

산업용 IoT를 위한 IPFS가 결합된 DDS 기반 블록체인 기법

이늘숨¹, 이재민², 전태수³, 김동성*

금오공과대학교 {IT융복합공학^{1,2,*}, 컴퓨터소프트웨어공학³}

{alwaysom², ljmpaul², taesoo.jun³, dskim*}@kumoh.ac.kr

DDS-based Blockchain Scheme with IPFS for Industrial IoT

Neul-Som Lee¹, Jae-Min Lee², Tae-Soo Jun³ and Dong-Seong Kim*

Kumoh National Institute of Technology Dept. of {IT Convergence^{1,2,*}, Computer Software³} Eng.

요약

산업용 IoT(IIoT, Industrial Internet of Things)는 산업 공정의 효율성과 생산성을 높이는 데 핵심이 되는 환경으로, 광범위한 기기종 장비와 프로토콜 간의 상호 작용 및 빠른 데이터 처리가 중요하다. 이를 지원하기 위해 확장성과 실시간성을 갖춘 미들웨어 도입과 데이터 무결성 및 보안 강화를 위한 블록체인 도입 연구가 이루어졌다. 그러나 제한된 리소스로 인해 블록체인 데이터 용량을 줄이는 것이 요구되었다. 기존에도 IPFS(InterPlanetary File System)를 이용해서 블록체인을 경량화하는 시도가 있었지만, IIoT 환경에서 미들웨어, 블록체인, IPFS를 효과적으로 연합하는 연구는 미흡한 실정이다. 본 논문은 산업용 IoT에서 데이터 확장성 문제를 해결하기 위해 DDS(Data Distribution Service) 기반의 블록체인에 IPFS를 결합하는 기법을 제안한다.

I. 서론

IIoT는 산업 공정 자동화의 기반이 되는 환경으로, 대규모로 구성된 이기종 장치 및 프로토콜과 상호작용할 수 있는 유연성과 각종 제어 명령, 생성 데이터를 빠르게 전달하고 처리할 수 있는 실시간성을 확보하는 것이 중요하다. 이와 관련하여 이기종 특성을 지원하는 확장성과 실시간성을 만족하기 위해 데이터 중심 미들웨어 도입에 대한 연구가 이루어졌으나 확장이 용이한 미들웨어를 역으로 이용하는 데이터 위변조, 무단 접근 등 악의적 행위에 취약하여 보안을 향상하고 데이터 위변조를 방지할 방안이 필요했다[1]. 이에 네트워크 내 모든 사용자가 모든 트랜잭션을 블록 단위로 저장하여 연결되는 블록체인 기술을 결합하여 데이터 무결성 및 보안성을 보장하는 플랫폼이 연구되었다[2]. 그러나 블록체인은 모든 원장의 저장과 블록 생성 및 합의 알고리즘 처리에 높은 리소스와 시간을 요구하므로 제한된 리소스로 인해 복잡도가 높은 연산이나 대용량의 데이터를 처리할 수 없는 IIoT 환경에 그대로 적용하기에 한계가 있었다. 기존 연구에서는 블록체인 데이터 용량을 줄이기 위해 분산 파일 시스템인 IPFS를 활용하는 시도가 있었지만, IIoT와 같은 대규모 환경에 미들웨어, 블록체인, IPFS를 효율적으로 통합하는 접근법에 대해서는 아직 추가적인 논의가 필요하다. 특히 미들웨어의 경우 Broker, Publisher, Subscriber 간의 메시징 프로토콜인 MQTT(Message Queuing Telemetry Transport)를 사용한 경우가 대부분이다[3]. MQTT는 가볍고 효율적이지만 소규모 시스템이나 저대역폭 네트워크에 유리하여 대규모 시스템에서 요구하는 높은 처리 능력과 규모 가변성을 만족하기 어렵다.

본 논문에서는 IIoT 환경에서 데이터 확장성을 확보하기 위해 IPFS를 활용한 DDS 기반 블록체인 기법을 제안한다. 제안된 기법은 IPFS를 통해 데이터를 시스템 외부에 분산 저장함으로써 리소스 제한을 극복하고 암호화된 해시 값으로 데이터 무결성을 강화할 수 있다. 또한 DDS로 대규모 시스템인 IIoT 환경이 요구하는 안정성과 실시간성을 충족하고자 한다.

II. 기존 연구 및 문제점 분석

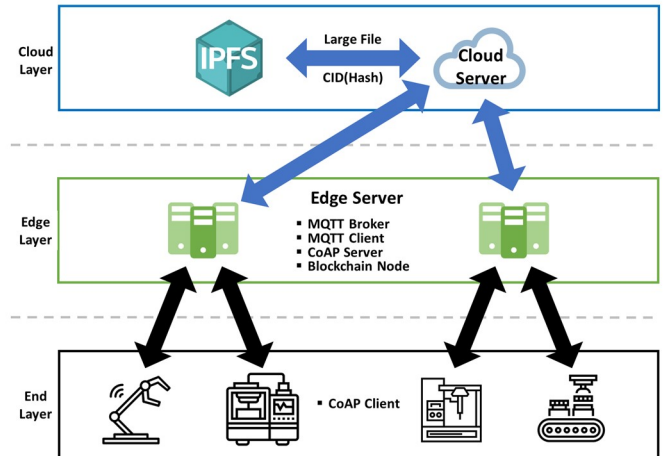


그림 1 경량화된 블록체인 기반 엣지 컴퓨팅 시스템

그림 1은 IIoT 환경에서 IPFS를 사용하여 블록체인의 확장성을 개선한 [3]의 엣지 컴퓨팅 시스템의 구성을 보여준다. 이 시스템은 프라이빗 블록체인, IPFS, CoAP 및 MQTT를 이용하여 엔드 - 엣지 - 클라우드 레이어를 구성한다. CoAP 및 MQTT를 기반한 통신 모델을 통해 엣지 레이어에서 엔드 레이어로부터 전송된 데이터를 처리하여 블록체인에 저장한다. 이때, 트랜잭션 규모 제한으로 블록체인에 직접 저장할 수 없는 데이터는 MQTT를 통해 클라우드 레이어로 전송된다. 클라우드 서버는 데이터를 IPFS에 업로드하고 해시 값을 반환받아 엣지 레이어로 전달한다. 엣지 서버는 전달된 해시 값을 블록체인에 저장한다. 하지만 이러한 접근 방법은 Broker가 데이터를 중개하는 방식인 MQTT의 네트워크 혼잡과 패킷 손실에 취약한 특성상, 참여 노드의 수가 방대해지면 통신 성공률이 낮아지고 지연시간이 높아지는 등 성능 저하가 일어난다는 문제가 있다. 따라서 IIoT 환경에 그대로 적용하기에 적합하지 않다[4].

III. 제안하는 DDS 기반 블록체인의 데이터 확장성 향상 기법

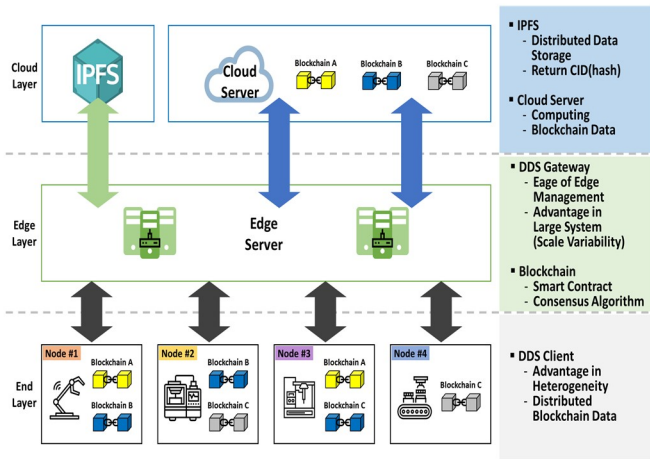


그림 2 IPFS를 결합한 DDS 기반 블록체인 기법의 아키텍처

본 논문이 제안하는 산업용 IoT를 위한 IPFS가 결합된 DDS 기반 블록체인 기법의 아키텍처는 그림 2와 같다. 제안하는 아키텍처는 엔드 레이어의 DDS 클라이언트, 엣지 레이어의 DDS 게이트웨이, 클라우드 레이어의 IPFS와 클라우드 서버로 구성된다. 각 엔드 디바이스는 DDS 클라이언트가 설치되어 디바이스의 각 애플리케이션이 서로 다른 특성이 있더라도 DDS 통신이 가능하다. DDS 게이트웨이는 각 노드가 데이터를 중개자 없이 Topic에 따라 Publish 및 Subscribe 함으로써 직접 통신하게 하여 엣지 관리를 용이하게 하고 대규모 시스템에 유리하게 한다. 또한 엣지 레이어에서는 엔드 디바이스에서 발생하는 데이터를 블록체인에 분산 저장하기 위해 DDS를 활용하여 트랜잭션 과정을 진행한다. 제안된 시스템에서 채택한 블록체인의 종류는 사전에 네트워크 참여를 허가받은 노드로만 이루어지는 폐쇄형 네트워크에 적합한 프라이빗 블록체인이다. DDS 기반 트랜잭션 생성으로 각 노드는 전체 시스템에서 발생한 모든 블록체인 데이터를 저장하지 않고 Subscribe 한 Topic 별로 저장하여 리소스를 확보할 수 있다. 이때 합의 알고리즘을 거쳐 트랜잭션을 생성하기 위해 클라우드 서버도 노드로 참여한다. 그리고 블록체인에 저장할 수 없는 대용량 데이터의 저장 문제를 해결하고 블록체인 데이터를 더욱 경량화하기 위해 모든 엔드 디바이스에서 발생한 데이터는 IPFS에 업로드한 후 반환되는 해시 값, 즉 CID(Content Identifier)로 대체하여 블록체인에 저장된다.

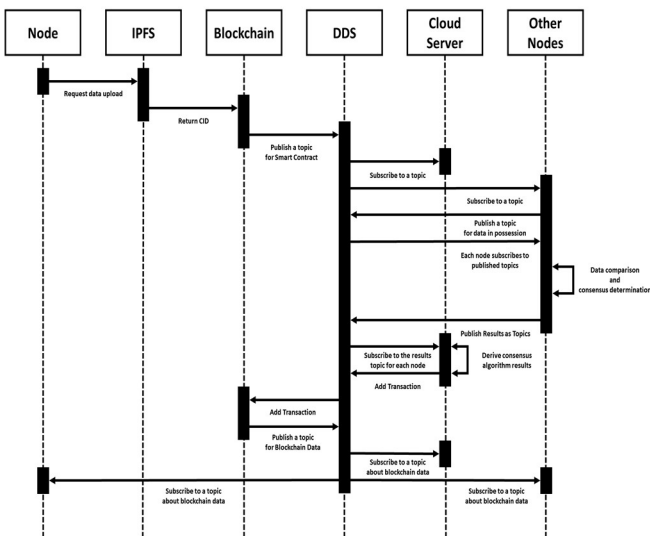


그림 3 IPFS를 결합한 DDS 기반 블록체인 기법의 순서도

그림 3은 제안하는 기법으로 산업 데이터를 블록체인에 저장하는 과정을 나타낸 순서도이다. 엔드 디바이스에서 데이터가 발생하면 IPFS에 업

로드하여 CID를 얻는다. CID는 원본 데이터 대신 블록체인 데이터에 저장되기 위해 블록체인 노드로 전달되며, 블록체인 노드는 스마트 계약을 위한 Topic을 Publish 한다. 다른 노드들과 클라우드 서버는 합의 알고리즘을 진행하기 위해 이 Topic을 Subscribe 한다. 그 후 클라우드 서버를 제외한 각 노드는 데이터를 비교하고 동기화하기 위해 각각의 데이터를 Publish 하고 Subscribe 한다. 데이터를 비교하여 합의를 이룰 수 있다고 판단되면 각 노드는 판단 결과를 Publish하고, 클라우드 서버는 이를 Subscribe 하여 합의 알고리즘에 따라 합의 여부를 최종 판단한다. 합의가 도출되면 트랜잭션 추가가 요청되어 블록체인 노드에 트랜잭션이 생성된다. 추가된 블록체인 데이터는 Topic으로 Publish 되고, 각 노드가 Subscribe 하여 분산 저장이 완료된다.

VI. 결론 및 향후 연구

본 논문은 IIoT 환경에서 DDS 기반 블록체인에 IPFS를 결합하는 기법을 제안하여 데이터 확장성을 향상하고자 하였다. 또한 해당 접근법은 DDS, 블록체인, IPFS를 유기적으로 구성하여 각자의 한계점을 상호 보완함으로써 리소스 제약을 극복하고 데이터 무결성을 강화하며, 안정성과 실시간성을 만족할 수 있도록 설계되었다.

향후에는 적합한 합의 알고리즘을 선택하여 스마트 컨트랙트 과정을 시스템 구조에 맞게 최적화하고 데이터 쿼리와 관련된 과정을 추가 설계할 계획이며, 성능 평가를 수행하고 실시간성을 고도화하는 연구를 진행할 예정이다.

ACKNOWLEDGMENT

이 논문은 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 지역진흥화혁신인재양성사업(IITP-2024-2020-0-01612, 33%)과 2023년도 정부(교육과학기술부)의 재원으로 한국연구재단의 대학중점연구소 지원사업(2018R1A6A1A03024003, 33%)과 과학기술정보통신부 및 정보통신기획평가원의 ICT혁신인재4.0 사업의 연구결과로 수행되었음(IITP-2023-2022-00156394, 33%)

참고 문헌

- [1] J.-H. Cha, J.-W. Lee, J.-M. Lee and D.-S. Kim, "Real-time Middleware Application and Trend Study for Civil and Military ICT Convergence Technologies," The Journal of The Korean Institute of Communication Sciences, vol. 37, no. 10, pp. 47-54, 2020
- [2] J.-W. Lee, H.-J. Kim, J.-M. Lee, T.-S. Jun, and D.-S. Kim, "Blockchain-Based Data Sharing Scheme to Enhance Reliability and Security for Naval Combat Systems," The Journal of Korean Institute of Communications and Information Sciences, vol. 47, no. 6, pp. 809-817, 2022
- [3] W. Li, M. He, W. Zhu and J. Zheng, "A Study on Lightweight And Secure Edge Computing Based Blockchain," 2021 IEEE 12th International Conference on Software Engineering and Service Science (ICSESS), Beijing, China, pp. 256-261, 2021
- [4] C. Gundogan et al., "The Impact of Networking Protocols on Massive M2M Communication in the Industrial IoT," in IEEE Transactions on Network and Service Management, vol. 18, no. 4, pp. 4814-4828, Dec. 2021