Chapter
03

고속 트랜잭션 처리 기술

이중희_고려대학교 조교수

I. 결과물 개요

개발목표시기	2021. 12.	기술성숙도 (TRL)	개발 전	개발 후
			4	7
결과물 형태	SW-System, SW-library	검증방법	자체 검증, 시험인증, 3자 검증	
Keywords	블록체인, 확장성, 순환 영지식 증명, 축약, 롤업 Blockchain, Scalability, Recursive zk-SNARK, Aggregation, Rollup			
외부기술요소	Open source 사용, 상용보드/시스템 이용	권리성	특허, 설계도, SW	

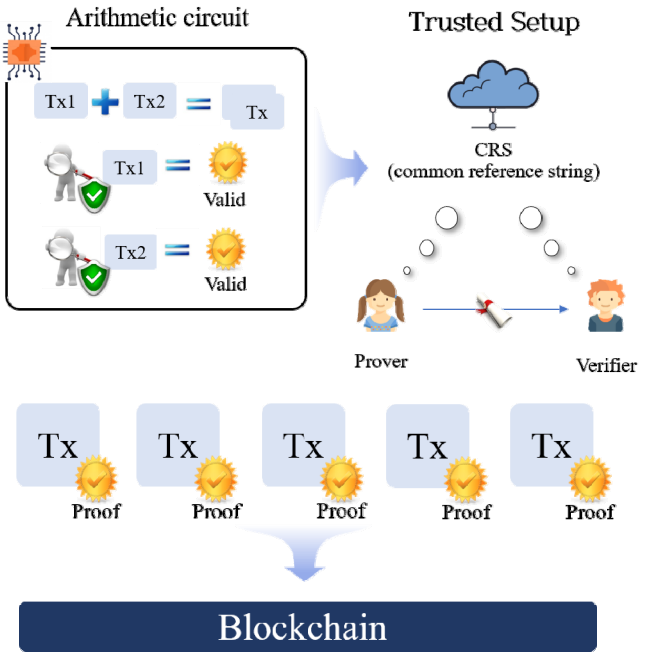
II. 기술의 개념 및 내용

➢ 본 기술은 트랜잭션 고속처리 기술에 관한 것으로, 트랜잭션 유효성과 멤버십/비멤버십 증명을 통한 UTXO 및 Account 기반 트랜잭션 유효성의 고속 검증이 가능하며, 효율적인 스마트 컨트랙트 수행결과의 검증이 가능한 기술임

* 본 내용은 이중희 조교수(☎ 02-3290-4887, j_lee@korea.ac.kr)에게 문의하시기 바랍니다.

** 본 내용은 필자의 주관적인 의견이며 IITP의 공식적인 입장이 아님을 밝힙니다.

***정보통신기획평가원은 현재 개발 진행 및 완료 예정인 ICT R&D 성과 결과물을 과제 종료 이전에 공개하는 "ICT R&D 사업화를 위한 기술예고"를 2014년부터 실시하고 있는 바, 본 칼럼에서는 이를 통해 공개한 결과물의 기술이전, 사업화 등 기술 활용도 제고를 위해 매주 1~2건의 관련 기술을 소개함



[그림 1] 트랜잭션 고속처리 지원 블록체인의 예

III. 국내외 기술 동향 및 경쟁력

1. 기술의 특성 및 성능

- 고속 트랜잭션 처리를 위해 트랜잭션 및 블록체인의 크기를 줄여 대역폭을 증가
- 서명 축약기술을 활용
- 영지식 증명 기술을 활용하여, 블록 검증자가 스마트컨트랙트를 직접 수행해 보지 않고 증명 검증을 통해 빠른 트랜잭션 검증이 가능

2. 경쟁기술/대체기술 동향 및 현황

- Optimistic Rollup: 최종 결정되지 않은 모든 블록에 기록된 상태 루트 값(state root)의 유효성을 검증하고, 유효하지 않은 루트 값이 존재하면 해당 루트 값의 유효하지 않음에

대한 증명을 만들고 증명이 검증되면 해당 루트 값 이전의 상태로 되돌리는 방식을 사용

3. 우수성 및 차별성

경쟁기술	본 기술의 우수성/차별성
Optimistic Rollup	Optimistic Rollup처럼 상태 변화에 대해 사후 검증하는 것이 아니라 루트 값 및 축약된 트랜잭션을 만들 때 zk-SNARK 증명을 포함하는 방식으로 축약된 트랜잭션에 대한 정확성을 보장함

4. 표준화 및 특허 동향

➢ 표준화 동향

- ZKProof Standards에서 영지식 증명 관련 기술에 대한 표준안 기고 및 채택을 진행하고 있으며, 아직 순환증명 기술에 대한 표준안은 채택되지 않음

➢ 관련 특허 보유

No.	국가	출원 · 등록번호(출원 · 등록일)	상태	명칭
1	대한민국	10-2020-0034862	출원	간결한 비상호적 영지식 증명에 특화된, 검증 가능 암/복호화 및 암호문 갱신을 지원하는 동형 암호
2	대한민국	10-2019-0062516	출원	변형 불가 및 단일 검증을 지원하는 이차산술회로 기반 비상호적 영지식 증명

Ⅳ. 국내외 시장 동향 및 전망

1. 국내외 시장 동향 및 전망

➢ 2017년 KISTI 자료에 의하면, 국내 블록체인 시장은 2016년에 201억 원에 이르렀으며, 2022년까지 연평균 약 62% 성장하여 2022년에는 3,562억 원으로 증가할 것으로 전망되고 있으며, 이와 같은 추세 성장 시 2026년 2조 3,863억 원, 2028년 6조 1,856억 원에 이를 것으로 예상

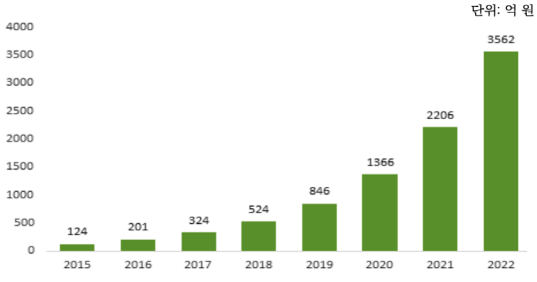
[표 1] 국내외 시장 동향 및 전망 (단위: 억 원)

구분	2021년	2026년	2028년
세계 시장 규모	24,970	1,538,482	7,997,649
한국 시장 규모	2,206	23,863	61,856

* 본 기술/제품과 직접적으로 관련된 시장 규모
* 2021 세계 블록체인 사업 규모(부가가치 포함) 22.7억 달러(24,970억 원), Gartner
* 2021 국내 블록체인 사업 규모(부가가치 포함) 2,206억 원, NIPA
* 세계 블록체인 연간성장률 128%, 국내 블록체인 연간성장률 61% 기준으로 예상 수치 산정

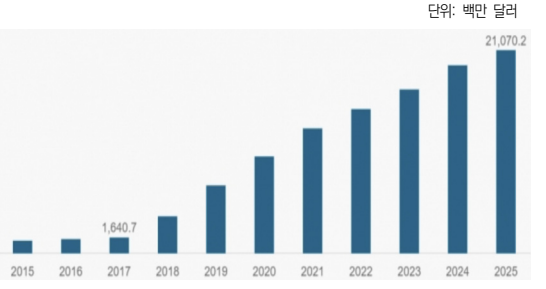
➢ 2020년 포춘 비즈니스 인사이트는 시장보고서를 통해 2017년 블록체인 기술 시장 규모는 16억 4,000만 달러였으며, 매년 38% 이상 성장하여 2025년에는 210억 달러 규모에 이를 것으로 전망

➢ 보고서에서는 블록체인 기술을 가장 적극 활용하는 산업으로 은행, 금융 서비스업과 보험업을 제시하였으며, 제조와 의료, 도소매 유통, 에너지, 공공 부문도 블록체인 기술 적용이 활발할 것으로 예상



〈자료〉 KISTI, 2017.

[그림 2] 국내 블록체인 시장 전망



〈자료〉 포춘 비즈니스 인사이트, 2020.

[그림 3] 세계 블록체인 기술 시장 전망

2. 제품화 및 활용 분야

활용 분야(제품/서비스)	제품 및 활용 분야 세부내용
블록체인	다수의 증명 검증에 필요한 노드 연산량 절감 및 증명 축약 기법을 통한 저장 용량 절감

V. 기대효과

1. 기술도입으로 인한 경제적 효과

- 블록체인의 확장성 문제 해결을 통해 탈중앙성 강화를 이끌냄으로써 블록체인의 신뢰성이 강화될 것으로 기대되며, 이에 따라 블록체인 기반 B2C/C2C 전자상거래 시장 확대 및 신뢰 기반 서비스의 블록체인 활용 저변 확대가 이루어질 것으로 기대됨
- 또한, 블록체인 상에서 트랜잭션, 스마트 컨트랙트 등 다양한 상태의 저장을 위해 공개 노드들이 지불하고 있는 저장 비용을 절약해 블록체인의 지속적인 운영에 필요한 비용절감을 이루어 낼 것으로 기대됨
- 이를 통해 블록체인 생태계의 혁신 기반을 구축하고, 데이터가 가치를 창출하는 데이터 기반 경제에 기여하여 큰 경제적 효과를 이루어 낼 것으로 기대

2. 기술사업화로 인한 파급효과

- 본 연구 과제에 의한 고성능, 대용량 블록체인 개발을 통해 블록체인의 처리량을 목표로 하는 200,000TPS(프라이빗 블록체인), 20,000TPS(퍼블릭 블록체인) 수준 달성과, 트랜잭션/블록체인 용량 최소화로 경량 노드도 참여 가능하도록 합의 노드 확장을 통한 탈중앙성 강화를 통해 블록체인 기술의 산업 실제 적용 및 다양한 암호 원천 기술과의 접목으로, 국내 블록체인 산업 범위 확장과 암호 원천 기술 경쟁력 강화를 이루어 블록체인 기술의 실용화에 결정적 역할을 할 것으로 기대