IoT 환경에서 동작 가능한 경량 블록체인 연구 분석

김요한, 오경우, 오시몬, 김동규, 김호원

부산대학교

yohan@islab.re.kr, kyeongwoo@islab.re.kr, simon@islab.re.kr, donggyu@islab.re.kr, howonkim@gmail.com

A Review of Study on Lightweight Blockchain Operational in IoT Environment

Kim Yo Han, Oh Kyeong Woo, Oh Si Mon, Kim Dong Gyu, Kim Ho Won

Pusan National University

요 약

블록체인 기술은 분산, 보안, 감사 가능성을 비롯한 주요 기능들로 인해 많은 주목을 받고 있다. 그 특성들을 IoT 기술에 적용하여 데이터의 보안 문제를 해결하고자 하는 연구들이 등장했다. 그러나 블록체인 기술을 IoT 기반 환경에 적용하기 위해서는 많은 조건이 필요하다. IoT 기반 환경의 장치들은 대부분 연산 및 저장, 대역폭 등의 리소스가 제한되어 있어서, 이러한 장치에서 동작할 수 있어야 한다. 또한 트랜잭션 처리량이 많아야 하며, 키워드 기반 검색으로 각 장치에 빠르게 접근할 수 있어야 한다. 본 논문에서는 IoT 환경에서 동작 가능한 경량 블록체인을 제안한 연구를 조사하여, IoT에 블록체인을 적용하는 데 필요한 기능들과 과제들을 분석할 것이다. 또한 각 연구의 성과를 분석하여, 앞으로의 연구 방향을 제시할 것이다.

Ⅰ. 서론

현재 IoT 기술과 서비스는 점차 다양한 분야에 적용되고 발전되고 있다. IoT 네트워크에서는 온도나 습도 및 진동을 센서를 통해 모니터링하고 조명이나 온습도를 조절하는 등 무선 통신이 가능한 다양한 저성능 장치들이 연결되어 서비스를 제공한다. 하지만 IoT 장치의 구현 목적에 따라 성능상 데이터의 보안 처리에 미흡하여 공격에 취약하다는 문제점이 존재한다.

이 문제점을 해결하기 위해 다양한 방향의 접근이 존재한다. 본 논문에서는 그 중 블록체인을 적용한 사례에 주목하였다. 블록체인 기술은 분산된 노드들의 합의로 데이터를 생성하고, 분산된 모든 노드가 동일한 데이터를 동기화하는 분산 원장 기술이다. 블록체인은 구조적 특성 때문에 원장의 내용이 위변조될 가능성이 매우 낮아 데이터 무결성을 확보할 수 있다는 장점이 있다. 이 데이터 무결성에 주목하여 IoT에 블록체인을 적용하는 연구들이 등장했다.

그러나 블록체인 기술을 IoT 환경에서 적용하기 위해서는 여러 조건이 갖추어져야 한다. 먼저 블록체인에서 각 노드에 대한 서비스를 사용하기 위해서는 스마트 컨트랙트를 실행해야 한다. 그리고 IoT 장치는 저성능인 경우가 많은데, 만약 노드가 스마트 컨트랙트를 실행하지 못하는 저성능 장치일 경우 해당 노드는 블록체인 서비스를 사용하지 못할 수도 있다. 따라서 IoT 환경에서 블록체인을 정상적으로 동작시키기 위해서는 블록체인 자체의 연산 능력과 리소스를 제한하여 저성능 장치에서도 동작할 수 있도록 만들어야 한다. 그 밖에도 블록체인의 확장성과 탈중앙성 등 서비스를 원활하게 제공하기 위한 조건들이 존재한다.

따라서 본 논문에서는 이를 위해 제안된 IoT 환경에서 동작 가능한 경량 블록체인 사례에 대해 분석할 것이다.

Ⅱ. 본론

블록체인이 탈중앙화 및 원장 동기화를 위해 필요한 메커니즘을 합의 알고리즘이라고 하며, 분산된 각 노드가 보유하고 있는 원장의 내용은 합의 알고리즘에 의해 동일하게 유지된다. 그리고 IoT 환경은 연산 능력과 리소스가 한정되어 있어서 복잡한 합의 프로토콜을 사용하기 힘들기 때문에, 합의 시간이 빠른 합의 알고리즘을 사용해야 한다. 예를 들어 3분의 2 이상의 노드만 합의하면 검증되는 PBFT(Practical Byzantine Fault Tolerance) 합의 알고리즘은 모든 노드가 검증해야 하는 PoW(Proof of Work) 합의 보다 합의 시간이 빠르다. IoT 환경에서 블록체인을 적용하기 위해서는 합의 알고리즘이 중요한 역할을 가지기 때문에 경량 블록체인 연구 중에서 합의 알고리즘에 관한 연구가 꾸준히 이루어지고 있다.

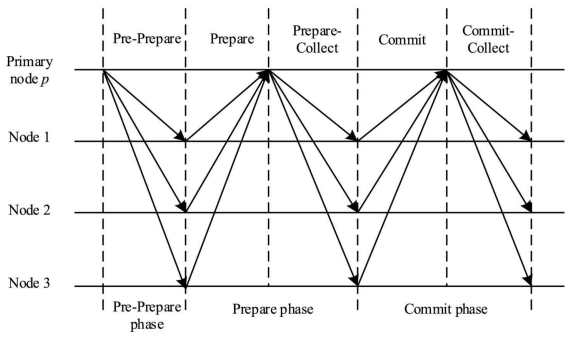

그림 1. SVBFT 합의 알고리즘

Li 등은 합의 알고리즘을 개선하여 경량 블록체인을 구현하는 방향으로 접근했다. 저자들은 보상 및 처벌 전략에 기반한 개선된 PBFT인 SVBFT(Score-Voting based BFT)를 제안했다. SVBFT은 [그림 1] 과 같이 합의 노드가 메시지를 프라이머리 노드에만 브로드캐스트하여 기존 PBFT 합의 알고리즘보다 통신을 간단하게 만들었다. 따라서 트랜잭션 처

리량을 효과적으로 개선하고 리소스가 제한된 장치들의 통신 부담을 감소시킬 수 있다. 또한 저자들은 블록체인 복구 가능성을 보장하고 스토리지 오버헤드를 줄이기 위해 RS-Erasure Code 기반의 블록체인 스토리지 최적화 체계를 제안했다. RS- Erasure Code 기술은 블록이 생성되면 여러 조각으로 인코딩하여 적절한 블록체인 노드에 저장시킨다. 이를 통해 스토리지 오버헤드와 블록체인 스토리지 임계값을 줄일 수 있으며, 결과적으로 합의 지연, 합의 통신 자원, 블록체인 저장 비용을 줄일 수 있다 [1].

Dorri 등은 IoT 애플리케이션을 위한 확장성을 제공하면서도, 가벼운 합의 알고리즘인 Tree chain을 제안했다. Tree chain은 검증자가 작업을 증명하거나, 새 블록을 저장하기 전에 증명을 제공할 필요가 없다. 또한 검증자 간 무작위 합의를 해시함수 출력에 의존하여 해결하였다. 이때 각 트랜잭션의 검증자가 무작위로 정의되는 트랜잭션 레벨과 각 검증자가 전담하는 블록체인 레벨의, 두 가지 무작위화 레벨로 나눈 병렬 체인 가지 개념을 도입했다. 이를 통해 Tree chain은 리소스가 제한된 IoT 환경에서도 실행할 수 있으며, 처리 오버헤드가 낮다 [2].

경량 블록체인의 합의 알고리즘에 관한 연구는 앞의 두 사례 모두 리소스 제한이 있는 IoT 환경에서도 서비스를 실행할 수 있도록 합의 알고리즘을 가볍게 만드는 것에 주목했다. 다만 [1] 의 경우 블록을 조각내어 여러 노드에 저장하는 것으로 스토리지 부담을 줄였다면, [2] 의 경우 검증자 간의 무작위 합의와 병렬 체인을 통해 트랜잭션 처리 속도를 높이고 처리 오버헤드를 줄였다.

한편 IoT 환경에서 사용이 가능한 경량 블록체인 아키텍처를 제안하는 연구도 존재한다. 이 연구들은 블록체인의 확장성은 물론 트랜잭션의 처리 속도, 성능 오버헤드 등을 고려하여 IoT 환경의 블록체인 아키텍처를 제안했다. 빠른 합의 알고리즘을 사용하는 것은 앞의 사례들과 같지만, 블록체인 아키텍처가 원활하게 작동하는 것을 우선으로 했다.

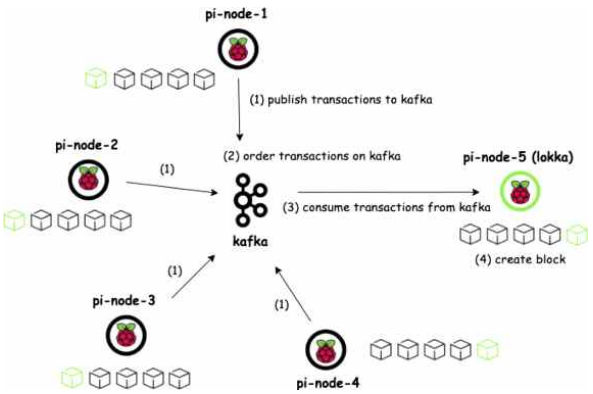

그림 2. Tikiri 블록체인 아키텍처 및 트랜잭션 흐름

Bandara 등은 IoT용 경량 블록체인 아키텍처 Tikiri를 제안했다. Tikiri는 경량 블록체인을 구현하기 위해 마이크로 서비스 기반 분산 시스템 아키텍처로 구성되어 있다. 그리고 블록체인 확장성을 위해 Apache Kafka 기반의 합의 알고리즘을 사용하는 것으로 실시간 트랜잭션 처리량도 증가시켰다. 그림 2와 같이 클라이언트가 게시한 모든 트랜잭션은 Kafka의 메시지 브로커에 저장되고 실행된다. 이를 통해 IoT 애플리케이션과 트랜잭션의 부하를 줄였다. 그리고 데이터 저장을 샤딩 기반 데이터 복제 메커니즘을 사용하여 기본 분산 데이터베이스에 처리하는 것으로 통신 및 계산을 포함하는 성능 오버헤드를 줄였다. 저자는 전력 그리드 센서 장치 모니터링 애플리케이션을 실증하면서 Tikiri가 IoT 환경을 위한 블록체인 시스템을 구성했다는 것을 보여주었다 [3].

Pradhan 등은 IOTA를 사용하는 경량 커뮤니티 에너지 거래 아키텍처를 제안했다. IOTA는 블록의 체인 기반이 아닌 트랜잭션에서 생성되는 DAG(Directed Acyclic Graph)를 사용하는 분산 원장 기술이다. 이 기술의 장점은 블록체인에 비해 확장성을 더 제공하고 수수료를 절감한다는 것에 있다. 그리고 경량 커뮤니티 에너지 거래 아키텍처는 IOTA를 통해 소액 거래에 대한 보상 오버헤드를 완화하고 확장성과 신뢰성 및 높은 처리량을 제공하는 DAG 기반의 에너지 거래 시장 아키텍처를 설계했다. 이 아키텍처는 경량 채널을 통해 생산자와 소비자가 각각 에너지 데이터 제공 및 구독에 중점을 두는 것으로 각 사용자에게 맞는 서비스를 제공하며, 이를 통해 대량의 소액 거래를 지원한다 [4].

앞의 두 연구는 IoT 환경에서 사용이 가능한 경량 블록체인 아키텍처를 제안하였다. 두 연구 모두 블록체인 확장성을 제공하는 아키텍처를 설계했지만, [3] 의 경우 트랜잭션 처리 속도에 주목했다면, [4] 는 거래 수수료 절감 및 신뢰성에 좀 더 주목하였다.

Ⅲ. 결론

IoT 기술은 다양한 장치들이 연결되는 구조 때문에 인증 및 데이터 보안이 필요하다. 그리고 블록체인은 다양한 노드가 있어도 데이터 무결성을 보장하는 기술이다. 이에 주목하여 본 논문에서는 IoT 보안 문제를 블록체인을 적용하여 해결하기 위한 연구를 조사하여 분석했다. 본 논문에서 다룬 것은 합의 알고리즘과 블록체인 아키텍처에 관한 연구다. 합의 알고리즘에 관한 연구는 리소스가 제한된 IoT 환경에서 작동이 가능한 블록체인 서비스와 빠른 합의 속도에 중점을 두었으며, 블록체인 아키텍처에 관한 연구는 블록체인의 확장성 및 트랜잭션 처리 속도에 중점을 두었다.

본 논문은 IoT 환경에서 경량 블록체인이 동작할 수 있기 위해 가져야 하는 핵심 기능과 그 기능들은 구현하기 위한 연구를 분석하였다. 총 네 가지의 사례를 조사하여 각 연구의 특징과 장점, 그리고 목표를 분석하였다. 향후 작업으로 분석한 기능을 토대로 경량 블록체인 서비스를 제안할 계획이다.

ACKNOWLEDGMENT

본 연구는 과학기술정보통신부 및 정보통신기획평가원의 대학ICT연구센터육성지원사업의 연구결과로 수행되었음 (IITP-2023-2020-0-01797)

참 고 문 헌

[1] C. Li, J. Zhang, X. Yang, and L. Youlong, “Lightweight blockchain consensus mechanism and storage optimization for resource-constrained IoT devices,” Inf. Process. Manage., vol. 58, no. 4, Jul. 2021, Art. no. 102602, doi: 10.1016/j.ipm.2021.102602

[2] A. Dorri and R. Jurdak, "Tree-chain: A fast lightweight consensus algorithm for IoT applications", Proc. IEEE 45th Conf. Local Comput. Netw. (LCN), pp. 369-372, Nov. 2020.

[3] Bandara, E., Tosh, D., Foytik, P., Shetty, S., Ranasinghe, N., & De Zoysa, K. (2021). Tikiri—Towards a lightweight blockchain for IoT. Future Generation Computer Systems, 119, 154-165.

[4] Pradhan, N. R., Singh, A. P., Verma, S., Wozniak, M., Shafi, J., & Ijaz, M. F. (2022). A blockchain based lightweight peer-to-peer energy trading framework for secured high throughput micro-transactions. Scientific Reports, 12(1), 1-15.