블록체인 51% 공격 : 위협과 대응 기법 연구

김세림 [1], 김미희 [2]
[1] 한경국립대학교 컴퓨터응용수학부 학부생
[2] 한경대학교 컴퓨터응용수학부 (컴퓨터 시스템 연구소) 교수
tpfla05@hknu.ac.kr , mhkim@hknu.ac.kr(교신저자)

Blockchain 51% Attack : A Study on Treats and Response Techniques

Se-rim Kim[1], Mi-hui Kim[2]
School of Computer Engineering & Applied Mathematics, Hankyong National University

요 약

블록체인은 탈중앙화 시스템의 장점이 알려지면서 다양한 산업에서 활용하려는 시도가 증가하고 있다. 그러나 여러 위협이 존재하며, 본 논문에서는 그 중 51% 공격을 중심으로 그 개념과 실제 사례를 검토하고, 취약성과 문제점, 그리고 대응 기법을 분석하였다. 블록체인의 보안성을 확보하기 위해 단일 합의 구조에 의존하지 않고, 다양한 위협을 포괄할 수 있는 종합적 대응 체계 마련의 필요성을 제시한다.

1. 서론

블록체인은 2009 년부터 비트코인과 함께 등장해 다양한 산업에 확산되며 주목받고 있다[1]. 중앙화된 기관 없이 분산된 참여자들이 거래 내역을 기록하고 검증하는 구조는 높은 투명성과 신뢰성을 제공한다. 이러한 이점에도 불구하고, 블록체인에는 여전히 51% 공격과 같은 심각한 위협이 존재한다.

본 논문에서는 51% 공격과 실제 사례를 살펴보고, 이를 방어하기 위한 대응 기법들을 조사하고 분석해 보고자 한다.

2. 51% 공격 개념 및 사례

51% 공격은 한 그룹의 채굴자들이 네트워크 해시 파워의 과반을 점유할 경우 발생할 수 있는 공격으로, 이중 지불과 거래 기록 조작을 가능하게 한다. 이러한 공격은 주로 작업증명(Proof-of-Work, PoW) 합의 알고리즘에서 발생한다. PoW 는 채굴자가 연산을 반복하며 논스 값을 조정해, 네트워크 난이도 조건을 충족하는 해시 값을 찾는 방식이다. 이 과정은 막대한 연산 능력을 요구하므로 공격 비용이 증가하고, 결과적으로 보안성이 강화된다. 그러나 특정 집단이 해시파워의 절반이상을 장악하게 되면 권력을 독점할 수 있어 51% 공격이 발생한다.

실제로 2018 년 비트코인 골드는 공격자 자신의 지갑으로 1860 만 달러를 전송한 것을 감지했다. 또한 젠캐시의 경우 2018 년 7500 만원의 피해를 입었다. 이러한 사례[2]들은 대규모 네트워크에서는 공격이 현실적으로 어렵지만, 상대적으로 해시파워가 적은 소규모 암호화폐에서는 실질적인 보안 위협으로 이어질 수 있음을 보여준다.

3. 51% 공격의 취약성과 문제점

51% 공격의 가장 큰 취약성은 이중 지불이다. 공격자는 거래소나 개인에게 송금한 후, 자신이 장악한 해시파워를 이용해 동시에 더 긴 체인을 형성하며 기존 거래를 무효화할 수 있다. 이 과정에서 공격자는 자산을 돌려받으며, 결과적으로 이중 지불 공격이 성공하게 된다.

그러나 문제는 단순한 경제적 피해를 넘어 51% 공격이 발생하거나 그 가능성이 제기되는 것만으로도 블록체인 네트워크 보안성의 신뢰성 저하를 불러온다. 투자자와 사용자들은 거래가 안전하게 이루어지지 않는다고 판단할 수 있으며, 이는 산업 전반의 불안정성으로 이어진다.

또한 해시파워가 소수의 채굴 풀이나 임대 서비스에 집중되는 현상은 공격과 별개로 네트워크 중앙화 문제를 야기한다. 이러한 문제는 블록체인의 핵심 특성으로 평가되는 탈중앙성, 불변성, 투명성을 훼손한다.

한 시뮬레이션 연구[2]에 따르면, 공격자가 해시파워의 30%를 보유한 경우에도 5 블록 뒤에서 정직한 체인을 따라잡을 확률은 약 0.18 에 이른다. 이는 거래가 얕은 깊이에 있을 때는 공격 위험이 존재함을 보여준다. 그러나 블록 깊이가 6 이상에 도달하면 되돌

릴 가능성은 극히 낮아지며, 이는 블록체인이 안정 상태에 도달했음을 의미한다.

따라서 51% 공격은 단순한 공격을 넘어, 배제할 수 없는 위험성 자체가 네트워크 신뢰를 약화시키고 있다.

4. 대응 기법 분석

4.1 지분증명(Proof-of-Stake, PoS) 전환

51% 공격의 가장 기본적인 대응 방안은 기존의 자원증명 방식인 PoW 방식을 PoS 방식으로 바꾸는 방식이다. PoS 방식은 지분증명방식으로 많은 지분을 가지고 있는 사람에게 이자로 보상이 지급되는 방식이다. 이로 인해 단순히 해시파워를 집중하는 것만으로는 네트워크 장악이 어렵다. 기존의 PoW 방식보다 공격에 필요한 비용이 더 많이 들어가므로 51%에 대한 보안성이 높아진다.

4.2 지연작업증명(Delayed-Proof-of-Work, dPoW)

dPoW 방식은 보안성이 높은 외부에 자체 블록을 저장해 기록하는 방법이다. 관련 사례로, 가상화폐 Komodo 는 자사의 블록을 비트코인 원장에 기록하며 외부 체인의 강력한 해시파워를 활용한다. 이후 Komodo 블록체인은 새로운 블록을 생성할 때 가장 최근에 공증된 백업과 일치하는지 확인하며 무결성을 검증한다[3].

이 방식은 상대적으로 보안 수준이 낮은 체인이 강력한 체인의 보안성을 이용한다는 점에서 효과적이다. 본질적으로 dPoW 방식을 공격하려면 비트코인 블록체인의 절반에 해당하는 해시파워를 보유하고 있어야 되기 때문에, 이는 추가적인 보안 안정망 역할을 제공한다.

4.3 시간 기반 난이도 조정 기법

기존 PoW 합의 방식에서는 네트워크 전체에 동일한 난이도가 적용되며, 모든 채굴자가 같은 조건에서 연산을 수행해야 한다. 이에 대한 대응으로 시간 기반 난이도 조정 기법이 있다[3]. 이 방식은 PoW 방식을 유지하면서 장기간 진행해온 채굴자들의 채굴 난이도를 낮추고, 새롭게 진입한 채굴자들에게는 더 높은 난이도가 적용된다.

따라서 장시간 참여한 채굴자는 블록 생성 확률이 높아지는 반면, 단기적으로 해시파워를 집중하려는 공격자의 성공 가능성은 크게 낮아진다.

4.4 네트워크 및 보안 관리

51% 공격은 합의 구조 자체의 한계에서 비롯되므로, 단순한 기술적 개선만으로는 근본적인 차단이 어렵다. 따라서 공격 발생 가능성을 낮추고 피해를 최소화하려면, 네트워크와 보안 관리가 동시에 이루어져야 한다.

먼저 보안 강화를 위해 블록체인 네트워크 상태를 실시간으로 모니터링해야 한다. 블록 생성 속도, 해시파워 분포 등을 지속적으로 관찰하면, 평소와 다른 이상 현상을 초기 단계에서 발견할 수 있다.

또한 탐지된 정보를 활용하여 보안 관리 체제 구축도 중요하다. 예를 들어, 사용자 인증과 권한 부여 등 액세스 제어를 강화하여 불법적인 접근을 차단할 수 있다. 이와 더불어, 스마트컨트랙트 보안 강화, 통신 프로토콜 암호화 등 보안 관리 조치도 병행한다면 블록체인 네트워크 전반의 보안성을 한층 높일 수 있다.

5. 종합적 대응체계 필요성

블록체인에는 51% 공격 외에도 다양한 위협이 존재한다. 예를 들어, 분산 서비스 거부 공격(Distributed-Denial-of-Service, DDoS)은 과도한 트래픽으로 블록체인 네트워크를 마비시켜 블록체인의 정상적인 운영을 방해한다. 또한 이클립스 공격은 네트워크 연결을 독점해 사용자를 고립시킨 뒤, 공격자의 의도에 따라 조종할 수 있도록 충분한 IP 주소를 확보해 공격한다. 이처럼 여러 위협이 공존하는 상황에서는 각 위협에 대한 별도의 대응체계만으로는 충분하지 않으며, 종합적인 보안 대응 체계를 구축하는 것이 더 효율적이며 안정성을 높일 수 있다.

6. 결론

본 논문에서는 블록체인 보안 위협 중 51% 공격의 개념, 실제 사례, 취약성과 문제점을 검토하고, 이에 대응하기 위한 다양한 대응 기법을 분석하였다. 51% 공격은 블록체인의 구조적 한계를 보여주며, 이중지불과 신뢰성 저하라는 심각한 문제를 야기한다. 그러나 블록체인은 지속적으로 발전하고 있으며, 51% 공격 이외에도 DDoS, 이클립스 등 다양한 위협이 존재한다. 따라서 특정 구조에 한정되지 않고, 블록체인의 종합적 보안 대응 체계를 마련하는 노력이 필요하다. 이에 따라 향후에는 이러한 체계를 설계하고 검증하는 연구를 지속적으로 수행할 계획이다.

사사 (Acknowledgement)

이 논문은 한경국립대학교 국립대학육성사업(2025) 지원을 받아 작성되었음

참고문헌

[1] 이은영 외 3인,“블록체인 네트워크 보안 위협 탐지 기술 동향 분석”, 정보보호학회지, 제 31 권 제 3 호, 2021, p.61-71

[2] Congcong Ye 외 4 인, “Analysis of Security in Blockchain: Case Study in 51%-Attack Detecting”, International Conference on Dependable Systems and Their Applications (DSA), 2018, p.16-24

[3] 김인영 외 2 인, "51% 공격에 저항 가능한 신규 합의 알고리즘", 추계학술발표대회 논문집, 제 25 권 제 2 호, 2018, p.288-291