부동산종합공부시스템에서의 블록체인 연계방안 연구

선종철, 김진욱
한국방송통신대학교 대학원 정보과학과
e-mail:hmomkr@knou.ac.kr

A Study on Linkage of Block Chain in Korea Real Estate Administration Intelligence System

Jong Cheol Sun, Jin Wook Kim
Dept of Computer Science, Korea National Open University

요 약

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

1. 서론

가상화폐 비트코인의 핵심기술로 세상에 알려진 블록체인은 위·변조가 어려운 데이터 구조와 분산원장이라는 기술특징을 갖는다. 이는 기존의 중앙집중형 서버 방식의 시스템에서 자주 발생하는 디도스(DDos)나 랜섬웨어(Ramsomware)의 해킹공격에 대해 보다 우수한 보안성을 제공함으로써, 해당 기술의 활용에 대한 다양한 연구가 이루어지고 있다[1][2][3].

특히, 스웨덴[4], 온드라스[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 부동산종합공부시스템에서 블록체인 분산원장 시스템은 어떻게 구성될 수 있고, 합의 알고리즘은 어떤 특징을 가져야하는지에 대한 참조모델을 제시한다.

2. 블록체인

2.1. 블록체인의 종류

블록체인은 여러 대의 컴퓨터 시스템이 참여하여 동일한 데이터를 보관하는 분산원장 시스템을 구성하고 있으며, 블록체인 분산원장 시스템 참가 자격의 부여 방법에 따라 퍼블릭(Public) 블록체인, 프라이빗(Private) 블록체인, 컨소시엄형 블록체인으로 구분될 수 있다[1].

<표 1> 블록체인의 종류 및 특징

종류	특징	예
퍼블릭	누구나 참여 가능한 공개된 형태의 블록체인	비트코인, 이더리움 1)
프라이빗	특정 기관 혹은 개인에 의해 운영되는 블록체인	Ripple
컨소시엄	미리 선정된 노드에 의해서 컨트롤되는 반 중앙형 블록체인	R3 CEV

2.2. 합의 알고리즘 [8]

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

합의 알고리즘은 분산 시스템에서 발생하는 장애 모델의 예방에 주안점을 두는데, P2P 네트워크에서 발생 가능한 장애 모델로는 ① FAIL STOP 모델(어떤 오류로 인해 중지된 서버는 깨끗이 퇴출되는 모델) ② FAIL RECOVER 모델(한 번 정지한 서버가 부활하는 모델) ③ BYZANTINE FAULT 모델 (임의 노드가 악의적으로 실

1) 가상화폐 비트코인, 이더리움의 기술은 공개되어 있으며, 해당 기술을 이용하여 퍼블릭 블록체인, 프라이빗 블록체인 시스템도 운영될 수 있으나, 본 논문에서는 퍼블릭 블록체인으로 운영되는 비트코인, 이더리움 가상화폐 시스템을 말한다.

수를 일으키는 모델) 3가지가 있다. 블록체인의 대표적인 합의 알고리즘인 PoW, PoS, PBFT는 ③ BYZANTINE FAULT 모델을 예방하는 것에 주안점을 둔 합의 알고리즘이다.

3. 주요 합의 알고리즘 특징

3.1. PoW (Proof of Work) [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 네트워크 상에 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 n번 째 블록에 대한 증명작업이 완료된다.

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

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

3.2. 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 공격이 가능하므로, PoW를 사용할 때 보다 해커 입장에서 공격에 드는 비용이 매우 증가하여 보안성이 같이 높아진다는 장점을 가진다.

3.2. PBFT (Practical Byzantine Fault Tolerance) [8][10]

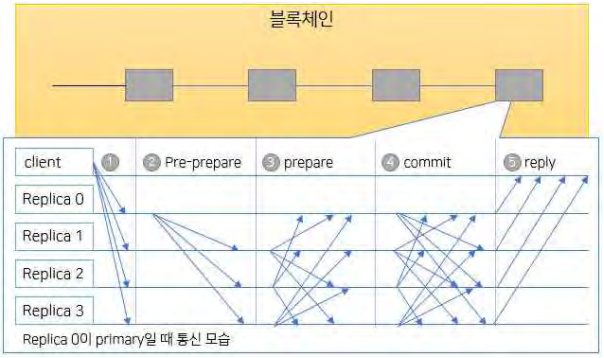
PoW와 PoS는 불특정 다수의 사용자가 참가하는 퍼블릭 블록체인에서 악의적인 참가자에 대한 대처에 초점을 맞춘 합의 알고리즘으로, 파이널리티(결제완전성 - 송금 등 결제 처리가 확실하게 집행되는 것)의 불확실성(블록체인이 분기할 경우 거래가 취소될 수도 있음)과 거래 처리의 성능한계(10분 단위)를 내포하고 있다. 이러한 특성으로 인해 PoW와 PoS는 신뢰된 참가자들이 컨소시엄 형태를 구성하여 운용하는 컨소시엄 블록체인이나 프라이빗 블록체인에서 사용하기에는 적절하지 않은 합의 알고리즘이다.

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 + 1이 된다. 이때, f는 결함이 있는 노드 수이며, 확정에는 f+1개 이상의 노드가 필요하다.

구체적인 처리 절차는 다음과 같다.

① 클라이언트가 모든 노드에 요청을 브로드캐스트
② Replica0이 Primary(리더)가 되고 순차적으로 명령을 다른 노드에 전달
③ 각 노드는 ②의 명령을 받으면 Primary(replica0)를 포함한 모든 노드에 회신
④ 각 노드는 ③에서 전달된 명령을 일정 수 이상(2f) 수신하면 Primary(Replica0)를 포함한 모든 노드에 수신한 신호를 전송
⑤ 각 노드는 ④에서 보낸 명령을 일정 수 이상(2f) 수신하면 명령을 실행하고 블록을 등록해 client에 reply를 반환



(그림 1) PBFT의 구조

PBFT는 (그림1) 처럼 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 하고자해도 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 증가하기 때문에 PoW/ PoS와는 달리 네트워크에 참가할 수 있는 노드의 수가 수십개로 제한된다.

4. 부동산종합공부시스템에서의 블록체인 구성

4.1. 부동산종합공부시스템

부동산종합공부시스템은 공간정보의 구축 및 관리 등에 관한 법률(약칭: 공간정보관리법)에 따라 부동산종합공부시스템 운영 및 관리규정에 의해 국토교통부 장관의 책임하에 운영되는 정보관리체계 중 지방자치단체가 지적공부 및 부동산종합공부 정보를 전자적으로 관리·운영하는 시스템이다[11]. 또한 부동산종합공부시스템은 부동산등기법 및 같은법 시행규칙에 의해 법원에 의해 관리되는 부동산등기시스템과 특정 정보를 공유하고 있다[12].

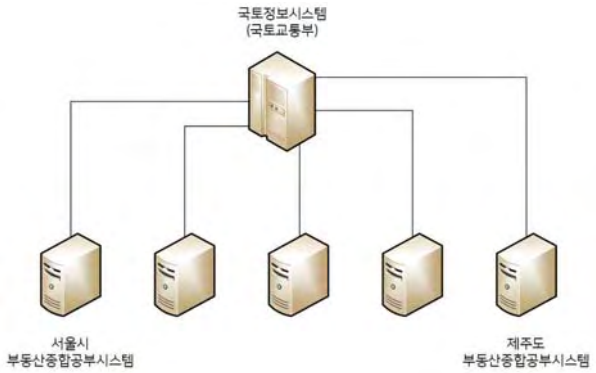
4.2. 블록체인 구성

부동산종합공부시스템은 법률에 따라 크게 다음 <표2>와 같이 권한이 분배되어 있다.

<표2> 부동산종합공부시스템의 참여자별 사용권한

기관	국토교통부	지방자치단체	법원
권한	읽기, (제한적)쓰기	읽기, 쓰기	(제한적)읽기

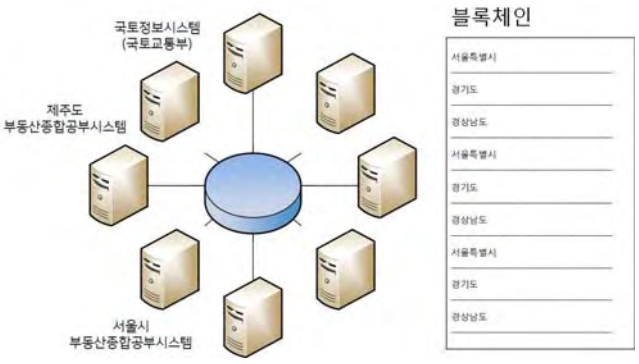
또한, 규정에 따라 부동산종합공부시스템의 시스템 구성은 (그림2)과 같이 유추해볼 수 있다.



(그림2) 부동산종합공부시스템의 구성

현재의 부동산종합공부시스템은 각각의 지자체별로 부동산종합공부시스템이 존재하고, 국토교통부의 국토정보시스템에서 각 지자체의 부동산종합공부시스템의 데이터를 종합하는 구조로 시스템이 구성되고 운영되고 있다. 이러한 시스템구조로 인해 각 지자체의 부동산종합공부시스템이 해킹공격을 받거나, 국토교통부의 국토정보시스템이 해킹공격으로 인해 서비스의 지장이 생길 경우, 국가단위의 서비스가 정상적으로 운영되지 않을 수 있어, 심각한 보안 위협에 노출되어 있고, 이를 위한 각 지자체별로 많은 예산을 투입해야하는 실정이다[2].

현행 법률 규정의 사용권한에 따라 부동산종합공부시스템에 블록체인을 적용해보면 (그림3)과 같은 구성이 가능하다.



(그림3) 부동산종합공부시스템의 블록체인 적용

즉, 각 지자체별로 운영되고 관리되던 부동산종합공부시스템을 하나의 시스템으로 묶고, 응용소프트웨어의 변경을 통해 블록체인 기반의 통합원장으로 변경하여, 각 시스템별로 해당 통합원장을 분산 보관하는 것이다.

부동산종합공부시스템의 이러한 변화는 다음과 같은 장점을 가진다.

① 각 지자체의 부동산종합공부시스템을 통합하고 매칭하는 국토교통부 국토정보시스템의 역할 감소

② 각 지자체별로 부동산종합공부시스템의 운영 및 백업을 위해 소요되는 중복 예산의 절감

③ 해킹공격으로 인해 특정 부동산종합공부시스템의 운영이 중단되더라도, 응용프로그램의 접속 서버 변경 등을 통해 서비스 중단이 발생되지 않음

하지만, 블록체인 시스템의 변화로 인해 ① 응용 소프트웨어 등 시스템 통합을 위한 초기 구축 비용 ② 통합원장에 대한 권한 관리 (정보보안) 등의 문제가 유발될 수 있다.

5. 부동산종합공부시스템에서의 합의 알고리즘

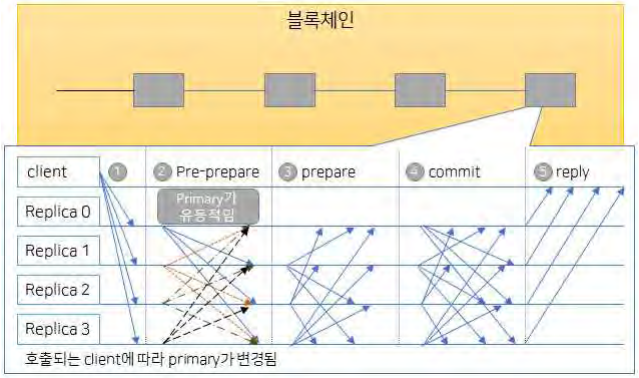
부동산종합공부시스템은 법률에 의해 사용자 권한이 제한되어 있어 컨소시엄형 블록체인으로 볼 수 있다. 이에 따라 블록체인의 여러 합의 알고리즘 중 컨소시엄형 블록체인에 적합한 알고리즘인 PBFT기반의 알고리즘을 운영하는 것이 적절하다.

다만, PBFT 알고리즘을 사용할 경우 법률에 의해 권한의 문제가 발행하여, (그림1)의 PBFT 처리 절차 중 ②번 절차에 대한 변경이 필요하다. PBFT 알고리즘에서는 Primary(리더)가 정해져있고, Primary에 대한 문제가 발생되지 않는 한 Primary는 변경되지 않는다. 그러나, 현행 규정[3]은 Client가 누구냐에 따라 Primary가 결정된다. 예를 들어, 서울특별시 공무원이 사용할 경우 서울시 부

2) 2018년 국토교통부 '부동산종합공부시스템 유지보수' 예산 약 22억, 기능개선 예산 3억원, '국토공간정보체계구축 및 지원' 예산 약 38억원, 출처: 국토교통부 2018년 예산서

3) 부동산종합공부시스템 운영 및 관리규정

동산종합공부시스템이 Primary가 된다.



(그림 4) PBFT 기반의 공적장부 합의 알고리즘 참조모형

이를 바탕으로 부동산종합공부시스템의 블록체인 합의 알고리즘 참조모형을 도출해보면 (그림4)와 같고, 처리 절차는 다음과 같다.

① 클라이언트가 모든 노드에 요청을 브로드캐스트
② Client가 누구냐에 따라 (법률 규정에) 정해진 노드가 유동적으로 Primary(리더)가 되어 순차적으로 명령을 다른 노드에 전달
③ 각 노드는 ②의 명령을 받으면 Primary(replica0)를 포함한 모든 노드에 회신
④ 각 노드는 ③에서 전달된 명령을 일정 수 이상(2f) 수신하면 Primary(Replica0)를 포함한 모든 노드에 수신한 신호를 전송
⑤ 각 노드는 ④에서 보낸 명령을 일정 수 이상(2f) 수신하면 명령을 실행하고 블록을 등록해 client에 reply를 반환

변경된 ②번 절차를 살펴보면, PBFT 알고리즘에서는 Primary가 정해져 있으나, 변형된 알고리즘에서는 규정에 따라 유동적으로 Primary가 결정된다. 즉, 서울시 공무원이 Client가 되면, 서울시 부동산종합공부시스템인 Replica0이 Primary가 되고, 제주도의 공무원이 Client가 되면, 제주도 부동산종합공부시스템이 Primary가 되어 리더 역할을 수행하게 된다.

6. 결론

이상에서 블록체인의 종류와 합의 알고리즘, 주요 합의 알고리즘의 특징을 살펴보고, 부동산종합공부시스템에 블록체인을 적용하기 위해, 블록체인 시스템은 어떻게 구성되어야하고, 합의 알고리즘은 어떤 방식으로 변경될 수 있는지 살펴보았다.

본 논문에서 도출한 부동산종합공부 블록체인 시스템 구성 및 합의 알고리즘은 법령에 의해 정해진 내용만을 토대로 도출한 기초모델로서, 실제 활용에는 많은 검토가 필요할 것이다.

따라서, 부동산종합공부 시스템 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.

참고문헌

[1] 임명환, “블록체인 기술의 활용과 전망”, ETRI Creative Open ECO 시리즈, Insight Report 2016-03

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

[3] 손경호, “블록체인 응용 기술, 공공영역도 넘보나”, <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] Laura Shin, “Republic Of Georgia To Pilot Land Titling On Blockchain With Economist Hernando De Soto, BitFury”, <Forbes>, 2016.4.21.

[7] 국토교통부, http://www.molit.go.kr

[8] 아카하네 유시하루 외, “블록체인 구조와 이론”, 위키북스, 2016

[9] 이부형,임연주,이종혁,“블록체인 플랫폼에서의 합의 알고리즘”,한국통신학회 2017 동계종합학술발표회, 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, November 2002.

[11] 부동산종합공부시스템 운영 및 관리규정 (시행: 2014.12.31.)

[12] 부동산등기법 (시행: 2017.10.13.)