https://doi.org/10.14400/JDC.2017.15.8.203

블록체인을 활용한 국민주택채권 정보 중계시스템 개선방안 연구

남진석*, 양해술**
호서대학교 벤처대학원 정보경영학과 박사과정*, 호서대학교 벤처대학원 교수**

A Study on Improvement of Housing Bond Information Relay System Using Blockchain

Jin-Seok Nam*, Hae-Sool Yang**
Dept. of Information Management, Graduate School of Venture, Hoseo University*, Graduate School of Venture, Hoseo University, Professor**

요 약 국민주택채권 정보 중계시스템은 관련된 여러 기관들이 중계센터를 중심으로 연결된 대표적인 금융정보 중계시스템이다. 이러한 중앙 집중형 구조는 중계센터 구축 및 운영에 막대한 비용이 소요되고, 센터시스템에 장애나 사고가 발생할 경우 모든 네트워크가 단절되는 문제점이 존재한다. 본 논문에서는 블록체인 기술을 활용하여 안전하고 효율적으로 정보를 처리할 수 있는 블록체인 기반의 국민주택채권 정보 중계시스템 모델을 제안한다. 제안 모델은 국민주택채권 정보를 처리하는 각 기관들이 안전하게 정보를 전송할 수 있도록 블록체인 네트워크를 구성하고, 스마트 컨트랙트 기반의 분산 어플리케이션으로 동일한 분산원장을 관리한다. 제안 모델은 중계센터 없이 복잡한 국민주택채권 거래 정보를 처리할 수 있어 비용을 절감할 수 있으며 기존 시스템 대비 네트워크 사용률의 1.7%, 디스크 사용률의 8.53%의 개선 효과가 있다.

주제어 : 블록체인, 분산원장, 스마트 컨트랙드, 금융정보 중계시스템, 국민주택채권, 국민주택채권 정보 중계시스템

Abstract The National Housing Bond Information Relay System is a representative financial information relay system in which institutions are connected with center system. A centralized structure is expensive to construct and operate center, and there is a problem that all networks are disconnected when a failure occurs in the center system. In this paper, we propose the national housing bond information relay system model based on Blockchain technology that can process information safely and efficiently. The proposed model constructs a Blockchain network so that each institution that processes the national housing bond information can transmit information safely, and each institution manages the same distributed ledge by a smart contract. The proposed model can reduce the cost because it can process complicated national housing bond transaction information without a relay center, and a network usage and disk usage decreased by 1.7% and 8.53%.

Key Words : Blockchain, Distributed Ledger, Smart Contract, Financial Information Relay System, Housing Bond, Housing Bond Information Relay System

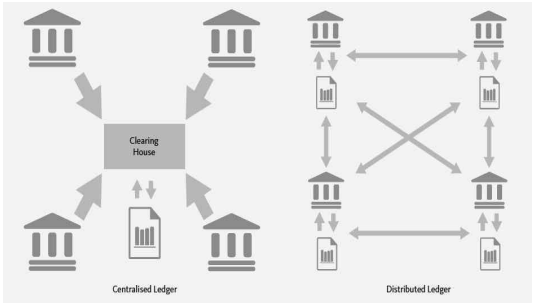
Received 21 June 2017, Revised 24 July 2017
Accepted 20 August 2017, Published 28 August 2017
Corresponding Author: Hae-Sool Yang
(Graduate School of Venture, Hoseo University)
Email: hsyang@hoseo.edu

ISSN: 1738-1916

1. 서론

블록체인은 신뢰할 수 있는 제 3자(TTP : Trusted Third Party) 없이 금융거래를 수행하는 비트코인의 핵심 기술로서[1] 최근 전 세계적으로 핀테크 열풍과 함께 IT기술로서는 유래를 찾아보기 힘들 정도로 매우 높은 관심을 받고 있다. 블록체인 기술을 활용하면 거래 참가자들이 중계센터를 거치지 않고 직접 거래정보를 전달할 수 있기 때문에 중계센터 구축·유지 비용을 절감할 수 있으며 모든 참가자들이 동일한 원장을 보유하기 때문에 해킹 등 보안에 상대적으로 안전하다[1,2].

이러한 잠재적 가치가 있는 블록체인 기술에 JP모건 체이스, 시티그룹 등 글로벌 금융회사를 중심으로 구성된 R3CEV와 IBM, 시스코, Ripple 등 IT기업을 중심으로 구성된 Hyperledger 등 여러 컨소시엄이 구성되고 공동 블록체인 시스템 개발 및 표준화에 연구와 투자를 확대하고 있다. 국내에서도 금융위원회를 중심으로 블록체인 협의회를 구성하고 금융권 공동 블록체인 컨소시엄을 운영하여 효율적인 공동연구 및 파일럿 프로젝트 등을 추진하고 있다.



[Fig. 1] Centralised and distributed ledgerapproaches[3].

글로벌 금융회사의 블록체인 컨소시엄은 금융회사 간 금융거래에 블록체인을 활용하여 빠르고 안전하게 자금을 거래하는 것에 초점을 맞추고 있고, IT회사 중심의 컨소시엄은 기존 시스템에 분산원장 기술을 쉽게 도입하는 방법을 찾기 위한 프로젝트를 진행하고 있다. 국내 금융권 공동 블록체인 컨소시엄은 인증, 자금이체, 무역거래에 블록체인을 활용하는 방안을 검토 중이다.

이와 같이, 여러 컨소시엄이 미래 블록체인 시장에서의 주도권을 잡기 위하여 다양한 연구를 진행하고 있으나, 금융 전산시스템의 많은 부분을 차지하고 있는 금융정보 중계시스템에 대한 블록체인 활용 방안에 대해서는 연구가 미진한 편이다.

국민주택채권 정보 중계시스템은 국민주택채권 유관기관 간 국민주택채권 거래 내역이 중계시스템을 경유하여 전달되는 대표적인 중앙 집중형 금융정보 중계시스템이다. 거래의 종류가 다양하고, 유관기관의 성격에 따라 처리할 수 있는 권한이 다르며, 처리결과에 따라 국민주택채권 정보와 상태가 순차적으로 변경되는 등 자금이체와 같은 일반적인 금융거래와는 처리절차가 상이하다.

국민주택채권 정보 중계시스템과 같이 중계센터 중심의 중앙 집중형 시스템 구조는 절차가 단순하고 개발 및 유지보수가 용이하나 해킹, 시스템 장애 등의 사유로 중계시스템이 서비스를 정상적으로 제공할 수 없을 경우 참가기관 전체의 서비스가 중지될 수 있다. 따라서, 각종 보안 관련 장비 및 S/W를 구입하고 중계서버를 이중화하며 원격지에 재해복구시스템을 구축하여 주기적으로 전환 훈련을 하는 등 중계센터를 구축하고 관리하는데 막대한 인적·물적 비용을 투입하고 있다.

본 논문은 블록체인의 특성 및 관련 기술을 활용하여 분산원장 기반의 국민주택채권 정보 중계시스템 모델을 제안한다. 제안 모델은 중계센터 비용을 절감하고, 거래에 대한 안정성을 확보하며, 성능을 향상시키는데 목적이 있다.

2. 관련연구

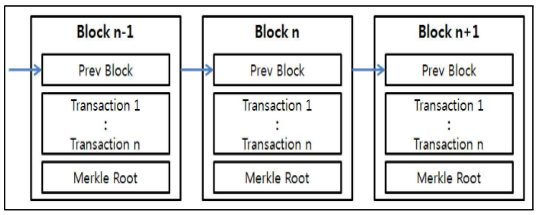
2.1 블록체인

블록체인(Blockchain)은 2008년 사토시 나카모토의 논문 '비트코인 : 개인간 전자화폐 시스템(Bitcoin : A Peer-to-Peer Electronic Cash System)' 에서 P2P(Peer-to-Peer) 방식으로 전자통화를 거래할 때 발생할 수 있는 이중지불(Double-Spending) 문제를 해결하기 위한 솔루션으로 제안된 분산원장(Distributed Ledger) 기술이다[2].

블록체인 네트워크의 모든 참가자에게 거래 내역이 공개되고 거래의 유효성에 대해 공동으로 검증하여 최종적으로 동일한 원장을 공유하게 된다. 이러한 블록체인의 특징 때문에 블록체인을 공공장부(Public Ledger)라

부르기도 한다[4]. 즉, 블록체인 기반의 거래 내역은 특정한 중앙 집중형 서버에 기록하여 보관하는 것이 아니라 모든 참가자가 각각 저장하고 관리한다. 또한, 분산형 시점기록(TimeStamp) 서버를 통해 각 거래들의 순서를 보장하고 이중지불 문제를 해결한다[5]. 이 방법은 거래 유효성 검증에 충분한 시간이 필요하다는 단점이 있지만 정직한 노드의 CPU 성능 총량이 동일한 공격을 하는 악의적 노드의 CPU 성능 총량 보다 높은 경우 안전하다고 할 수 있다[2,6]. 이와 같이, 블록체인은 네트워크 참가자들의 공공장부를 기반으로 신뢰할 수 있는 제 3자 없이 인터넷 공간에서 발생하는 거래에 대하여 기술적으로 신뢰성을 확보할 수 있는 전자결제시스템을 구축할 수 있다[7]. 비트코인, 이더리움과 같이 일부 참가자의 시스템에 문제가 발생하여도 전체 네트워크에는 크게 영향을 미치지 않는다[8].

블록체인은 다른 분산원장 기술과 차별화된 2가지 핵심 기술로 구성된다. 첫째, 각각 독립된 거래내역을 포함하고 있는 블록을 생성하고 생성된 블록을 시간 순으로 연결하여 순서를 보장하는 기술이다. 각 블록의 순차적 연결을 위하여 암호학적 해쉬(Hash) 함수로 생성한 직전 블록의 해쉬 값을 뒤에 연결되는 블록에 기록한다[2,9]. 이와 같이 직전 블록의 해쉬 값을 사용하여 블록을 시간 순서대로 연결함으로써 블록의 위·변조를 방지하는 것을 체이닝(Chaining) 기술이라 한다[10].



[Fig. 2] A Chain of Blocks

둘째, 거래의 유효성을 증명하기 위한 참가자들 간의 동의·합의 기술이다. 블록체인은 신뢰할 수 없는 다수의 참가자 간의 거래의 신뢰성을 보장하여야 한다는 문제가 있다. 이러한 문제를 '비잔틴 장군 문제'(Byzantine generals problem)라 한며[11], 익명의 상대방과 금융거래를 하기 위해서는 신뢰성을 기술적으로 보장하기 위한 방법이 반드시 필요하다. 사토시 나카모토는 그의 논문에서 비트코인 거래의 신뢰성을 확보하기 위해 참가자의 과반수 이상이 동의하여야만 유효한 거래로 인정되는 작업증명(PoW : Proof of Work) 알고리즘을 제안하였다.

현재에는 작업증명 알고리즘 외에도 지분증명(PoS : Proof of Stake), 소유증명(PoS : Proof of Take), 중요도증명(PoI : Proof of Importance), 비잔티움 장애허용(BFT : Byzantine Fault Tolerance) 등의 알고리즘[8,10]이 많이 사용되고 있으며 계속해서 새로운 방법이 개발되고 있다.

블록체인은 참가자의 범위, 네트워크 성격 등에 따라 퍼블릭 블록체인(Public Blockchain)과 프라이빗 블록체인(Private Blockchain), 컨소시엄 블록체인(Consortium Blockchain)의 3가지 유형으로 구분된다. 퍼블릭 블록체인(Public Blockchain)은 비트코인, 이더리움과 같이 누구나 블록체인 네트워크에 참가할 수 있는 공개형 블록체인으로 서비스 대상자의 확대가 쉬운 장점이 있는 반면 거래 검증에 충분한 시간이 필요하기 때문에 사용자가 요청하는 즉시 거래가 처리되어야하는 일반적인 금융서비스에는 적합하지 않다[12]. 프라이빗 블록체인은 하나의 기관에서 내부적으로 사용하는 블록체인이다. 정보의 소유자만 정보에 대한 모든 접근 및 관리 권한을 가지는 구조이므로 비잔티움 장애허용(BFT : Byzantine Fault Tolerance) 등 속도가 빠른 합의 알고리즘을 사용한다. 컨소시엄 블록체인(Consortium Blockchain)은 허가받은 참가자들로만 네트워크가 구성되고 각 참가자들은 부여된 권한만 사용할 수 있기 때문에 퍼블릭 블록체인과 프라이빗 블록체인의 중간 형태라 할 수 있다. 따라서, 퍼블릭 블록체인과 같이 분산된 구조를 유지하면서 참가자들의 권한을 제어할 수 있다는 것이 특징이다. 컨소시엄 블록체인을 구성하는 각 노드는 접근 권한을 허가받은 참가자로 구성되기 때문에 프라이빗 블록체인(Private Blockchain)과 마찬가지로 비잔티움 장애허용(BFT : Byzantine Fault Tolerance) 등의 속도가 빠른 합의 알고리즘을 사용한다.

2.2 스마트 컨트랙트(Smart Contract)

스마트 컨트랙트는 Nick Szabo가 1994년 제안한 개념으로 계약 시 합의된 조건 및 수행 내용을 프로그램 코드로 작성하고 계약 체결과 동시에 프로그램 코드 상의 수행 내용이 자동으로 실행되는 것을 말한다. 스마트 컨트

랙트는 비트코인에도 적용되어 있으며 이를 비트코인 스크립트라 한다[13]. 비트코인에서 제공하는 스크립트는 비트코인 거래로 기능이 제한되어 있으나[14], 비트코인을 개선한 모델인 이더리움은 프로그램 코드를 실행할 수 있는 컴파일러가 내장되어 있으므로, 이더리움에서는 계약의 수행을 위하여 다양한 프로그램을 만들 수 있다[15,16].

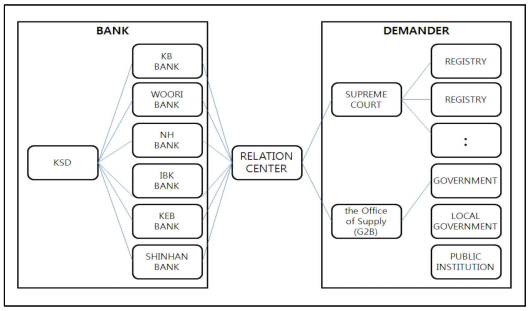
이와 같이 블록체인 네트워크에서 스마트 컨트랙트를 활용하면 비트코인과 같은 화폐 대신 프로그램 코드 형태의 데이터를 전송하고 계약된 조건 충족 시 프로그램 코드를 강제적으로 실행하여 그 결과를 확인할 수 있다[17], 스마트 컨트랙트 프로그램 코드는 블록체인의 거래 데이터와 동일하게 처리되므로 데이터를 임의로 조작하기 매우 어렵다. 따라서, 블록체인 기반의 스마트 컨트랙트 기술은 거래내역뿐 아니라 프로그램 코드에 대해서도 동일한 수준의 안정성을 제공한다[18].

3. 국민주택채권 정보 중계시스템

국민주택채권이란 무주택 서민들에게 주택을 공급할 목적으로 국민주택사업에 필요한 국민주택기금을 조달하기 위하여 주택도시기금법 제 7조, 제 8조, 동법시행령 제4조 내지 제 11조와 국채법에 의거 정부에서 발행하는 국채이며, 「주택도시기금법」 제 8조 및 동법 시행령 제 8조 에서 정한 해당 면허의 인・허가 또는 등기・등록을 신청하는 자, 국가・지방자치 단체 및 공공기관과 건설공사의 도급계약을 체결하는 자 등이 의무적으로 매입하여야 하는 첨가소화형 채권이다. 과거에는 무기명 실물채권으로 발행하였으나 무기명 채권의 특성상 편법 증여・상속 등 불법적으로 활용될 수 있어 이를 방지하기 위하여 2004년 4월에 전자발행 방식으로 변경되었다. 또한 용도에 따라 제 1종, 제 2종, 제 3종 국민주택채권으로 구분하던 것이 폐지 및 기능 통합되어 현재는 제 1종 국민주택채권 이외에는 신규 발행이 중지되었다. 국민주택채권은 유가증권이므로 발행 목적을 위한 고유 기능 이외에 할인, 양도 등 증권으로서의 일반적인 성격도 갖고 있으나 본 논문에서는 다루지 않는다.

3.1 네트워크 구성

국민주택채권 유관기관은 [Fig. 3]과 같이 국민주택채권 발행기관, 국민주택기금 취급은행, 징구기관 및 중계센터로 구성되어 있으며, 본 논문에서는 국민주택기금 취급은행에서 국민주택채권 발행 업무를 대행하고 있으므로 국민주택채권 발행기관과 국민주택기금 취급은행을 분리하지 않고 발행은행으로 통칭한다. 징구기관은 등기, 인・허가, 도급계약 시 국민주택채권 매입 여부를 정상적으로 매입하였는지를 확인하는 등기소, 조달청 등을 말한다.



[Fig. 3] Map of Housing Bond Information Relay System

3.2 국민주택채권 정보

국민주택채권 정보는 기본정보와 상태정보 2가지로 구성되어 있으며, 기본정보는 최초 국민주택채권을 발행(매입)할 때 확정되는 채권발행번호, 채권발행고객명, 주민등록번호(또는 사업자번호), 등기용 등록번호, 매입목적, 발행일자, 매입금액, 징구기관코드, 상호명, 발행은행코드, 발행은행 지점명, 발행은행 지점 담당자명, 발행은행 지점 전화번호, 채권과세구분코드, 매출일자 등의 발행정보와 등기소 등에서 사용될 때 확정되는 등기소코드, 등기소명, 접수일련번호, 담당공무원번호, 담당자전화번호, 미사용금액, 접수일자, 접수번호, 처리접수부번호, 등기유형, 담당계 등의 사용정보로 나누어진다. 상태정보는 특정 시점에서 채권의 상태를 나타내며 발행, 발행취소, 사용중, 사용완료, 환급완료 등이 있다.

3.3 처리절차

국민주택채권의 일반적인 처리절차 다음과 같다. 매입자가 등기・도급계약 등을 위해 발행은행에 국민주택채

권 매입을 요청하면 발행은행은 국민주택채권을 전자적으로 발행하고 해당 정보를 중계센터 앞으로 전송한다. 중계센터는 해당 채권의 정보를 확인하여 이상이 없을 경우 대상 징구기관 앞으로 전달하며, 최종적으로 징구기관에서 채권을 사용하여 목적을 달성한다. 가장 많이 발행되고 있는 주택 등기를 예로 들면, 등기소에서 주택 등기를 할 경우 등기 신청서가 적합하고 각하할 사유가 없으면 등기부에 등기원인, 등기원인일자, 등기의무자, 등기권리자 정보와 신청사건 유형별 필요기재사항을 등기부에 '기입' 하고, 등기관은 신청서와 부속서류를 검토하여 신청 내용 및 등기부의 기재에 착오가 없는지 다시 한 번 확인한 후 이상이 없을 경우 '교합' 처리하여 등기를 완료한다. 등기부에 기입 완료 시 국민주택채권은 사용중(Using) 상태가 되고 교합까지 완료하면 사용완료(Used) 상태가 된다. 이러한 업무 절차에 따라 발행은행은 발행, 변경, 취소, 환급, 환급취소의 5가지 상태를 처리하고 징구기관은 사용중, 사용중취소, 사용완료, 사용완료취소의 4가지 상태를 처리한다. 전산시스템에서는 각 상태에 따라 다음과 같이 단계별로 처리한다.

첫째, 국민주택채권이 신규로 발행되면 발행은행은 국민주택채권 기본정보 및 발행 상태정보를 징구기관 앞으로 전송한다. 징구기관은 발행에 대한 오류처리는 할 수 없으며 수신된 정보를 저장한다.

둘째, 발행은행은 국민주택채권 매입자의 요청에 의해 일부 정보를 변경할 수 있으며 변경되는 정보를 포함한 기본정보와 변경 상태정보를 징구기관 앞으로 전송한다. 징구기관은 국민주택채권이 변경 가능한 상태인지 확인 후 이상이 없으면 변경 처리 후 변경완료 상태를 발행은행 앞으로 전송한다.

셋째, 발행은행은 국민주택채권 매입자의 요청에 의해 기 발행된 국민주택채권을 발행취소 할 수 있으며 발행취소 상태를 징구기관 앞으로 전송한다. 변경과 마찬가지로 징구기관은 국민주택채권이 취소가 가능한 상태인지 확인 후 이상이 없으면 발행취소 처리 후 취소완료 상태를 발행은행 앞으로 전송한다.

넷째, 징구기관은 등기・계약 등 요청이 접수되면 기 발행된 채권을 사용할 수 있으며, 국민주택채권 사용정보와 사용중상태를 발행은행 앞으로 전송한다. 발행은행은 수신된 정보를 저장하며, 사용중인 채권은 정보 변경 및 발행취소 처리를 할 수 없다.

다섯째, 등기・계약 과정에서 서류 미비 등의 사유로 절차가 취소된 경우 국민주택채권의 사용중 상태를 취소하며, 발행은행 앞으로 사용중취소 상태정보를 전송한다. 발행은행은 사용중취소 상태를 수신하면 국민주택채권을 발행완료 상태로 변경한다.

여섯째, 징구기관에서 등기・계약이 정상적으로 완료되면 사용완료 상태정보를 발행은행 앞으로 전송한다. 사용완료된 채권은 정보 변경 및 발행취소 처리를 할 수 없다.

일곱째, 사용완료된 채권에 대해 사후 문제가 발생한 경우 징구기관은 사용완료 상태를 취소하며, 발행은행 앞으로 사용완료취소 상태정보를 전송한다. 발행은행은 사용완료취소 상태를 수신하면 국민주택채권을 발행완료 상태로 변경한다.

여덟째, 사용완료된 국민주택채권에 미사용금액이 있는 경우 발행은행은 매입자의 요청에 의해 환급 처리를 할 수 있으며 징구기관 앞으로 환급금 정보를 포함한 기본정보와 환급 상태정보를 전송한다. 징구기관은 환급완료된 채권은 사용완료취소 처리를 할 수 없다.

아홉째, 발행은행에서 환급이 완료된 국민주택채권에 대해 매입자가 요청할 경우 환급취소를 할 수 있으며 징구기관 앞으로 환급취소 상태 정보를 전송한다. 환급취소가 완료되면 국민주택채권은 사용완료 상태가 된다.

4. 블록체인 기반의 국민주택채권 정보 중계시스템 개선 모델

본 논문에서는 처리 절차가 가장 복잡한 주택 등기를 위한 국민주택채권 거래를 처리하는 것으로 가정한다. 등기부 등의 장부에 기입하는 절차가 없어 사용중 상태가 없는 도급계약은 등기를 위한 국민주택채권 정보 처리가 가능하다면 발행된 채권이 사용중 상태를 거치지 않고 사용완료될 수 있도록 약간의 조건 변경만으로 처리가 가능하다.

제안 모델은 국민주택채권 유관기관 간 표준화된 블록체인 네트워크 구성, 네트워크 참가기관 시스템에 설치되어 자율적으로 작동하는 스마트 컨트랙트 기반의 분산 어플리케이션(Distributed Application) 및 각 네트워크 참가기관이 공유하는 블록체인 기반의 국민주택채권 정보 분산원장의 세 가지 요소로 구성된다.

4.1 블록체인 네트워크 구성

국민주택채권은 지정된 발행은행과 징구기관에서만 매입 및 사용이 가능하기 때문에 제한된 기관만이 블록체인 네트워크의 참여자가 될 수 있다. 또한, 발행은행과 징구기관 간 국민주택채권 정보가 매우 신속하게 전달되어야 하므로 퍼블릭 블록체인(Public Blockchain)보다는 컨소시엄 블록체인(Consortium Blockchain) 구조가 적합하다. 따라서, 본 논문에서는 발행은행, 징구기관 및 네트워크 리더로 구성된 국민주택채권 컨소시엄 블록체인 모델을 제안한다[19]. 네트워크 리더는 별도로 분리하거나 참가기관 중 하나 또는 다수가 리더 역할을 수행할 수 있다. 블록체인 네트워크에 발행은행과 징구기관이 참가하기 위해서는 네트워크 리더로부터 승인을 득하고 권한을 위임 받아야 하며 그 과정은 다음과 같다.

① 네트워크 리더로부터 참가 승인을 득한 발행은행 및 징구기관은 스마트 컨트랙트 기반의 국민주택채권 정보 중계시스템 플랫폼을 다운로드 받아 내부 시스템에 설치한다.

② 발행은행 및 징구기관은 해당 기관 정보를 네트워크 리더 앞으로 전송한다. 전송하는 정보는 참가기관(발행은행 및 징구기관)의 필요 권한, 기관명 등 기관정보, 네트워크 리더로부터 받은 승인코드 및 공개키 등이 있으며, 참가기관의 전자서명을 포함하여 네트워크 리더의 공개키로 암호화하여 전송한다. 참가기관들은 자신의 주소로 공개키, 공개키의 해쉬값 또는 별도의 ID를 사용할 수 있으며 참가기관의 요청에 의해 네트워크 리더가 승인한다.

③ 네트워크 리더는 참가기관으로부터 정보를 수신하면 오류 여부를 검증한 후 이상이 없을 경우 현재 참여하고 있는 참가기관의 정보 및 공개키 등을 네트워크 리더의 전자서명을 포함하여 참가 요청 기관의 공개키로 암호화하여 전송한다.

4.2 스마트 컨트랙트 기반의 국민주택채권 정보 중계시스템 플랫폼

제안 모델의 국민주택채권 정보 중계시스템 플랫폼은 참가기관이 네트워크 리더로부터 제공받아 내부 시스템에 설치하는 분산 어플리케이션으로서 자체적으로 블록체인 네트워크에 연동하여 동작하는 응용 프로그램이다. 분산 어플리케이션은 관리자(Admin Layer), 블록체인 엔진(Blockchain Engine Layer), 인터페이스(Interface Layer)의 세 가지 계층으로 구성되며 비트코인과 마찬가지로 JSON(Javascript Object Notation)[] 형식으로 데이터 객체를 생성하여 전송한다.

각 계층 역할을 세부적으로 살펴보면 다음과 같다. 관리자 계층은 블록체인 네트워크에 접속하고, 네트워크 리더로부터 참가 승인을 요청하며 거래 권한 획득 및 타 참가기관의 정보와 버전을 관리한다. 블록체인 엔진 계층은 원장 저장, 거래 처리, 동의・합의 등 블록체인 기반의 거래 전반을 처리하고 관리한다. 인터페이스 계층은 발행은행 및 징구기관 등 각 참가기관의 고유 업무를 처리하기 위한 업무처리 프로그램 접속 환경을 제공한다.

4.3 블록체인 기반의 국민주택채권 분산원장

국민주택채권 분산원장은 각 거래내역을 시간 순서대로 블록에 누적하며 각 블록들은 해쉬값을 기반으로 체인을 형성한다. 각 블록의 유효성을 빠르게 검증하기 위해서 머클트리를 사용하고 거래내역 보관주기(5년)이 지난 블록은 머클트리만 남기고 삭제하여 데이터 저장 공간을 확보한다. 거래내역이 블록에 저장될 때 발행은행, 징구기관, 거래일시, 직전거래가 포함된 블록번호(신규 발행일 경우 현재 블록번호) 등의 메타정보가 쌍으로 등록되어 검색 속도를 높인다.

4.4 거래정보 전송

기존 국민주택채권 정보 중계시스템은 610 byte(헤더 : 160 byte, 거래 : 450 byte)의 고정 길이의 전문을 생성하여 국민주택채권 정보를 전송한다. 실제로는 Filler 길이 등의 차이로 발행은행과 징구기관의 전문 길이가 약간 다르지만 전송하는 정보는 동일하기 때문에 본 논문에서는 발행은행과 징구기관이 동일한 전문 형식으로 전송한다고 가정한다.

제안 모델은 거래 발생 시 국민주택채권 정보를 포함하는 JSON 객체를 생성하여 정보를 전달하며, 발행은행에서 생성하는 데이터 객체(<Table 1>)와 징구기관에서 생성하는 데이터 객체(<Table 2>) 두 가지가 있다. 채권의 상태 정보는 데이터 객체 내의 'bondstate(채권상태)' 항목에 'value(값)'로 전달한다.

기존 시스템은 실제 전달이 필요한 데이터의 양과 관계없이 450 byte(헤더 제외)의 고정 길이의 전문으로 채권 정보를 전달하지만, 제안 모델은 JSON을 기반으로 불필요한 정보는 제외하고 필요한 정보만 전달할 수 있다. 즉, 발행 및 사용중의 처리 시에는 <Table 1>과 <Table 2>의 대부분 항목을 전송하여야 하지만, 기 발행된 국민주택채권을 발행취소하거나 사용완료된 채권을 사용완료취소하는 등 상태만 변경하는 경우에는 <Table 1>과 <Table 2>의 항목 중 대부분의 정보를 삭제하고 채권발행번호 및 채권상태만 징구기관 또는 발행은행 앞으로 전송하면 된다.

<Table 1> Housing Bond Information of Bank

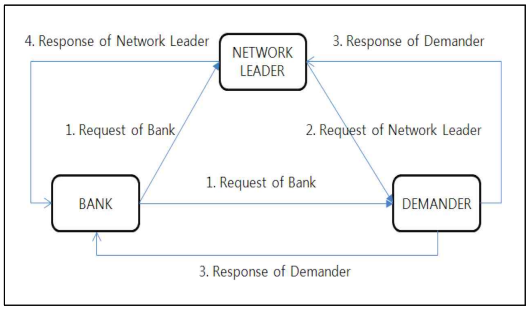
```
{ "Housing Bond Information of Bank" :
  [ { "bankcode" :"value", "demandercode" :"value",
      "bondstate" :"value", "sequence" :"value",
      "bondnumber" :"value",
      "amount" :"value", "demandercode" :"value",
      "bankname" :"value", "branchname" :"value",
      "branchperson" :"value", "branchphone" :"value",
       "taxcode" :"value", "registnumber" :"value",
      "bondgoal" :"value", "bondbuyer" :"value",
       "buyernumber" :"value", "contractnumber" :"value",
      "issuedate" :"value", "salenumber" :"value"
   } ]
}
```

<Table 2> Housing Bond Information of Demander

```
{ "Housing Bond Information of Demander" :
  [ { "bankcode" :"value", "demandercode" :"value",
      "bondstate" :"value", "sequence" :"value",
      "bondnumber" :"value",
      "demandername" :"value", "applyyear" :"value",
      "receiptnumber " :"value", "officialnumber" :"value",
      "officialphone" :"value", "bondchange" :"value",
      "registdate" :"value", "registnumber" :"value",
      "receiptnumber" :"value", "registkind" :"value",
      "agentcode" :"value", "applystate" :"value",
      "confirmdate" :"value", "confirmtime" :"value"
  } ]
}
```

4.5 거래정보 검증

발행은행에서 블록체인 네트워크에 전파한 국민주택채권 정보는 [Fig. 4]과 같이 해당 채권의 징구기관에서 수신하여 처리한다. 이때 네트워크 리더도 전송된 거래를 수신하여 요청한 거래를 검증하고 오류가 없을 경우 이를 전자서명하여 블록체인 네트워크에 전파한다.

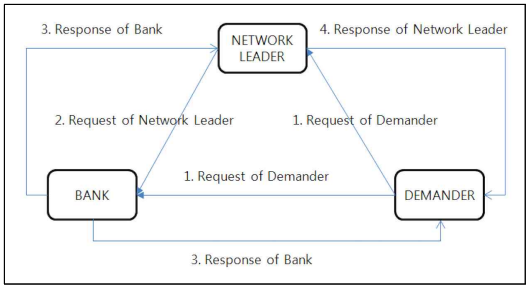


[Fig. 4] Bank Request Transaction

네트워크의 각 참가기관은 네트워크 리더의 승인이 완료되어 권한을 위임받은 기관이므로 거래의 유효성 검증은 네트워크 리더만으로 충분하고, 따라서 빠른 처리가 가능하다. 네트워크 리더는 국민주택채권 거래내역의 머클트리를 확인하여 요청받은 거래내역의 유효성을 빠르게 검증하고 네트워크에 전파할 수 있으며, 징구기관은 발행은행의 요청 내역과 네트워크 리더의 요청 내역이 동일하면 정상 거래로 판단하여 처리한다.

네트워크 리더는 완료된 거래에 대하여 거래 정보를 블록으로 만들어 기존 블록에 연결하고 네트워크의 각 참가기관 앞으로 전송하며 모든 네트워크 참가기관은 이 블록을 수신하여 블록체인 원장을 동기화한다. 이때 네트워크 리더는 일정 건수의 거래가 발생하거나 직전 블록생성 후 일정 시간이 경과한 경우 블록을 생성하도록 함으로서 블록 처리에 대한 컴퓨팅 파워 및 네트워크 낭비를 최소화 한다.

징구기관에서 블록체인 네트워크에 전파한 국민주택채권 정보는 [Fig. 5]와 같이 발행은행의 거래와 처리절차는 동일하며 방향이 반대가 된다.



[Fig. 5] Demander Request Transaction

4.6 장애대책

금융정보 시스템에서 가장 중요한 요소는 장애에 대한 리스크를 최소화 하는 것이다. 제안 모델에서 네트워크 리더는 네트워크 참가기관 거래 내역에 심각한 오류가 발생할 경우 즉각적으로 거래중지 처리를 할 수 있다.

예를 들어 발행은행이 아닌 징구기관에서 국민주택채권 발행 정보를 송신할 경우 네트워크 리더는 이를 오류거래로 처리하고, 해당 참가기관에 해킹 등 심각한 문제가 발생한 것으로 간주하여 발행을 요청한 징구기관의 거래를 즉시 중단한다. 중단하는 방법은 중지 대상 참가기관을 제외한 참가기관 정보를 재배포하거나 참가기관의 거래 권한을 박탈하는 등의 방법으로 가능하다.

네트워크 리더가 문제가 발생한 경우 다른 네트워크 리더나 참가기관 중 하나가 네트워크 리더의 역할을 대행한다. 다만, 대행하는 참가기관은 거래에 대한 검증만 할 수 있으며 네트워크 참가 승인, 참가기관 정보 배포 등 네트워크 리더 고유의 역할은 대행할 수 없다. 네트워크 리더의 장애가 복구되고 정상화 될 경우 전체 참가기관 앞으로 네트워크 리더 복구 완료를 전파하고 블록체인을 동기화한 후 다시 업무를 수행한다.

5. 국민주택채권 정보 중계시스템 개선 모델 검증

모든 거래내역이 공개되는 블록체인의 특성상 중앙집중형 구조보다 거래에 대한 트랜잭션이 많이 발생하며, 제안 모델은 기존 중앙 집중형에 비해 [Fig. 4], [Fig. 5]와 같이 1.5배의 트랜잭션이 발생함을 알 수 있다. 그러나, 기존 시스템이 거래를 위해 450 byte(헤더 제외)의 고정길이 데이터를 계속 전송하여야 하는 반면 개선된 모델은 JSON을 기반으로 불필요한 정보는 배제하고 필요한 정보만 전송하기 때문에 거래 시 전송되는 데이터를 최소화할 수 있다. 발행 및 사용중과 같이 거래정보 및 상태정보(450 byte)를 전송하는 거래를 '그룹1' 이라하고, 발행취소, 변경, 사용중취소, 사용완료, 사용완료 취소, 환급, 환급취소 등 국민주택채권 번호와 상태정보(12 byte)만 전송하는 거래를 '그룹2'라 가정하면 거래량에 따른 두 그룹의 네트워크 사용률 공식은 다음과 같다.

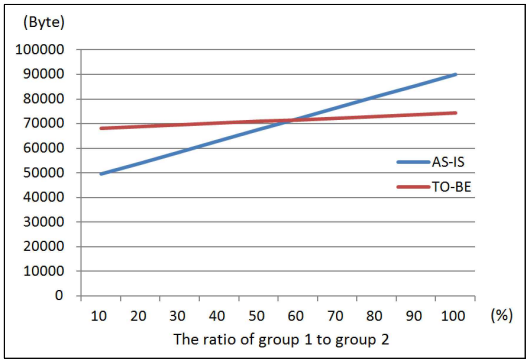
○ 기존 시스템의 네트워크 사용률

= 450 × (그룹1 거래량 + 그룹2 거래량)

○ 제안 모델의 네트워크 사용률

= ((450 × 그룹1 거래량) + (12 × 그룹2 거래량)) × 1.5

이 공식을 그래프로 그리면 [Fig. 6]와 같으며, 그룹2의 거래량이 그룹1의 거래량에 비해 약 52.08% 이상 발생하면 기존 시스템에 비해 제안 모델의 네트워크 사용이 더 효율적이라고 할 수 있다.



[Fig. 6] Network Utilization by Group 1, Group 2

최근 3개월 및 1년간 국민주택채권 상태별 실제 거래량(<Table 3>)을 바탕으로 제안 모델의 성능을 테스트한 결과, 3개월 거래내역 기준으로 그룹1의 거래가 2,662,102건, 그룹2의 거래가 1,459,874건이 발생하였고 이에 따라 약 1.71% 의 개선효과가 있다. 또한, 동일한 방법으로 1년 거래기록 기준으로는 약 1.7%의 개선효과가 있다는 것을 알 수 있다.

<Table 3> Transaction of Housing Bond Information (2017.7.27.)

	3 Month	1 Year
issue	1,404,559	5,024,107
cancel	55,246	227,589
using	1,257,543	4,561,472
used	1,243,985	4,547,861
refund	69	344
not used	160,574	476,246
total	4,121,976	14,837,619

디스크 사용률의 경우 기존 중계시스템은 국민주택채권의 원장과 거래 히스토리를 별도로 관리하여야 하므로 '450 * (발행량 + 거래량)' 이 되지만 제안 모델의 경우 '(450 * 그룹1 거래량) + (12 * 그룹2 거래량) + (256(해쉬값) + 거래량)' 이 되기 때문에 <Table 3>의 3개월 거래량을 기준으로 약 8.7%, 1년 거래량을 기준으로 약 8.53%의 절감효가를 기대할 수 있다.

마지막으로, 제안 모델은 블록체인을 이용하여 P2P 방식으로 모든 네트워크 참가자에게 데이터를 전송하기 때문에 네트워크 리더 및 각 참가기관은 동일한 원장을 보유하며 복수의 참가기관이 블록에 대한 검증을 수행하므로 기존 시스템에 비해 위·변조할 수 있는 가능성이 매우 낮고, 해커가 공격을 하더라도 네트워크 리더 및 전체 참가기관을 동시에 공격하여 성공하지 않는 이상, 네트워크 리더 및 참가기관들은 언제든지 원장을 확인하고 복구가 가능하다.

정성적인 효과로는 개선 모델은 실시간 거래에 따른 원장 불일치를 방지하기 위한 정기적인 원장 대사를 하지 않아도 되며, 발행되는 채권이 모두 사용된다고 가정하더라도 발행 이외의 여타 거래는 거래량 증가에 따른 시스템 부하 증가율이 기존 시스템보다 훨씬 작다. 따라서, 제안 모델은 시스템 유지를 위해 필요한 전체 성능에 대하여 기존 중계시스템에 비하여 예측하기 쉽다.

6. 결론

기존 신뢰할 수 있는 제 3자 및 중계센터 중심의 중앙집중형 구조의 금융전산 시스템은 구조가 단순하여 개발 및 유지보수 측면에서는 효율적이지만 높은 중계센터 관련 비용 소요되고, 해킹 및 장애에 상대적으로 취약하다는 단점이 있다. 이를 기술적으로 해결한 블록체인에 이미 글로벌 금융사 및 IT기업은 대규모 컨소시엄을 구성하여 치열하게 경쟁하고 있으며, 국내에도 뒤늦게나마 다양한 시도를 하고 있다. 그러나, 이러한 노력에도 불구하고 비트코인, 이더리움 등 가상화폐 이외의 영역에서는 아직 뚜렷한 성과가 나오지 않고 있다.

본 논문에서는 금융권과 공공기관에 서비스를 제공하는 대표적인 금융정보 중계시스템인 국민주택채권 정보중계시스템을 블록체인 기반으로 구축하는 방안을 제안하였다. 제안 모델은 블록체인의 장점을 그대로 수용하면서도, 최근 1년간 거래내역을 기준으로 네트워크 사용률 측면에서 약 1.7%, 디스크 사용률 측면에서는 약 8.53%의 개선 효과가 있는 것으로 나타났다.

향후, 본 논문에서 제안한 모델을 금융정보 시스템 전반을 대상으로 적용할 수 있도록 표준화하고, 빠른 검색 및 효율적인 데이터 관리를 위해 '이중 해쉬체인을 사용한 계층적 다중처리 기법[20]' 등을 적용하여 성능을 향상시킬 수 있을 것이다.

REFERENCES

[1] Jin Hwa Kim "The Future of the Internet to Change BitCoin and Blockchain (Distributed Ledger Technology)" Software Knowledge Channel of Software Asset Bank, 2015.

[2] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", 2008.

[3] Santander InnoVentures, "The Fintech 2.0 Paper : rebooting financial services", 2015.

[4] Byung Hwan Lim, "Effect of Blockchain technology and it's Implications", Weekly ICT Trends of IITP, VOL. 1776, No. 1, pp.2-13, 2016.

[5] Jin Wan Kim, "Prospect of development of blockchain and response of financial institution", BNK Financial Group Research Report, 2016.

[6] Financial Security Institute, "Blockchain and Bitcoin security technology", 2015.

[7] Jong Hyun Kim, "Block Chain Concept and Introduction of Domestic and Foreign Financial Sector", The Banker, Vol. 742, Jan, 2016.

[8] Korbit, "Block Chain Primer", White Paper, 2016.

[9] Financial Security Institute, "Confidence structure and double-spending threats of Bitcoin", 2016.

[10] Sungshin University, "Research for the introduction of blockchain technology in the financial sector", 2016.

[11] Leslie Lamport, Robert Shostak, Marshall Pease, "The Byzantine Generals Problem", ACM Transactions on Programming Languages and Systems, Vol. 4,

No. 3, pp.382-401, 1982.
[12] Jong Chan Baek, Seung Hwan Han, Sang Wook Ahn, Young Jin Kim, Chris Hong, "Development process and understanding of blockchain technology", Finector Report, 2016.
[13] Andreas M.Antonopoulos "Mastering Bitcoin" O'REILLY, 2014.
[14] Malte Möser, Ittay Eyal, Emin Gün Sirer, "Bitcoin Covenants", International Conference on Financial Cryptography and Data Security, pp.126-141, 2016.
[15] Vitalik Buterin, "A Next-Generation Smart Contract and Decentralized Application Platform", Ethereum White Paper, 2014.
[16] DR. Gavin Wood, "Ethereum : A Secure Decentralised Generalised Transaction Ledger", Ethereum Yellow Paper, 2014.
[17] Soo Min Park, Seung Pil Hong, "A Study on Privacy and Information Protection in Distributed Network Environment - Focused on Blockchain", Journal of Security Engineering, Vol.14, No.2, pp.167-180, 2017.
[18] Financial Security Institute, "Introduction and characterization of etherium", 2016.
[19] Jung Ho Seo, Dae Gi Lee, Gong Pil Choi, "Using Blockchain in the financial industry and policy issues", Report of KIF, 2017.
[20] Yoon.Su Jung, Yong Tae Kim, Gil Choel Park, "An Efficient data management Scheme for Hierarchical Multi-processing using Double Hash Chain", Journal of Digital Convergence, Vol. 13, No. 10, pp. 271-278, Oct. 2015.

남 진 석(Nam, Jin Seok)

- 1989년 2월 : 홍익대학교 전자계산학과(이학사)
- 2007년 8월 : 연세대학교 산업정보경영학과(공학석사)
- 1989년 3월 ~ 현재 : 금융결제원 감사실장
- 관심분야 : 전자금융, 핀테크
- E-Mail : nam1351@kftc.or.kr

양 해 술(Yang, Hae Sool)

- 1975년 2월 : 홍익대학교 전기공학과 졸업(학사)
- 1978년 8월 : 성균관대학교 정보처리학과 졸업(석사)
- 1991년 3월 : 日本 오사카대학 정보공학과 SW공학 전공(공학박사)
- 2006년 2월 : Kazakhstan 유러시안 경제대학(명예경영학박사)
- 1975년 5월 ~ 1979년 6월 : 중경단 전산실 시스템 분석장교
- 1980년 3월 ~ 1995년 5월 : 강원대 전자계산학과 교수
- 1986년 12월 ~ 1987년 12월 : 日本오사카대학 객원연구원
- 1995년 6월 ~ 2002년 12월 : 한국 Software 품질연구소장
- 2010년 3월 ~ 2012년 2월 : 호서대학교 창업대학원 원장
- 2012년 11월 : 대통령표창(SW산업발전유공) 수상
- 1999년 11월 ~ 현재 : 호서대학교 벤처대학원 교수
- 관심분야 : SW공학(특히, SW품질보증과 품질평가, 품질관리 및 컨설팅, SI), SW프로젝트관리, 품질경영
- E-Mail : hsyang@hoseo.edu