블록체인(Blockchain) 전파 지연 최소화를 위한 CDS(Connected Dominating Set) 기반 가상 백본 구축 기법

나하르 캄룬, 신인철
컴퓨터공학과, 부경대학교
e-mail : lima0711@pukyong.ac.kr, icshin@pknu.ac.kr

Constructing Virtual Backbone To Reduce Propagation Delay on Blockchain using CDS(Connected Dominating Set)

Nahar Kamrun, Incheol Shin
Department of Computer Engineering, Pukyong National University

요 약

본 논문에서는 다양한 분야에서 정보의 무결성과 투명성을 보장하기 위해 활용되는 분산 디지털(digital) 저장 및 기록 방법의 하나인 블록체인의 성능저하의 주요요인인 전파 지연(propagation delay)을 최소화 하기 위한 기법을 연구하였다. 이 같은 기법은 그래프(graph) 이론 및 수학 분야에서 연구되어온 Connected Dominating Set 문제에 대한 해결 방안을 활용하여 가상 백본을 구성하고 이를 통해 블록을 전파하는 네트워크 토폴로지 기반 블록 전파 지연 최소화 기법을 소개한다. 이를 통해 블록체인 프로토콜의 변형이나 블록 내 데이터의 크기 및 내용을 수정하는 등의 방법에서 발생할 수 있는 보안성 약화에 대한 문제를 해결하고 초당 트랜잭션 처리속도 (TPS, Transaction Per Second)를 향상할 수 있는 방안을 연구하였다. 본 연구에서 다루고자 하는 블록체인 전파 지연 문제는 NP-Hard에 속하는 문제로 다항식 시간(polynomial-time)에 해결할 수 없기 때문에 근사 알고리즘(Approximation Algorithm)을 통해 제시되었으며, 실험을 통해 그 효용성을 검증하였다.

1. 서 론

최초의 분산 암호화폐(distributed cryptocurrencies) 비트코인(Bitcoin)[1] 기반 거래의 무결성(integrity)을 지원하기 위해 블록체인이 고안되었다. 하지만, 분산 환경의 특성상 신뢰를 기반으로 네트워크에 참여하는 그룹(group)의 일부 노드의 고장이나 악의적으로 전파하는 정보로 인한 문제인 '비잔티움 장군 문제(Byzantine Generals Problem)'는 블록체인의 가장 큰 문제였다. 따라서, 비트코인 네트워크에 참여하고 있는 분산 노드(node)들 간에 공유되는 정보의 합의(consensus)를 위해 Nakamoto가 제안한 작업증명(PoW, Proof-of-Work)이라는 분산 알고리즘이 채택되었다.[2] 간단히 말해서, 비트코인 네트워크에서 블록(block)을 생성하기 위해 매우 많은 작업량이 필요한 무작위 대입 기법을 활용함으로써, 분산 장부(distributed ledgers) 수정을 위한 참여자들 간 합의를 이끌어 내기 위한 방법이다. 이 같은 방법은 비트코인 이후에도 Litecoin[3], Ethereum[4] 등과 같은 다양한 암호화폐 거래를 기록하기 위한 네트워크 참여 노드 간 합의 알고리즘으로 활용되고 있다.

블록체인은 기존의 암호화폐 이외에도 다양한 시스템[5][6][7]의 무결성을 제공하기 위한 기술로 활용되고 있으나, 블록체인에서 새로운 트랜잭션(transaction) 및 블록이 네트워크에 전파되는 지연 시간이 길어질 경우, 블록체인 확장성과 보안성에 심각한 문제를 초래하고 있다. 특히나, 트랜잭션 처리 속도인 TPS를 포함한 확장성 측면에서 네트워크 성능이 한계로 작용하고 있으며, 체인의 fork 발생률 증가에 따른 보안성 저하로 이중 지불(Double-spend) 공격으로까지 연결 가능하다. 여기서 fork란 같은 이전 블록 위에 서로 다른 새 블록들이 동시에 채굴되어 체인이 두 개 이상으로 분리되는 현상으로 노드 간 합의를 어렵게 하는 주요 요인으로 인식되고 있다.

비트코인은 일반적으로 5 ~ 7개의 트랜잭션을, 이더리움은 약 40개 정도를 처리하고 있으나 이 같은 처리 속도는 초당 1700개를 처리하는 VISA, 초당 110개의 PayPal 그리고 초당 40개를 처리하는 Ethereum과 비교하여 턱없이 낮은 수준이라고 볼 수 있다.

본 논문은 앞서 언급한 문제를 해결하기 위해 2장에서는 기존에 수행되었던 연구 중 관련된 문제를 해결하기 위한 접근 방식에 대해 설명한다. 또한, 3장에서는 네트워크 토폴로지(network topology) 측면에서 블록 전파 지연을 최소화하기 위한 방법 중 CDS를 활용한 가상 백본 구축 방법과 알고리즘을 제시하고 4장에서 실험을 통해 이 같은 기법의 효용성을 검증하고 효과에 대한 논의를 수행한다. 이후 5장에서 본 연구를 진행한 결과를 기술한다.

2. 관련 연구

블록체인 네트워크에서 블록 전파 지연 문제를 해결하고 TPS를 향상하기 위하여 블록 압축 기술, 릴레이 기술 등의 연구가 진행되었다. 이 같은 방식은 Nakamoto가 제시한 합의 프로토콜의 자료 구조(data structure)를 변형하거나 기능적 측면에서 알고리즘을 수정하는 방법을 제시하고 있으나, 이로 인해 기존의 블록체인과 연동이 불가능 한 확장성 문제가 발생할 수 있다. [9][10][11] 기존의 연구에서는 블록체인 네트워크의 문제점을 논의[12]하였으며, 블록 생성 시 이를 압축하고 블록 내 트랜잭션의 해시(hask) 값을 먼저 전송한 뒤 (수신 노드로부터 응답을 받은 후) 문제 발생 시에만 원본을 재전송함으로써 전파 지연을 최소화 하는 기법을 연구하였다. [13][14] 또한, 새로운 블록이 생성되기 시작하는 시점부터 네트워크의 참여자 노드에 해당 과정에 대한 내용을 선점적(preemptively)으로 알림으로서 합의를 시도하고 블록 생성을 마치는 시점에 해댱 정보를 전달하는 블록 전파 지연 최소화 기법 또한 연구되었다. [15]

블록체인 분배 네트워크(BDN, Blockchain Distribution Network)와 같이 블록의 전파 속도를 향상하기 위한 네트워크 구성을 위한 연구가 이미 진행되어, 네트워크 병목(bottleneck) 현상이 발생할 수 있는 지점에 높은 출력을 지원하는 서버를 통해 지연이 발생할 수 있는 대용량 블록을 전파 방법이 제시되었다.[16] 하지만 이 같은 방식은 분산 방식으로 동작하는 기존의 블록체인의 기본 원리를 고려하지 않고 중앙에서 노드들을 동작을 관리하는 서버를 이용함으로써 single point of failure의 위험성을 높이는 문제가 있다. FIBRE(Fast Internet Bitcoin Relay Engine)는 블록체인 네트워크의 전송 계층에 TCP(Transmission Control Protocol)가 아닌 오류 교정(error correction) 기능을 갖춘 UDP(User Datagram Protocol)를 활용함으로써 연결 구성 등에 대한 시간을 최소화 시키는데 목적이 있다.[17]

하지만, 이 같은 기법들은 기존의 네트워크 구조 및 프로토콜을 변형시키거나 블록체인에서 활용되는 데이터의 구조를 수정하는 과정을 거치게 되어 현재 사용되는 블록체인과 호환되지 못하는 단점이 존재하며 이로 인한 확장성 문제를 내포하고 있다. 또한, 기존의 비트코인을 지원하기 위한 목적에서 벗어나 다양한 분야에서 데이터의 무결성을 지원하기 위해 발전하고 있는 블록체인은 정형화되지 않은 형식을 갖추고 있어 이 같은 프로토콜이나 자료구조 변형을 통한 방식이 새로운 부작용을 발생시키게 된다.

따라서, 블록 전파를 최소화하기 위한 기법은 기존의 블록체인이 활용하고 있는 프로토콜이나 자료구조의 변경 없이 네트워크 TPS 수치를 향상할 수 있도록 네트워크 전파 지연을 최소화 할 수 있는 기법이 요구된다. 이 같은 요구사항을 만족하기 위해 기존에 연구된 CDS를 기반으로 하는 연구를 진행하고 이를 본 논문을 통해 소개한다.

3. 전파 지연 최소화 백본 구축

3.1 최소 CDS(Connected Dominating Set) 문제

그래프 이론과 수학분야에서 활발히 연구되는 주제로 네트워크의 모든 노드는 지배 노드(dominating node)이거나 비지배 노드(be dominated node)로 구분되어지며, 비지배 노드는 적어도 하나의 지배 노드와 연결되어야 한다. 이 같은 문제에서 지배 노드로써 상호 연결 구성된 그룹을 CDS라고 하며 최소(minimum) CDS 문제는 CDS 내 노드 수를 최소한으로 선택하는 문제이다.[18][19] 이 같은 문제는 NP-Complete로 분류되어 현재까지 다항식 시간에 해결할 수 있는 알고리즘이 N≠NP인 조건하에 존재하지 않는 것으로 알려져 있다. 이 같은 문제를 해결하기 위해서는 근사 알고리즘이 활용되고 있다. 근사 알고리즘이란 해결 하고자 하는 문제가 NP-Hard에 속하는 경우, optimal 결과 값에 다소 미치지 못하지만 다항식 시간에 optimum 결과를 도출할 수 있다.[20]

본 논문에서는 이 같은 접근 방식을 이용하여 블록체인 네트워크에서 최소한의 지배 노드들을 통해 최대한의 비지배 노드를 선택할 수 있는 최소 지배 노드 그룹(minimum dominating set)을 찾아내고 이들 간 최소 비용를 계산하여 최소 비용으로 연결된 노드 지배 그룹(minimum connected dominating set)을 구성하고 이를 가상 백본으로 블록을 전달하기 위한 구간으로 활용한다. 이를 통해 모든 노드들은 생산한 블록을 최소한의 노드를 통한 최소한의 비용으로 공유가 가능하다.

3.2 CDS 기반 가상 백본 구축 알고리즘

본 연구에서 고려하는 블록체인 네트워크는 참여자 노드 v들로 구성되었으며, 두 개의 노드 v와 u 사이에 통신이 가능한 경우 $e(v, u)$로 표현한다. 이때 가중치 $w(e)$는 임의의 노드 v와 u사이에 통신이 이루어질 때 요구되는 비용이다. 이와 같은 네트워크 그래프를 가중치 그래프(weighted graph)라고 하며, 본 논문에서 언급하고 있는 W는 모든 $w(e)$의 합으로써, 최소 CDS는 W의 값이 최소화된 지배 노드들의 집합이다.

본 논문에서 제시하고자 하는 알고리즘은 기존의 비용만을 고려한 최소 CDS를 식별하는 알고리즘에서 벗어나 전파 지연을 최소화하기 위해 해당 CDS 선택 시 최대 전달 비용(임의의 노드 v에서 u까지 통신 메시지가 전달되는 경로에 있는 모든 비용의 합)를 최소화한다. 따라서 최소한의 지배 노드 그룹 내에서 모든 노드별로 자신을 제외한 다른 노드로의 최단 비용 거리를 계산하고 이를 기반으로 정렬한 후 최대 비용을 가지는 구간을 선택한다. 선택된 구간에 있는 모든 노드를 CDS에 포함하고 나머지 지배 노드 그룹에 있는 노드별로 CDS에 포함된 노드와의 최소 비용이 소요되는 경로를 선택하여 해당 경로에 속한 구간과 노드를 CDS에 포함하는 과정을 반복한다. 이로써 지배 노드 그룹에 존재하는 모든 노드가 CDS에 포함될 때까지 반복함으로써 블록체인 네트워크에서 최소 비용

diameter를 가지는 가상 백본 네트워크 구성이 가능하다.

Algorithm: Constructing Minimum CDS with Minimum Diameter	
Input	**Blockchain Network B**
output	**A Set of Nodes with Minimum Cost in Minimum Diameter**

블록체인 네트워크 그래프 $G = (V, E)$ 생성
/* V는 네트워크 내 존재하는 참여 노드 v들의 집합
E는 직접 통신이 가능한 노드들 간 통신 e들의 집합
$e(v, u)$는 임의의 노드 v와 u사이의 통신
W는 e의 통신 비용 w들의 총합 */

/*최소한의 지배 노드로 최대한의 비지배 노드 연결이 가능한 그룹 선택*/
$DS \leftarrow empty$ /* 지배 노드 그룹 초기화 */
노드 v별 직접 통신이 가능한 노드 $N(v)$를 통해 내림차순 정렬
forall $v \in V$ **do**
  forall u $\in N(v)$ **do**
    $DS \leftarrow DS \cup u$
    $V \leftarrow V - u$
  end
end

$CDS \leftarrow empty$ /* 연결된 지배 노드 그룹 초기화 */
DS에 속한 모든 노드 쌍 v와 u별 최단 비용이 요구되는 경로를 계산하여 최대 비용 경로 $p(v, u)$를 선택
$CDS \leftarrow CDS \cup u$
$CDS \leftarrow CDS \cup v$
forall $z \in$ *every nodes along the path* $p(v, u)$ **do**
  $CDS \leftarrow CDS \cup z$
end

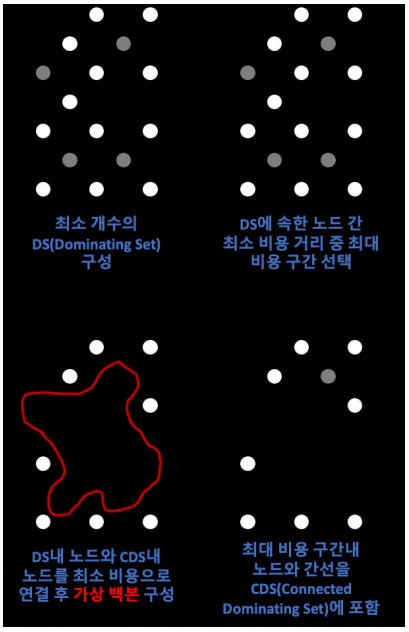
forall e $\in$ *every edges along the path* $p(v, u)$ **do**
  $CDS \leftarrow CDS \cup e$
end

forall $v \in DS$ but $v \notin CDS$ **do**
  CDS에 속한 임의의 노드 u까지 최단 비용 경로 $p(v, u)$계산
  $CDS \leftarrow CDS \cup v$
  forall $z \in$ *every nodes along the path* $p(v, u)$ **do**
    $CDS \leftarrow CDS \cup z$
  end

  forall e $\in$ *every edges along the path* $p(v, u)$ **do**
    $CDS \leftarrow CDS \cup e$
  end
end

return CDS

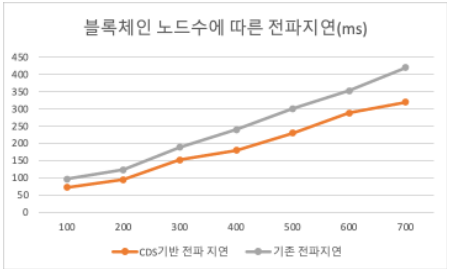
다음은 블록체인 네트워크에서 블록 전파 지연을 최소화할 수 있는 알고리즘에 대한 설명이다. 본 알고리즘은 최소한의 지배 노드를 통해 비지배 노드와 연결할 수 있는 그룹(DS, Dominating Set)을 선택하는 부분과 지배 노드 간의 연결을 최소한의 비용으로 연결하되 최대 비용이 요구되는 경로를 최소화하여 구성할 수 있는 부분으로 구성되어 있다. 본 알고리즘을 통해 반환된 CDS는 최소의 네트워크 비용으로 구성된 가상 백본으로써, 블록체인 네트워크의 참여자들이 생성된 블록을 전달하는데 필요한 다양한 비용을 할당할 수 있다.



(그림 1) Constructing Minimum CDS with Minimum Diameter 알고리즘 동작 도식화

4. 실험 결과

본 연구에서 제안하는 알고리즘을 통해 CDS 기반 가상 백본 구성 및 이를 활용한 블록체인 전파 지연 성능을 검증하기 위해 NS3를 통해 네트워크를 구성하고 각 노드별로 랜덤(random)한 시간 주기로 블록을 생성하고 이를 전파하는데 걸리는 시간을 측정하였다. 각 노드 수 별로 100회의 네트워크 구축과 블록 전파 시간을 측정하여 평균화하여 다음과 같이 표현하였다.



(그림 2) 블록체인 노드 증가에 따른 지연시간 변화 비교

각 네트워크에 참여하는 노드의 개수가 100개에서 700개로 증가함에 따라 전파 지연시간이 본 연구에서 제시한 가상 백본을 활용하는 경우 기존 블록체인 전파지연 시간보다 짧을 뿐 아니라 완만한 지연시간의 증가를 보인다.

5. 결론

다양한 암호 화폐의 거래를 분산 장부에 기록하기 위해 제시된 블록체인이 다양한 분야로 확산 적용되고 있음에 따라 무결성을 제공하기 위한 데이터의 양이 기하급수적으로 증가하고 있다. 본 논문에서는 이 같은 변화에 따라 심각한 문제로 대두되고 있는 전파 지연 문제를 해결하기 위해 가상 백본 네트워크를 효과적으로 구성하고 이를 통해 체인 네트워크 참여자들에게 신속히 업데이트된 정보를 공유하기 위한 기법을 제시하고 실험을 통한 검증을 수행하였다. 이를 통해 전파 지연 문제가 NP-Hard와 비슷한 난이도를 가지며 근사 알고리즘을 통해 최적값에 근사한 네트워크 토폴로지를 식별할 수 있음을 설명하였다.

Acknowledgement

이 논문은 2021년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임 (2020R1F1A107631612)

참 고 문 헌

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Manubot, Tech. Rep., 2019.

[2] S. Singh and N. Singh, "Blockchain: Future of financial and cyber security," in 2016 2nd international conference on contemporary computing and informatics (IC3I). IEEE, 2016, pp. 463-467.

[3] J. Reed, "Litecoin: An introduction to litecoin cryptocurrency and litecoin mining," 2017.

[4] G. Wood et al., "Ethereum: A secure decentralised generalised transaction ledger," Ethereum project yellow paper, vol. 151, no. 2014, pp. 1-32, 2014.

[5] W. D. Du, S. L. Pan, D. E. Leidner, and W. Ying, "Affordances, experimentation and actualization of fintech: A blockchain im- plementation study," The Journal of Strategic Information Systems, vol. 28, no. 1, pp. 50-65, 2019.

[6] N. Kshetri, "Can blockchain strengthen the internet of things?" IT professional, vol. 19, no. 4, pp. 68-72, 2017.

[7] M. Kouhizadeh and J. Sarkis, "Blockchain practices, potentials, and perspectives in greening supply chains," Sustainability, vol. 10, no. 10, p. 3652, 2018.

[8] J. Go¨bel and A. E. Krzesinski, "Increased block size and bitcoin blockchain dynamics," in 2017 27th International Telecommunication Networks and Applications Conference (ITNAC). IEEE, 2017, pp. 1-6.

[9] A. Gervais, G. Karame, K. Wu¨st, V. Glykantzis, H. Ritzdorf, and S. Capkun, "On the security and performance of proof of work blockchains," in Proceedings of the 23nd ACM SIGSAC Conference on Computer and Communication Security (CCS). ACM, 2016.

[10] W.Wang, D.T.Hoang, P.Hu, Z.Xiong, D.Niyato, P.Wang, Y.Wen, and D. I. Kim, "A survey on consensus mechanisms and mining strategy management in blockchain networks," IEEE Access, vol. 7, pp. 22 328-22 370, 2019.

[11] C. Natoli, J. Yu, V. Gramoli, and P. Esteves-Verissimo, "Decon- structing blockchains: A comprehensive survey on consensus, membership and structure," arXiv preprint, 2019, [Online]. Avail- able: https://arxiv.org/abs/1908.08316.

[12] T. Neudecker and H. Hartenstein, "Network layer aspects of permissionless blockchains," IEEE Communications Surveys & Tu- torials, vol. 21, no. 1, pp. 838-857, 2018.

[13] M. Corallo, "Compact block relay. bip 152," 2017.

[14] A. P. Ozisik, G. Andresen, G. Bissias, A. Houmansadr, and B. Levine, "Graphene: A new protocol for block propagation using set reconciliation," in Data Privacy Management, Cryptocurrencies and Blockchain Technology. Springer, 2017, pp. 420-428.

[15] C. Decker and R. Wattenhofer, "Information propagation in the bitcoin network," in IEEE P2P 2013 Proceedings. IEEE, 2013, pp. 1-10.

[16] U. Klarman, S. Basu, A. Kuzmanovic, and E. G. Sirer, "bloxroute: A scalable trustless blockchain distribution network whitepaper," IEEE Internet of Things Journal, 2018.

[17] M. Corallo, "Fibre: Fast internet bitcoin relay engine," 2017.

[18] Thai, M.T., Tiwari, R., Du, D.Z. On construction of virtual backbone in wireless ad hoc networks withunidirectional links. IEEE Trans. Mob. Comput. 2008, 7, 1098 - 1109.

[19] Kamei, S.; Kakugawa, H. A self-stabilizing distributed approximation algorithm for the minimum connecteddominating set. Int. J. Found. Comput. Sci. 2010, 21, 459 - 476.

[20] Garey, M.; Johnson, D.S. Computers and Intractability, a Guide to the Theory of NP-Completeness; Freeman:San Francisco, CA, USA, 1979.