사물인터넷(IoT)에서의 블록체인 활용 관련 연구동향 분석

강창훈, 최원석, 우종수, 홍원기
포항공과대학교 컴퓨터공학과

{chkang, ws4583, woojs, jwkhong}@postech.ac.kr

Analysis of Research Trends Related to the Use of Blockchain in the Internet of Things (IoT)

Changhoon Kang[1], Wonseok Choi[1], Jongsoo Woo[2], James Won-Ki Hong[1]
[1]Department of Computer Science and Engineering, POSTECH
[2]Graduate School of Information Technology, POSTECH

요 약

사물인터넷(Internet of Things, IoT)은 사물에 연산 및 통신 기능을 부여함으로써 이들을 연결해주는 기술을 말한다. 지금까지 스마트홈, 스마트팩토리, 커넥티드카 등의 분야에서 IoT 기술이 많이 활용되고 있으며, 점점 더 다양한 영역으로 활용 범위가 넓어질 것으로 기대된다. 기존의 전통적인 IoT 시스템은 중앙화 된 주체가 네트워크에 연결된 모든 기기들의 인증이나 접근 권한 등을 관리한다. 하지만 이런 형태의 모델은 단일 장애점 (Single Point of Failure)과 같은 위험을 가지고 있으며, 수많은 기기들의 신원 관리와 그들로부터 수집한 데이터의 무결성을 보장하는 것이 어렵다. 따라서 탈중앙화 되어 있고 신원 관리 기능을 제공하며 조작이 불가능한 특성을 가지는 블록체인을 IoT 와 접목시켜 해당 어려움을 해결하려는 여러 연구가 진행되고 있다. 일반적인 블록체인들은 시스템 운영을 위해, 연결된 노드들이 충분한 연산 능력과 많은 저장 공간을 갖고 있어야 한다. 반면에 대부분의 IoT 기기들은 제한된 크기의 연산 능력과 저장 공간을 갖고 있기 때문에, 기존의 블록체인 시스템에서 노드로 동작하기에는 어려움이 있다. 본 논문에서는 IoT 기기와 같이 자원이 제한된 디바이스들로 구성된 네트워크에서 블록체인을 효율적으로 활용하기 위한 연구의 동향을 분석했다. 블록체인의 경량화를 통해 IoT 기기가 블록체인 노드로써 동작할 수 있게 하거나, 충분한 자원을 가진 기기를 IoT 네트워크에 추가하고 동시에 블록체인 노드 역할을 하도록 하는, 현재 크게 두 가지 다른 방식의 접근법으로 연구가 진행되고 있다.

Ⅰ. 서론

IoT [1] 기술은 현재 여러 가전제품과 자동차 등 다양한 기기에 이미 적용되어 일상속에서 많이 사용되고 있다. 인터넷을 통해 연결된 수많은 IoT 기기들은 방대한 양의 데이터를 생성하고 축적한다. 센서와 같은 작은 디바이스가 생산하는 많은 양의 데이터를 수집함으로써 이후 빅데이터 분석을 통해 더욱 발전된 서비스를 제공할 수 있게 된다. 일반적으로 IoT 시스템은 client/server paradigm 으로 디자인되었기 때문에, 네트워크에 속해 있는 기기로부터 생산되는 데이터와 기기들의 접근 제어 (Access Control)를 모두 중앙화 된 주체가 담당해야 한다. 이런 구조는 단일 장애점 (Single Point of Failure) 위험을 야기하고, 데이터의 무결성을 보장할 수 없다. 중앙화 된 주체가 공격받는다면 전체 시스템이 동작할 수 없게 되고, 생산되었던 모든 데이터들이 소실될 수 있다. 따라서 이런 문제점을 블록체인과의 융합을 통해 해결하려는 시도들이 이어지고 있다.

블록체인은 데이터를 블록 단위로 가공하여 사슬 구조로 원장에 저장하고, Peer-to-Peer (P2P) 네트워크 [2] 내에 속한 분산된 모든 노드들이 각자 동일한 원장을 관리한다. 따라서 누구도 임의로 데이터를 몰래 수정할 수 없다. 또한 모든 참여자들이 하나의 온전한 원장을 저장하기 때문에 일부 노드에 Failure 가 발생하더라도 시스템이 동작하는 것에는 아무런 문제가 없다. 이러한 블록체인의 특성 덕분에 블록체인을 IoT 에 결합한다면 앞서 언급된 기존 IoT 시스템의 문제점을 해결할 수 있다.

Proof-of-Work (PoW) [2] 합의 알고리즘을 사용하는 일반적인 블록체인 시스템이 동작하기 위해서는 높은 연산능력 (Computing Power)와 충분한 데이터 저장 공간이 필요하다. [3] 블록 생성을 위해 복잡한 암호학적인 계산들이 필요하고, 시간이 지남에 따라 매번 생성되는 모든 블록들을 영구적으

로 보관해야 하기 때문이다. 하지만 IoT 기기들은 사용할 수 있는 CPU, 메모리, 스토리지 등의 자원이 제한되어 있기 때문에 블록체인 시스템의 노드로써 이용되기에 적합하지 않다. 적정한 수준 이상의 보안을 유지하기 위해서 기존과 같은 수준의 복잡도를 가지는 계산이 필요하다면, 블록을 생성하고 저장하는데 아주 오랜 시간이 걸리게 된다. 또한 시스템 동작 이후 얼마 가지 않아서 스토리지가 가득 차는 상황이 발생할 것이다. 이런 문제점을 해결하기 위해 효율적으로 IoT 와 블록체인 기술을 융합하는 것이 해당 분야의 주요 연구 과제이다.

본 논문에서는 이를 위해 어떤 연구들이 수행되고 있는지 동향에 대해 알아본다. 연구는 크게 두 가지 다른 접근법으로 나눌 수 있었다. 첫 번째 접근은 블록체인의 경량화를 통해 IoT 기기가 블록체인 노드로써 동작할 수 있도록 하는 것이다. 두 번째 방법은 충분한 자원을 가진 기기를 IoT 네트워크에 추가하여 동시에 블록체인 노드의 역할을 수행하도록 하는 것이다. 본 논문의 나머지 부분에서는 각 접근 방식에 해당하는 연구들을 소개한다.

II. IoT 와 블록체인의 융합

본 논문에서는 IoT 와 블록체인의 융합에 대한 연구를 크게 두 가지 다른 접근 방식을 정의하여 분류했다. IoT 기기를 그대로 블록체인 노드로 사용할 수 있도록 블록체인의 경량화를 진행하는 연구 방식이 한 가지 접근법이다. 반대로 IoT 네트워크에 자원이 충분한 기기를 추가하여 이것이 블록체인 노드의 역할을 수행하도록 하는 접근법이 존재한다. 대부분의 연구들이 이 두 가지 접근법 중 하나에 포함되는 것을 확인했다.

1. IoT 기기를 블록체인 노드로 사용

첫번째 접근법은 제한된 크기의 자원을 가진 IoT 기기들을 직접 블록체인 노드로 활용하는 방식이다. 대부분의 연구에서 기기들의 연산능력과 스토리지의 부족을 극복하기 위해, 블록체인을 구성하는 블록이나 트랜잭션의 구조를 수정하고 더욱 가벼운 합의 메커니즘을 새롭게 제안하는 등 블록체인의 경량화에 초점을 두고 있다.

Koshy, Babu, and Manoj [4]는 IoT 시스템 적용에 적합하도록 블록체인 구조를 수정한 Sliding Window Blockchain (SWBC)을 제안했다. (그림 1) 이 연구의 주요 목적은 IoT 시스템의 보안 문제를 블록체인 적용을 통해 해결하는 것이다. 해당 연구에서는 IoT 기기들을 각각 하나의 블록체인 노드로써 동작하도록 했고, IoT 기기들의 제한된 자원만으로도 블록체인 시스템이 운영될 수 있도록 Sliding Window 라는 개념을 통해 새로운 블록을 생성 및 관리하는 방법을 제안했다. 기존 블록체인 구조에서는 블록 헤더에 이전 블록의 Hash 값을 저장한다. 따라서 기록된 데이터를 수정하는 것은 그 이후로 생성된 모든 블록들을 새롭게 생성해야 하기 때문

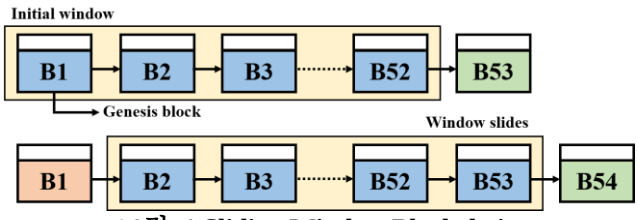

그림 1 Sliding Window Blockchain

에 매우 어렵다. 제안된 방법은 이전 블록 하나의 Hash 를 저장하는 것이 아니라 Sliding Window 크기만큼의 최근 블록들의 hash 를 저장한다. Sliding Window 의 크기는 현재 N 개의 블록이 있다면 1 과 (N-1) 사이의 값을 임의로 가질 수 있다. 즉 마이닝을 하기 위해서는 Window Size 와 그만큼의 최신 블록들을 알고 있어야 하고 이 Window Size 는 마이너들에게만 공개된다. 이 방법을 사용하면 IoT 기기들은 Window Size 보다 앞서서 생성된 블록들을 로컬 스토리지에 저장해둘 필요가 없기 때문에 이를 삭제함으로써 기기의 스토리지 오버헤드를 줄일 수 있다. 모든 블록 데이터들은 IoT 기기에서는 시간이 지나면서 삭제되지만 프라이빗 클라우드에 따로 저장해 계속 보관된다. 또한 이 방법에서는 Proof-of-Work (PoW)의 Difficulty 를 불필요하게 높이지 않고 상황에 따라 알맞게 선택하는 기술을 이용해 PoW 를 간소화함으로써 효율성을 높였다. 결론적으로 스토리지와 연산의 오버헤드를 줄임으로써 IoT 시스템에 블록체인이 적용될 수 있도록 했고, 이를 통해 기존 IoT 시스템의 보안 문제를 해결할 수 있었다.

Huang, et al. [5]는 엣지 컴퓨팅 환경에서 효율적으로 블록체인의 블록 데이터를 저장하는 방법을 제안하고 에너지 소비를 줄일 수 있는 새로운 Proof-of-Stake (PoS) [6] 메커니즘을 제안했다. 이 방법에서 달성하고자 하는 주요 목표는 효율적인 스토리지 사용과 IoT 기기들의 에너지 소비를 낮추는 것이다. IoT 기기들처럼 엣지 컴퓨팅 환경의 기기들은 블록체인의 전체 데이터를 모두 저장하기에는 저장 공간이 매우 부족하다. 따라서 특정 블록 데이터를 모든 기기가 저장하는 것이 아니라 할당된 기기의 저장 공간에만 저장한다. IoT 기기들은 모두 제한된 크기의 스토리지를 갖고 있지만 기기마다 전체 크기나 남은 용량의 차이가 존재한다. 이 기법의 핵심 아이디어는 남은 용량이나 접근의 용이성에 따라 최적의 기기를 데이터 저장을 위해 할당하는 것이다. 시스템은 모든 기기들이 동등한 비율의 저장공간을 사용하도록 한다. 즉, 자원이 많은 기기에는 그만큼 더 많은 공간의 할당이 발생한다. 데이터에 쉽게 접근하기 위해서는 무선 통신에서 데이터 손실을 줄이기 위해 노드의 이동성 (Mobility)이 작은 것이 유리하다. 따라서 특정 두 노드들 간의 거리와 각자의 이동성에 대한 비용을 계산하여 이를 스토리지 할당에 활용했다. 결과적으로 시스템은 효율적으로 모든 기기들의 저장 공간을 관리할 수 있고, 블록 데이터의 탐색이 빨라진다.

이 연구에서는 에너지 소비가 심한 PoW 대신 새로운 형태의 PoS 합의 메커니즘을 제안했다. 각 기기의 시스템에 대한 기여도에 따라 마이닝 성공 확률이 달라진다. 많은 저장 공간이 할당되어 있을수록 더 높은 확률로 블록 채굴에 성공할 수 있다. 이런 특징 덕분에 데이터를 생성하는 기기가 아니더라도 단순히 저장 공간을 제공하기 위해 시스템에 더 많은 노드들이 참여하는 것을 유도할 수도 있다.

2. 충분한 자원의 기기를 블록체인 노드로 사용

두 번째 접근법은 자원이 충분한 다른 기기들을 IoT 기기 대신에 블록체인 노드로 사용하는 방식이다. 이 방법에서는 IoT 기기들을 그룹화하고, 각 그룹마다 블록체인 노드 역할을 하는 충분한 자원의 기기를 둔다. 따라서 해당 충분한 자원의 기기들을 통해서 IoT 기기가 블록체인과 상호작용하게 된다.

Yazdinejad, et al. [7]는 SDN controller 를 블록체인 노드로 사용하는 아키텍처를 제안했다. 이 연구의 핵심 아이디어는 자원이 한정되어 있는 IoT 기기들 대신 이미 네트워크 상에 존재하면서 블록체인 노드로써 역할을 하기에 충분한 자원을 가진 SDN controller 를 활용하는 것이다. 이 연구가 제안한 아키텍처에서는 IoT 기기들이 클러스터 구조로 나누어져 있고, 각 클러스터를 담당하는 SDN controller 가 존재한다. SDN controller 들 사이의 퍼블릭 블록체인을 구성하고, 각 클러스터들마다 IoT 기기들 간의 프라이빗 블록체인을 운영한다. 즉, 자원이 부족해도 운영이 가능한 프라이빗 블록체인을 통해 IoT 기기들의 신원 관리를 수행하고, 운영에 충분한 자원이 필요한 퍼블릭 블록체인을 SDN controller 가 관리한다. 이를 통해 데이터 무결성 보장 등 기존 IoT 시스템의 문제점을 해결할 수 있다.

Novo [8]는 블록체인을 이용해 IoT 시스템에서의 분산 접근 제어 시스템을 제안했다. 이 연구는 기존 IoT 시스템의 보안보다는 확장성 문제에 초점을 맞추고 있다. 하나의 중앙화 된 서버에서 수십억 개의 IoT 기기로의 접근을 모두 관리하게 되면 확장성 문제가 발생한다. 접근 제어 과정이 자주 발생하게 되면 병목현상이 일어나 시스템 전체의 성능을 저하시키게 된다. 이 연구에서는 일반적인 형태의 블록체인을 구성하고 하나의 노드가 관리 허브 (Management Hub)를 통해 하나의 지정된 IoT 기기 그룹과 상호작용하도록 한다. (그림 2) 관리 허브는 IoT 기기들과 블록체인 노드 사이의 인터페이스 역할을 수행한다. 접근 제어와 관련된 규칙은 모두 블록체인에 등록된 하나의 스마트 컨트랙트 내에 정의되어 있다. IoT 기기로부터 접근 제어 쿼리가 발생하게 되면 기기가 속한 그룹의 관리 허브를 통해 연결된 노드로 전달된다. 모든 노드는 블록체인 데이터를 다 저장하고 있기 때문에 스마트 컨트랙트에 쿼리를 보낼 필요없이 노드의 로컬 데이터 확인을 통해 전달받은 쿼리에 응답할 수 있다. 결과적으로 IoT 기기들의 그룹마다 별도의 담당 노드를 둠으로써 시스템의 확장성을 더욱 높일 수 있다.

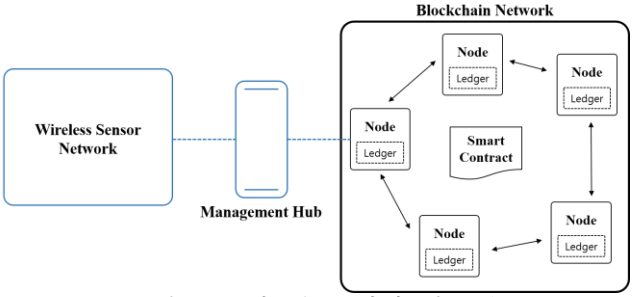

그림 2 분산 접근 제어 시스템

Ⅲ. 결론

본 논문에서는 자원이 제한된 IoT 기기들로 구성된 네트워크에 블록체인을 적용시키기 위해서 진행되고 있는 연구의 동향에 대해 분석하였다. 크게 두 가지 다른 접근법을 정의할 수 있었고, 각각에 해당되는 연구들을 정리해 소개하였다. 첫 번째 방법은 블록체인을 구성하는 요소들의 구조를 변경하거나 새로운 합의 메커니즘을 제안함으로써 블록체인 시스템 자체를 경량화 한다. 따라서 자원이 한정된 IoT 기기들이 직접 블록체인 노드로 네트워크에 참여하는 형태를 갖고 있다. 두 번째 방법은 자원이 충분한 다른 기기들이 블록체인 네트워크의 노드로써 동작하도록 한다. IoT 기기들을 그룹화하여 각 그룹마다 지정된 노드를 통해 블록체인과 상호작용하게 된다.

현재 해당 분야의 연구들은 대부분 기존 IoT 시스템이 client/server paradigm 으로 인해 가지는 보안이나 확장성 문제를 블록체인과의 접목을 통해 해결하기 위해서, IoT 시스템과 블록체인의 효율적인 융합 방법을 찾아내는 것이 목적이다. 블록체인이 가지는 탈중앙성, 데이터 불변성 등의 특징을 해치지 않으면서 자원이 제한된 IoT 기기들로 구성된 시스템에 접목시킬 수 있는 방법을 지속적으로 연구하는 것이 필요해 보인다.

ACKNOWLEDGMENT

본 연구는 2021 년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (2018-0-00749, 인공지능 기반 가상 네트워크 관리기술 개발, IITP-2021-2017-0-01633*, 대학 ICT 연구센터육성지원사업)

참 고 문 헌

[1] ATZORI, Luigi; IERA, Antonio; MORABITO, Giacomo. The internet of things: A survey. Computer networks, 2010, 54.15: 2787-2805.

[2] Zheng, Zibin, et al. "An overview of blockchain technology: Architecture, consensus, and future trends." 2017 IEEE international congress on big data (BigData congress). IEEE, 2017.

[3] GERVAIS, Arthur, et al. On the security and performance of proof of work blockchains. In: Proceedings of the 2016 ACM SIGSAC conference on computer and communications security. 2016. p. 3-16.

[4] KOSHY, Prescilla; BABU, Sarath; MANOJ, B. S. Sliding Window Blockchain Architecture for Internet of Things. IEEE Internet of Things Journal, 2020, 7.4: 3338-3348.

[5] HUANG, Yaodong, et al. Resource allocation and consensus on edge blockchain in pervasive edge computing environments. In: 2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS). IEEE, 2019. p. 1476-1486.

[6] King, Sunny, and Scott Nadal. "Ppcoin: Peer-to-peer crypto-currency with proof-of-stake." self-published paper, August 19 (2012): 1.

[7] YAZDINEJAD, Abbas, et al. An energy-efficient SDN controller architecture for IoT networks with blockchain-based security. IEEE Transactions on Services Computing, 2020.

[8] NOVO, Oscar. Blockchain meets IoT: An architecture for scalable access management in IoT. IEEE Internet of Things Journal, 2018, 5.2: 1184-1195.