데이터 처리량 향상을 위한 유향 비순환 그래프 기반의 멀티블록체인 시스템

천호천*, 김태우*, 박종혁*
*서울과학기술대학교 컴퓨터공학과
e-mail: a670627525@gmail.com, {tang_kim, jhpark1}@seoultech.ac.kr

Multi-blockchain System based on Directed Acyclic Graph for Increasing Data Throughput

Hao-Tian CHEN*, Tae Woo Kim*, Jong Hyuk Park*
*Dept. of Computer Science and Engineering, Seoul National University of Science and Technology

요 약

블록체인은 탈집중화, 위변조 방지, 추적 가능, 노드 간 공동 유지 및 보수가 가능한 데이터베이스로서 서로 신뢰하지 않은 노드 간 통신 신뢰 문제를 해결할 수 있는 점 대 점 통신 네트워크를 실현할 수 있다. 최근 몇 년 동안, 블록체인 기술은 지속적으로 발전하여 데이터 보안 문제를 해결하기 위한 중요한 기술로 주목받고 있다. 블록체인의 응용은 최초의 디지털 화폐 영역에서 금융·정무·공업 제조 영역으로 확대되고 있다. 블록체인의 특성에 따라 블록체인의 성능은 분산형 데이터 통신에 비해 크게 떨어지고 처리량이 제한되는 문제점이 존재한다. 본 논문에서는 최근 연구되고 있는 블록체인의 보안 구조 및 성능 분석에 대해 조사하고, 기존에 연구되었던 기술과 비교하여 블록체인의 안전성을 유지하며 성능을 향상시키는 방법에 대해 고찰한다. 이후 유향 비순환 그래프 (DAG: Directed Acyclic Graph) 및 샤딩 (Sharding)을 이용하여 안전성과 성능을 강화시키는 방법에 대해 제안한다. 제안하는 시스템은 DAG를 사용하여 위변조 방지 및 처리 속도 향상의 이점을 가지고 있으며, 샤딩을 사용함으로써 데이터 처리량을 향상시킨다. 마지막으로 제안하는 시스템은 기존 블록체인과 비교하여 안정성과 데이터 처리량 측면에서 비교 분석을 진행한다.

1. 서론

블록체인이란 탈집중화, 위변조 방지, 거래 정보 추적이 가능하며 노드 간 데이터를 공동 유지하거나 보수할 수 있는 데이터베이스이다 [1]. 블록체인은 비트코인과 함께 탄생한 기술로 탈집중화, 위조 방지 기능을 핵심으로 하여 전자 화폐 분야에서 사용한다. 이 외에도 고가치 데이터의 관리, 저장 및 유통 등 과정에서도 블록체인을 사용하고 있다 [2].

비트코인의 사용과 함께 블록체인의 보안 문제가 발생하였으며, 이를 대응하기 위해 블록체인의 여러 분야에서 활발한 연구가 시작하였다. 블록체인은 금융 데이터 관리, 고가치 데이터를 운용 네트워크 등의 환경에서 활용되고 있다. 특히 지능화된 디지털 환경에서는 안전성 요구사항이 높기 때문에 블록체인의 실제 활용을 위해 블록체인의 안전성을 가장 중요한 문제이다 [3]. 시스템의 안정성 문제를 해결하기 위해 블록체인의 관한 여러 연구가 진행되고 있다. 그러나 블록체인의 안전성을 향상시키는 반면 블록체인의 성능 및 효율은 일반 디지털 정보 처리보다 크게 떨어진다는 문제점이 존재한다.

본 논문에서는 최근 연구되고 있는 블록체인의 동향에 대한 조사를 진행하고, 전통적인 데이터베이스와 비교를 통해 블록체인의 장단점 및 발전 동향을 분석한다. 이후 기존 연구를 바탕으로 네트워크에서 발생하는 전통적인 보안 문제와 통신의 안정성 및 성능을 유지하는 방법에 대해 고찰한다.
마지막으로 유향 비순환 그래프 (DAG: Directed Acyclic Graph) 기반의 블록체인 시스템을 제안하고, 기존 연구된 블록체인과 성능과 안전성 측면에서 비교 분석을 진행한다.

2. 관련연구

2.1. 블록체인의 구조

데이터 위조의 불가능성을 실현하기 위해 블록체인은 블록 단위의 체인 구조를 도입하였다. 이것은 블록 단위로 데이터를 저장하고 브로드케스트 형식

으로 네트워크 안에 노드 간 통신을 진행한다. 또한 블록체인의 탈집중화 특징으로 인해단일 기관의 관리 및 유지 보수의 필요가 없어 신뢰성 문제를 해결할 수 있다. 이외에도 블록체인의 각 노드마다 이전 노드의 해시 값을 저장하여 위조 방지 및 이전 노드 추적 가능한 기능을 제공한다.

2.2. 일반 데이터베이스와의 비교

알고리즘 측면에서 전통적인 분산형 데이터베이스는 분산 일관성 문제 (Distributed Consistency Issues)를 해결하기 위해 Paxos & Raft 등 알고리즘을 사용한다. 이때 전제 조건은 네트워크 안에 모든 노드는 악성 노드가 아니어야 한다. 그러나 집중 네트워크에 연결되어 있는 노드는 개인 이익을 위해 악성 노드로 변화할 수 있다는 문제가 있다. 또한 전통적인 분산형 데이터베이스는 알고리즘이 신뢰성 문제로 인해 블록체인 네트워크에서 사용이 불가능하다. 따라서 블록체인에 사용하기 위해 PoW, PBFT, Pos, DPos 등의 알고리즘이 고안되었다. PoW은 무의미하게 전력 자원을 소망하고 51% 공격에 약한 취약점이 존재한다. PBFT는 네트워크 안에 2/3 이상의 노드는 악성 노드 아니면 안전한 통신 환경을 제공할 수 있는 반면 성능이 높지 않다.

백업 측면에서 데이터베이스는 대기 데이터베이스를 통해 예외 처리를 진행하여 구조가 복잡하고 유지 보수하는 비용이 비싸다는 문제가 있다. 그러나 블록체인 네트워크는 메인/보조 개념이 존재하지 않아 임의의 노드 활동이 활발하게 진행될 수 있다. 따라서 소부분 노드가 고정이 난 경우에 고장을 고친 후에 전체 시스템 운행에 영향이 없고 자동으로 데이터 동기화할 수 있다 [4].

2.3. 블록체인 처리량에 관한 연구 동향

블록체인은 보통 LevelDB를 사용하여 엄격한 트랜젝션 (Transaction)을 제공하기 때문에 처리 속도가 빠르지 않다. 즉 블록체인에서 사용되는 P2P (Peer to Peer) 네트워크도 좋은 동시성 서비스 제공하지 않고, 블록체인의 검사 기능이 효율적지 않아 확장성 측면에서도 문제가 발생한다. 이 외에도 블록체인은 데이터의 소속 및 통신 과정의 위조 불가능성을 제공하지만 탈집중화 유형의 네트워크상에서 액세스 제어 문제점이 존재한다. 결론적으로 블록체인은 엄격한 트렌젝션, 효율적이지 않은 검사기능, 엑세스 제어 등의 문제로 데이터 처리량이 높지 않다는 문제점이 생긴다.

Xu 등은 빅데이터 추적 분야에 블록체인을 이용하기 위한 DHR (dynamic heterogeneous redundance) 모델을 제안했다 [5]. 블록체인의 잠재적인 보안 문제를 목표로, 보안과 결합한 동적 비동기 중복 (Asynchronous redundancy) 아키텍처 및 암호 로또 아이디어를 참조하고 정의 및 매개 변수 선택 규칙 결합하여 동적 비동기 합의 메커니즘과 동적 비동기 중복 디지털서명 알고리듬의 관점에서 블록체인의 보안 솔루션이 제안된다. 체인처럼 데이터의 소원 기록을 구축하여 전체 연결을 흐트러뜨리지 않는 조건에서는 깨지거나 다시 정렬할 수 없기 때문에 RFID 빅데이터 자국 추적 과정의 안전성을 보장할 수 있다.

앞서 살펴본 DHR 및 RFID 빅데이터 자국 추적 모델 등의 블록체인 구조는 빅데이터, 사물인터넷 (IoT), 클라우드 등 많은 기술과 결합하여 응용 영역을 확장할 수 있다. 그러나 규모가 증가할수록 디자인이 복잡해지고 실제 설치하여 운영하는 비용도 높고 성능이 떨어지기 때문에 아직도 이론 단계에서 탐구되고 있으며 블록체인의 데이터 처리속도는 큰 문제점으로 지적되고 있다. 이에대한 예로 최초의 블록체인은 처리량이 7TPS/s에 불과하고 현재 운용되고 있는 가상화폐인 Ethereum의 처리량은 20~30TPS/s에 불과하다. 그러나 현재 실제로 사용되고 있는 데이터베이스는 대부분 1000TPS/s를 넘는 데이터 처리 속도를 제공하고 있다.

ZHANG PY 등은 합의 메커니즘 알고리즘의 효능 최적화 연구에 대한 종합적인 분석을 진행했다 [6]. 연구에서 모든 자원 중에서 가장 주요한 자원은 사회 자원이고 블록체인의 자원, 에너지 소모, 성능으로 세 방면으로 합의 메커니즘 알고리즘의 효능 평가 조건을 정의하였다.

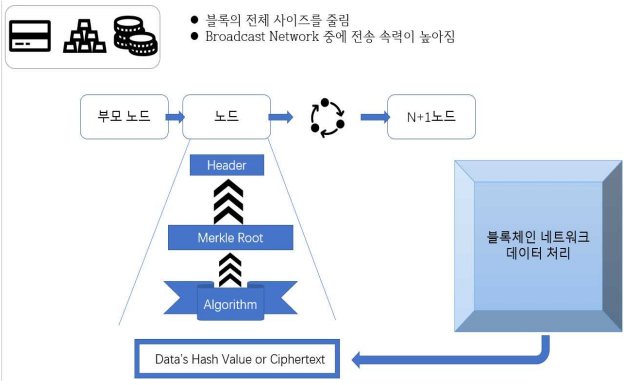
Zuan 등은 제안한 TCCM 알고리즘 [7] 과 Milutinovic 등이 제안한 새로운 합의 언어 및 PoL (Proof of Luck) 알고리즘 [8]을 통해 에너지 소모의 문제를 개선하고자 하였다. TCCM는 PoW보다 에너지 소모를 줄이는 동시에 10min/회의 시간 지출부터 1min/회 시간 지출로 감소하니 합의 메커니즘 알고리즘의 에너지 지출을 감소한다. PoL 알고리즘은 TEE의 Proof of Work/Time/Proprietorship 및 개편한 프리미티브 기반의 기술이고 에너지 소모 평가할 때에 전통적인 PoW 알고리즘보다 더 효율적이기 때문에 에너지 소모를 줄이게 된다.

그러나 공유 체인에서 합의 메커니즘 알고리즘은 효율성이 부족 하다는 문제점이 존재한다. Zeng 등은 PoW 기반의 MPoW 알고리즘을 제안했다 [9]. 이것은 해시 함수의 핵심 메서드 SHA-256에 대해 개선하고 최대 30%의 마이닝 시간 (Mining time)을 절약할 수 있다. 이 외에도 연구를 통해 추후 투표 메커니즘, PoT (Proof of Trust), RSF 알고리즘을 개선하였다. 이것을 통해 하드웨어 입장의 영향을 최소화하여 자원 이용률을 확보한다는 연구 성과를 보였다.

3. DAG 그래프 및 Sharding를 이용한 멀티체인

본 논문에서는 DAG 및 샤딩 이용한 멀티 블록체인 구상을 제안한다. 제안하는 시스템은 블록체인의 특성에 따라 블록의 사이즈는 클수록 전송 지연이 커지는 것을 전송 효율 및 처리량을 증가시키며, 보안 공격 측면에서 지연을 이용한 공격의 확률이 감소한다는 장점을 가진다. 즉, 블록체인의 사이즈를 감소시켜 전송 지연 및 처리량을 개선할 수 있다. 기존 블록체인의 데이터 부분에서 수많은 디지털 거래 기록를 기록하기 때문에 데이터양이 크다는 문제점이 존재하였으나 제안한 모델을 통해 멀티 체인으로 처리량을 증가시키고 위변조 방지 능력을 강화할 수 있다.

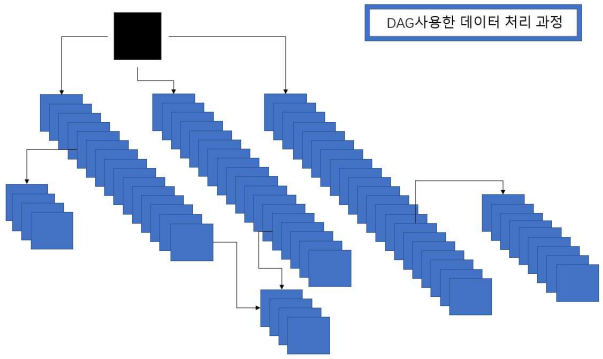
그림 1은 제안하는 DAG 기반 멀티블록체인 아키텍처이다. 제안하는 모델은 블록체인 네트워크의 노드를 메인 체인 및 보조 체인으로 랜덤하게 분할한다. 메인 체인에서 기존 블록체인이고 보조 체인을 통해 포크 (Fork) 최소화 시킬 수 있다.



(그림 1) 제안하는 DAG 기반 멀티 블록체인 아키텍처

보조 체인은 DAG 모델을 사용하여 성능 및 위변조 방지의 효과를 발생시킨다 또한 Sharding 중심의 구조를 사용하여 데이터의 유형에 따라 네트워크 안의 노드를 나누어 데이터 처리를 시간 동기화부터 비동기식 동시성 (Asynchronism&Concurrency)으로 변화하여 성능을 향상한다.

그림 2는 보조 체인에서 메인 체인의 블록을 출력하는 과정을 표현한다. 보조 체인에서 규모가 더 큰 블록체인 네트워크 자원을 사용하고 포크에 대한 제어를 최소화한다. 즉 모든 계산을 시간 표준 계산에서 데이터의 종류에 따른 비동기 동시성으로 진행한다. 이것은 데이터는 대체로 거래 정보, 제어 정보, 상태 기록 정보 등 분산형 데이터베이스처럼 처리한다.



(그림 2) 보조 체인에서 메인 체인 출력 과정

DAG를 사용하는 것을 이용하여 한 블록의 부모 블록은 복수 존재할 수 있어 부모 노드를 추적을 통해 복수의 부모 블록을 찾을 수 있다. 전체 네트워크를 DAG (Directed acyclic graph) 네트워크로 구성하여 네트워크의 처리량을 향상한다. 한 블록에서 부분적인 정보를 사용하여 다른 모든 노드의 인증이 필요한 악성 코드를 검증할 수 있으며, 공격자가 어떤 블록의 데이터를 변경을 위해 현재 노드의 체인뿐만 아닌 모든 DAG 후계 방향에 있는 노드 전체를 변경해야 하므로 공격을 실현하는 것은 더욱 어려워지고 위변조 방지할 수 있다. 만약 가장 긴 체인이 선정된 경우에 모든 데이터를 통합 인증 단계를 진행하여 데이터의 상태와 거래 정보와 제어 정보 등을 합친다. 긴 체인의 정보 처리 끝난 후에 해당 수많은 거래 사건을 승인을 받아서 해시 함수 및 암호 알고리즘을 사용하고 고정된 길이의 해시 값이나 데이터 상대적 단축한 암호문을 출력하고 메인 체인의 데이터 부분으로 되고 메인 체인에서 앞서 언급한 성능이 나은 합의 알고리즘을 사용하여 Merkle 루트를 얻는다.

전체 과정에서 제안한 모델은 보조체인은 샤딩을 이용하여 비동기 동시성 정보 처리를 통해 구역을

분할하여 소규모의 네트워크에서 고속 계산을 실현한다. 이것을 통해 메인 체인의 포크 최소화 및 보조 체인의 DAG 포크를 통해 네트워크에서 정보 위조를 막고 무결성을 보장한다.

4. 결론

블록체인은 현재 사용되고 있는 분산형 데이터베이스에 비해 성능이 너무 떨어지기 때문에 블록체인 구조 및 네트워크 환경의 처리량 문제가 발생한다. 본 논문에서 제안한 모델은 블록체인 네트워크 노드를 랜덤하게 배정하여 보조 체인의 비동기 정보 처리를 처리량을 개선하면서 메인 체인에 블록을 추가할 때에 보조 체인의 데이터 합병 및 인증을 통해 데이터의 무결성을 확보한다. 제안하는 모델은 기존 블록체인 모델과 비교하여 탈집중화의 특성을 부분적으로 희생하고 전체 노드에 대해 제어 수단을 추가하여 블록체인의 확장성 및 안전성을 강화할 수 있다. 따라서 제안하는 모델은 기존 블록체인의 탈중앙화 특성을 노드의 요구조건에 맞게 일부 권한을 해제하여 안정성과 데이터 처리량을 증가 시킨다. 이것은 탈중앙화의 특성을 가지지만 탈중앙화의 일부부분을 강제시킨다는 문제점을 가지고 있다. 추가적인 연구를 통해 탈중앙화 특성 요소를 제한하지 않고 성능을 개선시키는 방안에 대해 연구할 필요가 있다.

Acknologyment

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (NRF-2019R1A2B5B0107041613).

참고문헌

[1] SHAO Qi-feng, JIN Che-Qing, ZHANG Zhao, Qian Wei-Ning, and Zhou Ao-Ying. "Blockchain technology: architecture and progress", Chinese Journal of Computers, vol. 41, no. 5, pp. 969-988, 2018

[2] Zhao Tian, Wei An, and Zhou Ming'ai. "Blockchain security development status, problems and countermeasures", Cyberspace Security, vol. 10 no. 11, pp. 1, 2020

[3] Xu MX, Yuan C, Wang YJ, Fu JH, Li B. "Mimic blockchain－Solution to the security of blockchain" Ruan Jian Xue Bao (in Chinese)/Journal of Software, vol. 30, no. 6, pp. 1681－1691, 2019

[4] Kotobi, K., and Bilen, S. G., "Secure blockchains for dynamic spectrum access: A decentralized database in moving cognitive radio networks enhances security and user access", Ieee vehicular technology magazine, vol 13, no. 1, pp. 32-39, 2018

[5] Liu YaoZong, and Liu YunHeng, "RFID big data security traceability model based on blockchain", Computer Science, vol. 45, no. 11A, pp. 367-368, 2018

[6] Zhang Pengyi, and Song Jie, "Research progress on efficiency optimization of blockchain consensus algorithm", Computer Science, vol. 47, no. 12, pp. 296-303, 2020

[7] Zuan W., Youliang, T., Chaoyue, Y., and Duo, Z., "Consensus Mechanism Based on Threshold Cryptography Scheme", Journal of Computer Research and Development, vol. 56, no. 12, pp. 2671, 2019

[8] Milutinovic, M., He, W., Wu, H., and Kanwal, M. "Proof of luck: An efficient blockchain consensus protocol", In proceedings of the 1st Workshop on System Software for Trusted Execution, pp. 1-6. 2016

[9] Zeng, L., Xin, S., Xu, A., Pang, T., Yang, T., and Zheng, M., "Seele's New Anti-ASIC Consensus Algorithm with Emphasis on Matrix Computation" arXiv preprint arXiv:1905.04565, 2019