영지식 증명 기반 EBaaS(Edge Computing based Blockchain as a Service) 모델 제안

이현희 [1], 오상봉 [1], 김호원 [1]
[1] 부산대학교 정보융합공학과
hyeonhui@islab.re.kr, sangbong@islab.re.kr, howonkim@gmail.com

Proposal of Zero-Knowledge Proof based EBaaS(Edge Computing based Blockchain as a Service) model

Hyeon-Hui Lee[1], Sang-Bong Oh[1], Ho-Won Kim[1]
[1]Dept. of Computer Engineering, Pusan National University

요 약

BaaS(Blockchain as a Service)는 블록체인의 사용이 어렵다는 단점을 유연한 자원운용이 가능하고 뛰어난 접근성의 특징을 가진 클라우드와 접목하여 쉽게 블록체인을 구축하고 사용할 수 있도록 해주는 클라우드 서비스이다. BaaS 의 등장으로 블록체인의 접근성은 큰 범위로 증가하였으며 다양한 도메인에 활용되고 있다. 하지만 클라우드 기반 서비스이기 때문에 클라우드 서비스의 문제점인 보안 이슈가 제기되었다. 본 논문에서는 BaaS 에 ZKP(Zero-Knowledge Proof)와 엣지 컴퓨팅 기술을 활용하여 보안성을 제공할 수 있는 새로운 BaaS 모델인 EBaaS 를 제안한다. EBaaS 는 엣지 컴퓨팅 기술을 적용하여 클라우드 서비스 공급업체에 대한 데이터 종속성을 제거하고 블록체인의 고가용성을 제공할 수 있으며 ZKP 를 활용하여 내부적으로 민감한 데이터에 대한 보안성도 제공할 수 있다.

1. 서론

4 차산업혁명의 핵심 기술로써 빠르게 발전을 거듭하고 있는 블록체인 기술은 불변성, 추적성, 익명성, 투명성의 성질을 가지고 있어 다양한 분야에서 활용되고 있으며, 여러 기업이 블록체인 기술 도입을 고려하고 있다. 한편, 블록체인 기술에 대한 관심이 증가함에 따라 전문적인 지식 없이도 쉽고 간편하게 블록체인 시스템을 구축 및 관리할 수 있는 BaaS(Blockchain as a Service)라는 새로운 서비스도 등장하였는데, BaaS 는 블록체인 시스템의 배치와 관리의 복잡성 및 어려움을 완화하고 개발자가 비즈니스 로직 구현에 집중할 수 있도록 도와주는 클라우드 기반 블록체인 제공 서비스이다. BaaS 의 등장으로 기업은 전보다 편리하게 블록체인 시스템을 도입할 수 있었지만, 블록체인 데이터가 클라우드 서비스 제공업체에 저장되어 서비스 제공업체를 전적으로 신뢰해야 한다는 점과 이에 따라 프라이버시에 위협이 발생할 수 있다는 문제가 남아있었다. 이를 해결하기 위해 엣지 컴퓨팅(Edge Computing) 기술을 적용하여 블록체인 데이터를 on-premise 환경에 저장함으로써 프라이버시 보호를 달성하려는 연구가 진행되었다. [1] 하지만, 엣지 컴퓨팅 기술을 이용한 BaaS 서비스는 외부자에 대한 프라이버시 보호 목적은 달성하였지만, 내부의 악의적인 사용자에 대한 보안에는 취약하다는 문제가 존재하였다. 본 논문에서는 기존의 클라우드 기반 BaaS 시스템에 엣지 컴퓨팅 기술을 적용하여 블록체인 데이터를 on-premise 환경에 저장하고, 영지식증명(Zero Knowledge Proof)을 이용하여 저장된 블록체인 데이터에 대한 보안을 향상하는 새로운 모델인 EBaaS 를 제안한다. 제안하는 모델은 엣지 컴퓨팅 기술을 통해 외부자에 대한 프라이버시 보호 목적을 달성하고, 영지식 증명을 통해 내부의 악의적인 사용자에 대한 데이터 보호 목적 또한 달성한다. 본 연구를 통해 향후 블록체인 도입을 고려하는 기업은 프라이버시 침해에 대한 우려 없이 쉽고 편리하게 블록체인 시스템을 구축 및 관리할 수 있을 것으로 기대한다.

2. 배경지식

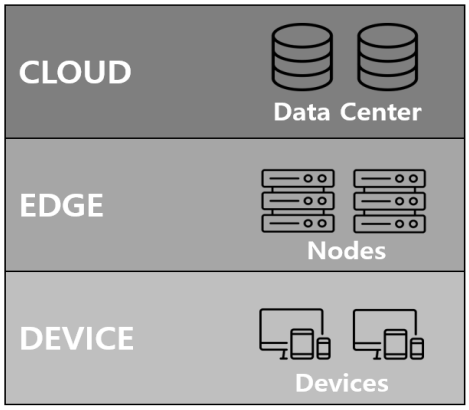
2.1 BaaS

BaaS(Blockchain as a Service)는 블록체인 프레임워크를 클라우드 컴퓨팅 플랫폼에 내장함으로써 클라우드 서비스 인프라의 배치 및 관리 이점을 활용하여 개발자에게 편리하게 고성능 블록체인 생태계 및 관련 서비스를 제공하는 것을 의미한다. 개발자들은 이

러한 기본 클라우드 서비스를 통해 블록체인 네트워크를 빠르게 구축하여 기본 아키텍처의 복잡성을 무시하고 애플리케이션을 지원할 수 있다. [2] 현재까지 IBM, 마이크로소프트, 아마존과 같은 많은 글로벌 기업들이 BaaS 플랫폼을 출시했고 좋은 결과를 얻었다. 하지만 앞서 설명한 것과 같이 기존의 BaaS 플랫폼들은 클라우드 서비스 제공업체에 블록체인 데이터가 저장되는 형태이기 때문에 프라이버시 보호 측면에서 해결해야 할 부분이 남아 있다.

2.2 엣지 컴퓨팅

엣지 컴퓨팅(Edge Computing)이란 네트워크의 가장자리에서 클라우드 서비스를 대신하여 다운스트림 데이터를, IoT 서비스를 대신하여 업스트림 데이터를 계산할 수 있도록 하는 기술을 의미한다. 엣지는 데이터 소스와 클라우드 데이터 센터 사이에서 컴퓨팅을 처리하는 위치를 의미하는데, 예를 들어 스마트폰은 신체와 클라우드 사이의 엣지, 스마트 홈의 게이트웨이는 가정과 클라우드 사이의 엣지라고 할 수 있다. [3]

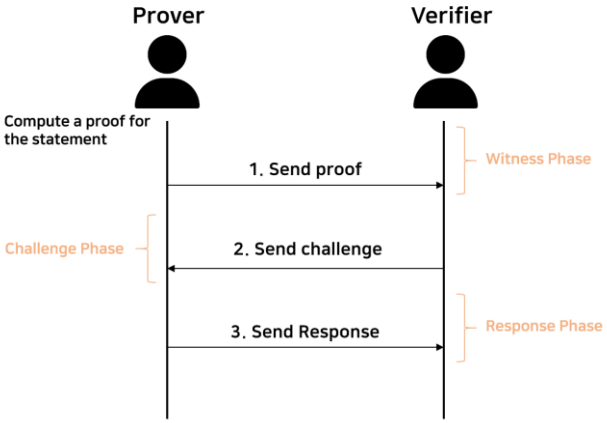


(그림 1) 엣지 컴퓨팅 구조

(그림 1)은 엣지 컴퓨팅의 구조를 나타낸 그림이다. 클라우드에 데이터센터가 있고, 실제 데이터 처리 및 분석, 컴퓨팅은 엣지 노드에서 수행된다. 즉, 엣지 컴퓨팅은 데이터 처리가 데이터 소스 근처에서 이루어지기 때문에 클라우드 컴퓨팅 방식에 비해 지연시간이 적고, 실행 시간 및 응답시간이 빠르다는 장점이 있다.

2.3 영지식 증명

영지식 증명(Zero Knowledge Proof)은 증명자 P 와 검증자 V 사이의 대화형 프로토콜이다. 영지식 증명의 동작 방식은 다음과 같다. 증명자 P 와 검증자 V 에게 계산 문제 x 가 있고, x 의 해답 w 는 P 만 알고 있을 때, 영지식 증명은 P 가 V 에게 자신이 문제 x 에 대한 해답 w 를 알고 있다는 사실을 w 와 관련된 어떠한 정보도 제공하지 않고 증명할 수 있게 한다. 즉, 자신이 알고 있는 정보를 공개하지 않으면서, 그 정보를 알고 있다는 사실을 증명할 수 있는 시스템이다.



(그림 2) 영지식 증명 프로토콜

(그림 2]은 영지식 증명 프로토콜의 동작 방식을 나타낸 그림이다. 영지식 증명은 아래의 3 가지 특성을 반드시 만족하여야 한다. [4]

1. Completeness: P 가 w 를 알고 있을 때, V 는 P 에 의해 이 사실을 납득할 수 있어야 한다.
2. Soundness: P 가 w 를 알지 못할 때, P 는 V 에게 w 를 알고 있다는 사실을 결코 증명할 수 없다.
3. Zero-knowledge: 검증 과정에서 V 는 w 에 대한 어떠한 추가 정보도 알 수 없다.

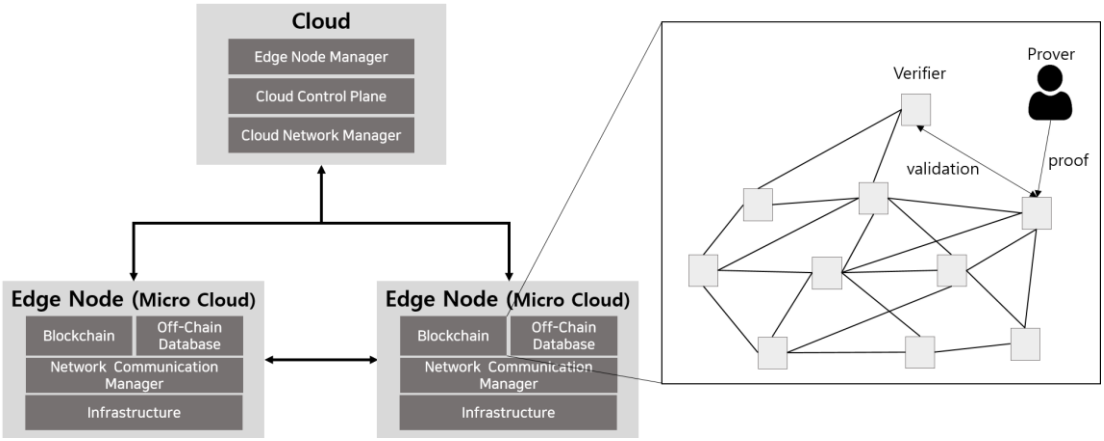
3. 이전 사례 및 연구

3.1 RBaaS

[1] 에서는 기존의 클라우드 기반 BaaS 플랫폼의 프라이버시 침해 문제를 해결하기 위해 엣지 컴퓨팅 환경까지 확장한 RBaaS 모델을 제안하였다. 해당 연구에서 제안한 모델은 클라우드와 Tunnel 로 연결된 각각의 EdgeZone 에 블록체인 데이터가 저장되고, 클라우드는 EdgeZone 을 관리하는 역할을 수행한다. 이렇게 함으로써 기존의 클라우드 서비스 제공업체에 저장되던 블록체인 데이터를 localize 하여 외부의 제 3 자로부터 민감한 정보를 보호하였다. 하지만, on-premise 환경에 구축된 EdgeZone 에 저장된 블록체인 데이터는 내부의 사용자가 블록 안의 내용을 확인할 수 있었다. 이는, 블록 안에 기업의 민감한 정보가 저장되어 있다면 문제가 될 소지가 있다.

3.2 Kaleido

BaaS 플랫폼을 운영하고 있는 글로벌 기업인 Kaleido 는 앞서 3.1 절의 RBaaS 에서 발생하는 내부적 프라이버시 침해 문제를 클라우드에 저장되는 블록체인에 영지식 증명 기술을 적용하여 해결하고자 하였다.



(그림 3) EBaaS 아키텍처

하지만, 여전히 데이터는 서비스 제공업체에 저장되기 때문에 기존 BaaS 의 문제점인 공급업체에 대한 데이터 종속성 문제가 발생한다. 이러한 문제점으로 인해 Kaleido 역시 서비스 제공업체에 대한 신뢰성 문제가 존재한다.

본 논문에서는 인용된 각 선행연구의 문제점을 해소할 수 있도록 연구된 새로운 BaaS 의 모델을 제안한다. 본 연구는 각 블록체인상에서 민감정보가 사용되어야 할 때 BaaS 서비스 제공업체에 대한 데이터의 종속성을 없애고 내부적으로 데이터의 보호가 가능하도록 설계되었다. 제안하는 BaaS 의 모델에 대해서는 4 장에서 후술한다.

4. 제안모델

본 논문에서는 기존의 클라우드 기반 BaaS 플랫폼의 프라이버시 보호 이슈를 해결하기 위해 엣지컴퓨팅 기술과 영지식 증명 기술을 접목시킨 새로운 모델을 제안한다. 제안하는 모델은 향후 블록체인 도입을 고려하는 기업 또는 사회가 빠르고 편리하게 블록체인 시스템을 구축할 수 있을 뿐 아니라 데이터 보호 차원에서도 전보다 높은 보안 수준을 통해 민감한 정보를 보다 안전하게 보관 및 관리할 수 있을 것으로 기대한다.

4.1 아키텍처

[그림 3]은 EBaaS 의 구조를 나타낸 그림이다. 최상단에 클라우드가 위치하고, 클라우드에 엣지 노드가 연결된 형태이다. 클라우드는 연결된 엣지 노드를 관리하는 Edge Node Manager, 클라우드 환경 전반에 걸쳐 관리 및 조정을 제공하는 Cloud Control Plane, 네트워크를 관리하는 Cloud Network Manager 로 구성되며, 엣지노드는 Infrastructure 와 블록체인 및 오프체인 데이터베이스, 네트워크 연결을 담당하는 Network Communication Manager 로 구성된다. 엣지노드에 블록체인이 구축되기 때문에 블록체인 데이터는 클라우드가 아닌 엣지노드에 저장되며, 블록체인에는 영지식 증명 기술이 적용되었다.

4.2 동작 시나리오

제안하는 모델의 동작 시나리오를 외부/내부 주체에 대한 프라이버시 보호 관점에서 설명하면 다음과 같다. 먼저, 구축된 클라우드에 여러 엣지 노드들이 연결되어 있다. 이때, 연결된 엣지 노드는 클라우드의 Edge Node Manager 가 관리한다. 각각의 엣지 노드에는 블록체인 및 오프체인 데이터베이스가 존재하며, 각 노드 간 통신은 Network Communication Manager 가 담당한다. 이러한 구조에서 블록체인 데이터는 클라우드가 아닌 on-premise 환경에 구축된 엣지 노드에 저장되기 때문에 사용자는 클라우드 서비스 제공업체(외부 주체)를 신뢰하지 않아도 민감한 데이터를 보호할 수 있다. 다음은 내부 주체에 대한 프라이버시 보호 관점이다. 엣지 노드에 구축된 블록체인에 영지식 증명 기술이 적용되어 검증자가 블록 안의 데이터를 모른 채 검증이 가능하다. 이러한 구조를 통해 on-premise 환경이지만 내부 주체에 대한 보안에는 취약하던 기존의 문제를 해결할 수 있다.

5. 결론

본 논문에서는 클라우드의 서비스형 블록체인(BaaS)의 기반인 클라우드와 블록체인의 보안 측면 결점인 데이터 종속성과 민감한 정보에 대한 보안을 해결해줄 수 있는 새로운 형태의 서비스형 블록체인 모델 EBaaS 를 제시하였다. 현재 BaaS 의 시장 규모는 2019 년 19 억달러에서 2027 년까지 약 249 억 4,000 만 달러까지 성장할 것으로 예측되고, 이는 39.5%에 달하는 성장률이다[5]. 하지만 현재 BaaS 의 적절한 보안 측면 대안은 제시되지 않고 있다. BaaS 의 보안과 함께 균형 있는 기술적 성장이 이루어지지 않는 경우 올바른 성장이라고 볼 수 없다. 이와 관하여 BaaS 의 보안에 대한 선행 연구의 경우 클라우드에 대한 보안적 관점을 제시한 경우 내부 데이터 보안에 대한 결점이 존재하고 영지식 증명을 활용한 연구 또한 데이터의 종속성이 존재하여 외부적으로 보안적 위험이

존재하였다. EBaaS 는 BaaS 의 가장 큰 문제점으로 대두되고 있던 클라우드의 데이터 종속성 문제를 엣지 컴퓨팅 기술을 활용하여 해소하고, 블록체인 내부에 영지식 증명 기술을 접목하여 내부의 민감한 정보에 대한 보안성도 향상하고자 하였다. 본 연구를 통해 성장하는 BaaS 시장에서 고객의 프라이버시 침해에 대한 불안감을 해소할 수 있으며, 블록체인 기술에 있어 BaaS 의 더욱 큰 성장을 할 수 있는 바람을 불어올 것으로 기대한다.

본 연구는 국토교통부/과학기술정보통신부/국토교통과학기술진흥원의 스마트시티 혁신성장동력 프로젝트 지원으로 수행되었음(과제번호 18NSPS-B149388-01).

참고문헌

[1] Cai, Zhenggong, et al. "RBaaS: A Robust Blockchain as a Service Paradigm in Cloud-Edge Collaborative Environment." IEEE Access (2022).

[2] Zheng, Weilin, et al. "Nutbaas: A blockchain-as-a-service platform." Ieee Access 7 (2019): 134422-134433.

[3] Shi, Weisong, et al. "Edge computing: Vision and challenges." IEEE internet of things journal 3.5 (2016): 637-646.

[4] Ruangwises, Suthee, and Toshiya Itoh. "Physical zero-knowledge proof for ripple effect." Theoretical Computer Science 895 (2021): 115-123.

[5] “Blockchain-as-a-Service(BaaS) Market Size, Share & Industry Analysis By Component, By Application, By Industry, and Regional Forecast, 2020-2027”,Fortune Business Insight (2019)