51% 공격에 저항 가능한 신규 합의 알고리즘

김인영, 박지수, 이창훈*
서울과학기술대학교 컴퓨터공학과
e-mail : {somem123, qkrtk27, chlee}@seoultech.ac.kr

New consensus algorithm against 51% attack

In-Yeung Kim, Ji-Soo Park, Chang-Hoon Lee*
Dept of Computer Science and Engineering, Seoul National University of Science and Technology

요 약

블록체인은 암호화폐의 기반이 되는 기술로 데이터를 P2P 분산 방식으로 체인 형태로 기록하여 보안성과 안전성을 갖췄다. 중앙 집권화에서 벗어나 사용자들의 네트워크에서 자유롭고 안전한 거래를 가능하게 하는 블록체인은 현재 스마트 계약, 암호화폐, 개인 정보 인증 등 다양한 방법으로 활용되고 있다. 블록체인 사용자들은 거래의 안전성을 위해 채굴이라는 과정으로 블록을 인증하는데 절반 이상의 해시파워를 가진 공격자가 거래내역을 조작하는 것이 51% attack 이다. 채굴자들은 채굴을 위해 전문 장비를 개발하고 이익을 도모하기 위해 모이면서 큰 집단으로 모이면서 51% attack 에 대한 공격가능성이 높아졌고 실제로 엄청난 피해를 입힌 공격 사례가 있다. 따라서 본 논문은 51% attack 의 사례와 기존 대응방안인 PoS 방식과 dPoW 방식 및 각 방식에 대한 한계를 분석하였고 이를 보완한 새로운 블록체인 모델을 제안한다.

1. 서론

블록체인은 데이터들을 블록에 모아 P2P 방식으로 체인을 만들어 연결해 나가는 기술이다.[1] 블록체인은 분산데이터 저장기술로 사용자들에 의해 서버가 운영되고 데이터들을 분산 저장 하여 공격자가 임의적으로 데이터를 변경하지 못하게 한다.[2,3]

또한 블록체인은 해시함수 SHA-256 과 디지털서명 ECDSA 를 사용함으로써 데이터의 무결성과 신뢰성을 보장한다.[4] 블록체인은 이러한 구조를 바탕으로 거래의 보안성과 활동감사 추적 가능성으로 현재 스마트계약, 암호화폐, 개인정보 인증 등 다양한 방법으로 활용되고 있다.

암호화폐는 블록체인 기술로 발행되고 있는 가상통화로 중앙 기관이 존재하지 않는 대신 P2P 분산 네트워크 서버에 의해서 자유로운 거래가 이뤄진다. 블록체인의 안전성은 채굴자 (miner)들의 네트워크에 의해 암호 퍼즐을 푸는 것으로 성립된다. 블록체인에서 더 많은 채굴 능력(mining power)은 가장 먼저 퍼즐을 풀 수 있는 기회를 더 많이 갖게 됨을 의미한다. 채굴자들은 채굴능력을 모으기 위해 풀(pool)을 형성하여 더 많은 이익을 추구해왔다.[5] 하지만 풀에 채굴자들이 악의적인 의도로 결합하여 51%의 점유율을 가지면 거래 내역을 조작할 수 있는 방법이 있다. 이를 51% attack 이라 한다.

본 논문은 51% attack 의 공격 가능성을 조사하고 이로 인해 나타날 수 있는 문제와 해결안을 분석하였다. 이것은 향후 블록체인에서 51% attack 을 방지하는 방안 마련의 기초가 될 것이다.

본 논문의 2 장에서는 51% attack 방법에 대해 설명하고, 3 장에서는 51% attack 의 위험성과 사례를 설명한다. 4 장에서는 51% attack 의 기존 대응 방안을 분석하고 5 장에서는 대안 블록 체인 모델을 제시한다. 마지막 6 장에서는 본 논문을 결론을 맺고 향후 연구 방향을 제시한다.

2. 51% attack 방법

51% attack 이란 공격자 혹은 공격자 그룹이 전체 해시파워의 50% 이상을 점유하고 있을 때 일어날 수 있는 공격이다. 마이닝 과정에서 블록을 생성할 때 두개의 최신 블록이 거의 동시에 생성될 경우 블록체인은 일시적으로 두 갈래로 나뉘어 질 수 있다. 이때 대다수가 선택한 블록으로 체인이 이어지게 되는데 공격자는 이를 악용한다. 공격자는 임의로 블록을 두 갈래로 나눈 후 나뉘어진 체인 각각에 거래내역을 만들고 메인 체인을 교체한다. 그렇게 한 체인의 거래내역이 취소되어 일어나는 이중지불로 공격자는 부정한 이득을 취한다. 이를 51% attack 이라 한다. 51% attack 의 방법은 다음과 같다.[6,7]

① 51%의 점유율을 가진 공격자는 [그림 1]과 같이 병렬로 비공개 채굴을 시작한다. 이들이 생성하는 블록은 나머지 채굴자들이 생성하는 체인과 병렬로 실행된다. 공격자를 제외한 나머지 49%는 이를 알지 못한다.

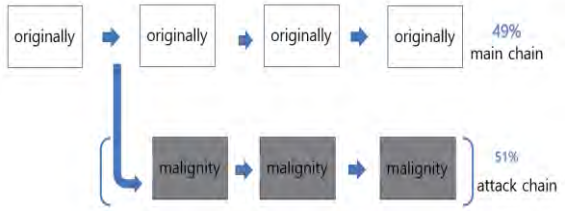
* 교신저자: (chlee@seoultech.ac.kr)

② 공격자가 보유한 가상화폐를 거래소 계좌로 보낸다. 그리고 거래소로 보내는 것을 무효화 하기 위해서 [그림 2]와 같이 자신이 가지고 있는 다른 계좌로 가상화폐를 보내는 블록을 비공개 블록에 추가시킨다. 공격자는 메인 체인 블록과 비공개 블록체인 양쪽에 거래내역 블록을 추가시킨 것이다.

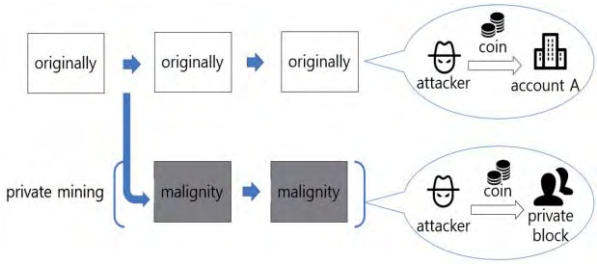
③ 공격자는 [그림 3]과 같이 블록의 안정성을 확인하는 개수의 블록이 생성되는 시간만큼 블록 생성을 기다리며 비공개 채굴을 지속한다.

④ 블록 개수가 충분히 쌓여 거래소로 보낸 기록이 확인이 되면 [그림 4]와 같이 거래소에 해당 화폐를 팔아 다른 화폐를 구매하고 본인의 계좌로 보낸다.

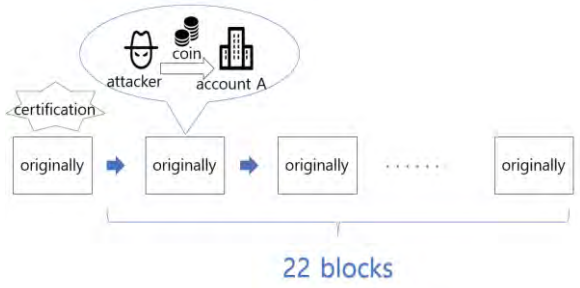
⑤ [그림 5]와 같이 비공개로 채굴한 블록을 공개하여 메인 체인이 바뀌게 한다. 51%가 만든 체인의 길이가 나머지가 만든 길이보다 길어 메인 체인이 교체된다. 공격자가 거래소로 보낸 기록은 무효화가 되어 공격자는 가상 화폐를 거래소로 보내지 않은 것 과 가상 화폐를 거래소에 보내 다른 화폐를 산 것으로 자산을 2 배로 늘리게 된다.



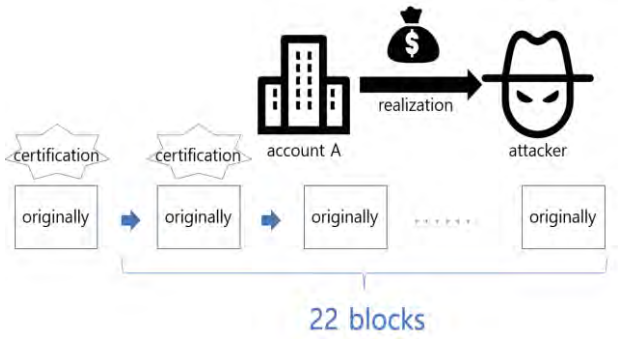
(그림 1) 비공개 채굴



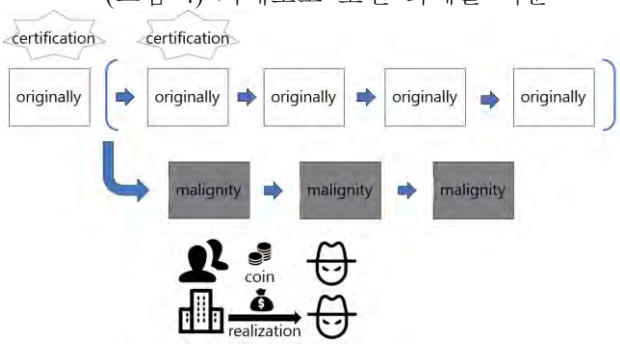
(그림 2) 이중지불을 위한 거래 내역 등록



(그림 3) 공격자의 안정성 확보 대기



(그림 4) 거래소로 보낸 화폐를 처분



(그림 5) 메인 체인을 비공개 체인으로 교체

3. 51% 공격의 위험성

해시파워는 블록체인 네트워크에서 채굴자들의 채굴 능력을 의미한다. 블록체인의 채굴자들은 더 많은 보상을 얻기 위해 해시파워를 높이기 시작했다. 채굴자들은 전문 장비를 개발하기도 하고 안정적으로 블록을 채굴하기 위해 채굴자들의 연합체인 마이닝풀을 형성했다. 마이닝풀은 채굴자들의 해시파워를 병렬적으로 모아 블록을 채굴할 확률을 높이고 이에 기여한 만큼 보상을 배분한다.

예를 들어 채굴자들은 특정한 용도에 집중한 반도체인 ASIC(Application-Specific Integragted Circuit)로 채굴에 특화된 전문 채굴장비를 만들어 해시파워를 높였다. 전문 채굴장치인 AntMiner S7 의 경우 473 만 Mhash/s 의 해시파워[8]를 가지며 비트코인 채굴량중 19.6% 의 점유율을 가진 BTC.com 은 9.9Ehash/s 의 해시파워[9]을 갖추고 있다. 이렇게 소수의 사람, 그룹들에게 해시파워가 집중되면서 51%공격의 가능성이 증가하고 있다.

채굴경쟁이 치열한 비트코인과 달리 후발 암호화폐를 통칭하는 알트코인은 그 규모가 작다. 51%공격을 하는데 필요한 금액이 시간당 500 달러 미만인 알트코인으로는 현재 2018 년 9 월 기준으로 Dogecoin, Bytecoin, Metaverse ETP, Vertcoin 등 수십가지 가상화폐가 존재한다.[10] 이렇게 소수에게 집중되고 있는 채굴파워는 전체 체굴량이 작은 알트코인에게 51%공격 위협이 되고있다. [표 1]은 발생한 51%공격과 공격에 대한 대응이다.

실제로 비트코인 골드는 2018 년 5 월달, 51%공격을

감지했고 공격자는 자신의 지갑으로 388,200 BTG 인 1860 만 달러를 전송했다.[11] 공격 직후 비트코인 골드 개발팀은 공격에 대응하기 위해 거래 완결성 안전의 기준을 20 개에서 50 개 블록으로 상향 조정했다.
일본에서 시작된 모나코인은 2018 년 5 월 13 일 발생한 51% attack 으로 인해 약 1 억원의 피해를 입었다. 모나코인은 공격에 대응하여 완결성기준을 늘리고 거래소의 입금을 정지시켰다.[12]
젠캐시의 경우 2018 년 6 월 2 일 7500 만원의 피해를 입었다. 젠캐시의 개발진들은 공격에 대하여 해시파워 분배를 조절했고, 거래소측과 연결해 거래 확인 시간을 늘리도록 조정했다.[13]

피해 화폐	피해 금액	대응
비트코인골드	약 200 억원	거래 완결성 기준 상향조정
모나코인	약 1 억원	거래 완결성 기준 상향조정, 거래소 입금정지
젠캐시	약 7500 만원	거래 완결성 기준 상향조정, 해시파워 분배 조절

(표 1) 51%공격 사례와 대응

4. 기존 대응 방안 분석

51%공격의 대응방안으로는 컴퓨팅 자원을 소모하여 블록의 타당성을 증명하는 기존의 자원증명 방식인 PoW(Proof-of-Work) 방식을 PoS(Proof-of-Stake) 방식으로 바꾸는 방법이 있다. PoS 방식은 지분증명방식으로 많은 지분을 가지고 있는 사람에게 이자로 보상이 지급되는 방식이다. PoS 방식에서 51%공격을 위해서는 컴퓨팅자원과 별개로 공격자가 가져야 하는 전체 화폐에 대한 지분이 51%이상이어야 한다. 51%공격을 위해서 필요한 금액이 PoW 의 방식보다 더 많은 양의 비용이 들어가므로 51%공격에 대한 보안성이 높아진다.[14]

가상화폐 Komodo 는 51%공격에 대응하기 위해 dPoW (delayed proof of work)방식을 채택했다.[7] dPoW 보안 메커니즘은 블록체인의 백업을 비트코인 원장에 저장하여 비트코인의 해시 속도로 체인을 보호하는 방법이다. 먼저 체인의 스냅샷을 찍어 각 체인의 모든 주소의 자산을 기록하고 그 다음 스냅샷을 체인에 작성한다. 그 다음 이 정보를 블록체인의 블록에 저장한다. 이런 블록을 공증 블록이라고 한다. 이후 블록체인은 가장 최근에 공증된 백업과 일치하는지 확인하고 생성된다. 이 과정은 10 분마다 수행되며 이를 변경하거나 삭제하기 위해서는 비트코인의 체인을 장악해야 한다. 본질적으로 dPoW 방식은 일종의 보험을 제공한다. 공격자는 해당 화폐의 블록체인을 공격하기 위해서는 비트코인의 블록체인의 절반에 해당하는 해시파워를 보유 하고 있어야 한다.

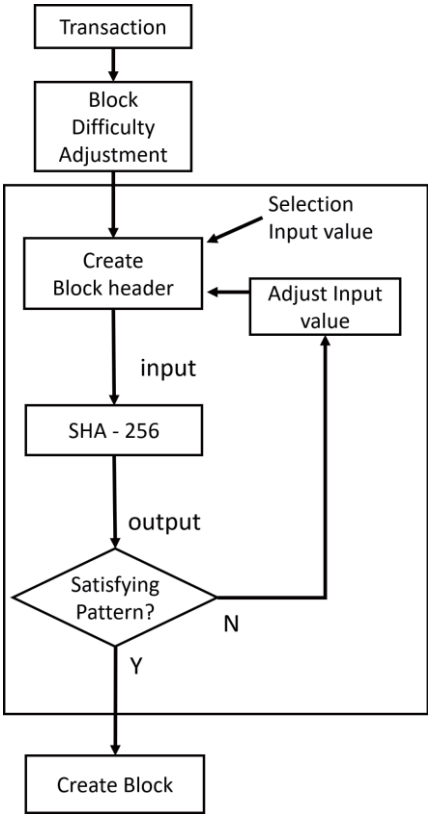
5. 대안 블록 체인 모델

기존의 51%attack 에 대응 방안에는 한계점이 있다. PoS 의 방식은 해시 문제의 공정함은 흉내내지 못한다는 한계점이 있고 dPoW 방식도 공증 블록으로 다른 블록체인에 백업을 저장했기 때문에 그에 대한 수수료를 지불해야 하는 문제점이 있다. 따라서 본 논문에서는 위와 같은 기존 대응 방안의 한계를 보완하기 위해 새로운 모델을 제시하고자 한다.

PoW 방식을 유지하면서 오랫동안 채굴을 진행해 왔던 채굴자들의 채굴 난이도를 낮춰 신규 대형공격자들에게 대항할 수 있는 방법을 제시한다. 이 방법은 다음과 같이 진행된다.

1. 일정시간 동안 진행된 거래를 모아 하나의 블록을 만든다.
2. 블록의 난이도를 조절해 오랫동안 채굴한 노드들에게는 쉬운 난이도의 블록을 제공하고 새롭게 채굴을 시작한 노드들에게는 어려운 난이도의 블록을 제공한다.
3. 모든 노드들은 생성된 블록을 검증하기 위해 채굴 난이도에 따른 연산작업을 수행한다.
4. 검증 작업을 완료하면 블록을 기존 체인에 추가하고 블록체인을 업데이트한다.

전체적인 알고리즘은 [그림 6]과 같다.



(그림 6) 제안하는 알고리즘

기존의 PoW 방식은 블록안에 있는 nonce 값을 1 씩 증가시키면서 난이도를 조절하는 값인 x 에 대해 조건을 만족하는 해시값을 찾는 것을 반복한다. PoW 방식은 해시 함수를 h(.)로 표시할 때 (1)과 같은 조건을 만족한다면 n 번째 블록에 대한 증명 작업이 완료된다. [4]

$$h(\,h(n-1\ \text{th block header}\,)\,||nonce) < x \qquad (1)$$

본 논문에서 제시하는 방법은 시간에 따른 난이도 조절 값을 t 로 표시할 때 (2)와 같은 조건을 만족한다면 n 번째 블록에 대한 증명 작업이 완료되는 방법이다. 오래 채굴한 노드들에게 기존의 x 값보다 더 큰 x 값이 들어간 블록을 제공하여 다른 노드들보다 블록을 채굴할 확률을 높여준다.

$$h(\,h(n-1\ \text{th block header}\,)\,||nonce) < tx \qquad (2)$$

누적 시간 비율	상위 20%	상위 50%	상위 70%	신규
t 값	1.333	1.143	1.067	1
보강된 해시파워	133.3%	114.3%	106.7%	100%

(표 2) 누적 시간에 따른 해시파워

(표 2)와 같이 동등한 해시 파워를 가지고 있는 사용자라도 누적 시간에 따라 난이도가 조정되며 해시파워가 보강된다. 신규 사용자의 t 값을 1 라고 하면 상위 20%의 사용자는 1.333 의 t 값을 가지고 상위 50%의 사용자는 1.143 의 x 값을 가진다. 상위 70%의 사용자는 1.067 의 t 값을 가진다. 모든 채굴자는 t 값에 따른 해시파워를 보강 받는다.

이 방법을 사용하면 51% attack 에 대해 저항성을 가지게 된다.

5. 결론

본 논문에서는 51% 공격에 대한 정의와 실제 일어난 사례 그리고 그의 대응방안에 대해서 살펴보았다. 블록체인은 비트코인과 함께 2009 년에 개발되었다. 그 이후 전 세계적으로 굉장한 가상화폐와 블록체인에 대한 관심을 가졌고 그에 대한 활발한 연구도 함께 이루어 졌다. 블록체인이 미래를 바꿀 기술이라는 믿음으로 투기 열풍이 불기도 했고 많은 가상화폐들도 나오게 됐다. 그렇게 블록체인이 우리에게 익숙해질 때, 불가능하다고 여겨졌던 51%공격이 실행되었다. 블록체인의 51%를 장악하기 위해서는 막대한 예산이 필요한데 그를 블록체인에 투자한 공격자는 가상화폐의 신뢰도가 떨어지게 하는 공격을 할 수 없다는 이유로 불가능하다고 여겨졌던 공격이었다. 그러나 이는 높은 해시파워를 바탕으로 모인 마이닝 풀이 소규모 해시파워를 가진 가상화폐로 51% attack 을 감행할 때 얘기가 달랐다. 그들은 실제로 51% attack 을 실행했고 그에 대해 막대한 피해가 발생했다. 여전히 그들은 다른 소규모 가상화폐들의 위협이 되고있다. 가상화폐들은 PoS 로 컴퓨팅 자원의 소모가 아닌 지분 소유율에 따른 채굴 방식으로 바꾸거나 dPoW 방식으로 안전한 체인에 기대는 등의 대응을 하고있다. 그러나 이들 또한 마찬가지로 완벽하게 51%공격과 미래의 어떤 공격에 대해 저항성이 있다고는 말하기 힘들다.

본 논문에서는 기존의 pow 방식에 시간 개념을 더해 새로운 채굴 방법을 제시 하였다. 그러나 이 방식의 경우에도 오래된 채굴 노드를 구입하여 낮은 난이도를 가진 블록을 획득한 다음 공격자가 가지고 있는 다른 모든 노드에 공유하여 활용될 수 있다는 문제점을 가지고 있다. 차후 이에 대한 보안과 연구가 필요하다.

참고문헌

[1] 민병길, 성영조, 박원익. (2018). “비트코인과 블록체인의 쟁점 및 정책적 시사점”. 이슈&진단, 1-27.

[2] Bastiaan, M. (2015). “Preventing the 51%-attack: a stochastic analysis of two phase proof of work in bitcoin”.

[3] 최대선, 옥도민, 장대훈. (2018). “블록체인과 인증”. 한국통신학회지(정보와통신), 11-17.

[4] 이부형, 임연주, 이종혁. (2017). “블록체인 플랫폼에서의 합의 알고리즘”. 한국통신학회 학술대회논문집, 386-387.

[5] 이진우, 조국래, 염대현. (2018). “비트코인 채굴 수익성 모델 및 분석”. 정보보호학회논문지, 303-310.

[6] MentalNomad. (2018). “Anatomy of a Double-Spend / 51% attack”. https://forum.bitcoingold.org/t/anatomy-of-a-double-spend-51-attack/1398.

[7] Diniel. (2018). “The Anatomy Of A 51% Attack And How Komodo Can Help Prevent One”. https://komodoplatform.com/51-attack-how-komodo-can-help-prevent-one/.

[8]최승주, 김종배. (2017). “ASIC 채굴 방식과 GPU 채굴 방식의 채굴성능 비교”. 예술인문사회융합멀티미디어논문지, 829-836.

[9] https://btc.com/stats/pool?pool_mode=day. (2018 년 09 월 11 일).

[10] https://www.crypto51.app. (2018 년 09 월 12 일).

[11] MentalNomad. (2018). “Double Spend Attacks on Exchanges”. https://forum.bitcoingold.org/t/double-spend-attacks-on-exchanges/1362

[12] 윤형석. “모나코인에 BWA 공격, 블록체인은 과연 안전한가?”. 트렌트와칭. https://trendw.kr/2018-05233667.t1m.

[13] 김혜정.” 젠캐시(ZEN), 비트코인골드 · 버지 이어 51%공격 받아”. https://www.blockmedia.co.kr/news/article_view/?gCode=AB100&idx=1934&page=1.

[14] Y. Gao and H. Nobuhara. (2017). “A Proof of Stake Sharding Protocol for Scalable Blockchains”. Proceedings of the Asia-Pacific Advanced Network- journals.sfu.ca.