영지식 증명 기반 공개 블록체인용 프라이버시 보호 디지털 콘텐츠 거래 시스템

Privacy-Preserving Digital Content Trading System via Zero-Knowledge Proofs on a Public Blockchain

요 약

기존 디지털 콘텐츠의 거래에서 구매자와 판매자는 중앙 서버를 가지는 플랫폼을 통해 거래를 수행한다. 이러한 구매자와 판매자가 중개자인 중앙 서버 대한 신뢰와 권한 위임이 필요하며, 이에 따라 플랫폼에 대한 신뢰도 문제, 표현의 자유 침해, 그리고 구매자의 프라이버시 침해 문제 등이 연관될 수 있다. 본 연구는 블록체인 및 영지식 증명을 활용하여 중개자 없이 디지털 콘텐츠 거래를 가능하게 하는 새로운 시스템을 제시한다. 블록체인 기술을 통해 콘텐츠의 등록 및 거래를 하며, 영지식 증명 기술을 도입하여 구매자와 판매자의 익명성을 보장하면서 거래의 신뢰도를 보장한다. 제안하는 시스템은 거래량 무결성, 거래 익명성, 그리고 원자적 거래의 특성을 갖추고 있고 이를 증명했다. 실험 결과, 64Kb 데이터 기준으로 콘텐츠 등록 시 시간은 약 30초, 비용은 285,131 가스가 소요되며, 거래 요청 및 승낙은 각각 약 0.3초 내외의 시간과 거래 요청은 509,717가스 그리고 거래 승낙은 1,384,937의 가스가 소요된다.

1. 서 론

최근 디지털 콘텐츠를 제공하는 플랫폼의 시장 가치가 급증하고 있으며, 블록체인 기술의 발전으로 인해 블록체인을 활용한 콘텐츠 거래 시장이 점차 활성화되고 있다. 이로 인해 디지털 콘텐츠 제작자의 수가 증가하고 전체 콘텐츠 거래 시장이 빠르게 성장하고 있다.

본 논문에서는 기존의 중앙 서버를 사용하는 콘텐츠 거래 플랫폼의 한계와 이를 개선한 프로토콜을 제안한다. 기존 콘텐츠 거래 플랫폼의 가장 큰 문제로는 수익 분배 문제를 생각할 수 있다. 판매자의 수익은 대체로 콘텐츠 거래량에 비례하는데 판매자가 콘텐츠 거래량을 직접 확인할 수 없고 플랫폼이 제공한 정보를 믿을 수 밖에 없다. 또한, 판매자가 콘텐츠를 등록할 때, 플랫폼의 간섭을 받기 때문에 창작의 자유가 침해될 가능성이 있다. 만약 창작의 자유가 보장된다면 더 많은 사용자의 유입으로 플랫폼이 성장할 수 있는 동력을 얻을 수 있다. 마지막으로, 콘텐츠 거래 시 구매자와 판매자의 신원이 노출되기 때문에 이 노출을 꺼리거나 숨기고 싶은 거래자들의 유입을 촉진할 수 있다.

본 논문에서는 거래량이 투명하게 공개되기 위해서 공개 블록체인을 도입했다. 공개 블록체인은 거래 트랜잭션이 모두 공개되며 이 트랜잭션은 조작될 수 없기 때문에 모두가 콘텐츠 거래량을 확인할 수 있지만 공개 블록체인이기 때문에 프라이버시 문제가 있다. 이를 방지하기 위해서 판매자와 구매자의 신원을 숨길 수 있도록 거래 내용을 암호화하며 거래 내용을 공개하지 않고도 거래의 유효성을 증명할 수 있는 영지식 증명 기술[2][3]을 활용한다. 콘텐츠 데이터를 블록체인을 통해 전달하면 많은 비용이 소요되기 때문에 콘텐츠를 암호화하고 off-chain에서 공유하고 블록체인을 통해 복호화 키만을 거래하여 거래 비용을 최소화하고 시스템의 처리 속도를 유지한다. 제안하는 콘텐츠 거래 시스템은 거래량 무결성, 거래 익명성, 원자적 거래 특징을 충족시킨다.

본 논문의 기여를 정리하면 다음과 같다.

- 공개 블록체인과 공개키 암호화, 영지식 증명 기술을 사용한 콘텐츠 거래 시스템을 제안한다.
- 제안한 시스템에서 콘텐츠 거래를 위한 비용을 최소화 하기 위한 방법을 적용한다.
- 콘텐츠 거래 시스템의 거래량 무결성, 거래 익명성, 원자적 거래 특징을 정의하고, 제안한 시스템이 이를 만족함을 증명한다.
- 제안한 시스템을 구현하여 실생활에 사용 가능함을 보인다.

2. 배경지식

2.1.1 블록체인

블록체인이란 디지털 거래를 기록하는 분산형 데이터베이스이다. 이는 투명한 거래내역과 조작 불가능하다는 특징을 가지고 있다.

2.1.2 공개키 암호화 스킴

공개키 암호화 스킴은 공개키와 비밀키가 있을 때, 공개키로 암호화하면 비밀키로 복호화 할 수 있는 스킴이다.

2.1.3 영지식 증명(zk-SNARK)

영지식 증명은 증명자가 검증자에게 비밀정보를 노출시키지 않고, 증명할 수 있는 암호학적 도구이다. 해당 과정이 비상호적이며 증명의 크기가 작고 검증 과정이 간결하면 zk-SNARK라고 부른다.

2.1.4 약정 스킴(commitment)

약정(commitment, cm)이란 정보를 묶는 암호학적 도구로서 나중에 그 약정을 밝힘으로써 약정된 정보가 중간에 변경되지 않았음을 증명할 수 있다. 정보를 숨기는 hiding 그리고 정보를 종속시키는 binding 특징을 가지고 있다.

2.1.5 Azeroth(익명 자금 전송 프로토콜)[4]

Azeroth는 디지털 자산의 안전한 거래를 위한 프로토콜로서 프라이버시를 보호해주며 익명 거래를 가능하게 해준다. 사용자는 비밀키, 공개키(SK, PK)를 가지고 있다. 또한 외부적으로 공개되는 계좌인 EOA와 암호화된 계좌인 ENA가 있다. Azeroth는 보내고자 하는 사용자의 ENA을 사용하여 자금이 포함된 약정 $cm_{Azeroth}$를 생성한 후, Merkle tree 자료형에 넣어두면, 돈을 받는 사용자는 해당 자료형에서 $cm_{Azeroth}$을

가져와 $cm_{Azeroth}$에 포함되어 있는 자금을 받을 수 있다.

2.1.6 PRF(Pesudo random function)

주어진 입력에 대해 예측 불가능한 출력을 생성하며, 특정 키를 사용하여 동일한 입력에 대해 항상 동일한 출력을 생성한다.

3. 본 론

3.1 프라이버시를 보호하는 디지털 콘텐츠 거래 시스템

본 시스템은 판매자와 구매자로 이루어져 있다. 판매자는 디지털 콘텐츠의 저작권자로서 디지털 콘텐츠를 생산하고 판매한다. 판매자는 디지털 콘텐츠를 암호화하고, 이 암호화가 제대로 수행되었음을 증명하기 위한 정보를 생성하여 블록체인에 등록하는 과정을 따른다. 또한, 구매 요청이 들어오면 암호화된 디지털 콘텐츠의 암호화 키를 구매자의 공개키로 암호화하는 구매 승낙 과정을 수행한다. 구매자는 블록체인에 저장된 데이터를 검토하고 디지털 콘텐츠를 구매하는 주체이다.

디지털 콘텐츠 거래 시스템은 다음 알고리즘으로 구성되어 있다.

- 데이터 등록 :데이터를 판매하기위해 판매자가 콘텐츠를 등록한다.
- 데이터 구매요청 : 구매자가 데이터를 구매를 요청한다.
- 데이터 구매승낙 : 판매자가 콘텐츠를 구매자에게 보내주고, 구매자는 대금을 지불한다.

3.1.1 거래 비용 최소화 방법

디지털 콘텐츠를 블록체인을 통해 구매자에게 보내고자 한다면 매우 큰 데이터를 블록체인에 업로드 해야 하는데 이는 매우 비용이 많이 소요되는 작업이다. 이 비용을 최소화 하기 위해서 디지털 콘텐츠를 암호화 하여 복호화 키를 거래 하도록 하였다. 판매자는 키를 받아 암호화된 콘텐츠를 복호화 하여 콘텐츠 열람 가능하다.

3.1.2 프라이버시를 보호하는 디지털 콘텐츠 거래 시스템의 특성

제안하는 디지털 콘텐츠 거래 시스템은 다음 세가지 특징을 만족하는 디지털 콘텐츠 거래 시스템으로 정의한다.

- 거래 무결성(trade integrity) : 그 누구도 판매자가 등록한 데이터에 대한 거래를 조작할 수 없다.
- 거래 익명성(trade anonymity) : 거래에 참여하지 않은 제3자는 거래에 대한 어떠한 정보도 알 수 없다.
- 원자적 거래(atomistic trade) : 거래는 판매자와 구매자가 정당하게 참여한 경우에만 성립되며, 이 특징을 충족하는 한, 어떤 악의적인 행동으로 인해 거래가 방해받지 않는다.

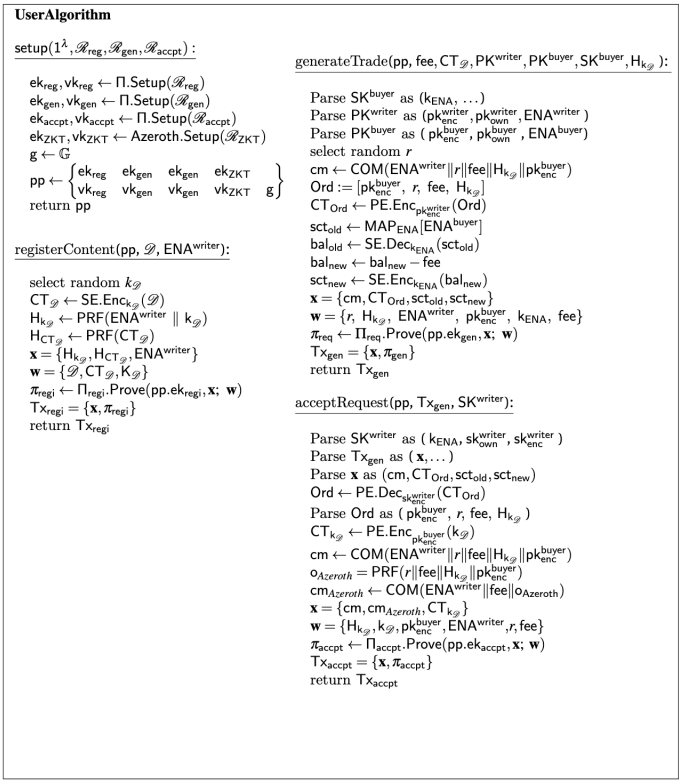
본 논문에서 제시한 시스템은 모든 거래가 블록체인 상에서 이루어지기 때문에 퍼블릭 블록체인의 조작이 불가능한 성격을 바탕으로 거래 무결성을 확보한다. 이를 통해 거래가 외부적으로 조작될 가능성이 없으며, 신뢰성 있는 거래 과정을 구축한다. 뿐만 아니라, 영지식 증명 및 공개키 암호화 기술을 적용함으로써 거래를 암호화하고 거래 정보를 익명으로 처리함으로써 거래의 익명성을 높인다. 이는 거래 당사자의 개인 정보 보호를 강화하고, 거래의 익명성을 달성한다. 더불어, 스마트 계약 및 영지식 증명을 효과적으로 활용함으로써 판매자가 구매자에게 정확한 콘텐츠 암호화 키를 제공해야 하는 원자적 거래를 달성한다.

3.3 시스템 알고리즘

디지털 콘텐츠 거래 시스템의 핵심 알고리즘은 사용자와 스마트 계약 알고리즘으로 구분된다. 제안하는 시스템에서는 증명의 크기가 $O(1)$으로 매우 작아 블록체인 환경에 적합한 Groth16[3] zk-SNARK를 사용한다.

3.3.1 사용자 알고리즘

- **setup**. zk-SNARK를 사용하기 위해서는 증명 키와 검증 키가 필요하다. registerContent, generateTrade 그리고 acceptRequest에서 사용될 zk-SNARK를 위한 증명 키와 검증 키를 생성한다. 추가로, 콘텐츠에 대한 비용을 거래하기 위한 Azeroth의 키를 생성한다.
- **registerContent**. 콘텐츠를 암호화 한뒤 이를 복호화 할 수 있는 키를 거래하며 콘텐츠 거래가 성사된다. 그렇기에 콘텐츠 등록 알고리즘은 해당 키가 암호화된 콘텐츠로부터 복호화 하여 콘텐츠를 확인 할 수 있음을 증명하는 영지식 증명 기술이 포함되어 있다. 또한 콘텐츠의 식별은 암호화된 콘텐츠의 해시값으로 식별할 수 있도록 설계 되어 있다.
- **generateTrade**. 구매자가 판매자에게 콘텐츠 구매 신청을 하는 과정이다. 구매자는 자신의 정보, 판매자의 정보, 콘텐츠의 정보 그리고 콘텐츠의 구매 비용를 사용하여 구매 신청을 진행한다. 판매자의 ENA, 콘텐츠의 가격, 콘텐츠 키의 해시값 그리고 구매자의 공개키를 통해 cm을 생성한다. 구매자의 잔고에서 콘텐츠 비용을 빼기 전과 후의 잔고를 암호화한다. 마지막으로 구매자의 공개키, 구매 비용 그리고 콘텐츠 키의 해시값을 판매자의 공개키로 암호화한다. 그 후, 영지식 증명 기술을 활용하여 콘텐츠를 구매하기에 충분한 금액을 보유하고 있다는 것과 앞서 생성한 cm이 본인이 생성했다는 것을 증명한다. cm을 증명함으로써 구매 신청은 타인이 아닌 구매자가 했음을 증명해준다. 증명과 함께 앞서 생성한 값들을 Tx_{gen}에 담아 반환한다.
- **acceptRequest**. generateTrade 과정을 통해 구매자가 보낸 구매 신청을 판매자가 승인한다. 판매자가 구매 신청을 승인한 후 구매 비용과 콘텐츠의 키의 거래가 동시에 이루어진다. 판매자는 블록체인으로부터 Tx_{gen}를 가져와 Tx_{gen}에 담겨져 있는 증명을 검증한다. 검증이 올바르게 확인 되었다면 구매자의 공개키로 콘텐츠의 키를 암호화한다. 또한 Tx_{gen}에 담겨져 있는 값들을 통해 구매 비용을 받기 위해 $CM_{Azeroth}$를 생성한다. 판매자는 생성한 콘텐츠의 키의 암호문과 $CM_{Azeroth}$이 올바르게 생성되었음을 증명하는 증명을 생성한다. 최종적으로 증명과 $CM_{Azeroth}$ 그리고 암호화된 콘텐츠의 키를 Tx_{accpt}에 담아 반환한다.



[그림 1: off chain 사용자 알고리즘]

3.3.2 스마트 계약 알고리즘

사용자 알고리즘에서 Tx로 표기되어 반환 된 값을 스마트 계약에서 zk-SNARK 증명을 검증하고, 검증이 완료되면 이후 작업들을 실행한다.

- **registerContent**. 데이터를 등록하는 스마트 계약 알고리즘으로 첫번째로 입력으로 들어온 zk-SNARK 증명을 검증한 후, 검증이 올바르면 $List_{data}$에 등록된 데이터의 정보를 입력한다.
- **generateTrade**. 디지털 콘텐츠 구매를 요청하는 스마트 계약 알고리즘으로 구매자의 암호화 된 비밀계좌 잔고가 올바른지 확인한 후, zk-SNARK 증명을 검증한다. 검증을 통과한다면 비밀계좌의 잔고를 갱신하고, waitList에 생성한 돈약정을 저장해서 일시적으로 스마트 계약에

금액을 위탁한다.

- **acceptRequest**. 구매 요청이 된 디지털 콘텐츠에 대해 구매를 승낙하는 스마트 계약 알고리즘이다. 디지털 콘텐츠를 암호화하는데 사용한 키를 구매자의 공개키로 암호화해서 스마트 계약을 통해 전송하고, 잘 전송이 되면 돈약정을 꺼내어 판매자에게 전송한다. 각각 값들이 정확하게 만들어 졌다는 증명은 zk-SNARK 증명을 통해서 증명한다.

Smart Contract Algorithm

Setup(pp):

Store $vk_{gen}, vk_{regi}, vk_{accpt}$ in smart contract
Initialize $MerkleTree_{Azeroth}$

registerContent(Tx_{regi}):

Parse Tx_{regi} as $(\mathbf{x}, \pi_{regi})$
Parse $\mathbf{x}$ as $(H_{k_\mathcal{G}}, H_{CT_\mathcal{G}}, ENA^{writer})$
require $\Pi_{regi}.pp.vk_{regi}, Verify(\pi_{regi}, \mathbf{x})$
$List_{data}.append([H_{k_\mathcal{G}}, H_{CT_\mathcal{G}}, ENA^{writer}])$

generateTrade(Tx_{gen}):

Parse Tx_{regi} as $(\mathbf{x}, \pi_{gen})$
Parse $\mathbf{x}$ as $(cm, CT_{Ord}, sct_{old}, sct_{new})$
require $MAP_{ENA}[msg.sender] == sct_{old}$
require $\Pi_{gen}.Verify(\pi_{gen}, \mathbf{x})$
$MAP_{ENA}[msg.sender] \leftarrow sct_{new}$
waitList.append(cm)
Emit Event CT_{Ord}

acceptRequest(Tx_{accpt}):

Parse Tx_{regi} as $(\mathbf{x}, \pi_{accpt})$
Parse $\mathbf{x}$ as $(cm, cm_{Azeroth}, CT_{k_\mathcal{G}})$
require $\Pi_{accpt}.Verify(\pi_{accpt}, \mathbf{x})$
require $cm \in$ waitList
waitList.delete(cm)
$TreeUptrade_{Azeroth}(cm_{Azeroth})$
Emit Event $CT_{k_\mathcal{G}}$

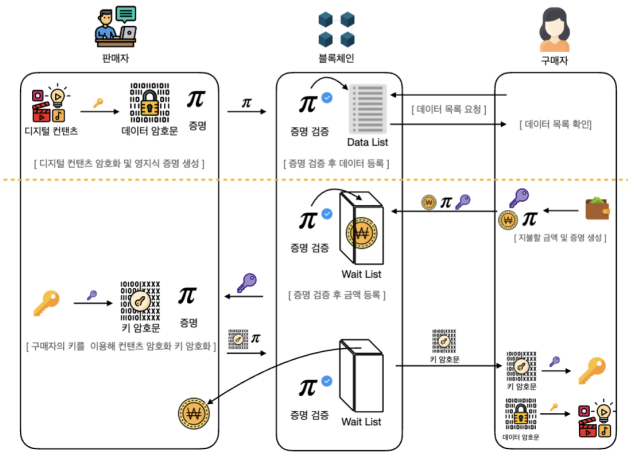
[그림2 : on chain 스마트 계약 알고리즘]

4. 실험

PRF 및 COM에는 효율적인 R1CS 회로로 구현할 수 있는 MiMC7[5] 해시 함수를 사용했고 zk-SNARK 알고리즘과 관계식은 C++로 구현했다. 디지털 콘텐츠의 크기에 따라 2^3KB ~ 2^6KB 사이즈의 회로를 구현했다. 실험은 그림 3의 시나리오를 가정하여 표 1의 환경에서 진행했다.

표 1: 실험 환경

OS	MacOS Ventura 13.4.1
CPU	Apple M1 Pro@3.2GHz
Memory	LPDDR5 32GB

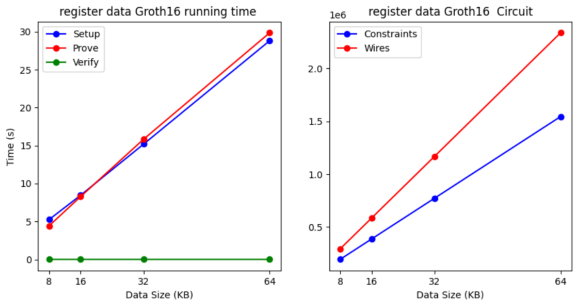


[그림3 : 시스템 시나리오]

1. 판매자는 **registerContent** 알고리즘을 사용하여 콘텐츠를 블록체인에 등록한다. 구매자는 블록체인에 등록된 콘텐츠 목록을 열람할 수 있다.
2. 구매자는 **generateTrade**를 통해 구매하고자 하는 콘텐츠에 대한 구매 요청을 블록체인에 보낸다.
3. 판매자는 블록체인에서 구매 요청을 확인하여 **acceptRequest**을 통해 거래 요청을 검증한다. 해당 과정에서 콘텐츠의 키와 구매비용이 동시에 교환된다.

4.1 zk-SNARK 증명

위 시스템에서 가장 많은 시간을 소비하는 것은 registerContent의 zk-SNARK 증명 생성 알고리즘이다. 콘텐츠를 등록하는데 필요한 증명 생성 시간은 8KB는 4.44초, 16KB는 8.19초, 32KB는 15.37초, 64KB는 29.84초이며 거래를 생성하고 진행하는데 필요한 증명 생성 시간은 0.3초 내외이다.



[그림 4 : 거래 요청 zk-SNARK 실험결과]

표 2: groth16 실험 결과

		setup (s)	prove(s)	verify(s)	constraint	wires
registerContent	8KB	5.25	4.44	0.01	193,187	292,390
	16KB	8.44	8.19		386,372	584,685
	32KB	15.11	15.37		772,742	1,169,275
	64KB	28.81	29.86		1,545,482	2,338,455
generateTrade		0.30	0.28		6,953	25,975
acceptRequest		0.31	0.31		7,315	26,502

4.2 스마트 계약

Truffle 프레임워크를 사용하여 이더리움 공개 블록체인[1]의 스마트 계약을 구현하고 Ganache 네트워크를 사용했다. 각 알고리즘의 가스 비용 데이터 등록에 285,131 가스, 거래 요청에 509,717 가스, 거래 승낙에 1,384,937 가스가 필요하다. 주요 원인은 Groth16 검증에 타원 곡선 페어링 연산이 사용되어 많은 가스가 소비되며, 거래 승낙 알고리즘은 Azeroth Merkle tree에 업데이트해야 하므로 더 많은 가스가 필요하다.

5. 결론

본 논문에서는 디지털 콘텐츠 거래 시스템을 블록체인과 영지식 증명 기술을 활용하여 설계했다. 블록체인은 거래 무결성을 유지하지만, 제 3자가 거래 내역을 확인할 수 있는 문제가 발생했다. 그러나 영지식 증명 기술을 도입하여 제 3자가 거래 내역을 확인할 수 없는 거래 익명성을 달성했다. 이로써 제3자 개입 없는 거래 시스템이 실현되었으며, 콘텐츠와 구매 비용이 동시에 전송되어야 하는 문제를 해결했다. 또한 블록체인과 영지식 증명을 사용하여 원자적 거래 특성을 만족시켜 거래 속도를 향상시키고 가스 비용을 최소화했다. 효율적인 영지식 증명 생성을 위해 대칭키와 비대칭키 암호화 알고리즘을 사용하여 빠른 결과를 얻었다. 이는 다양한 디지털 콘텐츠에 적용 가능한 거래 시스템을 제안하며, 블록체인과 콘텐츠 거래 플랫폼을 통한 거래 시스템이 확장 가능성을 보인다.

6. 참고문헌

[1] W. Nakamoto and V. Buterin, “A next generation smart contract & decentralized application platform,” Ethereum White Paper,@ inproceedings, pp. 1-36, 2015.

[2] J. Kim, J. Lee, and H. Oh, “Qap-based simulation-extractable snark with a single verification.,” IACR Cryptol. ePrint Arch., vol. 2019, p. 586, 2019.

[3] J. Groth, “On the size of pairing-based non-interactive arguments,” in Annual international conference on the theory and applications of cryptographic techniques, Springer, 2016, pp. 305-326.

[4] G. Jeong, N. Lee, J. Kim, and H. Oh, “Azeroth: Auditable zero-knowledge transactions in smart contracts,” IEEE Access, 2023.

[5] M. R. Albrecht, L. Grassi, C. Rechberger, A. Roy, and T. Tiessen, “Mimc: Efficient encryption and cryptographic hashing with minimal multiplicative complexity,” in ASIACRYPT, 2016, pp. 191-219.