IoT 시스템의 효율적인 리소스 관리를 위한 블록체인 기법

이종우[1], 이재민[2], 김동성[3], 김재우*
금오공과대학교 {IT 융복합공학과[1], 전자공학부[2,3], ICT융합특성화연구센터*}
{whddn4547[1], ljmpaul[2], dskim[3], jeawookim*}@kumoh.ac.kr

Blockchain Scheme for Efficient Resource Management of IoT Systems

Jong-Woo Lee[1], Jea-Min Lee[2], Dong-Seong Kim[3], and Jea-Woo Kim*
{Dept. of IT Convergence Eng.[1], School of Electronic Eng.[2,3], ICT-CRC*} Kumoh National Institute of Technology

요 약

본 논문에서는 IoT 네트워크 환경에서 사용되는 블록체인에서 각각의 노드들의 리소스를 효율적으로 관리하기 위한 블록체인 기법을 설계한다. 현재 블록체인은 다양한 분야에서 적용되고 있다. 그중 IoT 네트워크에서 사용되기 위해 경량화된 블록체인 기법들이 대두되고 있다. 그러나 각 노드가 오래된 블록체인의 데이터를 저장하기에는 많은 리소스가 소요된다. 이러한 문제점을 해결하기 위해 프라이빗 블록체인에서 각 노드의 리소스가 부족한 현상이 발생하기 전에 이미 저장되어 있던 블록체인을 하나의 블록으로 서버에 저장하고 각 노드의 블록체인 데이터를 제거한다. 서버에서는 블록체인 데이터가 저장된 블록을 체인으로 저장하고 각 노드는 저장을 위해 사용되는 리소스를 확보함으로써 리소스가 부족한 문제를 해결할 수 있다.

Ⅰ. 서 론

최근 2008년 Nakamoto의 논문을 시작으로 비트코인이 생겼으며 블록체인이 대두되고 있다[1]. 블록체인의 특징으로는 탈중앙화 특성이 있어 중앙서버를 두지 않아 SPF(Single Point of Failure) 문제를 해결하였다. 저장 방식으로는 분산저장 기법을 사용하여 네트워크에 속한 모든 노드가 똑같은 블록체인 데이터를 가지고 있다. 이렇게 저장되는 데이터는 네트워크의 노드들이 합의 알고리즘을 이용하여 합의가 이루어진 신뢰성 있는 데이터만 블록체인에 저장될 수 있다. 이렇게 신뢰성이 보장되는 트랜잭션을 블록에 저장하고 저장된 블록들은 체인 형태로 연결되어 저장된 데이터의 보안성을 향상된다.

이러한 블록체인은 최근 매디컬 분야, 차량, IoT 기반의 네트워크 등 다양한 분야에 적용되고 있다[2][3][4]. 그중에서도 IoT 기반의 네트워크에서는 각 노드의 리소스가 충분하지 않아 LightChain과 같은 경량화된 블록체인 시스템이 연구되고 있다[5]. 그러나 경량화된 블록체인 분야에서도 무한정 이어지는 블록체인 데이터의 관리에 관한 연구는 부족하다. 블록체인의 데이터는 체인과 같이 연결되어있고 모든 블록이 연결되어있어 블록체인 데이터를 중간에 끊을 수 없는 문제점이 있다.

제안하는 기법은 프라이빗 블록체인 네트워크에서 특정 노드의 리소스가 부족한 현상이 발생할 때, 각 노드가 분산저장하고 있는 블록체인 데이터를 서버의 한 블록에 저장한다. 이때, 기존에 저장됐던 블록체인 데이터는 한 블록으로 형성되어 서버에 저장되고 각 노드가 기존에 저장했던 데이터를 삭제함으로써 각 노드는 저장을 위해 사용되는 리소스를 확보할 수 있다.

Ⅱ. 기존연구 및 문제점

블록체인은 크게 퍼블릭 블록체인과 프라이빗 블록체인으로 나누어 진다[6]. 퍼블릭 블록체인은 공개형 블록체인이라고도 불리며 특징으로서는 비트코인, 이더리움과 같이 네트워크에 참여할 수 있는 조건만 갖추고 있다면 누구나 참여하여 블록을 생성할 수 있다. 프라이빗 블록체인은 폐쇄형 블록체인이라고도 불리며 퍼블릭 블록체인과 달리 서버가 존재한다. 프라이빗 블록체인 네트워크에 참여하기 위해서는 서버로부터 인증을 받아야만 하고 인증을 받은 참여자만 네트워크에 참여하여 블록을 생성할 권한을 가진다[7].

블록체인은 적용 분야에 따라 퍼블릭 블록체인 또는 프라이빗 블록체인을 사용한다. 누구에게나 정보를 공유하고 데이터의 투명성을 보장하기 위해서는 주로 퍼블릭 블록체인을 사용하고 그렇지 않다면 프라이빗 블록체인을 주로 사용한다.

IoT 기반의 시스템과 같이 모든 사람에게 정보를 공유할 필요가 없는 분야에서는 역시 프라이빗 블록체인이 주로 사용된다. 그러나 IoT 기반의 시스템에서 시간이 흐를수록 블록체인 데이터는 끝도 없이 증가하게 되고 노드는 데이터를 저장하기 위해 많은 리소스를 필요로 할 것이다. 노드가 저장하기 위해서 많은 리소스를 소모한다면 블록을 생성하거나 트랜잭션을 생성할 때에 사용될 리소스가 부족하여 노드의 부하가 증가하게 되고 그로 인해 트랜잭션 및 블록의 생성속도가 늦어진다.

Ⅲ. 제안하는 기법

프라이빗 블록체인이 적용된 IoT 기반의 시스템은 그림 1과 같이 하나의 서버와 서버로부터 인증받은 여러 노드로 구성된다. 제안하는 기법은 서브 블록체인과 메인 블록체인으로 저장되는 데이터가 구성되어 있다. 각 노드는 서브 블록체인 데이터를 저장하고 있다. 서브 블록체인은 각 노드가 트랜잭션은 생성하며 만들어지는 블록체인을 의미한다. 서버가 저장하는 메인 블록체인은 서브 블록체인 데이터를 블록의 트랜잭션에 저장하고 있는 블록체인 데이터이다.

그림 2에서 왼쪽 노드의 동작으로는 일반적인 프라이빗 블록체인과 같이 합의 알고리즘을 통해 신뢰성이 보장된 데이터를 서브 블록체인에 추가할

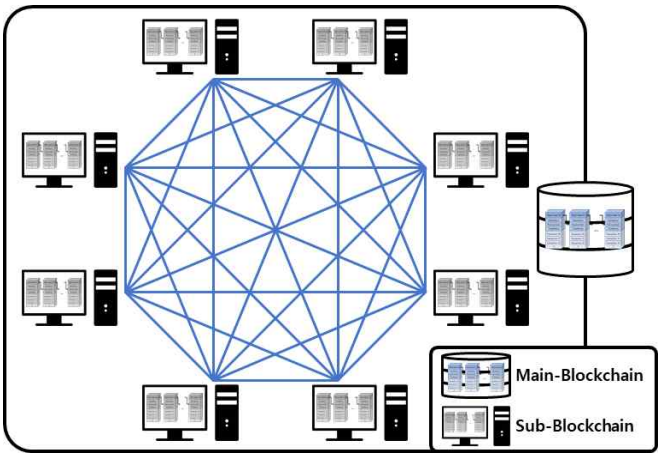

그림 1 제안하는 기법의 구성도

수 있다. 오른쪽 서버의 동작으로는 각 노드의 리소스에서 서브 블록체인 데이터 저장을 위해 사용되는 비중을 항시 파악한다. 만약 서버가 하나 이상의 노드에서 서브 블록체인 데이터 저장을 위해 사용되는 리소스 비중이 크다고 판단할 경우, 그 시점까지의 서브 블록체인 데이터를 트랜잭션으로 만들어 하나의 메인 블록을 생성하고 메인 블록체인에 추가한다. 그 후 각 노드는 저장했던 서브 블록체인 데이터를 삭제함으로써 네트워크에 속한 노드들의 리소스를 확보할 수 있다. 저장을 위해 사용하던 리소스가 확보됨으로써 노드들의 거래는 다시 활발히 이루어질 것이다. 또한, 각 노드는 서브 블록체인이 삭제된 각 노드는 제네시스 블록을 시작으로 새로운 서브 블록체인을 저장하여 새로운 서브 블록체인을 만든다.

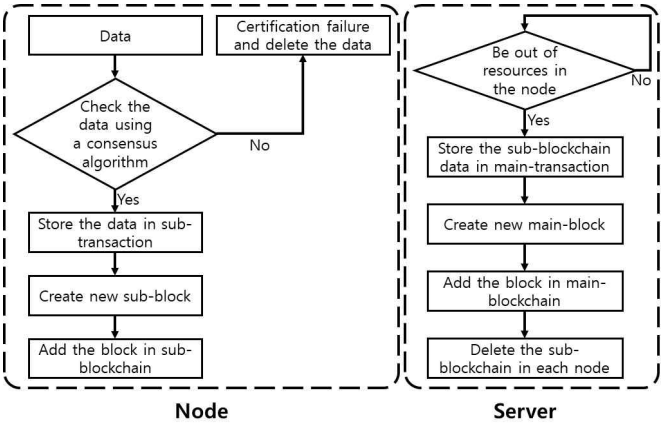

그림 2 제안하는 기법의 동작 구조

제안하는 기법을 통하여 저장된 메인 블록체인 데이터는 그림 3과 같이 구성되어 있다. 메인 블록체인과 서브 블록체인의 구조는 Merkle Root, Transaction, PreviousHash 등과 같이 기존 블록체인과 같은 데이터로 구성된다. 합의 알고리즘, 체인기법을 준수하는 저장형태 등 기존의 블록체인의 요구사항을 만족할 수 있다. 또한, 인증을 위한 하나의 서버와 서버로부터 인증을 받은 노드만이 네트워크에 참여할 수 있는 프라이빗 블록체인의 요구사항도 만족할 수 있다. 제안하는 기법과 일반적인 프라이빗 블록체인의 차이점은 메인 블록체인에서 저장되는 트랜잭션에는 서브 블록체인이 저장된다는 점이다. 그로 인해 메인 블록체인의 Merkle Root는 서브 블록체인의 해시값으로 구성된다. 특정 노드가 현재 서브 블록체인보다 이전의 데이터를 확인하고 싶다면 기존의 Merkel Root를 이용하여 데이터를 손쉽게 확인했던 방법과 똑같이 이미 저장된 데이터를 확인할 수 있다.

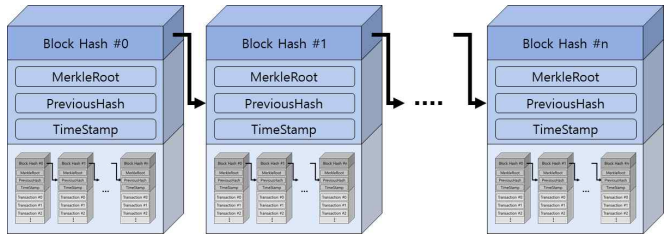

그림 3 서버에 저장된 블록체인 데이터 구조

Ⅲ. 결론

본 논문에서는 IoT 기반의 시스템에서 각 노드의 효율적인 리소스 관리를 위한 블록체인 기법을 설계한다. 제안하는 기법을 이용하여 서버는 네트워크에 참여한 각 노드의 블록체인 데이터를 저장하기 위해 사용되는 리소스 사용량을 효율적으로 관리할 수 있다. 노드의 저장을 위한 리소스를 관리함으로써 노드는 많은 리소스를 필요로 하지 않게 되고 컴퓨팅 속도도 향상될 수 있다. 향후 연구로는 실제 네트워크 시뮬레이션을 구현하여 성능평가가 필요하며 서버가 저장하는 메인 블록체인 데이터의 관리 방안에 관한 연구가 필요하다.

ACKNOWLEDGMENT

이 논문은 2019년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업이고(2019R1I1A1A01063895) 과학기술정보통신부 및 정보통신기획평가원의 Grand ICT연구센터지원사업의 연구결과로 수행되었음(IITP-2020-2020-0-01612).

참 고 문 헌

[1] Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, 2008.

[2] 권혁준, 김협, 최재원, “개인 의료정보 보호를 위한 블록체인 적용방안 : 프라이빗 블록 스킴을 중심으로”, 한국지식경영학회 Vol. 19, No. 4, pp. 119-131, Dec. 2018.

[3] 백재희, 박슬우, 신용태, “블록체인 기반의 차량 통합 관리 시스템에 관한 연구”, 한국정보과학회 학술발표논문집, pp. 1274-1276, June 2019.

[4] Daniel Minoli, and Benedict Occhiogrosso, “Blockchain mechanisms for IoT security”, Internet of Things, Vol. 1-2, pp. 1-13, Sep. 2018.

[5] Ronald Doku, Danda B. Rawat, Moses Garuba, and Laurent Njilla, “LightChain: On the Lightweight Blockchain for the Internet-of-Things”, 2019 IEEE International Conference on Smart Computing, pp. 444-448 , June 2019.

[6] Janvi Dattani, and Harsh Sheth, “Overview of Blockchain Technology”, Asian Journal of Convergence in Technology, Vol. 5, No. 1, pp. 1-3, Apr. 2019.

[7] 이종우, 이재민, 김동성, 김재우, “함정 전투 시스템의 신뢰성 향상을 위한 DDS 기반의 블록체인 기법”, 한국통신학회 학술대회논문집, pp. 291-292, 2020.