Journal of Convergence for Information Technology
Vol. 11. No. 2, pp. 31-40, 2021
e-ISSN 2586-4440
DOI : https://doi.org/10.22156/CS4SMB.2021.11.02.031

이더리움 기반의 이더를 사용한 법원 경매 시스템에 관한 연구

김효종[1], 한군희[2], 신승수[3*]
[1]동명대학교 컴퓨터미디어공학과 학생, [2]백석대학교 정보통신공학부 교수, [3]동명대학교 SW융합보안학과 교수

A Study on Court Auction System using Ethereum-based Ether

Hyo-Jong Kim[1], Kun-Hee Han[2], Seung-Soo Shin[3*]
[1]Student, Dept. of Computers & Media Engineering, Tongmyong University
[2]Professor, Division of Information & Communication Engineering, Baekseok University
[3]Professor, Dept. of Software Convergence Security, Tongmyong University

요 약 블록체인 기술이 부동산 거래분야에서도 활발히 연구되고 있으며 부동산 거래는 다양한 방법이 있다. 본 논문에서는 오프라인상 법원 경매의 문제점을 해결하기 위해 이더리움의 Ether를 사용하여 경매 시스템의 인증 절차를 간소화하는 모델을 제안한다. 제안하는 모델은 이더리움의 Solidity언어로 작성하고 법원에서 매각기일 및 매물의 Meta date를 DApp 브라우저에 등록하고 입찰자는 Meta mask의 Private key를 통해 만들어진 개인의 지갑 주소에 접속한다. 그리고 입찰자는 원하는 매물을 선택, 입찰가격 금액을 입력하여 경매에 참여한다. 입찰자가 원하는 매물의 입찰가격이 가장 높은 입찰자의 기록을 이더리움 테스트 네트워크에 스마트 계약으로 작성하고 블록을 생성한다. 마지막으로 네트워크에서 작성된 스마트 계약은 법원 경매 관리자가 블록체인 네트워크의 모든 노드에 배포하고, 블록체인 네트워크의 각 노드들은 열람 및 계약을 확인할 수 있다. 제안하는 모델의 스마트 계약과 시스템의 성능을 분석한 결과로 이더리움을 이용하는 플랫폼에서 Ether를 생성 및 사용, 그리고 참여로 인해 발생하는 수수료가 있다. Ether의 가치 변화에 따라 매물의 가격에 영향을 끼치며 매번 스마트 계약에서 일정하지 않은 수수료가 발생한다. 하지만 향후 연구에서는 자체 토큰을 발행하여 Ether의 가치 변화에 따른 시세 변동성 문제와 수수료 문제를 해결하며 복잡한 법원경매 시스템을 세분화한다.

주제어 : 블록체인, 스마트 컨트랙트, 이더리움, 전자계약, 법원경매

Abstract Blockchain technology is also actively studied in the real estate transaction field, and real estate transactions have various ways. In this paper, we propose a model that simplifies the authentication procedure of auction systems using Ethereum's Ether to solve the problem of offline court auctions. The proposed model is written in Ethereum's Solidity language, the court registers the sale date and the sale date with the DApp browser, and the bidder accesses the address of the individual's wallet created through Metamask's private key. The bidder then selects the desired sale and enters the bid price amount to participate in the auction. The bidder's record of the highest bid price for the sale he wants is written on the Ethereum test network as a smart contract. and creates a block. Finally, smart contracts written on the network are distributed by the court auction manager to all nodes in the blockchain network, and each node in the blockchain network can be viewed and contract verified. As a result of analyzing the smart contracts of the proposed model and the performance of the system, there are fees incurred due to the creation and use of Ether on platforms using Ethereum, and participation. Ether's changes in value affect the price of the sale, resulting in inconsistent fees in smart contracts each time. However, in future work, we issue our own tokens to solve the market volatility problem and commission problem with the value change of Ether, and refine complex court auction systems.

Key Words : Blockchain, Smart Contract, Ethereum, Electronic Contract, Court Auction

*This work was supported by the BB21+ Project in 2020
*This article is extended and excerpted from the conference paper presented at 2020 Korea Multimedia Fall Conference
*Corresponding Author : Seung-Soo Shin(shinss@tu.ac.kr)
Received December 2, 2020 Revised February 5, 2021
Accepted February 20, 2021 Published February 28, 2021

1. 서론

2018년 이후 비트코인 가격이 큰 폭으로 변동되면서 블록체인은 암호 화폐로서의 목적보다는 기술로서의 가치 발견을 통해 효율성에 대한 연구와 관심이 집중되고 있다[1,2]. 블록체인은 공개키 암호, 해시 함수, 머클 트리 등과 같은 핵심 암호기술이 필요하다.

부동산 거래 분야에서도 블록체인 기술이 활발히 연구된다. 부동산 거래는 개인 또는 중개사를 통한 거래, 상속 및 증여, 그리고 공매, 법원 경매 입찰을 통한 취득과 같은 다양한 방법이 있다. 그중 법원 경매는 다른 거래 방법보다 매입 시 시세가 낮고, 공정한 과정을 거친다. 법원 경매는 국가기관인 법원이 주체로 집행행위를 위한 집행 법원을 두고, 집행관이 집행행위 및 집행절차를 이행하는 방식이다[3-5].

기존 부동산 법원 경매에는 대면을 통해 경매에 참여하는 등 시간 제약, 그리고 신분증, 인감도장, 인감증명서, 입찰금 등 오프라인으로 신분을 증명한다. 또한 경매에 낙찰된 사람은 익명성이 보장되지 못한다. 그리고 입찰 보증금 손해 발생 가능성이 존재하며 군중심리 등의 여러 영향으로 인해 매수 가격이 상승하는 단점이 있다.

기존 오프라인 시스템은 시간의 제약에 따른 문제점으로 직접 법원에 가서 입찰을 진행하는 것과 패찰할 경우, 재방문에 대한 어려움이 존재한다. 만약 매각기일 직전에 취하, 변경, 연기되는 사례로 매물조사 후 법원에 갔으나 취하 등의 이유로 진행되지 않는 경우를 방지하기 위해 DApp 시스템이 요구된다. DApp 시스템에서 요구되는 사항은 익명성, 신분 인증, 스마트 계약, 보안성이 요구된다.

본 논문에서 제안하는 방안은 기존 부동산 법원 경매 시스템의 문제점[6]을 해결하기 위해 이더리움 플랫폼에서 부동산 법원 경매 DApp 시스템을 설계 및 구현을 한다. DApp 시스템은 부동산 거래의 일정 조건을 만족하면 당사자 간 자동으로 거래가 체결되는 스마트 컨트랙트 기술을 사용하는 디지털 전자계약 시스템이다. DApp을 활용하면 시간 소요를 최소한으로 하고 신분 인증을 간소화한다. 그리고 입찰자의 지갑 주소와 입찰가격을 블라인드 경매 방식을 사용하여 경매 참가자의 익명성을 보장한다.

본 논문의 구성은 다음과 같다. 2장에서는 법원 경매 시스템과 블록체인에 관련된 연구를 분석하고, 3장에서는 부동산 법원 경매 DApp 시스템을 설계하고 구현한다. 4장에서는 부동산 법원 경매 DApp 시스템의 성능을 비교 분석한다. 마지막으로 5장에서 결론을 맺는다.

2. 기존연구

분산 원장은 기존 은행 중심의 중앙화 방식과 달리 거래를 중앙 제어 없이 신뢰성 있는 방법으로 거래하는 분산형 디지털 장부이다[7,8]. 블록체인 기술은 비트코인 기반으로 중앙 시스템의 지원 없이 투명성과 무결성, 그리고 신뢰성 등을 제공한다. 블록체인에는 공개키 암호 및 머클 트리, 그리고 해시 함수 등 다양한 기술이 사용된다[9-11].

2.1 머클 트리

머클 트리는 비 단말 노드에 자식 노드의 해시값이 저장된 트리 구조로 블록의 용량을 효율적으로 관리하기 위해 사용되며 단말 노드들은 파일이나 특정 값 등의 데이터를 가리킨다[12,13]. 또한 각 블록의 트랜잭션을 대상으로 해시값을 생성하고 이진트리 형태로 연접 후 계산한다. 이때 최상위 노드를 루트 해시값이라 한다.

블록체인 네트워크에서 거래 내역을 위·변조 시도를 할 경우, 해시값이 변경된 머클 트리의 경로를 추적하여 위·변조 시도를 방지할 수 있다. 또한 거래량이 증가할 경우, 머클 트리의 이진트리 방식을 이용해 블록 데이터의 일부만 수신 받아 라이트 노드로 활용이 가능하다.

2.2 이더리움

이더리움은 스마트 컨트랙트와 블록체인 네트워크상에 배포 및 실행할 수 있는 목적의 분산 어플리케이션 DApp의 개발 및 실행 환경을 지원하는 플랫폼을 위한 플랫폼 역할을 한다. 이더는 이더리움 블록체인에서 사용되는 화폐이고, 가스는 계좌 간 거래에 필요한 수수료이다. 그리고 EVM(Ethereum virtual machine)에서 모든 네트워크 참여자들은 연산을 수행하고, 블록체인 합의를 한다[14].

이더리움 구조는 세 개의 Layer로 분류된다. 첫 번째로 하드웨어 층은 트랜잭션의 처리 및 시간에 따라 공유데이터베이스 업데이트하는 대규모 네트워크이다. 두 번째로 소프트웨어 층은 Solidity라는 프로그래밍 언어를 사용하여 스마트계약 프로그램을 실행할 수 있

게 해주는 소프트웨어 계층이다. 마지막 세 번째 DApp 계층은 사용자에게 다양한 서비스를 제공하는 애플리케이션계층이다.

2.3 스마트 컨트랙트

원장 기술에서 거래의 일정 조건을 만족시키면 당사자 간에 자동으로 거래가 체결되는 기술을 스마트 컨트랙트라 한다. 스마트 컨트랙트 기술을 적용하면 거래 절차가 간소화 되고 비용도 절감되며 거래 당사자 간에 안전한 계약이 이뤄진다. 스마트 컨트랙트는 Solidity 언어로 작성된 계약코드를 컴파일 하면 Byte Code, Function Signature, ABI (Application Binary Interface)로 구성된다[15].

Byte Code는 스마트 컨트랙트를 블록체인 네트워크에 배포하는 역할을 한다. Function Signature는 contract 내의 함수이름에 SHA-3한 Hash값의 4바이트 값이다. contract의 함수를 실행할 때 트랜잭션의 주소에는 contract 주소를 data 부분에 method signature 4바이트와 함께 파라미터 값이 탑재하여 들어가는 역할을 한다. ABI는 스마트 컨트랙트의 함수와 파라미터에 대한 Meta data가 정의되어 있고, Java Script 언어 기반 어플리케이션을 만들 때 객체를 만들 수 있다. 또한 객체의 메소드를 호출하는 것만으로 contract 함수가 호출될 수 있게 해주는 역할을 한다.

2.4 기존 DApp 시스템

DApp(Decent ralized Application)은 블록체인에서 실행되는 탈중앙화된 어플리케이션이다. DApp은 4가지의 기준을 준수해야 한다. 첫 번째로 어플리케이션이 오픈 소스로 구성되며 자율적으로 작동해야 하고, 대부분의 토큰을 제어하는 독립체가 없어야 한다. 두 번째로 어플리케이션 데이터와 작동 기록들은 공개적으로 분산된 블록체인에 암호화하여 저장되어야 한다. 세 번째로 해당 어플리케이션에 접근하는데 필요한 암호토큰을 사용해야하고, 이용자의 기여에 따라 어플리케이션 토큰으로 보상되어야 한다. 마지막으로 어플리케이션은 노드들이 가치를 증명하기 위해 표준 암호화 알고리즘에 따라 토큰을 생성해야 한다[15,16].

DApp의 환경은 smart contract를 Solidity 언어로 작성하고 배포하는 Back-end와 사용자 인터페이스를 구현하는 Front-end로 구성된다. 그리고 DApp을 이용하는 User들은 독립 노드간의 통신이 필요하다. DApp을 구현하기 위한 환경은 Fig. 1과 같다.

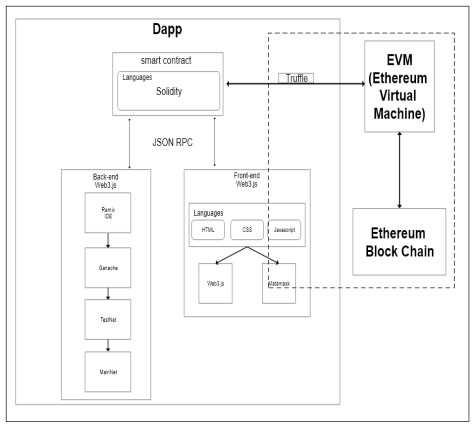

Fig. 1. DApp Environment

3. 부동산 법원 경매 DApp 시스템

본 장에서는 입찰자 관점에서 부동산 법원 경매절차의 불편사항을 해소하기 위해 이더리움 플랫폼에서 부동산 법원 경매 DApp 시스템을 설계한다.

3.1 DApp 시스템 구성 및 흐름도

부동산 법원 경매 DApp 시스템은 Meta mask의 private key를 통한 경매 참여로 신분증, 인감도장, 인감증명서, 입찰금 등 많은 준비물을 필요로 해야 하는 불편함을 해결할 수 있다. 여기서, Meta mask는 이더리움을 보유하고 송금 및 관리할 수 있는 암호화폐 지갑이다. 참여자들은 블라인드 경매로 참여하기 때문에 군중심리가 매물에 영향을 끼치지 못한다. 기존 시스템의 불편사항을 개선한 부동산 경매 시스템은 Fig. 2와 같다.

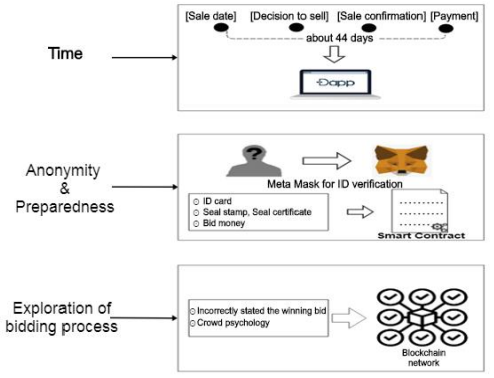

Fig. 2. Improvement of the Court Auction System

법원은 부동산 법원 경매 DApp 시스템에서 블록체인 네트워크의 법원 경매 관리자로서 계정의 정보를 관리하며 블록체인에 스마트 컨트랙트를 배포할 수 있고, 모든 노드들이 열람 및 계약을 확인 할 수 있게 해주는 권한을 가진다. 부동산 법원 경매 DApp 시스템은 6단계로 구성된다.

① 법원에서 매각기일 및 매물의 Meta date를 DApp 브라우저에 등록한다. 즉, 사건번호, 물건번호, 법원명칭, 담당계 명칭, 입찰일자, 등록일자 최초감정가, 최저경매가 등이 등록된다.
② 입찰자는 Meta mask의 Private key를 통해 만들어진 개인의 지갑주소에 접속한다.
③ 입찰자는 원하는 매물을 선택, 입찰가격 금액을 입력하여 경매에 참여한다.
④ 입찰자가 원하는 매물의 state 변화 기록(입찰가격이 가장 높은 입찰자의 기록)을 이더리움 테스트 네트워크에 스마트 컨트랙트로 작성된다.
⑤ 4번째 단계의 스마트 컨트랙트를 포함한 블록을 생성한다.
⑥ 테스트 네트워크에서 작성된 스마트 컨트랙트는 법원 경매 관리자가 블록체인 네트워크의 모든 노드에 배포하고, 블록체인 네트워크의 각 노드들은 열람 및 계약을 확인 할 수 있다.

경매에 유찰된 매물은 다시 최저경매 가에서 20% 감소한 후 관리자는 다시 DApp 브라우저에 등록하여 진행한다. 부동산 법원 경매 DApp 시스템의 구성은 Fig. 3과 같다.

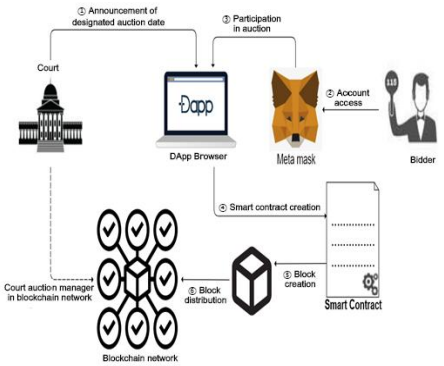

Fig. 3. DApp System Configuration

Meta mask는 User(입찰자)가 DApp 브라우저에서 Meta mask에 계정접속을 하면 본인인증을 통해 계정승인을 한다. User는 승인된 계정을 통해 DApp 브라우저에서 경매에 참여한다. 그리고 경매에 참여할 경우 필요한 ether를 Meta mask를 통해 확인하고 검증을 요구한다. Meta mask는 검증된 ether에 전자서명과 승인을 통해 계약을 진행하게 되며 경매에 참여한 State 정보를 가공하여 스마트계약을 작성한다.

DApp 브라우저에서 스마트 컨트랙트를 EVM에 배포하며 EVM은 부동산 경매에 대한 정보와 스마트 컨트랙트 내용이 들어있는 블록생성 후 이더리움 블록체인에 저장된다. 입찰자는 이더리움 블록체인을 열람 및 계약을 확인할 수 있다. 이와 같은 과정은 Fig. 4와 같다[17].

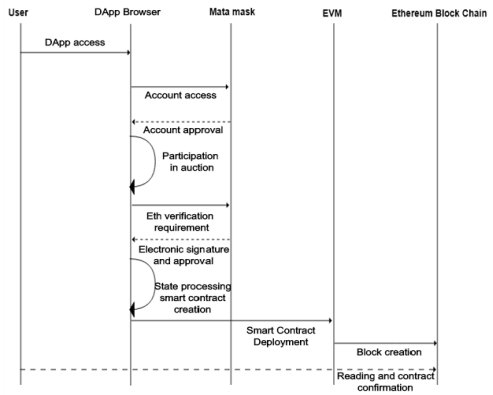

Fig. 4. DApp Flow Chart

3.2 DApp 시스템 구현

부동산 법원 경매 DApp 시스템 S/W 개발환경은 Window 10 Enterprise 현 OS이다. Visual Studio Code가 소스코드를 작성하고, 개발도구 Geth, Node.js, Ganache, Truffle, Meta mask를 사용한다. 시스템 구현을 위해 이더리움 가상머신에 스마트 컨트랙트를 배포하고, 실행은 개발도구를 통해 동작한다. Solidity는 계약 지향 프로그래밍 언어로서 블록체인 플랫폼의 스마트계약 작성 및 구현에 사용된다.

DApp 시스템상의 경매절차는 법원이 DApp 브라우저에 매물에 대한 정보를 등록하고, 경매에 참여할 입찰자는 Meta mask를 통해 법원이 등록한 매물의 정보를 파악 후 경매에 참여한다. 경매과정은 디지털 전자계약을 위해 스마트 컨트랙트를 사용하고, 하나의 매물에는 다수의 입찰자들이 경매를 참여한 정보인 트랜

잭션이 만들어지며 블록이 생성된다. 그러나 하나의 매물에 입찰자가 아무도 없거나 입찰서류 미비 등 사유로 입찰이 무효가 되는 경우에 '유찰'되어 종전 경매가격의 20% 감소한 후 다시 DApp 브라우저에 등록한다. DApp 시스템상의 경매절차는 Fig. 5와 같다.

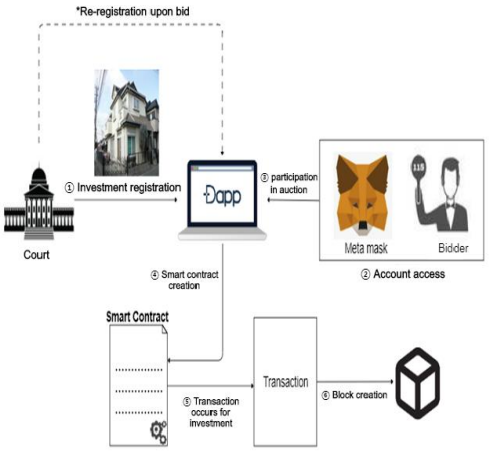

Fig. 5. Auction Procedure on the DApp System

DApp 시스템상의 경매절차는 매물등록, 계정접속, 경매참여, 스마트 컨트랙트 작성, 매물에 대한 트랜잭션 발생, 블록생성 순으로 이루어지며 유찰된 매물은 법원에서 다시 등록한다.

3.2.1 매물등록

관리자(법원)는 매각기일 및 매물의 Meta date에 대한 정보를 DApp 브라우저에 등록한다. 사진과 함께 사건번호, 물건번호, 물건종류, 감정평가액, 최저 경매가, 입찰방법 등을 필요한 정보만 나타내 사용자가 매물에 대한 검색이 쉽다.

3.2.2 계정접속

부동산 법원 경매 DApp 브라우저에 접속을 하면 입찰자는 본인인증을 위해 Meta mask를 통해 로그인 한다. Meta mask를 실행 후 로그인 하게 되면 private key와 연동되어있는 입찰자의 계정과 ether를 가져온다. ether를 입금, 송금을 할 수 있으며 본인 인증하는 과정은 Fig. 6과 같다.

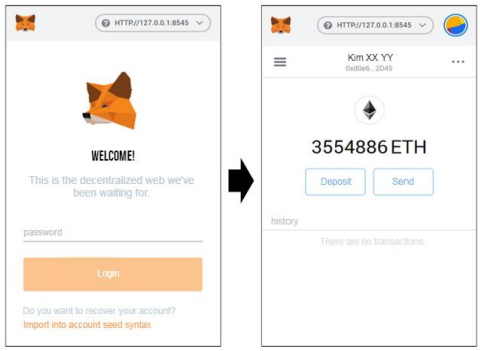

Fig. 6. Meta mask Authentication

3.2.3 경매참여

법원에서 DApp 브라우저에 등록한 정보들은 매입버튼이나 사진 클릭 시 상세 정보가 나타나며 사진, 사건번호, 물건번호, 소재지 및 내역, 비고, 감정평가액, 담당계 매각기일, 최저 매각 가격, 진행상태 정보를 알 수 있다. 입찰 칸에 입찰가격을 넣어 입력해서 입찰에 참가 할 수 있게 한다. 입찰이 진행되면 입찰자가 원하는 매물의 상태 변화 기록을 스마트 컨트랙트로 작성되고, 원하는 매물은 ether로 구매한다.

3.2.4 스마트 컨트랙트 작성

부동산 법원 경매 DApp 시스템의 스마트 컨트랙트는 입찰자 등록, 매물 구매, 블라인드 경매로 구성된다. 스마트 컨트랙트 구성은 Fig. 7과 같다.

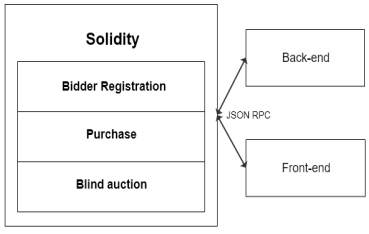

Fig. 7. Smart Contract Configuration

부동산 법원 경매 DApp의 스마트 컨트랙트에는 입찰자 등록(Bidder Registration), 매물구매(Purchase), 블라인드 경매(Blind auction) 순서대로 경매가 진행되며 pseudocode로 나타낸다.

① 입찰자 등록 스마트 컨트랙트

입찰자 등록 스마트 컨트랙트는 입찰자 지갑주소(Bidder)와 지갑주소에 들어있는 ether(Money)를 함께 검증한다. 입찰자 정보는 Bid라 정의하고 검증된 입찰자 지갑주소와 입찰가격(Value)를 묶어 해시 값을 취해 등록한다. 입찰자가 소유하고 있는 ether(Money)와 입력한 입찰가격 ether(Value)를 비교해서 입찰자가 소유하고 있는 ether가 입력한 입찰가격 ether보다 큰 경우에만 True 값으로 정의한다. True 값이 나와야만 거래가 진행되고 매물 구매 스마트 컨트랙트로 넘어간다.

② 매물 구매(Purchase) 스마트 컨트랙트

매물 구매 스마트 컨트랙트는 입찰자 등록 스마트 컨트랙트에서 Bid 정보를 가져오고, 관리자(법원)와 입찰자 주소를 검증한다. DApp 브라우저에서 나타낸 최저 경매가와 입찰자 등록 스마트 컨트랙트에서 검증된 입찰가격을 비교해서 구매여부가 결정된다. 검증된 입찰가격이 최저 경매가보다 크면 True로 정의하고 구매가 진행한다. True 값이 나오면 입찰여부가 확인되면서 관리자에게 ether를 전송 시도하고, 블라인드 경매 스마트 컨트랙트로 넘어간다. 검증된 입찰가격이 최저 경매가 보다 작으면 False로 정의하고 구매 실패가 된다.

③ 블라인드 경매 스마트 컨트랙트

블라인드 경매 스마트 컨트랙트는 경매시간, 입찰시간이 정의되고, 매물구매 스마트 컨트랙트에서 검증된 정보를 가져온다. 매물구매 스마트 컨트랙트에서 검증된 입찰가격과 가장 높은 금액을 제시한 입찰자의 입찰가격을 비교한 후, 검증된 입찰가격이 크면 가장 높은 금액을 제시한 입찰자로 갱신된다. 가장 높은 금액을 제시한 입찰자는 지갑주소, 입찰가격이 해시값으로 나타난다. 입찰과정은 실제로 공개되지 않기 때문에 블라인드 경매가 될 수 있다. 갱신되기 전 가장 높은 금액을 제시한 입찰자는 관리자로부터 ether를 다시 돌려받는다. 입찰에 성공한 가장 높은 금액을 제시한 입찰자의 잠겨있는 ether가 관리자(법원)에게 전송된다.

DApp 브라우저에서 입찰가격 입력 후 입찰버튼을 클릭시 스마트 컨트랙트에서 입찰자의 정보는 지갑주소와 소유하고 있는 ether로 묶여진다. 입찰자 정보는 Bid라 정의하고 해시값을 취해 등록한다. 입찰자가 소유하고 있는 ether와 입력한 입찰가격 ether를 비교해서 입찰자가 소유하고 있는 ether가 입력한 입찰가격 ether보다 큰 경우에만 True 값으로 정의한다. True 값이 나와야만 거래가 진행되고 매물 구매 스마트 컨트랙트로 넘어간다.

매물 구매 스마트 컨트랙트에서는 관리자(법원)와 입찰자 주소를 검증한다. DApp 브라우저에서 나타낸 최저 경매가와 입찰자 등록 스마트 컨트랙트에서 검증된 입찰가격을 비교해서 구매여부가 결정된다. 검증된 입찰가격이 최저 경매가보다 크면 True로 정의하고 구매가 진행한다. True 값이 나오면 입찰여부가 확인되면서 관리자에게 ether를 전송 시도하고, 블라인드 경매 스마트 컨트랙트로 넘어간다.

블라인드 경매 스마트 컨트랙트에서는 경매시간, 입찰시간이 정의된다. 매물 구매 스마트 컨트랙트까지 검증된 입찰가격과 가장 높은 금액을 제시한 입찰자의 입찰가격을 비교한다. 비교해서 검증된 입찰가격이 크면 가장 높은 금액을 제시한 입찰자로 갱신된다. 가장 높은 금액을 제시한 입찰자는 지갑주소, 입찰가격이 해시값으로 나타난다. 입찰시간이 마감했을 때 가장 높은 금액을 제시한 입찰자가 낙찰을 받는다.

④ 매물에 대한 트랜잭션 발생

smart contract를 통해 입찰자가 매물을 구입할 때 발생하는 트랜잭션이 생긴다. 특정 한 매물에 입찰을 진행한 트랜잭션은 Ganache에서 확인 할 수 있으며 Fig. 8과 같다.

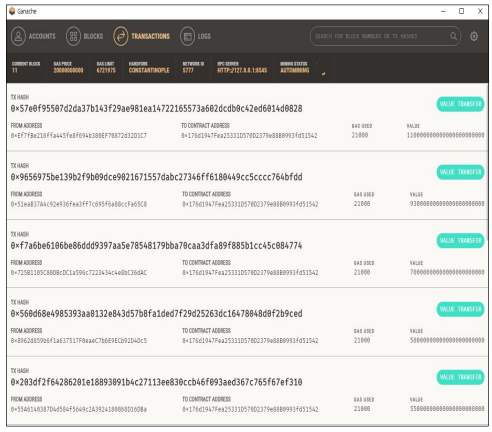

Fig. 8. Transaction at the Auction

⑤ 블록생성

한 매물에 입찰시간 동안 일어난 거래들은 하나의

블록에 담겨 저장된다. Etherscan 사이트를 통해 법원 경매 DApp을 이용하는 모든 이용자들은 정보들을 확인 및 검증할 수 있다. 물건에 입찰자가 아무도 없거나 입찰서류 미비 등 사유로 입찰이 무효가 되는 경우를 '유찰'이라한다. 유찰된 매물은 종전 경매가격의 20% 감소한 후 관리자는 다시 DApp 브라우저에 등록하여 진행한다. 입찰에 성공하면 DApp 브라우저에서 해당 매물은 더 이상 입찰불가하며 경매종료로 나타낸다.

4. 분석

본 장에서는 부동산 법원 경매 DApp 시스템, 오프라인상 부동산 법원 경매, Brik Bit DApp의 성능을 비교 분석한다. 그리고 입찰자 등록, 매물 구매, 블라인드 경매 smart contract Opcode 연산의 개수를 파악하여 Gas 비용을 분석한다.

4.1 성능 분석

기존 오프라인 부동산 법원 경매 시스템은 매물을 시세보다 낮은 가격에 살 수 있고, 수수료가 없다. 하지만 법원에 가야하는 점과 매각기일 직전에 취하, 변경, 연기되는 사례로 매물조사 후 법원에 갔으나 취하 등의 이유로 진행되지 않는 경우 등 시간이 많이 소모되고, 원하는 매물의 정보를 확인하기 위해 매물이 있는 곳에 직접 가야한다는 불편함이 있다. 또한 신분증, 도장, 보증금 등을 준비해야 하며 경매의 정해진 절차를 따라야 한다.

법원에서 진행하는 부동산 경매는 부동산 중개를 통한 거래에 비해 안전하지만 원하는 곳의 매물을 쉽게 구하지 못한다. 그리고 법원 경매에 낙찰된 사람은 보증금 영수증을 받기 때문에 누가 낙찰되었는지 익명성 보장을 받지 못한다.

블록체인과 부동산 시장의 결합한 Brik Bit DApp은 제안한 부동산 법원 경매 DApp과 비슷하지만 부동산 업계에서 전체 시스템을 개발하고 운영, 관리하는 시스템으로 자체적인 BRIK 토큰을 사용하고, 디지털로 표현되는 건물을 구현하기 위해 BIM 프로토콜을 사용해서 매물에 대한 정보를 DApp에서 조사 할 수 있다. 그러나 시세에 맞는 가격으로 매물을 구매해야한다. 또한 부동산 중개와 같이 중개 사고가 생길 여지가 있고, 거래 수수료가 발생하는 점이 있다.

본 논문에서 제안한 부동산 법원 경매 DApp 시스템은 디지털 계약 시스템을 사용하여 시간적 소모를 줄이고, 거래의 복잡성을 단순하게 했다. 그리고 익명성의 문제는 블라인드 경매로 보완했다. 하지만 이더리움의 ether를 사용해서 경매에 참여하기 때문에 ether의 가치의 변화에 따른 매물의 가격이 변할 수도 있다. 또한 이더리움 플랫폼에서 동작하기 때문에 스마트 컨트랙트가 만들어질 때마다 Gas라는 수수료가 발생한다.

Table. 1. Real Estate Transaction Performance Analysis

	Offline a real estate court auction	Real estate a court auction DApp	Brik Bit DApp
Time consuming	consume a lot	consume less	consume less
Sale price	below market price	below market price	same as market price
Transaction complexity	complexity	simple	simple
Type of auction	offline	DApp	DApp
Anonymity	not guaranteed	guaranteed	guarantee
Type of contract	auction	blind auction	online transaction
Sales information	Check it yourself	Check it yourself	Check via DApp
Requirements	identification card, stamp, deposit	Tokens	Tokens
Management type (Stability)	Court-managed (safe)	Court-managed (safe)	There is a possibility of a brokerage accident
fee	none	Fee (Gas) incurred on contract	Fees incurred on transaction

4.2 스마트 컨트랙트 분석

스마트 컨트랙트 분석은 어떻게 구성하느냐에 따라 실행에 소요되는 비용이 다르다. 이더리움 EVM은 스마트 컨트랙트를 컴파일링해서 바이트 코드로 바꾸어 실행하고 처리한다. 실행되는 EVM Opcode (Operation Code)마다 각각의 가스비가 정해져 있다. Opcode가 많이 구성되어 있을 경우 스마트 컨트랙트를 실행하는데 소요되는 비용이 증가한다. 즉 개발자가 작성한 smart contract가 어떻게 구성되는지 따라 실행에 필요한 가스비가 달라진다. 가스는 수수료와 같으며 다른 계정에 돈을 보내거나, 스마트 컨트랙트를 배포할 때, 함수에서 상태 변수에 변화를 줄 때 등이 있다. EVM의 실행과정은 Fig. 9와 같다.

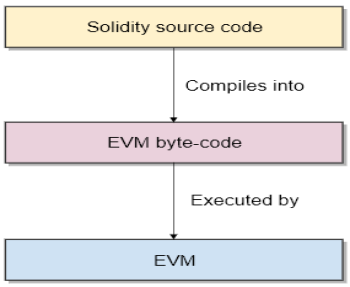

Fig. 9. EVM Execution Process

Opcode는 정지 및 산술 연산, 비교 및 비트 논리 연산, SHA3, 환경정보, 블록정보, (스택, 메모리, 스토리지) 흐름 작업, 푸시 작업, 복제 작업, Exchange 운영, 로깅 작업, 시스템 작동, 실행 중지 및 삭제로 분류된다.

부동산 법원 경매 DApp 시스템 분석을 위해 입찰자 등록, 매물 구매, 블라인드 경매~ 스마트 컨트랙트를 각각 컴파일링하여 바이트 코드로 변환한다. 변환된 바이트 코드는 디코딩한다. 바이트 코드를 디코딩하는 이유는 Opcode 연산을 분석하기 위해서이다. 입찰자 등록, 매물 구매, 블라인드 경매 smart contract Opcode 연산의 개수를 파악하여 Gas 비용을 분석한다.

4.2.1 입찰자 등록 스마트 컨트랙트

부동산 법원 경매 DApp 시스템에 사용된 입찰자 등록 스마트 컨트랙트를 바이트 코드로 변환한다. 변환한 바이트 코드는 디코딩한다. 입찰자 등록 smart contract Opcode의 사용횟수는 796개이고 가장 많이 사용된 상위 5개의 Opcode는 PUSH, DUP, SWAP, POP, JUMPDEST이다. Gas 비용이 비싼 저장연산 SSTORE를 12번 사용했다. Opcode의 개수로 나타낸 결과는 Fig. 10과 같다.

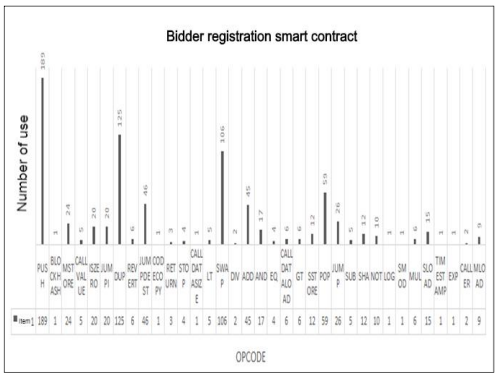

Fig. 10. Number of Bidder Registration Opcodes

4.2.2 매물 구매 스마트 컨트랙트

매물 구매 스마트 컨트랙트를 바이트 코드로 변환한다. 변환한 바이트 코드는 디코딩한다. 매물 구매 smart contract Opcode의 사용횟수는 840개 이며 가장 많이 사용된 상위 5개의 Opcode는 PUSH, DUP, SWAP, JUMPDEST, ISZERO이다. Gas 비용이 비싼 저장연산 SLOAD를 23번 SSTORE를 8번 사용했다. 계정의 잔액을 얻는 BALANCE를 2번 사용했고, 호출을 사용해서 새 계정 생성하는 CALL은 3번 사용했다. Opcode의 개수로 나타낸 결과 Fig. 11과 같다.

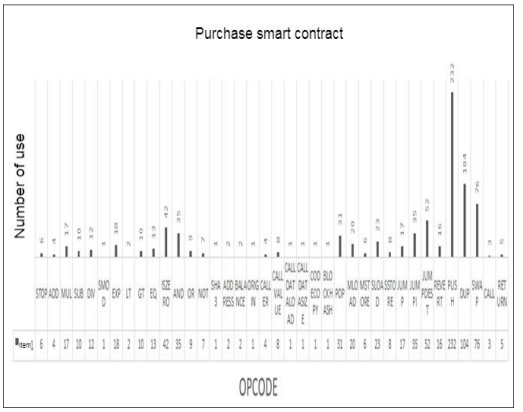

Fig. 11. Purchase Opcode Count

4.2.3 블라인드 경매 스마트 컨트랙트

블라인드 경매 스마트 컨트랙트를 바이트 코드로 변환한다. 변환한 바이트 코드는 디코딩한다. 블라인드 경매 smart contract Opcode의 사용횟수는 1704개 이며 가장 많이 사용된 상위 5개의 Opcode는 PUSH, DUP, SWAP, POP, ADD이다. Gas 비용이 비싼 저장연산 SLOAD를 35번 SSTORE를 14번 사용했다. 호출을 사용해서 새로운 계정을 생성하는 CALL은 3번 사용했다. Opcode 디코딩 한 결과 Fig. 12와 같다.

입찰자 등록, 매물구매, 블라인드 경매의 smart contract Opcode는 평균적으로 PUSH, DUP, SWAP, POP Opcode가 많이 사용되었고, Gas 가격이 비싼 SLOAD와 SSTORE, BALANCE, CALL Opcode도 많이 사용되었다. Opcode의 가격 측정은 스마트 컨트랙트를 배포할 때와 스마트 컨트랙트의 함수를 사용할 때로 구분된다. Gas 비용을 줄이기 위해 불필요한 코드 정리, 연산 줄이기, 불필요한 반복문 축소, string 대신 byte32로 사용해서 Gas량을 줄일 수 있다.

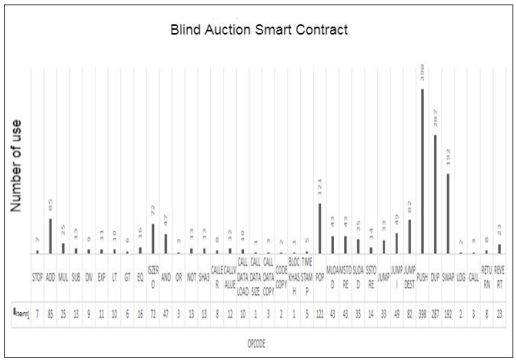

Fig. 12. Blind Auction Opcode Count

5. 결론

최근 블록체인 기술이 다양한 분야에서 관심을 받고 있는 가운데 스마트 컨트랙트와 DApp 기술 연구가 증가하고 있다. 특히, DApp 기술은 블록체인에서 실행되는 탈 중앙화된 어플리케이션으로 참여자 간의 계약 이외의 다양한 응용서비스 제공, 블록체인에서 분산되어 실행되고, 스마트 컨트랙트를 포함한 인터페이스로 여러 분야에서 적용되어 만들어지고 있다. 본 논문에서는 DApp 기술을 오프라인상의 법원 경매의 불편사항 등을 온라인으로 보완하여 입찰자가 법원에 가지 않고도 경매에 참여할 수 있으며 이더리움 플랫폼에서 부동산 법원 경매 DApp으로 제안했다.

제안 모델은 오프라인상의 법원 경매의 불편사항을 해소하기 위해 과도한 시간적 소요를 디지털 전자계약으로 해소했고, Meta mask를 이용해 인증을 간소화한다. 또한 법원이 관리하는 블록에서 안정성을 유지하고, 입찰자 지갑주소와 입찰가격 등에 해시 값을 취함으로서 블라인드 경매 형태로 익명성을 보완한다. 부동산 법원 경매 DApp 성능과 스마트 컨트랙트 분석 결과, 이더리움 플랫폼에서 동작하기 때문에 이더리움 지갑을 생성해야 하고, 이더리움의 ether를 사용해서 경매에 참여하기 때문에 ether의 가치의 변화에 따라 매물의 가격에 영향을 끼치며 스마트 컨트랙트가 작성될 때마다 수수료가 생기는 단점이 있다. 또한 오프라인 부동산 경매와 마찬가지로 매물의 세밀한 정보는 직접 가서 확인해야 하는 번거로움이 있다.

향후 연구에서는 ether가 아닌 자체 토큰을 만들어 ether의 가치의 변화에 따른 시세 변동성 문제와 수수료 문제를 해소하며 향후 복잡하고 정밀한 법원 경매 시스템을 세분화하여 온라인상에서 불편함 없이 경매를 진행할 계획이다.

REFERENCES

[1] E. S. Kang. (2019). Blockchain Finance. *The Korean Institute of Communication Sciences, 36(7)*, 3-9.

[2] Gartner. (2019). *Top 10 Strategic Technology Trends for 2019.*

[3] Korean court auction information. (n. d.) (Online). https://www. courtauction.go.kr/

[4] H. N. Yim, B. K. Kim & S. W. Shin. (2018). The Estimation and Prediction of the Duration of Residential Property through Court Auction. *The Korea Appraisal Society, 17(3)*, 109-127. DOI : 10.23843/as.17.3.6

[5] H. W. Park & K. B. Nam. (2011). Analysis of effect given by lien to difference between appraised value and winning bid in court auction for real estate. *The Journal of Korean Policy Studies, 11(3)*, 123-140.

[6] B. S. Noh & S. S Shin. (2019). Real Estate Court Auction System using DApp. T*he Korea Institute of Information and Communication Engineering, 23(2)*, 57-59

[7] S. J. Kim. (2018). *Cryptocurrency & Blockchain.* Center for High-Assurance Operating Systems

[8] H. J Kim. (2017). *Blockchain.* ETRI

[9] K. H. Han & S. O. Hwang. (2018). Introduction of Blockchain. *Communications of the Korean Institute of Information Scientists and Engineers, 36(12),* 11-16.

[10] H. J. Shin & J. P. Yoo. (2018). Blockchain Technologies and Applications. *Korea Institute of Enterprise Architecture, 15(3)*, 357-364.

[11] Y. W. Lee, H. Y. Kim, C. G. Kim, & J. S. No. (2018). On Cryptographic Primitives for Blockchain. *Communications of the Korean Institute of Information Scientists and Engineers, 36(12)*, 17-22.

[12] P. J. Lee. (1996). Hash- functions using an n-bit block cipher algorithm. *Korea Institute Of Information Security And Cryptology*, 79-88.

[13] Merkle Ralph. (1987). *A digital signature based on a conventional encryption function.*

[14] https://bitcoin.org/en/

[15] https://ko.wikipedia.org/wiki/

[16] http://terms.tta.or.kr/main.do

[17] H. S. Choi, H. J. Kim, J. Y. Lee & S. S. Shin. (2020). A study on the Auction System using Smart Contract. *Korea Multimedia Society, 23(2).*

김 효 종(Hyo-Jong Kim) [정회원]

· 2016년 2월 : 동명대학교 정보보호학과(공학사)
· 2017년 2월 ~ 현재 : 동명대학교 컴퓨터미디어공학과 석사과정
· 관심분야 : 웹 크롤링, 빅데이터 분석, 네트워크 보안
· E-Mail : khj47561404@gmail.com

한 군 희(Kun-Hee Han) [종신회원]

· 2008년 8월 ~ 현재 : 백석대학교 정보통신공학부 교수
· 관심분야 : 멀티미디어, 유비쿼터스, DB보안, 암호 프로토콜/알고리즘
· E-Mail : hankh@bu.ac.kr

신 승 수(Seung-Soo Shin) [정회원]

· 2001년 2월 : 충북대학교 수학과 (이학박사)
· 2004년 8월 : 충북대학교 컴퓨터공학과(공학박사)
· 2005년 3월 ~ 현재 : 동명대학교 SW융합보안학과 교수
· 관심분야 : 암호프로토콜, 네트워크 보안, U-헬스 케어, IoT, 데이터분석
· E-Mail : shinss@tu.ac.kr