미래사회
Journal of Future Society
2025. Vol. 16, No. 2, 170～185.
https://doi.org/10.22987/jifso.2025.16.2.170

공개형 블록체인 시스템 기반 대표자 선정 기법에 관한 연구 동향 및 고찰

신 영 아*　　노 건 태　　천 지 영**

고려대학교　　서울사이버대학교

본 연구는 공개형 블록체인 시스템에서 오라클에 의존하지 않고 무작위성을 확보하여 대표자를 선정하는 암호학적 기법에 대한 기술 동향을 조사하고, 그 적용 가능성을 분석하였다. 스마트 컨트랙트를 활용하는 블록체인 시스템을 위해 Verifiable Delay Function(VDF), Time-Lock Puzzle(TLP), Verifiable Random Function(VRF) 세 가지 후보 기술을 비교 분석하였으며, 각각의 기법을 유일성, 공정성, 예측불가능성 등 대표자 선정의 안전성 요구사항 관점에서 분석하였다. 또한 블록체인 합의 알고리즘, DeFi 확장성 프로토콜, 오프체인 결제 시스템 등의 분야에서의 활용 사례를 조사하였다. 분석 결과, 세 기법은 각기 다른 안전성과 구현 특성을 가지며, 특정 환경에 따라 보완적으로 사용될 수 있음을 확인하였다. 본 연구는 향후 탈중앙화 자율조직 및 블록체인 기반 분산 시스템에서의 무작위성 기반 프로토콜 설계에 이론적 기초를 제공할 수 있을 것으로 기대된다.

주요어 : 공개형 블록체인, 대표자 선정 기법, 검증가능한 지연 함수, 타임락 퍼즐, 검증가능한 랜덤 함수

* 주저자: 신영아/고려대학교 정보보호대학원 정보보호학과 대학원생/서울특별시 성북구 안암로 145 로봇융합관 404호/Tel: 02-3290-4258/E-mail: yashin95@korea.ac.kr
** 교신저자: 천지영/서울사이버대학교 인공지능학과 조교수/서울특별시 강북구 솔매로 49길 60 /Tel: 02-944-5543/E-mail: jychun@iscu.ac.kr

Ⅰ. 서론

블록체인(Blockchain)은 탈중앙화, 무결성, 불변성, 투명성, 가용성을 특징으로 하는 분산 원장 기술로, 미래 사회의 스마트 혁신을 이끄는 핵심 인프라로 주목을 받고 있다 (안상선, 2021). 특히, 비트코인(Bitcoin), 이더리움(Ethereum) 등의 공개형(Public) 블록체인 시스템은 모든 참여자가 동등한 권한을 가진 상태에서 모든 장부 내역에 접근하고, 내역의 유효성을 검증하여 시스템 신뢰성을 제고한다. 이러한 특성으로 인해, 가트너(Gartner)가 선정한 2025년 10대 전략 기술 중 하나인 허위 정보 보안(Disinformation Security) 문제를 해결하기 위한 대안 기술로 언급된 바가 있다 (Gartner, 2024).

이더리움과 같은 공개형 블록체인 시스템은 튜링 완전성(Turing Completeness)을 만족하는 프로그래밍 언어를 기반으로 스마트 컨트랙트(Smart Contract) 기능을 제공한다. 스마트 컨트랙트를 통해 사용자 간 계약 조건을 맞춤형으로 개발할 수 있으며, 처리된 계약 내용은 분산 원장에 기록되어 모든 참여자에 의해 검증된다. 이로 인해 다양한 프로그램을 개발할 수 있게 되어 중앙기관 없이 운영 가능한 탈중앙화 자율조직(DAO, Decentralized Autonomous Organization)과 탈중앙화 금융(DeFi, Decentralized Finance) 산업이 확장되기 시작하였다.

한편, 스마트 컨트랙트를 제공하는 블록체인 시스템은 외부 데이터를 불러오는 과정에서 정보의 신뢰성과 관련된 오라클(Oracle) 문제에 직면한다 (Antonopoulos, 2024). 예를 들어, 스마트 컨트랙트에서 예측 불가능한 랜덤 정보를 불러와 DAO 조직 내에서 대표자를 무작위로 선정하고자 할 때, 랜덤 정보는 스마트 컨트랙트의 결정적(Deterministic) 특성상 블록체인 내부에서 자체적으로 생성할 수 없다. 따라서, 진정한 랜덤 정보를 스마트 컨트랙트에서 입력받기 위해서는 오라클을 통해 외부로부터 값을 전달받아야 한다. 그러나, 블록체인 시스템에서 오라클의 도움으로 진정한 랜덤 정보를 생성하는 기법은 그 설계 과정이 용이하지 않다. 특히, 암호학적 관점에서 무작위 방식으로 진정한 랜덤 정보를 불러와 대표자를 선정하고자 할 경우 공정성을 위해 불러오는 랜덤 정보가 사전에 조직 내외부 임의의 주체에 의해 예측되어서는 안 되며, 모든 참여자가 동일한 랜덤 정보를 공유해야 하고, 이를 통해 동일한 당선자 정보가 모든 참여자에게 일관되게 전달되어야 한다.

이러한 이유로 최근 암호학 및 블록체인 연구 분야에서는 오라클의 도움 없이 블록체인 시스템 자체의 환경을 이용하여 랜덤 정보를 생성하는 다양한 방법에 대한 연구가 활발히 진행되고 있다 (Gene, 2024; Antonopoulos, 2024; Lenstra, 2015; Boneh, 2018a; Wesolowski, 2019; Pietrzak, 2019; Boneh, 2018b; Rivest, 1996; Malavolta, 2019; Micali, 1999; Goldberg, 2021; Qian, 2017; Buterin, 2024; Chainlink Labs, 2024; Algorand Foundation, 2024; Boneh, 2020).

랜덤 정보는 블록체인 시스템 프로토콜과 시스템을 활용한 여러 응용 서비스에 필요한 정보이다. 각 암호화폐에서 규정하는 합의 알고리즘과 같이 블록체인 시스템 내부 프로토콜에서도 활용이 될 수 있으며, DAO, DeFi 등 블록체인 기반 금융 서비스에도 중요하게 활용된다. 특히, 어떠한 집단에 속한 참여자들 중에서 특정 역할을 수행해야 하는 대표자를 무작위로 선정해야 하는 상황에서는 주사위의 역할처럼 랜덤 정보의 활용이 반드시 요구된다.

1.1. 연구 목적 및 기여

본 연구는 해당 배경에 주목하여 공개형 블록체인 시스템 내에서 생성된 랜덤 정보를 활용한 무작위적 대표자 선정 프로토콜을 설계하기 위한 연구의 흐름으로, 이를 달성하기 위해 후보 기술로써 활용될 수 있는 암호학적 기법에 관한 동향 연구를

수행하고자 한다. 또한, 해당 기술이 블록체인 관련 분야에 어떻게 활용될 수 있는지에 대한 사례 분석을 수행한다. 이를 통해 신뢰성 높은 대표자 선정 기법 설계를 위한 연구 방향성을 제시함으로써 미래 사회의 분산형 조직 운영 방향에 학술적으로 기여하고자 한다. 본 연구는 향후 블록체인 자체 기술뿐만 아니라 공개형 블록체인 시스템을 기반으로 하는 다양한 자율 조직(DAO) 및 분산형 애플리케이션(DApp) 프로토콜 설계에 관해 실질적인 이론적 기초를 제공할 것으로 기대된다.

1.2. 연구 방법 및 범위

본 연구는 스마트 컨트랙트 기능을 제공하는 대표적인 공개형 블록체인 시스템인 이더리움(Ethereum) 암호화폐 및 이와 상호운용성(Interoperatbiliy)을 가지는 암호화폐 시스템을 대상으로 적용 범위를 설정하였다. 이에 따라, 스마트 컨트랙트와 분산 원장에 기록된 데이터를 활용하고, 타원 곡선 암호(ECC, Elliptic Curve Cryptography) 등 이더리움에서 규정하는 기술 명세 등을 바탕으로 설계할 수 있는 무작위 대표자 선정 프로토콜을 대상으로 연구 조사를 시행하였다. 해당 범위에서 이더리움 재단의 공식 홈페이지와 컴퓨터과학 분야 우수국제학술대회, 국제학술지의 문헌들을 중심으로 최근 대두되고 있는 유망 기술 및 연구 결과를 수집하여 연구를 수행하였다.

1.3. 논문 구성

논문의 구성은 다음과 같다. 2장에서는 블록체인 기술과 안전한 대표자 선정 기법을 실현하기 위해 만족되어야 하는 안전성 요구사항을 설명하고, 3장에서는 무작위적 대표자 선정 기법이 적용될 수 있는 블록체인 기술 분야에 대해 살펴본다. 이후, 4장에서는 대표자 선정을 실현하기 위해 활용될 수 있는 후보 기술로서 Verifiable Delay Function(VDF), Time-Lock Puzzle(TLP), Verifiable Random Function(VRF)에 관해 각각의 장단점과 적용 현황을 분석한다. 마지막으로, 안전한 대표자 선정 기법을 실현하는 방안에 대해 제언 및 결론을 제시한다.

Ⅱ. 이론적 배경

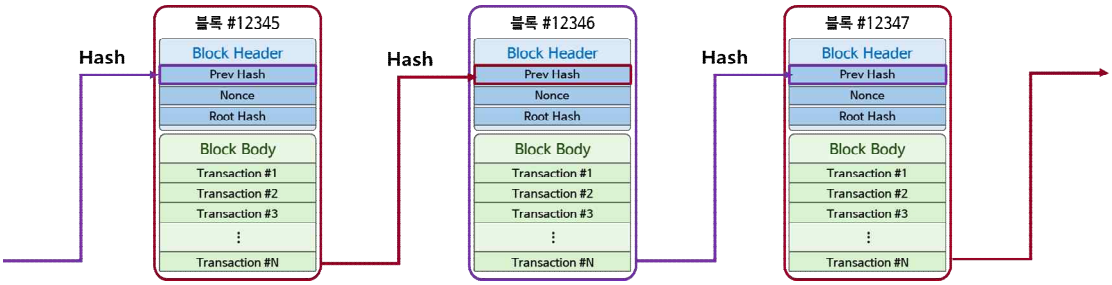
본 장에서는 블록체인 기술의 개요와 블록체인 시스템에서 무작위로 대표자를 선정할 시 만족되어야 할 안전성 요구사항에 관해 설명한다.

1. 블록체인

블록체인 시스템은 기존 중앙집중형 데이터베이스와 다르게 참여자 모두가 동일한 장부 내역을 저장한다. 만약 장부의 내역 간에 불일치 현상이 발생할 경우 일종의 투표 과정인 합의(Consensus)를 통해 해당 내역의 진위를 판별한다. 진위가 확정된 장부 내역은 이전 장부들과 암호학적 해시 함수(Cryptographic Hash Function)로 서로 연결되어 블록 단위로, 영구적으로 저장된다. 각 참여자는 이 장부를 보관함으로써 모든 내역에 쉽게 접근 및 열람할 수 있다. <그림 1>과 같이 하나의 블록 안에는 여러 개의 트랜잭션이 포함되며, 생성된 블록 간에는 순서가 보장된다. 이에 따라, 은행 등과 같이 별도의 신뢰 기관이 없이도 모든 시스템 참여자에 의해 특정 송신자가 동일한 자산을 두 번 사용하는 이중지불(Double-Spending) 공격을 방지할 수 있다.

스마트 컨트랙트는 블록체인 시스템에서 실행되는 탈중앙화된 프로그램이며, 튜링 완전성을 만족하는 프로그래밍 언어로 작성된다. 현실 세계의 계약처럼 특정 조건이 충족될 시 자동으로 실행되도록 설계할 수 있으며, 그 결과는 장부에 기록되어 모든 참여자에게 공개되고, 검증받을 수 있다.

한편, 스마트 컨트랙트는 결정론적 특성을 가지



<그림 1> 블록체인

기에 예측 불가능한 값을 생성해 낼 수 없다. 또한, 특정 날짜의 날씨나 미래의 주가 정보처럼 블록체인 시스템 내부에서 생성할 수 없는 데이터는 반드시 외부로부터 불러와야 한다. 오라클(Oracle) 문제는 이 과정에서 발생하는 신뢰 문제를 일컫는다.

오라클을 통한 외부 데이터 수집은 불러오는 시점, 대상, 주체, 정보의 획득순서 등의 원인으로 데이터 신뢰성 보장 과정에 복잡성이 수반된다 (Antonopoulos, 2024). 특히, 정보가 랜덤 정보를 생성하기 위한 시드(Seed) 정보일 경우 특정 참여자가 이를 선점할 경우 랜덤 정보를 조작하거나 예측할 가능성이 존재한다 (지의신, 2024). 이는 랜덤 정보를 중요하게 활용하는 프로토콜 전체에 공정성을 유의미하게 훼손할 수 있으며, 다양한 공격 벡터를 제공할 수 있게 한다. 이에 따라, 최근 외부의 유입 없이 온체인(On-Chain) 방식으로 랜덤 정보를 생성하기 위해 암호학 분야에서 활발히 연구되고 있다.

2. 무작위 대표자 선정을 위한 안전성 요구사항

2022년 Boneh 등은 이더리움 공개형 블록체인 합의 알고리즘에 특화된 블록체인 기반 대표자 선정 기법을 처음으로 제안하였다. 해당 연구는 다음의 블록을 제안하는 대표자를 선정하기 위해 만족하여야 하는 안전성 모델과 속성들을 암호학적으로 정의하였다 (Boneh, 2022). 본 장에서는 이를 바탕으로 합의 알고리즘에 국한하지 아니하고, 블록체인 환경 전반에 적용될 수 있도록 온체인 정보 기반 무작위 대표자 선정 기법을 설계하기 위해 모두 만족해야 하는 세 가지 안전성 요구사항을 다음과 같이 정의한다.

2.1. 유일성(Uniqueness)

유일성(Uniqueness)이란, 선정 과정에서 단 한 명의 참여자가 정확히 선출되어야 한다는 것을 의미한다. 만약 대표자를 선정하는 알고리즘을 수행한 결과 두 명 이상의 당선자의 결과가 나올 시 유일성의 성질을 보장하지 못한다고 말할 수 있다. 설계하고자 하는 시스템에 따라 두 명 이상의 당선자가 도출될 필요성도 존재할 수 있으나, 본 연구에서는 활용 분야의 환경 상 단 한 명의 당선자를 선정하는 것을 목표로 한다.

2.2. 예측불가능성(Unpredictability)

예측불가능성(Unpredictability)이란, 해당 시스템 내외부에서 대표자를 제어할 수 없는 공격자가 존재할 때, 그 공격자는 어느 참여자가 대표자로 당선될 것인지 알아낼 수 없어야 함을 의미한다. 당선된 자의 정보를 모든 참여자가 정당한 단계에서 동시에 알 수 없게 되거나, 당선되지 않은 자가 사전에 당선자를 확인할 수 있게 되면 예측불가능성을 만족하지 못한다고 말할 수 있다. 이러한 경우 공격자는

당선될 참여자를 대상으로 DoS(Denial-of-Service) 공격을 수행하여 대표자 당선 사실을 알아내지 못하게 하거나, 역할을 수행하지 못하도록 조작할 수 있다.

2.3. 공정성(Fairness)

공정성(Fairness)이란, 참여자 수를 N명이라 할 때, 각 참여자가 대표자로 선정되기 위한 확률은 동일하게 $\frac{1}{N}$이어야 함을 의미한다. 해당 성질은 표면적으로 예측불가능성을 만족하면 공정성 역시 만족하는 성질로서 여겨질 수 있다. 그러나, 예측불가능성은 공정성과 관련이 있지만, 예측불가능성만으로 공정성이 보장되지는 않는다. 공정성은 예측불가능성과 달리 공격자가 시스템을 제어할 수 있음을 전제한다. 이에 어떠한 참여자가 대표자가 될 확률을 자신에게 유리하게 높이거나 타 참여자의 당선 확률을 조작할 수 있게 할 경우 공정성을 보장하지 못한다고 말할 수 있다.

Ⅲ. 활용 분야 분석

본 장에서는 오라클의 도움 없이 블록체인 시스템 내부에서 생성한 랜덤 정보를 바탕으로 무작위 대표자 선정 기법 설계 시 적용될 수 있는 관련 분야 및 연구 사례들을 분석한다.

1. 블록체인 합의 알고리즘

공개형 블록체인 시스템은 중앙 기관 없이 자율적으로 운영되어야 하므로, 시스템의 모든 참여자가 블록 생성에 자발적으로 참여하도록 동기를 부여하는 메커니즘이 필요하다. 대표적인 참여 유도 방식으로는 비트코인에서 채택한 작업 증명(PoW, Proof-of-Work) 방식과 이더리움이 최근 도입한 지분 증명(PoS, Proof-of-Stake) 방식이 존재한다. 작업 증명 방식은 참여자 중 암호학적 해시 함수를 사용하여 정의된 암호 퍼즐을 해결하면 참여자(채굴자, Miner)는 트랜잭션을 모아 원장에 이어질 다음 블록을 제안할 수 있다. 이와 달리, 지분 증명 방식은 참여자의 암호화폐 보유 지분에 비례하여 지분이 높을수록 다음에 생성될 블록을 제안할 수 있도록 한다.

그런데, 이더리움 암호화폐 2.0 프로토콜에서는 블록을 제안하는 참여자(Proposer)는 특정 지분량(32 ETH)을 넘어설 경우 참여자(Validator) 중에서 무작위로 선정하는 방식을 채택한다. 지분량에 실시간으로 비례하여 참여자를 선정할 경우 참여자 수가 많아질 가능성을 고려했을 때, 네트워크 관점에서 비효율적일 수 있기 때문이다. 이에 따라, 32 ETH 이상을 이더리움 스마트 컨트랙트에 예치한 참여자는 온체인 정보를 활용하여 랜덤 정보를 생성하고, 이를 바탕으로 무작위 방식에 따라 참여자 중 한 명을 선정한다. 이때, 모든 참여자는 동일하게 $\frac{1}{N}$ 의 선정 확률을 가진다.

현 이더리움 2.0 프로토콜에서는 RANDAO (Random Decentralized Autonomous Organization) 방식을 활용하여 32 ETH를 예치한 참여자들을 대상으로 블록 생성자(Proposer)를 선정하고 있다 (Qian, 2017). 이더리움에서는 안정적인 블록 생성 구조를 실현하기 위해 시간 단위를 Epoch과 Slot의 개념을 통해 정의한다. 하나의 Epoch 주기는 약 6.4분의 시간 간격을 의미하며, 이는 32개의 Slot으로 구성된다. 즉, 하나의 Slot은 약 12초의 단위인 것이다. RANDAO 방식은 다음 Epoch에서 사용할 랜덤 시드, 즉, 랜덤 정보를 생성하기 위한 입력값을 현 Epoch 내의 32개의 Slot의 블록 생성자들이 생성한 값($randao\_reveal_s$)들을 누적하여 혼합(Mix)해 정의한다. 식 (1)은 다음 Epoch $e+1$에서 사용될 랜덤 시드를 계산하는 식을 나타낸다. 현 Epoch 내

모든 Slot의 블록 생성자들이 제출한 $randao_reveal_s$을 가지고, 현 Epoch의 랜덤 시드를 암호학적 해시 함수의 입력값으로 넣어 다음 Epoch의 랜덤 시드를 계산한다.

$$randao\_mix_{e+1} = H(randao\_mix_e \oplus randao\_reveal_s) \quad (1)$$

이때, 각 Slot의 블록 생성자가 제출하는 $randao_reveal_s$은 식 (2)와 같이 계산된다. 결정론적 특징을 가진 BLS(Boneh-Lynn-Shacham) 서명 기법 (Boneh. 2001)을 사용하여 자신의 개인키로 현재 Epoch 정보에 서명하여 생성한다.

$$randao\_reveal_s = \mathrm{BLS.Sign}(sk_s, e) \quad (2)$$

이후, 다음 Epoch에서는 시드 정보와 현 Slot 정보를 활용하여 Shuffling을 수행한 후 각 Slot에 해당하는 블록 제안자를 선정한다. 그러나, 현 RANDAO 방식은 암호학적 관점에서 안전한 대표자 선정 기법을 만족한다고 볼 수 없다. 이는 2.2장에서 기술한 무작위 대표자 선정을 위한 안전성 요구사항 중 예측 불가능성의 성질을 만족하지 않기 때문이다. 하나의 Epoch 주기 내에 32개의 Slot이 차례대로 존재할 때, 마지막 Slot의 블록 생성자는 랜덤 시드를 생성하는 알고리즘과 자신이 제출할 값($randao\_reveal_s$)을 다른 참여자들에 비해 먼저 알게 되므로, 이를 활용하여 랜덤 시드 및 다음 Epoch의 블록 생성자 정보를 예측할 수 있게 된다. 이더리움 2.0에서는 이러한 프로토콜 약점을 보완하기 위해 사전 예치 방식에 따라, 스마트 컨트랙트에 32 ETH를 예치해야지만 후보자(Validator)의 자격으로 참여하도록 조건을 규정하였다. 즉, 일종의 패널티를 부여함으로써 랜덤 정보를 미리 알게 되더라도 공격 수행 시 예치금의 상실 위험을 고려하여 공격 수행의 동기를 상실시키고자 하였다.

이더리움 합의 알고리즘에 암호학적으로 안전한 블록 생성자 선정 기법을 설계하기 위해 현재 블록체인 및 암호 학계에서는 활발히 연구를 수행 중이다. Boneh 등은 유일성, 공정성, 예측불가능성의 개념을 모두 달성하는 Single Secret Leader Election (SSLE)을 제안하였다. 해당 기법은 오라클의 도움 없이 온체인에서 대표자를 선정하되, 당선 사실은 당선자 자신만 먼저 알 수 있도록 보장하였다 (Boneh, 2020). Lenstra와 Wesolowski는 Verifiable Delay Function(VDF) 개념을 제안하여 안전한 기법을 실현하고자 하였다 (Lenstra, 2015). VDF는 마지막 참여자가 제출하는 정보를 먼저 알게 된다고 할지라도 이를 통해 랜덤 값을 계산하는 데 걸리는 시간은 오래 소요되도록 설계함으로써 타 참여자보다 당선 정보를 먼저 알 수 없게 하였다. 이외에도 다수의 연구가 존재하나, 대부분 제안된 기법은 현재 구현 효율성의 문제와, 신뢰하는 주체를 바탕으로 공개 파라미터를 배포해야 한다는 점으로 인해 현재까지 상용화를 위한 연구가 지속 중에 있다.

2. 블록체인 DeFi 프로토콜

온체인 대표자 선정 기법은 합의 알고리즘 이외에도 블록체인 기반 DeFi 프로토콜의 다양한 구조적 요소에 적용될 수 있다. DeFi(Decentralized Finance) 프로토콜은 중앙 기관 없이 블록체인 기술을 활용하여 금융 서비스를 구현한 탈중앙화된 시스템을 의미한다. 예컨대, 처리 속도 및 수수료 문제를 완화하기 위해 소액 거래를 블록체인 외부(오프체인)에서 처리하고, 최초 및 최종 거래 내역만을 온체인에 기록하는 오프체인 확장성 프로토콜도 DeFi 구조의 일환으로 분류될 수 있다.

오프체인 확장성 프로토콜은 이론적 연구뿐 아니라 실제 상용 서비스로도 활발히 제안되고 있다. 예를 들어, 2017년 이더리움에서는 플라즈마(Plasma)

및 그 변형인 Plasma MVP, Plasma Cash 등 다양한 구조를 통해 스마트 컨트랙트를 활용한 처리량 개선 기술을 개발하였다(Plasma, 2017; Plasma, 2024a; Plasama, 2024b). 이후에도 확장성 개선을 위한 다양한 연구가 지속적으로 발표되었다(Khalil, 2018; Ye, 2021; He, 2024).

그러나 오프체인 확장성 프로토콜은 일반적으로 거래 내역을 주도하거나 요약하여 온체인에 주기적으로 기록하는 중앙화된 개체인 오퍼레이터(Operator)의 존재를 필요로 한다. 오퍼레이터의 존재를 도입할 시 거래 내역에 대해 효율적으로 검증 및 온체인에 저장할 수 있다는 장점이 있지만, 특정 개체에 권한이 집중된다는 점에서 블록체인의 본래 목적과 상충할 수 있다. 즉, 해당 개체에 대한 신뢰를 전제로 해야 하며, 이는 탈중앙성의 기능이 저해될 수 있다는 것이다.

이러한 한계를 극복하기 위해, 중앙화된 오퍼레이터의 역할과 권한을 공정하게 분산시키는 동시에 시스템의 안정성을 확보하려는 연구가 시도되었다(Ye, 2021; He, 2024). 예를 들어, Espresso 프로젝트에서 제안한 탈중앙화 롤업(Decentralized Rollup)은 오프체인 거래 내역을 요약한 블록을 생성하고, 이를 제안할 주체를 무작위로 선정하는 구조를 통해 탈중앙성을 보장하고자 하였다.

또한, 블록체인 기반의 다자간 오프체인 결제 프로토콜에서도 무작위 대표자 선정 기법은 오프체인 기술의 탈중앙성을 개선하기 위한 수단으로 활용될 수 있다. 2021년 Ye 등은 기존 이더리움 기반 오프체인 확장 시스템(R. Khalil, 2018)에서 도입된 오퍼레이터의 존재를 참여자 중 무작위로 선정하는 방식을 제안하였다(Y. Ye, 2021). 그러나 해당 기법은 온체인 정보를 활용하여 대표자를 선정하는 구조임에도, 무작위성을 보장하는 데 필요한 랜덤 시드인 솔트(Salt) 값을 참여자 간 안전하게 분배하는 구체적인 과정이 제시되지 않아 실현 가능성에 한계가 있다. 제안된 방식은 유일성, 예측 불가능성, 공정성의 세 가지 요구 조건을 이론적으로는 만족할 수 있을지라도, 무작위 시드 값은 시스템 보안과 직결되는 민감한 파라미터이므로, 실제 구현을 위해서는 안전하고 검증 가능한 분배 절차가 함께 설계되어야 한다. 한편, 2023년 He 등은 Hyperpay 프로토콜을 통해 예치 금액의 비율에 따라 오퍼레이터를 선정하고, 이를 Verifiable Random Function(VRF) 기반으로 구현하는 기법을 제안하였다 (J. He, 2024). 그러나 이 방식은 당선 확률이 예치 금액에 비례하여 결정되므로 무작위성(Randomness)은 확보된다고 할지라도, 공정성(Fairness)은 만족하지 못한다는 한계를 지닌다. 즉, 모든 참여자가 동일한 확률로 대표자가 될 수 없는 구조이므로, 진정한 무작위 대표자 선정 방식으로 보기에는 부족하다.

이처럼, 오라클과 같은 외부 개입 없이 무작위 대표자 선정 기법을 실현할 수 있다면, DeFi 프로토콜에서 특정 참여자가 거래를 주도하거나 거래 내역을 요약(Batch) 업데이트하는 역할을 수행해야 하는 상황에서 효과적으로 활용될 수 있다.

Ⅳ. 활용 가능한 암호학적 기법 분석

본 장에서는 공개형 블록체인 시스템 내에서 생성된 랜덤 정보를 활용한 무작위적 대표자 선정 프로토콜을 설계하기 위해 후보 기술로써 활용될 수 있는 암호학적 기법의 원리를 설명한다. 이후, 대표자 선정을 위한 안전성 요구사항의 만족 여부, 각 암호학적 기법의 장단점을 분석한다.

1. Verifiable Delay Function(VDF)

Verifiable Delay Function(VDF)는 입력값에 대한 결괏값을 지연 시간을 두고 계산할 수 있되, 결괏값은 누구나 효율적으로 검증 가능한 함수를 의미한다. VDF 함수의 결괏값을 연산하는 과정은 병렬 연산에 상관없이 연속적인 연산이 지연 시간 T

횟수만큼 수행되어야 한다. 이후, 연산의 결괏값은 연산 결과의 정확성(Correctness)를 입증할 증명값 π와 함께 공개적으로 검증 가능하다. 이때, 연산 시간과 검증 시간의 차이가 지수 연산의 차이(Exponential Gap)만큼 비대칭성(Asymmetry)을 이룬다면 VDF 함수가 효율적으로 검증 가능하다고 말한다.

VDF 함수의 알고리즘은 다음과 같이 구성된다.

$\mathrm{pp}, T \leftarrow \mathrm{VDF.Setup}(\lambda, T)$: 키 생성 기관과 같은 신뢰하는 주체가 주로 수행하며, 안전성 파라미터 λ와 연산 횟수이자 지연 시간을 나타내는 T를 설정하여 입력할 시 공개 파라미터 pp를 출력한다.

$y, \pi \leftarrow \mathrm{VDF.Eval}(\mathrm{pp}, x)$: 증명자가 공개 파라미터 pp와 입력값 x를 입력하면 VDF의 연산 결괏값 y와 연산의 정확성을 입증하는 증명값 π를 출력한다.

$1/0 \leftarrow \mathrm{VDF.Verify}(\mathrm{pp}, x, y, \pi)$: 연산의 결과를 검증하고자 하는 누구나 수행 가능하며, 입력값x와 결괏값 y, 증명값 π를 입력하면 지연 시간 T보다 훨씬 적은 시간 내에 y가 x에 대한 연산 결과임을 검증할 수 있다. 검증 사실이 올바르다면 1, 그 외의 경우 0을 출력한다.

VDF의 개념은 2015년 Lenstra와 Wesolowski에 의해 처음 제안되었다 (Lenstra, 2015). 이후 2018년 Boneh 등 (Boneh, 2018)과, Pietrzak (Pietrzak, 2018), Wesolowski (Wesolowski, 2018)에 의해 효율적으로 실현할 수 있는 VDF 기법에 관해 연구가 수행되었다. VDF의 개념은 다양한 수학적 구조를 기반으로 구현될 수 있으며, 대표적으로 세 가지의 설계 방식이 존재한다. 첫 번째로는 반복적인 해시 체인(Hash Chain)을 통해 연산 결괏값을 계산하되, 연산 중간에 결괏값에 대한 검증 가능한 증명 값을 생성하는 Incrementally Verifiable Computation (IVC) 기법을 통해 검증의 효율성을 도모하는 기법이 있다. 해당 방식은 실용적으로 구현 가능하나 병렬 연산의 가능성을 제어하기 어렵다는 한계가 존재한다. 두 번째로는 RSA 모듈러 연산과 같이 모듈러 지수 연산을 활용하여 연산을 순차적으로 수행하는 모듈러 제곱근(Modular Square Roots) 기반 VDF 방식이 존재한다. 식 (3)은 해당 VDF의 식을 나타낸다.

$$\begin{aligned} \mathrm{VDF.Eval}(\mathrm{pp}, x) &= y \\ &= x^{2^T} \bmod N \end{aligned} \tag{3}$$

이러한 방식은 쉽게 구현이 가능하다는 장점이 있다. 그러나, 이론적으로 VDF를 강하게 만족하지 못하며, 신뢰 기관 없이 공개 파라미터를 생성하기 어렵다는 한계가 존재한다. 이 외에도 유한체 상에서 특정 순열 다항식의 GCD(Greatest Common Divisor) 연산이 연속적으로 수행되어야 함을 이용하여 설계하는 방식 등이 존재한다.

공개형 블록체인 시스템에서 다수의 참여자가 협력하여 하나의 랜덤 정보를 생성하고자 할 경우 마지막 참여자가 랜덤 정보를 생성하기 위한 보조 정보를 블록체인 시스템에 저장하여 모두에게 공유하고자 할 때, 보조 정보를 선제적으로 알게 되어 최종 랜덤 정보를 먼저 알 수 있게 된다는 문제가 존재하였다. VDF 함수를 적용하여 랜덤 정보를 생성하고, 이를 활용하여 대표자를 선정한다면 마지막 참여자가 악의적이라 할지라도 연산의 결괏값을 빠르게 먼저 계산할 수 없게 된다는 점에서 예측불가능성의 요건을 만족할 수 있다. 다만, VDF의 암호학적 개념 및 안전성 모델을 만족하는 효율적인 구현 기법이 현재까지는 연구 단계에 있다.

2. Time-Lock Puzzle(TLP)

Time-Lock Puzzle(TLP)는 어떠한 문제에 대한 답을 연산하기 위해서 일정 시간 T만큼 순차적으로 연산을 수행해야 하는 암호학적 퍼즐 기법이다.

연산의 결괏값을 계산하는 과정에서 지연 시간 T 만큼의 연산 횟수가 요구된다는 점에서 VDF와 유사하다. 더불어, 병렬 연산을 허용한다고 할지라도 T보다 짧은 시간 내에 결괏값을 계산하는 것이 매우 어렵게 설계되어야 한다는 점에서도 유사하다. 다만, 두 개념은 검증 과정에서 차이를 가진다. VDF의 경우 최소 한 사람이 연산을 완료하면, 누구나 결괏값을 활용해 효율적으로 검증 가능하다는 특징이 있으나, TLP는 참여자가 연산의 결괏값을 계산하기 전까지 누구도 결괏값에 대해 접근하기 어려운 특징을 가진다. 또한, 작동 방식에서도 차이를 가진다. TLP는 다음과 같은 알고리즘으로 구성된다.

$Z \leftarrow \mathrm{TLP.PGen}(\lambda, T, s)$: 키 생성 기관과 같은 신뢰하는 주체가 주로 수행하며, 안전성 파라미터 λ와 연산 횟수이자 지연 시간을 나타내는 T, 문제에 대한 정답 s값을 먼저 지정하여 입력하면, 정답에 대응하는 암호학적 퍼즐인 Z이 출력된다.

$s \leftarrow \mathrm{TLP.PSolve(Z)}$: 암호학적 퍼즐$Z$를 입력하면 지연 시간 T가 지난 후 정답인 s가 출력된다.

Rivest 등이 처음 제안한 TLP의 개념은 주로 RSA의 모듈러 연산을 기반으로 하여 설계 가능하다(Rivest, 1996). 그러나, 전통적인 TLP의 기법은 참여자의 수가 증가하고, 정직하게 참여자가 연산을 T만큼 수행하지 못하는 참여자가 발생할수록 각 문제에 대한 정답을 알아내는 데 시간이 증가한다는 한계가 존재한다. 이에 따라, 2019년 Malavolta 등은 참여자 수가 증가하여도 확장성을 보장하는 Linearly Homomorphic Time-Lock Puzzle (LHTLP)의 기법을 설계하였다(Malavolta, 2019). 이는 블록체인 기반 랜덤 정보 생성, 투표 및 경매 시스템에 활용되었다.

3. Verifiable Random Function(VRF)

Verifiable Random Function(VRF)는 검증 가능한 랜덤 값을 생성하는 함수를 의미한다. 주어진 랜덤 시드 x에 대해 개인 키 sk를 보유하고 있는 사람만 시드 x에 대한 랜덤 값을 확인할 수 있게 한다. 그리고, 출력된 랜덤 값은 올바른 개인 키로부터 생성된 값이 맞다는 사실을 누구나 검증할 수 있다.

VRF는 1999년 Micali 등의 연구에 의해 처음으로 제안되었다 (Micali, 1999). 이후 IETF 표준을 위한 타원곡선 암호(ECC, Elliptic Curve Cryptography) 기반 설계 기법이 제안되었다 (Goldberg, 2017). VRF의 알고리즘은 다음과 같이 구성된다.

$sk, pk \leftarrow \mathrm{VRF.KGen}(\lambda)$: 키 생성 기관과 같은 신뢰하는 주체가 주로 수행하며, 설계의 기반이 되는 암호에 따라 각 참여자가 수행 가능하다. 안전성 파라미터 λ를 입력받으면 개인키 sk와 공개키 pk를 출력한다.

$y, \pi \leftarrow \mathrm{VRF.Eval}(sk, x)$: 자신의 개인키 sk와 랜덤 시드인 x를 입력하면, 랜덤 값 y와 이에 대한 증명 값인 π가 출력된다.

$1/0 \leftarrow \mathrm{VRF.Verify}(pk, x, y, \pi)$: 생성한 참여자의 공개키 pk와 랜덤 시드 x, 랜덤 값 y, 증명 값 π를 입력하면 랜덤 y에 대한 증명 사실의 검증되면 1, 그 외의 경우 0이 출력된다.

VRF 함수는 VDF, TLP와 달리 출력값 y자체가 랜덤 값이 된다. 그리고, 개인 키를 보유하는 자만 랜덤 값을 생성할 수 있어 타 참여자는 생성된 랜덤 정보에 대해 사전에 예측할 수 없다. 또한, 랜덤 값인 y는 예측 불가능한 난수임에도 불구하고, 특정 개인 키로부터 생성되었음을 증명 값 π를 통해 입증할 수 있다는 특징이 존재한다. 또한, VRF의 랜덤 시드는 TLP와 달리 공개된 상태로 공유가 가능한 입력 정보이다. 개인 키 정보만 비밀 정보로 관리된다면 랜덤 시드는 블록체인 시스템에서 누구

나 접근 가능한 정보로 설정하여도 된다.

VRF는 알고랜드(Algorand), 체인링크(Chainlink) 2.5의 블록체인 시스템에서 현재 구현되어 있다(Algorand, 2024). 알고랜드의 경우 합의 알고리즘 내에서 알고리즘을 운영할 특정 대표자 및 그 집단을 선정하는 과정에서 활용되고 있으며, 구현 과정은 오픈 소스로 공개되어 있다. 체인링크의 경우 랜덤 정보를 생성하여 스마트 컨트랙트에서 입력받고자 할 때, 오라클 문제의 대안으로써 적용되어 있다.

4. 비교분석

공개형 블록체인 시스템에서 탈중앙화된 환경에서 참여자 간 오라클의 도움 없이 랜덤 정보를 생성하고, 이를 통해 무작위 대표자 선정 프로토콜을 설계하기 위해 후보 기술로써 활용될 수 있는 대표 암호학적 기법의 비교분석 결과는 <표 1>과 같다. 본 연구에서는 각 기법의 구체적인 구현체에 국한하지 않고 일반적인 관점에서 무작위 대표자 선정 기법의 안전성 요구사항 세 가지인 유일성(Uniqueness), 공정성(Fairness), 예측불가능성(Unpredictabiliy)를 만족하는지를 조사하였다. 그리고, 생성된 결괏값을 활용하여 대표자 선정하는 방법의 예(Election Result)를 표현하였다. 그리고, 각 후보 기술의 기능을 비교하기 위해 결괏값 연산에 필요한 입력값에 대해 프라이버시를 보장해야 하는지(Input Privacy)와 결괏값의 검증 과정을 누구나 수행 가능한지(Public Verifiability), 그리고 검증 과정에서의 효율성(Efficient Verifiablity)과 이를 위한 영지식 증명 생성이 요구되는지(Proof Generation)에 대해서도 분석하였다. 암호학적 기법의 알고리즘을 탈중앙화된 환경에서 구현되기 위해서는 초기 공개 파라미터 pp, 키 쌍 (sk, pk) 등의 값을 생성 및 배포하는 Setup 과정에서 신뢰 기관을 전제로 하며 신뢰 기관과 안전한 채널을 요구로 하는지(Trusted Setup)에 대한 고려가 수반되어야 한다. 이를 위한 분석 결과도 <표 1>에 제시하였다. 더불어, 대표자를 선정하기 위해서는 후보 대표자가 여러 명일 경우를 고려해야 하기에 후보 기술이 다자간 환경으로 어렵지 않게 설계할 수 있으며, 안전하게 수행 가능한지를 판단하기 위해 참여자의 수 증가에 따른 기법의 효율성 정도(Scalability)에 대해서도 분석한다. 또한, 다자간 환경에서 안전한 프로토콜을 설계하기 위해서는 시스템 참여자가 악의적일 가능성도 고려해야 하므로 허용 가능한 공격자의 수(Corrupting Parties)를 분석하였다.

먼저, 안전성 요구사항 측면에서 비교한 결과, VDF, TLP, VRF 기술은 모두 예측불가능성의 성질을 만족함을 확인하였다. VDF와 TLP는 지연 시간 T에 의해 보장되고, VRF는 생성자의 개인키 sk정보의 접근 불가능성에 의해 보장된다. 다만, TLP에서는 퍼즐 Z 생성을 하기 위해 먼저 정답 s를 입력해야 하므로, Setup을 수행하는 자가 악의적이거나 입력값 s정의하는 과정에서 참여자와 공모할 시 공정성의 성질이 보장되지 않을 위험이 존재한다. VRF는 구체적인 구현 기법에 따라 요구사항 만족 결과가 달라질 수 있으나, 현재 알고랜드와 같이 VRF를 사용하는 과정에서 참여자의 결괏값에 대해 가중치를 부여하는 경우 공정성이 만족되지 않을 수 있다.

Election Result는 각 후보 기술을 활용하여 대표자 선정 기법을 설계하는 경우 정의될 수 있는 간단한 알고리즘의 식을 나타낸다. 각 참여자가 생성한 결괏값에 대해 모두 XOR 연산을 수행하고, 이를 전체 참여자 수 n으로 모듈러 연산을 수행하면, 그 결괏값이 스마트 컨트랙트에 저장된 참여자 리스트에서 당선자의 인덱스 정보가 된다. 이때, 결괏값을 계산하는 과정에서 VDF는 공개된 입력값을 사용하여 입력값에 대한 프라이버시를 보장하지 않고, TLP는 정답을 먼저 생성하기에 시스템에서 입력값의 프라이버시가 보장되어야 한다. 이러한 경우 신뢰하는 기관이 초기 퍼즐을 생성하는 과정을

<표 1> 공개형 블록체인 기반 무작위 대표자 선정 기법 실현을 위한 후보 기술 비교 분석

	VDF	TLP	VRF
Uniqueness	○	○	○
Fairness	○	×	△
Unpredictability	○	○	○
Election Result	$\bigoplus_{i=1}^{n} y_i \bmod n$	$\bigoplus_{i=1}^{n} s_i \bmod n$	$\bigoplus_{i=1}^{n} y_i \bmod n$
Input Privacy	×	○	○
Public Verifiablity	○	△	○
Proof Generation	Slow	N/A	Fast
Efficient Verifiabilty	○	×	○
Trusted Setup	○	○	×
Scalability	High	Low	Medium
Corrupting Parties	$n-1$	$n-1$	less than $\frac{n}{2}$
Constructions	Hash Chain with IVC, RSA Modulus, Permutation Polynomial	Modular Square Roots	ECC
Implementability	Low	Medium	High
Limitation	Delay time T, Trusted Setup	Delay time T, Trusted Setup, Inefficient Verifiability	Majority of Honest Parties

수행해야 하는 가정 사항이 존재한다. VRF는 입력 정보 x는 공개된 정보로 블록체인 시스템을 통해 참여자 간 공유될 수 있으나, 계산하는 과정에서 각 참여자의 개인키 sk에 대한 프라이버시는 보장해야 된다.

결괏값에 대한 공개적인 검증 여부와 이를 효율적으로 수행한 결과는 다음과 같다. 먼저, VDF와 VRF는 각각 증명값 π 또는 생성자의 공개키 pk를 활용하여 참여자와 상관없이 누구나 검증이 가능하다. 그러나, TLP의 경우 검증을 위해서는 지연 시간 T만큼의 연산을 필요로 하기에 △가 되며, 효율적인 검증은 ×가 된다. 그리고, 연산 결과에 대한 증명값은 VRF가 일반적으로 VDF와 비교하여 빠른 시간 내에 생성이 가능하다. VDF는 연산 결괏값 생성 시간을 기본적으로 요구하기 때문이다.

한편, VDF는 공개된 입력값 x과 결괏값 y, 증명값 π가 주어지기 때문에 최소 한 명 이상의 정직한 참여자가 존재할 경우 누구나 쉽게 결괏값을 검증할 수 있어 확장성이 높다고 말할 수 있다. 이에 반해 VRF의 경우 적어도 과반수 이상의 참여자가 정직하거나, 모든 참여자가 결괏값을 블록체인 시스템을 통해 공유해야 하는 가정으로 인해 확장성이 상대적으로 저하될 수 있다. TLP의 경우. 지수 연산을 빨리 수행하기 위한 오일러 함수 $\phi(n)$에 대한 정보를 알고 있는 신뢰 기관만 정답 s를 빨리 계산할 수 있다는 특징이 존재하여 일반 참여자는

정답을 계산하는데 오랜 시간이 소요된다. 때문에, 2019년 Malavolta 등은은 TLP의 확장성 문제를 개선하기 위해 선형적으로 동형(Linearly Homomorphic)의 성질을 제공하여 최소 하나의 문제에 대해서만 해결하여도 되는 기법을 제안한 바가 있다. 이처럼, 확장성 개선을 위해 TLP는 아직 지속적으로 연구가 수행되고 있다 (Malavolta, 2019; Katz, 2020).

현재까지 VDF, TLP, VRF 기법은 공통적으로 기초연구 단계에 있다고 볼 수 있다. 특히, VDF의 기법은 다양한 수학적 구조를 기반으로 구현될 수 있으나, 구현에 관한 연구는 아직까지 진행 중으로 이더리움에서도 아직 적용 계획에 대해 검토 중에 있다. 반면, VRF의 경우 알고랜드에서 제공하는 오라클 서비스에 현재 구현이 되어 있으나, 대표자 선정 기법으로 활용되어지는 경우는 드문 실정이다. TLP는 신뢰를 기반으로 Setup 단계가 진행되어야 하는 요건과 비동기식 환경에서 파라미터 설정이 어렵다는 점으로 인해 실용화엔 이르지 못하고 있다. 이처럼, 후보 기법 모두 안전하게 블록체인 기술 분야에 적용되기 위해서는 언급된 분류기준의 관점에서 연구가 발전되어야 할 것으로 보인다.

Ⅴ. 논의 및 고찰

최근 <표 1>처럼 각 후보 기술의 장단점과 안전한 구현을 위한 연구의 필요성으로 인해 컴퓨터, 암호 및 블록체인 학계와 산업계에서 이를 개선하는 연구를 수행 중이다. 일례로, 2021년 Galindo 등은 EuroS&P에서 VRF의 완전한 탈중앙성을 보장하고, 안전한 랜덤 정보를 생성하기 위한 연구 결과를 발표하였다 (Galindo, 2021). 2023년 Tyagi 등은 ACM CCS 학회에서 2019년 Malavolta 등의 LHTLP (Linearly Homomorphic Time-Lock Puzzle) 기법을 발전하여 블록체인 시스템 기반 탈중앙화 경매 시스템을 발표하였다. VDF의 개념은 2018년에 Boneh 등의 연구(Boneh, 2018)를 통해 암호학적으로 처음 개념이 완성된 이후 현재까지 블록체인 샤딩(Sharding), 합의 알고리즘, 영지식 증명(ZKP, Zero-Knowledge Proof) 분야와 함께 활발히 연구되고 있다(Xu, 2023; Wang, 2019; Kothapalli, 2022).

무작위 대표자 선정 기법은 블록체인 시스템의 내부 프로토콜과 더불어 블록체인 기반의 다양한 DeFi, DAO 시스템에도 적용될 수 있는 암호학적 기법이다. 이에 따라 암호학적으로 안전하고, 대표자 선정을 위한 요구사항을 모두 달성하는 기법에 관한 연구가 지속적으로 수행되어야 할 것으로 전망된다. VDF, TLP, VRF 외 기타 암호학적 기법을 활용한 무작위 대표자 선정 기법도 연구될 수 있다. 함수의 결정론적인 특징을 이용하여 타원곡선 기반의 결정론적 서명을 활용해 서명 값은 당사자만 생성할 수 있되, 랜덤 시드를 잘 활용하여 결괏값은 공개적으로 검증 가능한 방향도 가능할 것으로 보인다. 그리고, 안전성 모델을 고려하여 다자간 환경으로 확장할 시 탈중앙성과 신뢰 기반 Setup과정을 없애기 위해 분산화된 키 생성(Distributed Key Generatrion) 기법 또한 활용할 수 있을 것으로 고찰된다. 이와 같은 방향으로 연구될 시 전체 시스템의 강건성(Robustness)를 보장하기 위한 공모자 수(Corrupting Parties)에 관한 가정사항도 VRF에 비해 완화될 가능성도 존재할 것으로 예측된다.

Ⅵ. 결론

본 연구는 미래 사회의 핵심 인프라로 주목받고 있는 블록체인 기술과, 미래 금융의 중심으로 불리는 DAO 및 DeFi 산업에 적용할 수 있는 무작위 대표자 선정 기술의 실현을 위해, 관련 암호학적 후보 기법들을 조사하였다. 특히 블록체인의 신뢰성과 탈중앙화 특성을 보존하면서, 공개형 블록체인 시스템 내에서 활용 가능한 무작위 대표자 선정 기법에 주목하였다.

무작위 대표자 선정 과정에서는, 외부 오라클에 대한 의존 없이 블록체인 내부의 공개 정보를 기반으로 예측 불가능한 랜덤 정보를 먼저 생성한 후, 이를 바탕으로 대표자를 선정해야 한다. 이에 따라 본 연구는 무작위성을 안전하게 확보하고 이를 대표자 선정에 활용할 수 있는 암호학적 기법으로, VDF(Verifiable Delay Function), TLP(Time-Lock Puzzle), VRF(Verifiable Random Function)를 중심으로 기술적 원리 및 특징, 안전성, 장단점, 구현 가능성, 최신 연구 동향을 종합적으로 분석하였다.

해당 기법들은 모두 최근 컴퓨터, 암호학 및 블록체인 분야에서 활발히 연구되고 있는 주요 기술로, 특히 공개형 블록체인 플랫폼인 이더리움에서도 VDF 도입을 적극적으로 검토 중이다. 이러한 점에 비추어볼 때, 본 연구의 결과는 향후 블록체인 기반의 무작위성 활용 기술 개발에 실질적인 기여를 할 수 있으며, 암호학적 관점에서도 학술적 가치와 실용 가능성 측면에서 주목받을 것으로 기대된다.

참고문헌

안상선 (2021). 암호화폐 자산의 정보 효율성에 대한 연구, Journal of the Future of Society, 12(4), 51-73.

Alvarez, G. (2024.10). *2025 Top 10 Strategic Technology Trends*. *Gartner*. https://www.gartner.com/en/articles/top-technology-trends-2025. 2024.10.21. 자료 얻음

Antonopoulos, A. M., & Wood, G. (2024). *Chapter 11: Oracles. Mastering Ethereum (GitHub Repository)*. https://github.com/ethereumbook/ethereumbook/blob/develop/11oracles.asciidoc. 2024.04.30. 자료 얻음

Lenstra, A. K., & Wesolowski, B. (2015). A random zoo: sloth, unicorn, and trx. *IACR Cryptology ePrint Archive, 2015, 366*.

Boneh, D., Bonneau, J., Bünz, B., & Fisch, B. (2018). Verifiable delay functions. *In Advances in Cryptology - CRYPTO 2018, 10991*, 757-788.

Wesolowski, B. (2019). *Efficient verifiable delay functions. In Advances in Cryptology - EUROCRYPT 2019, 11476*, 379-407.

Pietrzak, K. (2019). *Simple verifiable delay functions. Innovations in Theoretical Computer Science Conference (ITCS)*, 60, 1-15.

Boneh, D., Bünz, B., & Fisch, B. (2018). A survey of two verifiable delay functions. IACR Cryptology ePrint Archive, *2018, 601*.

Rivest, R. L., Shamir, A., & Wagner, D. A. (1996). Time-lock puzzles and timed-release crypto. *Technical Report, MIT Laboratory for Computer Science*.

Malavolta, G., & Thyagarajan, S. A. K. (2019). Homomorphic time-lock puzzles and applications. In Annual International Cryptology Conference (CRYPTO), Springer. *LNCS 11692*, 620-650.
Micali, S., Rabin, M. O., & Vadhan, S. (1999). Verifiable random functions. In Proceedings of the 40th Annual Symposium on Foundations of Computer Science (FOCS), 120-130.

Goldberg, S., & Paz, A. (2021). Verifiable random functions in blockchain systems: security and applications. ACM Computing Surveys, *54*(5), 1-34.

Qian (2017). *Randao: Verifiable random number generation*. Randao. https://randao.org/whitepaper/Randao_v0.85_en.pdf. 2024.04.30. 자료 얻음

Buterin, V. (2024.10). *Possible futures of the Ethereum protocol, part 6: The Splurge*. https://vitalik.eth.limo/general/2024/10/29/

futures6.html. 2024.04.30. 자료 얻음

Chainlink Labs (2024.11). *VRFBilling. Chainlink Documentation*. https://docs.chain.ink/vrf/v2-5/billing. 2024.04.30. 자료 얻음

Algorand Foundation (2024). *AVM vs. EVM: Implementing Randomness*. Algorand Developer Portal. https://developer.algorand.org/solutions/avm-evm-randomness/. 2024.04.30. 자료 얻음

Boneh, D., Eskandarian, S., Hanzlik, L., & Greco, N. (2020). Single Secret Leader Election. IACR Cryptology ePrint Archive, *2020, 025*. https://eprint.iacr.org/2020/025. 2024.04.30. 자료 얻음

지의신, 이자흔, 이수현, 이중희 (2024). 이더리움 네트워크에서의 VDF 검증 방법 연구. 정보보호학회논문지, 34(6), 1385-1401.

Boneh, D., Lynn, B., & Shacham, H. (2001). Short signatures from the Weil pairing. In C. Boyd (Ed.), Advances in Cryptology - ASIACRYPT 2001, Springer, Lecture Notes in Computer Science, *2248*, 514-532.

Goldberg, S., Reyzin, L., Papadopoulos, D., & David, O. (2017). *Verifiable Random Functions (VRFs)*, draft-goldbe-vrf-01. IETF Internet-Draft. https://datatracker.ietf.org/doc/draft-goldbe-vrf/. 2024.04.30. 자료 얻음

Poon, J., & Buterin, V. (2017.08). *Plasma: Scalable autonomous smart contracts*. https://plasma.io/plasma.pdf. 2024.04.30. 자료 얻음

Plasma Group (2024). *Plasma MVP: Minimum Viable Plasma*. LearnPlasma.org. https://www.learnplasma.org/en/learn/mvp.html. 2024.04.30. 자료 얻음

Plasma Group (2024). *Plasma Cash. Learn Plasma.org*. https://www.learnplasma.org/en/learn/cash.html. 2024.04.30. 자료 얻음

Khalil, R., Zamyatin, A., Felley, G., Moreno-Sanchez, P., & Gervais, A. (2018). Commit-chains: Secure, scalable off-chain payments. IACR Cryptology ePrint Archive, *2018, 642*. https://eprint.iacr.org/2018/642. 2024.04.30. 자료 얻음

Ye, Y., Ren, Z., Luo, X., Zhang, J., & Wu, W. (2021). Garou: An efficient and secure off-blockchain multi-party payment hub. IEEE Transactions on Network and Service Management, 18(4), 1-15.

He, J., Zhang, K., Li, T., & Wang, Y. (2024). An efficient multi-party payment protocol for IoT micro-payments. IEEE Internet of Things Journal, *11*(4), 3200-3212.

Katz, J., Loss, J., & Xu, J. (2020). On the security of time-lock puzzles and timed commitments. In Y. Ishai & V. Rijmen (Eds.), Theory of Cryptography - TCC 2020, Part III, Lecture Notes in Computer Science, *12552*, 471-501. Springer. https://doi.org/10.1007/978-3-030-64378-3_18

Galindo, D., Gagliardoni, T., Pereira, O., & Slamanig, D. (2021). Fully distributed verifiable random functions and their application to decentralised random beacons. In 2021 IEEE European Symposium on Security and Privacy (EuroS&P), 556-571. IEEE.

Xu, J., Wang, C., & Jia, X. (2023). A survey of blockchain consensus protocols. ACM Computing Surveys, *55(13s)*, 1-35.

Wang, G., Yu, Z., Kosba, A., & Ren, L. (2019). SoK: Sharding on blockchain. In Proceedings of the 1st ACM Conference on Advances in

Financial Technologies (AFT 2019), 41-61. ACM.

Kothapalli, A., Setty, S., & Tzialla, I. (2022). Nova: Recursive zero-knowledge arguments from folding schemes. In T. Malkin & C. Peikert (Eds.), Advances in Cryptology - CRYPTO 2022, Lecture Notes in Computer Science, *13509*, 228-256. Springer.

투고일자: 2025. 4. 30.
심사일자: 2025. 5. 27.
게재확정일자: 2025. 5. 29.

미래사회
Journal of Future Society
2025. Vol. 16, No. 2, 170～185.
https://doi.org/10.22987/jifso.2025.16.2.170

A Survey of Leader Election Techniques without Oracles in Public Blockchain Systems

Young Ah Shin　　Geontae Noh　Ji Young Chun

Korea University　　Seoul Cyber University

This study investigates the current state and applicability of cryptographic techniques for achieving randomness in public blockchain systems without relying on external oracles. It focuses on three candidate mechanisms, Verifiable Delay Functions (VDF), Time-Lock Puzzles (TLP), and Verifiable Random Functions (VRF), which are suitable for blockchain systems that utilize smart contracts. Each technique is analyzed in terms of its ability to satisfy key security requirements for leader election, including uniqueness, fairness, and unpredictability. The study also explores real-world use cases in blockchain consensus protocols, DeFi scalability solutions, and off-chain payment systems. The comparative analysis reveals that the three techniques differ in their security guarantees and implementation characteristics, and may be used complementarily depending on the system environment. This research is expected to contribute a theoretical foundation for the design of randomness-based protocols in decentralized autonomous organizations (DAOs) and blockchain-based distributed systems.

Keywords: Public Blockchain, Leader Election, Verifiable Delay Function, Time-Lock Puzzle, Verifiable Random Function