 블록체인에 포함될 때까지 주요 거래절차를 차례대로 살펴보고자 한다.

2.1. 지갑설치 및 주소생성

비트코인 거래를 위해서 지갑 프로그램을 확보해야 한다. 프로그램 설치 형태 또는 웹서비스 형태의 지갑프로그램 등이 사용 가능하다. 지갑 프로그램은 비트코인 거래를 위한 열쇠인 개인키와 돈을 받을 때 수신자의 주소가 되는 공개키를 생성한다.

2.2. 송금지시

송금하고자 하는 사람은 자신의 지갑 프로그램을 이용해 송금 거래내역을 작성하고 자신의 지갑에 있는 개인키를 이용해 거래내역에 서명한다.

송금 거래내역에는 송신자가 이전에 비트코인을 수신했던 거래내역의 해쉬 값(Previous tx)과, 송금하고자 하는 비트코인 금액(Value) 그리고 수신자의 주소(공개키, scriptPubKey)가 포함된다. 거래내역 작성이 완료되면 지갑 프로그램은 송신자의 개인키를 사용해 거래내역에 대한 전자서명(scriptSig)을 생성한다.

[표 1] 송금 거래내역 예

Input: Previous tx: f5d8ee39a430901c91a5917b9f2dc19d6d1a0e9cea205b009ca73dd04470b9a6 Index: 0 scriptSig: 304502206e21798a42fae0e854281abd38bacd1aeed3ee3738d9e1446618c4571d1090db022100e2ac980643b0b8 2c0e88ffdfec6b64e3e6ba35e7ba5fdd7d5d6cc8d25c6b241501 Output: Value: 5000000000 scriptPubKey: OP_DUP OP_HASH160 404371705fa9bd78 9a2fcd52d2c580b65d35549d OP_EQUALVERIFY OP_CHECKSIG

2.3. 송금지시 발송

지갑프로그램을 통해 거래내역에 서명을 완료하면 지갑 프로그램은 거래내역과 서명 값을 인접 노드에 전파하고, 최종적으로는 전체 비트코인 네트워크에 전파된다.

2.4. 송금지시 검증

비트코인 네트워크로 전파된 거래내역은 다수의 채굴자에게 도달하게 되며, 거래내역을 수신한 채굴자들은 해당 거래내역에 대해 검증을 수행한다. 검증은 크게 송금액 검증과 송신자 및 거래내역 무결성 검증으로 구분된다. 송금액 검증은 블록체인에 기록된 과거 거래내역을 참조해 송금액의 존재 여부를 확인하는 것이며, 송신자 및 거래내역 검증은 거래내역에 포함된 전자서명 값(scriptSig)을 확인(verify)하여 거래내역 및 송신자를 검증하는 것이다.

2.5. 블록 생성 및 배포

검증을 마친 채굴자 중 채굴에 성공한 채굴자는 자신이 검증한 거래내역을 포함시킨 블록을 생성하게 된다. 생성한 블록의 헤더에는 논스, 타임스탬프, 이전 블록의 헤더에 대한 해쉬 값, 생성된 블록에 포함될 거래내역 집합의 해쉬 값 등이 포함되게 된다. 블록은 송금지시의 집합과 블록헤더로 구성된다.

2.6. 블록체인 생성 및 공유

채굴된 블록은 해당 노드가 보유중인 블록체인에 연결된다. 채굴자를 포함한 노드들은 각자 자신이 가지고 있는 블록체인의 길이를 주변 노드들에 공유하고 있는데, 신규 블록이 채굴되어 블록체인에 연결되면 1만큼 길어진 블록체인 길이가 주변 노드에 공유되며 보유중인 블록체인의 길이가 상대적으로 짧은 주변 노드들은 새롭게 생성된 블록을 전달받게 된다.

Ⅲ. 비트코인의 신뢰구조

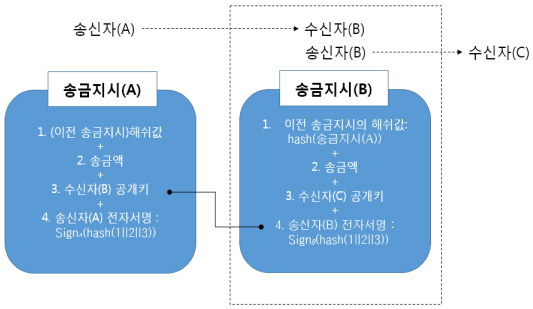
비트코인의 신뢰구조는 크게 전자서명, 해쉬로 구성

된 연결구조 그리고 검증 주체에 대한 비용지불로 이루어진다 [2].

3.1. 송신자, 수신자 및 거래내역의 무결성 검증

채굴자는 거래내역에 포함된 전자서명으로 송신자와 거래내역의 무결성을 검증한다. 이를 위해서 블록체인에 기록된 과거 거래내역을 참조해 과거 거래내역에 기록된 수신자 주소가 현재 거래내역에 기록한 송신자의 전자서명과 일치하는지 검증해 송신자의 정당성을 확인한다.

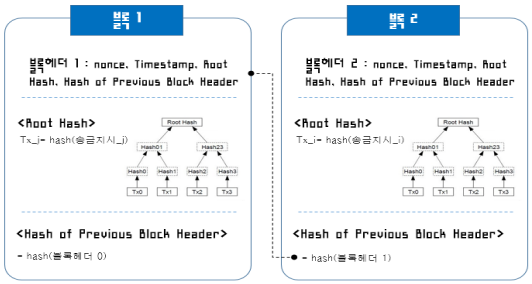
송금지시(A)에 있는 B의 공개키로 송금지시(B)에 있는 송신자(B)의 전자서명을 검증한다. 전자서명 절차는 개인키를 이용한 전자서명 생성과 공개키를 이용한 전자서명 검증으로 구성되며 개인키와 공개키는 한 쌍(pair)로 구성된다. 개인키를 소유한 자(B)가 생성한 전자서명임을 검증하는 과정은 B의 공개키와 전자서명을 검증 알고리즘에 입력하여 실패(Fail) 또는 성공(Success) 결과를 확인함으로써 이루어진다. 이러한 검증 절차는 비트코인을 받은 송신자(B)가 다음 수신자(C)에게 비트코인을 보낸 자이고 거래내역 생성 주체(B)임을 확인하는 과정이다. 또한 전자서명은 송금지시 내역의 해쉬 값에 대해 생성되기 때문에, 전자서명의 정확성이 확인된다면 송금지시 내역의 변조 여부에 대한 확인도 함께 이루어지게 된다. 노드와 채굴자는 전자서명을 검증해 불일치하는 경우 해당 거래내역 또는 해당 거래내역이 포함된 블록과 블록체인을 거절한다.



[그림 1] 송수신자 검증

3.2. 연결구조기반 블록체인의 무결성 검증

블록체인은 해쉬 기반 트리(Tree) 구조와 연결리스트(Linked List) 구조로 이루어져 있다. 이러한 구조를 통해 임의적인 거래내역과 블록의 삽입 또는 삭제가 이루어질 경우 선의의 노드 및 채굴자가 적은 비용으로 임의적 삽입 및 삭제 여부를 발견할 수 있다.

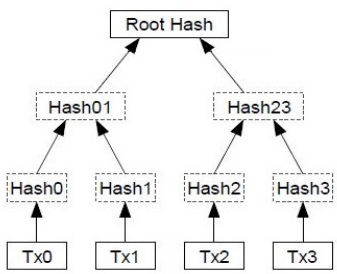


[그림 2] 블록간 연결구조 기반 블록체인 형성

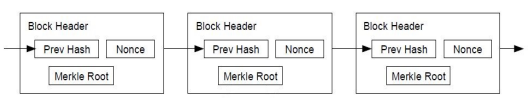
머클트리(Merkle Tree)의 루트해쉬(Root Hash)는 블록마다 1개씩 존재하며 트리구조에서 송금지시를 최하위 노드로 하여 계산된 값인 루트해쉬를 통해 송금지시의 무결성 검증 기능을 제공한다.

블록 생성 시 머클트리의 루트 값이 정해져 블록에 기록되며, 임의로 특정 거래내역을 변조할 경우 머클트리의 루트 값과 불일치하게 되기 때문에 탐지할 수 있다. 블록의 헤더에는 바로 이전 블록의 헤더에 대한 해쉬 값이 기록되어 있어 블록을 연결하고 있다.

노드와 채굴자는 이전 블록 헤더를 해쉬해 블록의 헤더에 기록된 이전 블록의 해쉬 값과의 일치 여부를 확인함으로써 블록의 삽입·삭제를 확인한다. 불일치 시 해당 블록 및 블록체인을 위변조된 것으로 판단해 거절한다.



[그림 3] 머클트리



[그림 4] 블록체인 연결리스트

3.3. 비용지불에 따른 성실한 검증 유도

비트코인 네트워크는 채굴 난이도 조정을 통해 채굴 환경 구축에 고비용을 부여하고 채굴 성공 시 높은 보상을 제공함으로써 채굴자의 성실한 검증을 유도한다.

블록 채굴에 성공하기 위해서는 특정 값(Nonce)를 찾아야 하는데 이를 찾기 위해서는 고비용은 연산을 수행해야 한다. 2016년 3월 초당 $1,292\times10^{15}$회 해쉬 연산을 10분간 수행해야 하며 특정 값을 찾는 연산에 성공한 채굴자에게 25_{BTC}가 보상으로 지급된다. 채굴자가 거래내역 검증을 미흡하게 하였을 경우 채굴에 성공해 해당 거래내역이 포함된 블록을 생성하더라도 비트코인 네트워크상의 다른 노드들이 해당 거래내역을 검증해 오류를 발견하고 블록을 거절하기 때문에 채굴자에 지급된 보상은 인정받지 못한다. 따라서 채굴자는 미흡한 검증으로 인해 자신이 받은 보상이 인정받지 못하는 상황을 방지하기 위해 거래내역을 성실히 검증하게 된다. 분산 환경의 특징으로 인해 노드 간 블록체인 마지막의 일부 블록들이 상이한 경우가 발생할 수 있다. 이처럼 서로 다른 블록체인을 가진 노드로부터 블록체인 정보를 업데이트해야 하는 경우 노드들을 보다 긴 블록체인을 신뢰한다. 상대적으로 긴 블록체인을 받아들이도록 시스템을 구성한 것 또한 검증에 더 많은 비용을 사용한 블록체인이 악의적인 조작 가능성이 더 낮을 것이라는 것을 전제로 하고 있다.

Ⅳ. 비트코인의 이중지불(Double Spending) 위협 유형

비트코인에 대한 위협은 크게 송금을 지시할 때 전자서명 생성에 사용되는 개인키에 대한 위협과 송금지시 거래내역의 블록체인 포함에 대한 위협으로 나눌 수 있다.

4.1. 비트코인의 일반적 보안 위협

비트코인에 대한 위협 중 개인키 탈취 및 이로 인한 부정인출이 있다. 개인키를 획득하면 송금지시 전자서명 생성이 가능하기 때문에 비트코인 거래소나 지갑 프로그램을 공격해 저장된 개인키를 획득한 후 비트코인을 인출하는 공격 사례가 다수 있다. 실례로 2014년 12월 비트스탬프라는 거래소 서버가 공격당해 개인키가 유출되었으며 이로 인하여 18,866BTC가 도난당하기도 했다. 거래소나 지갑 프로그램에 저장된 개인키가 직접적으로 유출되지 않더라도 개인키 복구정보를 통해 개인키가 유출되는 경우도 있을 수 있다. 개인키 생성 시 분실에 대비해 복구 정보를 저장해놓는 경우가 있는데 복구 정보를 안전하지 않은 장소에 저장해둘 경우 이를 탈취 당하면 복구정보가 유출된다. 복구정보를 이용하면 개인키를 복구할 수 있고 복구한 개인키로 송금을 위한 전자서명을 생성할 수 있다. 송금 거래내역이 블록체인에 포함되지 못하도록 하는 위협도 있다. 비트코인으로 지불 받기로 한 재화 공급자가 송금 거래내역을 보고 비트코인을 받았다고 생각해 재화를 공급하지만 최종적으로는 송금 거래내역이 블록체인에 포함되지 않을 수 있는 가능성이다. 이러한 위협을 현실화 시키는 것이 이중지불 공격이다.

4.2. 비트코인 구조에 기반한 이중지불 공격 유형

이중지불 공격은 공격자가 기 지불된 비트코인을 회수하거나 재지불하여 거래를 완료하는 것으로 최종적으로는 지불받지 못한 자의 손실이 발생하게 된다. 공격은 크게 두 가지 방식으로 이루어지는데 블록체인에 송금지시가 포함되는 것을 방해하는 방식(미승인형)과 송금지시가 블록체인에 포함되었으나 이를 제거하는 방식(승인형)이다.

미승인형 공격은 돈을 받는 사람이 해당 거래내역이 블록체인에 포함되었는지 여부를 확인하지 않을 경우 발생할 수 있는데 레이스(Race) 공격, 피니(Finney) 공격 등이 있다.

4.2.1. 레이스 공격

비트코인 수신자가 승인 (블록체인 내 거래내역의 포함여부) 하지 않고 거래를 완료할 때 가능한 공격으로 공격자 (송신자 역할)는 다른 수신자에게 거래를 발생시키고 해당 거래내역을 블록체인에 포함시키면 공격에 성공하게 된다. 즉 공격자 입장에서는 이중지불된 거래내역이 정상 거래내역보다 먼저 채굴에 성공하여 블록체인에 포함시켜야 한다. 따라서 공격자는 이중지불 거래내역을 네트워크에 먼저 전파시켜야 한다.

4.2.2. 피니 공격

공격 성공 확률을 높이기 위해 공격자는 직접 채굴을 수행하여 이중지불 거래내역에 대해 블록을 생성한다. 먼저 공격자는 이중지불 거래내역이 포함된 블록을 생성하고 대기하고 정상 지불이 발생하면 공격자는 사전 계산된 블록을 블록체인에 포함시켜 정상 지불 내역보다 빠르게 전파가 가능하게 된다. 공격을 성공시키기 위해 공격자는 고비용을 지불하여 채굴환경을 구축할 때 성공확률이 높아진다.

다음 승인형 공격은 돈을 받는 사람이 해당 거래내역의 블록체인 포함 여부를 확인하는 경우 공격자가 고비용의 채굴환경 구축하여 블록체인에 포함되었던 거래내역을 제거하는 공격이다. 승인형 공격을 위해서 공격자는 상충된 긴 블록체인을 새롭게 생성해야 하며 이를 위해서는 고비용의 채굴환경이 필요하다 [3]. 승인형 공격으로는 무작위 공격 (Brute Force Attack), >50% 공격, <50% 공격 등이 존재한다.

4.2.3. 무작위 공격

상당한 해쉬 속도를 보유한 공격자가 부당한 거래내역이 포함된 블록체인에 비해 채굴을 계속하여 해당 블록체인의 길이가 정당한 거래 내역이 포함된 블록체인의 길이보다 길어지는 순간 네트워크에 전송하는 공격으로 만일 공격자의 해쉬 속도가 충분치 못하여 블록체인에 대한 채굴이 더디게 진행되는 경우 공격을 포기하게 된다.

4.2.4. >50% 공격

공격자의 채굴성능이 전체 네트워크 채굴 성능의 50% 이상을 갖고 있을 때 가능한 공격으로 무작위 공격 방식과 동일이다. 공격자는 50% 이상의 해쉬 속도를 사용해 충분한 시간 동안 이중지불 거래내역을 블록체인에 포함시키기 위해 기존 블록체인과 상충된 긴 블록체인을 새로 생성하여 공격을 시도한다.

4.2.5 <50% 공격

공격자의 채굴성능이 전체 네트워크 채굴 성능의 50% 미만을 갖고 있을 때 비트코인 네트워크 단절시켜 채굴성능을 50%이상으로 끌어올리는 방식이다.

Ⅴ. 비트코인의 이중지불 위협에 대한 대응

미승인형 공격의 경우 1회 이상의 승인횟수 확보를 통해 방어가 가능하며 승인형 공격의 경우 블록체인 및 비트코인 네트워크 모니터링을 통해 피해를 예방할 수 있다.

5.1. 충부한 승인 횟수 확보

승인 횟수가 1회 증가할 때마다 블록체인에 포함된 거래내역 위변조가 급격히 어려워지는 비트코인 블록체인의 특성을 활용해 충분한 승인 횟수를 확보하여 이중지불에 대응할 수 있다.

거래의 중요도에 따라 거래 완료 전 확인할 승인 횟수를 조정하여 채굴자에 의한 승인형 공격을 방지한다.

5.2. 블록체인 모니터링

비트코인 블록체인이 공개되어 있다는 특성을 활용해 네트워크 전체의 채굴속도 및 채굴 주체별 채굴속도 점유율 등 거래의 안전성에 영향을 미칠 수 있는 요소들을 모니터링 한다. 이러한 모니터링을 통해 위협이 발견될 경우 이를 공개적으로 알려 잠재적 악성 채굴자들을 견제하고 선의의 참가자들이 거래연기, 중지 등 스스로를 보호할 수 있도록 한다.

5.3. 대규모/장시간 네트워크 단절에 대한 대응

대규모 네트워크 장애가 발생하여 장시간 단절된 경우, 단절된 네트워크에 각기 포함된 채굴자들은 서로 다른 블록체인을 생성하게 된다. 이 경우 단절이 해소된 후 길이가 짧은 블록체인은 거절되게 되는데, 네트워크 단절 발생 시 거래 완료를 연기하거나 거래를 취소해 이러한 사태로 인해 피해를 보는 상황을 예방할 수 있다.

Ⅵ. 결 론

다양한 이중지불 공격유형이 존재하지만, 거래 시 1회 이상의 승인을 확인함으로써 상당 부분의 공격에 대해서는 방어가 가능하다. 일부 공격의 경우 네트워크 내

최장 블록체인 승인이라는 비트코인의 구조적인 문제에서 기인하기 때문에 기술적 방어가 불가능하다. 모든 거래 정보가 투명하게 공개된 비트코인의 특성을 활용해 선의의 참가자가 지속적으로 모니터링하고 이를 적극적으로 공유함으로써 거래의 안전성을 확보해 나가야 한다.

참 고 문 헌

[1] 안드레아스 M. 안토노풀로스, "*비트코인, 블록체인과 금융의 혁신*", 고려대학교 출판부, 2015

[2] Satoshi Nakamoto, "Bitcoin: A Peer-to- Peer Electronic Cash System", November 2008

[3] Meni Resenfeld, "Analysis of hashrate-based double-spending", February 2014

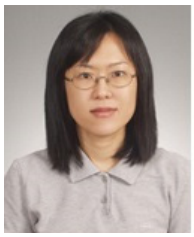
[4] 금융보안원 보안기술팀, "블록체인 활용사례로 알아보는 금융권 적용 고려사항", 전자금융과 금융보안, January 2016

[5] Tyler Moore, Nicolas Christin, "Beware the Middleman: Empirical Analysis of Bitcoin-Exchange Risk", Financial Cryptography and Data Security, 2013

〈저 자 소 개〉

이 혁 준 (Hyukjoon Lee)

2006년 2월 : 한국과학기술원 전산학과 졸업
2006년 2월~2015년 4월 : 금융결제원 금융ISAC부
2015년 4월~현재 : 금융보안원 보안연구부 과장
<관심분야> 정보보호, 트러스티드 컴퓨팅, 블록체인



이 수 미 (SooMi Lee)
정회원

2006년 2월 : 고려대학교 정보보호대학원 박사
2005년 12월~현재 : 금융보안원 보안연구부 팀장
2010년 3월~현재 : 고려대학교 정보보호대학원 겸임교수
<관심분야> 금융보안, 핀테크보안