

Patent Information

- 발명자
류재철
- Patent Number
10-2021-0003531
(2021.01.11)

Keyword

- 영지식 증명
(Zero-Knowledge Proof)
- 블록체인
- 스마트 컨트랙트
- 프라이버시 보호
- 오프체인/온체인
(Off-chain/On-chain)

Applications

- 금융 거래 보안
- 전자투표
- 전자계약
- 의료 정보 보호
- 공급망 관리

Patentee & Contact Point



충남대학교
Chungnam National University

충남대학교
기술가치센터
042-821-7174
cnutlo@cnu.ac.kr

Technology Overview

비밀 값의 공개 없이 신뢰 가능한 검증을 제공하는 기술

- 블록체인 기반의 시스템에서 프라이버시 보호가 중요해지면서 영지식 증명(ZKP) 기술이 도입되었는데, 사용자가 비밀 값을 드러내지 않고도 자신이 그 값을 알고 있음을 증명할 수 있는 암호학적 기법임
- 블록체인 기술에 적용되어 트랜잭션의 진위를 비공개 상태로 검증할 수 있도록 하며, 스마트 계약이나 금융 거래와 같은 블록체인에서의 데이터가 투명하게 유지되면서도 개인정보를 드러내지 않으면서 신뢰성을 유지할 수 있는 중요한 요소로 사용되고 있음

시스템 구조 및 작동 과정

- 영지식 증명 시스템은 증명부와 검증부로 구성되는데, 증명부는 오프체인(off-chain)에서 비밀 값을 처리하여 증명 값을 생성하며, 검증부는 온체인(on-chain)에서 이 증명 값을 기반으로 검증을 수행함
- 동적 서킷은 파라미터에 따라 유연하게 생성되며, 이는 for문 반복 횟수 또는 변수 길이에 따라 조정됨
- 신뢰 기관 없이 자체적으로 증명 회로를 생성, 이를 통해 Trusted Setup이 필요 없는 방식으로 검증 가능

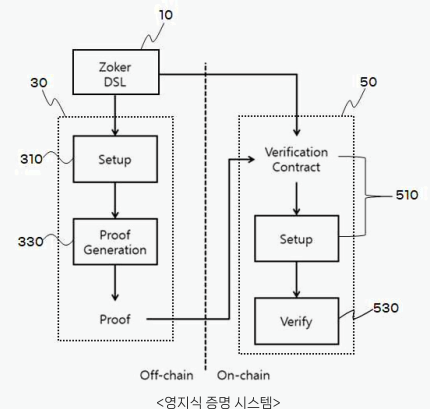
Technology Highlights

비밀 값 검증을 위한 영지식 증명 시스템

- 비밀 값을 공개하지 않고 해당 값의 신뢰성을 검증할 수 있는 영지식 증명 시스템
- 증명자는 자신의 비밀 값을 블록체인 상에 공개하지 않으면서도 그 값의 유효성을 증명할 수 있음
- 이는 거래 내역과 같은 민감한 정보를 보호하면서도 시스템의 신뢰성을 유지하는 데 기여함
- 오프체인에서 복잡한 증명 값을 생성하고, 온체인에서 상대적으로 가벼운 검증을 수행
- Trusted setup 가정을 사용하지 않는 알고리즘 중 Bulletproofs보다 비교적 검증 시간이 짧은 ZKBoo 알고리즘을 이용
- 블록체인 네트워크의 부하를 줄이면서도 신뢰성을 보장 가능

scheme	Verification time	proof size	Trusted setup
SNARK	l	1	O
Bulletproofs [15]	$n \log(n)$	$\log(n)$	X
ZKBoo [16]	$c \log(e) + h \log(h)$	$\sqrt{n}$	X

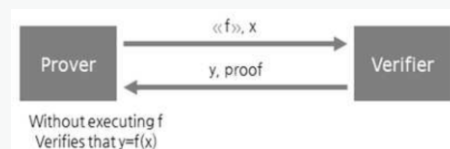
<영지식 증명 implementation 성능 비교>



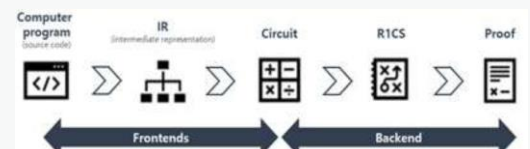
<영지식 증명 시스템>

신뢰 기관을 필요로 하지 않는 검증 구조

- for 문의 반복 횟수나 변수 길이에 따라 동적으로 검증 회로를 생성할 수 있음
- 고정된 회로 대신, 조건에 따라 회로를 유연하게 생성 및 변경할 수 있어, 다양한 상황에서 증명과 검증 작업을 지원
- 이를 통해 복잡한 연산의 유연성을 보장하고 효율성을 향상시킴
- 또한 Trusted Setup 과정 없이 자체적으로 검증 회로를 생성할 수 있어, 신뢰 기관에 의존하지 않고도 검증이 가능
- 이를 통해 신뢰성과 독립성을 강화하며, 특히 fake proof 문제를 방지하는 데 기여함



<연산 검증기법의 개념>



<증명 셋업부와 증명값 생성부를 통해 증명값을 생성하는 과정>

Technology Readiness Level(TRL)



Technology Applications

금융 거래 보안



전자투표



전자계약

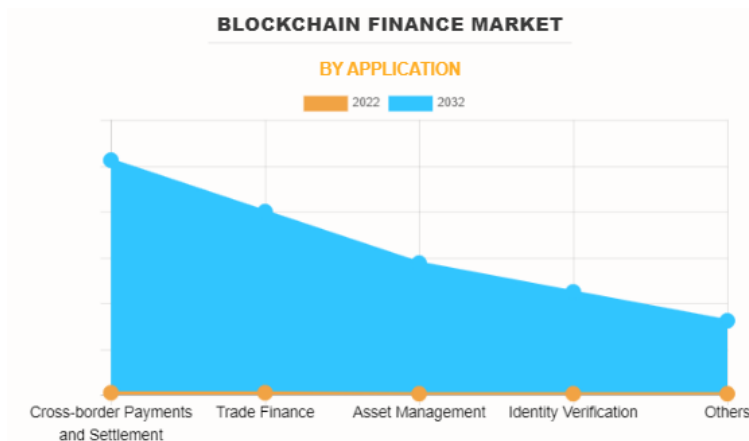
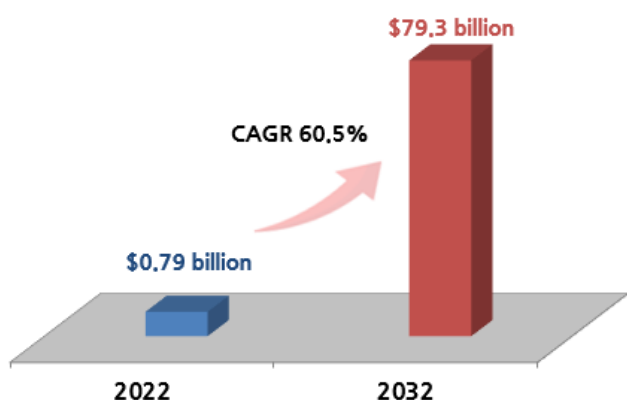


Market Trends

기술의 주요 적용 시장: 글로벌 블록체인 기반 금융 시장

블록체인 기반 금융 시장규모

- 글로벌 블록체인 기반 금융 시장규모는 2022년 7억 9,230만 달러(한화 약 1조 764억 원)로 평가되었으며, 연평균(CAGR) 60.5%씩 성장하여 2032년에는 793억 달러(한화 약 107.7조 원)에 이를 것으로 전망됨



[글로벌 블록체인 기반 금융 시장규모]

(출처: Blockchain Finance Market Opportunities and Forecast 2023-2032, AlliedMarketResearch)

- 블록체인 금융 시장 내 소규모 기업부터 거대 기업에 이르기까지 블록체인 주식과 기술 구현에 상당한 투자를 하면서 블록체인을 빠르게 채택하고 있음
- 금융에서 블록체인은 중개자의 필요성을 제거하면서 피어 투 피어 거래를 촉진하며, 시스템 계층의 통합은 즉각적인 결제 정산을 가능하게 하여 금융 거래 속도에 혁명을 일으키고 있음
- 또한 블록체인의 전문성은 국경 간 결제로 확장되어, 블록체인 기반 결제 시스템으로 즉각적인 국경 간 거래를 가능하게 함
- 이러한 요인들은 블록체인 금융 시장의 기회를 증대시킬 것으로 예상됨