수신자 중심 거래 : 프라이빗 블록체인에서 이중 지불 공격을 피하는 기법

Recipient-Oriented Transaction for Avoiding Double Spending Attacks in Private Blockchain

요 약

블록체인(Blockchain)에서 다음 블록의 선택을 위해 더 긴 체인을 택하는데, 이러한 블록체인의 본질을 악용하는 이중 지불 공격(Double Spending Attack) 가능성이 존재한다. 이 논문은 모네로(Monero)의 스텔스 어드레스(Stealth Address)와 대시(Dash)의 마스터노드(Masternode) 원리를 활용하여, 송신자로부터 수신자로의 일방적으로 진행되는 거래방식에서 수신자가 직접 해당 거래를 통제할 수 있도록 하여 이중 지불 공격을 피하도록 한다. 이러한 접근 방식에 기반하여, 본 논문에서 제안된 방법은 수신자가 직접 전파(broadcast)하는 지연 시간을 조절함으로써 해당 거래에 대한 권한과 책임을 부여하고, 악의적 협의 노드들의 공격을 피하도록 유도한다.

1. 서 론

블록체인 암호화폐 (Blockchain cryptocurrency)의 최초 사례인 비트코인(Bitcoin)은 신뢰성을 가진 제 3자(third party)에 의존하지 않고 분산 네트워크 시스템(distributed network system)에서 안전한 전자 화폐를 구성하는 논리적 방법을 제시했다. 그러나 전자 화폐가 사용자들 간에 교환되는 트랜잭션 과정에서의 문제점이 존재한다. 전자화폐에서는 전자 서명을 통해서 화폐의 소유자를 증명하고, 트랜잭션의 송신자를 증명한다. 하지만 전자 서명은 같은 화폐가 2번 소비되는 이중 지불 문제(Double Spending Problem)를 해결할 수는 없으며 이는 정보의 비대칭에서 발생한다.

예를 들어, 송금자가 1BTC를 소유한 상태로 여러 사람들에게 동시에 1BTC씩 보낸다면, 받은 사람은 송금자가 보냈다는 것은 확인할 수 있지만, 이것이 여러 번 사용되었는지는 확인할 수 없다. 이렇게 발생한 여러 번의 거래 중 올바른 거래를 추려 내기 위해서 공동 장부를 만든다. 이 과정에서 위의 거래들 중 어떤 거래가 장부에 기록이 될 지는 알 수 없으며, 서로 다른 거래를 올바른 거래로 기록을 하게 되는 경우가 발생한다. 이 때 블록체인에 분기(fork)가 일어나게 되며 분기된 블록체인들 중 어떤 블록체인을 선택할지에 대한 합의가 필요하다. 블록체인의 본질은 그 체인의 데이터를 공유하는 참여자(node)들의 합의 구조이다. 비트코인의 경우는 작업증명방식(Proof of Work)을 기반으로 컴퓨팅 파워를 많이 소모하여 가장 긴 체인을 만든 쪽으로 합의한다.

블록체인의 더 긴 체인을 수용(accept)하는 본질을 악용하여 수신자에게 피해를 입히는 이중 지불 공격이 존재한다. 대부분의 이중 지불 공격[1]은 거래 시 1회 이상의 승인을 함으로써 방어가 가능하지만, 네트워크 내 최장 블록체인 승인하는 블록체인의 특징으로 인해 방어가 불가피한 경우가 있다. 이러한 문제는 프라이빗 블록체인(Private Blockchain)에서도 충분히 발생 될 가능성이 있다. 프라이빗 블록체인은 허가형 원장(Permissioned Ledger)으로써 읽기, 쓰기, 합의 과정에 사전에 허가된 사용자만 참여가 가능하다. 프라이빗 블록체인에서 합의는 작업증명방식, 지분증명방식(Proof of Stake), 경과시간증명방식(Proof of elapsed time) 등의 방법이 존재한다. 하지만 여전히 악의적 협력 노드들이 존재한다면, 이중 지불 공격이 발생할 수 있다. 본 논문은 수신자가 거래의 전파 시기를 통제함으로써 해당 공격을 피하는 방법인 수신자 중심 거래(Recipient-Oriented Transaction)을 제시한다.

2. 배경

1) 스텔스 어드레스[2] : 이 개념은 알트코인(Altcoin) 중 개인정보 보호에서 대표적인 모네로에서 착안되었다. 모네로에서 수신자의 정보를 보호하기 위해 이 개념을 쓰는데, 스텔스 어드레스란 수신자의 공개 읽기 키와 쓰기 키에 랜덤 데이터를 합하여 생성한 유일한 일회용

공개키(Public key)이다. 모든 거래는 생성 즉시 각자의 유일한 스텔스 어드레스를 가진다. 그리고, 송신자는 자신의 개인 키(Private key)를 이용하여 이 거래를 찾을 수 있다. 이 개념은 아래의 유일한 일회용 공개키를 생성하는 5단계의 알고리즘으로써 적용되었다.

1) 수신자의 공개 키 A : A = $a.G$
2) 송신자의 공개 키 B : B = $\beta.G$
3) 디피-헬멘 키 교환(Diffie-Hellman key exchange) [5]을 이용한 공유 키 S : S = $\beta.A = a.B$
4) 스텔스 어드레스 SA 와 개인 키 ɣ
: SA = $H(S).G$, ɣ = $H(S) \bmod Q$
5) 수신자는 거래를 탐지하기 위한 전송 주소 T
: T = $H'(H(\beta.A).G)$

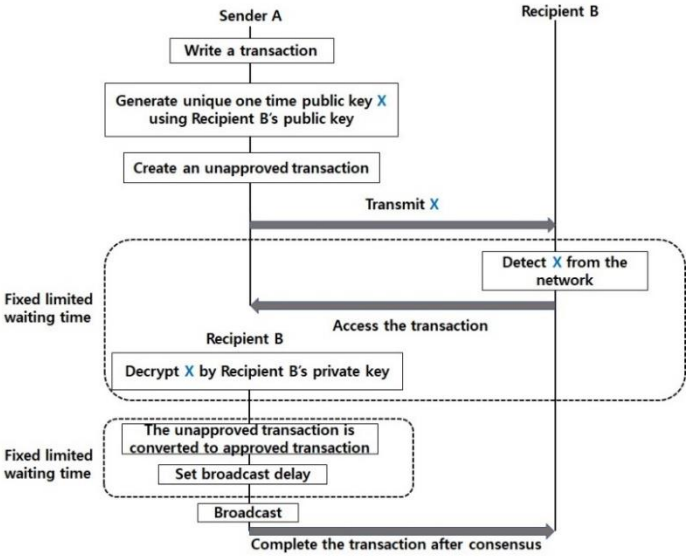
수신자가 T를 이용하여 거래에 접속하려 할 때, 거래를 가지고 있는 송신자의 지갑은 접속자의 개인 키가 타원 곡선 암호화[4]를 통해 거래 안에 있는 공개 키를 생성할 수 있는 지를 확인한다. 생성한 공개키가 거래 안의 공개 키와 일치한다면, 접속자는 수신자인 것이 증명된다. 따라서, 생성된 T는 오직 거래의 수신자만이 해당 거래에게 권한이 부여할 수 있도록 한다.

2) 마스터노드[3] : 이 개념은 또 다른 알트코인인 대시에서 착안되었다. 대시에서 마스터노드는 즉각전송(InstantSend)와 사적전송(PrivateSend)기능을 제공하며 송신자와 수신자 사이에서 중재자이자 보증인의 역할을 한다. 마스터노드는 송신자들로부터 받은 거래를 섞어서 해당 거래들을 추적불가능 하도록 만든다. 이는 사적전송 기능을 제공할 수 있도록 해준다. 또한, 마스터노드는 블록을 생성하지 않는 지분증명 기반의 노드이기 때문에, 거래가 블록에 삽입되려면 기다려야만 한다. 대신에 마스터노드는 미확인상태의 거래를 확인상태로 바꾸면서 즉각전송 기능을 수행할 수 있을 뿐만 아니라, 거래가 블록에 기록되기 전에 이중 지불을 방지한다. 이 개념은 대시의 마스터노드가 거래가 이루어지는 과정에서 중간다리 역할을 해주는 것을 논리적으로 활용하였다.

3. 시스템 모델

이 알고리즘은 수신자가 자신에게 오는 거래가 블록에 작성되기 이전에 해당 거래를 확인하고 직접 전파할 수 있도록 한다. 수신사 중심 거래는 아래와 같이 진행된다.

1) 현재의 거래 과정과 비슷하게 송신자가 거래를 생성할 때 수신자의 필수 정보를 입력한다.
2) 송신자의 지갑은 거래가 생성할 때 해당 거래에 대한 유일한 일회용 공개키를 수신자의 공개 키와 랜덤데이터를 혼합하여 자동적으로 생성하며 해당 거래를 미승인상태로 생성한다.
3) 송신자는 생성된 일회용 공개키를 수신자에게 전달한다.
4) 수신자는 해당 키를 이용해 네트워크에 있는 해당 거래를 탐지한다.
5) 거래에 무분별한 접근을 막기 위해, 거래에 접근한 지갑의 개인 키가 해당 거래에 입력된 수신자 공개 키를 생성할 수 있는 지를 타원 곡선 암호화를 통해 검증한다.
6) 검증이 완료되면, 해당 접속자는 거래의 수신자로 인증이 되고 거래에 접속한다.
7) 거래에 접속되면, 해당 거래는 미승인상태에서 승인상태로 전환되며 수신자는 언제 거래가 전파가 될지 전파 지연 시간을 설정한다.



4. 수신자 권한

본 논문에서 제시된 알고리즘은 수신자가 일방적으로 받는 거래에 대해 책임과 권한을 부여한다. 이 방법으로 수신자는 직접 전파 지연 시간을 설정하게 된다.

기본적으로 미승인 거래가 너무 짧게 혹은 오랫동안 존재하지 못하도록 고정된 대기 시간을 둔다. 또한, 악의적 협력 노드들이 공격 대상 거래 전파를 기다리다가 전파가 확인되는 동시에 전파하는 것을 피해야만 한다. 이를 위해 수신자는 미승인거래를 승인상태로 전환하는 것과 전파하는 시점을 따로 관리한다. 미승인 거래와 마찬가지로, 승인은 되었지만 전파되지 않은 거래도 고정된 대기 시간으로 제한을 둔다. 이 과정에서 송신자는 전환된 거래가 승인상태라는 사실은 파악할 수는 있지만, 수신자가 정한 전파 대기 시간은 알 수 없으므로 기존의 이중 지불 공격과 같이 대기하여 발생하는 공격을 피할 수 있다.

이와 반대로, 악의적인 제 3자들 뿐만 아니라, 이 기능을 악의적으로 이용할 수신자들에 대한 대비책도 강구해야 한다. 악의적인 수신자들을 판별하기 위해, 일정 기간의 전파 대기 시간의 총합을 해당 기간의 사용횟수로 나누어 일정 기준치를 초과한다면, 매 거래마다 악의적으로 전파 대기 시간을 최대한으로 사용한 것으로 판단한다. 각 프라이빗 블록체인 모델에 맞게 이를 제재한다.

3. 결론 및 향후 연구

본 논문은 블록체인의 가장 본질적인 특징인 가장 긴 블록체인 승인으로부터 발생되는 이중 지불 공격을 피하기 위해 수신자 중심 거래를 제안한다. 수신자 중심 거래는 수신자가 거래 과정 중간에 개입을 하는 것이 기본 동작 원리이다. 이 알고리즘은 스텔스 어드레스와 마스터노드의 개념을 활용하는데, 각각 수신자가 접속할 거래 주소와 수신자가 중개인 역할을 하여 이를 가능케한다. 수신자가 승인상태로 거래를 전환시킬 때, 송신자는 전환된 거래의 상태는 알 수 있지만 수신자가 설정한 전파 지연 시간 값을 알 수는 없다. 이 점은 악의적 협력 노드가 피해 대상 노드를 대기하여 승인된 직후 전파하는 공격법을 피할 수 있도록 한다.

앞으로 연구할 과제는 이 모델이 송신자와 수신자의 개인정보를 보호할 수 있도록 보안을 강화하는 것이다. 그 방법으로 기밀 전송(Confidential Transaction)을 연구하여 적용하려 한다. 뿐만 아니라, 이 모델이 블록체인을 활용하는 다방면의 분야에 적용될 것을 고려하여 알고리즘은 내부에 적용하되 보안이 결여되지 않는 명료한 인터페이스를 구현하고자 한다.

참 고 문 헌

[1] Karame, Ghassan, Elli Androulaki, and Srdjan Capkun. "Two Bitcoins at the Price of One? Double-Spending Attacks on Fast Payments in Bitcoin." *IACR Cryptology ePrint Archive* 2012.248 (2012).*IEEE Symposium on*. IEEE, 2017.

[2] Courtois, Nicolas T., and Rebekah Mercer. "Stealth Address and Key Management Techniques in Blockchain Systems." *ICISSP*. 2017

[3] Duffield, Evan, and Daniel Diaz. "Dash: A PrivacyCentric CryptoCurrency." (2014).

[4] Kapoor, Vivek, Vivek Sonny Abraham, and Ramesh Singh. "Elliptic curve cryptography." *Ubiquity* 2008.May (2008): 7

[5]https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange