

블록체인 기반 농업기계 공유 시스템 설계

Design of Agricultural Machine Sharing System Based on Blockchain

손용범, 김영학
금오공과대학교 컴퓨터공학과

Yong-Bum Son(sonyb@kumoh.ac.kr), Young-Hak Kim(kimyh@kumoh.ac.kr)

요약

최근 국내외 많은 국가들이 블록체인을 활용하여 관련 응용분야에 활용하고 있다. 기업 중심의 경제가 아닌, 개인이 주체가 될 수 있는 공유 경제의 개념도 확산되었다. 그러나 농업분야의 공유 경제 실현에 필요한 시스템 구축은 아직 미비하다. 현재 농업정책 중 농업기계 임대사업은 국가가 주체가 되어 시행되는 사업으로 지자체에서 비치하여 제공하기 때문에 한정된 수량과 자원으로 제한적이다. 고가의 농업기계의 경우 바쁜 농번기에는 수량이 한정되어 있기 때문에 임대 물량이 부족한 현실이다. 본 논문에서는 농업기계 소유주 개개인을 연결하여 한정된 수량의 농업기계를 블록체인 기술을 이용하여 개인의 농업기계를 경작자에게 차용해주는 공유 시스템을 제안한다. 따라서 본 시스템은 한정된 수량의 농업기계 자원을 해결하고 경작자 모두에게 안전한 서비스와 같은 분산 시스템을 제공한다.

■ **중심어** : | 블록체인 | 비트코인 | 농업기계 | 암호화폐 | 분산 시스템 |

Abstract

Many domestic and international countries recently apply the blockchain technology to its related application fields. Not the enterprise-centered economy, the concept of the sharing economy which is controlled by individuals has been expanded. However, the development of the necessary system to realize the sharing economy in the agricultural sector has still been insufficient. Because the agricultural machinery rental business in the recent agricultural policies is managed by the government and the local government keeps and provides limited quantities and resources, its operation system has several problems. In case of high-priced agricultural machines, the machines can not be supplied adequately at the right time due to the limited quantities during the busy farming season. This paper proposes the sharing system that individual owners rent their agricultural machinery to growers using the blockchain technology. Thus, the proposed system provides the distributed method to solve agricultural machines of a lack of resources and also gives the secure service to all the growers.

■ **keyword** : | Blockchain | Bitcoin | Agricultural Machinery | Crypto-currency | Distributed System |

1. 서 론

사토시 나카모토(Satoshi Nakamoto)라는 가공의 인

물이 비트코인(Bitcoin)에 대한 논문을 발표하면서 블록체인(Blockchain)의 개념이 알려지게 되었다[1]. 비트코인은 종래의 은행과 같은 제3자의 개입 없이 개인 간

* 본 연구는 금오공과대학교 학술연구비로 수행되었습니다.(2017-104-059)

접수일자 : 2018년 09월 11일

수정일자 : 2018년 09월 19일

심사완료일 : 2018년 09월 19일

교신저자 : 김영학, e-mail : kimyh.kumoh.ac.kr

의(P2P, Peer-to-Peer) 안전한 거래가 가능한 결제 시스템으로써 블록체인 기술을 사용한 첫 사례이다. 비트코인 결제 시스템에 참여하고 있는 모든 사용자들은 시스템에서 발생하는 모든 거래에 대한 기록(Transaction)을 자신의 블록체인에 저장하고 저장된 기록을 토대로 시스템에서 발생하는 모든 거래를 검증하여 유효한 거래만 자신의 블록체인에 새롭게 추가한다. 이 동작을 시스템의 모든 사용자가 개별적으로 수행하여 최종적으로 시스템의 모든 사용자가 하나의 동일한 블록체인을 유지·보관하는 분산원장기술이다[2]. 블록체인 기술은 현재 금융업 분야에 가장 널리 사용되고 있다. 이는 운영절차의 간소화, 규제 효율성 향상, 거래상대방 위험감소, 정산 및 결제시간 단축, 유동성 개선, 부정거래발생 최소화 등의 변화를 가져올 것이라 예상된다. 비 금융업 분야에서는 온라인 스마트 계약 서비스와 사물인터넷 간의 금융거래 및 분권형 관리 시스템을 개발 중에 있다. 또한 의료분야에서도 블록체인 기술이 도입되기 위한 노력이 진행 중이며 국내 의료정보시스템 HIS(병원정보시스템)와 EMR(전자의무기록) 등에 적용되고 있다[3].

현재 지자체에서 시행되고 있는 농업기계 임대사업은 경작자의 초기 비용 부담을 줄이고, 일손 부족 해결 및 농가 수익을 올리는 것이 목적이다. 하지만 농업기계 임대사업에 대한 인식부족으로 뚜렷한 목표와 세부적인 기준을 마련하지 않고 추진함으로써 일관성 없이 운영되고 있다. 일부 지자체에서는 농업기계 임대사업으로 구입한 농업기계를 특정인에게 장기 임대해줌으로써 실질적으로 이용해야 하는 소규모 농가들이 이용하지 못하는 사례가 있어 이를 개선하기 위해 농업기계 임대기준 선정기준을 제시하고 발작물용 농업기계의 경우 본체보다는 가격이 낮고 유지관리가 용이한 작업기 중심으로 추진하도록 유도하고 있으며, 농업기계 임대사업을 운영하고 있는 대부분의 지자체에서는 저가의 임대료를 받고 사업을 추진하고 있어 내용연한 종료 후 새로운 대체 농업기계 구입을 위한 재원이 확보되지 못하고 있다. 따라서 추가 예산 확보가 어려운 자치단체에서 자칫 지속적인 사업추진이 어려울 것으로 전망되므로 수익성 확보를 위한 다양한 임대 농업사업 개발

이 필요하다[4].

블록체인 기술을 접목한 사례들은 많은 관심과 지속적인 연구 개발로 발전하고 있지만, 농업분야의 농업기계 임대사업에는 블록체인을 접목한 기술이 현재 적용되지 않고 있다. 본 논문에서는 국가에서 운영하는 농업기계 임대사업의 부족한 농업기계 자원을 블록체인 기술을 이용하여 개인 소유의 농업기계를 다른 경작자에게 공유 가능한 분산 시스템을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 블록체인 종류와 기술적 특성에 대해서 설명한다. 3장에서는 기존 시스템 및 운영사례에 대해서 소개한다. 4장은 블록체인을 이용한 제안 기법을 제시한다. 5장에서는 성능평가를 수행하고, 6장에서는 본 논문에 대한 결론을 제시한다.

II. 관련 연구

1. 블록체인

블록체인은 분산 데이터베이스의 한 모양으로, 지속적으로 발전하는 데이터 기록 리스트로서 분산 데이터의 운영자에 의한 임의 조작이 불가능하도록 고안되었다. 잘 알려진 블록체인의 응용사례로는 암호화폐의 거래과정을 기록하는 전자장부로서 비트코인이 있다. 거래 기록은 의무적으로 암호화되며 블록체인 소프트웨어를 실행하는 컴퓨터에서 운영된다. 중앙 집중형 방식인 Client/Server 자원공유를 하지 않고 P2P 자원공유 방식을 사용하기 때문에 원하는 자원을 서버에서 허가해야 받을 수 있는 것이 아니라 서로에게 요청을 하여 블록체인으로 연결되어 있는 공동체끼리 자원을 자연스럽게 공유할 수 있다[5].

블록체인 기법에는 2가지 종류가 있다. 사설형 블록체인(Private blockchain)과 공개형 블록체인(Public blockchain)이다.

1.1 사설형 블록체인

사설형 블록체인은 중앙기관이 모든 권한을 보유하며 중앙기관에 의해 허가받은 사용자만 접근이 가능한

시스템이다. 거래 주체의 식별이 가능하고 처리 속도가 빠르며 네트워크 확장이 용이할 뿐 아니라 중앙기관의 결정에 따라 거래 법칙의 변경이 가능하다. 블록체인의 소유자가 블록체인을 생성하고 관리하기 때문에 블록체인을 중앙시스템처럼 관리하고자 하는 경우 적합하다. 실시간 거래가 중요한 시스템은 전통적 형태의 중앙시스템으로 운영하고 거래가 체결된 이후 해당 거래 내역을 안전하고 낮은 비용으로 보관 및 검증하는 용도로 사설 블록체인을 활용할 수 있어 금융권에서 특히 관심이 높다[6].

1.2 공개형 블록체인

공개형 블록체인은 가장 기본적인 형태로 불특정 다수가 제한 없이 참여 가능한 네트워크이다. 제 3자에 의한 중앙통제 없이 모든 네트워크 참여자는 자유롭게 블록 내의 자료를 열람할 수 있고 또한 참여자들 간 거래도 자유롭게 이루어질 수 있다. 공개형 블록체인의 가장 큰 특징은 참여자의 익명성이 보장되는 것이다. 그러나 검증되지 않은 불특정 다수가 거래원장을 분산 보관해야 하며, 네트워크의 조건이 변경될 경우 참여자들의 동의나 합의를 구해야하기 때문에 네트워크의 작업 증명이라는 고도의 암호화 검증 작업이 필요하다. 따라서 거래 속도가 매우 느리고 네트워크 확장이 어렵다는 단점을 지닌다[6]. 또한 중앙시스템의 제어가 필요한 서비스에는 적합하지 않아 다양한 산업에 널리 사용되기 어렵고 불특정 다수의 참가와 네트워크에 대한 충성도를 유도하기 위해서 블록체인 상에서 발행된 코인(Coin) 등의 지불과 같은 경제적 인센티브가 필요하다[7].

2. 합의 과정

블록체인 시스템에서 노드들 간에 무결성과 신뢰성을 제공하는 블록을 생성하기 위해서 노드간의 블록을 합의하는 과정이 필요하다. 합의하는 과정에서 합의 알고리즘을 사용하여 특정 조건을 만족하는 노드가 블록을 생성하고 블록체인에 생성된 블록을 연결하게 된다. 대표적인 합의 알고리즘으로는 작업증명(PoW, Proof of Work), 지분증명(PoS, Proof of Stake), 지분위임증

명(DPoS, Delegated PoS)이 있다. 합의하는 과정을 통해서 생성된 블록의 무결성과 신뢰성을 제공한다[8].

3. Smart Contract

Smart Contract는 Nick Szabo가 1994년 최초 제안한 개념으로 기존 계약서(Contract)는 서면으로 되어있어 계약 조건을 이행하려면 사람이 직접 수행해야 하지만 디지털 계약(Digital contract)은 조건에 따라 자동으로 체결이 된다고 주장하였다. 블록체인은 다수의 노드가 데이터를 검증하고, 검증된 것들을 기반으로 노드들끼리 공유하는 방식을 통해 디지털 데이터의 신뢰를 생성한다. 믿을 수 있는 데이터를 기반으로 Smart contract는 블록체인과 함께 이슈화되기 시작했다. Smart Contract 기법을 적용한 블록체인 동작 구조는 다음과 같다. 물품을 구매하려는 구매자와 판매자가 있다고 가정할 때 판매자는 블록체인에 팔고자하는 물품을 등록시킨다. 이때 Smart contract는 Transaction에 따라 해당 블록체인에 새로운 노드를 등록하고 실시간으로 최신화 한다. 구매자는 검색(Query)을 이용해 해당 블록체인을 조회할 수 있고 물품을 구매한다면 Smart contract가 해당 노드의 데이터베이스를 최신화 한다[9].

4. 디지털 서명

전자서명이란 서명자를 확인하고 서명자가 당해 전자 문서에 서명하였음을 인증하기 위하여 당해 전자 문서에 첨부되거나 논리적으로 결합한 전자적 형태의 정보를 말한다. 공개키 암호기술에 기반을 두는 방식으로 서명자는 한 쌍의 공개키와 개인키를 소유하며 자신의 개인키와 암호화 알고리즘을 통하여 메시지에 서명한다. 검증자는 서명자의 공개키와 암호화 알고리즘으로 서명의 유효성을 검증한다[10].

블록체인을 통한 거래에서 직접적인 당사자들의 서명행위는 발생하지 않지만 특정 조건을 이행하기 위한 전자서명 절차로 보는 견해도 존재하는데, 만약 블록체인의 디지털 서명 기술이 법률상의 전자서명의 범위에 해당한다면 동법에 따라 정부는 가입자 및 이용자를 보호해야 할 의무를 갖게 되며, 또한 전자서명의 상호인

정을 위해 외국과의 협정을 체결할 수 있게 되므로 블록체인의 거래의 글로벌화에 매우 중요한 영향을 미칠 수 있게 된다[11].

5. 향만물류분야

비트코인으로 금융 분야에서 먼저 발전하기 시작한 블록체인은 그 다음으로 물류 분야에서 주목받기 시작했다. 이는 블록체인의 특징인 거래 원장이 분산되고, 신뢰할 수 없는 사용자에게 안전하며, 거래 내역이 투명하고, 데이터의 위변조가 어려운 것이 물류 사업에 적합하기 때문이다. 블록체인을 물류 공급망에 적용하면 데이터 위변조가 어려운 블록체인의 특성에 따라 제품의 생산부터 최종 소비까지 공급 이력이 투명하게 공개된다. 이로써 유통 과정에서 원산지 조작, 제조 및 유통기간 변경, 제품 바꿔치기 등이 불가능해진다. 이에 소비자들은 식자재에 대한 신뢰도를 높일 수 있고, 제품의 정품 유무와 제품의 가격에 대한 정당한 가치를 측정할 수 있다[12].

III. 기존 시스템 및 운영 사례

1. 농업기계 임대사업 배경

농업기계 임대사업은 농촌인구 감소와 고령화로 인한 일손 부족을 해결하고 고가의 농업기계 구입비용을 덜어줌으로써 농가부채를 경감하기 위해 일정부분 정부에서 지원하는 사업이다. 연간 농업 작업에 필요한 다양한 종류의 농업기계를 농업인에게 소비비용 부담 없이 이용할 수 있도록 지원한다. 발·논 경작시 농업기계를 비교적 낮은 임대료로 장·단기 임대하는 것을 말한다. 2003년 5개소를 시작으로 2011년까지 120개 지자체 시·군 농업기술센터에 220개소가 지원되어 시·군당 평균 1.8개소를 설치하였으며, 사업비로 1,679억원이 지원되었다. 지속적인 임대사업의 추진과 투자로 인하여 임대사업 기종의 연간 작업일수는 해당 평균 7일로 일반 농업기계 작업일수 1.5일 대비 4.7배의 이용률을 기록하고 있고, 농가의 농업기계 구입비용도 2,429억원을 절감하는 효과가 있어 농업인들이 정부의 농업분야 지

원사업 중 가장 인기 있는 사업으로 자리매김하게 되었다[13].

정부에서 추진하는 농업기계 임대사업의 문제점은 농번기에 특정 농업기계의 집중화로 임대 지연 및 임대료 납부방법 등의 불편을 들 수 있다.

2. 농업기계 임대시스템 사례

현재 지방자치단체에서 운영하는 농업기계 임대사업을 위한 시스템 구조는 Client/Server 기반의 중앙 집중형 서비스를 제공한다. 국가 예산으로 농업기계 자원을 할당 받아 웹 사이트를 통해 농업기계 임대서비스를 운영하고 있다. 농업기계 임대시스템 절차는 아래와 같다.

1. 임대인은 시스템을 통해 회원가입
2. 농업기계 재고 여부 확인
3. 장비대여 신청
4. 임대료 이체 후 완료

세부적인 농업기계 임대시스템의 절차는 다음 [그림 1]과 같다.

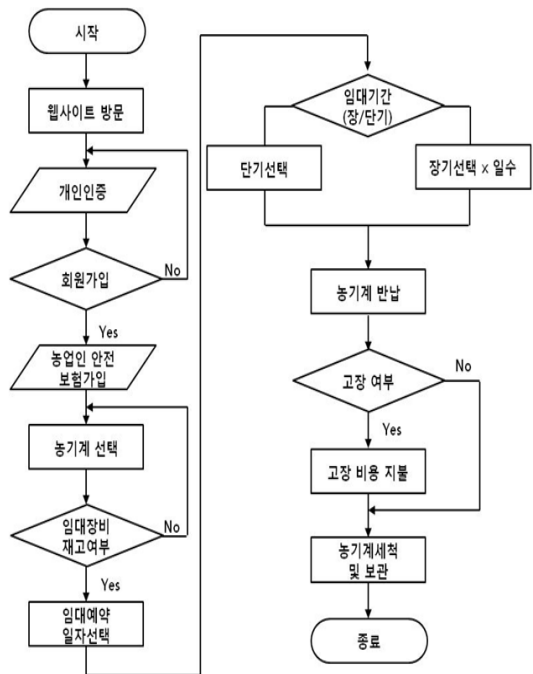


그림 1. 농업기계 임대 절차

3. 기존 시스템 문제점

국가에서 운영하고 있는 농업기계 임대시스템의 경우 중앙 집중형 기반 서비스를 제공한다. 바쁜 농번기에는 농업기계 임대를 위해 많은 경작자들이 시스템을 이용하고 있으며, 중앙 집중형의 경우 일시적으로 접속량이 늘어나면 과부하로 인해 정상적인 서비스 제공이 불가능하다. 또한 메인 서버에 악의적인 공격을 받게 되면 서비스 이용에 차질과 개인정보 누출 등 보안 위협을 받게 된다. 뿐만 아니라 현재 시스템은 초기 장비 도입 단계와 운영 예산이 많이 들어가는 단점이 있다. 국가에서 운영하는 농업기계 임대사업은 한정된 자원으로 농번기에는 대여하기 힘든 실정이다.

IV. 블록체인을 이용한 제안 기법

1. 제안 시스템

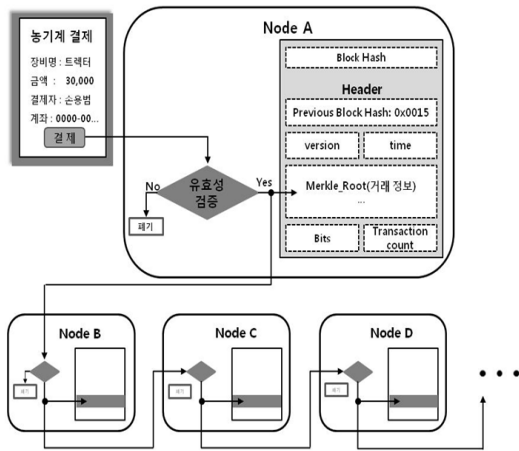


그림 2. 제안 시스템 블록체인 구조

본 논문에서는 기존 중앙 집중형 서비스 방식에서 블록체인 기술을 이용하여 분산 구조 방식(P2P)의 농업기계 공유 시스템을 제안한다. 블록체인 기반의 분산 시스템의 구조는 모든 노드들이 연결되어 정보를 공유하는 방식이다.

위 [그림 2]처럼 선택된 농업기계를 결제 신청하면 거래 기록은 모든 회원에게 공유된다. 계약 정보는 모

든 회원에게 저장되어 있기 때문에 거래가 투명하고, 개인 대 개인 결제가 체결됨으로써 악의적인 공격으로부터 안전하다. 또한 일시적으로 접속량이 증가해도 분산 시스템 특성상 정상적인 서비스 제공이 가능하다.

2. 농업기계 공유 및 임대 절차

개인이 소유하고 있는 농업기계를 해당 시스템을 통해서 공유하는 절차는 다음과 같다.

- a. 시스템 사용을 위해서는 본인인증을 통해 회원가입을 한다. 회원가입 완료와 함께 전자지갑이 생성된다.
- b. 농업기계 소유자는 임대를 위해 농업기계 정보(모델명, 거래위치, 대여기간, 대여비용)를 입력하고 등록을 신청한다.
- c. 등록된 농업기계 정보는 시스템에 정의해 놓은 규약에 적합한 경우에 승인 처리된다.
- d. 승인 처리된 농업기계 정보는 시스템에 참여한 모든 회원에게 공유된다.

기존 시스템에서 불편했던 농업기계 임대료 결제 부분을 개선하여 암호화폐 결제 방식을 적용한다. 임대료 결제를 위해서 농업기계 공유 시스템을 통해 암호화폐를 구입하고, 임대인에게 농업기계 임대료를 전자지갑으로 이체하면 계약이 완료된다. 암호화폐의 기준은 거래 기반이며, 이자 및 수수료는 지불하지 않는다. 다음은 농업기계를 임대하는 절차를 알아본다.

- a. 시스템 사용을 위해서는 본인인증을 통해 회원가입을 한다. 회원가입 완료와 함께 전자지갑이 생성된다.
- b. 시스템에 공유된 농업기계 정보를 확인하고, 원하는 장비를 대여 신청한다.
- c. 임대료 결제를 위해서 시스템을 통해 암호화폐를 구입하고, 임대인의 전자지갑으로 임대료를 이체하면 계약이 완료된다.
- d. 계약 정보는 시스템에 참여한 전체 회원에게 공유된다.
- e. 거래가 완료된 후에는 해당 거래에 대해 완료 처리되고, 해당 농업기계 정보는 출력되지 않는다.
- f. 임대료로 받은 암호화폐는 실제 통화로 환전가능

하다.

3. 핵심 알고리즘 기법

PoW 알고리즘을 사용하고 있는 비트코인은 시스템에 참여한 컴퓨터를 이용하여 해시 연산을 수행하고 블록생성 및 검증의 대가로 암호화폐를 받는 채굴 방법과 실제 통화를 암호화폐로 교환해서 사용하는 2가지 방법이 있다. 본 논문에서 제안하는 농업기계 공유 시스템은 PoW 알고리즘을 그대로 사용하면서 실제 통화를 암호화폐로 교환해서 사용하는 방법만 적용하고자 한다.

비트코인의 PoW 알고리즘을 구성하는 하나의 블록 헤더(Block Header)에는 Merkle Root, Previous Block Hash, Version, Time, Bits, Nonce 6가지 정보로 구성된다. 이때 Nonce 값을 제외한 요소들은 블록 해시(Block Hash)를 만드는 시점에서 값이 정해져 있다. Nonce 값은 확정되어 있지 않고, 채굴(mining)을 할 때 0부터 1씩 증가 시켜 조건을 만족하는 해시 값을 찾아내는 역할을 한다.

본 논문에서는 기존 알고리즘의 복잡한 계산 작업인 채굴 과정을 생략하고 블록생성 시간을 단축시키고자 한다. 먼저, 시스템을 통해 회원가입을 하면, 계좌번호와 같은 지갑주소(Wallet Address)가 생성된다. 상대방의 지갑주소로 암호화폐를 이체하면 거래 가능하다. PoW 알고리즘에서 채굴을 할 때 사용하는 Bits 대신 Wallet Address로, Nonce 대신 Transaction count(거래 횟수)로 대체한다. 블록체인을 구성하는 하나의 블록 크기는 0.98MB이며, 1,800건의 계약 정보를 저장한다. 블록 생성 방법은 계약 건수가 1,800건 단위로 다음 블록을 생성한다. 블록체인을 연결하는 블록 해시의 값은 블록 헤더를 SHA256한 값으로 다음 블록의 Previous Block Hash와 연결하여 체인을 구성한다. 블록 해시는 하나의 블록 식별자 역할을 하며, 블록 헤더를 해시한 값으로 이루어져 보안 측면에서도 안전하다. 농업기계 공유 시스템은 비트코인의 PoW 알고리즘과 같은 채굴 과정을 통해 암호화폐를 받는 과정이 필요 없으며, 본 논문에서 제안하는 알고리즘이 농업기계 공유 시스템의 분산 시스템을 구성하는데 더 적합하다.

본 시스템의 수행 절차는 아래와 같다.

1. A가 B에게 송금한다.
2. 계약 정보는 P2P 네트워크를 통해 전체 회원에게 공유된다.
3. 블록생성은 계약 정보가 1,800건 단위로 블록을 생성하고, 시스템에 참여한 전체 노드에 공유한다. 블록해시 값은 블록 헤더를 해시한 값으로 생성된다.
4. 블록을 받은 각 노드는 블록을 검증 후 이상이 없는 경우 자신의 블록체인에 추가한다.
5. 동시에 블록을 생성한 경우 분기가 일어나며, 이후 체인의 길이가 긴 쪽이 기준이 된다.
6. 계약은 완료된다.

V. 성능 평가

본 시스템의 알고리즘은 PoW 알고리즘에서 개선된 알고리즘으로 블록 헤더 구성을 변형하였으며, 두 알고리즘을 비교 분석한다.

PoW 알고리즘의 채굴은 확률적으로 해답이 어려운 문제를 가장 빨리 해결한 사람에게 블록을 만들 수 있도록 허가하고 그 보상으로 코인을 준다[12]. 이 방식은 중앙 집권적인 관리자가 없지만 사람들이 보상을 위해 P2P 네트워크에 참여하기 때문에 시스템이 자율적으로 운영된다. 네트워크 불일치가 발생해 블록이 분기한 경우에는 가장 긴 블록체인을 올바른 것으로 함으로써 데이터의 일관성을 보장하고 있다. PoW 알고리즘의 수행 과정은 아래 [그림 3]과 같다.

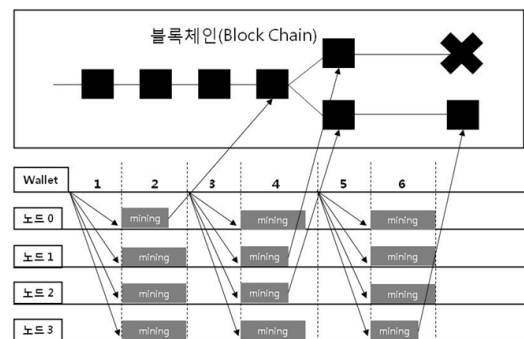


그림 3. Proof of Work 구조[14]

1. Wallet이 거래를 수행하고 모든 노드에 공유한다.
2. 받은 승인자는 해시를 계산하고, 먼저 발견한 노드 0이 만든 블록이 블록체인에 추가된다.
3. Wallet이 거래를 수행하고 모든 노드에 공유한다.
4. 받은 승인자는 해시를 계산하고, 먼저 발견한 노드 1과 노드 2가 동시에 발견했기 때문에 블록체인이 분기된다.
5. Wallet이 거래를 수행하고 모든 노드에 공유한다.
6. 받은 승인자는 해시를 계산하고, 먼저 발견한 노드 3이 만든 블록을 노드 2 뒤에 추가한다. 이후 체인의 길이가 긴 쪽이 올바른 것으로 변경된다.

PoW 알고리즘은 채굴을 할 때 Bits보다 작은 Nonce를 찾는 과정을 반복하고, 값을 찾게 되면 보상의 개념으로 코인을 획득한다. 하지만 본 논문에서는 채굴을 통해 코인을 지급하는 방식을 사용하지 않고, 블록 헤더 정보를 변형하였다. 채굴 과정에서 사용되는 Bits를 Wallet Address로, Nonce를 Transaction count로 대체하였으며, 비교한 블록 구조는 아래 [그림 4]와 같다.

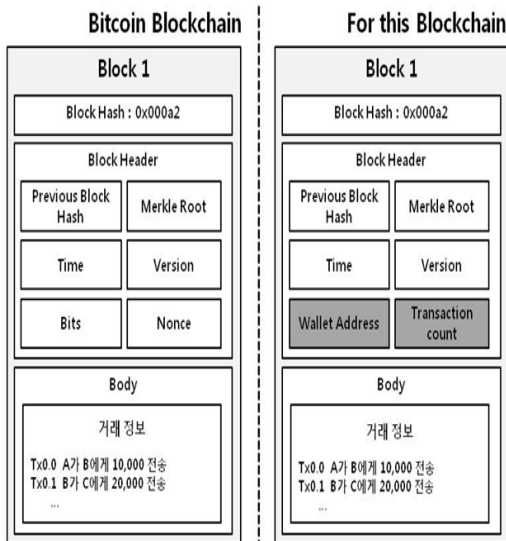


그림 4. 비트코인 블록과 제안 시스템 블록 비교

비트코인의 PoW 알고리즘 같은 경우 하나의 블록을 체인에 생성하는데 약 10분이라는 시간이 소요된다. 본

논문에서는 채굴을 생략하기 때문에 보다 빠른 시간에 블록을 생성한다. 비트코인과 본 시스템의 성능 비교는 아래 [표 1]과 같다.

표 1. 비트코인과 제안 시스템 알고리즘 타입 비교

	Bitcoin[15]	For this system
Algorithm	PoW	Make by self
Mining	Yes	No
Network	Public	Public
Transaction time	Slow	Fast

VI. 결론

농촌인구 감소와 고령화로 인해 부족한 일손 문제를 해결하기 위해 정부에서는 농업기계 임대사업을 추진해 왔다. 고가의 농업기계를 경작자가 구입하지 않고, 지자체에서 시행하는 농업기계 임대사업을 통해 사용할 수 있어 큰 비용을 절감할 수 있다. 하지만 정부 지원의 한계와 농번기에만 과다 사용되는 농업기계는 한정된 자원으로 인해 경작자가 필요한 시점에 사용할 수 없어 제철 작물 시기를 놓치는 문제점이 발생한다.

본 연구에서는 이를 해결하기 위해 블록체인 기술을 이용하여 개인 소유의 농업기계를 경작자에게 임대 가능한 분산 시스템을 제시하였다. 기존 시스템에서 불편했던 결제 방식을 비트코인 PoW 알고리즘을 개선하여 암호화폐 기반의 결제를 통해 편리하게 대여 신청 가능하다. 그 결과 개인 소유의 자산인 고가의 농업기계를 필요로 하는 경작자와 공유함으로써 지연 없이 사용할 수 있고 농가의 제철 작물 계획이 가능하다. 현재 시행되고 있는 지자체의 임대사업을 개선하여 한정된 수량의 농업기계를 확보하여 부족한 예산을 해소함으로써 농업기계 유지비용을 절감한다. 또한 안전한 결제 방식으로 신뢰할 수 있고 임대 수익은 경작자에게 지불함으로써 농가 수익을 올릴 수 있는 방안을 제시하였다.

하지만 본 연구의 한계로는 농업기계의 자원 확보를 위해 공유를 함으로써 경작자가 실사용에 발생할 수 있는 고장과 관련된 부분이다. 고장이 났을 때의 비용 산정과 수리 기간 절차의 프로세스가 필요하다. 경작자가

자발적으로 참여하여 지속 가능한 사업으로 발전하기 위해서는 고장에 관한 안전한 장치가 마련되어야 한다. 향후에는 본 논문에서 제시한 시스템 설계를 바탕으로 구현 및 테스트를 통해 검증하는 연구를 진행할 계획이다.

참 고 문 헌

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. [Internet]. Available: <https://bitcoin.org/bitcoin.pdf>

[2] 노시완, 이경현, "퍼블릭 블록체인 보안 위협과 블록체인 확장성 문제의 연관성에 대한 분석," 정보보호학회지, 제28권, 제3호, pp.26-32, 2018.

[3] 박정홍, "의료산업 블록체인 도입을 위한 연구," 한국콘텐츠학회논문지, 제18권, 제6호, pp.155-168, 2018.

[4] 홍순중 허윤근, 정선옥, "IPA 분석을 통한 농업기 계 임대사업의 전략적 개선방안," 농업과학연구, 제40권, 제4호, pp.385-394, 2013.

[5] 홍성혁, 박상희, "블록체인 기반 사물인터넷 인증 연구," 한국융합학회논문지, 제8권, 제11호, pp.57-62, 2017.

[6] 양재훈, "물류산업의 블록체인 적용효과와 법적 과제에 대한 연구," 제8권, 제1호, pp.187-199, 2018.

[7] 정승화, "블록체인 기술기반의 분산원장 도입을 위한 법적 과제-금융산업을 중심으로-, " 한국금융법학회, 제13권, 제2호, pp.107-138, 2016.

[8] 이성범, 이부형, 명세인, 이종혁, "블록체인 시스템의 보안성 분석 : 암호 화폐에서의 사례 연구," 정보보호학회논문지, 제28권, 제1호, pp.5-14, 2018.

[9] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk:The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts," 2016 IEEE Symposium on Security and Privacy, pp.839-858, 2016.

[10] 권상완, 김동욱, 이경우, "프락시 기반 애플리케이션 전자서명 검증 시스템," 정보보호학회논문지, 제27권, 제4호, pp.743-751, 2018.

[11] <http://www.law.go.kr/lsInfoP.do?lsiSeq=195204&efYd=20170726#0000>

[12] 최종석, 박종규, 김명길, 김호원, "블록체인 기반 탈중앙화 사물인터넷 플랫폼 연구," 정보보호학회지, 제27권, 제6호, pp.5-14, 2017.

[13] 홍순중, 허윤근, 정선옥, 홍성현, "자료포락분석법을 이용한 농기계 임대사업의 효율성 분석," 충남대학교 농업과학연구소, 제39권, 제2호, pp.279-289, 2012.

[14] 아카하네 요시하루, 아이케이 마나부, *블록체인 구조와 이론*, 위키북스, 2018.

[15] 안규황, 서화정, "블록체인 기반 기부 시스템 개발," 한국정보통신학회논문지, 제22권, 제5호, pp.812-817, 2018.

저 자 소 개

손 용 범(Yong-Bum Son)

정회원



- 2010년 8월 : 금오공과대학교 컴퓨터공학과(공학사)
- 2012년 8월 : 금오공과대학교 컴퓨터공학과(공학석사)
- 2016년 9월 ~ 현재 : 금오공과대학교 컴퓨터공학과(박사과정)

<관심분야> : 블록체인, 임베디드시스템, 분산처리 등

김 영 학(Young-Hak Kim)

중신회원



- 1984년 2월 : 금오공과대학교 전자공학과(공학사)
- 1989년 2월 : 서강대학교 전자계산학과(공학석사)
- 1997년 8월 : 서강대학교 전자계산학과(공학박사)

• 1999년 3월 ~ 현재 : 금오공과대학교 컴퓨터공학과 교수

<관심분야> : 블록체인, 병렬알고리즘, 분산처리, 임베디드시스템 등