

# 신뢰체인기반 네트워크 접근제어 메커니즘

최환석, 이우섭\*  
KAIST, 한밭대학교\*

hkrock7904@gmail.com, wsrhee@hanbat.ac.kr\*

## Trust Chain based Network Access Control Mechanism

Choi Hoan Suk, Rhee Woo Seop\*  
KAIST, Hanbat National University\*

### 요약

최근 대용량의 데이터들이 수집 및 분석되고 있어 데이터의 오용, 무단 사용 등이 빈번히 발생하고 있다. 더욱이 개인 정보에 대한 무단 수집과 사용은 새로운 사회 문제로 대두되고 있다. 이를 위해, 블록체인 기술을 이용해 데이터에 대한 무단 접근을 제어하는 기술이 새로이 주요 이슈로 부각되고 있다. 본 논문에서는 기 연구된 신뢰 체인을 이용한 네트워크 접근 제어 메커니즘을 제안한다.

### I. 서론

최근 사물인터넷과 인공지능 기술의 발달로 대용량의 데이터들이 수집 및 분석되고 있어 데이터의 오용 및 침해, 무단 사용 등이 빈번히 발생하고 있다. 더욱이 개인 정보에 대한 무단 수집과 사용은 새로운 사회 문제로 대두되고 있다. 이를 위해, 데이터에 대한 무단 접근을 제어하는 기술이 새로이 주요 이슈로 부각되고 있으며 이를 위해 블록체인 기술을 이용하는 연구도 진행되고 있다.[1]

접근제어란 시스템이 인증된 주체 (subject)의 객체 (object)에 대한 접근 요청을 승인 또는 거절하는 절차를 의미한다[1]. 이는 네트워크 자원에 대한 허용되지 않은 접근을 감시하며 접근 요청에 대한 사용자를 식별하고 기록하며 보안 정책에 따라 승인 또는 거절함으로써 비인가자로부터 불법적인 접근을 예방할 수 있다.[2]

한편, 블록체인의 분장 원장 기술을 이용하면 P2P 분산 네트워크 상에서 모든 참여자가 검증과 합의를 통해 네트워크 상의 정보 및 기록을 분산 저장함으로써 중앙 서버가 아닌 분산된 네트워크 노드들이 공유하여 정보의 투명성, 보안성 및 신뢰성을 보장할 수 있다. 이러한 블록체인의 특성을 이용하면 기존 접근제어의 문제점인 효율성, 확장성, 데이터 소유권 및 체계적인 데이터 수명주기 접근 문제를 해결할 수 있다.[2]

그러나, 기존의 연구에서는 블록체인을 이용하여 데이터의 접근제어에만 관점을 두었지 블록체인 기술 자체의 복잡성을 간과하였다. 이는 블록체인 기술이 근본적으로 개방형 구조이기 때문에 누구나 네트워크에 접근할 수 있다. 따라서, 개방형 분산구조에서 정보의 보안성과 투명성을 높이기 위해 복잡한 암호화 해시 알고리즘 및 합의 알고리즘을 사용하기 때문에 블록체인의 노드로 등록하기 위해서는 이에 상응하는 컴퓨팅 자원을 갖추어야 한다.

이 문제점의 해결책으로 일부 연구에서는 승인된 사용자만 접근이 가능하도록 통제하는 프라이빗 블록체인을 사용하여 합의 알고리즘의 복잡성을 줄이려 하였지만[2] 이는 완전 분산형이 아니라 중앙집중 제어를 사용하기 때문에 정보의 보안성 유지에 문제가 존재한다.

이를 위해 본 논문에서는 기 연구된 신뢰 기반의 체인 메커니즘인 신뢰체인[3]을 사용하여 경량화된 블록체

메커니즘을 사용하는 신뢰체인 기반의 네트워크 접근제어 메커니즘을 제안한다.

### II. 신뢰체인 메커니즘

신뢰체인은 그림 1의 개념도와 같이 체인 메커니즘에 참여하는 모든 장치들과 입력 데이터들에 대한 신뢰도 평가 메커니즘을 적용하여 신뢰할 수 있는 장치들만 참여할 수 있는 프라이빗 체인을 구성하고 여기에 경량화된 합의 알고리즘과 해시 알고리즘을 이용하는 블록 생성 메커니즘을 적용한다. 이는 분산 네트워크 형태이지만 블록체인의 복잡한 알고리즘과 빠른 연산 능력을 요구하지 않는 경량화된 블록체인 기술을 적용시켜 트랜잭션들과 블록들에 대한 기밀성과 무결성이 보장되는 메커니즘이다.[3]

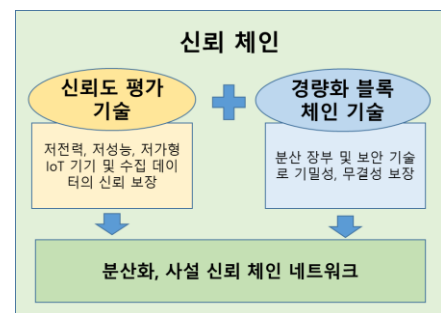


그림 1. 신뢰체인 개념도

또한, 선행 연구인 [4]에서는 블록체인 기반의 분산 네트워크를 구성하는 노드의 신뢰 정도에 따라 역할 및 권한을 차등적으로 적용하며 노드를 신뢰 노드, 후보 노드, 접근 노드로 구분하는 방법도 제안하였다.

### III. 신뢰체인기반 접근제어 메커니즘

#### 3.1 신뢰체인의 계층적 구조

본 논문에서 제안하는 신뢰체인 기반 네트워크 접근제어 메커니즘은 기존 블록체인 메커니즘에서 접근제어와 인증을 위한 네트워크 전체의 부하를 줄이기

위해 그림 2 와 같이 인증관리 체인 (AMC: Authentication Management Chain)과 서비스 체인의 2 계층 구조로 설계되었다.

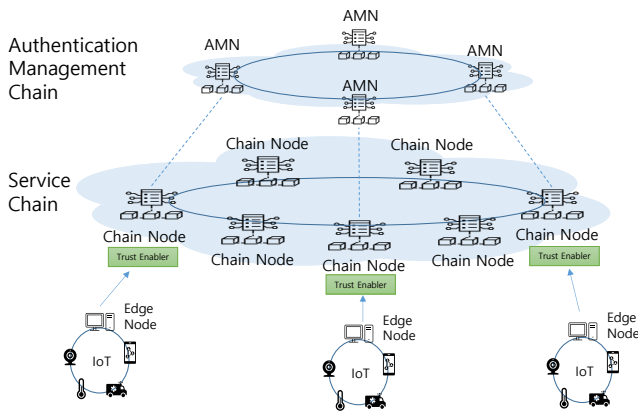


그림 2. 계층적 신뢰체인 구조

서비스 체인은 본 연구의 신뢰 체인을 이용하여 사물인터넷 기반의 블록체인 서비스를 제공하는 체인이고, 인증 관리 체인 (AMC)은 서비스 체인의 접근제어를 위한 별개의 관리 체인으로 인증 관리 노드 (AMN: Authentication Management Node)들로 구성된 체인이다. 인증 관리 노드는 다음 그림 3 과 같이 한 관리 지역 (Area)내에서 서비스 체인 노드, 장치 및 사용자의 접근제어, 인증을 관리하는 대표 노드이다. 즉, 지역내 노드나 장치는 서비스 체인에 등록하기 전에 AMN의 인증을 받아야 등록이 가능하다.

이와 같이, 신뢰체인을 2 단계의 계층적 구조로 운영함으로써 노드 및 장치에 대한 인증 및 접근제어 관리를 AMN에 국한시키고 전체 서비스 체인에 대해서는 부하를 줄일 수 있다. 또한, AMN들로 구성된 인증 관리 체인을 이용하여 접근제어를 기능을 네트워크 전역으로 분산시킬 수 있다.

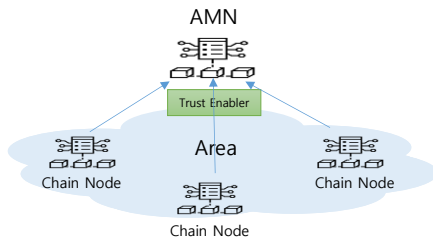


그림 3. AMN의 개념

### 3.2 제안하는 네트워크 접근제어 메커니즘

기존의 블록체인 기반 접근제어 방법들은 최초 한번의 등록으로 인증이 유지되어 서비스 중에 노드나 장치의 이상 동작이나 의도적인 공격을 탐지하기 위해 블록체인의 복잡한 합의 알고리즘을 사용하고 있다.

그러나, 본 논문에서 제안하는 접근제어 메커니즘은 서비스체인을 운영하면서 노드나 장치의 신뢰 상태를 추적함으로써 노드나 장치의 이상을 감지하고 신뢰 정도가 낮아지면 노드나 장치의 접근 제어 권한을 제한하는 방법이다. 이는 현재의 노드나 장치의 신뢰 정도에 대한 상태를 항상 추적하고 있기 때문에 이상 감지나 비정상 동작을 검출하기 위한 복잡한 합의 알고리즘이 필요 없게 된다.

이 알고리즘은 현재 이슈가 되고 있는 제로트러스트 네트워크의 개념을 신뢰 메커니즘으로 해결할 수 있는 방안을 제시해 준다. 제로트러스트는 누구도 무엇도

신뢰할 수 없으니 모든 것을 검증해야 한다는 개념[5]으로 본 논문에서 제안하는 네트워크 접근제어는 사용자 식별 및 지속적인 추적, 관찰을 통해 실시간으로 상태를 파악하며 그에 따른 권한을 제공할 수 있어 제로트러스트 네트워크를 구현할 수 있는 기술이다.

한편, 본 논문에서 제안하는 신뢰체인 기반 접근제어 메커니즘의 신뢰 레벨 평가 방법은 기본적으로 REK(Reputation, Experience, knowledge) 모델을 사용하며 네트워크 노드에 대한 Reputation 평가는 다음 예와 같이 트랜잭션 응답률과 트랜잭션 평가 성공률을 이용한다.

- 트랜잭션 응답률 =  $\frac{\text{응답 트랜잭션 수}}{\text{요청 트랜잭션 수}}$
- 트랜잭션 평가 성공률 =  $\frac{\text{평가 성공 트랜잭션 수}}{\text{평가 요청 트랜잭션 수}}$

또한, 그림 2 에서와 같이 접근제어 기술을 담당하는 트러스트 인에이블러(Trust Enabler)라는 기능 블록으로 구현하여 신뢰체인이 아닌 일반 블록체인의 메커니즘에도 적용 가능하도록 독립 모듈 형태로 구현이 가능하다.

## IV. 결론

본 논문에서는 사물인터넷 서비스 환경을 위해 블록체인의 단점을 보완할 수 있는 신뢰도 평가 기술 기반의 신뢰체인 메커니즘을 제안하였다. 블록체인을 사용하여 사물인터넷 서비스에 신뢰성을 높이려는 기존의 연구와 본 논문에서 제안하는 신뢰체인의 기본적인 차이점은 신뢰도 평가 메커니즘의 사용에 있다. 즉, 신뢰체인은 먼저 사물인터넷 장치들에 신뢰도 평가를 수행하여 체인에 참여하는 모든 장치와 데이터에 대한 신뢰를 보장하며 신뢰도 레벨을 기반으로 허가된 장치들만 참여할 수 있는 프라이빗 체인을 구성하고 경량화 된 블록체인 기술을 적용시켜 트랜잭션들과 블록들에 대한 기밀성과 무결성을 보장한다.

앞으로 각 계층별 신뢰 체인 메커니즘들에 적용될 신뢰도 평가 알고리즘과 경량화 된 합의 알고리즘의 완성도를 높이고 성능 평가를 수행할 예정이다.

## ACKNOWLEDGMENT

이 논문은 2021 년도 정부 (과학기술정보통신부)의 재원으로 정보통신기획 평가원의 지원을 받아 수행된 연구임 (No. 2020-0-00833, 5G 기반 지능형 IoT 트러스트 인에이블러 핵심기술 연구)

## 참 고 문 헌

- [1] 박환, 김미선, 서재현, “분산원장을 이용한 토큰기반 사물인터넷 접근제어 기술,” 정보보호학회논문지, Vol. 29, No. 2, 2019.4.
- [2] 김승현, 김수형, “블록체인 기반 접근제어 기술 동향,” 전자통신동향분석, ETRI, 제 34 권, 제 4 호 pp. 117-128, 2019. 8.
- [3] Hoan-suk Choi, Gyu-Myoung Lee, Woo-Seop Rhee, “Hierarchical Trust Chain Framework for IoT Services,” IEEE ICUFN2019, 2019. 7.
- [4] 최환석, 이우섭, “신뢰수준 기반의 분산원장 네트워크 구성 방법,” 한국통신학회 하계종합학술대회, 2020. 12.
- [5] 권정수, IT Daily, “‘제로트러스트’ 네트워크 근간으로 주목 IoT·OT로 영역 확장,” <https://www.itdaily.kr/news/articleView.html?idxno=202868>