허가형 블록체인을 위한 보안 컨테이너 활용 방안 연구

강윤경, 노태윤, 이준석, 최원미, 유연호, 양경식, 유혁
고려대학교 정보대학 컴퓨터학과

ykkang@os.korea.ac.kr, nrbsld@korea.ac.kr, {jslee,ymcui,yhyoo}@os.korea.ac.kr,
g_yang@korea.ac.kr, chuckyoo@os.korea.ac.kr

Exploring the Secure Container for Permissioned Blockchains

Yunkyung Kang, Taeyun Roh, Junseok Lee, Wonmi Choi, Yeonho Yoo,
Gyeongsik Yang, Chuck Yoo
Department of Computer Science and Engineering, Korea University

요 약

허가형 블록체인은 허가된 특정 참여자만이 접근할 수 있도록 설계된 블록체인으로 의료, 금융 서비스 등 데이터의 무결성, 보안성이 중요한 비즈니스에서 널리 사용되고 있다. 허가형 블록체인은 참여자들의 신원을 서로 확인하고 요청받은 거래를 스마트 컨트랙트를 통해 검증함으로써 블록체인의 무결성을 보장한다. 대표적인 허가형 블록체인 플랫폼인 하이퍼레저 패브릭은 참여하는 노드들의 독립성을 보장하기 위해 각 노드들이 독립된 환경에서 스마트 컨트랙트를 실행하게 한다. 특히, 최신 하이퍼레저 패브릭에서는 빠른 배포와 높은 블록체인 성능을 보장하기 위해 각 노드를 도커 컨테이너로 배포한다. 그러나 도커 컨테이너 사용은 완전한 격리를 제공하지 못하는 한계가 있다. 본 논문에서는 블록체인 노드를 경량성과 격리성 모두 제공하는 보안 컨테이너로 사용하는 방안을 제안한다.

Ⅰ. 서 론

허가형 블록체인은 허용된 특정 참여자들만 블록체인 네트워크에 참여하거나 스마트 컨트랙트를 검증할 수 있는 블록체인이다. 허가형 블록체인에서는 참여자들의 신원을 확인하고 승인하는 과정을 통해 블록체인의 무결성을 보장한다. 또한, 데이터에 대한 접근을 제어하여 민감한 정보를 안전하게 관리할 수 있다.[1] 허가형 블록체인을 사용함으로써 데이터 관리에 있어 높은 무결성과 보안성을 기대할 수 있기 때문에 허가형 블록체인은 주로 의료 서비스, 금융 서비스, 공급망 관리 등의 비즈니스 환경에서 주로 활용된다.[2]

아마존, IBM 등의 클라우드 기업에서도 허가형 블록체인을 통해 블록체인 서비스를 제공하고 있으며, 허가형 블록체인 네트워크를 구축하기 위해 하이퍼레저 패브릭을 사용한다.[3] 하이퍼레저 패브릭에서는 블록체인 네트워크에 참여하는 피어 노드들이 클라이언트로부터 받은 트랜잭션을 처리하기 위해 체인코드(스마트 컨트랙트)를 각각 독립적으로 실행하게 한다.

각 피어 노드는 독립적으로 트랜잭션을 실행하고 검증한 이후 실행 결과는 오더러 노드에 전송된다. 오더러 노드는 여러 트랜잭션을 순서대로 정렬하여 블록을 생성하고, 이 블록을 네트워크의 모든 피어 노드에게 배포한다. 피어 노드들은 전달받은 블록에 대해서 검증한 후 자신의 원장에 추가하여 트랜잭션을 기록한다. 이 과정을 통해 트랜잭션에 대한 처리의 무결성을 보장할 수 있다. 하이퍼레저 패브릭에서는 참여하는 모든 피어 노드들이 체인코드를 격리된 환경에서 실행하도록 보장하기 위해 각 노드를 가상머신으로 배포한다. 특히 하이퍼레저 패브릭 버전 2.0 에서는 도커 컨테이너를 런타임으로 활용하여, 각 노드의 독립성을 제공한다.

그러나, 단순히 네이티브 도커 컨테이너를 사용하는 것으로 완전히 격리된 환경을 제공하는데 한계가 존재한다. 도커 컨테이너는 기존 가상머신 환경과 다르게 호스트 운영체제의 커널을 공유하기 때문에 자원 효율성이 높고 배포하는데 걸리는 시간이 짧지만, 호스트 운영체제가 보안 공격을 받거나, 컨테이너가 공격을 받을 경우 다른 컨테이너들도 영향을 받을 수 있다. 특히 허가형 블록체인이 대부분 자원이 공유되는 클라우드 환경에서 배포 및 구동됨을 고려할 때, CPU, 네트워크, 메모리를 비롯한 격리성과 경량성을 확보하는 것은 매우 중요하다.[4] 따라서 본 논문에서는 가상머신의 격리성과 컨테이너의 경량성 모두를 고려하여 설계된 보안 컨테이너를 블록체인 네트워크의 노드에 런타임으로 활용한다.

본 논문에서는 네이티브 도커 컨테이너의 구조적 특성으로 인한 보안적 문제를 지적하며, 이를 대체할 수 있는 보안 컨테이너 사용을 제안한다. 본 논문에서는 여러 보안 컨테이너 중 Kata 컨테이너를 기반하며, 기존 컨테이너와 비교하여 블록체인 노드들을 동작시키는데 적합한지 분석한다.

Ⅱ. 배경지식: 하이퍼레저 패브릭의 구성 요소

하이퍼레저 패브릭을 통해 생성되는 블록체인 네트워크는 채널과 피어 노드 및 오더러 노드 두 종류의 노드로 구성된다. 그림 1 은 3 개의 노드와 하나의 채널로 이루어진 블록체인 네트워크의 예시이다. 3 개의 노드 중 2 개는 피어 노드이며, 1 개는 오더러 노드이다. 먼저, 피어 노드는 사용자가 전달한 트랜잭션을 체인코드를 실행하여 검증한다. 검증된 트랜잭션의

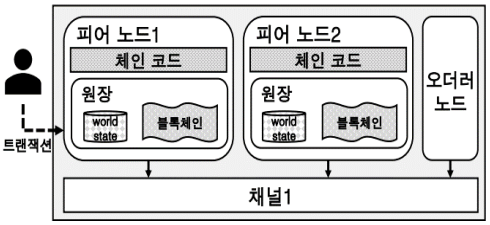

그림1. 허가형 블록체인 네트워크 예시

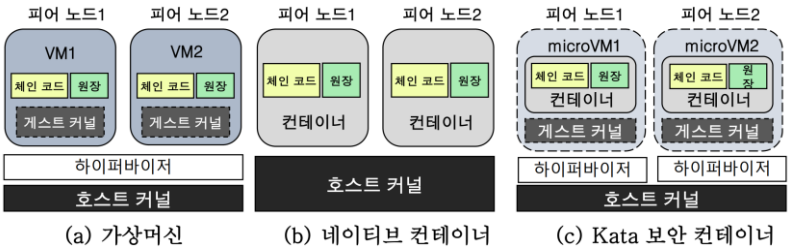

그림 2. 가상머신, 네이티브 컨테이너, Kata 컨테이너 구조 비교

결과는 이후 오더러 노드를 통해 재정렬되어 블록 단위로 모든 피어 노드의 원장에 기록된다. 두번째로, 오더러 노드는 일련의 트랜잭션들을 블록화하고 정렬하여 모든 피어 노드의 원장에 블록이 동일한 순서로 저장되도록 한다.

하이퍼레저 패브릭은 트랜잭션의 무결성 및 보안성을 보장하기 위해 각 노드들이 독립된 가상머신으로 배포된다. 하이퍼레저 패브릭 버전 1.0 에서는 기본적으로 도커 컨테이너 런타임을 사용한다. 다음 장부터는 허가형 블록체인의 노드들을 생성할 때 네이티브 컨테이너와 보안 컨테이너를 보안적 관점으로 비교한다.

Ⅲ. 네이티브 컨테이너와 보안 컨테이너의 구조 비교

하이퍼레저 패브릭에서는 각 노드에서 스마트 컨트랙트를 격리된 환경에서 실행하기 위해 네이티브 도커 컨테이너를 사용한다. 기존 가상머신(그림 a)과 다르게 네이티브 컨테이너(그림 2b)는 호스트 운영체제의 커널을 공유하며, 필요한 라이브러리와 응용 프로그램만 포함하기 때문에 가상머신보다 가볍고 배포가 용이하다. 그러나, 네이티브 컨테이너를 사용하면 하이퍼바이저를 통해 완전히 독립된 운영체제를 갖는 가상머신 환경과 달리, 컨테이너들이 호스트 머신과 커널을 공유하기 때문에 격리 수준은 비교적 낮다.

대표적인 보안 컨테이너인 Kata 컨테이너(그림 2c)는 하나의 호스트 커널에서 여러 개의 하이퍼바이저를 통하여 각각의 microVM 을 실행한다. Kata 컨테이너는 1)하이퍼바이저, 2) microVM, 3) 호스트 머신 사이의 통신을 최적화하여 부팅 시간과 메모리 사용량을 줄임으로써 경량화 된 가상머신을 생성할 수 있다. 이러한 이중 보안구조를 통하여 체인코드 실행 등의 보안 및 격리 수준을 향상시킬 수 있다.

Ⅳ. 네이티브 컨테이너와 보안 컨테이너의 구조 비교

네이티브 컨테이너는 하나의 운영체제 커널을 공유하기 때문에, 격리 수준이 낮아 호스트 머신이 악의적인 공격에 노출될 경우 모든 컨테이너 보안이 위협받을 수 있다는 단점이 존재한다. 예를 들어 커널의 공유 메모리 관리 취약점을 이용한 공격(CVE-2017-5123)과 시스템콜의 부적절한 사용자 입력 처리를 통한 공격(CVE-2016-5195)[5]이 발생한 경우, 공유된 호스트 커널을 통해 모든 컨테이너가 영향을 받아 전체 시스템의 안정성이 저하될 수 있다.

반면, Kata 컨테이너는 독립적인 운영체제 커널을 사용하는 microVM 속에 컨테이너를 배치하는 이중 구조이기 때문에 동일한 공격에 노출되더라도 공격받은 가상머신에만 영향을 미치기 때문에 네이티브 컨테이너에 비해 높은 수준의 보안성을 제공한다. 따라서, 호스트가 공격을 받거나 하나의 컨테이너가 취약점에 노출되더라도 다른 컨테이너나 호스트 시스템에 미치는 영향을 최소화할 수 있다. 하이퍼레저 패브릭에서는 참여하는 모든 노드들이 데이터를 검증하기 때문에 하나의 노드가 공격받더라도 데이터를 보존할 수 있다.

Ⅴ. 결론 및 향후 연구

본 논문에서는 하이퍼레저 패브릭에서 블록체인 노드들을 배포할 때 기존 가상머신 구조와 컨테이너 구조의 장점들을 결합한 보안 컨테이너를 고려한다. 보안 컨테이너는 네이티브 컨테이너 수준의 경량화를 제공하는 동시에, 가상머신 수준의 보안 및 격리를 제공하기 때문에 블록체인의 무결성을 보존하는데 매우 효과적이다. 그러나, Kata 컨테이너의 보안 구조는 보안적 이점을 주지만, 트랜잭션을 처리하는데 성능 상의 손실을 발생시킬 수 있기 때문이다. 향후 연구로 하이퍼레저 패브릭에서 보안 컨테이너의 보안성과 성능 간의 상충관계를 실험을 통해 분석하고자 한다.

ACKNOWLEDGMENT

이 논문은 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업(NRF-2021R1A6A1A13044830), 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원(NRF-2023R1A2C3004145, RS-2024-00336564), 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 ICT 명품인재양성사업(IITP-2024-2020-0-01819)의 지원을 받아 수행된 연구임. 교신저자: 양경식, 유혁.

참 고 문 헌

[1] Gyeongsik Yang et al., Resource analysis of blockchain consensus algorithms in HyperLedger Fabric, IEEE Access, vol. 10, pp 74902-74920, 2022

[2] Rebecca Yang et al., Public and private blockchain in construction business process and information integration, Automation in Construction, Volume 118, 2020

[3] Elli Androulaki et al., Hyperledger Fabric: a distributed operating system for permissioned blockchains, Proceedings of the Thirteenth EuroSys Conference, 30, pp. 1- 15, 2018

[4] Yoo, Yeonho, et al. "Control Channel Isolation in SDN Virtualization: A Machine Learning Approach." 2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing (CCGrid). IEEE, 2023.

[5] S. Sultan et al., Container Security: Issues, Challenges, and the Road Ahead, IEEE Access, vol. 7, pp. 52976-52996, 2019