94

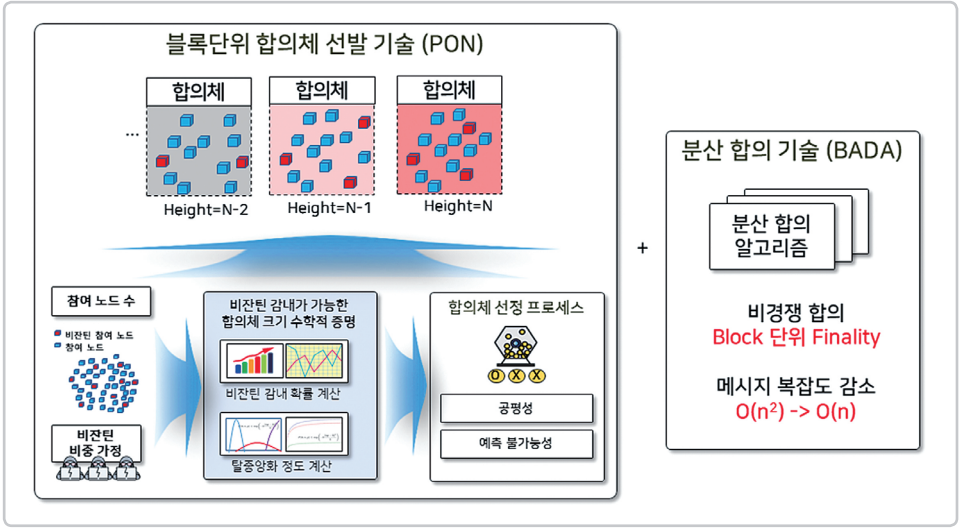
탈중앙화 비잔틴 감내 분산합의 기술

기술개요

- 대규모 참여 노드에서 블록 단위로 비잔틴 감내가 가능한 합의체를 랜덤하게 선정하고, 이들 랜덤 합의체가 분산합의를 하게 하는 기술

기술특성

- 본 기술은 넌스체인을 이용한 랜덤 합의체 선정 및 검증 기술(PON)과 랜덤 합의체 기반 비경쟁 분산합의 기술(BADA)로 구성됨
- 랜덤 합의체 구성 기술 (PON) : 주어진 참여 노드의 크기에 따라 비잔틴 노드 비율이 33%이하게 되게 선택하는 알고리즘
- 분산 합의 기술(BADA) : 분산 합의를 위한 메시지 복잡도가 O(N) 으로, 큰 규모의 합의체가 합의를 할 수 있는 분산 합의 기술



적용분야

- 물류·유통·지식거래 분야
- 의료 등 공공서비스 분야

기술완성도 (TRL)

5단계 : 확정된 소재/부품/시스템시작품 제작 및 성능 평가

기술이전 내용

대규모 노드 간에 분산 합의를 가능하게 하는 비경쟁 합의 기술(PON+BADA)

- PON : 비잔틴 감내 블록단위 합의체 선발
  - 증명 가능한 랜덤 넘버 생성(증명 가능, 예측 불가능, 블록당 한번만 생성)
  - 참여노드 수에 따라 합의체 크기 확정(확률기반)
  - 비잔틴 환경에서도 확장성을 제공하는 비잔틴 감내 합의체 구성 방법 제공
- BADA : 분산합의 알고리즘
  - 블록단위 Finality 제공, 우수한 확장성 제공으로 수만 노드까지 합의 가능
  - 합의 복잡도(O(C<N)) 및 합의 단계 최소화(3단계) 가능
  - EC-Schnorr 다중 서명 기술 적용
- 블록체인 플랫폼 연동
  - 블록체인 플랫폼 연동을 위한 인터페이스 제공

지식재산권 현황

No.	출원·등록번호	특허명	상태
1	2451115	난스를 이용한 합의 노드 선택 방법 및 그것을 이용한 블록체인 생성 방법 및 장치	등록
2	11063746(미국)	Method for selecting consensus node using nonce and method and apparatus for generating blockchain using the same	등록
3	201910507584.4(중국)	난수 증명에 기초하여 분산 협력 노드를 선택하는 방법 및 장치	출원
4	2342840	난스 증명 기반 분산합의 노드 선정 방법 및 장치	등록
5	16/431333(미국)	METHOD AND APPARATUS FOR SELECTING DISTRIBUTED CONSENSUS NODE BASED ON PROOF OF NONCE	출원
6	2461653	비잔틴 환경에서의 합의 주체 선택 장치 및 방법	등록
7	2406020	탈 중앙화된 비잔틴 오류 감내 분산 합의 장치 및 방법	등록
8	2021-0002482	블록 합의 방법 및 트랜잭션 상태 관리 방법	출원
9	17/566411(미국)	METHOD FOR BLOCK CONSENSUS AND METHOD FOR MANAGING TRANSACTION STATE	출원
10	2021-0178912	블록체인 네트워크에서의 합의 노드 정보 동기화 장치 및 방법	출원
11	2021-0180097	다중 서명 분산 합의 장치 및 방법	출원

기술이전 문의

ETRI 연구성과확산실 | 042-860-4881 / etri_tco@etri.re.kr