KIPS Trans. Comp. and Comm. Sys.
Vol.7, No.11 pp.281~288 pISSN: 2287-5891

https://doi.org/10.3745/KTCCS.2018.7.11.281

A Reference Model for Korea Real Estate Administration Intelligence System Using Block Chain

Sun Jong-Cheol† · Kim Jin Wook††

ABSTRACT

The block chain, which is characterized by a distributed ledger that stores the same data in several places, has various technical features including security and stability. Due to these characteristics, various researches are being conducted on the application of the block chain. In this paper, we consider the issues to be considered for applying the block chain to the Korea Real Estate Administration Intelligence System (KRAS). Based on this, we propose a block chain reference model for KRAS including a system configuration method and a consensus algorithm.

Keywords : Block Chain, KRAS, PBFT, Agreement Algorithm, Public Ledger

블록체인을 이용한 부동산종합공부시스템 참조모델

선 종 철† · 김 진 욱††

요 약

동일한 데이터를 여러 곳에 보관하는 분산원장을 특징으로 갖는 블록체인은 보안성과 안정성을 비롯한 여러 가지 기술적 특징을 가지며, 이로 인해 블록체인의 활용처에 관한 연구가 다양하게 이루어지고 있다. 본 논문에서는 공적장부의 하나인 부동산종합공부시스템에 블록체인을 적용하기 위해 고려할 사항들을 도출하고, 이를 바탕으로 블록체인 시스템 구성 방안과 합의 알고리즘을 포함하는 블록체인 참조모델을 제시한다.

키워드 : 블록체인, 부동산종합공부시스템, PBFT, 합의 알고리즘, 공적장부

1. 서 론

가상화폐 비트코인의 핵심기술로 세상에 알려진 블록체인은 위·변조가 어려운 데이터 구조와 분산원장이라는 기술특징을 갖는다. 이는 기존의 중앙집중형 서버 방식의 시스템에서 자주 발생하는 디도스나 랜섬웨어의 해킹공격에 대해 더 우수한 보안성을 제공함으로써, 해당 기술의 활용에 대한 다양한 연구가 이루어지고 있다[1-3].

특히, 스웨덴[4], 온두라스[5], 조지아[6]의 경우 국가가 관리하는 부동산관련 공적장부에서 블록체인을 적용하기 위한 연구들이 진행되고 있으며, 국내에서도 국토교통부를 중심으로 부동산종합공부시스템과 같은 공적장부에서 블록체인을 적용하기 위한 연구를 진행하고 있다[7].

본 논문에서는 공적장부의 하나인 부동산종합공부시스템을 위한 블록체인 분산원장 시스템의 구성 방법과 이에 적합한 합의 알고리즘을 제시한다. 이를 바탕으로 블록체인 참조모델을 제안하고, 참조모델을 적용하기 위해 선행되어야 할 과제에 대해서도 논의한다.

2. 블록체인

2.1 블록체인의 종류

블록체인은 여러 대의 컴퓨터 시스템이 참여하여 동일한 데이터를 보관하는 분산원장 시스템을 구성하고 있으며, 블록체인 분산원장 시스템에의 참가 자격 부여 방법에 따라 Table 1과 같이 퍼블릭(Public) 블록체인, 프라이빗(Private) 블록체인, 하이브리드 또는 컨소시엄(Hybrid or Consortium) 블록체인으로 구분될 수 있다[1].

※ 이 논문은 2018년도 한국정보처리학회 춘계학술발표대회에서 '부동산종합공부시스템에서의 블록체인 연계방안 연구'의 제목으로 발표된 논문을 확장한 것임.

† 준 회 원 : 가치더함사회적협동조합 이사장
†† 정 회 원 : 한국방송통신대학교 컴퓨터과학과 교수

Manuscript Received : July 6, 2018
Accepted : August 2, 2018

* Corresponding Author : Kim Jin Wook(gnugi@knou.ac.kr)

Table 1. Types and Characteristics of Block Chain

Types	Characteristics	Examples
Public Blockchain	Publicly available block chain	Bitcoin, Etherium[1)]
Private Blockchain	A block chain that is managed and exercised by one organization	Ripple
Hybrid or Consortium Blockchain	Semi-centric block chain controlled by preselected nodes	R3 CEV

2.2 합의 알고리즘[8]

합의 알고리즘이란 네트워크에 참여하는 참가자들 간에 정보 도달에 시차가 있는 P2P 네트워크와 같은 분산시스템에서, 참가자들이 하나의 결과에 대한 합의를 얻기 위한 알고리즘이다. 블록체인은 분산시스템으로 여러 참가자가 네트워크에 참여하기 때문에, 각 노드에서 만든 블록의 정당성을 검토하고 네트워크 전체에서 공유하는 블록체인에 반영하기 위해 이러한 합의 알고리즘을 사용한다.

합의 알고리즘은 분산시스템에서 발생하는 장애 모델의 예방에 주안점을 두는데, P2P 네트워크에서 발생 가능한 장애 모델로는 FAIL STOP 모델(어떤 오류로 인해 중지된 서버는 깨끗이 퇴출되는 모델), FAIL RECOVER 모델(한 번 정지한 서버가 부활하는 모델), BYZANTINE FAULT 모델(임의 노드가 악의적으로 실수를 일으키는 모델)의 세 가지가 있다. 블록체인의 대표적인 합의 알고리즘인 PoW, PoS, PBFT는 BYZANTINE FAULT 모델을 예방하는 것에 주안점을 둔 합의 알고리즘이다.

2.3 주요 합의 알고리즘 특징

1) PoW (Proof of Work) [8-9]

PoW는 가상화폐 비트코인에서 사용하는 가장 많이 알려진 합의 알고리즘이다. 비트코인에서는 10분 단위로 발생한 모든 거래를 하나의 블록으로 묶어 시간 순서에 따라 하나의 체인처럼 연결하여 전체 P2P 네트워크상에 공유한다. 네트워크 내의 노드들은 이전 블록 헤더의 해시값과 nonce를 연접한 값을 해시 연산하여 특정한 값 x를 찾는 연산을 수행하게 된다. 즉, 해시 연산을 $h()$로 표시할 때 다음과 같은 조건을 만족한다면 n번째 블록에 대한 증명작업이 완료된다.

$$h(h(n-1\text{th block header})||\text{nonce}) < x$$

x는 처음 몇 개의 비트가 0으로 구성된 256비트의 수로, 이를 만족시키는 nonce는 해시 연산의 특성상 직접 찾을 수 없고 nonce를 변화시키면서 순차적으로 대입하여 연산하는 과정이 필수적으로 요구된다. 이러한 이유로 컴퓨팅 파워가 높은 노드일수록 블록 생성에 걸리는 시간은 줄어든다.

2) PoS (Proof of Stake) [8-9]

PoW의 대안으로 제안되어 개발된 PoS는 화폐량을 더 많이 소유하고 있는 승인자가 우선하여 블록을 생성할 수 있는 특징이 있다. 이것은 '대량 통화를 소유하고 있는 참가자는 그 통화 가치를 지키기 위해 시스템의 신뢰성을 손실하지 않을 것이다'라는 전제를 바탕으로 하고 있다. 일반적으로 블록체인을 공격하기 위해서는 공격자가 51% 이상을 점령해야 하는데 PoS를 사용하면 총 화폐 보유량 중 51% 이상을 가지고 있어야 공격할 수 있으므로, PoW를 사용할 때 보다 해커 관점에서 공격에 드는 비용이 매우 증가하여 보안성이 같이 높아진다는 장점이 있다.

3) PBFT (Practical Byzantine Fault Tolerance) [8][10]

PoW와 PoS는 불특정 다수의 사용자가 참가하는 퍼블릭 블록체인에서 악의적인 참가자에 대한 대처에 초점을 맞춘 합의 알고리즘으로, 파이널리티(결제완전성 - 송금 등 결제 처리가 확실하게 집행되는 것)의 불확실성(블록체인이 분기할 경우 거래가 취소될 수도 있음)과 거래 처리의 성능한계(비트코인 PoW의 경우 10분 단위)를 내포하고 있다. 이러한 특성으로 인해 PoW와 PoS는 신뢰된 참가자들이 컨소시엄 형태를 구성하여 운용하는 컨소시엄 블록체인이나 프라이빗 블록체인에서 사용하기에는 적절하지 않은 합의 알고리즘이다.

PBFT는 PoW나 PoS와 마찬가지로 BYZANTINE FAULT 모델이지만 PoW와 PoS의 단점인 파이널리티의 불확실성과 성능 문제를 해결한 것으로 컨소시엄형 블록체인에서 많이 채택되고 있는 합의 알고리즘이다.

PBFT는 네트워크의 모든 참가자를 미리 알고 있어야 한다. 참가자 중 1명이 Primary(리더)가 되고 자신을 포함한 모든 참가자에게 요청을 보낸다. 그 요청에 대한 결과를 집계한 뒤 다수의 값을 사용해 블록을 확정한다. 참여한 노드의 수는 R로 표시하고, $|R| = 3f + 1$이 된다. 이때, f는 결함이 있는 노드 수이며, 확정에는 $f + 1$개 이상의 노드가 필요하다.

PBFT의 구체적인 처리 절차는 다음과 같다(Fig. 1 참고).

① 클라이언트가 모든 노드에 요청을 브로드캐스트

② Replica0이 Primary가 되고 순차적으로 명령을 다른 노드에 전달

③ 각 노드는 ②의 명령을 받으면 Primary를 포함한 모든 노드에 회신

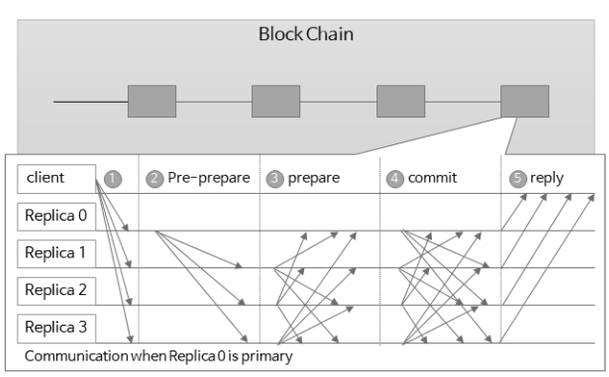

Fig. 1. Structure of PBFT

1) Cryptocurrency Bitcoin and Etherium's technologies are disclosed, and it can be operated as a public block chain and a private block chain system. In this paper, Bitcoin or Etherium is cryptocurrency operated as a public block chain.

④ 각 노드는 ③에서 전달된 명령을 일정 수 이상($2f$) 수신하면 Primary를 포함한 모든 노드에 수신한 신호를 전송

⑤ 각 노드는 ④에서 보낸 명령을 일정 수 이상($2f$) 수신하면 명령을 실행하고 블록을 등록해 클라이언트에 reply를 반환

PBFT는 Fig. 1과 같이 다수결로 의사결정한 뒤 블록을 만들기 때문에 블록체인의 분기가 발생하지 않고, PoW와 같이 조건을 만족시킬 때까지 계산을 반복하지 않아도 되기 때문에 매우 고속으로 동작한다.

PBFT에서 부정사용을 하고자 해도 과반수를 획득해야 하며, Primary가 부정사용을 한다면 모든 참가자가 Primary의 움직임을 감시해 거짓말이라고 판단하면 다수결로 Primary 교체를 신청할 수 있다.

다만, PBFT는 언제나 참자가 전원과 의사소통을 하기 때문에 참가자가 증가하면 통신량과 처리량이 증가하여 PoW/PoS와는 달리 네트워크에 참가할 수 있는 노드의 수가 수십 개로 제한된다.

2.4 스마트 컨트랙트[11]

스마트 컨트랙트(Smart Contract)는 금융 거래나 부동산 거래 등 다양한 형태의 계약을 컴퓨터 코드화하여 미리 정의된 일정 요건이 충족되면 자동적으로 체결된 계약이 이행되는 것을 말한다.

일반적인 계약은 중개인이 필요하고 계약 이행을 사람이 직접 챙겨야 하지만, 스마트 컨트랙트는 블록체인과 결합하여 중개인 없는 당사자들 간의 직접 계약 및 계약의 자동 이행을 가능하게 한다.

3. 부동산종합공부시스템

3.1 부동산종합공부시스템 개요

부동산종합공부시스템(Korea Real Estate Administration Intelligence System, KRAS)은 공간정보의 구축 및 관리 등에 관한 법률(약칭: 공간정보관리법)에 따라 제정된 부동산종합공부시스템 운영 및 관리규정에 의해 국토교통부(Ministry of Land, Infrastructure and Transport, MOLIT) 장관의 책임 하에 운영되는 정보관리체계 중 지방자치단체가 지적공부 및 부동산종합공부 정보를 전자적으로 관리·운영하는 시스템

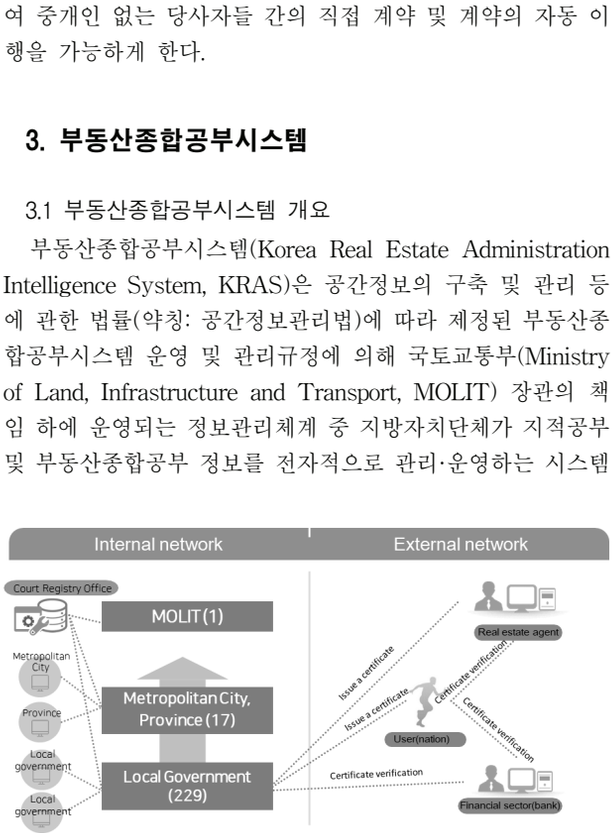

Fig. 2. Current KRAS Composition [13]

이다. 또한, 부동산종합공부시스템은 부동산등기법 및 같은 법 시행규칙에 따라 법원 등기소에 의해 관리되는 부동산등기시스템과 특정 정보를 공유하고 있다[12].

Fig. 2와 같이 현 부동산종합공부시스템은 내부망으로 연결되어, 자치단체가 생성한 자료를 시도가 취합하고 국토교통부가 종합하고 있으며, 외부망을 통해 사용자인 국민의 요청에 따라 자치단체의 부동산종합공부시스템의 자료를 열람하고, 서면 증명서를 발급하는 구조로 이루어져 있다.

3.2 부동산종합공부시스템 자료 구조

부동산종합공부시스템은 법률 규정[12]에 따라 크게 다음 Table 2와 같이 권한이 분배되어 있다.

Table 2. KRAS's Per-User Usage Rights

Organization	Authority
MOLIT	read
Metropolitan City, Province	read, (limited) write
Local Government	read, write
Court Registry Office	(limited) read

이러한 규정에 따라 현 부동산종합공부시스템의 자료구조는, 시군구 자치단체 담당자가 Web Client를 통해 통합DB라고 불리는 부동산종합공부 자료를 생성 및 관리하고, 각 시도가 해당 지역의 자치단체 부동산종합공부 자료를 취합하여 국토교통부 국가공간정보시스템으로 전송하고, 국토교통부가 각 시도로부터 취합된 자료를 바탕으로 일사편리 부동산 통합민원 서비스를 통해 국민들에게 서비스를 제공하고 있는데, 이를 그림으로 도식하면 Fig. 3과 같다.

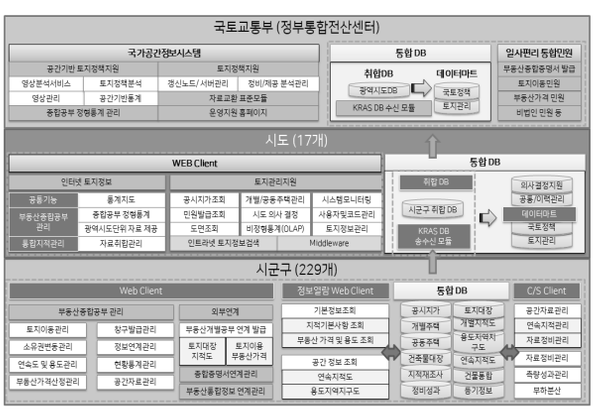

Fig. 3. Current KRAS Data Structure [13]

현재의 부동산종합공부시스템은 각각의 지자체별로 부동산종합공부시스템이 존재하며, 공부DB, 이력DB, log DB, 사용자DB라는 4개의 데이터베이스로 운영되고 있으며, SOAP 기반 정보 전달 체계를 통해 시군구 서버 DB 정보가 변경되면 국토교통부 통합 DB가 변경되는 데이터베이스 복제(replication) 형태로 관리되고 있다[13].

3.3 부동산종합공부시스템의 특성

현재의 부동산종합공부시스템은 내부망과 외부망을 구분하여, 각각의 지자체별로 부동산종합공부시스템이 존재하고, 국토교통부의 국토정보시스템에서 각 지자체의 부동산종합공부시스템의 데이터를 종합하는 구조로 시스템이 구성되고 운영되고 있고, 이러한 구조로 인해 Table 3과 같은 특성이 있다.

Table 3. Characteristics of Current KRAS [13]

Characteristics	Service Level	Description
Convenience	Very High	Real-time information collection system, Integrated public ledger issuance
Stability	Low	Integration stop in case of integration center failure
Transparency	Very Low	Lack of response to intentional change of DB by insider
Performance	Usually	Requiring Real-time information transfer and collection process

Table 3에서 살펴본 바와 같이, 각 지자체의 부동산종합공부시스템이 해킹공격 또는 시스템 장애를 일으키거나, 국토교통부의 국토정보시스템에 대한 장애 발생 시, 국가단위의 서비스가 정상적으로 운영되지 않을 수 있는 심각한 위험에 노출되어 있고, 이를 예방하기 위한 지자체별로 많은 예산을 투입해야 하는 실정이다. 또한, 현행 시스템은 중앙집중형 데이터베이스 사용으로 인해, 내부자가 실수 또는 악의적인 데이터베이스 정보에 대해 변경을 하면 해당 부동산의 소유자와 이해관계자에 대한 심각한 문제가 발생하고, 이를 바로잡기 위한 상당한 행정상의 노력이 수반되어야 한다.

이에 따라, 국토교통부는 현행 부동산종합공부시스템의 개선을 위해 연구 용역[2]을 통해, 차세대 부동산종합공부시스템 발전방향을 Fig. 4와 같이 도출하여, 블록체인과 스마트 컨트랙트 기술을 부동산종합공부시스템에 도입하고자 계획하고 있다.

4. 부동산종합공부시스템 블록체인 참조모델

본 장에서는 국토교통부가 추진 중인 Fig. 4의 차세대 부동산종합공부시스템 발전 방향을 참고하여 부동산종합공부시스템에서 블록체인을 효과적으로 적용하기 위한 참조모델을 도출해보고자 한다.

4.1 블록체인 구성

1) 블록체인 참가자의 범위

부동산종합공부시스템에서 블록체인을 구성하기 위해서는 우선 참가자의 범위를 결정해야 한다. Fig. 4를 살펴보면, 차세대 부동산종합공부시스템에서는 내부망에는 법령에 따라

2) 국토교통부, 블록체인과 부동산종합공부와의 연계방안 종합 연구(2017.09).

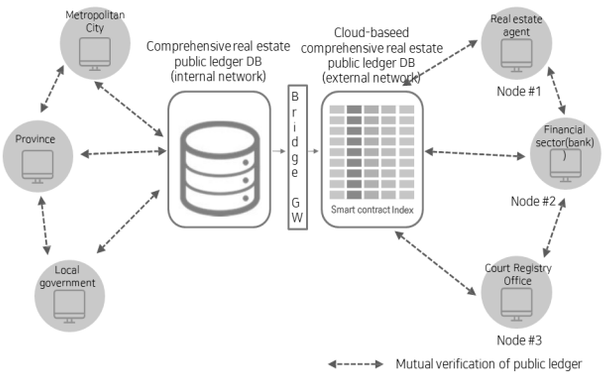

Fig. 4. Developing Direction of Next Generation KRAS [13]

부동산종합공부시스템의 운영 및 유지관리의 책임을 지는 자치단체인 시군구와 그 상급기관인 광역시도가 참여하고, 외부망에는 부동산 거래와 연관된 부동산중개업자, 금융권, 법원 등기소가 참여한 것을 확인할 수 있다. 본 논문에서도 차세대 부동산종합공부시스템과 동일한 참가자가 블록체인을 구성한다고 가정한다. 이에 따라, 부동산종합공부시스템의 블록체인에서 참가하는 참가자들의 역할을 살펴보면, Table 4와 같다.

Table 4. KRAS Block Chain Participants and Role

Division	Participants	Role	Authority
Internal Network	local Government	KRAS operation and maintenance	read, write
	Metropolitan City, Province	Support of local government and collection of local government DB	read, (limited) write
	MOLIT	KRAS operation and management support	read
External Network	Real Estate Agent	Real estate transaction information transfer (owner change request)	(limited) read
	Financial Sector (bank)	Confirm payment and loan information related to real estate transactions	(limited) read
	Court Registry Office	Identify owner information related to real estate transactions	(limited) read

2) 블록체인을 구성하는 방법

부동산종합공부시스템에서 블록체인을 구성할 때 첫 번째 검토될 사항은 내부망과 외부망을 통합하여 블록체인을 구성할 것인지, 아니면 내부망과 외부망을 구분하여 블록체인을 구성할 것인지 여부일 것이다. Fig. 4의 차세대시스템은 외부망과 내부망을 분리하여 서비스를 운영하고 있는데, 이는 해킹 등 주요 사이버 공격으로부터 국가 기밀 등 중요자료의 유출을 근본적으로 차단하기 위해 정부의 지침[14]을 따른 것이므로, 본 논문에서도 내부망과 외부망을 구분하여 블록체인을 구성하는 방법을 도출한다.

a) 내부망 블록체인 구성 방법

내부망에서 블록체인을 구축하는 방법으로는 ① 퍼블릭(Public) 블록체인, ② 프라이빗(Private) 블록체인 형태로 Table 5와 같이 검토해 볼 수 있다.

Table 5. Type of Internal Network Block Chain

Type	Participants
Public Blockchain	Not applicable
Private Blockchain	MOLIT, Metropolitan City, Province Local government

내부망에서의 블록체인은 내부망의 특성상 지방자치단체를 포함한 국가 행정기관만 참여할 수 있으므로, 프라이빗 블록체인으로 구성하는 방법이 적절하다.

내부망 블록체인의 형태를 컨소시엄 블록체인으로 보지 않은 이유는, 부동산종합공부시스템이 국토교통부가 표준 가이드라인을 정하고 자치단체가 이에 따라 운영하는 형태를 취하고 있기 때문에 하나의 주체가 운영하는 프라이빗 블록체인으로 보는 것이 바람직하기 때문이다.

b) 외부망 블록체인 구성 방법

외부망에서 블록체인을 구축하는 방법으로는 ① 퍼블릭(Public) 블록체인, ② 프라이빗(Private)블록체인, ③ 컨소시엄(Consortium) 블록체인 형태로 Table 6과 같이 검토해 볼 수 있다.

Table 6. Type of External Network Block Chain

Type	Participants
Public Blockchain	MOLIT, Financial Sector (bank), Real Estate Agent, Court Registry Office
Private Blockchain	Not applicable
Hybrid or Consortium Blockchain	MOLIT, Financial Sector (bank), Real Estate Agent, Court Registry Office

외부망에서의 블록체인은 컨소시엄 블록체인으로 구성하는 방법이 적절하다. 차세대 부동산종합공부시스템의 외부망 구성은 선택된 부동산중개업체가 참여하는 컨소시엄 블록체인 정책을 취하고 있으며, 이는 전자서명법[15]에 의해 운영되는 공인인증서 시스템과 유사한 정책을 취할 것으로 예측된다. 즉, 전자서명법 제4조에 따라 기술능력·재정능력·시설 및 장비 기타 필요한 사항을 갖춘 공인인증기관을 지정하고, 그 기관들과 협약된 등록대행기관(은행, 우체국, 협회 등)들이 공인인증기관과 시스템 연동을 통해 공인인증서 업무를 취급하듯, 부동산종합공부시스템의 외부망 블록체인도 특정 업체를 지정하여 참여할 것으로 예측된다.

실제로 국내에서 2017년 한 해 동안 거래된 부동산 거래건수[16]는 토지 3,314,801필지, 건물 2,208,529동(호)로서 일평균 15,132건 정도에 지나지 않아, 시스템 효율성 측면에서 소수의 부동산중개업체를 선정하여 블록체인에 참여시키는 것이 효과적일 것이다. 앞서 예를 든 공인인증 업무의 경우에도 2017년 기준 전자서명법에 의해 지정된 공인인증기관[17]은 총 6곳으로, 공인인증서 누적 발급건수[18]는 3,659만 건이고, 일평균 약 100,246건으로 업체당 16,707건 정도를 하루에 처리하고 있다.

4.2 합의 알고리즘

부동산종합공부시스템은 4.1절에서 살펴본 것처럼, 프라이빗 및 컨소시엄 블록체인으로 구성하는 것이 가장 효과적이라고 볼 수 있다. 이에 따라 블록체인의 여러 합의 알고리즘 중 프라이빗, 특히 정해진 참가자에 의해 운영되는 컨소시엄형 블록체인에 적합한 알고리즘인 PBFT기반의 알고리즘을 운영하는 것이 적절하다.

1) 내부망 블록체인에서의 합의 알고리즘

내부망 블록체인에서는 앞에서 언급한 것처럼 PBFT 알고리즘을 사용하는 것이 적절한데, PBFT 알고리즘을 사용할 경우 법률에 의해 권한의 문제가 발행하여 Fig. 1의 PBFT 처리 절차 중 ②번 절차에 대한 변경이 필요하다. PBFT 알고리즘에서는 Primary(리더)가 정해져 있고, Primary에 대한 문제가 발생하지 않는 한 Primary는 변경되지 않는다. 그러나 현행 규정[12]은 클라이언트가 누구냐에 따라 Primary가 결정된다. 예를 들어, 서울특별시 공무원이 사용할 경우 서울시 부동산종합공부시스템이 Primary가 되어야 한다.

이를 바탕으로 부동산종합공부시스템의 블록체인 합의 알고리즘 참조모형을 도출해보면 Fig. 5와 같고, 처리 절차는 다음과 같다.

① 클라이언트가 모든 노드에 요청을 브로드캐스트

② 클라이언트가 누구냐에 따라 (법률 규정에) 정해진 노드가 유동적으로 Primary가 되어 순차적으로 명령을 다른 노드에 전달

③ 각 노드는 ②의 명령을 받으면 Primary를 포함한 모든 노드에 회신

④ 각 노드는 ③에서 전달된 명령을 일정 수 이상($2f$) 수신하면 Primary를 포함한 모든 노드에 수신한 신호를 전송

⑤ 각 노드는 ④에서 보낸 명령을 일정 수 이상($2f$) 수신하면 명령을 실행하고 블록을 등록해 클라이언트에 reply를 반환

변경된 ②번 절차를 살펴보면, PBFT 알고리즘에서는 Primary가 정해져 있으나, 변형된 알고리즘에서는 규정에 따라 유동적으로 Primary가 결정된다. 즉, 서울시 공무원이 클라이언트가 되면, 서울시 부동산종합공부시스템이 Primary가 되고, 제주도의 공무원이 클라이언트가 되면, 제주도 부동산종합공부시스템이 Primary가 되어 리더 역할을 수행하게 된다.

2) 외부망 블록체인에서의 합의 알고리즘

외부망 블록체인에서는 앞에서 언급한 것처럼 PBFT 알고리즘을 사용하는 것이 적절한데, 외부망 블록체인에서는 누구를 Primary로 정할 것이냐의 문제가 제기된다. 외부망 블

Table 7. Examples of Consensus Requests by External Network Block Chain Participants

Participants	Cases of Requests	Requesters
Real Estate Agent	Owner change based on real estate transactions	Trading party, Agent
Financial Sector	Real estate mortgage, Deposit information for real estate transactions	Trading party, Lender
Court Registry Office	Owner's personal information change, Information on property rights such as Mortgage	Owner, Legal representative

록체인 참가자별로 합의 처리를 요청하는 주요 사례를 살펴보면 Table 7과 같다.

Table 7에서 살펴본 바와 같이, 참가자별로 합의 요청하는 사례의 특성이 차이가 있고, 각각의 처리를 요청하는 건수가 2017년 부동산 거래건수를 기반으로 일간 15,000건 정도로 예측되는바, PBFT 알고리즘처럼 Primary를 지정하기보다는, Fig. 5와 같이 합의를 요청하는 사례에 특성에 따라 Primary를 유동적으로 결정하는 것이 효과적일 것이다. 즉, 부동산중개와 관련된 합의가 발생하면 부동산중개업자가 Primary가 되고, 대출 등 금융거래와 관련된 합의가 발생하면 금융권이 Primary로, 등기 변경과 관련된 합의가 발생하면 법원 등기소가 Primary가 되어 리더 역할을 수행하면 된다.

4.3 블록체인 참조모델

4.1절과 4.2절을 통해 부동산종합정보시스템에 적합한 블록체인 구성 방법과 합의 알고리즘을 살펴보았다. 여기에 추가적으로 참여 노드 및 대상 데이터의 범위를 고려하여 최종적인 참조모델을 제시한다.

1) 내부망 블록체인 참여 노드의 조정

내부망에서 효과적으로 블록체인을 구성하기 위해서는 다음과 같은 이유로 참여하는 노드 수를 조정해야 할 필요가 있다.

a) PBFT 알고리즘의 효과적 구현

4.2절에서 내부망 블록체인의 합의 알고리즘으로 PBFT 기반의 알고리즘이 효과적임을 도출하였다. PBFT 알고리즘은 2.3절에서 살펴본 것처럼 네트워크에 참가할 수 있는 노드의 수가 수십 개로 제한된다. 하지만 Fig. 4의 차세대 부동산종합공부시스템은 법령에 따라 부동산종합공부시스템의 운영 및 관리 주체가 '자치단체'로 규정되어 있어, 국토교통부를 포함하여 총 247개의 기관의 노드들이 참여하고 있다. 즉, 발생한 거래에 대한 합의를 위해 247개 노드간 통신과 내부 처리를 위해 많은 시스템 자원을 사용하기 때문에 PBFT 알고리즘을 효과적으로 구현하기 어렵다.

b) 시스템의 효과적 운영

Fig. 2의 현재의 부동산종합공부시스템은 법령에 따라 229개 자치단체가 내부망을 통해 각자의 부동산종합공부시스템을 보유하고 있다. 이로 인해, 각 지자체별로 시스템 유지보수 및 장애가 발생할 경우 해당 지자체의 서비스 뿐 아니라 이와 연동되는 광역단체 및 국토교통부의 대국민 서비스에도 일부 차질을 유발하고 있다.

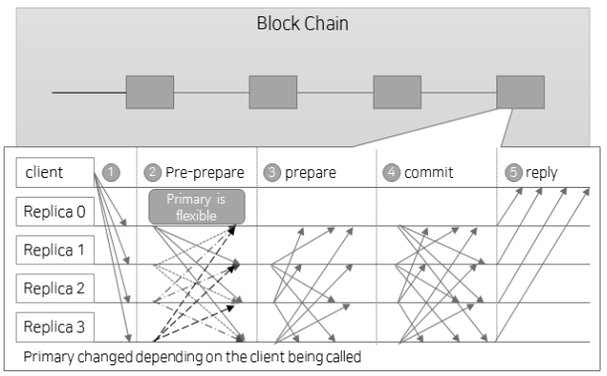

Fig. 5. PBFT based Public Ledger Consensus Algorithm Reference Model

일례로, 대국민 부동산통합민원 서비스인 일사편리[3]의 2018년 5월 1일 공지사항을 살펴보면, 4개의 지자체가 5월 2일부터 5월 7일까지 시스템 유지보수로 인해 해당 자치단체의 부동산 공부에 대한 열람 및 발급이 중단됨을 알리고 있다. 이와 같이 많은 노드가 부동산종합공부시스템에 참여하게 되면 잦은 FAIL STOP과 FAIL RECOVER 장애를 유발하게 되고, 이는 블록체인 네트워크의 효과적 운영을 저해하는 요인이 된다.

c) 중복예산의 절감

국내 229개 자치단체 중 하나인 경기도 이천시의 부동산종합공부시스템 시스템 구성 및 취득비용은 281,252,145원이고, 2018년 한 해 동안 해당시스템을 유지 보수하기 위한 예산은 29,765,040원이 책정되었다[19]. 국내 229개 자치단체는 경기도 이천시와 유사한 구조의 부동산종합공부시스템을 개별적으로 운영하고 있고, 이에 대한 연간 3,000만원~5,000만원 사이의 유지보수비용을 자치단체별로 지출하고 있다.

뿐만 아니라 각 자치단체는 이러한 고정적인 연간 유지보수 비용을 제외하고도 시스템 고도화, 전산장비 구입 등의 명목으로 비정기적인 비용을 지출하고 있다. 즉, 자치단체에서 운영하고 있는 부동산종합공부시스템의 데이터 처리량에 비해 과도한 중복투자가 이루어지고 있음을 알 수 있다.

2) 참조모델에서의 내부망 블록체인 노드의 구성

1)에서 살펴본 바와 같이, 부동산종합공부시스템의 내부망에서 블록체인을 효과적으로 구축하기 위해서는 현재 참여하고 있는 노드의 수준을 자치단체에서 광역시도로 변경하는 것이 적절하다(Fig. 6 참고). 즉, 각 지자체별로 운영되고 관리되던 부동산종합공부시스템을 광역시도 단위로 통합하여 운영하고, 각 시스템별로 해당 통합원장을 분산 보관하는 것이다.

3) Internet - http://www.kras.go.kr

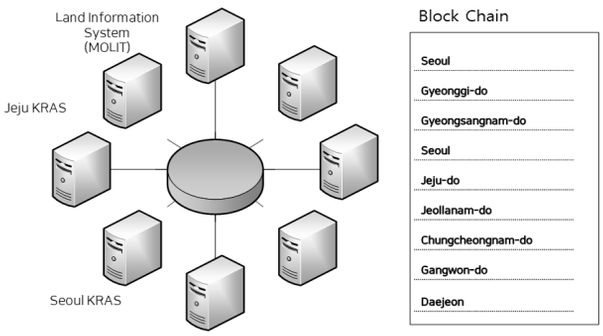

Fig. 6. Construction of Internal Network Block Chain Nodes in the Reference Model

그러나 현행 법률은 부동산종합공부시스템의 운영 및 관리의 주체가 자치단체로 규정되어 있어 이러한 변화를 위해서 Table 8과 같은 선행 절차가 필요하다.

Table 8. Procedures for Changing Administrator of KRAS

Legal Amendment	Changing Procedures
Possible	Change the management institution of Article 2, Clause 4 of the regulations on the operation and management of KRAS from the local government to the metropolitan city & the province
Impossible	Consensus through consultation between the local government and the metropolitan city & the province

3) 블록체인과 상용 데이터베이스

국가 및 자치단체는 부동산과 관련하여 다양한 데이터를 생성하고 관리하고 있는데, 이러한 과정 중에 발생하는 데이터 중 어느 부분의 데이터를 블록체인화 할 것인가 하는 범위의 문제가 발생한다. 본 논문에서는 Fig. 7의 집합건물물대장과 같은 부동산종합공부와 직접적으로 연관된 데이터의 생성 및 변경과 관련된 부분에 대해서 블록체인을 적용하고, 기타 부분의 데이터에 대해서는 기존 상용 데이터베이스를 사용하는 것을 가정하고 있다.


집합건축물대장(전유부, 갑)

Fig. 7. Collective Building Public Ledger

즉, 부동산종합공부시스템에서 발생하는 토지대장 변경 이력이나 집합건축물대장 변경 이력 부분에는 블록체인을 적용하여, 블록체인 내에서 합의 완료된 후 상용 데이터베이스를 변경하는 구조를 채택함으로써, 블록체인의 장점과 상용 데이터베이스의 장점을 활용함과 동시에 상용 데이터베이스에서 발생하는 내부자의 의도적인 DB 정보 변경에 따라 발생할 수 있는 문제를 예방하고자 한다.

4) 도출된 블록체인 참조모델

이상의 검토를 통해 도출된 블록체인 참조모델의 주요 특징은 Table 9와 같고, 시스템 구성은 Fig. 8과 같다.

Table 9. Features of Block Chain Reference Model for KRAS

Features	Description
Separation of internal network and external network	• Separating internal and external network • Operating bridge server for internetworking
Internal network participant	• 18 nodes - MOLIT (1), Province and Metropolitan city (17) • Change of law or consultation of parties is needed
External network participant	• 3+n nodes - MOLIT (1), Real Estate Agents (n), Financial Sector (1), Court Registry Office (1) • In case of court registry office, change of real estate registration system is needed
Consensus algorithm	• PBFT based Consensus Algorithm • Flexible Primary
Commercial database	• Internal network - Comprehensive real estate public ledger DB • External network - Cloud-based comprehensive real estate public ledger DB • DB information related to real estate comprehensive public ledger is changed through block chain agreement.

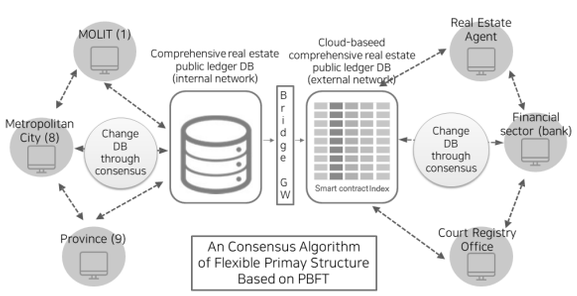

Fig. 8. Block Chain Reference Model for KRAS

5. 결 론

본 논문에서는 현행 부동산종합공부시스템의 특성 및 구조 분석을 통해, 부동산종합공부시스템에 블록체인을 적용하기 위한 블록체인 시스템의 구성 방법과 변형된 합의 알고리

즘을 제시하였다.

부동산종합공부시스템은 정부의 망 분리 가이드라인에 따라 내부망과 외부망이 분리되어 운영되고 있으며, 생성되고 교환되는 정보의 범위와 내용이 구분되어 있다. 따라서 부동산종합공부시스템에 블록체인의 적용을 위해서는 내부망과 외부망을 구분하여 블록체인 구성을 검토하여야 하며, 망별로 참여자간 합의에 필요한 정보를 토대로 별개의 분산원장을 도출할 필요가 있음을 발견하였다.

이러한 고찰을 통해 부동산종합공부시스템의 블록체인 적용과 관련된 참조모델을 도출하였고, 참조모델에서는 참여노드의 수에 대한 조정을 제안하였다. 이를 통해 부동산종합공부시스템의 효과적 운영, PBFT 알고리즘의 효과적 구현, 중복 예산의 절감 효과를 기대할 수 있는데, 이를 위해서는 법률 개정 또는 참여자간의 합의가 필요함을 제시하였다.

본 논문에서 도출한 부동산종합공부 블록체인 시스템 구성 및 합의 알고리즘은 법령에 의해 정해진 내용 및 현행 부동산종합공부시스템의 공개된 자료만을 토대로 도출한 참조모델로서, 실제 활용에는 많은 검토가 필요할 것이다.

따라서 부동산종합공부시스템 등 국가가 관리하는 공적장부에 블록체인을 적용하여 효과적으로 운영하기 위해서는 네트워크, 합의 알고리즘, 보안 부분에 대한 면밀한 검토를 통해, 공적장부의 특성에 맞는 블록체인 시스템의 개발이 필요하다.

References

[1] Lim Myung Hwan, “Application and Prospect of Block Chain Technology,” ETRI Creative Open ECO series : Insight Report 2016-03, ETRI, 2016.0531.

[2] Kasper Triebstock, “How to solve the digital identity and bring privacy to a whole new level?,” Medium, 2016.8.31.

[3] Son Kyung Ho, “Block Chain Application Technology, Public Domain,” ZDNet Korea, 2016.1.25.

[4] Pete Rizzo, “Sweden’s Blockchain Land Registry to Begin Testing in March,” Coindesk, 2017.1.10.

[5] Pete Rizzo, “Blockchain Land Title Project ‘Stalls’ in Honduras,” Coindesk, 2015.12.26.

[6] Pete Rizzo, “Blockchain Land Title Project ‘Stalls’ in Honduras,” Coindesk, 2015.12.26.

[7] MOLIT, Bidding Instructions [Internet], https://goo.gl/7YG1KD.

[8] Akahane Yoshiharu and others, “Block Chain Structure and Theory,” Wikibooks publisher, 2016.

[9] Boohyung Lee, Yeon-Joo Lim, and Jong-Hyouk Lee, “Consensus algorithms in blockchain platforms,” *Proceedings of Symposium of the Korean Institute of communications and Information Sciences*, pp.386-387, 2017.

[10] Miguel Castro and Barbara Liskov, “Practical Byzantine Fault Tolerance and Proactive Recovery,” *ACM Transactions on Computer Systems*, Vol.20, No.4, Nov. 2002.

[11] Lee Young-Hwan, “A Study on Application of Block Chain Technology to Ensure Transparency of Budget Execution of Public Institutions under the Ministry of Information and Communication,” Ministry of Science and ICT, 2018.03.28.

[12] Regulations for the operation and management of KRAS (Act: 2014.12.31.)

[13] Department of Space Information System, “Block-chain cloud-based KRAS pilot project,” MOLIT, 2018.03.16.

[14] Ministry of the Interior and Safety and National Intelligence Service, “National agency network separation building guide,” Korea Information Society Agency, 2008.05.

[15] Digital Signature act (Act No. 14577, Mar. 14, 2017)

[16] Korea Appraisal Board, R-ONE Real estate statistical information [internet], http://www.r-one.co.kr.

[17] Ministry of Employment and Labor, ILMOA, Guidance on Issuance of Certified Certificates [Internet], https://goo.gl/fN97U8.

[18] Pyo Dal Su, “Number of accredited certificate cumulative issuance,” <Consumer Post>, 2018.03.08.

[19] Korea ON-Line E-Procurement System, Bid announcement number: 20171235045-00 (2017.12.26.) [Internet], https://goo.gl/mfKeDP.

선 종 철

https://orcid.org/0000-0002-7847-8368

e-mail : hmomkr@knou.ac.kr

2013년 한국방송통신대학교 경영학과 (학사)

2018년 한국방송통신대학교 정보과학과 (석사)

2016년~현 재 가치더함사회적협동조합 이사장

관심분야 : Block Chain & E-Commerence

김 진 욱

https://orcid.org/0000-0003-4986-0848

e-mail : gnugi@knou.ac.kr

1998년 서울대학교 수학과(학사)

2000년 서울대학교 컴퓨터공학과(석사)

2006년 서울대학교 전기・컴퓨터공학부 (박사)

2013년~현 재 한국방송통신대학교 컴퓨터과학과 교수

관심분야 : 컴퓨터이론, 알고리즘, 생물정보학, 정보보호