정 보 보 호 학 회 지
제28권 제3호, 2018. 6

퍼블릭 블록체인의 보안 위협과 블록체인 확장성 문제의 연관성에 대한 분석

노 시 완*, 이 경 현**

요 약

최초의 암호화폐인 비트코인의 등장과 함께 그 기반기술인 블록체인에 대한 국내외의 관심이 증가하는 가운데 국외에서는 블록체인의 확장성 문제에 대한 논의가 활발히 이루어지고 있다. 블록체인은 시스템을 관리하는 중앙기관 대신 네트워크의 사용자들의 합의에 기반하여 시스템을 유지한다. 신뢰할 수 없는 사용자 간의 합의를 위해 작업증명이라는 신뢰성 보장을 위한 기술을 사용하였고 이로 인해 비트코인과 같은 퍼블릭 블록체인은 제한된 처리량을 가지게 되었다. 현재까지 알려진 대부분의 공격들이 이러한 제한된 처리량으로 인한 처리 지연으로 공격 성공률이 증가하기 때문에 확장성 문제 해결을 위한 연구가 필요한 실정이다. 본 논문에서는 현재 알려진 퍼블릭 체인에서의 보안 위협을 분석하고 확장성 문제와 함께 현재 알려진 확장성 문제 솔루션에 대한 소개 및 앞서 서술한 보안 위협과의 연관성에 대해 분석한다.

Ⅰ. 서 론

비트코인[1]은 종래의 은행과 같은 제3자의 개입 없이 개인 간의(Peer-to-Peer, P2P) 안전한 거래가 가능한 결제 시스템으로서 블록체인 기술을 사용한 첫 사례이다. 비트코인 결제 시스템에 참여하고 있는 모든 사용자들은 시스템에서 발생하는 모든 거래에 대한 기록(transaction)을 자신의 블록체인에 저장하고 저장된 기록을 토대로 시스템에서 발생하는 모든 거래를 검증하여 유효한 거래만 자신의 블록체인에 새롭게 추가한다. 이 동작을 시스템의 모든 사용자가 개별적으로 수행하여 최종적으로 시스템의 모든 사용자들이 하나의 동일한 블록체인(거래장부)을 유지·보관하는 분산원장기술(Distributed ledger technology)이다.

신뢰할 수 없는 사용자들 간에 하나의 원장을 선택토록 해야 하는 비잔틴 장군 문제(Byzantine fault tolerance)를 비트코인에서는 작업증명(Proof-of-Work, PoW)을 사용하여 해결하고 있다. 하지만 이로 인해 하나의 새로운 블록(거래기록의 집합)을 블록체인에 추가하는 것에는 상당한 시간을 필요로 하게 되었고 결과적으로 시간당 처리 가능한 거래의 수는 제한되게 되었다.

이러한 제한된 시간당 처리량으로 인한 확장성 문제(Scalability)를 해결하고자 국외에서는 많은 연구가 이루어지고 있으나 국내에서는 관련 연구가 미흡하여 본 논문에서는 퍼블릭 체인에서 알려진 보안위협과 함께 확장성 문제 해결의 필요성을 연관하여 분석하고 대표적인 해결방법들을 소개하고자 한다.

Ⅱ. 퍼블릭 블록체인 공격 유형

대표적인 퍼블릭(public) 블록체인인 비트코인은 기존의 화폐와 달리 디지털데이터로서 무단 복사 및 해킹 등으로 인한 탈취 등에 취약하다. 때문에 비트코인은 전 세계 모든 사용자의 거래기록을 하나의 공개장부로 만들어 블록체인으로 저장하고 네트워크의 모든 사용자가 이를 유지·관리한다. 블록체인에는 시스템의 모든 사용자들의 비트코인 소유권 이전에 대한 기록이 저장되어 있으며 새로운 코인의 사용을 위해서는 장부에 기재된 해당 코인의 소유권 이전 기록에 대해 디지털서명을 통한 소유권 증명을 필요로 한다. 비트코인에서 모든 코인

이 논문은 2017년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (No.2017-0-00156, 블록체인의 정보보호 프레임워크 및 평가 방법 개발)
* 부경대학교 IT융합응용공학과 (khrhee@pknu.ac.kr)
** 부경대학교 정보보호학협동과정 (nosiwan@pukyong.ac.kr)

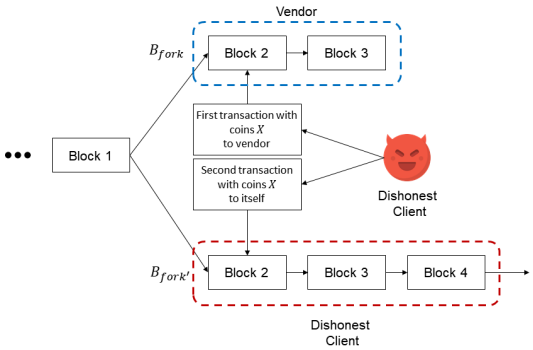
은 고유한 식별정보(transaction identifier)를 가지며 거래를 통해 보다 작은 금액의 코인으로 분할되거나 다른 코인과 합쳐져 큰 금액의 화폐가 된다. 이렇듯 거래에 한번이라도 사용된 화폐는 소비되어 다른 거래에 사용될 수 없어야하지만 이미 사용된 코인을 재사용하는 이중 지불(double spending)이 암호화폐에서 가장 큰 보안 이슈로 알려져 있다. 본 논문에서 소개할 공격들 중 대부분은 이중지불 자체를 목적으로 하거나 이중지불의 성공률을 높이는데 부가적으로 사용된다. 하지만 이중지불 외에도 블록 채굴보상을 시스템 상의 개인 혹은 단체가 독점하거나 결제 시스템 자체를 무력화시키는 등 다양한 공격 목적이 존재한다.

비트코인 결제 시스템에서는 생성한 트랜잭션이 채굴자(miner)에 의해 블록에 포함되어 네트워크에 전파되고 해당 블록을 이전 블록으로 하는 새로운 블록이 6개 이상 추가됐을 경우(6-Confirmations) 해당 블록을 유효한 거래기록으로 간주하는 것을 권고한다. 이는 동일한 블록을 이전 블록으로 하는 블록이 2개 이상 존재할 경우 일시적으로 네트워크에 분기(fork)가 발생하고 먼저 새로운 블록이 연결되는 블록체인이 주 체인이 되는 경쟁이 시작되는 메커니즘을 따르기 때문이다. 경쟁에서 승리한 블록체인이 네트워크에 승자로 알려지고 패배한 다른 블록체인은 폐기 되어 분기 발생시점 이후 생성된 블록에 포함되어 있던 거래 또한 취소되기 때문에 이러한 문제를 방지하기 위해 최소 6개의 승인을 획득한 블록의 경우 분기로 인한 경쟁 중일 확률이 매우 낮기 때문이다. 하지만 매 10분마다 하나의 블록이 추가되는 비트코인 시스템의 특성상 6개의 승인을 얻기 위해서는 평균적으로 약 1시간이 필요하다. 때문에 소액 거래의 경우 트랜잭션이 블록에 포함된 것만을 확인하는 제로 컨펌(zero confirmation)을 사용하는 경우가 존재한다. 판매자는 소비자의 판매대금 트랜잭션이 블록에 포함된 것을 확인한 뒤 사용자에게 서비스를 제공함으로서 결제로 인한 지연을 줄일 수 있다. 이 장에서는 이러한 제로 컨펌을 기반으로 하는 공격들을 살펴본다.

2.1. 이중 지불

분기를 이용한 기본적인 이중 지불 시나리오는 다음과 같다. 이중 지불 공격자 C_d는 판매자 V의 물품 구입을 위한 대금 지불 트랜잭션 $T_V^{C_d}$를 생성하여 블록체인 네트워크에 전파한다. 동시에 동일한 비트코인을 소비하는 트랜잭션 $T_{C_d}^{C_d}$를 생성하여 네트워크에 전파한다(송신자와 수신자를 동일하게 본인으로 설정하여 수수료를 제외한 다른 손실이 발생하지 않도록 함). 판매자는 그림 1과 같이 네트워크에 전파된 정상 거래 트랜잭션 $T_V^{C_d}$가 블록에 포함된 것을 확인하고 물품(혹은 서비스)을 전달한다. 하지만 동시에 이중 지불 트랜잭션 $T_{C_d}^{C_d}$가 정상 거래 트랜잭션 $T_V^{C_d}$와 다른 블록에 포함되어 분기가 발생하고 이후 경쟁에서 정상 거래 트랜잭션이 포함된 블록이 경쟁에서 패배할 경우 정상 거래 트랜잭션 $T_V^{C_d}$는 취소되고 공격자는 코인의 소비 없이 물품을 구매할 수 있다(여기서 T_A^B는 A가 B에게 보내는 트랜잭션이다).

공격과정에서 공격의 성공은 분기의 발생 여부와 발생시점, 분기 발생이후 분기 경쟁에서 공격 트랜잭션의 승리 등에 영향을 받는다. 정상 트랜잭션과 공격 트랜잭션이 네트워크에 동시에 존재하더라도 정상 트랜잭션이 먼저 블록에 포함되어 모든 네트워크에 전파되거나 혹은 공격 트랜잭션이 먼저 블록에 포함되거나 혹은 분기가 발생하였으나 경쟁에서 질 경우 공격은 실패하므로 단순히 위의 시나리오만으로 공격에 성공할 확률은 매우 낮다.



〔그림 1〕 이중지불 공격

2.2. 블록 보류(Block Withholding)

현재까지 알려진 많은 공격들은 2.1절에서 기술한 바

와 같이 기본적으로는 매우 낮은 공격 성공률을 높이는 것을 목적으로 하고 있다. 블록 보류 공격[2,3]은 2.1절의 시나리오에서 공격자가 이중 지불 트랜잭션의 생성 이후 공격자가 공격에 더 이상 관여하지 않는 것과 대조적으로 공격의 성공률을 높이는 행동을 함으로서 최종적으로 분기된 이중지불 트랜잭션의 블록이 경쟁에서 승리하도록 유도한다. 다음은 블록 보류를 통한 이중지불 공격인 Finney 공격[4]의 시나리오이다.

공격자 C_d는 사전에 이중 지불 트랜잭션 $T_{C_d}^{C_d}$를 포함한 블록 $B^{'}$을 생성한다. 생성한 블록을 네트워크에 전파하지 않고 보관한 뒤 정상적인 지불 트랜잭션 $T_V^{C_d}$를 네트워크에 전파하고 블록에 포함되어 판매자 V에게 확인될 때까지 대기한다. 블록에 포함되어 판매자에게 확인된 이후 사전에 생성한 블록 $B^{'}$을 네트워크에 전파하여 분기를 발생 시킨다(네트워크에는 정상적인 트랜잭션 $T_V^{C_d}$을 포함한 분기 B_{fork}와 이중지불 트랜잭션 $T_{C_d}^{C_d}$을 포함한 분기 B'_{fork}가 존재한다). 이후의 경쟁에서 B'_{fork}가 승리하여 주 체인이 될 경우 정상적인 트랜잭션을 포함한 블록 B_{fork}에 포함된 트랜잭션들은 취소되고 공격자는 이중 지불 공격에 성공할 수 있다.

비트코인 관련 연구에서 유명한 공격 유형중 하나인 이기적인 채굴(selfish mining)[5,6]은 이러한 블록 보류를 통해 공격자가 원하는 시점에 사전에 생성한 블록을 네트워크에 전파함으로써 분기를 생성하는 전략을 기본으로 하며 특정 시점 이후 비공개적인 분기를 발생시켜 비공개적으로 채굴중인 분기와 본래 블록체인 분기의 상태에 따라 보류 중인 블록의 공개를 결정하는 이기적인 채굴 전략을 통해 채굴 보상을 극대화할 수 있다.

2.3. 네트워크 지연

2.1절에서 설명한 것과 같이 공격의 성공에는 분기의 발생과 더불어 분기 경쟁의 승리가 필요하다. 분기 경쟁의 승리 요인은 사용자들이 공격자의 블록을 자신의 블록체인에 포함하고 채굴 작업을 수행하는 것으로 공격자는 경쟁에서 승리하기 위해서 공격을 위한 블록이 정상 블록보다 많은 사용자들에게 전파되어 경쟁에서 승리하도록 유도하는 것이 필요하다.

공격자는 네트워크에 더미 노드(dummy helper node)를 설치하여 자신의 블록이 보다 빨리 전체 네트워크에 전파되도록 하고 경쟁 블록은 전파하지 않음으로써 네트워크에서 공격자의 블록의 점유율이 증가하도록 유도하는 시빌 공격(sybil attack)[7]이 가능하다. 또한 특정한 개인 혹은 집단의 P2P 네트워크에서의 연결을 공격자가 제어 가능한 노드만으로 구성되도록 유도하여 특정 대상을 블록체인 네트워크로부터 고립되도록 하여 공격자가 원하는 데이터만 대상에게 전달되도록 하는 이클립스 공격(eclipse attack)[8]이 가능하다. 이러한 공격들을 이용하여 공격자는 임의로 분기를 발생시키고 원하는 분기 블록이 경쟁에서 승리하도록 유도하여 이중지불 공격 혹은 다른 공격이 성공하도록 하는 것이 가능하다.

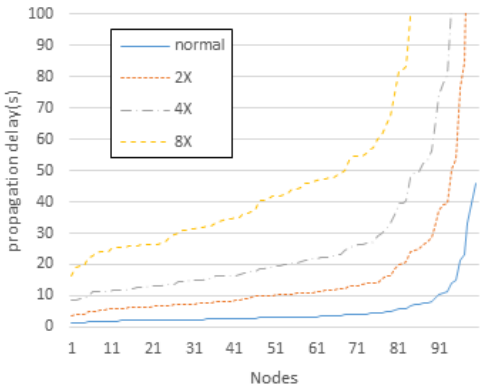
Ⅲ. 블록체인 확장성

7년 전 비트코인의 하루 트랜잭션 처리 수는 5,357개(‘11.12.31.기준)이였지만 최근에는 340,980개(‘17.01.02.기준)으로 60배 이상 증가하였다[9]. 비트코인 시스템이 평균적으로 10분에 하나의 블록을 처리하고 각 블록은 최대 1MB의 크기를 가지며 포함되는 트랜잭션이 2개의 입력과 3개의 출력을 가진다고 가정할 때 시스템이 하루에 처리 가능한 트랜잭션의 수는 약 305,085개(시간당 약 12,712개)로서 만약 특정 시간대에 처리를 기다리는 트랜잭션의 수가 시간당 최대 처리량을 초과할 경우 처리되지 못한 트랜잭션은 평균 대기 시간보다 더 오랜 시간을 대기하거나 처리되지 못할 가능성이 존재한다. 때문에 IoT와 같은 방대한 데이터를 처리하는 분야에 이러한 시스템을 그대로 적용할 경우 확장성 문제에 직면할 수 있다. 2장에서 살펴본바와 같이 현재까지 알려진 많은 공격[2-8]이 이러한 트랜잭션 처리 지연 혹은 분기로 인한 트랜잭션의 취소에 기반하고 있고 지연이나 분기의 증가에 따라 공격확률이 증가하므로 이러한 확장성 문제의 존재는 블록체인 시스템에 치명적인 위협이 될 수 있다. 이 장에서는 이러한 확장성 문제에 대한 대중적인 접근방법 중 파라미터 재설정과 페이먼트 채널에 대해 소개한다.

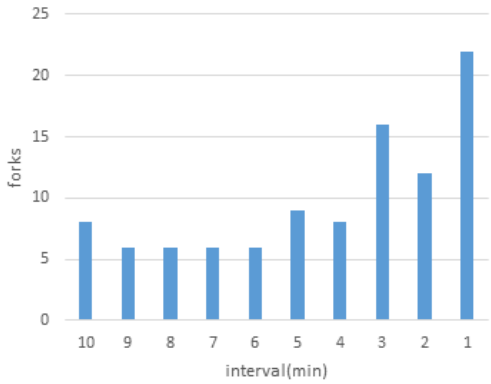
3.1. 파라미터 재설정(Reparameterization)

비트코인의 경우 확장성 문제에 대한 논의가 개발자들 간에 오래전부터 진행되어왔다. 대표적인 해결방안으로는 현재 클라이언트에서 제한해놓은 블록 크기 제한(1MB)을 수정하여 블록에 포함될 수 있는 트랜잭션의 수를 증가시키자는 것이었지만 개발자들 간의 의견충돌로 기존 시스템과 다른 독립된 블록체인을 만드는 하드포크(Hard fork)를 통해 기존 비트코인 클라이언트에서 파라미터를 재설정하여 시간당 처리량을 증가시킨 비트코인 캐시, 비트코인 클래식, 비트코인 언리미티드와 같은 새로운 암호화폐들이 만들어졌다. 이렇듯 블록의 최대크기를 증가시켜 블록에 포함되는 트랜잭션의 수를 증가시키거나 새로운 블록의 추가에 필요한 생성주기를 감소시킴으로써 시간당 처리량(transaction per second, tx/s)을 증가시킬 수 있지만 이로 인해 또 다른 문제가 발생할 가능성이 증가한다. 그림 2는 네트워크 노드의 수가 100개일 때 블록 크기의 증가에 따른 전파지연을 나타낸 것으로 블록의 크기가 증가할수록 모든 네트워크의 노드가 블록을 수신하는데 걸리는 시간이 증가함을 확인할 수 있다.

지연시간의 증가는 하나의 블록이 네트워크에 전파되는 도중에 새로운 블록의 전파가 발생하는 분기의 발생 확률이 증가함을 의미한다. 즉, 이러한 전파 지연의 증가는 2장에서 설명한바와 같이 이를 기반으로 하는 공격의 성공률 또한 증가시킴으로 단순히 블록의 크기를 증가시키는 방식은 적절하지 못하다고 볼 수 있다. 또한 블록생성 주기를 감소시킬 경우 실질적으로 전체



〔그림 2〕 블록의 크기 변화에 따른 각 노드의 전파지연 (네트워크의 노드 수=100, 생성주기=10min, 생성된 블록의 수=100)



〔그림 3〕 블록 생성 주기 변화에 따른 분기 횟수 (네트워크의 노드수=100, 블록크기=1MB, 생성된 블록의 수=1000)

처리량을 증가시킬 수 있다. 하지만 생성주기의 감소를 위해서는 PoW의 난이도(difficulty)를 감소시켜야하므로 블록의 크기와 마찬가지로 새로운 블록의 발견 확률이 증가하므로 그림 3과 같이 분기 발생 가능성이 증가한다. Croman 등[10]은 이러한 파라미터 재설정에 대해 네트워크 상황에 따른 재설정 한계치를 계산하여 네트워크의 전파지연을 예상하여 전체 노드 중 X%의 노드가 블록을 전달 받을 효과적인 처리량(effective throughput)을 구하는 공식을 다음과 같이 구하였다. 본 논문에서는 시뮬레이션을 통해 비트코인 테스트 넷에서의 전파지연을 측정하여 표 1과 같이 효과적인 처리량을 계산하였다.

X% effective throughput :=
(block size) / X% block propagation delay

이에 대한 처리량 한계치(throughput limit)는 다음과 같다.

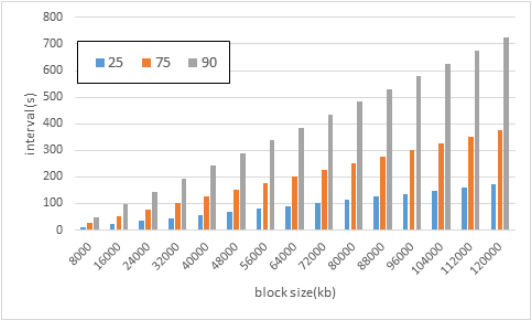
block size / X% effective throughput
< block interval

위와 같이 정의된 공식에 대해 시뮬레이션[1]한 결과 그림 4와 같이 블록 크기의 경우 90%의 효과적인 처리

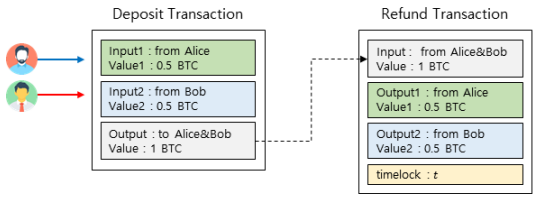
1) 실험은 http://arthurgervais.github.io/Bitcoin-Simulator에서 배포한 오픈소스 시뮬레이터를 사용하였으며 비트코인 테스트 넷에서 10,000개의 네트워크 노드를 가정하고 수행함

〔표 1〕 X% 노드에 대한 효과적인 처리량 (intreval=10m, nodes=10,000)

X%	effective throughput	translated to transaction/sec
25%	703 Kbps	351 tx/sec
75%	318 Kbps	159 tx/sec
90%	166 Kbps	83 tx/sec



〔그림 4〕 블록크기에 따른 X%의 처리량 한계치



〔그림 5〕 페이먼트 채널 초기 상태(on-chain)

량에서 최대 12MB이며 생성 주기의 경우 1MB 블록에 대해 최소 48초로 확인되었다. 이는 전파되는 네트워크 대역폭과 같은 네트워크 성능에 의해 변동되므로 시스템 환경을 고려하지 않은 파라미터 재설정은 위험성을 내포하고 있음을 알 수 있다.

3.2. 페이먼트 채널(Payment Channel)

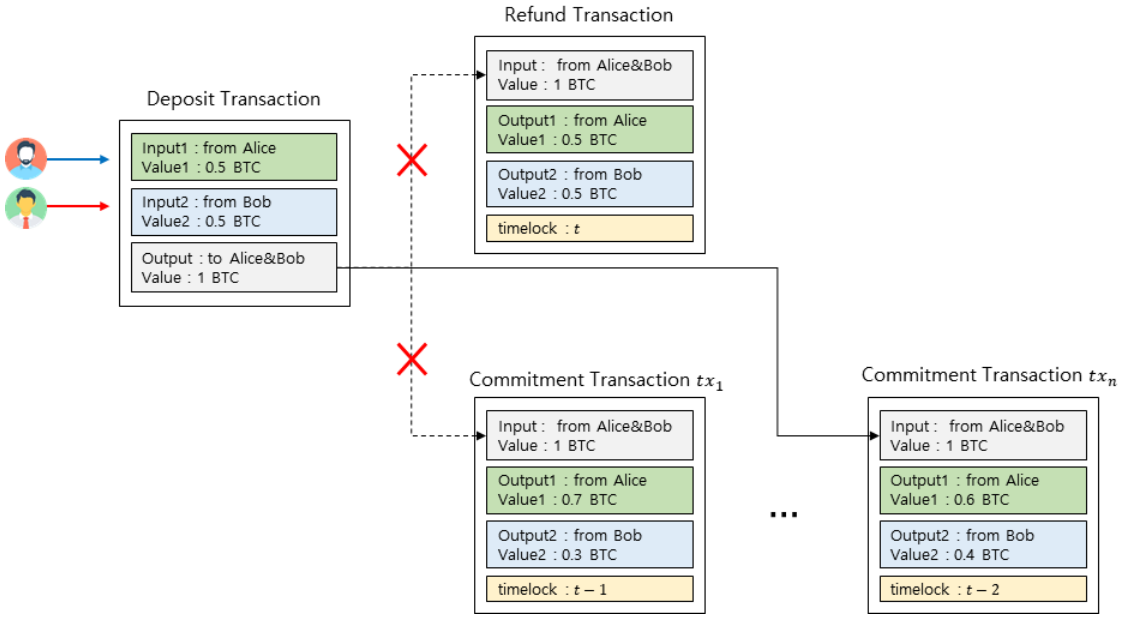
페이먼트 채널[11-13]은 특정한 사용자 사이에 트랜잭션을 자주 주고받는 상황에서 생성되는 모든 트랜잭션이 아닌 일부만을 블록체인 상에(on-chain)에 저장하고 나머지는 해당 사용자 간(off-chain)에 보관하는 형태로 특정 사용자 간에 하나의 채널을 형성하여 채널 간 거래는 블록체인 외부에서 처리하는 개념이다. Poon[11]에서 제안한 양방향(bidirectional) 페이먼트 채널의 생성은 다음과 같다(그림 5,6).

1) 채널을 생성하기를 원하는 사용자 A와 B는 자신이 보유한 미사용 출력(unspent transaction output)을 사용하여 하나의 2-of-2 다중서명(multi-signature) 출력을 생성하는 담보(deposit) 트랜잭션을 생성한다.
2) 담보 트랜잭션의 출력을 사용하여 1)에서 각 사용자가 소비한 출력을 원래 사용자에게로 반환하는 반환(refund) 트랜잭션을 타임락(timelock) t와 함께 생성한다.
3) A는 1)의 담보 트랜잭션의 출력을 사용하여 A와 B에게 금액를 배분하는 확약(commitment) 트랜잭션 tx_1을 타임락 $t-1$과 함께 생성하여 서명 후 B에게 전달한다.
4) B는 3)에서 생성된 tx_1의 내용에 동의할 경우 tx_1에 대한 자신의 서명을 첨부하여 A에게 전달한다.
5) 3)~4)의 과정을 더 이상 거래가 필요하지 않다고 판단될 때까지 반복하여 tx_1을 수정하여 최종적으로 생성된 tx_n을 시간 t 이전에 블록체인에 전파한다.

위와 같이 생성된 트랜잭션은 최초의 담보 트랜잭션과 이를 반환하는 반환 트랜잭션, A와 B사이에 주고받는 $\{tx_1,...,tx_n\}$와 같이 총 $n+2$개이지만 실제 블록체인 상에는 담보 트랜잭션과 최종적으로 업데이트된 tx_n만이 추가된다. 담보 트랜잭션의 출력을 반환하는 반환 트랜잭션은 최종적으로 합의된 트랜잭션 tx_n이 시간 t 이전에 블록체인에 추가될 경우 동일한 출력을 사용하는 반환 트랜잭션은 이중지불로 인해 네트워크의 노드들에 의해 취소된다.

페이먼트 채널은 네트워크에 전파되는 트랜잭션의 수를 감소시킬 뿐 아니라 전파된 트랜잭션이 블록에 포함되어 추가되는 것을 기다릴 필요가 없기 때문에 매우 빠른 처리속도를 보장 받을 수 있다. 또한 채널에 속한 사용자 간에만 트랜잭션을 주고받음으로써 사용자의 프라이버시 또한 보장받을 수 있지만 네트워크의 모든 사용자들 사이에 채널을 생성할 경우 $O(N^2)$의 담보 트랜잭션의 생성이 필요하기에 Poon[11]에서는 일부 사용자들이 몇몇 불특정다수의 사용자와 채널을 형성하고 있을 경우 A와 B 사이에 이러한 여러 페이먼트 채널을 경유하여 통신하는 페이먼트 네트워크가 제안되었다.

하지만 페이먼트 채널의 경우 사전에 생성한 담보 트



(그림 6) n차 업데이트 후 채널 종료 시의 트랜잭션 상태

랜잭션에 포함된 담보 금액만큼의 트랜잭션만을 생성 가능하기에 담보 트랜잭션에서 정의한 금액을 초과하여 사용해야할 경우 발생하는 고갈문제가 존재한다. 이러한 담보를 초과하는 트랜잭션의 생성을 위해서는 채널을 닫고(close) 새로운 담보 트랜잭션을 생성할 수밖에 없으며 off-chain에서 생성된 트랜잭션은 채널이 종료되어 블록체인에 포함될 때까지 제3자에게 트랜잭션의 유효성을 인정받을 수 없다는 문제가 존재한다. Miller 등[14]에서는 채널의 종료없이 담보 트랜잭션의 값을 변경하는 방법과 함께 Poon[11]에서 제안한 페이먼트 네트워크에서 채널에 필요한 시간비용을 줄이는 상태 채널(State Channel)에 대한 개념를 제안하였다.

앞서 분석한 파라미터 재설정과 페이먼트 채널은 확장성 문제를 해결하기 위해 제안되었으나 현재까지 이를 완전하게 해결할 수 있는 단일 솔루션은 존재하지 않는다. 블록체인 어플리케이션을 적용하고자하는 시스템의 특성과 사용하는 네트워크의 성능에 따라 현재 존재하는 여러 솔루션을 복합적으로, 혹은 단일로 사용하여 시스템 환경에 맞는 방법을 적용하는 방법이 블록체인 시스템 구축 전에 필요할 것으로 보인다.

Ⅳ. 결 론

본 논문에서는 퍼블릭 블록체인에 대한 보안 위협과 블록체인 확장성 문제를 연관하여 소개하였으며 또한 확장성 문제에 대해 국외에서 가장 대중적인 솔루션인 파라미터 재설정과 페이먼트 채널에 대해 소개하였다. 현재 국내 블록체인 관련 산업은 꾸준히 증가하고 있고 많은 기업에서 기존 시스템에 블록체인을 접목한 기술을 소개하고 있지만 기반기술에 대한 연구보다는 응용에 초점을 맞추고 있기에 추후 국내 기술이 국외기술에 종속될 위험이 높으며 국가 경쟁력 제고 및 안전한 블록체인 어플리케이션의 개발을 위해서도 확장성 문제와 같은 블록체인 기반기술에 대한 연구가 필요하다. 본 논문을 통해 보다 많은 사람들이 블록체인 보안에 관심을 갖고 국내에서도 블록체인 보안과 관련하여 활발한 연구가 진행되기를 기대한다.

참 고 문 헌

[1] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system.” 2008.

[2] N. T. Courtois and L. Bahack, “On subversive miner strategies and block withholding attack in

bitcoin digital currency," *CoRR,* abs/1402.1718, 2014.

[3] S. Bag, S. Ruj, and K. Sakurai, "Bitcoin block withholding attack :Analysis and mitigation," *IEEE Transactions on Information Forensics and Security*, PP(99), pp. 1-12, 2016.

[4] H. Finney, "Best practice for fast transaction acceptancehow high is the risk?" Available: https://bitcointalk.org/ index.php?topic=3441.msg48384#msg48384, 2011.

[5] I. Eyal, and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," *In International conference on financial cryptography and data security*, Springer, pp. 436-454, 2014.

[6] R. Zhang, and B. Preneel, "Publish or Perish: A Backward-Compatible Defense against Selfish Mining in Bitcoin," *In Cryptographers' Track at the RSA Conference*, Springer, pp. 277-292, 2017.

[7] J. R. Douceur, "The sybil attack," *In the First International Workshop on Peer-to-Peer Systems*, ser. IPTPS '01. London, UK: Springer-Verlag, pp. 251–260, 2002.

[8] E. Heilman, A. Kendler, A. Zohar, and S. Goldberg, "Eclipse Attacks on Bitcoin's Peer-to-Peer Network," *In USENIX Security Symposium*, pp. 129-144, 2015.

[9] https://blockchain.info/charts/n-transactions

[10] K. Croman, C. Decker, I. Eyal, A. E. Gencer, A. Juels, A. Kosba, A. Miller, P. Saxena, E. Shi, E. G. Sirer, D. Song, and R. Wattenhofer,"On Scaling Decentralized Blockchains (A Position Paper)." *In 3rd Workshop on Bitcoin and Blockchain Research,* 2016.

[11] J. Poon and T. Dryja. "The bitcoin lightning network.", https://lightning.network/lightning-network-paper.pdf,

[12] C. Decker and R. Wattenhofer. "A fast and scalable payment network with bitcoin duplex micropayment channels." *In Symposium on Self-Stabilizing Systems*, pp. 3–18. Springer, 2015.

[13] C. Burchert, C. Decker, and R. Wattenhofer. "Scalable Funding of Bitcoin Micropayment Channel Networks." *International Symposium on Stabilization, Safety, and Security of Distributed Systems*, 2017.

[14] A. Miller, I. Bentov, R. Kumaresan, C. Cordi, and P. McCorry, "Sprites and State Channels: Payment Networks that Go Faster than Lightning." arXiv preprint arXiv:1702.05812. 2017.

〈저자소개〉

노 시 완 (Siwan Noh)
학생회원

2016년 2월 : 부경대학교 IT융합응용공학과 졸업
2018년 2월 : 부경대학교 대학원 정보보호학(협) 석사
2018년 3월~현재 : 부경대학교 대학원 정보보호학(협) 박사과정
관심분야 : 정보보호, 접근제어, 의료정보보안, 블록체인

이 경 현 (Kyung-Hyune Rhee)
종신회원

1982년 2월 : 경북대학교 수학교육과 졸업
1985년 2월 : 한국과학기술원 응용수학과 석사
1992년 8월 : 한국과학기술원 수학과 박사
1985년 2월~1993년 2월 : 한국전자통신연구원 연구원, 선임연구원
1993년 3월~현재 : 부경대학 IT융합응용공학과 교수
관심분야 : 정보보호, 암호이론, 암호 프로토콜, 통신보안, 블록체인