논문 22-47-07-09 The Journal of Korean Institute of Communications and Information Sciences '22-07 Vol.47 No.07
https://doi.org/10.7840/kics.2022.47.7.974

탈중앙화 네트워크에서 콘텐츠 전송 증명

박 건 우◆°

Proof of Content Delivery in a Decentralized Network

Kunwoo Park◆°

요 약

본 논문은 탈중앙화 네트워크(Decentralized Network)에서 제3의 신뢰기관 없이 전송된 콘텐츠를 증명하는 방식(PoCD)을 제안한다. PoCD는 콘텐츠를 수신하였음에도 송신자를 보상하지 않는 무임승차자(free-rider)를 식별하고, 해당 무임승차자가 더 이상 콘텐츠를 전송받지 못하도록 네트워크에서 제외한다. 모의실험 결과 무임승차자가 콘텐츠를 완전히 수신하지 못하는 것을 확인하였다.

Key Words : proof of content delivery, free-rider, decentralized network, probabilistic sequential retrieval, Blockchain

ABSTRACT

This paper presents a Proof of Content Delivery (PoCD) mechanism in a decentralized network. PoCD proves content delivery between two peers without any trusted third party. PoCD can detect and exclude a free-riding peer, i.e., it cannot retrieve any more content from the network, which is verified by simulation results.

Ⅰ. 서 론

블록체인과 같은 탈중앙화 네트워크에는 중앙서버나 인증기관 등 신뢰기관이 존재하지 않는다[1]. 따라서 콘텐츠 송신자가 수신자로부터 약속된 보상을 지불 받지 못하더라도 그 수신자(무임승차자, free-rider)에게 취할 수 있는 조치는 제한적이다. 중앙서버가 없어 송신자의 콘텐츠 전송 사실을 객관적으로 증명하기 어렵고, 무임승차자를 제재할 신뢰기관도 없기 때문이다.

탈중앙화 네트워크에 기반한 콘텐츠 전송[2] 또는 저장[3] 프로젝트들은 무임승차자 문제를 소액지불(micropayment) 방식으로 대응한다. 소액지불 방식에서 콘텐츠는 작은 전송단위(chunk)로 분할하여 전송되는데, 콘텐츠 송신자는 각 전송단위에 대한 보상을 수신자로부터 받았을 때만 그 다음 전송단위를 전송한다. 그 결과 송신자는 수신자로부터 보상을 받을 때까지 다음 전송을 지연해야 하므로 콘텐츠 전송 효율이 현저히 저하되는 문제가 발생한다.

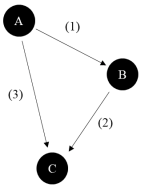
본 논문에서는 블록체인을 활용하여 탈중앙화 네트워크에서 제3의 신뢰기관 없이 전송된 콘텐츠를 증명하는 방식(PoCD, Proof of Content Delivery)을 제안한다. PoCD는 콘텐츠 전송 사실을 네트워크에 공유하므로 모든 피어(peer)가 독자적으로 무임승차자를 식별할 수 있다. 나아가 무임승차자가 콘텐츠 송신자에게 보상을 지불할 때까지 무임승차자를 네트워크에서 제외시킴으로써 무임승차자가 더 이상 콘텐츠를 전송받을 수 없도록 설계되었다.

Ⅱ. 콘텐츠 전송증명

PoCD는 블록체인 지불내역(transaction record)을 활용하여 탈중앙화 네트워크에서 콘텐츠 전송을 증명한다. PoCD는 현존하는 블록체인 지불내역에 콘텐츠의 전송단위 인덱스(chunk index)를 추가로 메모한다. 대표적인 블록체인 프로젝트인 이더리움의 DATA 필드[4]가 이러한 콘텐츠 전송단위 인덱스 메모에 활용될 수 있다. 따라서 PoCD에서의 지불내역은 '누가 누구에게 보상 얼마를 어떤 전송단위에 대하여 지불하였음'을 나타낸다.

그림 1은 세 개의 피어 A, B, C로 구성된 네트워크의 PoCD 지불내역을 나타낸다. 화살표의 시작점은 보상을 지불한 피어(콘텐츠 수신자), 화살표의 끝점은 보상을 수령한 피어(콘텐츠 송신자)를 의미한다. 지불내역 (1)은 콘텐츠 수신자 A가 송신자 B에게 보상 0.1

※ 본 논문의 선행 연구가 IEEE International Conference on Blockchain and Cryptocurrency (ICBC 2019)에 발표되었고, 해당 학술대회 논문집[6]에 게재되었습니다.
◆° First and Corresponding Author : (ORCID:0000-0001-6060-2714)LTER Inc., nusider@gmail.com, 이사, 정회원
논문번호 : 202205-111-C-LU, Received May 27, 2022; Revised June 9, 2022; Accepted June 9, 2022



Transaction Records	Content Receiver	Content Sender	Reward	Chunk Index
(1)	A	B	0.1	#3
(2)	B	C	0.1	#2
(3)	A	C	0.1	#4

그림 1. 세 개 피어로 구성된 네트워크의 지불내역 (좌측은 네트워크 토폴로지, 우측은 지불내역)
Fig. 1. Transaction records of three peers (left shows network topology and right shows transaction records)

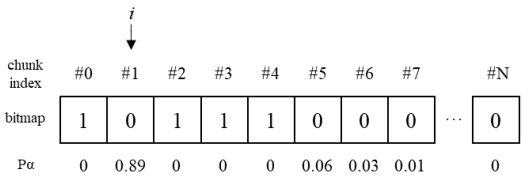


그림 2. 피어 A의 전송단위 인덱스 비트맵 ('1'은 해당 인덱스의 전송단위를 수신했음을 의미함)
Fig. 2. Chunk index bitmap of peer A ('1' indicates that the chunk has been retrieved)

을 전송단위 #3에 대하여 지불하였음을 나타낸다. 콘텐츠 수신자가 송신자에게 보상을 지불하였다는 것은 해당 송신자가 수신자에게 전송단위를 전송하였다는 것도 의미하므로, 지불내역 (1)로부터 송신자 B가 수신자 A에게 전송단위 #3을 전송하였음도 알 수 있다.

PoCD 지불내역은 보상을 지불/수령한 내역이자 콘텐츠가 수신/송신된 내역이다. 모든 피어는 독자적으로 블록체인 지불내역을 분석할 수 있으므로, 각각의 피어는 누가 누구에게 어떤 콘텐츠를 전송하였고 그에 대한 보상이 어떻게 지불되었는지 확인할 수 있다. 즉 PoCD 지불내역은 콘텐츠 수신자의 보상 지불 여부를 증명할 뿐만 아니라 콘텐츠 송신자의 전송 사실 또한 증명하는 것이다.

Ⅲ. 무임승차자 식별 및 제외

PoCD는 전송 효율을 향상시키기 위하여 N개의 전송단위로 분할된 콘텐츠를 확률적 순차전송 (probabilistic sequential retrieval)[5] 방식으로 전송한다. 모든 피어는 하나의 콘텐츠를 구성하는 N개의 전송단위를 모두 수신할 때까지 자신만의 확률함수 $P_\alpha^{i,j}$에 기반하여 전송단위를 요청한다. 그림 2는 특정 콘텐츠에 대하여 피어 A가 수신한 (따라서 지불내역에서 보상을 지불한) 전송단위 #0, #2, #3, #4를 나타내는 비트맵(bitmap)이다.

$P_\alpha^{i,j}$는 피어가 전송단위 j를 요청할 확률로 아래와 같이 정의된다.

$$P_\alpha^{i,j} = \begin{cases} 0 & \text{, if } \#j \text{ is retrieved} \\ \alpha^{j-i+1} \cdot \frac{1}{\beta} & \text{, if } \#j \text{ is not retrieved} \end{cases}$$

여기서 i는 아직 수신하지 못한 가장 낮은 전송단위 인덱스이고 (그림 2에서 i = 1), j는 이번에 요청할 전송단위 인덱스이다 ($i \le j \le N$). α는 각 피어의 위험선호도에 따라 0과 1 사이에서 독자적으로 설정할 수 있는 값이지만 현재로서는 모든 피어가 α를 0.5로 설정한다고 가정한다. 정규화 상수(normalization constant)인 β는 $\sum_{j=i}^{N} P_\alpha^{i,j} = 1$로 조정한다. 그림 2에서 A가 전송단위 #1, #5, #6, #7을 요청할 확률은 각각 0.89, 0.06, 0.03, 0.01이다.

전 장에서 설명한 바와 같이 블록체인에 공개된 지불내역을 바탕으로 누구든지 다른 피어의 현재 전송단위 비트맵을 재구성할 수 있다. 따라서 A가 B에게 전송단위 #6를 요청했을 경우, B는 A의 지불내역을 분석하여 그림 2와 동일한 비트맵을 재구성하고 A가 확률이 더 높은 #1 ($P_{0.5}^{1,1}$ = 0.89)을 아직 수신하지 못했음에도 #6 ($P_{0.5}^{1,6}$ = 0.03)를 요청했다는 사실을 알 수 있다. 만약 B의 위험선호도가 낮다면 B는 A를 무임승차자로 식별하고 A의 #6 요청을 거부할 수 있다. 왜냐하면 A가 실제로 #1을 수신했음에도 보상을 지불하지 않은 무임승차자라면 #6 전송에 대한 보상도 지불하지 않을 가능성이 높기 때문이다. 반면 B의 위험선호도가 높다면 요청받은 #6를 A에게 전송한 후 보상을 기대할 수도 있다.

하지만 A가 #7 ($P_{0.5}^{1,7}$ = 0.01)보다 높은 전송단위를 요청했다면, 위험선호도와 무관하게 B는 A의 요청을 거부할 확률이 높다. A가 #7 보다 높은 전송단위를 요청할 확률은 0.01보다 낮기에 B는 A를 #1에 대한 보상을 지불하지 않은 무임승차자로 식별할 것이기 때문이다. A의 #1 지불내역이 확인되지 않는 한 B를 포함한 모든 피어들은 결국 A를 무임승차자로 식별하고 A의 전송 요청을 거부함으로써 네트워크에서 제외시킬 것이다. 즉, PoCD로 식별된 무임승차자는 콘텐츠 전송단위 N개를 전부 수신하기 어렵게 된다.

앞서 모든 피어가 α를 0.5로 설정한다고 가정했으나 각 피어는 본인의 위험회피/위험선호 성향에 따라 0과 1사이에서 α를 설정할 수 있다. 위험회피 성향이 강하거나 공공 네트워크에 속한 피어는 α를 낮게 설

정하여 잠재적인 무임승차자에게 보수적으로 대응할 수 있다. 반면 위험선호 성향이 강하거나 안전한 사설 네트워크에 속한 피어는 α를 높게 설정하여 적극적인 송신자 역할을 함으로써 높은 보상을 꾀할 수 있다. 어느 경우든지 무임승차자는 결국 식별될 것이고 네트워크에서 제외됨에는 변함이 없다.

Ⅳ. 모의실험 결과

PoCD가 무임승차자를 효과적으로 식별하고 제외하는지 확인하기 위하여 200개 피어의 α를 0.1부터 0.9까지 변화시키며 콘텐츠를 전송받는 모의실험을 진행하였다. 본 실험에서 α = 0.1인 경우 평균 0.1, 분산 0.2를 따르는 정규분포 형태로 피어들의 α가 설정되었음을 의미한다. 각 피어는 총 100개의 전송단위로 분할된 콘텐츠를 전송받는데, 200개 피어 중 무임승차자로 설정된 피어는 #10 전송단위에 대한 보상을 지불하지 않았다.

그림 3은 무임승차자가 총 100개의 전송단위 중 최종적으로 수신한 전송단위의 개수를 나타낸다. 앞서 살펴본 바와 같이 α가 낮게 설정되면 피어들의 높은 위험회피 성향이 반영되어 무임승차자의 전송 요청이 대부분 거부된다 (α = 0.1인 경우 평균 12.4개 수신). 반면에 α를 높게 설정하면 상대적으로 많은 무임승차자의 요청이 승인된다 (α = 0.9인 경우 평균 63.8개 수신). 하지만 어느 경우에도 무임승차자는 결국 네트워크에서 제외되어 콘텐츠 전송단위 100개를 전부 수신하지 못하는 것을 확인할 수 있다.

그림 4에서는 무임승차자가 네트워크에 미치는 영향을 살펴보았다. 네트워크에 존재하는 무임승차자의 비율을 달리하며 무임승차자를 제외한 모든 피어가 콘텐츠를 완전히 전송받기 위하여 필요한 반복시행

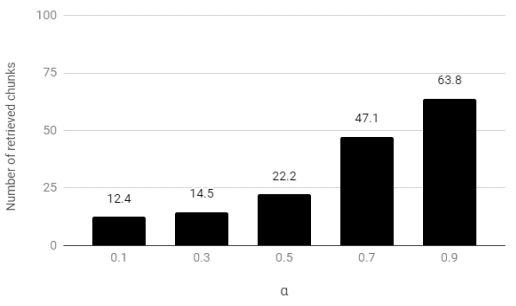


그림 3. α에 따라 무임승차자가 수신한 전송단위 개수
Fig. 3. Number of retrieved chunks of a free-rider according to α

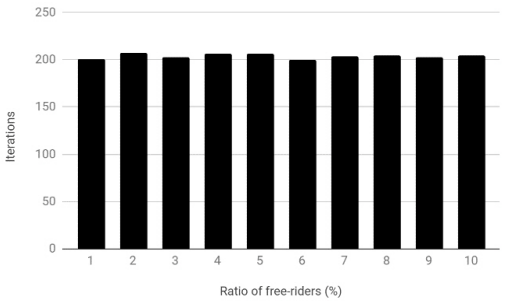


그림 4. 콘텐츠 수신에 필요한 반복시행 횟수
Fig. 4. Number of iterations required to retrieve a content

횟수가 세로축에 표현되었다. 무임승차자의 비율이 달라지더라도 필요한 반복시행 횟수가 거의 일정하게 유지(최소 199.4회, 최대 207.4)됨을 알 수 있다. 이는 PoCD가 무임승차자를 효과적으로 식별하고 네트워크에서 제외시킴으로써 정상 피어들로 이루어진 콘텐츠 전송 네트워크 성능이 저하되지 않기 때문이다.

Ⅴ. 결 론

본 논문에서는 탈분산화 네트워크에서 콘텐츠의 전송을 증명할 수 있는 PoCD를 제안하였다. 모든 피어는 PoCD를 활용하여 제3의 신뢰기관 없이 독자적으로 콘텐츠 전송 및 보상 여부를 증명할 수 있다. PoCD 지불내역 분석으로 무임승차자를 효과적으로 식별하고 네트워크에서 제외할 수 있음을 모의실험 결과로 확인하였다.

References

[1] S. Myung and J. Lee, "Analysis of the ethereum node discovery protocol," *J. KICS*, vol. 43, no. 12, pp. 2081-2088, Dec. 2018.

[2] Theta Labs, *Theta blockchain 4.0 whitepaper* (2022), Retrieved May 26, 2022, from https://docs.thetatoken.org/docs/whitepapers

[3] Filecoin, *Filecoin Spec: Markets* (2020), Retrieved May 26, 2022, from https://spec.filecoin.io/systems/filecoin_markets/

[4] Ethereum, *Development Documentation: Transactions* (2022), Retrieved May 26, 2022, from https://ethereum.org/en/developers/docs/

[5] K. Park, J. Kim, K. Cho, T. Kwon, Y. Choi, and S. Pack, "Waterfall: Video distribution by

cascading multiple swarms," *IEEE Journals on Selected Areas in Communications (JSAC)*, vol. 31, no. 9, pp. 165-174, Sep. 2013.

[6] K. Park, K. Cho, D. Han, T. Kwon, and S. Pack, "Proof of delivery in a trustless network" in *Proc. IEEE International Conference on Blockchain and Cryptocurrency 2019*, pp. 196-200, Seoul, Korea, Jul. 2019.