

# 하이브리드 블록체인의 트랜잭션 추적성 제공 지원을 위한 아키텍처

강동원<sup>10</sup>, 정수민<sup>2</sup>, 박준석<sup>3</sup>, 염근혁<sup>4\*</sup>교신저자

<sup>1</sup>부산대학교 정보컴퓨터공학부 학부생

<sup>2</sup>부산대학교 정보융합공학과 박사과정

<sup>3</sup>부산대학교 지능물류빅데이터연구소 연구교수

<sup>4</sup>부산대학교 정보컴퓨터공학부 교수

{okcdbu, sumin2708, pjs50, yeom}@pusan.ac.kr

## Architecture to Support Hybrid Blockchain Transaction Traceability

Deungwon Kang<sup>10</sup>, Sumin Jeong<sup>2</sup>, Joonseok Park<sup>3</sup>, Keunhyuk Yeom<sup>1\*</sup>

<sup>1</sup>School of Computer Science and Engineering, Pusan National University

<sup>2</sup>Dept. of Information Convergence Engineering, Pusan National University

<sup>3</sup>Research Institute of Intelligent Logistics Big Data, Pusan National University

### 요 약

하이브리드 블록체인은 퍼블릭, 프라이빗 각 플랫폼의 특성을 활용한 비즈니스 거래를 지원할 수 있는 블록체인 기술이다. 현재 하이브리드 블록체인은 트랜잭션 데이터의 특징에 기반하여 운영을 지원하는 방법이 부족하여 원활한 비즈니스 거래 지원을 수행하기 어렵다. 따라서, 본 논문에서는 비즈니스 거래를 지원하는 방안을 하이브리드 블록체인 트랜잭션 추적 지원 아키텍처를 통해 제시한다. 제안하는 방법은 사례 시스템을 구성하여 아키텍처의 적용 가능성을 보이고 시각화 결과를 나타내었다. 또한 트랜잭션 추적 시 평균 0.599초의 실행 시간이 소요됨을 실험을 통해 확인하였다. 본 논문에서 제시하는 아키텍처는 하이브리드 블록체인 운영의 기반으로 적용할 수 있을 것으로 기대된다.

### 1. 서론

하이브리드 블록체인[1]은 퍼블릭 블록체인과 프라이빗 블록체인이 결합된 형태의 블록체인을 말한다. 하이브리드 블록체인 기술은 프라이빗 블록체인을 통해 신뢰 가능한 사용자 간의 거래를 지원하고 퍼블릭 블록체인의 공개 네트워크를 통한 유연한 거래 환경을 제공한다는 점에서 B2B(Business to Business)와 같이 신뢰성과 유연성이 필요한 경우 활용하는 기술이다.

하이브리드 블록체인 환경의 비즈니스 거래는 각 블록체인 플랫폼의 특성에 따라 개별 흐름으로 수행되어 저장되므로 이를 직관적으로 분석하고 흐름을 쉽게 파악하기는 어렵다. 블록체인에서 발생하는 거래 데이터는 비즈니스 거래를 새로 수행하기 위한 분석 데이터 및 스마트 컨트랙트(Smart Contract)를 생성하기 위한 기반 자원으로도 활용될 수 있다. 현재 개별적인 블록체인 플랫폼에서 거래를 추적하는 메커니즘은 일부 존재하고 있으나, 하이브리드 블록체인에서 발생하는 비즈니스 거래를 추적하는 연구는 부족한 실정이다.

따라서, 본 논문에서는 대표적인 퍼블릭 블록체인인 이더리움과 프라이빗 블록체인인 하이퍼레저 패브릭을 결합한 하이브리드 블록체인의 운영 시 트랜잭션 추적을 지원하는 아키텍처를 제시한다.

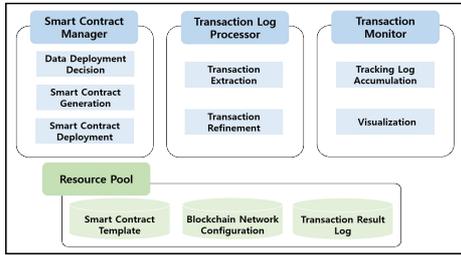
### 2. 관련 연구

이더스캔(Etherscan)[2]은 이더리움(Ethereum) 블록체인 플랫폼의 거래를 추적하는 기술이다. 강명조 등[3]은 BaaS(Blockchain as a Service)를 전자 투표로 제시할 수 있는 하이브리드 블록체인 연계방법을 제시하였다. 반면, 본 논문은 이더스캔이 보장하는 퍼블릭 블록체인의 추적성을 프라이빗 블록체인과 연계하는 기술을 제시한다. 또한, BaaS등의 블록체인 활용 시스템을 지원할 수 있는 하이브리드 블록체인 분석기술을 제공한다는 점에 차이가 있다.

### 3. 트랜잭션 추적 지원 아키텍처

#### 3.1 지원 아키텍처

(그림 1)은 본 논문에서 제안하는 트랜잭션 추적 분석 방법을 제공하는 아키텍처를 나타낸 것이다.



(그림 1) 트랜잭션 추적 지원 아키텍처

(그림 1)에서 제안하는 아키텍처는 스마트 컨트랙트 매니저(Smart Contract Manager), 트랜잭션 로그 처리기(Transaction Log Processor), 트랜잭션 모니터(Transaction Monitor)로 구분된다.

스마트 컨트랙트 매니저는 하이브리드 블록체인에서 동작을 수행하는 스마트 컨트랙트의 설계, 생성, 수정을 수행하는 것이다.

트랜잭션 로그 처리기는 하이브리드 블록체인에서 발생한 트랜잭션을 추적할 수 있게 데이터를 가공하는 것이다.

트랜잭션 모니터는 정제된 트랜잭션 정보를 축적하여 추적성을 부여하고 운영 기반이 되는 자료를 제공하는 기능이다.

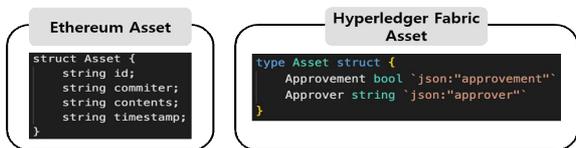
### 3.2 사례 시스템 구축 및 성능 실험

본 논문에서는 이더리움 플랫폼과 하이퍼레저 패브릭 플랫폼을 활용하여 (그림 1)의 아키텍처를 반영하는 <표 1>의 사례 시스템을 구축하였다.

<표 1> 사례 시스템 환경

사례 환경	구성요소	
블록체인 종류	퍼블릭	허가형
플랫폼	Ethereum	Hyperledger Fabric
네트워크	ganache	test-network
스마트 컨트랙트 언어	Solidity 0.8.21	Golang 1.21.1
스마트 컨트랙트 매니저	Python 3.10	Python 3.10
트랜잭션 로그 처리기	web3	Filebeat, LogStash
트랜잭션 모니터	python, json	ElasticSearch, Kibana

(그림 2)는 각 플랫폼이 대표하는 네트워크 환경의 주요 트랜잭션 추적 요소(데이터)를 구분한 것이다.



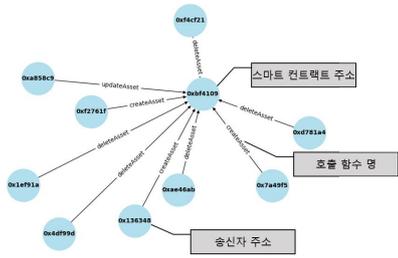
(그림 2) 트랜잭션 추적 요소(데이터)

(그림 2)의 트랜잭션 추적 요소에서 이더리움 자원(Ethereum Asset)은 퍼블릭 블록체인의 거래 수행 관련 운영 요소를 나타낸다(거래 수행 시간, 거래자, 거래 내역 등). 또한, 하이퍼레저 패브릭 자원(Hyperledger Fabric Asset)에서는 계약 승인 관련 요소

를 나타낸다(거래 승인자, 거래 승인 여부 등).

(그림 3)은 퍼블릭 블록체인 이더리움에서 트랜잭션 추적 내역을 그래프 형태로 표현한 것이다.

Ethereum Transaction Network Graph



(그림 3) 이더리움 자원 추적 그래프

<표 2> 트랜잭션 추적 및 시각화 시간

회차(회)	1	2	3	4	5	평균
시간(s)	0.688	0.563	0.575	0.574	0.595	0.599

(그림 3)을 통해 하이브리드 블록체인의 트랜잭션 추적 결과와 <표 2>의 결과를 통해 소요 시간을 평가하였다. <표 2>의 실험에서 시각화 과정은 평균 0.599초가 소요되었다. 기존 퍼블릭 블록체인 트랜잭션 추적 방법인 이더스캔 API를 활용하는 경우 추적을 위한 비용이 발생하는 반면, 본 방법은 비용 부담이 없다는 장점이 있다.

### 5. 결론

본 논문에서는 하이브리드 블록체인 환경에서 트랜잭션의 추적 및 분석 지원 아키텍처를 제시하였다. 제시한 아키텍처는 사례 시스템으로 구축하여 방법의 적용가능성을 확보하였다. 제안하는 방법은 하이브리드 블록체인의 비즈니스 프로세스 운영에 적용 가능할 것으로 기대된다.

### 사사

본 연구는 과학기술정보통신부 및 정보통신기획평가원의 대학ICT연구센터육성지원사업의 연구결과로 수행되었음 (IITP-2024-2020-0-01797)

### 참고문헌

[1] H. W. Marar and R. W. Marar, "Hybrid Block chain," Jordanian Journal of Computers and Information Technology (JJCIT), Vol. 6, No. 4, pp. 317-325, 2020.  
 [2] Etherscan, <https://docs.etherscan.io/>  
 [3] 강명조, 김미희, "BaaS를 이용한 하이브리드 블록체인 기반 전자투표 시스템," 정보처리학회논문지, Vol. 12, No. 8, pp. 253-262, 2023.