블록체인 기반 조작불가능한 확률제어 시스템

김명길[O], 권민호[*], 김진혁[*]
[O]부산대학교 정보융학공학과,
[*](주)스마트엠투엠 기업부설연구소
e-mail: clevermk7211@gmail.com[O], jinhyeok@smartm2m.co.kr[*], alsgh458@smartm2m.co.kr[*]

Blockchain-based non-manipulable probability control system

Myeongkil Kim[O], Minho Kwon[*], Jinhyeok Kim[*]
[O]Dept. of Information Convergence Engineering, Pusan University,
[*]Corporate R&D Center, SmartM2M

● 요 약 ●

본 논문에서는 블록체인 기반의 투명성/신뢰성을 제공하는 조작 불가능한 확률 제어 시스템을 제안한다. 해당 시스템은 클라이언트에 의해 질의 된 확률값을 블록체인상에서 산출해냄으로써, Legacy 시스템 아키텍처의 한계인 조작 가능성을 원천적으로 배제할 수 있다. 이는 블록체인 참여 노드 간의 데이터를 동일하게 공유하여 투명성을 확보하고, 이를 기반으로 데이터에 대한 신뢰성을 확보한 확률 제공 기능이다. 특히 해당 시스템은 Private/Permissioned 구조 기반의 블록체인 네트워크를 기반으로 운영 노드에 의해서 유지/관리되어 별도의 트랜잭션 수수료가 블록체인상에서 발생하지 않는다. 또한 Public Blockchain 메인 네트워크상의 미래 블록에 대한 정보를 확률값 산출 Seed에 활용함으로써, Non-deterministic 한 환경을 제공한다. 이는 클라이언트가 확률 질의에 대한 검증 과정을 직접 수행하거나 Third-party 검증을 통해 확률값에 대한 조작 여부를 확인할 수 있다.

키워드: 블록체인(blockchain), 비결정론(non-deterministic), 투명성(Transparency), 신뢰성(Reliability)

I. Introduction

Server-Client 구조에서 확률 서비스를 제공하고자 하는 경우, BFT(Byzantine Fault Tolerance) 환경의 특성상 서버에서 확률값을 계산하고 제공할 수밖에 없다. 하지만 서버를 운영하는 조직이 임의로 확률을 조작한다면 운영 조직 외 누구도 조작 여부를 확인하거나 확률값을 검증해낼 수 없다는 단점이 존재한다. 특히 최근 여러 회사의 확률 조작 사례들이 빈번히 발생하면서 관련한 법률 또한 제정되고 있다[1,2]. 하지만 서버의 운영 조직에 대한 별도의 감사 과정이 요구될 수밖에 없어 비효율적이라는 단점이 존재하여 이를 해소하기 위한 수단이 필요하다.

본 논문에서 제안한 블록체인 기반 확률제어 시스템은 투명성과 신뢰성을 기반으로 별도의 감사기관 없이 시스템 레벨에서 신뢰할 수 있는 확률을 제공할 수 있을 뿐 아니라, 스마트 컨트랙트를 통해 누구나 확률 검증 및 조작 여부를 확인할 수 있다.

II. Preliminaries

1. Related works

1.1 국내 동향

확률 기반 서비스 신뢰성에 대한 사회적 요구가 점차 증가함에 따라, 게임 내에서 확률형 아이템을 생성하는 루트 박스에 대한 문제점 분석 같은 시사점을 도출하는 연구는 활발히 진행되고 있지만, 확률 시스템 내에서 서비스 사용자가 신뢰할 수 있는 확률 도출에 대한 근본적인 해결책을 제시하는 연구는 활발히 이루어지고 있지 않은 실정이다[3,4].

III. The Proposed Scheme

1. System architecture

본 논문에서 제안하는 시스템은 아래 그림 1과 같이 메인 블록체인을 기반으로 하며, 해당 블록체인상에서 확률 도출 및 검증을 수행하는

스마트 컨트랙트와, 이를 이용하는 DApp으로 구성된다.

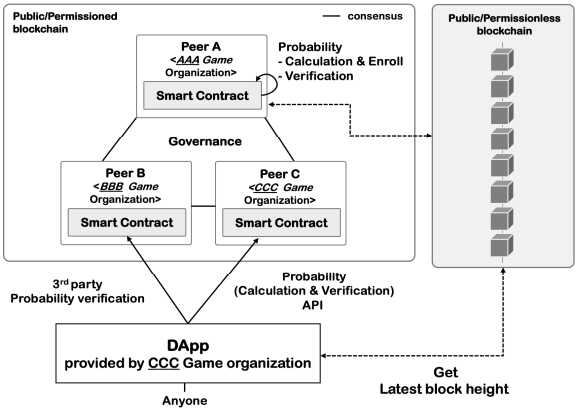

Fig. 1. System Architecture

이 시스템의 메인 블록체인 네트워크는 Public 구조로, 데이터를 모두 공개하여 투명성을 기반으로 신뢰성을 확보한다. 서비스를 제공하는 스마트 컨트랙트의 경우 다음과 같은 2가지 기능을 보유하여야 한다.

1) 입력된 정보 기반의 확률 요청
2) 요청된 확률에 대한 검증 수행

2번 과정에서, 확률값 산출 및 검증 수행 시 발생하는 deterministic problem을 해소하기 위해, 예측 불가능한 미래 데이터를 사전에 정의하고 이를 수집하여 Seed 값 생성 변수로 활용한다. 본 논문에서는 Public/Permissionless 구조의 블록체인(bitcoin/ethereum 등)의 미래 블록에 대한 정보를 연계하여, 예측 불가능한 Non-deterministic 한 환경을 제공한다.

이 시스템의 DApp 서비스는 누구나 개발하여 사용자에게 제공할 수 있다. 해당 서비스에서 발생하는 확률 요청 및 검증 결과는 모두 블록체인에 기록되며, 사용자가 직접 검증을 수행하거나, 신뢰할 수 있는 검증된 third-party 인증 기관을 통해 조작 여부를 확인할 수 있다.

2. User Scenario

1) 확률 등록 요청: 사용자의 요청에 따라, DApp이 제공하는 정보를 기반으로 확률을 사전에 등록하는 과정이다. 사용자에 의해 정해진 offset 값을 필수적으로 입력 받아야 하며, 외부 블록체인의 최근 블록 높이 값과 함께 본 시스템의 블록체인에 저장한다.

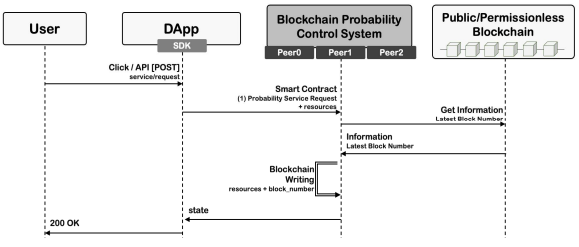

Fig. 2. 입력된 정보 기반의 확률 요청

2) 확률 검증 요청: 사전에 등록된 확률값을 산출하는 과정으로, 미리 등록된 정보인 offset과 블록 높이 값을 더한 블록 헤더의 Hash 정보를 획득하여 랜덤 함수의 Seed로 활용, 확률값을 도출한다.

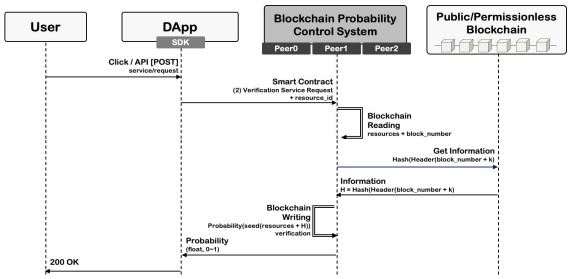

Fig. 3 요청된 확률에 대한 검증 수행

IV. Conclusions

본 논문에서 제안한 블록체인 기반 확률 제어 시스템은, 확률에 대한 투명성과 신뢰성을 확보하여 기존 시스템의 조작 가능성을 원천적으로 차단했다. 또한 미래에 발생하는 불특정 데이터를 연계함으로써 Non-deterministic 한 환경을 제공하여 예측 불가능한 확률값을 산출할 수 있도록 했다. 물론 미래 데이터 연계에 따른 비동기 상황에서의 Latency 이슈가 발생할 여지가 충분하기 때문에, 이에 대한 최적화 관점에서의 요소를 고려하여야 한다.

ACKNOWLEDGEMENT

This work was supported by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government(MSIT) (No.2022-0-00627, Development of Lightweight BIoT technology Highly Constrained Devices)

REFERENCES

[1] Ye-Jin Park, et al. "Analysis of the Issues of Gacha System in Online Games" Proceedings of the Korea Computer Information Society Summer Conference Vol. 26, No. 2, July, 2018

[2] Jong-Min Oh, et al. "A Study on the Probability and Actual Probability ofProbabilistic Items in Mobile Games" Proceedings of the Korea Computer Information Society Summer Conference Vol. 28, No. 2, July, 2020

[3] Xiao, Leon Y., et al. "Gaming the system: suboptimal compliance with loot box probability disclosure regulations in China" Behavioural Public Policy, pp. 1-27, 2021.

[4] Han, Sukhee, "Analysis of Loot Box System in Overwatch," Journal of Korea Game Society, Vol. 8, pp. 95-104, Nov. 2018.