영지식 증명과 Hyperledger Fabric 기반의 부동산 법원 경매 전산화 시스템 설계

박태수*, 임해영*, 최수린*, 구정태**, 손윤식*
*동국대학교 컴퓨터공학과
**동국대학교 산업시스템공학과
e-mail : sonbug@dongguk.edu

Design of Real Estate Court Auction Computerized System based on the Zero Knowledge Proof and Hyperledger Fabric

Tae-Su Park*, Hae-Young Lim*, Soo-Lyn Choi*, Jeong-Tae Ku**
,Yunsik Son*
*Dept. of Computer Science and Engineering, Dongguk Univ., Seoul, Korea
**Dept. of Industrial System Engineering, Dongguk Univ., Seoul, Korea

요 약

현재 부동산 법원 경매 시스템은 전통적인 방식으로 입찰금 중 최고가를 적어낸 입찰자가 낙찰을 받는 시스템으로 진행되고 있어 전산화가 이루어지지 않은 데에 따른 문제점들이 발생한다. 따라서 전산화 된 시스템이 필요한데, 이러한 시스템은 경매 특성상 큰 금액이 오고 가기 때문에 보안을 비롯한 문제가 발생한다. 본 연구에서는 정보의 노출을 줄이면서도, 투명성과 신뢰성을 얻기 위해 영지식 증명과 Hyperledger Fabric을 이용한 부동산 법원 경매 시스템을 제안하고자 한다.

1. 서론

현재 법원을 통해 실시되는 부동산 경매는 총 2가지로 기일입찰 방식과 기간입찰 방식이 있다. 기일입찰은 매물의 매각 기일에 출석하여 현물화한 보증금(감정가의 10%)과 입찰표를 제시하여 참여하는 방식이며 기간입찰은 정해진 입찰기간동안 법원에서 지정해 놓은 가상계좌로 보증금을 입금하고 입금증명서와 입찰표를 직접, 또는 등기우편으로 제출하는 방식이다.

그러나 현재의 방식에는 몇 가지의 문제점들이 발생한다. 경매를 진행하는 절차가 전산화 되어 있지 않아 직접 경매장까지 가거나 우편을 발송해야 되기 때문에 시간적 소모가 크다. 또한, 기일입찰의 경우 보증금을 현물화 하는 과정에서 분실의 위험성이 있다.

상기의 문제점들을 해결하기 위해서는 전산화 된 시스템을 구축하여야 한다. 하지만 전산화 된 시스템에는 신원인증 과정에서 개인 정보의 노출, 해킹에 의한 보안 취약점 등의 문제가 발생할 수 있기에 본 논문에서는 영지식 증명과 Hyperledger Fabric 기반의 시스템을 구축하여 신뢰성 있고 투명한 부동산 경매 시스템을 제안하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 본 논문에서 제안하는 시스템의 기본인 영지식 증명 및 Hyperledger Fabric과 관련된 기술에 대해 살펴보고, 3장에서는 제안된 시스템에 적용할 영지식 증명 모델을 소개한다. Hyperledger Fabric을 이용한 시스템 모델의 전체적인 구성에 대해 소개하며 끝으로 5장에서는 결론과 향후연구에 대해 간략히 소개하며 마치도록 한다.

"본 연구는 과학기술정보통신부 및 정보통신기획평가원의 SW 중심대학지원사업의 연구결과로 수행되었음"(2016-0-00017)

2. 관련연구

정보가 노출되는 것을 막으면서도 투명하고 신뢰성 있는 부동산 경매 시스템을 구현하기 위해서 본 논문에서는 영지식 증명과 블록체인 기술을 사용한다. 각 기술에 대해서는 다양한 방면에서의 연구가 진행되고 있다.

2.1 영지식 증명

표 1. 영지식 증명의 조건

완전성 (completeness)	증명하고자 하는 명제가 참이면, 정직한 증명자는 정직한 검증자에게 명제가 참인 사실을 납득시킬 수 있어야 함.
정당성 (soundness)	증명하고자 하는 명제가 거짓이면, 부정직한 증명자가 부정직한 검증자에게 명제가 참이라고 알릴 수 없어야 함.
영지식성 (zero-knowledgeness)	어떠한 명제가 참일 때, 검증자는 명제에 대한 참, 거짓에 대한 정보 이외에는 어떠한 정보도 알 수 없어야 함.

영지식 증명이란 암호학에서 사용되는 방법으로 특정 명제가 참이라는 것을 증명할 때, 해당 명제가 참인지 거짓인지의 여부만 판단할 수 있고 그 외의 정보에 대해서는 어떠한 것도 노출되지 않는 방법이다. 이 때, 특정 명제가 참인지를 보이는 측을 증명자라고 하며 해당 명제가 참인지에 대한 정보를 주고받는 측을 검증자라 한다. 영지식 증명은 상기 표의 3가지의 특징을 모두 만족해야 한다[7].

2.2 Hyperledger Fabric

Hyperledger란 리눅스 재단에서 주관하는 블록체인 오픈소스 프로젝트로 범산업용 분산원장 표준화 프로젝트(Cross-Industry open standard for distributed ledgers)로 여러 산업 분야에서 응용 가능한 블록체인 기술들을 구현하는 것을 목표로 하고 있다[1]. Hyperledger Fabric은 Hyperledger의 하위 프로젝트 중 하나로 컨소시엄 블록체인이다. 따라서 미리 허가 받은 참여자만이 블록체인 네트워크에 접근 할 수 있다. Hyperledger Fabric은 체인코드로 제어되는 트랜잭션을 사용하여 스마트 계약을 발생시킨다. 이 트랜잭션을 통하여 공유 원장과 상호작용을 할 수 있도록 하였으며 채널 기능을 통해 네트워크 참여자들 중 원하는 멤버들 간 원장의 공유가 가능하다[2].

2.3 영지식 증명을 사용한 암호화폐 Zcash

Zcash란 퍼블릭 블록체인에서 개인의 거래 정보를 완전히 보호하는 암호화폐이다. 누구나 거래내역을 확인할 수 있는 기존의 퍼블릭 블록체인과는 정보 노출의 관점에서 확연한 차이를 보이는데, 이는 영지식 증명 기술을 사용한 zk-SNARK(Zero-Knowledge Succint Non-Interactive Argument of knowledge) 프로토콜을 적용했기 때문이다[5][6]. 따라서 Zcash 거래시 수신자와 송신자, 거래 금액 등의 정보를 노출하지 않으면서 해당 트랜잭션의 유효성을 검증 받을 수 있다[4].

3. 부동산 법원 경매를 위한 영지식 증명과 Hyperledger Fabric 적용 모델

3.1 부동산 경매 시스템 전산화의 위험성

전산화 된 부동산 경매 시스템은 큰 금액이 거래되기 때문에 해커의 표적이 되기 쉬우며 해킹 되었을 때 개인정보가 유출 될 수 있다. 따라서 본 논문에서는 앞서 소개한 영지식 증명을 적용하여 정보 노출을 방지하면서, 최고가를 입찰한 입찰자만 알 수 있는 방법을 제안한다.

3.2 영지식 증명 적용 모델 개요

먼저 각각의 입찰자를 영지식 증명의 증명자로 정의하고, 검증자는 입찰자의 금액 정보를 모르는 상태에서 최고가를 입찰한 증명자를 판단할 수 있어야 한다. 그리고 부동산 경매의 특성상, 결과는 개표 시 공개하기 때문에 진행과정 중 증명자 개인이 최고가 입찰여부를 알 수 없어야 한다. 쉽게 설명하기 위해 동굴 문제를 응용하여 설명한다[3].

표 2. 영지식 증명 적용 모델 진행순서

1	각 증명자는 입구가 2개인 동굴에 임의의 순서로 진입한다. 이 때, 동굴의 중간에는 문이 존재하며 문에는 크기가 1인 버퍼와 최고가를 저장하는 공간이 존재한다.
2	저장 공간에 어떤 금액이 적혀있는지 증명자는 알 수 없다. 랜덤한 입구로 들어간 증명자는 문의 버퍼에 자신의 금액을 적어낸다.
3	금액을 읽어들인 문은 저장 공간의 금액와 비교하여 증명자가 문을 통과할 수 있는지 없는지의 여부만 증명자에게 알려준다. 입찰 금액이 저장 공간의 금액보다 크거나 같으면 해당 금액으로 갱신하고 버퍼는 초기화 된다.
4	여기서 문은 저장 공간의 금액이 갱신되어야 통과가 가능한 문 A와 갱신되지 않아야 통과가 가능한 문 B의 2가지가 있다. 문은 각 증명자에게 임의로 나타난다.
5	문이 A인지 B인지는 검증자만이 알 수 있으며, 증명자는 자신이 문을 통과하여도 문의 종류를 알 수 없다.
6	검증자는 증명자가 어떤 입구로 들어갔는지 알 수 없다. 따라서 검증자는 한쪽 입구를 정해 증명자를 호출한다.
7	여기서 증명자가 문을 통과했다면 검증자가 정한 입구로 항상 나올 수 있을 것이고 아니라면 50%의 확률로 나올 수 있을 것이다.
8	검증자는 증명자를 반복해서 호출하여 확률을 통해 문을 통과할 수 있는 증명자인지 아닌지의 여부를 판단한다. 여기서 문 A에서 100%에 근접한 확률을 보이면 저장 공간을 갱신시킨 증명자임을 알 수 있고 문 B에서 100%에 근접한 확률을 보이면 저장 공간을 갱신 시키지 못한 증명자임을 알 수 있다.
9	위 과정을 한번 진행하면 다수의 증명자가 문 A에서 100%에 근접한 확률을 보일 것이다.
10	그러한 증명자들을 추려 다시 임의의 순서로 위 과정을 반복한다. 이 때, 저장 공간은 초기화된다.
11	검증자는 반복되는 과정동안 항상 문 A에서 100%의 확률을 보이는 증명자가 최고 금액을 적어낸 입찰자인 것을 알 수 있다.

3.3 Hyperledger Fabric 적용 시스템 설계 모델

법원을 Fabric의 구성요소 중 organization으로, 해당 법원에 위치한 서버 컴퓨터를 peer로 하여 하드웨어를 구성한다. 트랜잭션이 발생했을 때 각 입찰 정보는 영지식 증명 방식을 통해 오직 확률값으로만 분산원장에 기록되며 그 확률값을 통해 최고금액 입찰자를 특정할 수 있다. 블록체인의 특성상 데이터의 신뢰성이 보장 된다.
Hyperledger가 컨소시엄 블록체인이므로 참여자마다 권한

을 제한하여 조회가 가능한 범위 역시 제한할 수 있다.

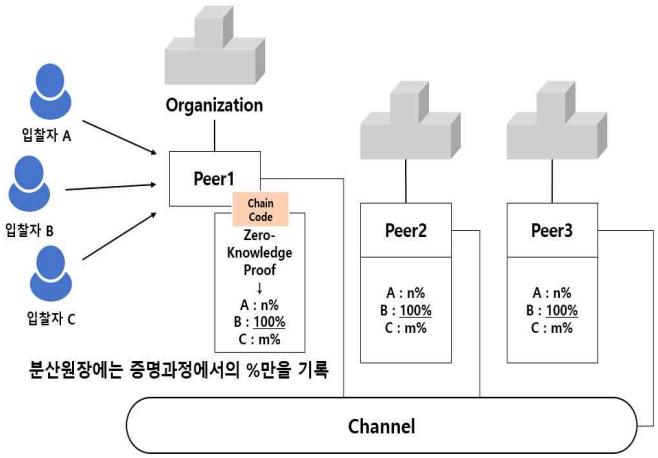

그림 1. 영지식 증명과 Hyperledger Fabric 적용 모델

4. 결론 및 향후연구

본 논문에서는 영지식 증명을 이용한 입찰 메커니즘과 Hyperledger Fabric기반의 부동산 법원 경매 시스템을 제안하였다. 현재의 부동산 법원 경매가 제안된 시스템으로 구축 된다면 전산화 되지 않은 시스템의 문제점들을 해결할 수 있고 경매 참여 과정 중 발생할 수 있는 개인 정보의 노출 역시 방지할 수 있다. 또한 사용된 Hyperledger Fabric을 통해 투명하고 신뢰성 있는 시스템이 구축된다. 따라서 부동산 경매와 관련된 법 조항들을 참고하여 시스템을 보완하고 확장하면 보다 많은 사람들이 쉽게 참여하여 활성화 된 부동산 경매가 될 것으로 판단된다.

참고문헌

[1] Christian Cachin, “Architecture of the Hyperledger Blockchain Fabfric“, 2016

[2] Mattias Scherer, “Performance and Scalability of Blockchain Networks and Smart Contracts“, 2017

[3] Quisquater Jean-Jacques, “How to Explain Zero-Knowledge Protocols to Your Children” , 1990

[4] Tommy Koens, Coen Ramekers and Cees van Wijk, “Efficient Zero-Knowledge Range Proofs in Etheruem”, 2017

[5] Eli Ben-Sasson Technion, Alessandro Chiesa, Eran Tromer, Madars Virza, “Succinct Non-Interactive Zero Knowledge for a von Neumann Architecture”, 2019

[6] Ahmed Kosba , Andrew Miller , Elaine Shi , Zikai Wen , Charalampos Papamanthou, “Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts”, 2016

[7] 이찬혁, 김기형. (2017). 개인정보보호를 위한 Zero-Knowledge Proof을 도입한 블록체인 전력 IoT 시스템 제안. 한국정보과학회 학술발표논문집, 1129-1131.