www.osia.or.kr

OSIA S&TR Journal

ISSN 1738-9887 Vol. 32, No. 1, March 2019
• 발행인 : 이혁준 회장/OSIA • 편집위원 : 김형식 교수/성균관대학교

(사)한국컴퓨터통신연구회
Open Standards and ICT Association

블록체인의 보안 및 상호운용성 연구 동향

성균관대학교
김 형 식

이미 “블록체인”이라는 용어는 더 이상 새롭거나 낯설지 않고, 인터넷과 웹처럼 친숙한 용어가 되고 있습니다. 2년 전의 암호화폐의 열기를 거쳐 학계와 산업계에서는 블록체인 기술을 둘러싼 많은 토론이 진행되고 있습니다. 그 중 일부는 블록체인 기술에 대한 무용론부터 시작하여 차세대 인터넷 플랫폼에 대한 가능성까지 논의하고 있습니다. 중요한 것은 블록체인 기술은 아직 현재 진행 중이며, 성능 및 보안성에 대한 많은 기술적인 난제들을 풀어야 하는 상황이라는 점입니다.

본 호에서는 현재 논의되고 있는 가장 중요한 블록체인 이슈인 보안성과 상호운용성에 대한 연구 결과를 소개하고 있습니다. 블록체인의 특성상 발생할 수밖에 없는 이중 지불 문제와 이기종 간의 블록체인 네트워크를 통합하기 위한 인터 체인 기술을 논의합니다. 블록체인의 중요한 응용 분야인 ID 관리 기술 및 IoT 관리 기술에 대한 최신 연구 동향을 소개하고 있습니다.

첫 번째 논문은 이중 지불이라는 블록체인의 고전적인 보안 문제에 대한 논문으로서 이중 지불에 대한 기존의 명제인 51% 이상의 컴퓨터 자원이 필요하다는 가정에 대한 의문을 제기하고 있습니다. 현실 블록체인 네트워크에서는 공격자의 컴퓨터 자인이 50% 미만인 경우에도 여전히 효과적인 이중 지불 공격이 가능하다는 것을 공격 성공률 및 공격자의 이윤을 모델링하여 몬테카를로 시뮬레이션을 통하여 증명하고 있습니다.

두 번째 논문은 이기종 간 블록체인 트랜잭션 및 데이터를 상호 교환 관리할 수 있도록 제안되고 있는 Inter-Chain 기술에 대해서 소개하고 있습니다. 현존하는 다양한 블록체인 네트워크 기술을 고려했을 때, 상호 운용성을 위하여 서로 다른 블록체인간 데이터 교환을 가능하게 해주는 Inter-Chain 기술은 향후 블록체인 기반 생태계를 구축하는데 중요한 이슈가 될 것이라 판단됩니다.

세 번째 논문은 블록체인을 이용한 사용자 계정 관리 기술을 소개하고 있습니다. 기존의 ID 관리 기술은 사용자의 개인 정보가 중앙의 특정 기관에서 관리되기 때문에 사용자의 자기 정보 통제 기능이 미흡하고, 개인 정보가 유출되는 사고 등이 발생할 수 있는 문제를 가집니다. 따라서 이러한 문제를 해결하기 위해서 사용자가 스스로 자신의 계정을 관리할 수 있는 방안이 필요합니다. 본 논문에서는 블록체인을 이용하여 어떻게 이러한 문제를 해결하고 탈중앙화된 사용자 계정 관리 시스템을 구축할 수 있는지를 소개하고 있습니다.

네번째 논문은 IoT 환경에서의 블록체인 기술에 대한 요구 사항을 분석하고, 요구 사항에 적합한 다양한 프로젝트를 소개하고 있습니다.

본 특집호 발간을 위해 소중한 시간을 내어 원고를 집필해 주신 집필자분들과 편집에 수고해 주신 학회지 편집 위원회 여러분께 깊은 감사를 드립니다.

50%미만 이중지불 공격

장재혁, 이흥노
광주과학기술원

Abstract

블록체인은 전 세계에 분포된 수많은 네트워크 노드들이 하나의 거래장부를 공동으로 기록, 관리하는 분산화 장부 시스템이다. 블록체인 기술은 합의와 분산화를 바탕으로 거래 기록의 위조가 불가능하도록 설계되었으나, 가상화폐 시장의 성장과 함께 이중지불 공격 (double-spending attack)을 통해 장부를 위조하여 부당이득을 취하려는 시도가 끊임없이 존재해 왔다. 본 논문에서는 이중지불 공격의 위험성을 분석한다. Satoshi Nakamoto는 2008년 비트코인에 대한 이중지불 공격의 성공을 위해서는 전 세계의 노드들이 보유한 컴퓨터 자원보다 더 많은 컴퓨터 자원, 즉 51% 이상의 컴퓨터 자원이 필요하다는 결론을 내렸다. 반면, 본 논문에서는 50% 미만의 적은 컴퓨터 자원을 사용하는 이중지불공격도 위협적임을 보였다. 이러한 결론은 이중지불 공격의 성공 확률이 아닌 기대 이윤을 분석함으로써 얻을 수 있었다. 구체적으로는, 대규모 시뮬레이션을 통해 실제 작동중인 블록체인 네트워크에 50% 미만의 이중지불 공격을 행할 경우에 대한 공격자가 얻는 기대 이윤을 측정하였으며, 이러한 공격을 방지 할 수 있는 방안을 제시한다.

I. 서론

블록체인은 비트코인과 이더리움 등 현존 가상화폐의 핵심 기술이며, 세계에 분포된 수많은 노드들이 하나의 거래장부를 공동으로 기록, 관리하는 분산화 장부 시스템이다. 분산화 장부는 은행, 국가 혹은 중개사가 거래를 관리 및 기록하는 중앙화 장부 시스템과 대조적이며, 중앙화 장부에 비해 해킹 혹은 위조 등에 강인하다. 그러나 거래내용을 전세계의 노드들에게 검증 받아야 하기 때문에 거래속도가 상대적으로 느리다는 단점이 있다. 블록체인과 비트코인은 2008년 Satoshi Nakamoto의 백서에서 소개되었으며 [1], 2019년 기준 약 60억 달러의 유통 규모를 보유한 거대 가상화폐로 성장하였다.

블록체인 기술은 합의와 분산화의 개념을 바탕으로 거래기록의 위 변조가 불가능하도록 설계되었다. 그러나 가상화폐시장의 성장과 함께 이중지불 공격 (double-spending attack)과 같은 보안성 공격을 통해 부당이득을 취하려는 시도가 끊임없이 존재해 왔다. 이중지불공격은 공격자가 서비스 혹은 재화의 대가로 지불한 가상화폐의 거래기록을 무효화하여 재사용하는 공격이다. 예를 들어, 가상화폐 거래소에게 가상화폐를 지불한 대가로 현금을 출금한 후, 이러한 거래 기록을 블록체인상에서 지워버리는 것이다. 실제로 지난 2018년에는 BitcoinCash, Zcash, ZenCash, LitecoinCash와 같은 대규모 가상화폐들이 이중지불 공격의 피해를 받았으며, 그 피해액은 수백만 달러에 달한다 [2], [3], [4].

이중지불공격은 블록체인 합의 알고리즘을 역이용하면 가능하다. 블록체인 합의 알고리즘은 통신지연 등의 이유로 노드들이 보유한 블록체인이 서로 다를 때, 어느 것을 유지하고 어느 것을 버릴지를 결정하는 알고리즘이다. 비트코인의 합의 알고리즘인 longest chain consensus는 길이가 더 긴 블록체인이 더 많은 노드들에게 검증 받았으며, 따라서 더 신뢰 할 수 있다고 결정한다 [1]. 결과적으로, 이중지불공격이 성공하려면 전 세계에 분포된 노드들이 공동으로 생성한 블록체인보다 길이가 더 긴 사기 블록체인을 생성하여 합의 알고리즘을 속여야 한다.

Nakamoto [1]와 Rosenfield [5]는 이러한 합의 알고리즘의 의의를 수학적으로 분석하였고, 이중지불 공격의 성공률이 100%가 되기 위해서는 전 세계의 노드들이 보유한 컴퓨터 자원보다 더 많은 컴퓨터 자원(51%)이 필요하다는 결론을 내렸다. 이중지불 공격이 51% 공격으로 불리는 이유이다. 개인 혹은 하나의 집단이 전 세계의 컴퓨터 자원보다 더 많은 자원(51%)을 보유하는 것은 현실적으로 매우 어렵고, 따라서 비트코인이 이중지불 공격으로부터 안전하다는 주장이다. 그러나 만약 50% 미만의 컴퓨팅 자원을 사용하는 이중지불 공격, 즉 50%미만 이중지불 공격이 공격자에게 큰 이윤을 가져다 줄 수 있다면, Nakamoto와 Rosenfield의 결론은 재검토되어야 한다.

본 논문은 IEEE Transactions on Information Forensics and Security 에 제출된 논문의 수학적 정리[6]를 바탕으로 50%미만 이중지불 공격의 가능성을 시뮬레이션을 통해 보여준다. 구체적으로는 이중지불 공격의 성공률이 아닌, 이중지

불 공격이 가져다 주는 기대 이윤을 분석하였다. 이러한 관점은 Nakamoto와 Rosenfield의 결론과는 전혀 다른 결론을 가져다 주었다. 시뮬레이션을 통해 50% 미만 이중지불 공격의 성공이 보장되지 않더라도, 공격의 대상이 되는 거래의 가치가 충분히 크면 공격자 입장에서 이중지불 공격의 기대 이윤은 크다는 것을 보였다. 만약 한번의 공격이 실패하더라도, 계속 시도하면 결국 그 동안의 지출을 모두 상쇄하고도 남는 이윤이 돌아온다는 것이 기대 이윤의 의미다. 공격자가 이중지불 공격을 수행하며 소요하는 지출은 공격시간 동안 소요한 컴퓨터 자원의 운용 비용뿐인데, 이를 상쇄할 만큼 가치가 큰 거래를 공격하면 결국 이윤을 기대할 수 있다는 것이다. 결론적으로, 상대적으로 적은 (50% 미만) 컴퓨터 자원을 이용하는 쉬운 이중지불공격도 위험하다는 것이다.

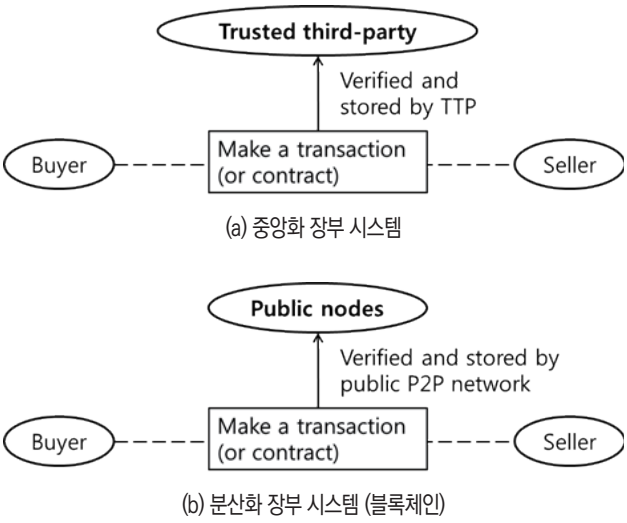
본 논문은 다음과 같이 구성되어 있다. 2장에서는 블록체인의 작동 원리를 소개한다. 3장에서는 이중지불 공격을 소개하고 공격의 성공 조건을 정의한다. 4장에서는 이중지불 공격의 성공률 분석에 관한 기존 연구문헌을 소개하고 분석의 한계점을 제시한다. 5장에서는 이중지불 공격의 이윤을 분석하고 50% 미만의 컴퓨터 자원을 이용하는 이중지불 공격도 위협적임을 실험을 통해 보인다. 마지막으로, 6장에서 요약과 함께 결론을 맺는다.

II. 블록체인

블록체인은 분산화 거래 시스템으로써, 기존 거래 시스템인 중앙화 거래 시스템과 대조적이다. 그림 1은 중앙화 거래 시스템과 분산화 거래 시스템을 비교하여 보여준다. 중앙화 거래 시스템은 공인된 3자인 trusted third-party (TTP)에 의해 거래내용이 검증 및 기록된다. 이러한 기존 방식은 TTP에 완전히 의존하고 있기 때문에, TTP가 부정한 행동을 취하거나 해킹당할 시 거래자는 금전적 피해를 받을 수 있다. 반면, 블록체인에 의한 분산화 거래 시스템은 전 세계에 분포한 풀 노드 (채굴자)에 의해 거래내용이 공동으로 검증 및 기록된다. 따라서 블록체인은 TTP에 의한 거래 시스템보다 더 신뢰할 수 있는 거래 시스템을 제안한다.

블록체인 네트워크를 구성하는 노드는 크게 거래자 노드와 채굴자 노드로 구분 할 수 있다. 거래자 노드는 거래(transaction)을 생성하여 채굴자 노드에게 공표한다. 채굴자 노드는 검증되지 않은 거래들을 모아서 검증하고, 블록에 담는다. 이후 채굴자 노드는 블록에 담긴 거래들이 수정되지 못하게 하기 위해 작업증명을 수행한다.

작업증명의 방식은 블록체인 프로토콜마다 차이가 있으며, 본 논문에서는 비트코인 프로토콜의 작업증명 (proof-of-work)를 소개한다. 비트코인의 작업증명은 블록의 특별한 해쉬 (hash) 값을 찾는 것이다.



(a) 중앙화 장부 시스템

(b) 분산화 장부 시스템 (블록체인)

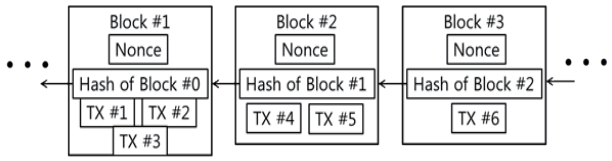
〈그림 1. 중앙화 장부 시스템과 분산화 장부 시스템〉

해쉬는 SHA-256 함수에 의해 1MByte 크기의 블록이 압축된 256bit 길이의 이진 문자열이다. SHA-256 해쉬 함수의 특성은 입력 블록의 이진 값 중 하나의 값이라도 수정되면, 출력되는 해쉬 값이 불규칙적으로 변한다는 것이다. 다시 말해, 누군가 악의적인 목적으로 블록의 거래내용을 수정하고 다시 해쉬 값을 계산하면, 이전에 계산된 해쉬 값과는 전혀 다른 결과를 얻는다. 이러한 SHA-256 해쉬 함수의 특성이 거래내용 위조 및 변조를 방지하기 위해 사용된다.

작업증명의 목적은 수 많은 채굴자가 하나의 블록을 함께 검증하였다는 사실을 증명하는 것이다. 이러한 목적을 달성하기 위해 비트코인 프로토콜은 채굴자에게 블록의 특별한 해쉬 값을 찾도록 요구한다. 구체적으로, 블록의 내용에 임시 값(nonce)을 추가한 후, 프로토콜이 요구하는 조건을 만족하는 블록의 해쉬 값이 출력될 때까지 임시 값을 변경하도록 지시한다. 특별한 해쉬를 찾으면 하나의 블록을 완성하는 것이며, 블록을 완성한 노드에게는 암호화폐가 보상으로 주어진다. 특별한 해쉬 값의 조건이 어렵기 때문에, 조건을 만족시키려면 SHA-256 함수를 수없이 많이 실행하여야 한다. 즉, 조건을 만족시키기까지 오랜 시간이 소요되며, 그 시간 동안 더 많은 채굴자가 거래들을 검증 하는데 참여 할 수 있다.

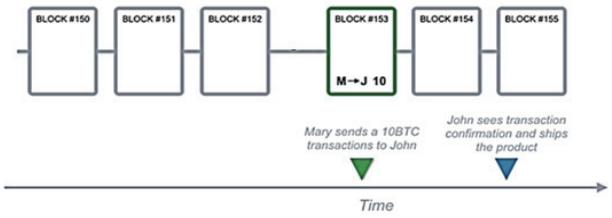
블록체인의 블록들은 서로 연결되어있다. 그림 2은 블록체인의 구조를 보여준다. 작업증명을 통해 하나의 블록이 완성되면, 그 다음 블록의 내용에는 이전 블록의 특별한 해쉬 값이 포함된다. 이러한 체인 구조는 누군가 악의적인 목적으로 이미 검증된 거래 내용을 위조 및 변조하는 것을 어렵게 만든다. 예를 들어 그림 2에서, 블록 #1에 들어있는 거래 #2를 수정하기 위해서는 먼저 블록 #1의 특별한 해쉬 값을 새롭게 찾아야

한다. 그리고 새롭게 찾은 블록 #1의 특별한 해쉬 값은 블록 #2의 해쉬 값에도 영향을 주기 때문에, 블록 #2의 특별한 해쉬 값도 새롭게 찾아야 한다. 이러한 일련의 과정을 가장 최신 블록까지 반복해야 한다. 특별한 해쉬 값을 찾는 작업증명 과정은 많은 시간을 소요한다. 따라서 혼자서 수 많은 작업증명을 완성하는 것은 매우 어렵다.



〈그림 2. 블록체인의 구조〉

거래가 포함된 블록 이후에 더 많은 블록이 연결된다면, 그 거래는 위-변조의 위험에 더욱 강인해진다. 이러한 이유로 거래자는 이체 확인 (block confirmation)라는 과정을 수행한다. 이체 확인은 거래를 완료하기 전에, 거래내용이 기록된 블록을 포함하여 몇 개의 블록이 더 생성되기까지 기다리는 것이다. 이때 생성을 기다리는 블록의 개수를 이체확인 수 (block confirmation number, N_{BC})라고 한다. 예를 들어, 그림 3은 Mary가 John에게 10 BTC의 암호화폐를 지불하고, John은 Mary에게 그 대가에 상응하는 제품을 제공하는 거래의 이체확인 과정을 보여준다. 이체확인 수 (N_{BC})가 2개이면, 거래가 포함된 블록과, 그 이후에 하나의 블록이 생성되는 것을 기다린다. 이체확인 수 N_{BC}가 클수록 위-변조의 위험에 더 강인해지지만, 거래처리 속도는 느려진다.



〈그림 3. 이체확인 과정의 예 (출처: Telemaximum.com)〉

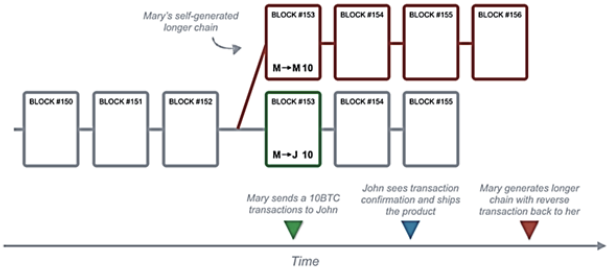
블록체인의 블록은 전 세계의 노드가 공동으로 형성하기 때문에, 네트워크 지연 등의 이유로 서로 연결되지 않는 블록들이 동시에 생성 될 수 있다. 구체적으로, 하나의 블록에 서로 다른 두 개 이상의 블록이 연결되어 체인의 갈래(fork)가 발생 할 수 있다. 비트코인 프로토콜은 여러 갈래가 존재하는 것을 허용하지 않는다. 다수의 갈래 중 하나의 갈래만 유지하는 과정을 합의 (consensus)라 한다. 합의는 여러 방식이 존재하며 [7], 비트코인의 경우 길이가 가장 긴 갈래를 유지시키는 longest chain 합의를 사용한다.

III. 이중지불 공격

이중지불 공격은 longest chain 합의를 악용하여 거래 내용을 변조하고 부당이득을 취하는 공격이다. 그림 4은 Mary (이하 M)가 John (이하 J)에게 이중지불 공격을 수행하는 과정을 보여준다. 공격에 앞서, M은 J에게 10 BTC의 암호화폐를 지급하고 재화를 공급받는 정상적인 거래를 작성 후 공표한다. 정상적인 거래는 채굴자들에 의해 검증된 후 정상블록 #153에 포함된다. 이후 채굴자들은 정상블록 #153을 잇는 또 다른 정상블록들을 지속적으로 생성한다. 한편, M은 정상적인 거래를 공표하자마자 정상적인 거래의 내용을 무효화하는 비정상적인 거래를 작성한다. 비정상적인 거래의 내용은, 예를 들어, "M이 M에게 10 BTC를 이체한다"가 될 수 있다. M은 비정상적인 거래를 채굴자들에게 공개하지 않는다. 채굴자들이 정상적인 거래가 포함된 정상블록을 생성하는 동안, M은 은밀하게 비정상적인 거래가 포함된 비공개블록 #153을 생성하고, 이를 잇는 또 다른 비공개블록들도 생성한다. M은 비정상적인 거래가 포함된 비공개 블록들의 갈래를 다음의 조건이 충족되면 공개한다.

i. 채굴자들의 정상블록의 개수가 이체확인 수 (N_{BC}) 보다 크고,
ii. 공격자의 비공개블록의 개수가 정상블록의 개수보다 많음

M이 비공개 블록들의 갈래를 공개하는 시점에서는, 첫 번째 조건에 의해 정상적인 거래는 완료되었고, 따라서 M은 J로부터 재화를 공급받았다. 그리고 두 번째 조건에 의해 네트워크 모든 노드의 lognest chain 합의는 M이 은밀하게 개발한 갈래를 선택한다. 즉, 두 번째 조건에 의해 M이 J에게 10 BTC를 지급한다는 거래가 무효화되기 때문에 M은 10 BTC를 재사용 할 수 있다.



〈그림 4. 이중지불 공격의 예 (출처: Telemaximum.com)〉

Ⅳ. 이중지불 공격의 성공률 분석

이중지불 공격의 성공확률은 Nakamoto [1]와 Rosenfield [5]에 의해 계산되었다. 확률 분석을 위해, 채굴자와 공격자가 일정시간 동안 생성한 블록의 개수를 독립적인 Poisson 확률 분포[8]를 갖는 랜덤 변수들로 모델링 하였다. Poisson 확률 모델을 바탕으로, 이중지불공격의 성공을 위한 두 조건의 달성 확률 P_1과 P_2를 각각 계산 한 후 곱하였다.

먼저, 두 번째 조건인 ii) 비공개블록의 개수가 정상블록의 개수보다 많을 확률은 Gambler's ruin theorem [9]를 적용하여 계산하였다. 채굴자와 공격자가 보유한 컴퓨터 자원의 비를 각각 p와 q라 칭하겠다 ($p+q=1$). 이중지불공격이 시작된 이후 어느 시점에서 채굴자 갈래의 정상블록 개수가 h개이고 공격자 갈래의 비공개블록 개수가 a개 ($h \geq a$)라 가정하겠다. 이후 무한정한 시간이 지났을 때, 공격자가 언젠가는 두 번째 조건을 달성할 확률은

$$P_2(h-a)=\begin{cases}\left(\frac{q}{p}\right)^{h-a+1}, & if\ p>q\ and\ h\geq a,\\ 1, & otherwise\end{cases} \quad (1)$$

이다.

Nakamoto와 Rosenfield의 분석 결과는 첫 번째 조건인 i) 정상블록의 개수가 이체확인 수 보다 클 확률의 계산 방법에서 차이가 있다. 이 확률을 계산하기 위해서는 채굴자가 생성한 정상블록의 개수가 이체확인 수 (N_{BC})와 같아지기까지 소요되는 시간에 관한 확률모델이 필요하다. Nakamoto는 이 소요시간을 상수로 가정한 반면, Rosenfield는 이 소요시간을 랜덤 변수로 정의하여 보다 일반적인 방법으로 접근하였다.

구체적으로, 채굴자가 하나의 정상블록을 생성하는데 평균 D_H의 시간이 소요될 때, 공격자의 비공개블록 생성 평균 소요시간 D_A를 다음과 같이 계산 할 수 있다.

$$D_A = D_H \frac{p}{q}. \quad (2)$$

이는 블록생성 평균 소요시간이 공격자 혹은 채굴자가 보유한 컴퓨터 자원에 반비례한다는 가정을 바탕으로 계산되었다. Nakamoto는 공개블록의 개수가 N_{BC}와 같아지기까지 소요된 시간을 $D_H N_{BC}$로 가정하였다. 따라서 $D_H N_{BC}$의 시간 동안 공격자가 생성한 비공개 블록의 평균 개수는 $D_H N_{BC}/D_A$ 이며, 식 (2)에 의해 이 값은 qN_{BC}/p와 같다. Poisson 확률 분포에 의해, Nakamoto가 계산한 정상블록이 N_{BC}개 생성되기까지 소요된 시간 동안 공격자가 생성한 비공개블록의 개수가 k 개일 확률은

$$G_1(k)=\left(\frac{qN_{BC}}{p}\right)^k \frac{e}{k!}^{\frac{qN_{BC}}{p}} \quad (3)$$

이다. 반면 Rosenfield는 정상블록의 개수가 N_{BC}와 같아지기까지 소요된 시간이 랜덤 변수 일 때, 그 시간 동안 공격자가 생성한 비공개블록의 개수가 k 인 확률이 negative binomial 확률 분포를 따른다는 사실을 적용하였다. 다시 말해, Rosenfield가 계산한 공개 블록이 N_{BC}개 생성되기까지 소요된 시간 동안 공격자가 생성한 비공개 블록의 개수가 k 개일 확률은

$$P_1(k)=\binom{N_{BC}+k-1}{N_{BC}-1}p^{N_{BC}}q^k \quad (4)$$

이다. Rosenfield의 계산 결과를 바탕으로, 공격자가 언젠가는 이중지불공격에 성공할 확률 P_{AS}는

$$\begin{aligned}P_{AS}&=\sum_{k=0}^{\infty}P_1(k)P_2(N_{BC}-k)\\&=\begin{cases}\sum_{k=0}^{N_{BC}}\binom{N_{BC}+k-1}{N_{BC}-1}p^{N_{BC}}q^k\left(\frac{q}{p}\right)^{N_{BC}-k+1}+\sum_{k=N_{BC}+1}^{\infty}\binom{N_{BC}+k-1}{N_{BC}-1}p^{N_{BC}}q^k, & if\ p<q,\\ 1, & if\ p\geq q\end{cases}\\&=\begin{cases}1-\sum_{k=0}^{N_{BC}}\binom{N_{BC}+k-1}{N_{BC}-1}p^{N_{BC}}q^k\left(1-\left(\frac{q}{p}\right)^{N_{BC}-k+1}\right), & if\ p<q,\\ 1, & if\ p\geq q\end{cases}\end{aligned} \quad (5)$$

이다.

식 (5)에 의해, $P_{AS}=1$, 즉 이중지불 공격의 성공을 보장하기 위한 필요-충분 조건이 $p \leq q$ 이라는 것을 알 수 있다. 다시 말해, 공격자가 채굴자보다 더 많은 컴퓨터 자원을 보유하는 것이 공격 성공의 조건이다. 이러한 결론은 Nakamoto의 계산식에서도 마찬가지로 유도될 수 있다. Gambler's ruin theorem을 적용하여 얻은 이 결론은 공격자에게 무한정의 시간이 주어진다는 가정이 내포되어 있다. 그러나, 공격을 시도하는 시간 동안 컴퓨터 자원을 운용하는 비용이 지속적으로 발생되기 때문에 이러한 가정은 비현실적이다. 뿐만 아니라, 공격 성공확률 100%가 아니어서 실패의 위험이 존재한다고 하더라도, 공격 성공 시 얻을 수 있는 이윤이 소요된 비용보다 훨씬 크다면 공격자의 입장에서는 공격을 시도해 볼 수 있다. 따라서 이중지불 공격의 성공률뿐만 아니라 이윤도 분석 할 필요가 있다.

V. 이중지불 공격의 이윤 분석

앞서 이중지불 공격의 성공률 분석을 통해 공격자의 컴퓨터 자원이 채굴자의 컴퓨터 자원보다 더 적을 때, 즉 $p > q$ 일 때는 이중지불 공격이 실패 할 수 있음을 확인하였다. 본 장에서는 $p > q$ 이더라도, 50% 미만 이중지불 공격이 수익성이 있으며 따라서 거래자에게는 위협적임을 Monte-Carlo 시뮬레이션을 통해 확인한다. 본 장의 내용은 [6]에서 수학적으로 증명되었다.

공격자의 컴퓨터 자원의 비율이 q 일 때, 이중지불 공격의 이윤 $F(q)$ 를 다음과 같이 정의 하였다.

$$F(q) = V(q) - C(q), \tag{6}$$

여기서 $V(q)$ 는 이중지불 공격으로부터 얻는 수익이며, $C(q)$ 는 q 만큼의 컴퓨터 자원을 운용하는데 소요된 지출이다.

지출 $C(q)$ 는 컴퓨터 자원을 운용한 시간과 컴퓨터 자원의 크기에 비례한다고 가정한다. $C(q)$ 를 계산하기에 앞서, $p > q$ 이기 때문에 이중지불 공격이 실패할 가능성이 존재함을 주의해야 한다. 만약 이중지불 공격이 실패하면, 컴퓨터 자원을 운용하는 시간이 무한정 늘어나며, 따라서 지출 $C(q)$ 도 무한대로 발산한다. $p > q$ 인 경우에서 이러한 무한대의 지출을 방지하기 위해, 중단 시간 (cut time) t_{cut} 을 정의한다 [참조문헌 6의 Theorem 7]. 공격자는 t_{cut} 의 시간 내에 이중지불 공격에 성공하지 못할 경우, 지출의 발산을 방지하기 위해 공격을 중단한다. 만약 t_{cut} 내에 공격이 성공할 경우, 지출 $C(q)$ 는 공격 성공 시간 동안 소요된 컴퓨터 자원 운용 비용이다. 공격 성공 시간은 불확정적이기 때문에 랜덤 변수 T_{AS} 로 모델링 될 수 있다. 컴퓨터 자원의 크기는 공격자의 시간당 평균 블록 생성량, 즉 D_A^{-1} 에 비례한다고 가정한다. 종합하면, 공격자의 컴퓨터 자원 비율이 q 이고 중단 시간이 t_{cut} 일 때의 지출 $C(q)$ 은

$$C(q) = \begin{cases} \gamma D_A^{-1} T_{AS}, & if\ attack\ succeeds, \\ \gamma D_A^{-1} t_{cut}, & otherwise \end{cases} \tag{7}$$

이며, 여기서 γ 는 하나의 블록을 생성하는데 소요되는 평균비용이다.

식 (7)의 지출을 계산하기 위해서는 파라미터 D_A 와 γ 가 필요하다. D_A 는 채굴자의평균 블록생성 주기인 D_H 로부터 (2)번 식을 통해 계산이 가능하다. 파라미터 D_H 와 γ 는 공격 대상 블록체인 네트워크에 따라 다르며, 그 값은 인터넷에 공개된 정보로부터 얻을 수 있다. 본 논문에서는 BitcoinCash 네트워크를 예로 들겠다. BitcoinCash의 평균 블록생성 주기는 $D_H = 600$ 초로 네트워크 개발자에 의해 고정되어있다. 채굴자가 보유한 컴퓨터 자원의 크기가 변동하면, 채굴 알고리즘에 D_H 가 유지되도록 채굴 난이도가 변경된다. 또 다른 파라미터인 γ 의 값은 컴퓨터 자원 대여 서비스를 제공하는 업체인 nicehash.com에 의해 결정 될 수 있다. nicehash.com에 따르면, 2018년 12월을 기준으로 BitcoinCash에서 하나의 블록을 채굴하는데 소요되는 비용은 $\gamma = 0.33$ 비트코인(BTC) 이다.

수익 $V(q)$ 는 이중지불 공격이 성공 할 경우 이중지불 공격의 대상이 되는 거래의 가치 v 와 같으며, 공격이 실패할 경우 0이다. 공격이 성공 할 확률은 공격자의 컴퓨터 자원 q 에 영향을 받는다. 수식으로는,

$$V(q) = \begin{cases} v, & if\ attack\ succeeds, \\ 0, & otherwise \end{cases} \tag{8}$$

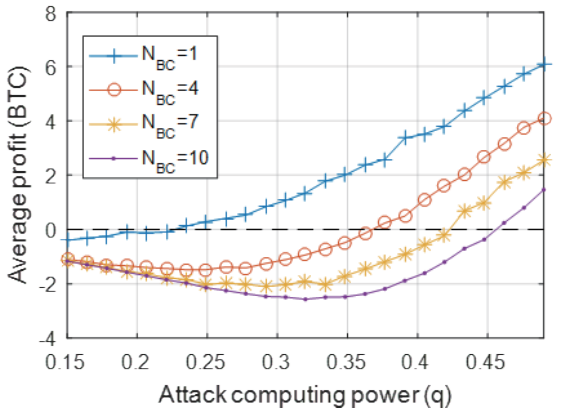
으로 표현 될 수 있다. 공격 대상 거래의 가치는 공격자가 상대 거래자 (피해자)와의 합의를 통해 함께 결정한다.

식 (6)의 이윤을 계산하기 위해 남은 변수는 랜덤 변수인 공격성공 소요시간 T_{AS} 이다. 랜덤 변수 T_{AS} 의 정확한 확률 분포는 [참조문헌 6의 Proposition 4]에서 계산되었으며, 본 논문에서는 T_{AS} 를 Monte-Carlo 실험으로 측정하였다. 실험을 위해, MATLAB상에서 두 개의 독립적인 Poisson counting process (PCP)를 구현하였다. 두 개의 PCP는 각각 공격자와 채굴자가 생성한 블록들의 생성 시간을 나타내며, 평균 블록생성 시간에 영향을 받는다. 공격자 PCP의 평균 블록생성 주기는 D_A 이며 채굴자 PCP의 평균 블록생성 주기는 D_H 이다. 중단 시간 t_{cut} 까지의 두 PCP의 블록생성 시간들을 실현 (realization) 한 후, 두 PCP를 비교하여 이중지불 공격의 두 가지 성공 조건이 달성유무를 판단하였다. 식 (7)의 지출을 계산하기 위해, 만약 이중지불 공격이 성공하였다면, PCP로부터 성공 시간 T_{AS} 를 추출하여 대입하였으며, 만약 공격이 실패하였다면, t_{cut} 을 대입하였다. 마찬가지로, 식 (8)의 수익을 계산하기 위해 만약 이중지불 공격이 성공하였다면, $V(q) = v$ 로 계산하였고, 그렇지 않을 경우 $V(q) = 0$ 으로 계산하였다. 이러한 일련의 과정을 5000번씩 반복한 후 계산 결과들에 평균을 취하였다.

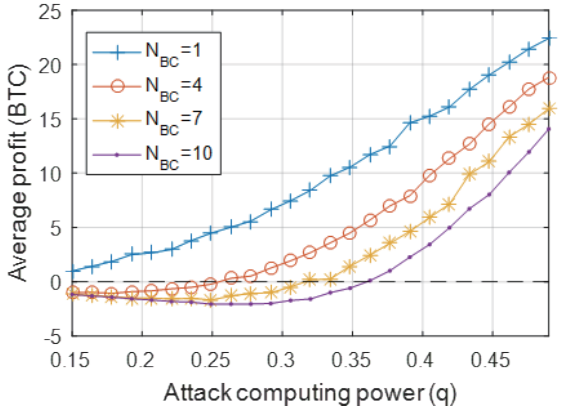
그림 5는 이중지불공격 실험 결과를 보여준다. 실험에 사용된 블록체인 네트워크 파라미터는 블록생성 평균비용 $\gamma = 0.33$ BTC와 블록생성 평균주기 $D_H = 600$ 초이며, 이는 2018년 12월 기준의 BitcoinCash 네트워크의 파라미터와

같다. 중단 시간 $t_{cut} = 12000$초로 설정하였다. 그래프는 다양한 이체확인 수 (N_{BC})와 다양한 공격대상 거래가치 (v)에 대해 이중지불 공격의 표본평균 이윤을 공격자의 컴퓨터 자원 (q)의 함수로 나타내었다.

그림 5로부터 공격자의 컴퓨터 자원이 네트워크 채굴자의 컴퓨터 자원보다 적은 경우, 즉 $q < p$ 인 경우에도 이중지불 공격에서 이윤을 기대할 수 있음을 알 수 있다. 다시 말해, 50% 이상의 컴퓨터 자원을 사용하는 이중지불공격뿐만 아니라 50% 미만의 컴퓨터 자원을 사용하는 이중지불공격도 위협적이다. 그래프는 이중지불 공격에 이윤을 가져다 주기 위한 공격대상의 거래가치 (v)의 요구조건이 이체확인 수 (N_{BC})가 커질수록 증가함을 보여준다. 즉, 가치가 큰 거래가 50% 미만 이중지불공격으로부터 안전하기 위해서는 충분히 큰 N_{BC}가 필요함을 보여준다. 수익성이 있는 50%미만 이중지불공격을 위한 공격대상 거래가치에 대한 정확한 조건은 [참조문헌6의 Theorem 8]에서 계산되었다.



(a) 거래가치 BTC



(b) 거래가치 BTC

〈그림 5 다양한 거래가치와 이체확인 수에 대한 50% 미만 이중지불 공격의 평균 이윤〉

VI. 결론

이중지불공격에 관한 기존 문헌들은 공격자의 컴퓨터 자원이 네트워크 채굴자의 컴퓨터자원보다 더 클 때, 즉 공격자가 전체 컴퓨터 자원의 50% 이상을 보유해야만 이중지불 공격이 성공 할 수 있다는 것을 보였다. 이러한 이유로 이중지불 공격은 51% 공격으로 알려져 왔다. 반면 본 논문에서는 50% 미만의 컴퓨터 자원을 사용하는 이중지불공격, 즉 50%미만 공격의 위험성을 분석하였다. 대규모 시뮬레이션을 통해 50% 미만의 컴퓨터 자원을 사용하는 이중지불공격도 공격자에게 큰 이윤을 가져다 줄 수 있음을 보였다. 구체적으로는, 거래자가 설정하는 이체확인 수가 작을수록 이중지불공격의 이윤이 커짐을 보였다. 다시 말해, 이체확인 수가 작을수록 거래의 처리속도는 빠르지만 50%미만 공격에는 매우 취약하다. 본 논문의 실험 결과는 블록체인의 거래자가 거래 가치와 이체확인 수를 결정하는 것에 관한 가이드라인을 제공 할 수 있다.

Acknowledgement

이 논문은 2019년도 광주과학기술원의 재원으로 GRI(GIST연구원) 사업의 지원을 받아 수행된 연구임. 이 논문은 2019년도 광주과학기술원의 재원으로 "과학기술응용연구단의 실용화 연구개발사업"의 지원을 받아 수행된 연구임.

References

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System." [Online]. Available: https://bitcoin.org/bitcoin.pdf.

[2] C. Osborne, "Bitcoin Gold suffers double spend attacks, $17.5 million lost," ZDNet, 25-May-2018. [Online]. Available: https://www.zdnet.com/article/bitcoin-gold-hit-with-double-spend-attacks-18-million-lost.

[3] "ZenCash Statement on Double Spend Attack," Horizen, 03-Jun-2018. [Online]. Available: https://blog.zencash.com/zencash-statement-on-double-spend-attack/.

[4] A. Hertig, "Blockchain's Once-Feared 51% Attack Is Now Becoming Regular," CoinDesk, 08-Jun-2018. [Online]. Available: https://www.coindesk.com/blockchains-feared-51-attack-now-becoming-regular/.

[5] M. Rosenfeld, "Analysis of Hashrate-Based Double Spending," arXiv:1402.2009 [cs], Feb. 2014.

[6] J. Jang and H.-N. Lee, "Profitable Double-Spending Attacks," submitted to IEEE Transactions on Information Forensics and Security, Mar. 2019. Available: arXiv:1903.01711 [cs]
[7] G.-T. Nguyen and K. Kim, "A Survey about Consensus Algorithms Used in Blockchain," Journal of Information Processing Systems, vol. 14, no. 1, pp. 101 - 128, 2018.
[8] A. Papoulis and S. U. Pillai, "Random walks and other applications," in Probability, Random Variables and Stochastic Processes, 4th edition., Boston, Mass.: McGraw-Hill Europe, 2002.
[9] W. Feller, "Random walk and ruin problems," in An introduction to probability theory and its applications, New York: Wiley, 1968.

Biographies

장재혁

2014년: 금오공과대학교 전자공학 학사
2016년: 광주과학기술원 정보통신공학 석사
2016년~현재: 광주과학기술원 전기전자컴퓨터공학 박사과정
관심분야: 블록체인, 신호 및 시스템, 압축센싱, 레이더
E-mail: jjh2014@gist.ac.kr

Heung-No Lee

Heung-No Lee (SM'13) received the B.S., M.S., and Ph.D. degrees from the University of California, Los Angeles, CA, USA, in 1993, 1994, and 1999, respectively, all in electrical engineering. He then worked at HRL Laboratories, LLC, Malibu, CA, USA, as a Research Staff Member from 1999 to 2002. From 2002 to 2008, he worked as an Assistant Professor at the University of Pittsburgh, PA, USA. In 2009, he then moved to the School of Electrical Engineering and Computer Science, GIST, Korea, where he is currently affiliated. His areas of research include information theory, signal processing theory, communications/networking theory, and their application to wireless communications and networking, compressive sensing, future internet, and brain-computer interface. He has received several prestigious national awards, including the Top 100 National Research and Development Award in 2012, the Top 50 Achievements of Fundamental Researches Award in 2013, and the Science/Engineer of the Month (January 2014).
E-mail: heungno@gist.ac.kr