통신망 지연이 다양한 블록체인 프로토콜에 미치는 영향에 관한 연구

이우용
한국전자통신연구원

wylee@etri.re.kr

A Study on the Effect of Communication Network Delay in Various Blockchain Techniques

Lee Woo Yong
Electronics and Telecommunications Research Institute (ETRI)

요 약

최근 연구로 다양한 형태의 블록체인 프로토콜에 대한 분석이 통신모델 기반으로 수행되었다. 본 연구에서는 통신망 지연이 다양한 블록체인 프로토콜에 어떤 영향을 끼칠 수 있는지 분석한다. 분석 과정에서 복잡한 증명과정은 모두 생략했고 직관 (insight) 중심으로 설명했다. 채굴 속도가 커짐에 따라 병렬로 채굴되는 블록 수 역시 증가되고 통신망의 지연으로, 최장 체인 분기 선택 규칙에서 안정성(Security)이 저하되는 것으로 알고 있었다. 하지만 본 결과는 단순해 보이지만 통신망 지연이 블록체인 프로토콜 안정성에 영향을 주지 않는다는 중요한 결과를 도출한 것으로 보인다.

Ⅰ. 서 론

2008년 나카모토 사토시는 분산 원장을 유지하기 위한 기술로 블록체인 개념을 고안했다[1]. 최근 연구로 다양한 형태의 블록체인 프로토콜에 대한 분석이 통신모델 기반으로 수행되었다[2-4]. 이러한 연구의 핵심적인 기여는 가장 긴 체인 프로토콜, 아주 단순한 합의 알고리즘이라는 것이다. 기존 비트코인 프로토콜은 PoW (Proof of Work, 작업증명) 설정의 맥락에서 고안되었지만, 가장 긴 체인 프로토콜은 많은 블록체인 기법에서 채택되었으며, PoS (Proof of Stake, 지분증명)[5-7] 및 PoSpace (Proof of Space, 공간증명)[8]와 같은 다른 에너지 효율 설정으로 확장되었다.

개인정보의 관리와 공유에 있어서 모범적인 모델 중 하나는 분산원장 기반의 정보 유통 서비스 모델이다[9-10]. 이러한 분산원장 기술의 특성은 다수의 노드가 참여하는 분산형 데이터베이스를 이용하여 신뢰성을 제공하고, 디지털 서명과 해시 값을 이용하여 검색 자료에 대한 투명성을 보증함에 있다. 이러한 안정성 보장에 대한 분석을 위하여 [11]는 체인 공통 접두, 체인 품질, 및 체인 성장의 주요 근간(backbone) 속성을 정의하여 블록체인 보안 분석을 시작했다.

최장 체인 프로토콜을 분석하기 위하여 잠금 단계별 연속 순환(lock step round by round) 모델에서 작업증명 체계(framework)를 적용할 때, 분석하기 가장 어려운 특성인 공통 접두 특성이, 긴 창에서 공격자 블록의 수가 독보적으로(uniquely) 성공적인 정직한 블록 수보다 적다면, 충족됨을 알 수 있었다[11]. 유사한 블록 집계(counting) 분석은 Δ-동기 모델의 경우 [12]에 의해 수행되며, 독보적 성공 블록의 개념은 수렴 기회 개념으로 대체되었다. 지분 없음(NaS: Nothing-at-Stake) 문제로 인해 지분증명의 가장 긴 체인 프로토콜을 분석하기 위한 블록 집계 기술은 완전히 실패한다[5-8].

이 문제를 극복하기 위해 두 가지 새로운 아이디어가 고안되었다. 우로보로스 프라오스(Ouroboros Praos) 연구[5]에서 새로운 분할 끈(strings) 개념이 발명되었고, 공격자 지분이 문턱 값(threshold) 미만인 경우, 공격자 행동에 관계없이 가장 긴 체인의 수렴을 보여주기 위해 마코프(Markov) 체인 분석이 수행되었다. 슬리피 컨센서스(Sleepy Consensus)와 스노우화이트(SnowWhite) [6-7]는 서로 다른 접근 방식을 취하고 중심점(pivot) 개념을 정의했다.

본 논문에서는 이러한 다양한 블록체인 프로토콜을 블록 제안에 대한 추첨 방식의 관점에서 두 가지 부류로 분류하고 통신망 지연이 프로토콜에 어떤 영향을 끼칠 수 있는지 분석한다.

Ⅱ. 블록체인 기법에서 통신 지연 영향에 관한 분석

가장 긴 체인 채택하는 프로토콜은 1) 원래 나카모토 작업증명 프로토콜; 2) 우로보로스[5] 및 스노우화이트[6-7] 지분증명 프로토콜; 3) 치아(Chia) 공간증명 프로토콜[8]로 분류할 수 있다. 2)와 3)은 모두 가장 긴 체인 규칙을 사용하지만 블록 제안에 대한 추첨 방식이 다르다. 즉 2)의 경우는 다른 블록에 동일한 무작위성(randomness)이 사용되지만, 3)의 경우 여러 블록들에 독립적인 무작위성이 사용된다. 본 논문에서는 무작위성 추첨 형태가 종속적인 1)과 2)에 해당하는 프로토콜(PoW & PoS)과, 독립적인 무작위성 3)의 최장 체인 프로토콜(PoSpace)로 나누어 통신 지연에 대한 영향과 조건을 분석한다.

개방(permissionless) 환경에서 가치 있는 자산의 원장을 유지하는 데 사용되는 가장 긴 체인 프로토콜의 가장 중요한 속성은 보안(security, 안정성)이다. 나카모토는 특정 공격, 개인 이중-지불 공격을 제안하여 이 속성을 분석했다[1]. 공격자는 공개적으로 가장 긴 체인을 능가하기 위해 경쟁에서 개인 비공개 블록체인을 키워 공개 체인에서 한 블록의 깊이가 최장 길이로 깊어지면 이를 대체한다. λ_h와 λ_a는 각각의 해시 파워에 비례하는 정직한 노드와

공격자의 채굴 속도라고 하자. 그렇다면 $\lambda_a > \lambda_h$ 라면, k 가 아무리 길더라도 공격자는 높은 확률로 공격을 성공할 것이라는 것은 큰 수의 법칙으로부터 명백하다. 반대로, $\lambda_a < \lambda_h$ 이면, 공격자의 성공 확률은 k 와 함께 기하 급수적으로 감소한다. 정직한 노드간에 네트워크 지연이 Δ 인 경우 보안에 대한 조건은 다음과 같다[5]:

$$\lambda_a < \frac{\lambda_h}{1+\lambda_h \Delta} \quad (1)$$

여기서 $1+\lambda_h\Delta$는 정직한 체인의 성장률에 대한 네트워크 지연의 영향이다. 우리가 β를 공격자 힘의 비율이라면, (1)은 다음과 같은 조건을 산출한다.

$$\beta < \frac{1-\beta}{1+(1-\beta)\lambda\Delta} \quad (2)$$

여기서 λ 는 총 채굴 속도이고 $\lambda\Delta$ 는 네트워크 지연당 채굴된 블록 수이다. 등식으로 (2)를 풀면 [Nak08]에서 나카모토의 중심 주장으로 이어진다. 공격자가 전체 해시 성능의 50% 미만이고 채굴 속도가 낮게 설정되어 있으면 가장 긴 체인 프로토콜이 안전하다. 블록체인 속도를 높이기 위해보다 적극적인 채굴 속도는 보안 임계 값을 줄인다. 따라서 (2)는 보안과 통신 지연을 포함한 블록 생성 속도 사이의 절충으로 볼 수 있다. 이때 통신 지연이 블록체인 보안에 어떤 영향을 주는지 분석해 볼 것이다.

우선, 무작위성 추첨 형태가 종속적인 1)과 2)에 해당하는 프로토콜(PoW & PoS)에서 통신망 지연을 포함한 블록 생성 속도 사이에서 보안을 위한 조건은 (2)에 해당한다. 공격자 힘의 비율 β의 영향이 거의 없는 경우 즉, $\beta \approx 0$ 는 통신망 지연이 블록체인 보안에 어떤 영향도 없는 것이 자명해 보인다. 하지만, 공격자 힘의 비율 β의 영향이 최고조에 달했을 때 즉 $\beta \approx 0.5$ 인 경우를 분석하는 것이 중요할 것이다. 이때 공격자의 채굴 속도 조건은 다음과 같은 조건으로 표현이 가능하다.

$$\lambda\Delta < \frac{1}{\beta} - \frac{1}{1-\beta} \quad (3)$$

(3)의 조건은 $\beta \approx 0.5$ 인 경우를 0 으로 근사화 된다. 그러므로 $\lambda\Delta$ 는 통신망 지연당 채굴된 블록 수의 영향은 거의 없는 것으로 분석할 수 있다.

두 번째 무작위성 추첨 형태가 독립적인 3)의 프로토콜(PoSpace)에서 통신망 지연을 포함한 블록 생성 속도 사이에서 보안을 위한 조건은 다음(4)에 해당한다[8].

$$e\beta < \frac{1-\beta}{1+(1-\beta)\lambda\Delta} \quad (4)$$

여기서 e 는 자연상수이고, 무작위성 추첨 형태가 독립적인 영향으로 공격자 힘의 비율의 영향이 $e\beta$로 증폭되는 것이다. 이러한 프로토콜 특성상 공격에 상당한 계산 자원이 필요하지 않기 때문에 이를 지분 없음 (NaS) 공격이라고 한다. 특히 이것은 공격자가 비공개 블록 가지(개인 NaS 가지라고 함)를 빠르게 성장시키고 정직한 체인을 매수할 수 있게 한다.

첫 번째 부류의 프로토콜 분석과 같이, 공격자 힘의 비율 β의 영향이 거의 없는 경우 즉, $\beta \approx 0$ 는 통신망 지연이 블록체인 보안에 어떤 영향도 없는 것이 자명해 보인다. 하지만, 공격자 힘의 비율 β의 영향이 최고조에 달했을 때를 분석하는 것이 중요할 것이다. 이때 공격자의 채굴 속도 조건은 다음과 표현이 가능하다.

$$\lambda\Delta < \frac{1}{e\beta} - \frac{1}{1-\beta} \quad (5)$$

(5)의 조건은 $e\beta \approx (1-\beta)$인 경우를 0 으로 근사화 된다. 이 경우도 (4)의 조건을 만족하는 한 프로토콜은 안전하다고 할 수 있다. 그러므로 $\lambda\Delta$ 는 통신망 지연당 채굴된 블록 수에 대한 영향은 거의 없고, 또한 지분 없음 공격에도 영향을 끼치지 못한다고 할 수 있다.

III. 결론

최근 연구 결과로 다양한 형태의 블록체인 프로토콜에 대한 분석이 통신모델 기반으로 수행되었다. 본 연구에서는 통신망 지연이 다양한 블록체인 프로토콜에 어떤 영향을 끼칠 수 있는지 분석했다. 분석 과정에서 복잡한 증명과정은 모두 생략했고 직관 중심으로 설명했다. 보다 자세한 분석 내용을 알고 싶으면 참고 문헌을 독서하면 될 것이다. 본 결과는 단순하지만 통신망 지연이 블록체인 프로토콜 안정성에 영향을 주지 않는다는 중요한 결과를 도출한 것으로 보인다.

ACKNOWLEDGMENT

이 논문은 2020 년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임. [2018-0-01477, 블록체인 기술을 활용한 스마트헬스 서비스 표준개발].

참 고 문 헌

[1] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008, https://bitcoin.org/bitcoin.pdf.

[2] V. Bagaria, S. Kannan, D. Tse, G. Fantiz, and P. Viswanath, “Prism: Deconstructing the Blockchain to Approach Physical Limits,” ACM SIGSAC Conference on Computer and Communications Security, pp. 585-602, Nov. 2019.

[3] 이우용, 김경표, 유돈식, 최미란, “물리적 한계에 접근하는 블록체인 기법의 보안 취약성에 관한 연구,” 한국통신학회 하계종합학술발표회, pp. 228-9, 2019.

[4] 이우용, 김경표, “통신모델 기반 블록체인 기법의 최장 체인 보장에 관한 연구,” 한국통신학회 추계종합학술발표회, pp. 79-80, 2019.

[5] B. David, P. Gazi, A. Kiayias, and A. Russell, “Ouroboros praos: An adaptively secure, semi synchronous proof of stake blockchain,” International Conference on the Theory and Applications of Cryptographic Tech., pp. 66-98. Springer, 2018.

[6] R. Pass and E. Shi, “The sleepy model of consensus,” Conference on the Theory and Application of Cryptology and Information Security, pp. 380-409. Springer, 2017.

[7] I. Bentov, R. Pass, and E. Shi, “Snow white: Provably secure proofs of stake,” IACR Cryptology Archive, 2016:919, 2016.

[8] B. Cohen and K. Pietrzak, “The chia network blockchain,” https://www.chia.net/assets/ChiaGreenPaper.pdf, 2019.

[9] W. Y. Lee, D. Yoo, D. Y. Lee, and K. P. Kim, “Requirements of distributed ledger systems (DLS) for secure human factor services,” ITU-T Question 24 Study Group 16, Aug. 2019.

[10] W. Y. Lee, D. Yoo, D. Y. Lee , and M. Choi, “Added text on the Requirements of distributed ledger systems (DLS) for secure human factor services,” ITU-T Question 24 Study Group 16, Apr. 2020.

[11] J. Garay, A. Kiayias, and N. Leonardos, “The bitcoin backbone protocol: Analysis and applications,” Annual International Conference on the Theory and Applications of Cryptographic Techniques, pp. 281-310, Springer, 2015.

[12] R. Pass, L. Seeman, and A. Shelat, “Analysis of the blockchain protocol in asynchronous networks,” In Annual International Conference on the Theory and Applications of Cryptographic Techniques, 2017.