



Technical – White Paper

(한글판)

Ver 1.0

blockchain기반 비즈니스 플랫폼 구현을 위한 Qcity

작성 유영근

qcitycoin@gmail.com

qnapse@qcitycoin.org

목 차

1. Proof of Online
2. 온라인 증명 블록체인 생성 시스템 및 방법
(System and Method for generating blockchain with proof of online)
3. 카드 매출 채권 기반 가상 화폐 발행 방법 및 발행 장치
(Issuing method of virtual money based on credit card receivables and
Issuing apparatus of virtual money based on credit card receivables)

Proof Of Online - 온라인 블록 생성 증명

배경

블록체인의 51% 공격 중 BWA(Block Withholding Attack)에 대한 보완책으로 블록의 온라인 동기화 여부에 대한 증명 (Proof Of Online) 을 사용한다.

현재의 문제점

공격자가 블록체인의 51% 이상의 해쉬 파워를 취득하여 의도적으로 오프라인 상태에서 더 긴 블록을 생성한 뒤 온라인화할 경우 이중지불공격이 가능하다.

이의 방지를 위해서 블록이 온라인 상태에서 동기화 되어 있는지를 증명하는 방식을 고안하였다.

51% Attack 시나리오

공격자가 51%의 해쉬 파워를 취득한 경우 공격자는 자신의 블록을 네트워크에 전파하지 않고 가지고 있을 수 있다.

블록체인의 네트워크 동기화 알고리즘은 노드가 보유하고 있는 높이보다 더 높은 높이의 블록이 존재할 경우 해당 블록을 최종블록으로 판단하여 보유하고 있는 블록을 파기하고, 더 높은 블록을 받아 들이도록 설계되어 있다.

공격자는 이를 이용하여, 외부의 노드보다 더 많은 블록을 오프라인 상태에서 생성하고 거래소등을 통해서 자신이 보유한 코인을 사용한 이후, 자신의 노드를 네트워크에 공개하여 자신이 사용한 코인을 사용이전의 상태로 되돌릴 수 있다.

기존 비트코인등을 비롯한 모든 PoW 기반의 코인은 잠재적으로 해당 위험을 보유하고 있으며, 적은 PoW의 해쉬파워를 보유한 코인들은 해당 공격에 노출되어 있다. 실제로 몇몇 코인들에게 해당 공격으로 자금이 이중지불 되는 등의 공격이 발생한 사례들이 존재하며, 최근에도 이러한 공격의 예가 보고되어 있다.

기술의 내용

위의 위험을 보완하기 위한 방법으로 공격자가 오프라인 상태에서 일정 길이 이상의 블록을 보유하지 못하도록 하는 온라인 증명 방식이다.

이 기술의 기본적인 논리는 다음과 같다

트랜잭션

기존의 블록체인 트랜잭션은 코인베이스 트랜잭션과 일반적인 트랜잭션 두가지로 나눌 수 있다.

일반적인 트랜잭션에는 전송자와 수신자가 존재하며, 전송자의 주소(공개키)는 입력부에, 수신자의 주소(공개키) 정보는 출력부에 들어간다. 전송자는 거래 내용을 개인키로 서명(암호화)하고, 수신자는 이를 전송자의 공개키로 해독하여 실제 자격있는(해당 공개키의 개인키를 소유한) 사람이 생성한 거래인지 확인한다.

이에 비해 Coinbase 트랜잭션(tx[0])은 채굴된 코인의 첫번째 트랜잭션으로서 수신자만 존재하므로 서명정보가 필요 없다. 그러나 PoO 블록에서는 별도로 정해진 검증자들만 블록을 생성할 수 있고 이에 대한 확인을 위해 서명정보가 필요하므로 CoinOnline 이라는 새로운 형태의 트랜잭션 구조를 갖는다.

PoO 블록

블록체인의 height % n == 0 번째 블록을 PoO 블록이라 칭하며, 항상 특정 서명자가 서명한 블록을 포함하도록 한다. 큐시티는 n =10 으로하여 매 10번째 블록 즉, xxx00 , xxx10, xxx20, ... , xxx90 이 PoO 블록이 된다.

여기서 특정 서명자라 함은 해당 블록체인을 초기 설계하거나, 해당 블록체인을 운영하는 재단 또는 조직이 소유한 계정으로 검증자라 칭하며, 공개된 주소의 비밀키로 PoO 블록에 서명함으로써 해당 블록이 네트워크에 동기화 되어 있음을 제공한다. 기타 모든 노드들은 PoO 블록이 재단이 공개한 주소로 서명이 되었음을 확인하여, 해당 블록을 받아 들인다.

검증자 공개키

일반적인 블록체인 재단등에서는 운영하는 노드들을 프로그램 소스에 반영하거나, SeedDns 에 최우선적으로 등록하여, 네트워크상의 대부분의 노드들이 기본적으로 접속을 하고, 기타 네트워크를 찾는 Seed 가 되게 하는 SeedNode 방식을 사용한다.

이 방식을 따라서 재단이 운영하는 검증자 공개키 목록을 프로그램 소스에 반영하고, 온라인 증명을 위한 블록 추가 작업은 검증자 공개키에게만 서명 권한을 부여한다.

운영의 방식

소스에 하드코딩된 검증자 공개키가 설정된 노드인 검증자노드 vn[0], vn[1], vn[2], vn[3], vn[4] 가 있고, 일반 채굴노드 n[0], n[1], n[2], n[3]이 있다고 하자.

검증자노드와 채굴자노드는 모두 새로운 블록 생성되었다는 정보를 수신함과 동시에 다음 블록을 만들 준비를 시작한다. 블록의 첫번째 트랜잭션은 생성된 블록에 대한 보상을 주는 코인베이스 트랜잭션이라 하는데, 자신을 수신자로 하여 생성하고, 블록에 실을 나머지 트랜잭션을 선택하여 해쉬값을 산출하고 이 값이 목표값보다 작은 경우 블록정보가 완성되어 배포할 수 있게 된다. 그러나, 새로 만들 블록이 10 번째 블록에 해당한다면 일반 채굴노드들은 자신을 수신자로하는 코인베이스 트랜잭션을 생성할 수 없다. 반면, 검증자 노드 중 하나인 $vn[0]$ 가 블록을 생성한다면, 코인베이스 트랜잭션의 출력부에 자신의 공개키를 넣고, 이 트랜잭션의 내용을 자신의 개인키로 서명(암호화)한 정보를 블록의 헤더에 담는다. 이 정보를 담기 위해 우리는 `VchBlockSig` 라는 필드를 추가했고 이 트랜잭션의 형태가 일반적인 코인베이스 트랜잭션과 다르므로 이를 코인온라인 트랜잭션이라 칭한다.

블록수신시 10번째 블록에 해당한다면 첫번째(코인온라인) 트랜잭션의 출력부에 기록된 공개키가 검증자 노드 목록중에 있는 지 확인한 다음, 이 공개키로 `VchBlockSig` 의 내용을 복호화한 데이터가 코인온라인 트랜잭션의 정보와 일치하는지 확인함으로써 정당한 검증자가 서명한 PoO 블록임을 확인한다.

온라인 증명(Proof Of Online)

위와 같은 논리로 공격자는 $\%n$ 으로 정의된 수 미만의 블록만 보유할 수 있으므로, 네트워크 해시파워를 장악하더라도, 악의적인 이중지불 공격을 할 수 있는 충분한 시간을 확보할 수 없어진다. 모든 블록의 채굴자들은 재단이 운영하는 seed 노드와 연결이 되어 있음을 해당블록으로서 확인할 수 있으며, 이러한 이유로 이 알고리즘의 이름을 온라인 증명(Proof Of Online)이라 명명한다.

채굴자와의 합의

PoO 블록의 서명을 재단이 함으로써 채굴자에게는 그만큼의 기회가 없어지므로, 적절한 $\%n$ 값의 설정이 필요하다. (20 블록마다 서명을 확인하도록 설정한 경우 채굴자는 1/20 만큼의 채굴의 기회가 사라진다.). 위의 보상방법으로 $\%n$ 블록에 대해서는 채굴보상을 지급하지 않음으로써 채굴자의 역차별을 제거한다.

위험에 대한 대비

온라인이 되어 있음을 확인하는 공개키 주소의 제공은 기본적으로 하드코딩된 주소를 이용하며, 추후 검증자가 추가되거나 권한의 이양이 필요한 경우, 검증자들에게만 주어진 권한을 이용하여 과반수 이상의 공동 서명을 통해 새로운 검증자를 추가하고, 이 내용은 각 노드의 클라이언트 내부 DB 에 보관된다.

만약 재단에서 운영하는 노드가 중단되었을 경우 모든 블록체인은 해당 블록이 생성되기를 기대하며, 기타 PoW 블록을 받아들이지 않아, 전체 블록은 운영이 중단되는 상황이 만들어 질수 있다.

이를 보완하기 위한 방법으로 %n 번째 블록이 기대 되어지는 블록타임의 2 배를 넘어 설경우 (규시티 기준 1 * 2 분) %n 번째 블록은 일반 블록을 받아 들일 수 있도록 설계되었다.

최악의 경우 검증자 노드 전체의 운영이 멈추더라도, 해당 블록체인은 지정된 블록의 채굴시간이 늦어질 뿐 전체 운영의 장애가 발생하지는 않는다.

구현의 방식

재단의 운영자는 검증자 공개키의 과반수가 넘는 노드에서 PoO 마이닝을 항상 유지 해야 하며, 그 구현 방법은 다음과 같다.

일반적인 블록의 첫번째 트랜잭션인 tx[0]는 마이닝에 대한 보상인 Coinbase 트랜잭션이나, PoO 블록의 tx[0]는 이를 변형한 형태이며 CoinOnline 트랜잭션이라 칭한다.

	CoinBase	CoinOnline
입력[0]	size()== 1, prevout == null	size()==1,prevout == null
출력	size()>=1	size()>=1 && size()<=3 출력[0]==empty() 출력[1].scriptPubkey== 제공된 공개키중 하나 출력[2].scriptPubkey = 새롭게 제공되어지는 공개키
Validation Code	vin.size()==1 &&vin[0].prevout.IsNull()	vin().size()==1&& &&vin[0].prevout.IsNull() vout.size()>=1 && vout[0].isEmpty() && vout.size()<=3 && vout[1].scriptPubKey == 제공된 공개키중 하나&& vout[1].nValue== Block.nFees&& vout[2].scriptPubKey == invalid() &&vout[2].nValue== 0

(prevout : 이전 트랜잭션의 정보, vin : 입력부, vout : 출력부)

위와 같이 CoinOnline 트랜잭션은 Coinbase 나 일반적인 트랜잭션과 구조가 다르므로, 다음과 같은 일반적인 블록체인의 구조 중 헤더 영역에 VchBlockSig 필드를 추가하여 PoO 블록의 검증자 서명정보를 담는다.

version	0250000	}	Header
previous block hash	3450b3d32g3257d...		
Merkle root	8a239d32kfs34hg...		
timestamp	35680433		
bits	2451d126		
nonce	4286321		
VchBlockSig	[]		
transaction count	53		
CoinBase transaction		}	Body
transaction			
...			

[코인베이스 트랜잭션의 구조]

version	0250000	}	Header
previous block hash	3450b3d32g32...		
Merkle root	8a239d32kfs34...		
timestamp	35680433		
bits	2451d126		
nonce	4286321		
VchBlockSig	32kfs34hg318...		
transaction count	53		
CoinOnline transaction		}	Body
transaction			
...			

[코인온라인 트랜잭션의 구조]

출원번호통지서

출원일자 2018.09.21
특기사항 심사청구(유) 공개신청(무)
출원번호 10-2018-0113973 (접수번호 1-1-2018-0947430-44)
출원인성명 유명근(4-2000-044972-3)
대리인성명 장인구(9-2010-000243-9)
발명자성명 유명근 김지한
발명의명칭 온라인 증명 블록체인 생성 시스템 및 방법

특 허 청 장

<< 안내 >>

1. 귀하의 출원은 위와 같이 정상적으로 접수되었으며, 이후의 심사 진행상황은 출원번호를 통해 확인하실 수 있습니다.
2. 출원에 따른 수수료는 접수일로부터 다음날까지 동봉된 납입영수증에 성명, 납부자번호 등을 기재하여 가까운 우체국 또는 은행에 납부하여야 합니다.
※ 납부자번호 : 0131(기관코드) + 접수번호
3. 귀하의 주소, 연락처 등의 변경사항이 있을 경우, 즉시 [특허고객번호 정보변경(경정), 정정신고서]를 제출하여야 출원 이후의 각종 통지서를 정상적으로 받을 수 있습니다.
※ 특허로(patent.go.kr) 접속 > 민원서식다운로드 > 특허법 시행규칙 별지 제5호 서식
4. 특허(실용신안등록)출원은 명세서 또는 도면의 보정이 필요한 경우, 등록결정 이전 또는 의견서 제출기간 이내에 출원서에 최초로 첨부된 명세서 또는 도면에 기재된 사항의 범위 안에서 보정할 수 있습니다.
5. 외국으로 출원하고자 하는 경우 PCT 제도(특허·실용신안)나 마드리드 제도(상표)를 이용할 수 있습니다. 국내출원일을 외국에서 인정받고자 하는 경우에는 국내출원일로부터 일정한 기간 내에 외국에 출원하여야 우선권을 인정받을 수 있습니다.
※ 제도 안내 : <http://www.kipo.go.kr>-특허마당-PCT/마드리드
※ 우선권 인정기간 : 특허·실용신안은 12개월, 상표·디자인은 6개월 이내
※ 미국특허상표청의 선출원을 기초로 우리나라에 우선권주장출원 시, 선출원이 미공개상태이면, 우선일로부터 16개월 이내에 미국특허상표청에 [전자적교환허가서(PTO/SB/39)]를 제출하거나 우리나라에 우선권 증명서류를 제출하여야 합니다.
6. 본 출원사실을 외부에 표시하고자 하는 경우에는 아래와 같이 하여야 하며, 이를 위반할 경우 관련법령에 따라 처벌을 받을 수 있습니다.
※ 특허출원 10-2010-0000000, 상표등록출원 40-2010-0000000
7. 종업원이 직무수행과정에서 개발한 발명을 사용자(기업)가 명확하게 승계하지 않은 경우, 특허법 제62조에 따라 심사단계에서 특허거절결정되거나 특허법 제133조에 따라 등록이후에 특허무효사유가 될 수 있습니다.
8. 기타 심사 절차에 관한 사항은 동봉된 안내서를 참조하시기 바랍니다.

【발명의 설명】

【발명의 명칭】

온라인 증명 블록체인 생성 시스템 및 방법{System and Method for generating block chain with proof of online}

【기술분야】

<0001> 본 발명은 온라인 증명 블록체인 생성 시스템 및 방법에 관한 것이다.

【발명의 배경이 되는 기술】

<0002> 비트코인은 2008년 사토시 나카모토라는 정체불명의 인물이 발표한 논문에서 시작되었다. 비트코인은 정부나 은행과 같은 중앙화된 조직이 아닌 분산 네트워크 상에서 발행, 저장 및 유통되는 전자 화폐이다. 비트코인은 2009년 처음 발행되어 현재시점까지 중앙화된 기관 없이 화폐의 가치를 유지하고 있으며, 사용자 수와 거래 규모가 꾸준히 증가하고 있다.

<0003> 이러한 비트코인의 화폐 가치를 유지하는 배경에는 블록체인 기술이 있다. 블록체인은 중앙화된 서버 없이 탈중앙화된 네트워크 환경에서 보안성과 무결성을 유지하는 기술이다. 달리 표현하면, 블록체인은 중앙 관리 기관이 없이 임의의 사용자가 데이터를 위변조하는 것을 불가능하게 하여 거래의 무결성을 유지한다.

<0004> 블록체인이 무결성 유지를 위해 블록체인 네트워크에 참여한 모든 참여 노드는 거래 내역(장부)를 저장하고, 새롭게 생성되는 트랜잭션을 저장된 장부를 통해 검사한다.

<0005> 예를 들어, 한 참여 노드가 거래를 조작하여 이중 결재를 감행하여도, 다른

모든 노드가 이중 결제 여부를 검증하여 합의를 부결함으로써, 거래의 승인이 거부된다.

<0006> 그러나 작업 증명(Proof of Work) 같은 방식으로 수행되는 종래 블록체인 시스템은 전체 노드 중 51% 이상이 거짓으로 합의하면 데이터 조작이 가능한 일명 51퍼센트 어택(51 percent attack)이 발생할 수 있다.

<0007> 보다 상세히, 종래 블록체인 시스템에서 노드는 기 보유하고 있는 블록체인보다 긴 블록체인이 존재할 경우 해당 블록체인을 기준으로 작업을 수행하도록 설계되어 있다.

<0008> 51퍼센트 이상의 해쉬 파워를 보유한 공격자는 조작된 장부를 포함하고, 현재 무결성을 가지는 블록체인보다 긴 블록체인을 만들어 네트워크에 공유시키는 방식으로 데이터를 조작할 수 있다.

【발명의 내용】

【해결하고자 하는 과제】

<0009> 본 발명의 실시예는, 외부 공격자에 의한 조작이 어려운 블록체인을 생성하는 시스템을 제공하는 것이다.

【과제의 해결 수단】

<0010> 본 발명의 일 측면에 따르면, 트랜잭션을 포함하는 블록이 순차적으로 연결되는 블록체인을 생성하는 시스템으로서, 상기 블록체인에 새롭게 연결될 블록이 설정된 순번의 블록일 때, 인증 데이터를 포함하고, 해당 설정된 순번에 배치되는 인증 블록을 생성하는 인증 노드; 및 상기 블록체인에 새롭게 연결될 블록이 설정

된 순번이 아닌 순번의 블록일 때, 해당 순번에 배치되는 일반 블록을 생성하는 채굴 노드를 포함하는, 온라인 증명 블록체인 생성 시스템이 제공될 수 있다.

<0011> 상기 인증 데이터는, 상기 인증 노드에 할당된 공개키 데이터와, 상기 인증 노드에 할당된 비밀키로 암호화된 암호화 데이터를 포함할 수 있다.

<0012> 상기 인증 블록은 이전 블록의 해시값이 기재되는 헤더부와 트랜잭션이 기재되는 바디부를 포함하는 구조를 가지고, 상기 바디부는 상기 인증 블록의 코인베이스 트랜잭션이 기재되는 코인베이스 트랜잭션 기재부와 일반 트랜잭션이 기재되는 일반 트랜잭션 기재부를 포함하는 구조를 가지며, 상기 공개키 데이터는 상기 코인베이스 트랜잭션 기재부에 기재되고, 상기 암호화 데이터는 상기 헤더부에 기재될 수 있다.

<0013> 상기 암호화 데이터는 상기 코인베이스 트랜잭션 기재부에 기재된 데이터를 상기 인증 노드에 할당된 비밀키로 암호화하여 생성될 수 있다.

<0014> 상기 인증 노드는 상기 인증 블록을 생성한 후 상기 인증 블록을 상기 채굴 노드로 전송하고, 상기 채굴 노드는 수신한 상기 인증 블록에 포함된 상기 인증 데이터를 기초로 상기 인증 블록이 상기 인증 노드에 의해 생성되었는지 여부를 검증한다.

<0015> 상기 인증 노드는, 상기 블록체인에 새롭게 연결될 블록이 설정된 순번의 블록이면서, 현재 시점이 기준 시점으로부터 설정된 시간 내일 때, 해당 설정된 순번에 배치되는 인증 블록을 생성한다.

<0016> 상기 채굴 노드는, 상기 블록체인에 새롭게 연결될 블록이 설정된 순번의 블

록이라도, 현재 시점이 기준 시점으로부터 설정된 시간을 초과하면, 해당 설정된 순번에 배치되는 일반 블록을 생성할 수 있다.

<0017> 본 발명의 다른 측면에 따르면, 트랜잭션을 포함하는 블록이 순차적으로 연결되는 블록체인을 생성하는 방법으로서, 인증 노드가 상기 블록체인에 새롭게 연결될 블록이 설정된 순번의 블록일 때, 인증 데이터를 포함하고, 해당 설정된 순번에 배치되는 인증 블록을 생성하는 단계; 및 채굴 노드가 상기 블록체인에 새롭게 연결될 블록이 설정된 순번이 아닌 순번의 블록일 때, 해당 순번에 배치되는 일반 블록을 생성하는 단계를 포함하는 온라인 증명 블록체인 생성 방법이 제공될 수 있다.

<0018> 상기 인증 데이터는, 상기 인증 노드에 할당된 공개키 데이터와, 상기 인증 노드에 할당된 비밀키로 암호화된 암호화 데이터를 포함할 수 있다.

<0019> 상기 인증 블록은 이전 블록의 해시값이 기재되는 헤더부와 트랜잭션이 기재되는 바디부를 포함하는 구조를 가지고, 상기 바디부는 상기 인증 블록의 코인베이스 트랜잭션이 기재되는 코인베이스 트랜잭션 기재부와 일반 트랜잭션이 기재되는 일반 트랜잭션 기재부를 포함하는 구조를 가지며, 상기 공개키 데이터는 상기 코인베이스 트랜잭션 기재부에 기재되고, 상기 암호화 데이터는 상기 헤더부에 기재될 수 있다.

<0020> 상기 암호화 데이터는 상기 코인베이스 트랜잭션 기재부에 기재된 데이터를 상기 인증 노드에 할당된 비밀키로 암호화하여 생성될 수 있다.

<0021> 상기 인증 노드는 상기 인증 블록을 생성한 후 상기 인증 블록을 상기 채굴

노드로 전송하고, 상기 채굴 노드는 수신한 상기 인증 블록에 포함된 상기 인증 데이터를 기초로 상기 인증 블록이 상기 인증 노드에 의해 생성되었는지 여부를 검증할 수 있다.

<0022> 상기 인증 노드는, 상기 블록체인에 새롭게 연결될 블록이 설정된 순번의 블록이면서, 현재 시점이 기준 시점으로부터 설정된 시간 내일 때, 해당 설정된 순번에 배치되는 인증 블록을 생성할 수 있다.

<0023> 상기 채굴 노드는, 상기 블록체인에 새롭게 연결될 블록이 설정된 순번의 블록이라도, 현재 시점이 기준 시점으로부터 설정된 시간을 초과하면, 해당 설정된 순번에 배치되는 일반 블록을 생성할 수 있다.

【발명의 효과】

<0024> 본 발명의 실시예에 따르면, 네트워크 상에서 블록체인이 생성되는 과정에서 블록체인의 설정된 순번에 인증 노드에 의해 인증된 인증 블록이 연결되도록 함으로써, 외부의 공격자에 의한 블록체인의 위변조가 어려워지고, 블록체인의 무결성을 보장할 수 있다.

【도면의 간단한 설명】

<0025> 도 1은 본 발명의 일 실시예에 따른 블록체인 생성 시스템의 개략 구성도이다.

 도 2는 본 발명의 일 실시예에 따른 블록체인 생성 시스템에 의해 생성된 블록체인의 개략적인 구조를 나타내는 도면이다.

 도 3은 본 발명의 일 실시예에 따른 블록체인 생성 시스템에서 생성되는 일

반 블록의 구조를 나타내는 개략도이다.

도 4는 본 발명의 일 실시예에 따른 블록체인 생성 시스템에서 생성되는 인증 블록의 구조를 나타내는 개략도이다.

도 5는 본 발명의 일 실시예에 따른 블록체인 생성 시스템에서 인증 노드가 인증 블록을 생성하는 과정의 일례를 설명하기 위한 도면이다.

도 6은 본 발명의 일 실시예에 따른 블록체인 생성 시스템에서 채굴 노드가 일반 블록을 생성하는 과정의 일례를 설명하기 위한 도면이다.

도 7은 본 발명의 일 실시예에 따른 블록체인 생성 시스템에서 노드가 다른 노드에서 생성되어 전파된 블록을 수신하여 검증하는 과정의 일례를 설명하기 위한 도면이다.

도 8은 본 발명의 일 실시예에 따른 블록체인 생성 시스템에서 인증 노드가 인증 블록을 생성하는 과정의 다른예를 설명하기 위한 도면이다.

도 9는 본 발명의 일 실시예에 따른 블록체인 생성 시스템에서 채굴 노드가 일반 블록을 생성하는 과정의 다른예를 설명하기 위한 도면이다.

도 10은 본 발명의 일 실시예에 따른 블록체인 생성 시스템에서 노드가 다른 노드에서 생성되어 전파된 블록을 검증하는 과정의 다른예를 설명하기 위한 도면이다.

【발명을 실시하기 위한 구체적인 내용】

본 발명은 다양한 변환을 가할 수 있고 여러 가지 실시예를 가질 수 있는 바, 특정 실시예들을 도면에 예시하고 상세한 설명에 상세하게 설명하고자 한다.

그러나, 이는 본 발명을 특정한 실시 형태에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변환, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다. 본 발명을 설명함에 있어서 관련된 공지 기술에 대한 구체적인 설명이 본 발명의 요지를 흐릴 수 있다고 판단되는 경우 그 상세한 설명을 생략한다.

<0027> 이하, 본 발명의 실시예를 첨부도면을 참조하여 상세히 설명하기로 하며, 첨부 도면을 참조하여 설명함에 있어, 동일하거나 대응하는 구성 요소는 동일한 도면 번호를 부여하고 이에 대한 중복되는 설명은 생략하기로 한다.

<0028> 도 1은 본 발명의 일 실시예에 따른 블록체인 생성 시스템의 개략 구성도이고, 도 2는 본 발명의 일 실시예에 따른 블록체인 생성 시스템에 의해 생성된 블록체인의 개략적인 구조를 나타내는 도면이다.

<0029> 도 1 및 도 2를 참조하면, 블록체인 생성 시스템은 적어도 하나의 인증 노드와, 적어도 하나의 채굴 노드(30)를 포함한다. 인증 노드(10)는 인증 블록(IB)을 생성한다. 인증 노드(10)는 블록체인 생성 시스템 개발사 또는 운영사에서 운영하는 노드이다. 인증 노드(10)는 블록체인 생성 시스템 개발사 또는 운영사로부터 할당된 비밀키와 공개키를 가진다.

<0030> 인증 노드(10)는 기존 블록체인에 새롭게 연결될 블록이 설정된 순번의 블록일 때, 해당 설정된 순번에 배치되는 인증 블록(IB)을 생성한다.

<0031> 예컨대, 인증 노드(10)는 블록체인의 20의 배수에 해당하는 순번마다 인증 블록(IB)을 생성할 수 있다. 이 경우, 인증 노드(10)는 블록체인의 20번째 블록,

40번째 블록, 60번째 블록 등을 인증 블록(IB)으로 생성한다.

<0032> 인증 블록(IB)은 해당 인증 노드(10)에서 생성하였음을 증명하는 인증 데이터를 포함한다. 인증 노드(10)가 인증 블록(IB)에 인증 데이터를 포함시키는 것은 일종의 서명이라 할 수 있다.

<0033> 인증 블록(IB)은 후술하는 일반 블록(AB)과 마찬가지로 트랜잭션 데이터를 포함한다.

<0034> 인증 노드(10)가 인증 블록(IB)을 생성하는 과정 및 인증 블록(IB)의 구조는 후술한다.

<0035> 채굴 노드(30)는 기존 블록체인에 새롭게 연결될 블록이 설정된 순번이 아닌 순번의 블록일 때, 다시 말해 기존 블록체인에 새롭게 연결될 블록이 설정된 순번이 아닐 때, 해당 순번에 배치되는 일반 블록(AB)을 생성한다. 채굴 노드(30)는 예컨대 작업 증명(Proof Of Work)과 같은 공지된 방법으로 일반 블록(AB)을 생성할 수 있다.

<0036> 예컨대, 채굴 노드(30)는 이전 블록의 해시값(보다 상세히, 이전 블록의 헤더의 해시값)과 트랜잭션 데이터 등을 모아 후보 블록을 생성하고, 후보 블록의 헤더에 기재되는 난스(Nonce) 값을 증가시키면서 후보 블록의 헤더의 해시값이 특정 숫자보다 작은 값을 찾으면 채굴에 성공하여 일반 블록(AB)을 생성한다.

<0037> 인증 노드(10)와 채굴 노드(30)는 네트워크를 통해 상호 연결된다. 인증 노드(10)와 채굴 노드(30)는 정보처리 기능과 통신 기능을 갖는 네트워크 상의 호스트이다.

<0038> 인증 노드(10) 및 채굴 노드(30)는 각각 기존 블록체인에 연결되는 새로운 블록을 생성하여 다른 노드에 전송하거나 다른 노드에서 생성된 새로운 블록을 수신하고 검증하여 이를 기존 블록체인에 연결한다.

<0039> 한편, 블록체인 기술의 특성 상 새로운 블록이 동시에 서로 다른 노드에서 탄생될 수 있고, 이로 인해 '블록체인의 분기'가 발생할 수도 있으나 이러한 '블록체인의 분기'는 본 명세서에서는 논외로 한다.

<0040> 다만, 비트 코인 블록체인의 경우 시스템 상으로 작업증명을 많이 수행한 블록이 우선시되기 때문에 시간이 지남에 따라 가장 긴 블록체인만이 살아 시스템을 운영함에 있어서 '블록체인의 분기'가 문제되지 않는다는 것을 이론과 현실로 확인할 수 있다.

<0041> 본 실시예에 따른 블록체인 생성 시스템은 네트워크 상에서 블록체인이 생성되는 과정에서 블록체인의 설정된 순번에 인증 노드(10)에 의해 인증된 인증 블록(IB)이 연결되도록 함으로써, 외부의 공격자에 의한 블록체인의 위변조가 어려워지고, 블록체인의 무결성을 보장할 수 있다.

<0042> 다시 말해, 네트워크 상에 접속된 노드들만이 인증 노드(10)에 의해 인증된 인증 블록을 수신 및 검증한 후 다음 블록을 생성할 수 있어, 네트워크에 접속하지 않은 공격자가 블록체인을 위변조하는 것은 대단히 어렵고, 이에 따라 블록체인의 무결성이 보장된다.

<0043> 본 출원인은 이와 같이 본 실시예에 따른 블록체인 생성 시스템에서 생성되는 블록체인을 소위 온라인 증명 블록체인이라 명명한다.

<0044> 도 3은 본 발명의 일 실시예에 따른 블록체인 생성 시스템에서 생성되는 일반 블록의 구조를 나타내는 개략도이고, 도 4는 본 발명의 일 실시예에 따른 블록체인 생성 시스템에서 생성되는 인증 블록의 구조를 나타내는 개략도이다.

<0045> 도 1 및 도 3을 참조하면, 채굴 노드(30)가 생성하는 일반 블록은 헤더부와 바디부를 포함하는 구조를 가진다.

<0046> 헤더부는 이전 블록의 해시값을 기재하는 '이전 블록 해시 필드'와, 해당 블록의 생성 시간 값을 기재하는 '타임스탬프(timestamp) 필드'와, 난스(nonce) 값을 기재하는 '난스 필드' 등을 가진다. 각 필드에는 해당 값이 기재된다. 예컨대, 난스 필드'에는 채굴 노드(30)가 작업 증명(Proof Of Work)과 같은 공지된 방법으로 채굴에 성공할 때 찾아낸 난스(nonce) 값이 기재된다.

<0047> 그리고 헤더부는 후술하는 인증 블록의 구조에 대응하도록 암호화 데이터를 기재하는 '암호화 데이터 필드'를 가진다. 본 실시예에서 일반 블록은 인증 블록과 달리 암호화 데이터와 무관하기 때문에 일반 블록의 '암호화 데이터 필드'에는 설정된 디폴트 값이 기재된다.

<0048> 참고로 도 3에서 헤더부의 각 필드에 기재된 값은 설명의 편의를 위해 임의로 기재된 값이다.

<0049> 바디부에는 코인베이스 트랜잭션 기재부와 일반 트랜잭션 기재부를 포함하는 구조를 가진다.

<0050> 코인베이스 트랜잭션 기재부에는 블록 생성의 보상에 관한 데이터가 기재된다.

<0051> 일반 트랜잭션 기재부에는 해당 블록을 생성할 당시 네트워크를 통해 수집된 적어도 하나의 트랜잭션이 기재된다.

<0052> 도 1 및 도 4를 참조하면, 인증 노드(10)가 생성하는 인증 블록은 헤더부와 바디부를 포함한다.

<0053> 헤더부는 이전 블록의 해시값을 기재하는 '이전 블록 해시 필드'와, 해당 블록의 생성 시간 값을 기재하는 '타임스탬프(timestamp) 필드'와, 암호화 데이터를 기재하는 '암호화 데이터 필드'등을 가진다.

<0054> 그리고 헤더부는 일반 블록의 구조에 대응하도록 난스(nonce) 값을 기재하는 '난스(nonce) 필드'를 가진다. 본 실시예에서 인증 블록은 일반 블록과 달리 작업 증명(Proof Of Work)과 같은 공지된 방법으로 생성되지 않기 때문에 인증 블록의 '난스 필드'에는 설정된 디폴트 값이 기재된다.

<0055> 참고로 도 4에서 헤더부의 각 필드에 기재된 값은 설명의 편의를 위해 임의로 기재된 값이다.

<0056> 바디부에는 코인베이스 트랜잭션 기재부와 일반 트랜잭션 기재부를 포함하는 구조를 가진다.

<0057> 코인베이스 트랜잭션 기재부에는 블록 생성의 보상에 관한 데이터가 기재된다. 다만, 인증 블록을 생성하는 인증 노드(10)는 블록체인 생성 시스템 개발사 또는 운영사에서 운영하는 노드이기 때문에 블록 생성의 보상에 관한 내용은 일반 블록에 적용되는 보상에 관한 내용과 상이하다.

<0058> 일반 트랜잭션 기재부에는 해당 블록을 생성할 당시 네트워크를 통해 수집된

적어도 하나의 트랜잭션이 기재된다.

<0059> 본 실시예에서 인증 블록은 인증 데이터를 포함한다.

<0060> 예컨대, 인증 데이터는 인증 노드(10)에 할당된 공개키 데이터와 인증 노드(10)에 할당된 비밀키로 암호화된 암호화 데이터를 포함한다.

<0061> 이때, 공개키 데이터는 코인베이스 트랜잭션 기재부에 블록 생성의 보상에 관한 데이터와 함께 기재되고, 암호화 데이터는 헤더부의 '암호화 데이터 필드'에 기재된다.

<0062> 이때, 암호화 데이터는 코인베이스 트랜잭션 기재부에 기재된 데이터를 인증 노드(10)에 할당된 비밀키로 암호화하여 생성된다.

<0063> 도 5는 본 발명의 일 실시예에 따른 블록체인 생성 시스템에서 인증 노드가 인증 블록을 생성하는 과정의 일례를 설명하기 위한 도면이다. 도 1 및 도 5를 참조하면, 인증 노드는 기존 블록체인에 새롭게 연결될 블록이 설정된 순번인지를 판단한다.

<0064> 만약, 새롭게 연결될 블록이 설정된 순번이라면, 인증 노드(10)는 자신이 만들었음을 증명하는 인증 데이터를 포함하는 인증 블록을 생성한다. 이후, 인증 노드(10)는 생성된 인증 블록을 다른 노드에 전파한다.

<0065> 만약, 새롭게 연결될 블록이 설정된 순번이 아니라면, 인증 노드(10)는 일반 블록을 생성할 수 있다. 이후, 인증 노드(10)는 생성된 일반 블록을 다른 노드에 전파한다. 다만, 인증 노드(10)는 설정 순번이 아닌 특정 순번의 일반 블록을 생성하는 과정에서 다른 채굴 노드(30)에서 먼저 생성하여 전파시킨 해당 특정 순번의

일반 블록을 수신하게 되면, 이를 검증하고 검증에 성공하면 검증된 블록을 기존 블록체인에 연결하고 다음 작업을 수행한다.

<0066> 한편, 도시되지 않았으나 인증 노드(10)는 새롭게 연결될 블록이 설정된 순번이 아니라고 판단되어도 도 5와 같이 일반 블록을 생성하는 작업을 수행하지 않을 수 있다. 이 경우, 인증 노드(10)는 현재 시점에서 새롭게 연결될 블록이 설정된 순번인지를 계속적으로 판단하고, 계속된 판단 과정에서 다른 노드들의 지속적인 채굴 작업으로 인해 네트워크 상에서 동기화되어 공유된 블록체인에 새롭게 연결될 블록이 설정된 순번이 되었을 때 인증 블록을 생성할 수 있다.

<0067> 도 6은 본 발명의 일 실시예에 따른 블록체인 생성 시스템에서 채굴 노드가 일반 블록을 생성하는 과정의 일례를 설명하기 위한 도면이다. 도 1 및 도 6을 참조하면, 채굴 노드(30)는 기존 블록체인에 새롭게 연결될 블록이 설정된 순번인지를 판단한다.

<0068> 만약, 새롭게 연결될 블록이 설정된 순번이 아니라면, 채굴 노드(30)는 일반 블록을 생성한다. 이후, 채굴 노드(30)는 생성된 일반 블록을 다른 노드에 전파한다.

<0069> 만약, 새롭게 연결될 블록이 설정된 순번이라면, 채굴 노드(30)는 새롭게 연결될 블록이 설정된 순번인지를 계속적으로 판단한다. 이 과정에서 인증 노드(10)가 설정된 순번에 배치될 인증 블록을 생성하여 전파시킴으로써 네트워크 상에서 동기화된 블록체인에 새롭게 연결될 블록은 설정된 순번의 다음 블록이 된다. 이후, 채굴 노드(30)는 새롭게 연결될 블록이 설정된 순번이 아니라고 판단하게 되어

일반 블록을 생성한다.

<0070> 한편, 채굴 노드(30)는 특정 순번의 일반 블록을 생성하는 과정에서 다른 노드에서 먼저 생성하여 전파시킨 해당 특정 순번의 일반 블록을 수신하게 되면, 이를 검증하여 기존 블록체인에 연결하고, 해당 특정 순번의 일반 블록의 다음 순번에 배치될 일반 블록의 생성 작업을 수행한다.

<0071> 도 7은 본 발명의 일 실시예에 따른 블록체인 생성 시스템에서 노드가 다른 노드에서 생성되어 전파된 블록을 수신하여 검증하는 과정의 일례를 설명하기 위한 도면이다.

<0072> 도 7을 참조하면, 노드(이하, 설명의 편의를 위해 '검증 노드'라 함)는 다른 노드에서 생성하여 전파시킨 새로운 블록, 즉 검증 노드가 보유하고 있는 기존 블록체인에 새롭게 연결될 블록을 수신한다. 도 7에서 검증 노드는 도 1에 도시된 인증 노드(10) 중 하나 또는 채굴 노드(30) 중 하나일 수 있다.

<0073> 이후, 검증 노드는 새로운 블록이 기존 블록체인의 설정된 순번의 블록인지 판단한다.

<0074> 만약, 새로운 블록이 설정된 순번의 블록이면, 검증 노드는 인증 블록 검증을 수행한다.

<0075> 여기서, 인증 블록 검증은 검증 대상인 인증 블록에 포함된 인증 데이터를 기초로 해당 인증 블록이 해당 인증 노드에 의해 생성되었는지 여부를 검증하는 것이다.

<0076> 보다 상세히, 검증 노드는 검증 대상인 인증 블록에서 인증 데이터를 추출한

다. 앞서 설명한 바와 같이 인증 데이터는 해당 인증 노드의 공개키 데이터와 암호화 데이터를 포함한다.

<0077> 검증 노드는 검증 대상인 인증 블록에서 해당 인증 노드의 공개키 데이터와 암호화 데이터를 추출한다.

<0078> 이후, 검증 노드는 추출된 공개키 데이터로 암호화 데이터를 복호화한다. 앞서 설명한 바와 같이 암호화 데이터는 해당 노드가 해당 인증 블록의 코인베이스 트랜잭션 기재부에 기재된 데이터를 자신의 비밀키로 암호화하여 생성된다.

<0079> 이후, 검증 노드는 복호화된 데이터와 검증 대상인 인증 블록의 코인베이스 트랜잭션 기재부에 기재된 데이터를 비교하여 일치 여부를 확인한다. 두 데이터가 일치하면 검증 대상인 인증 블록이 해당 인증 노드에서 생성되었다고 신뢰할 수 있다.

<0080> 검증 노드는 위와 같은 과정을 통해 검증 대상인 인증 블록이 해당 인증 노드에 의해 생성되었는지 여부를 검증한다.

<0081> 인증 블록 검증 결과, 검증 대상인 인증 블록이 인증 블록 검증을 통과하면, 검증 노드는 기존 블록체인에 연결하고, 다른 노드에 성공 메시지를 전송한다. 또는 인증 블록 검증 결과, 검증 대상인 인증 블록이 인증 블록 검증을 통과하지 못하면, 검증 노드는 다른 노드에 거절 메시지를 전송한다.

<0082> 한편, 검증 노드는 수신된 새로운 블록이 설정된 순번의 블록인지 판단한 결과 설정된 순번의 블록이 아니면, 일반 블록 검증을 수행한다.

<0083> 여기서 일반 블록 검증은 작업 증명(Proof Of Work)과 같은 공지된 방법에서

새로운 블록을 검증하는 과정으로 수행될 수 있다. 예컨대, 검증 노드는 수신된 검증 대상인 일반 블록의 헤더의 해시값이 특정 숫자보다 작은지, 블록 데이터 구조가 적정한지 등을 검증할 수 있다.

<0084> 일반 블록 검증 결과, 검증 대상인 일반 블록이 일반 블록 검증을 통과하면, 검증 노드는 해당 일반 블록을 기존 블록체인에 연결하고, 다른 노드에 성공 메시지를 전송한다.

<0085> 또는 일반 블록 검증 결과, 검증 대상인 일반 블록이 일반 블록 검증을 통과하지 못하면, 검증 노드는 다른 노드에 거절 메시지를 전송한다.

<0086>
<0087> 도 8은 본 발명의 일 실시예에 따른 블록체인 생성 시스템에서 인증 노드가 인증 블록을 생성하는 과정의 다른예를 설명하기 위한 도면이다. 도 1 및 도 8을 참조하면, 인증 노드(10)는 기존 블록체인에 새롭게 연결될 블록이 설정된 순번인지를 판단한다.

<0088> 만약, 새롭게 연결될 블록이 설정된 순번이라면, 인증 노드(10)는 현재 시점이 기준 시점으로부터 설정 시간 내인지 여부를 판단한다.

<0089> 예컨대, 기준 시점은 기존 블록체인에 새롭게 연결될 블록의 이전에 생성된 블록일 수 있다. 달리 표현하면, 기준 시점은 기존 블록체인의 마지막에 배치된 블록이 생성된 시점일 수 있다.

<0090> 이 경우, 인증 노드(10)는 현재 시점이 기준 시점으로부터 설정 시간 내인지 여부를 판단한다. 예컨대,

설정 시간은 5분 또는 10분일 수 있으나 이에 국한되지 않는다.

<0091> 인증 노드(10)는 기존 블록체인에 새롭게 연결될 블록의 이전 블록의 헤더부의 '타임스탬프 필드'에 기재된 데이터를 통해 해당 이전 블록의 생성 시점을 확인할 수 있다.

<0092> 만약, 현재 시점이 기준 시점으로부터 설정된 시간 내라면, 인증 노드(10)는 자신이 만들었음을 증명하는 인증 데이터를 포함하는 인증 블록을 생성한다. 이후, 인증 노드(10)는 생성된 인증 블록을 다른 노드에 전파한다.

<0093> 만약, 현재 시점이 기준 시점으로부터 설정된 시간을 초과하면, 인증 노드(10)는 해당 설정된 순번에 배치되는 일반 블록을 생성할 수 있다. 이 경우, 현재 시점이 기준 시점으로부터 설정된 시간을 초과하면 인증 노드(10)라도 인증 블록을 생성할 수 없다. 이에 대해 후술한다.

<0094> 한편, 인증 노드(10)는 기존 블록체인에 새롭게 연결될 블록이 설정된 순번 인지 판단한 결과, 설정된 순번이 아니라면, 일반 블록을 생성할 수 있다. 이후, 인증 노드(10)는 생성된 일반 블록을 다른 노드에 전파한다.

<0095> 한편, 인증 노드(10)가 앞서 설명한 바와 같이 설정 순번이지만 설정된 시간을 초과하여 해당 설정 순번의 일반 블록을 생성하거나 설정 순번이 아닌 특정 순번의 일반 블록을 생성하는 과정에서 다른 채굴 노드(30)에서 먼저 생성하여 전파시킨 해당 순번의 일반 블록을 수신하게 되면, 이를 검증하고 검증된 블록을 기존 블록체인에 연결한 후 다음 작업을 수행한다.

<0096> 도 9는 본 발명의 일 실시예에 따른 블록체인 생성 시스템에서 채굴 노드가

일반 블록을 생성하는 과정의 다른예를 설명하기 위한 도면이다. 도 1 및 도 9를 참조하면, 채굴 노드(30)는 기존 블록체인에 새롭게 연결될 블록이 설정된 순번인지를 판단한다.

<0097> 만약, 새롭게 연결될 블록이 설정된 순번이 아니라면, 채굴 노드(30)는 일반 블록을 생성한다. 이후, 채굴 노드(30)는 생성된 일반 블록을 다른 노드에 전파한다.

<0098> 만약, 새롭게 연결될 블록이 설정된 순번이라면, 채굴 노드(30)는 현재 시점이 기준 시점으로부터 설정 시간 내인지 여부를 판단한다.

<0099> 만약, 현재 시점이 기준 시점으로부터 설정된 시간 내라면, 채굴 노드(30)는 새롭게 연결될 블록이 설정된 순번인지를 계속적으로 판단한다.

<0100> 만약, 현재 시점이 기준 시점으로부터 설정된 시간을 초과하면, 채굴 노드(30)는 해당 설정된 순번에 배치될 일반 블록을 생성할 수 있다. 이후, 채굴 노드(30)는 블록 생성에 성공하면 생성된 일반 블록을 다른 노드에 전파한다.

<0101> 본 실시예에 따른 블록체인 생성 시스템에 있어서 인증 노드(10) 및 채굴 노드(30)는 도 8 및 도 9에서 설명한 바와 같이 기존 블록체인에 새롭게 연결될 블록이 설정된 순번의 블록이라도 기준 시간으로부터 설정된 시간을 초과한 경우 해당 설정된 순번에 배치될 일반 블록을 생성하는 알고리즘으로 작동한다. 이 경우, 모든 인증 노드(10)가 제대로 작동하지 않아 장시간 동안 해당 설정된 순번에 인증 블록이 생성되지 않아 시스템 전체가 기존 블록체인에 연결될 새로운 블록을 생성하는 과정이 장시간 지연되는 것을 미연에 방지할 수 있다.

<0102> 도 10은 본 발명의 일 실시예에 따른 블록체인 생성 시스템에서 노드가 다른 노드에서 생성되어 전파된 블록을 검증하는 과정의 다른예를 설명하기 위한 도면이다.

<0103> 도 10을 참조하면, 노드(이하, 설명의 편의를 위해 검증 노드라 함)는 다른 노드에서 생성하여 전파시킨 새로운 블록, 즉 검증 노드가 보유하고 있는 기존 블록체인에 새롭게 연결될 블록을 수신한다. 도 10에서 검증 노드는 도 1에 도시된 인증 노드(10) 중 하나 또는 채굴 노드(30) 중 하나일 수 있다.

<0104> 이후, 검증 노드는 새로운 블록이 기존 블록체인의 설정된 순번의 블록인지 판단한다.

<0105> 만약, 새로운 블록이 설정된 순번의 블록이면, 검증 노드는 새로운 블록이 생성 시점이 당시 기준 시점으로부터 설정 시간 내인지 여부를 판단한다.

<0106> 이때, 검증 노드는 새로운 블록의 생성 시점을 새로운 블록의 헤더부의 '타임스탬프 필드'에 기재된 데이터를 통해 확인할 수 있고, 당시 기준 시점은 새로운 블록의 이전 블록의 헤더부의 '타임스탬프 필드'에 기재된 데이터를 통해 확인할 수 있다.

<0107> 만약, 새로운 블록이 생성 시점이 당시 기준 시점으로부터 설정 시간 내라면, 검증 노드는 인증 블록 검증을 수행한다.

<0108> 인증 블록 검증 결과, 검증 대상인 인증 블록이 인증 블록 검증을 통과하면, 검증 노드는 기존 블록체인에 연결하고, 다른 노드에 성공 메시지를 전송한다. 또는 인증 블록 검증 결과, 검증 대상인 인증 블록이 인증 블록 검증을 통과하지 못

하면, 검증 노드는 다른 노드에 거절 메시지를 전송한다.

<0109> 만약, 새로운 블록이 생성 시점이 당시 기준 시점으로부터 설정 시간을 초과하면, 검증 노드는 일반 블록 검증을 수행한다.

<0110> 일반 블록 검증 결과, 검증 대상인 일반 블록이 일반 블록 검증을 통과하면, 검증 노드는 해당 일반 블록을 기존 블록체인에 연결하고, 다른 노드에 성공 메시지를 전송한다.

<0111> 또는 일반 블록 검증 결과, 검증 대상인 일반 블록이 일반 블록 검증을 통과하지 못하면, 검증 노드는 다른 노드에 거절 메시지를 전송한다.

<0112> 한편, 검증 노드는 수신된 새로운 블록이 설정된 순번의 블록인지 판단한 결과 설정된 순번의 블록이 아니면, 일반 블록 검증을 수행한다.

<0113> 일반 블록 검증 결과, 검증 대상인 일반 블록이 일반 블록 검증을 통과하면, 검증 노드는 해당 일반 블록을 기존 블록체인에 연결하고, 다른 노드에 성공 메시지를 전송한다.

<0114> 또는 일반 블록 검증 결과, 검증 대상인 일반 블록이 일반 블록 검증을 통과하지 못하면, 검증 노드는 다른 노드에 거절 메시지를 전송한다.

<0115>

<0116> 이상, 본 발명의 실시예들에 대하여 설명하였으나, 해당 기술 분야에서 통상의 지식을 가진 자라면 특허청구범위에 기재된 본 발명의 사상으로부터 벗어나지 않는 범위 내에서, 구성 요소의 부가, 변경, 삭제 또는 추가 등에 의해 본 발명을 다양하게 수정 및 변경시킬 수 있을 것이며, 이 또한 본 발명의 권리범위 내에 포

함된다고 할 것이다.

<0117>

【부호의 설명】

<0118>

10 : 인증 노드

30 : 채굴 노드

【청구범위】

【청구항 1】

트랜잭션을 포함하는 블록이 순차적으로 연결되는 블록체인을 생성하는 시스템에 있어서,

상기 블록체인에 새롭게 연결될 블록이 설정된 순번의 블록일 때, 인증 데이터를 포함하고, 해당 설정된 순번에 배치되는 인증 블록을 생성하는 인증 노드; 및

상기 블록체인에 새롭게 연결될 블록이 설정된 순번이 아닌 순번의 블록일 때, 해당 순번에 배치되는 일반 블록을 생성하는 채굴 노드를 포함하는, 온라인 증명 블록체인 생성 시스템.

【청구항 2】

제1항에 있어서,

상기 인증 데이터는,

상기 인증 노드에 할당된 공개키 데이터와, 상기 인증 노드에 할당된 비밀키로 암호화된 암호화 데이터를 포함하는, 온라인 증명 블록체인 생성 시스템.

【청구항 3】

제2항에 있어서,

상기 인증 블록은 이전 블록의 해시값이 기재되는 헤더부와 트랜잭션이 기재되는 바디부를 포함하는 구조를 가지고,

상기 바디부는 상기 인증 블록의 코인베이스 트랜잭션이 기재되는 코인베이스 트랜잭션 기재부와 일반 트랜잭션이 기재되는 일반 트랜잭션 기재부를 포함하는

구조를 가지며,

상기 공개키 데이터는 상기 코인베이스 트랜잭션 기재부에 기재되고,

상기 암호화 데이터는 상기 헤더부에 기재되는, 온라인 증명 블록체인 생성 시스템.

【청구항 4】

제3항에 있어서,

상기 암호화 데이터는 상기 코인베이스 트랜잭션 기재부에 기재된 데이터를 상기 인증 노드에 할당된 비밀키로 암호화하여 생성되는, 온라인 증명 블록체인 생성 시스템.

【청구항 5】

제1항에 있어서,

상기 인증 노드는 상기 인증 블록을 생성한 후 상기 인증 블록을 상기 채굴 노드로 전송하고,

상기 채굴 노드는 수신한 상기 인증 블록에 포함된 상기 인증 데이터를 기초로 상기 인증 블록이 상기 인증 노드에 의해 생성되었는지 여부를 검증하는, 온라인 증명 블록체인 생성 시스템.

【청구항 6】

제1항에 있어서,

상기 인증 노드는,

상기 블록체인에 새롭게 연결될 블록이 설정된 순번의 블록이면서, 현재 시

점이 기준 시점으로부터 설정된 시간 내일 때, 해당 설정된 순번에 배치되는 인증 블록을 생성하는, 온라인 증명 블록체인 생성 시스템.

【청구항 7】

제6항에 있어서,

상기 채굴 노드는,

상기 블록체인에 새롭게 연결될 블록이 설정된 순번의 블록이라도, 현재 시점이 기준 시점으로부터 설정된 시간을 초과하면, 해당 설정된 순번에 배치되는 일반 블록을 생성하는, 블록체인 생성 시스템.

【청구항 8】

트랜잭션을 포함하는 블록이 순차적으로 연결되는 블록체인을 생성하는 방법에 있어서,

인증 노드가 상기 블록체인에 새롭게 연결될 블록이 설정된 순번의 블록일 때, 인증 데이터를 포함하고, 해당 설정된 순번에 배치되는 인증 블록을 생성하는 단계; 및

채굴 노드가 상기 블록체인에 새롭게 연결될 블록이 설정된 순번이 아닌 순번의 블록일 때, 해당 순번에 배치되는 일반 블록을 생성하는 단계를 포함하는, 온라인 증명 블록체인 생성 방법.

【청구항 9】

제8항에 있어서,

상기 인증 데이터는,

상기 인증 노드에 할당된 공개키 데이터와, 상기 인증 노드에 할당된 비밀키로 암호화된 암호화 데이터를 포함하는, 블록체인 온라인 증명 생성 방법.

【청구항 10】

제9항에 있어서,

상기 인증 블록은 이전 블록의 해시값이 기재되는 헤더부와 트랜잭션이 기재되는 바디부를 포함하는 구조를 가지고,

상기 바디부는 상기 인증 블록의 코인베이스 트랜잭션이 기재되는 코인베이스 트랜잭션 기재부와 일반 트랜잭션이 기재되는 일반 트랜잭션 기재부를 포함하는 구조를 가지며,

상기 공개키 데이터는 상기 코인베이스 트랜잭션 기재부에 기재되고,

상기 암호화 데이터는 상기 헤더부에 기재되는, 온라인 증명 블록체인 생성 방법.

【청구항 11】

제10항에 있어서,

상기 암호화 데이터는 상기 코인베이스 트랜잭션 기재부에 기재된 데이터를 상기 인증 노드에 할당된 비밀키로 암호화하여 생성되는, 온라인 증명 블록체인 생성 방법.

【청구항 12】

제8항에 있어서,

상기 인증 노드는 상기 인증 블록을 생성한 후 상기 인증 블록을 상기 채굴

노드로 전송하고,

상기 채굴 노드는 수신한 상기 인증 블록에 포함된 상기 인증 데이터를 기초로 상기 인증 블록이 상기 인증 노드에 의해 생성되었는지 여부를 검증하는, 온라인 증명 블록체인 생성 방법.

【청구항 13】

제8항에 있어서,

상기 인증 노드는,

상기 블록체인에 새롭게 연결될 블록이 설정된 순번의 블록이면서, 현재 시점이 기준 시점으로부터 설정된 시간 내일 때, 해당 설정된 순번에 배치되는 인증 블록을 생성하는, 온라인 증명 블록체인 생성 방법.

【청구항 14】

제13항에 있어서,

상기 채굴 노드는,

상기 블록체인에 새롭게 연결될 블록이 설정된 순번의 블록이라도, 현재 시점이 기준 시점으로부터 설정된 시간을 초과하면, 해당 설정된 순번에 배치되는 일반 블록을 생성하는, 온라인 증명 블록체인 생성 방법.

【요약서】

【요약】

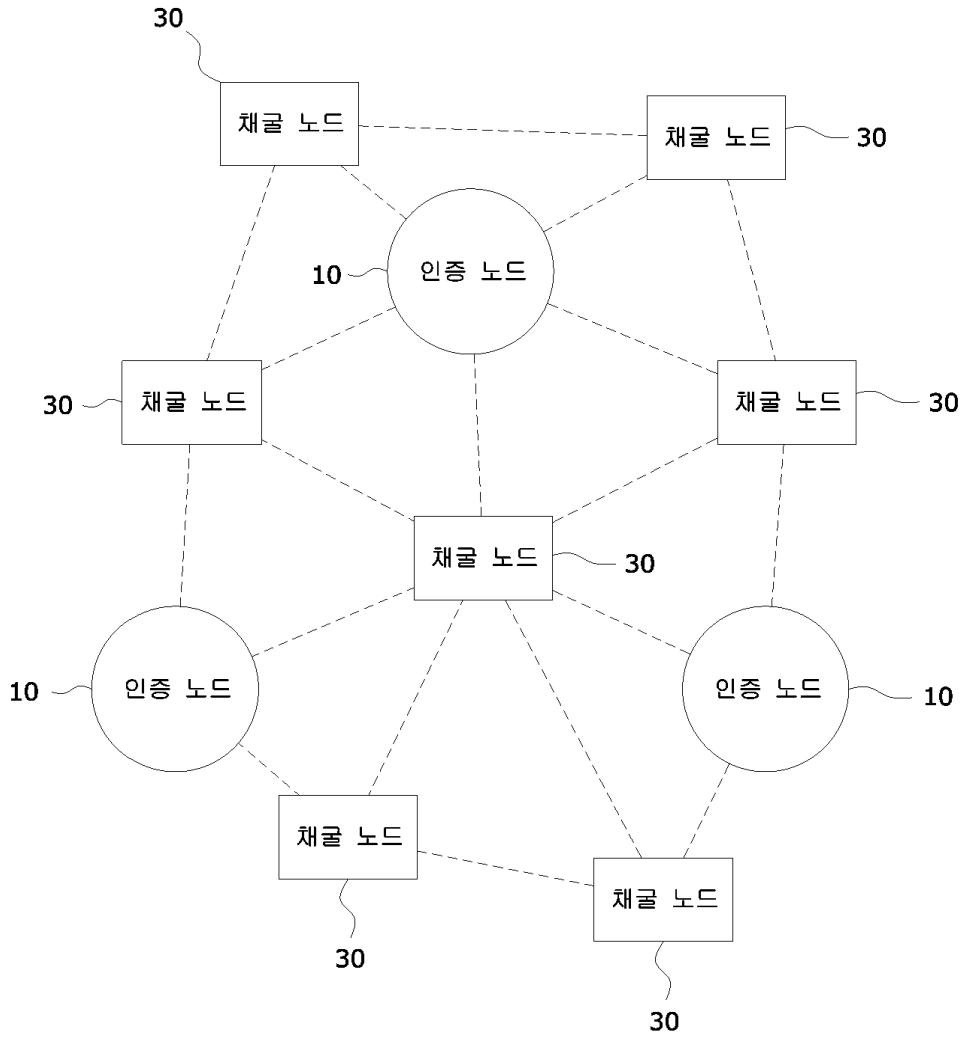
온라인 증명 블록체인 생성 시스템 및 방법이 개시된다. 본 발명의 일 측면에 따르면, 트랜잭션을 포함하는 블록이 순차적으로 연결되는 블록체인을 생성하는 시스템으로서, 상기 블록체인에 새롭게 연결될 블록이 설정된 순번의 블록일 때, 인증 데이터를 포함하고, 해당 설정된 순번에 배치되는 인증 블록을 생성하는 인증 노드; 및 상기 블록체인에 새롭게 연결될 블록이 설정된 순번이 아닌 순번의 블록일 때, 해당 순번에 배치되는 일반 블록을 생성하는 채굴 노드를 포함하는, 온라인 증명 블록체인 생성 시스템이 제공된다.

【대표도】

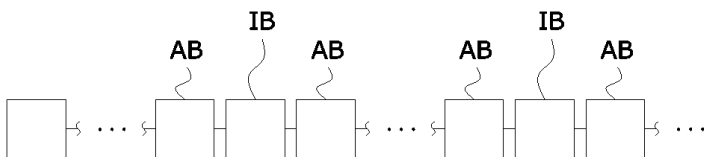
도 1

【도면】

【도 1】



【도 2】



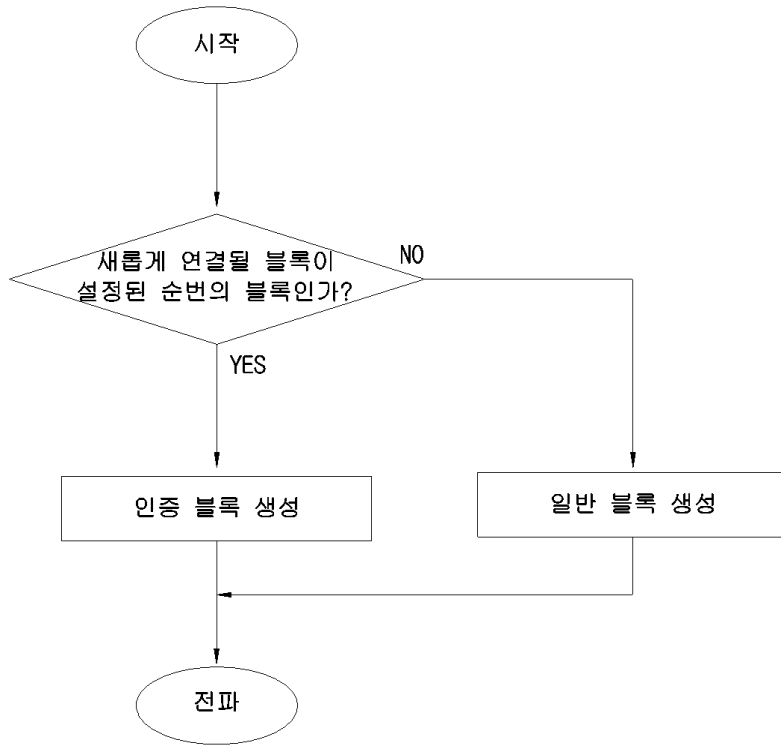
【도 3】

헤더부	⋮	⋮
	이전 블록 해시 (Previous block hash)	17975b97 ... 0df29759 330edab3 ... 01000000
	⋮	⋮
	타임스탬프 (timestamp)	358b0553
	⋮	⋮
	난스 (nonce)	48750833
	암호화 데이터	00000000
	⋮	⋮
바디부	코인베이스 트랜잭션 기재부 (Coinbase transaction)	
	일반 트랜잭션 기재부 (Transaction)	

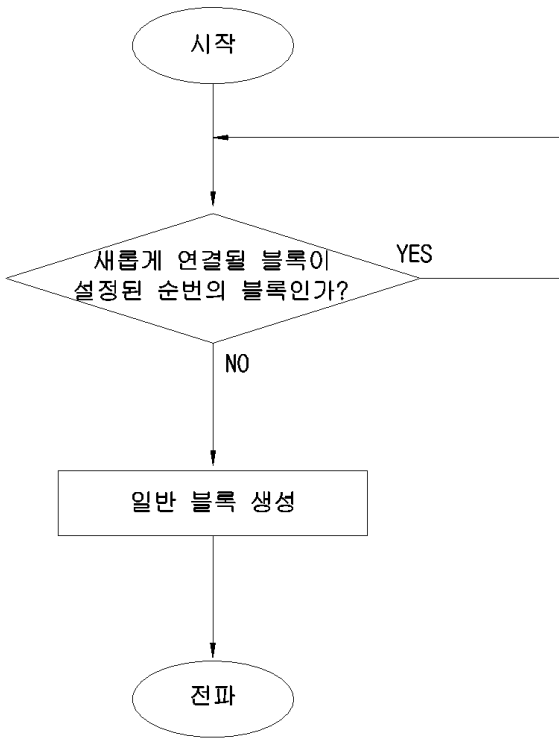
【도 4】

헤더부	⋮	⋮
	이전 블록 해시 (Previous block hash)	17975b97 ... 0df29759 330edab3 ... 01000000
	⋮	⋮
	타임스탬프 (timestamp)	358b0553
	⋮	⋮
	난스 (nonce)	00000000
	암호화 데이터	23976ba7
	⋮	⋮
바디부	코인베이스 트랜잭션 기재부 (Coinbase transaction)	
	일반 트랜잭션 기재부 (Transaction)	

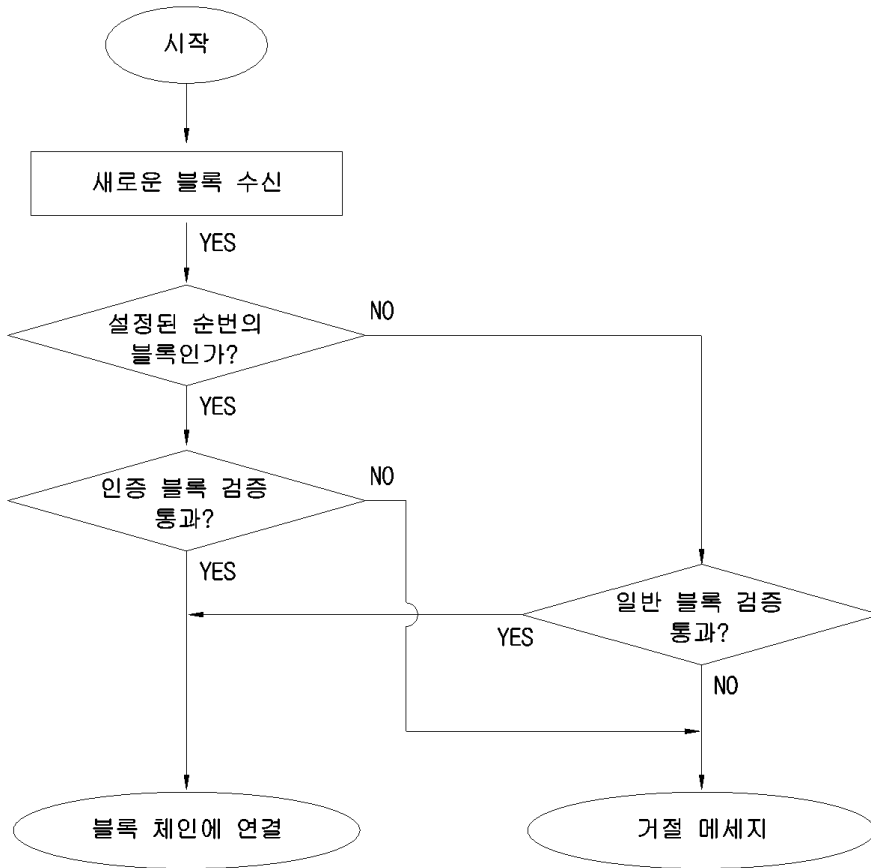
【도 5】



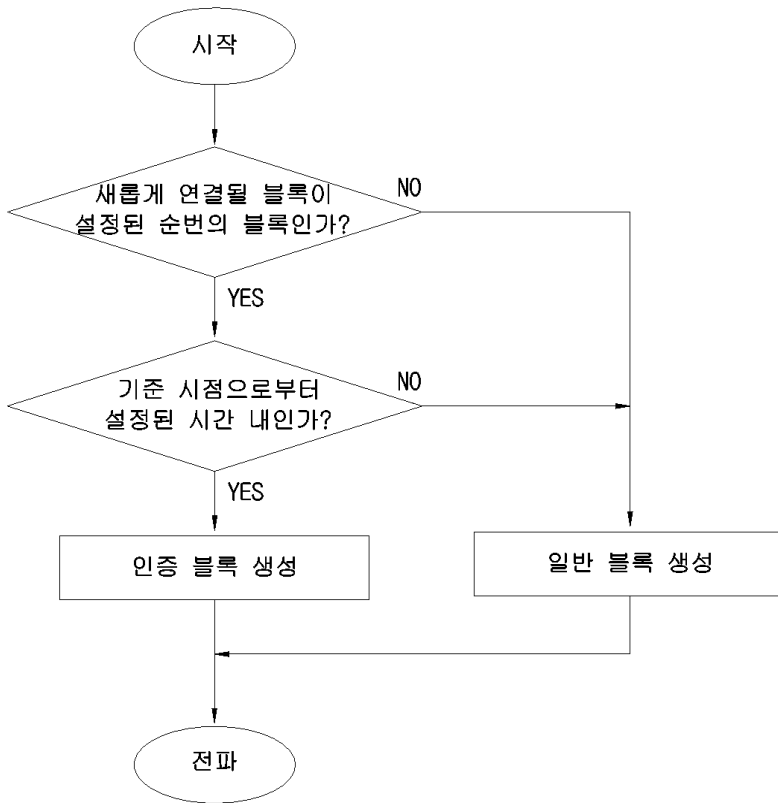
【도 6】



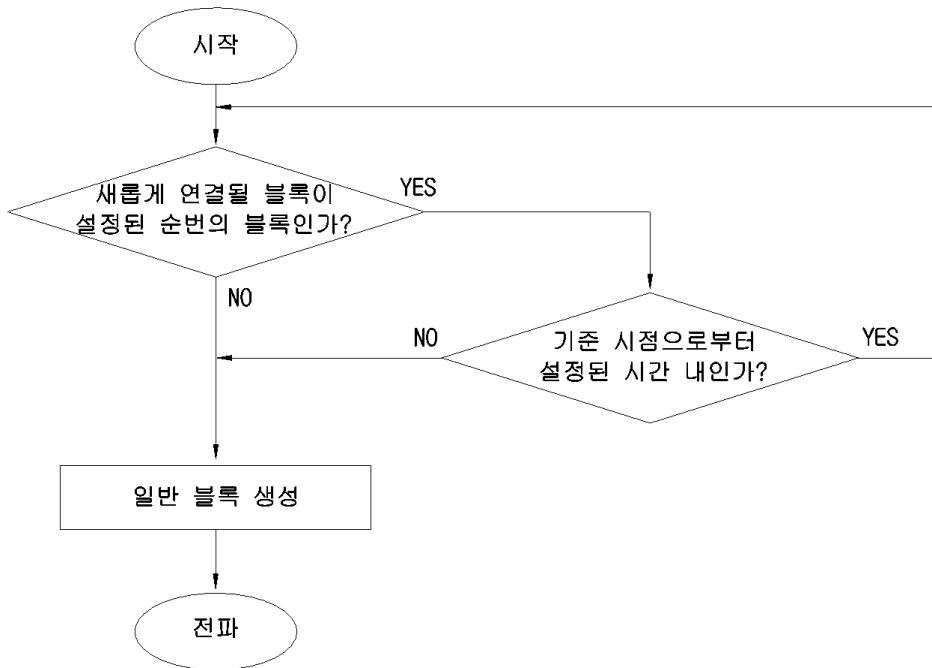
【도 7】



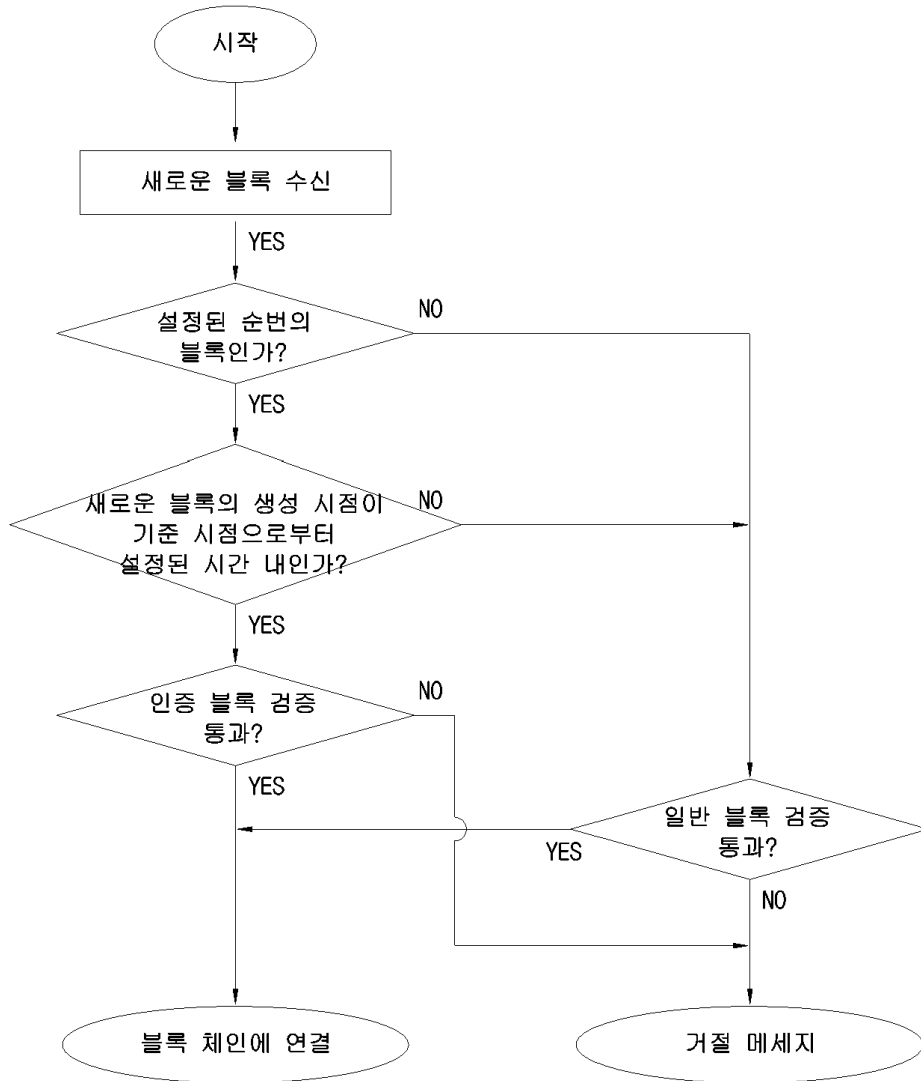
【도 8】



【도 9】



【도 10】



출원번호통지서

출원일자 2017.10.19
특기사항 심사청구(무) 공개신청(무) 참조번호(YK1102017049)
출원번호 10-2017-0135771 (접수번호 1-1-2017-1031614-53)
출원인성명 유영근(4-2000-044972-3)
대리인성명 김현중(9-2014-000344-1)
발명자성명 유영근
발명의명칭 카드 매출 채권 기반 가상 화폐 발행 방법 및 카드 매출 채권 기반 가상 화폐 발행 장치

특 허 청 장

<< 안내 >>

1. 귀하의 출원은 위와 같이 정상적으로 접수되었으며, 이후의 심사 진행상황은 출원번호를 통해 확인하실 수 있습니다.
2. 출원에 따른 수수료는 접수일로부터 다음날까지 동봉된 납입영수증에 성명, 납부자번호 등을 기재하여 가까운 우체국 또는 은행에 납부하여야 합니다.
※ 납부자번호 : 0131(기관코드) + 접수번호
3. 귀하의 주소, 연락처 등의 변경사항이 있을 경우, 즉시 [특허고객번호 정보변경(경정), 정정신고서]를 제출하여야 출원 이후의 각종 통지서를 정상적으로 받을 수 있습니다.
※ 특허로(patent.go.kr) 접속 > 민원서식다운로드 > 특허법 시행규칙 별지 제5호 서식
4. 특허(실용신안등록)출원은 명세서 또는 도면의 보정이 필요한 경우, 등록결정 이전 또는 의견서 제출기간 이내에 출원서에 최초로 첨부된 명세서 또는 도면에 기재된 사항의 범위 안에서 보정할 수 있습니다.
5. 외국으로 출원하고자 하는 경우 PCT 제도(특허·실용신안)나 마드리드 제도(상표)를 이용할 수 있습니다. 국내출원일을 외국에서 인정받고자 하는 경우에는 국내출원일로부터 일정한 기간 내에 외국에 출원하여야 우선권을 인정받을 수 있습니다.
※ 제도 안내 : <http://www.kipo.go.kr>-특허마당-PCT/마드리드
※ 우선권 인정기간 : 특허·실용신안은 12개월, 상표·디자인은 6개월 이내
※ 미국특허상표청의 선출원을 기초로 우리나라에 우선권주장출원 시, 선출원이 미공개상태이면, 우선일로부터 16개월 이내에 미국특허상표청에 [전자적교환허가서(PTO/SB/39)]를 제출하거나 우리나라에 우선권 증명서류를 제출하여야 합니다.
6. 본 출원사실을 외부에 표시하고자 하는 경우에는 아래와 같이 하여야 하며, 이를 위반할 경우 관련법령에 따라 처벌을 받을 수 있습니다.
※ 특허출원 10-2010-0000000, 상표등록출원 40-2010-0000000
7. 종업원이 직무수행과정에서 개발한 발명을 사용자(기업)가 명확하게 승계하지 않은 경우, 특허법 제62조에 따라 심사단계에서 특허거절결정되거나 특허법 제133조에 따라 등록이후에 특허무효사유가 될 수 있습니다.
8. 기타 심사 절차에 관한 사항은 동봉된 안내서를 참조하시기 바랍니다.

【서지사항】

【서류명】 특허출원서

【참조번호】 YK1102017049

【출원구분】 특허출원

【출원인】

【성명】 유영근

【특허고객번호】 4-2000-044972-3

【대리인】

【성명】 김현중

【대리인번호】 9-2014-000344-1

【발명의 국문명칭】 카드 매출 채권 기반 가상 화폐 발행 방법 및 카드 매출 채
권 기반 가상 화폐 발행 장치

【발명의 영문명칭】 Issuing method of virtual money based on credit card
receivables and Issuing apparatus of virtual money
based on credit card receivables

【발명자】

【성명】 유영근

【특허고객번호】 4-2000-044972-3

【출원언어】 국어

【취지】 위와 같이 특허청장에게 제출합니다.

대리인 김현중

(서명 또는 인)

【수수료】

【출원료】 0 면 46,000 원

【가산출원료】 49 면 0 원

【우선권주장료】 0 건 0 원

【심사청구료】 0 항 0 원

【합계】 46,000 원

【감면사유】 개인(70%감면)[1]

【감면후 수수료】 13,800 원

【첨부서류】 1. 위임장_1통

1 : 위임장

【서류명】 위임장

【수임자】

【명칭】 김현중

【대리인코드】 9-2014-000344-1

【전화번호】 02-543-2252

【주소】 서울특별시 서초구 반포로 324 아주빌딩 4층 401-2호

【위임사항】 발명의 명칭 : **카드 번호 기반 가상화폐 발행 방법 및 카드 번호 기반 가상화폐 발행 장치**

1. 특허출원에 관한 모든 절차
2. 특허출원의 변경, 포기, 취하에 관한 모든 절차
3. 특허권의 존속기간 연장등록출원의 취하
4. 특허법 제56조제1항의 규정에 의한 우선권주장이나 그 취하
5. 정보변경에 관한 모든 절차
6. 출원에 대한 심사청구서의 제출
7. 특허법 제132조의3 및 제132조의4의 규정에 의한 심판청구
8. 등록에 관한 모든 절차
9. 복대리인 선임
10. 청구의 취하
11. 신청의 취하
12. 특허권의 포기


【위임자】

【명칭(성명)】 유영근

【출원인코드】 4-2000-044992-33

【취지】 특허법 제7조·실용신안법 제3조·디자인보호법 제8조 및 상표법 제8조의 규정에 의하여 위와 같이 위임합니다.

【위임일자】 2017. 10. 13 .

위임인 유영근 (인) 

【발명의 설명】

【발명의 명칭】

카드 매출 채권 기반 가상 화폐 발행 방법 및 카드 매출 채권 기반 가상 화폐 발행 장치 {Issuing method of virtual money based on credit card receivables and Issuing apparatus of virtual money based on credit card receivables}

【기술분야】

【0001】 본 발명은 뱅(van, value added network)사 서버(server)로부터 수신되는 결제 승인 정보를 기초로 하여 가상 화폐를 발행함으로써 가상 화폐의 유통량을 신속히 확보할 수 있는 카드(card) 매출 채권 기반 가상 화폐 발행 방법 및 카드 매출 채권 기반 가상 화폐 발행 장치에 관한 것이다.

【발명의 배경이 되는 기술】

【0003】 비트 코인(bit coin), 이더리움(ethereum), 라이트 코인(lite coin) 등을 비롯하여 대부분의 가상 화폐들은 채굴(mining)이라는 방식으로 세상에 나오게 되며, 이를 작업 증명 방식(POW, proof of work)이라고 부른다.

【0004】 도면 1도는 가상 화폐가 발행되는 방식 중 작업 증명 방식을 설명하는 도면이다.

【0005】작업 증명 방식은 문자 그대로 작업을 증명한다는 뜻으로, 채굴 장비(miner)라 불리는 컴퓨터(computer)가 해쉬(hash) 연산을 수행하게 되고 네트워크(network)를 운영하는데 기여한 대가로서 가상 화폐를 받게 되는 방식이다. 그리고, 이 과정에서 컴퓨터가 작동하기 위하여 필요한 전원을 소모하게 되는데, 초기에는 컴퓨터가 풀어야 할 수학 문제의 난이도가 낮아서 개인이 사용하는 데스크탑(desk top)에서도 채굴이 가능하였으나, 가상 화폐의 발행량이 늘어날수록 컴퓨터가 풀어야 할 수학 문제의 난이도가 높아져서 이제는 대규모의 채굴용 컴퓨터를 연결한 채굴 풀(pool)을 구성하지 않으면 가상 화폐의 채굴이 어렵게 되었다.

【0006】이렇듯 작업 증명 방식을 통한 가상 화폐의 발행은 에너지(energy) 소비량이 너무 많다는 단점이 있으며, 이를 보완하기 위하여 지분 증명 방식(POS, proof of stakes)라는 새로운 가상 화폐 발행 방식이 고안되었다.

【0007】지분 증명 방식은 채굴자가 가상 화폐를 많이 가지고 있을수록 보유한 수량에 따라 이자를 받는 것과 같은 방식으로 채굴 수익을 얻는 방식으로, 작업 증명 방식의 에너지 낭비 문제를 해결할 수 있는 장점이 있다.

【0008】그러나, 지분 증명 방식은 포크(fork) 상황에서 양 블럭 체인(block chain)에 모두 투표를 해도 노드(node)가 전혀 손해 보지 않기 때문에 포크 문제를 해결하기 어렵다는 '아무 것도 수행하지 않는 문제(nothing at stake)'가 발생할 수 있는 문제점이 있다.

【0009】 무엇보다, 양 발행 방식은 가상 화폐가 화폐로서의 충분한 유동성을 갖기에는 상당한 시간과 네트워크가 필요한데, 다양한 가상 화폐가 발행되는 현 시장에서 새로이 출현한 가상 화폐는 다른 가상 화폐와의 경쟁에서 화폐로서 필요한 충분한 유동성을 확보하지 못하게 되는 문제점도 있다.

【발명의 내용】

【해결하고자 하는 과제】

【0011】 본 발명은 상기와 같은 문제점을 해결하기 위해 안출된 것으로, 뱅크 등에서 발행되는 카드 매출에 대한 결제 승인 정보를 이용하여 가상 화폐를 발행하여, 화폐로서 기능을 수행하기 위하여 필요한 충분한 유동량의 가상 화폐를 신속히 발행할 수 있는 카드 매출 채권 기반 가상 화폐 발행 방법 및 카드 매출 채권 기반 가상 화폐 발행 장치를 제공하고자 한다.

【0012】 또한, 가상 화폐의 편리함을 제공하는 동시에, 실물 화폐인 현금과 일 대 일로 매칭되는 가치를 보유토록 하여 가상 화폐의 가격 거품과 화폐로서의 안전성을 확보할 수 있는 카드 매출 채권 기반 가상 화폐 발행 방법 및 카드 매출 채권 기반 가상 화폐 발행 장치를 제공하고자 한다.

【0013】 또한, 카드 가맹점에게는 카드 매출 대금 즉시 입금의 효과를 제공할 수 있는 카드 매출 채권 기반 가상 화폐 발행 방법 및 카드 매출 채권 기반 가상 화폐 발행 장치를 제공하고자 한다.

【과제의 해결 수단】

【0014】 상기한 목적을 달성하기 위해, 본 발명에서는 카드 매출 채권 기반 가상 화폐 발행 장치가 뱅(van, value added network)사 서버(server)로부터 결제 승인 정보를 수신하는 단계; 상기 카드 매출 채권 기반 가상 화폐 발행 장치가 상기 결제 승인 정보의 결제액에 상응하는 금액의 가상 화폐를 발행하여 상기 카드 매출 채권 기반 가상 화폐 발행 장치의 전자 지갑에 저장하는 단계; 상기 카드 매출 채권 기반 가상 화폐 발행 장치가 상기 결제 승인 정보의 계정을 파악하는 단계; 상기 카드 매출 채권 기반 가상 화폐 발행 장치가 상기 결제 승인 정보의 결제액에 상응하는 금액의 가상 화폐를 상기 카드 매출 채권 기반 가상 화폐 발행 장치의 전자 지갑으로부터 상기 계정의 전자 지갑으로 이체하는 단계;를 포함하는 것을 특징으로 하는 카드 매출 채권 기반 가상 화폐 발행 방법을 제공한다.

【0015】 또한, 상기 카드 매출 채권 기반 가상 화폐 발행 장치가 상기 결제 승인 정보의 결제액에 상응하는 금액의 가상 화폐를 상기 카드 매출 채권 기반 가상 화폐 발행 장치의 전자 지갑으로부터 상기 계정의 전자 지갑으로 이체하는 단계 이후에, 상기 카드 매출 채권 기반 가상 화폐 발행 장치가 기설정된 일정 기간 경과 후 상기 계정의 은행 계좌로부터 상기 결제 승인 정보의 결제액을 상기 카드 매출 채권 기반 가상 화폐 발행 장치의 은행 계좌로 이체받는 단계;를 더 포함하는 것을 특징으로 하는 카드 매출 채권 기반 가상 화폐 발행 방법을 제공한다.

【0016】 또한, 상기 기설정된 일정 기간은 2일 내지 7일 중 어느 한 기간이 선택된 것을 특징으로 하는 가상 화폐 발행 방법을 제공한다.

【0017】 또한, 상기 카드 매출 채권 기반 가상 화폐 발행 장치가 기설정된 일정 기간 경과 후 상기 계정의 은행 계좌로부터 상기 결제 승인 정보의 결제액을 상기 카드 매출 채권 기반 가상 화폐 발행 장치의 은행 계좌로 이체받는 단계 이후에, 상기 카드 매출 채권 기반 가상 화폐 발생 서버가 상기 결제 승인 정보의 결제액의 전부가 상기 계정의 은행 계좌로부터 상기 카드 매출 채권 기반 가상 화폐 발생 서버의 은행 계좌로 이체되었는지 여부를 확인하는 단계; 상기 결제 승인 정보의 결제액의 전부가 이체되지 않은 경우, 상기 카드 매출 채권 기반 가상 화폐 발행 장치가 이체되지 않은 잔여 금액과 그에 대한 이자를 기설정된 일정 주기로 상기 계정의 은행 계좌에 대하여 청구하여 이체받는 단계;를 더 포함하는 것을 특징으로 하는 카드 매출 채권 기반 가상 화폐 발행 방법을 제공한다.

【0018】 또한, 상기 카드 매출 채권 기반 가상 화폐 발행 장치가 기설정된 일정 기간 경과 후 상기 계정의 은행 계좌로부터 상기 결제 승인 정보의 결제액을 상기 카드 매출 채권 기반 가상 화폐 발행 장치의 은행 계좌로 이체받는 단계 이후에, 상기 카드 매출 채권 기반 가상 화폐 발생 서버가 상기 결제 승인 정보의 결제액의 전부가 상기 계정의 은행 계좌로부터 상기 카드 매출 채권 기반 가상 화폐 발생 서버의 은행 계좌로 이체되었는지 여부를 확인하는 단계; 상기 결제 승인 정보의 결제액의 전부가 이체되지 않은 경우, 상기 카드 매출 채권 기반 가상 화폐 발행 장치가 이체되지 않은 결제액에 상응하는 금액의 가상 화폐를 상기 계정의 전자

지갑으로부터 상기 카드 매출 채권 기반 가상 화폐 발생 서버의 전자 지갑으로 이체받는 단계; 상기 카드 매출 채권 기반 가상 화폐 발행 장치가 이체된 가상 화폐를 소각하는 단계;를 포함하는 것을 특징으로 하는 카드 매출 채권 기반 가상 화폐 발행 방법을 제공한다.

【0019】 또한, 상기 카드 매출 채권 기반 가상 화폐 발행 장치가 이체된 가상 화폐를 소각하는 단계 이후에, 상기 카드 매출 채권 기반 가상 화폐 발행 장치가 이체되지 않은 결제액에 상응하는 금액의 가상 화폐의 전부가 소각되었는지 여부를 확인하는 단계; 이체되지 않은 결제액에 상응하는 금액의 가상 화폐의 전부가 소각되지 않은 경우, 상기 카드 매출 채권 기반 가상 화폐 발행 장치가 소각되지 않은 금액의 가상 화폐를 상기 카드 매출 채권 기반 가상 화폐 발행 장치의 전자 지갑에서 소각하는 단계;를 더 포함하는 것을 특징으로 하는 카드 매출 채권 기반 가상 화폐 발행 방법을 제공한다.

【0020】 또한, 이체되지 않은 결제액에 상응하는 금액의 가상 화폐의 전부가 소각되지 않은 경우, 상기 카드 매출 채권 기반 가상 화폐 발행 장치가 소각되지 않은 금액의 가상 화폐를 상기 카드 매출 채권 기반 가상 화폐 발행 장치의 전자 지갑에서 소각하는 단계 이후에, 상기 카드 매출 채권 기반 가상 화폐 발행 장치가 상기 계정으로부터 이체되지 않은 결제액과 그에 대한 이자를 기설정된 일정 주기로 상기 계정의 은행 계좌에 대하여 청구하여 이체받는 단계;를 더 포함하는 것을 특징으로 하는 카드 매출 채권 기반 가상 화폐 발행 방법을 제공한다.

【0021】 또한, 상기 카드 매출 채권 기반 가상 화폐 발행 장치가 이체된 가상 화폐를 소각하는 단계 이후에, 상기 카드 매출 채권 기반 가상 화폐 발행 장치가 이체되지 않은 결제액에 상응하는 금액의 가상 화폐의 전부가 소각되었는지 여부를 확인하는 단계; 이체되지 않은 결제액에 상응하는 금액의 가상 화폐의 전부가 소각되지 않은 경우, 상기 카드 매출 채권 기반 가상 화폐 발행 장치가 소각되지 않은 금액의 음의 가상 화폐를 발행하여 상기 계정의 전자 지갑으로 이체하는 단계;를 더 포함하는 것을 특징으로 하는 카드 매출 채권 기반 가상 화폐 발행 방법을 제공한다.

【0022】 또한, 가상 화폐의 발행, 이체 또는 소각에 대한 기록은 블록(block) 체인(chain) 기술을 이용한 공공 거래 장부에 기입되는 것을 특징으로 하는 카드 매출 채권 기반 가상 화폐 발행 방법을 제공한다.

【0023】 또한, 상기 카드 매출 채권 기반 가상 화폐 발행 장치가 상기 결제 승인 정보의 결제액에 상응하는 금액의 가상 화폐를 상기 카드 매출 채권 기반 가상 화폐 발행 장치의 전자 지갑으로부터 상기 계정의 전자 지갑으로 이체하는 단계에서, 상기 카드 매출 채권 기반 가상 화폐 발행 장치의 전자 지갑으로부터 상기 계정의 전자 지갑으로 이체된 가상 화폐에는 블록 체인 기술을 이용한 스마트(smart) 컨트랙트(contract)로 구현된 대출 조건이 부여되어 있는 것을 특징으로 하는 카드 매출 채권 기반 가상 화폐 발행 방법을 제공한다.

【0024】 또한, 상기 대출 조건은 상기 카드 매출 채권 기반 가상 화폐 발행 장치의 전자 지갑으로부터 상기 계정의 전자 지갑으로 이체된 가상 화폐를 기설정

된 일정 기간 이내에 사용하는 경우 사용된 금액에 대한 이자율, 총당 순서가 포함되어 있는 것을 특징으로 하는 카드 매출 채권 기반 가상 화폐 발행 방법을 제공한다.

【0025】 또한, 상기 음의 가상 화폐에는 블록 체인 기술을 이용한 스마트 컨트랙트로 구현된 대출 조건이 부여되어 있는 것을 특징으로 하는 카드 매출 채권 기반 가상 화폐 발행 방법을 제공한다.

【0026】 또한, 상기 대출 조건에는 발행된 상기 음의 가상 화폐에 대한 이자율, 총당 순서가 포함되어 있는 것을 특징으로 카드 매출 채권 기반 가상 화폐 발행 방법을 제공한다.

【0027】 또한, 본 발명은 카드 매출 채권 기반 가상 화폐 발행 장치가 계정으로부터 가상 화폐의 현금 전환 요청을 수신하는 단계; 상기 카드 매출 채권 기반 가상 화폐 발행 장치가 상기 계정의 전자 지갑으로부터 상기 카드 매출 채권 기반 가상 화폐 발생 서버의 전자 지갑으로 가상 화폐를 이체 받는 단계; 상기 카드 매출 채권 기반 가상 화폐 발행 장치가 상기 카드 매출 채권 기반 가상 화폐 발행 장치의 은행 계좌로부터 상기 계정의 은행 계좌로 상기 가상 화폐의 금액에 상응하는 현금을 상기 가맹점 회원의 은행 계좌로 이체하는 단계;를 포함하는 것을 특징으로 하는 카드 매출 채권 기반 가상 화폐 발행 방법을 제공한다.

【0028】 또한, 상기 결제 승인 정보의 결제액에 상응하는 금액의 가상 화폐는 상기 결제 승인 정보의 결제액과 일 대 일로 대응되는 금액으로 발행된 가상 화폐인 것을 특징으로 하는 카드 매출 채권 기반 가상 화폐 발행 방법을 제공한다.

【0029】 또한, 본 발명은 카드 매출 채권 기반 가상 화폐 발행 장치의 은행 계좌로 계정의 은행 계좌로부터 현금이 이체되는 단계; 상기 카드 매출 채권 기반 가상 화폐 발행 장치가 이체된 현금에 상응하는 금액의 가상 화폐를 발행하여 상기 카드 매출 채권 기반 가상 화폐 발행 장치의 전자 지갑에 저장하는 단계; 상기 카드 매출 채권 기반 가상 화폐 발행 장치가 상기 이체된 현금에 상응하는 금액의 가상 화폐를 상기 카드 매출 채권 기반 가상 화폐 발행 장치의 전자 지갑으로부터 상기 계정의 전자 지갑으로 이체하는 단계;를 포함하는 것을 특징으로 하는 카드 매출 채권 기반 가상 화폐 발행 방법을 제공한다.

【0030】 또한, 상기 이체된 현금에 상응하는 금액의 가상 화폐는 상기 이체된 현금과 일 대 일로 대응되는 금액으로 발행된 가상 화폐인 것을 특징으로 하는 카드 매출 채권 기반 가상 화폐 발행 방법을 제공한다.

【0031】 또한, 본 발명은 가상 화폐를 저장하는 전자 지갑; 뱅크 서버로부터 결제 승인 정보를 수신하는 결제 승인 정보 수신 모듈(module); 상기 결제 승인 정보 수신 모듈로부터 상기 결제 승인 정보를 전달 받아 상기 결제 승인 정보의 결제액에 상응하는 금액의 가상 화폐를 발행하여 상기 전자 지갑에 저장하는 가상 화폐 발행 모듈; 상기 결제 승인 정보 수신 모듈로부터 상기 결제 승인 정보를 전달 받아 계정 및 결제액을 파악하고, 해당 계정의 전자 지갑으로 결제액에 상응하는 가상 화폐를 이체하는 가상 화폐 이체 담당 모듈;을 포함하는 것을 특징으로 하는 카드 매출 채권 기반 가상 화폐 발행 장치를 제공한다.

【0032】 또한, 현금을 저장하는 은행 계좌; 계정의 전자 지갑, 은행 계좌를 포함하는 정보를 저장하는 계정 정보 저장 모듈; 상기 결제 승인 정보 수신 모듈로부터 상기 결제 승인 정보를 전달 받아 계정 및 결제액을 파악하고, 기설정된 일정 기간 경과 후 해당 계정의 은행 계좌로부터 결제액의 이체를 요청하며 미이체시 미이체 신호를 출력하는 현금 이체 관리 모듈;을 더 포함하는 것을 특징으로 하는 카드 매출 채권 기반 가상 화폐 발행 장치를 제공한다.

【0033】 또한, 상기 현금 이체 관리 모듈이 미이체 신호를 출력하는 경우, 이체되지 않은 잔여 금액과 그에 대한 이자를 기설정된 일정 주기로 해당 계정의 은행 계좌로 청구하여 이체받는 미이체금 관리 모듈;을 더 포함하는 것을 특징으로 하는 카드 매출 채권 기반 가상 화폐 발행 장치를 제공한다.

【0034】 또한, 상기 현금 이체 관리 모듈이 미이체 신호를 출력하는 경우, 이체되지 않은 결제액에 상응하는 금액의 가상 화폐를 해당 계정의 전자 지갑으로부터 상기 전자 지갑으로 이체받는 가상 화폐 회수 모듈;을 더 포함하는 것을 특징으로 하는 카드 매출 채권 기반 가상 화폐 발행 장치를 제공한다.

【0035】 또한, 상기 가상 화폐 회수 모듈이 회수한 가상 화폐를 소각하며, 회수되지 않은 잔여 가상 화폐는 상기 전자 지갑에서 소각하는 가상 화폐 소각 모듈;을 더 포함하는 것을 특징으로 하는 카드 매출 채권 기반 가상 화폐 발행 장치를 제공한다.

【0036】 또한, 상기 가상 화폐 소각 모듈이 상기 전자 지갑에서 가상 화폐를 소각시, 상기 미이체금 관리 모듈은 소각된 가상 화폐의 금액에 상응하는 현금과 그에 대한 이자를 기설정된 일정 주기로 해당 계정의 은행 계좌로 청구하여 이체받는 것을 특징으로 하는 카드 매출 채권 기반 가상 화폐 발행 장치를 제공한다.

【0037】 또한, 상기 가상 화폐 회수 모듈이 해당 계정으로부터 이체되지 않은 결제액에 상응하는 모든 금액의 가상 화폐를 회수하지 못하면, 상기 가상 화폐 발행 모듈은 회수되지 않은 잔여 가상 화폐에 대응되는 금액의 음의 가상 화폐를 발행하고, 상기 가상 화폐 이체 담당 모듈은 상기 음의 가상 화폐를 해당 계정의 전자 지갑으로 이체하는 것을 특징으로 하는 카드 매출 채권 기반 가상 화폐 발행 장치를 제공한다.

【0038】 또한, 상기 기설정된 일정 기간은 2일 내지 7일 중 어느 한 기간이 선택된 것을 특징으로 하는 가상 화폐 발행 장치를 제공한다.

【0039】 또한, 가상 화폐의 발행, 이체 또는 소각에 대한 기록은 블록 체인 기술을 이용한 공공 거래 장부에 기입되는 것을 특징으로 하는 카드 매출 채권 기반 가상 화폐 발행 장치를 제공한다.

【0040】 또한, 상기 가상 화폐 이체 담당 모듈이 해당 계정의 전자 지갑으로 이체한 가상 화폐에는 블록 체인 기술을 이용한 스마트 컨트랙트로 구현된 대출 조건이 부여되어 있는 것을 특징으로 하는 카드 매출 채권 기반 가상 화폐 발행 장치를 제공한다.

【0041】 또한, 상기 대출 조건에는 해당 계정의 전자 지갑으로 이체된 가상 화폐를 기설정된 일정 기간 이내에 사용하는 경우 사용된 금액에 대한 이자율, 총 당 순서가 포함되어 있는 것을 특징으로 하는 카드 매출 채권 기반 가상 화폐 발행 장치를 제공한다.

【0042】 또한, 상기 음의 가상 화폐에는 블록 체인 기술을 이용한 스마트 컨 트랙트로 구현된 대출 조건이 부여되어 있는 것을 특징으로 하는 카드 매출 채권 기반 가상 화폐 발행 장치를 제공한다.

【0043】 또한, 상기 대출 조건에는 발행된 상기 음의 가상 화폐에 대한 이자 율, 총당 순서가 포함되어 있는 것을 특징으로 하는 카드 매출 채권 기반 가상 화 폐 발행 장치를 제공한다.

【0044】 또한, 계정으로부터 가상 화폐의 현금 전환 요청 또는 현금의 가상 화폐 전환 요청을 수신하는 화폐 전환 요청 수신 모듈;을 더 포함하고, 상기 화폐 전환 요청 수신 모듈이 가상 화폐의 현금 전환 요청을 수신하면, 상기 가상 화폐 이체 담당 모듈은 해당 계정의 전자 지갑으로부터 가상 화폐를 이체받고 상기 현금 이체 관리 모듈은 상기 은행 계좌로부터 해당 계좌의 은행 계좌로 이체받은 가상 화폐에 상응하는 현금을 이체하며, 상기 화폐 전환 요청 수신 모듈이 현금의 가상 화폐 전환 요청을 수신하면, 상기 현금 이체 관리 모듈은 해당 계정의 은행 계좌로 부터 상기 은행 계좌로 현금을 이체받고 상기 가상 화폐 발행 모듈은 이체된 현금 에 상응하는 금액의 가상 화폐를 발행하며 상기 가상 화폐 이체 담당 모듈은 상기 전자 지갑으로부터 해당 계좌의 전자 지갑으로 상기 이체된 현금에 상응하는 가상

화폐를 이체하는 것을 특징으로 하는 카드 매출 채권 기반 가상 화폐 발행 장치를 제공한다.

【0045】 또한, 상기 결제 승인 정보의 결제액에 상응하는 금액의 가상 화폐는 상기 결제 승인 정보의 결제액과 일 대 일로 대응되는 금액으로 발행된 가상 화폐인 것을 특징으로 하는 카드 매출 채권 기반 가상 화폐 발행 방법을 제공한다.

【0046】 또한, 상기 이체된 현금에 상응하는 가상 화폐는 상기 이체된 현금과 일 대 일로 대응되는 금액으로 발행된 가상 화폐인 것을 특징으로 하는 카드 매출 채권 기반 가상 화폐 발행 방법을 제공한다.

【0047】 또한, 본 발명은 카드 매출 채권 기반 가상 화폐 발행 장치가 밴(van, value added network)사 서버(server)로부터 결제 승인 정보를 수신하는 단계; 상기 카드 매출 채권 기반 가상 화폐 발행 장치가 상기 결제 승인 정보의 결제액에 상응하는 금액의 가상 화폐를 발행하여 상기 카드 매출 채권 기반 가상 화폐 발행 장치의 전자 지갑에 저장하는 단계; 상기 카드 매출 채권 기반 가상 화폐 발행 장치가 상기 결제 승인 정보의 계정을 파악하는 단계; 상기 카드 매출 채권 기반 가상 화폐 발행 장치가 상기 결제 승인 정보의 결제액에 상응하는 금액의 가상 화폐를 상기 카드 매출 채권 기반 가상 화폐 발행 장치의 전자 지갑으로부터 상기 계정의 전자 지갑으로 이체하는 단계; 상기 카드 매출 채권 기반 가상 화폐 발행 장치가 기설정된 일정 기간 경과 후 상기 계정의 은행 계좌로부터 상기 결제 승인 정보의 결제액을 상기 카드 매출 채권 기반 가상 화폐 발행 장치의 은행 계좌로 이체받는 단계;를 더 포함하며, 상기 카드 매출 채권 기반 가상 화폐 발행 장치가 기

설정된 일정 기간 경과 후 상기 계정의 은행 계좌로부터 상기 결제 승인 정보의 결제액을 상기 카드 매출 채권 기반 가상 화폐 발행 장치의 은행 계좌로 이체받는 단계에서, 상기 은행 계좌는 상기 계정이 상기 가상 화폐 발행 서버에 회원 가입시 자동 이체를 동의하여 신고한 은행 계좌인 것을 특징으로 하는 카드 매출 채권 기반 가상 화폐 발행 방법을 제공한다.

【0048】 또한, 본 발명은 가상 화폐를 저장하는 전자 지갑; 뱅크 서버로부터 결제 승인 정보를 수신하는 결제 승인 정보 수신 모듈(module); 상기 결제 승인 정보 수신 모듈로부터 상기 결제 승인 정보를 전달 받아 상기 결제 승인 정보의 결제액에 상응하는 금액의 가상 화폐를 발행하여 상기 전자 지갑에 저장하는 가상 화폐 발행 모듈; 상기 결제 승인 정보 수신 모듈로부터 상기 결제 승인 정보를 전달 받아 계정 및 결제액을 파악하고, 해당 계정의 전자 지갑으로 결제액에 상응하는 가상 화폐를 이체하는 가상 화폐 이체 담당 모듈; 현금을 저장하는 은행 계좌; 계정의 전자 지갑, 은행 계좌를 포함하는 정보를 저장하는 계정 정보 저장 모듈; 상기 결제 승인 정보 수신 모듈로부터 상기 결제 승인 정보를 전달 받아 계정 및 결제액을 파악하고, 기설정된 일정 기간 경과 후 해당 계정의 은행 계좌로부터 결제액의 이체를 요청하며 미이체시 미이체 신호를 출력하는 현금 이체 관리 모듈;을 포함하고, 상기 계정 정보 저장 모듈에 저장된 계정의 은행 계좌는 해당 계정이 자동 이체를 동의하여 신고한 은행 계좌인 것을 특징으로 하는 카드 매출 채권 기반 가상 화폐 발행 장치를 제공한다.

【발명의 효과】

【0049】 본 발명의 바람직한 실시 예에 따른 카드 매출 채권 기반 가상 화폐 발행 방법 및 카드 매출 채권 기반 가상 화폐 발행 장치는 다음과 같은 효과가 있다.

【0050】 첫째, 가상 화폐의 발행이 카드 매출에 대한 결제 승인 정보에 의하여 이루어지므로, 가상 화폐의 유통량을 신속하게 증가되도록 하는 효과가 있다. 즉, 시장에서 처음 발행되는 가상 화폐라도 신속히 화폐로서의 기능을 수행할 수 있는 유통량을 확보할 수 있는 효과가 있다.

【0051】 둘째, 결제 승인 정보의 결제액에 상응하는 금액의 가상 화폐가 발행되도록 함으로써, 가상 화폐에서 발생할 수 있는 가격 거품을 해소하고 화폐로서의 안전성을 확보할 수 있는 효과가 있다. 보다 구체적으로는 결제 승인 정보의 결제액과 일 대 일로 매칭되는 가치의 가상 화폐를 발행함으로써, 가상 화폐의 편리함을 제공하는 동시에 화폐로서의 안전성을 제공할 수 있는 효과가 있다.

【0052】 셋째, 기존의 가상 화폐 발행 방식인 작업 증명 방식의 문제점인 에너지 과다 소모를 해결할 수 있는 동시에, 가상 화폐 발행의 중앙 은행 기능을 수행하는 카드 매출 채권 기반 가상 화폐 발행 장치를 통하여서만 가상 화폐가 발행됨으로써 포크 발생에 의한 '아무 것도 수행하지 않는 문제(nothing at stake)'를 해결할 수 있는 효과가 있다.

【0053】 넷째, 가상 화폐를 이체받는 계정의 정보를 카드 매출 채권 기반 가상 화폐 발행 장치가 사전에 미리 보유하고 있으므로, 가상 화폐가 자금 세탁이나

검은 돈으로 활용되는 것을 방지할 수 있는 효과가 있다.

【0054】 다섯째, 결제 승인 정보가 수신되는 곧바로 가상 화폐가 발행되어 가맹점 회원의 계정의 전자 지급으로 이체되므로 카드 매출 누락이 발생하는지를 손쉽게 확인할 수 있는 효과가 있다.

【0055】 여섯째, 가맹점 회원 계정의 전자 지급으로 입금된 가상 화폐를 기 설정된 일정 기간 이내에 사용하는 경우에만 단기 대출로서 이자를 부담하므로, 가맹점 회원 입장에서는 카드 매출 대금 즉시 결제 서비스의 효과를 누리면서도 수수료 부담을 줄일 수 있는 효과가 있다. 또한, 이러한 모든 과정은 블록 체인(block chain) 기술을 이용한 스마트 컨트랙트(smart contract)로 구현되어 있어서 사용에 따라 이자를 부과하여야 하는지 여부가 자동으로 결정되어 책정되는 효과가 있다.

【0056】 일곱째, 가상 화폐의 발행, 이체 또는 소각에 대한 기록이 블록 체인 기술을 이용한 공공 거래 장부에 기입되도록 함으로써 가상 화폐의 사용에 대한 신뢰성을 담보할 수 있는 효과가 있다. 또한, 가상 화폐 네트워크가 해킹되는 것을 방지할 수 있는 효과도 있다.

【0057】 여덟째, 카드 매출 채권 기반 가상 화폐 발행 장치의 은행 계좌로 수신된 현금을 활용하여 발생된 수익에 대한 가상 화폐는 지분 증명 방식을 통한 수익으로 계정들에 배분되므로, 가상 화폐 사용에 따른 편리함 뿐 아니라 부가 수익도 얻을 수 있는 효과가 있다.

【도면의 간단한 설명】

【0059】 도면 1도는 가상 화폐가 발행되는 방식 중 작업 증명 방식을 설명하는 도면이다.

도면 2도는 카드 결제시 카드 결제 매출이 입금되는 기존의 일반적인 과정을 보여주는 도면이다.

도면 3도는 기존의 카드 매출 결제 대금 즉시 결제 서비스에 대한 개념을 간략하게 보여주는 도면이다.

도면 4도는 본 발명의 바람직한 실시 예에 따른 카드 매출 채권 기반 가상 화폐 발행 방법 및 카드 매출 채권 기반 가상 화폐 발행 장치에서 가상 화폐가 발행되는 과정을 개념도로 보여주는 도면이다.

도면 5도는 본 발명의 바람직한 실시 예에 따른 카드 매출 채권 기반 가상 화폐 발행 방법의 순서도를 보여주는 도면이다.

도면 6도는 가상 화폐의 정상 발행 검증 방법의 제1 실시 예를 보여주는 도면이다.

도면 7도는 가상 화폐의 정상 발행 검증 방법의 제2 실시 예를 보여주는 도면이다.

도면 8도는 가상 화폐의 정상 발행 검증 방법의 제3 실시 예를 보여준다.

도면 9도는 본 발명의 바람직한 실시 예에 따른 카드 매출 채권 기반 가상 화폐 발행 방법 및 카드 매출 채권 기반 가상 화폐 발행 장치에서 사용되는 블록

체인을 간략하게 설명하는 도면이다.

도면 10도는 본 발명의 바람직한 실시 예에 따른 카드 매출 채권 기반 가상 화폐 발행 방법 및 카드 매출 채권 기반 가상 화폐 발행 장치가 발행하는 가상 화폐에 부여되는 스마트 컨트랙트를 간략하게 개념으로 보여주는 도면이다.

도면 11도는 본 발명의 바람직한 실시 예에 따른 카드 매출 채권 기반 가상 화폐 발행 방법에서 뱅크의 결제 승인 정보 없이 현금이 입금되었을 때 가상 화폐가 발행되는 방식을 보여주는 순서도이다.

도면 12도는 본 발명의 바람직한 실시 예에 따른 카드 매출 채권 기반 가상 화폐 발행 장치의 내부 구성을 블록도로 보여주는 도면이다.

【발명을 실시하기 위한 구체적인 내용】

【0060】 이하, 첨부한 도면을 참조하여 본 발명의 실시예들에 대해 상세히 설명한다. 본 발명은 다양한 변경을 가할 수 있고 여러 가지 형태를 가질 수 있는 바, 특정 실시예들은 도면에 예시하고 본문에 상세하게 설명하고자 한다. 그러나, 이는 본 발명을 특정한 개시 형태에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다.

【0061】 또한, 본 발명의 설명에서 "제1", "제2" 등의 용어는 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 사용되는 것이며, 어떠한 의미를 한정하기 위하여 사용되는 것이 아니다. 그리고, 단수의 표현은 문맥상 명백하게 다

르게 뜻하지 않는 한, 복수의 표현을 포함하며, "포함 하다" 또는 "가지다" 등의 용어는 명세서 상에 기재된 특징, 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

【0062】 먼저, 본 발명의 바람직한 실시 예에 따른 카드 매출 채권 기반 가상 화폐 발행 방법 및 카드 매출 채권 기반 가상 화폐 발행 장치를 통하여 가상 화폐가 발행되는 과정 및 본 발명이 카드 가맹점 회원에게 제공할 수 있는 기능 중의 하나로서 매출 대금 즉시 입금 효과를 보다 자세히 설명하기 위하여, 기존의 카드 매출 결제 과정과 기존의 카드 매출 대금 즉시 결제 서비스를 살펴보도록 한다.

【0063】 도면 2도는 카드 결제시 카드 결제 매출이 입금되는 기존의 일반적인 과정을 보여주는 도면이다.

【0064】 신용카드 시스템(system)은 신용카드 발급사와 가맹점 전표 매입사의 동일 여부에 따라 크게 폐쇄형 구조(3 당사자 구조)와 개방형 구조(4 당사자 구조)로 구분된다. 폐쇄형 구조는 카드회원, 가맹점, 카드 사업자 등 3개 당사자 중심으로 신용카드 거래가 이루어지는 구조이며, 폐쇄형 구조하에서 카드 사업자들은 자사 브랜드(brand)를 소유하며 자사 카드회원과 가맹점을 모집하고 이들 간에 신용카드 결제가 이루어질 수 있도록 신용카드 네트워크(network)를 구축한다. 반면, 개방형 구조는 카드회원, 가맹점, 카드 발급사, 전표 매입사의 4개 당사자와 신용카드 브랜드 사를 중심으로 신용카드 거래가 이루어지는 구조이다. 이 구조에서는

신용카드 브랜드 사는 자사 브랜드 카드를 발급하는 발급사와 자사 브랜드 카드로 결제된 매출 전표를 매입하는 매입사를 모집한다.

【0065】 국내 신용카드 산업의 구조적 특징은 이 두 개의 구조 중 다른 국가와는 달리 폐쇄형 구조의 비중이 현저히 높다는 점이다. 즉, 대부분의 신용카드 사업자가 신용카드 발급업무와 매출전표 매입업무를 동시에 수행하는 폐쇄형 구조를 채택하고 있다.

【0066】 이런 카드 시장 환경 속에서, 국내 가맹점 회원들은 개개의 신용카드 브랜드사와 별도의 가맹점 계약을 맺어야 하며, 대부분의 국내 가맹점들은 신용카드 사용 고객을 잃지 않기 위하여 국내 모든 신용카드 브랜드사와 각각 계약을 체결하고 있는 실정이다. 비록, 신용카드 승인업무 대행 및 가맹점을 관리하는 벤사를 통해 한번에 모든 신용카드 브랜드사와의 계약을 체결할 수 있으나, 신용카드 매출결제대금은 각각의 신용카드사로부터 각각 입금받아야 한다.

【0067】 도면 2도에서 보는 바와 같이, 가맹점 회원의 계정(10)은 가맹점 회원 단말을 통하여 카드사(30)로 매출 승인 신청을 하고, 이에 대하여 카드사(30)가 매출 승인을 하면, 매출 승인일로부터 3 내지 9일 후 수수료를 제한 금액을 입금받고 있다. 그러나, 카드사 별로 입금주기와 수수료율에 차이가 있으며 가맹점 계약을 맺은 신용카드 브랜드사 수가 많아질수록 입금된 매출 결제 대금의 확인 및 관리가 복잡해진다. 또한, 매출결제대금 입금 과정에서 문제가 발생할 경우 가맹점 회원이 직접 각각의 신용카드 브랜드사들과 접촉하여 해결하여야 하는 불편함이 있다. 또한, 카드 결제 승인이 나도 입금이 되기까지는 상당한 기일이 소요되므로,

가맹점 회원이 급하게 자금이 필요한 경우 이러한 자금을 조달하기 위하여 카드 매출 채권을 충분히 보유하고 있는 상황에서도 불가피하게 은행이나 대부업체로부터 비싼 이율의 자금을 조달해야 하는 불편이 있으며, 카드 매출을 담보로 하는 대출 서비스에서도 평가의 기초자료로서 충분히 활용되지 못하여 높은 이율을 부담해야 하는 불합리적인 면이 있었다.

【0068】 도면 3도는 기존의 카드 매출 결제 대금 즉시 결제 서비스에 대한 개념을 간략하게 보여주는 도면이다.

【0069】 앞서 살펴본 바와 같은 문제점을 해결하기 위하여, 도면 2도와 같은 카드 매출 대금 즉시 결제 서비스(service)가 현재 제공되고 있다.

【0070】 현재 제공되고 있는 카드 매출 대금 즉시 결제 서비스는 카드 가맹점 회원이 카드 매출 즉시 결제 서비스를 제공하는 회사와 약정하여 카드 매출금이 발생시 카드 매출금 발생 익일에 즉시 결제 서비스를 제공하는 회사에서 먼저 당일 카드 매출금에서 수수료를 제외한 전액을 먼저 입금해주고, 즉시 결제 서비스를 제공하는 회사에서는 3 내지 9일 정도의 소정기간 후에 신용카드사로부터 가맹점으로 입금되는 당일 카드 매출금으로 변제 처리하는 방식의 일종의 신용카드매출금을 담보로 하는 초단기 대출 서비스이다. 즉, 이를 도면으로 살펴보면, 가맹점 회원의 계정(10)로부터 카드사(30)로 카드 매출 승인 신청이 있고 이에 대하여 카드사(30)의 카드 매출 승인이 나면, 익일 날 카드 매출 결제 대금 즉시 결제 서비스를 제공하는 서버(2)는 가맹점 회원에게로 수수료를 제외한 결제 대금을 입금해 주고, 이에 대한 변제는 이후 카드사가 운용하는 카드사(30)로부터 입금받아 처리하는 과

정을 거치고 있다.

【0071】 이러한 카드 매출 대금 즉시 결제 서비스를 통하여, 가맹점 회원의 경우에는 카드 매출 대금을 익일 자금화할 수 있다는 점에서 유동자금활용 측면에서 매우 유익하며, 매일 정확한 카드매출 정산관리가 가능하여 카드 매출 대금 관리를 체계적으로 할 수 있다는 점에서 즉시 결제 서비스를 이용하고 있는 가맹점은 점차 늘고 있는 추세이다.

【0072】 그러나, 이러한 카드 매출 대금 즉시 결제 서비스는 그 성격이 초단기 대출의 성격을 지니고 있으므로, 카드사에 부담하는 수수료 외에 별도의 수수료를 부담해야 하므로 가맹점 회원 입장에서는 이중의 수수료를 부담해야 한다. 이는 현재에도 매출액의 상당 부분을 차지하고 있는 카드 수수료로 인하여 많은 부담을 가지고 있는 자영업자에게는 또 다른 부담으로 다가오고 있는 실정이다. 그리고, 실제적으로 가맹점 입장에서는 모든 카드 매출 대금 채권이 바로 다음날 유동화될 필요는 없다는 점에서 기존의 카드 매출 대금 즉시 결제 서비스는 불필요한 수수료를 과다하게 지불해야 하는 문제점이 있다.

【0073】 본 발명의 바람직한 실시 예에 따른 카드 매출 채권 기반 가상 화폐 발행 방법 및 카드 매출 채권 기반 가상 화폐 발행 장치에 의하면, 가상 화폐의 발행량을 신속히 증가시키면서도 기존의 이러한 카드 매출 대금 즉시 결제 서비스의 단점을 보완할 수 있는 효과를 달성할 수 있다.

【0074】도면 4도는 본 발명의 바람직한 실시 예에 따른 카드 매출 채권 기반 가상 화폐 발행 방법 및 카드 매출 채권 기반 가상 화폐 발행 장치에서 가상 화폐가 발행되는 과정을 개념도로 보여주는 도면이다.

【0075】먼저, 계정(10)으로부터 뱅사(20)로 카드 결제 전문이 전송되면 뱅사(20)는 카드사(30)로 결제 승인 요청을 하고, 결제 승인 요청을 수신한 카드사(30)는 결제 승인 요청 정보를 분석하여 승인 조건을 만족하는 경우 다시 뱅사(20)로 카드 결제 승인 정보를 송신할 수 있다. 그리고, 이러한 결제 승인 정보를 수신한 뱅사(20)는 가맹점 회원의 계정(10)으로 해당 결제 승인 정보를 통보하는 동시에, 이러한 결제 승인 정보를 카드 매출 채권 기반 가상 화폐 발행 장치(100)로 전송할 수 있다.

【0076】이러한 결제 승인 정보를 수신한 카드 매출 채권 기반 가상 화폐 발행 장치(100)는 결제 승인 정보의 결제액에 상응하는 가상 화폐를 발행하여 계정(10)의 전자 지갑으로 이체할 수 있으며, 결제 승인 정보를 수신한 날로부터 기설정된 일정 기간 이후에 계정(10)의 은행 계좌로부터 해당 결제 승인 정보의 결제액을 이체 받음으로써 가상 화폐의 발행이 완료되게 된다. 여기서, 결제 승인 정보의 결제액에 상응하여 발행되는 가상 화폐는 결제액에 일 대 일로 대응되는 금액으로 발행될 수 있다. 예를 들어, 결제 승인 정보의 결제액이 만원이고 가상 화폐의 단위가 코인이면, 만 코인이 발행될 수 있다.

【0077】본 발명의 바람직한 실시 예에 따른 카드 매출 채권 기반 가상 화폐 발행 방법 및 카드 매출 채권 기반 가상 화폐 발행 장치는 이렇게 카드 매출에 대

한 결제 승인 정보를 기반으로 가상 화폐를 발행함으로써 가상 화폐가 화폐로서의 기능을 수행하는데 필요한 유동량을 신속히 확보할 수 있는 효과가 있다. 또한, 카드 매출 채권 기반 가상 화폐 발행 장치(100)가 중앙 은행의 기능을 담당하여 가상 화폐의 발행을 책임지므로 에너지 과다 소모 및 "아무 것도 수행하지 않는 문제"를 해결할 수 있는 효과도 있다.

【0078】 도면 5도는 본 발명의 바람직한 실시 예에 따른 카드 매출 채권 기반 가상 화폐 발행 방법의 순서도를 보여주는 도면이다.

【0079】 먼저, 본 발명의 바람직한 실시 예에 카드 매출 채권 기반 가상 화폐 발행 방법은 카드 매출 채권 기반 가상 화폐 발행 장치(100)가 뱅사(20)로부터 결제 승인 정보를 수신하는 과정부터 수행될 수 있다.(S5-1) 이렇게 뱅사(20)로부터 결제 승인 정보를 수신한 카드 매출 채권 기반 가상 화폐 발행 장치(100)는 수신된 결제 승인 정보의 결제액에 상응하는 금액의 가상 화폐를 발행하고, 발행된 가상 화폐를 카드 매출 채권 기반 가상 화폐 발행 장치(100)의 전자 지갑에 저장하는 과정을 수행하며(S5-2), 결제 승인 정보 내에 포함된 계정(10)의 정보를 파악하여(S5-3), 계정(10)의 전자 지갑으로 가상 화폐를 이체하는 과정을 수행할 수 있다.(S5-4) 그리고, 여기서 발행된 가상 화폐의 금액은 수신된 결제 승인 정보의 결제액과 일 대 일로 매칭되는 금액일 수 있다.

【0080】 다음으로, 카드 매출 채권 기반 가상 화폐 발행 장치(100)는 기설정된 일정기간이 경과되었는지 여부를 확인하고(S5-5), 기설정된 일정 기간이 경과되면 결제 승인 정보의 결제액을 계정(10)의 은행 계좌로부터 카드 매출 채권 기반

가상 화폐 발행 장치(100)의 은행 계좌로 이체받는 과정을 수행할 수 있으며(S5-6), 마지막으로 발행된 가상 화폐가 정상적으로 발행되었는지 여부를 검증하는 과정을 수행할 수 있다.(S5-7) 여기서, 기설정된 일정 기간은 결제 승인 정보의 결제액이 카드사로부터 계정(10)의 은행 계좌로 입금되는 기간에 해당할 수 있으며, 2일 내지 9일 중 어느 한 기간이 선택될 수 있다.

【0081】 따라서, 본 발명의 바람직한 실시 예에 따른 카드 매출 채권 기반 가상 화폐 발행 방법 및 카드 매출 채권 기반 가상 화폐 발행 장치에 의하면, 결제 승인 정보가 수신되는 곧바로 가상 화폐가 발행되어 계정(10)의 전자 지갑으로 이체되므로 카드 매출 누락이 발생되는지 여부의 확인이 곧바로 가능한 카드 매출 대금 즉시 결제 서비스와 동일한 효과를 누릴 수 있는 동시에, 전자 지갑으로 이체된 가상 화폐를 기설정된 일정 기간 동안 사용하지 않는 경우는 그에 대한 이자를 지급하지 않아도 되므로 수수료 부담도 주는 효과도 더불어 달성할 수 있다. 그리고, 이 과정은 가상 화폐를 발행하면서 부여된 스마트 컨트랙트에 의하여 자동으로 수행될 수 있다.

【0082】 본 발명에서, 가상 화폐가 정상적으로 발행되었다 함은 가상 화폐와 현금이 일 대 일로 매칭되어 발행되었음을 의미하는 것이며, 만일 현금이 카드 매출 채권 기반 가상 화폐 발행 장치(100)로 이동되지 않았음에도 가상 화폐가 발행되었다면 이는 근거가 없는 발행이므로 해당 가상 화폐는 소각되어야 하거나 발행의 근거가 되는 현금의 이체를 요청하여야 한다. 이는 가상 화폐와 현금의 가치를 일 대 일 매칭시키기 위한 것으로서, 이를 통하여 본 발명의 바람직한 실시 예에

다른 카드 매출 채권 기반 가상 화폐 발행 방법 및 카드 매출 채권 기반 가상 화폐 발행 장치는 가상 화폐에 발생할 수 있는 거품이나 가치 하락을 제거할 수 있다.

【0083】 이하, 도면 6도 내지 도면 8도는 본 발명의 바람직한 실시 예에 따른 카드 매출 채권 기반 가상 화폐 발행 방법 및 카드 매출 채권 기반 가상 화폐 발행 장치에서 가상 화폐가 정상적으로 발행되었는지 여부를 검증하는 다양한 방법을 보여주는 순서도이다.

【0084】 먼저, 도면 6도는 가상 화폐의 정상 발행 검증 방법의 제1 실시 예를 보여주는 도면이다.

【0085】 앞서 살펴본 바와 같이, 본 발명의 바람직한 실시 예에 따른 카드 매출 채권 기반 가상 화폐 발행 방법 및 카드 매출 채권 기반 가상 화폐 발행 장치는 발행된 가상 화폐의 가치와 실물 화폐인 현금과의 가치가 일 대 일로 매칭(matching)되도록 하고자 한다. 이를 개념적으로 이해하자면, 가상 화폐의 1 코인은 현금 1 원과 교환되어야 한다는 것을 의미하며, 현금의 이체나 흐름이 없는 상황에서 발행된 가상 화폐는 잘못되거나 문제가 있는 가상 화폐의 발행이다.

【0086】 이러한 문제를 해결하기 위하여 제1 실시 예에 따른 가상 화폐의 정상 발행 검증 방법은 결제 승인 정보의 결제액의 전부가 계정(10)의 은행 계좌로부터 카드 매출 채권 기반 가상 화폐 발행 장치(100)의 전자 지급으로 발행되었는지 여부를 확인하고(S6-1), 이체되지 않은 잔여 금액이 있는 경우에는 이러한 잔여 금액과 그에 대한 이자를 기설정된 일정 주기로 계속적으로 청구(S6-2)하는 방식으로 발행된 가상 화폐와 이체되는 결제액을 매칭시킬 수 있다.

【0087】 다음으로, 도면 7도는 가상 화폐의 정상 발행 검증 방법의 제2 실시 예를 보여준다.

【0088】 제2 실시 예에 따른 가상 화폐의 정상 발행 검증 방법은 결제액의 전부가 해당 계정(10)의 은행 계좌로부터 카드 매출 채권 기반 가상 화폐 발행 장치(100)의 은행 계좌로 이체되었는지 여부를 확인하고(S7-1), 미이체된 금액이 있는 경우에는 이체되지 않은 결제액에 상응하는 금액의 가상 화폐를 계정(10)의 전자 지갑으로부터 카드 매출 채권 기반 가상 화폐 발행 장치(100)의 전자 지갑으로 이체 받는 과정을 수행할 수 있다.(S7-2) 이 과정은 가상 화폐를 발행할때 블록 체인 기술을 이용한 스마트 컨트랙트로 구현된 조건에 의하여 검증되어 수행되는 것일 수 있다. 따라서, 공공에 의하여 검증된 계약에 의한 것이므로 가상 화폐를 회수하므로, 가상 화폐의 회수에 따른 분쟁의 발생을 사전에 차단할 수 있는 효과를 달성할 수 있다.

【0089】 가상 화폐가 계정(10)의 전자 지갑으로부터 카드 매출 채권 기반 가상 화폐 발행 장치(100)의 전자 지갑으로 이체된 다음에는 이체된 가상 화폐를 소각하는 과정이 수행될 수 있으며(S7-4), 다음으로 이체되지 않은 현금 결제액에 상응하는 금액의 가상 화폐가 모두 소각되었는지 여부를 확인하는 과정을 진행할 수 있다.(S7-4) 만일, 이 과정에서 이체된 가상 화폐를 모두 소각하였는데도 소각된 가상 화폐의 금액이 현금 결제액에 미치지 못하는 경우, 카드 매출 채권 기반 가상 화폐 발행 장치(100)은 잔여 결제액과 이자를 기설정된 일정 주기로 계정(10)의 은행 계좌로 청구하는 과정이 수행될 수 있다.(S7-5)

【0090】도면 8도는 가상 화폐의 정상 발행 검증 방법의 제3 실시 예를 보여 준다.

【0091】제3 실시 예에 따른 가상 화폐의 정상 발행 검증 방법은 이체되지 않은 결제액에 상응하는 금액의 가상 화폐가 모두 소각되었는지 여부를 확인하는 과정(S8-4)까지는 앞서 살펴본 제2 실시 예에 따른 검증 방법과 동일하며, 이체되지 않은 현금 결제액에 상응하는 금액의 가상 화폐가 모두 소각되지 않은 경우에서의 조치에서만 차이가 난다.

【0092】제3 실시 예에 따른 가상 화폐의 정상 발행 검증 방법은 카드 매출 채권 기반 가상 화폐 발행 장치(100)의 은행 계좌로 이체되지 않은 결제액에 상응하는 금액의 가상 화폐가 회수되어 모두 소각되지 않은 경우, 소각되지 않은 금액의 음의 가상 화폐를 발행하여 계정(10)의 전자 지갑으로 이체하는 과정을 수행할 수 있다.(S8-5) 그리고, 이러한 음의 가상 화폐에는 블록 체인 기술을 이용한 스마트 컨트랙트로 구현된 대출 조건이 부여되어 있을 수 있으며 이를 통하여 계정(10)의 전자 지갑에는 마이너스(minus) 대출이 발생하며, 해당 계정(10)이 전자 지갑을 다시 사용하기 위하여는 전자 지갑의 음의 가상 화폐와 이에 대한 이자를 모두 변제할 수 있는 가상 화폐가 입금되어야 해당 전자 지갑을 사용할 수 있다.

【0093】앞서 살펴본 가상 화폐의 정상 발행 검증 방법은 모두 카드 매출 채권 기반 가상 화폐 발행 장치(100)가 발행한 가상 화폐와 카드 매출 채권 기반 가상 화폐 발행 장치(100)로 이체된 현금의 양을 동일하게 하여 가상 화폐와 현금의 가치가 동등하게 되도록 하는 효과를 달성한다.

【0094】 그리고, 본 발명의 바람직한 실시 예에 따른 카드 매출 채권 기반 가상 화폐 발행 방법 및 카드 매출 채권 기반 가상 화폐 발행 장치는 카드 매출 채권 기반 가상 화폐 발행 장치(100)의 은행 계좌에 쌓은 현금을 이용하여 발생된 수익을 기초로 하여 추가적으로 가상 화폐를 발행할 수 있으며, 이러한 가상 화폐는 계정(10)들에 네트워크 기여의 대가로 지분 증명 방식으로 분배되어 더 많은 사용자가 본 발명에 따른 카드 매출 채권 기반 가상 화폐 발행 방법 및 카드 매출 채권 기반 가상 화폐 발행 장치에 참여토록 유인하는 효과를 달성할 수 있다.

【0095】 도면 9도는 본 발명의 바람직한 실시 예에 따른 카드 매출 채권 기반 가상 화폐 발행 방법 및 카드 매출 채권 기반 가상 화폐 발행 장치에서 사용되는 블록 체인을 간략하게 설명하는 도면이다.

【0096】 본 발명의 바람직한 실시 예에 따른 카드 매출 채권 기반 가상 화폐 발행 방법 및 카드 매출 채권 기반 가상 화폐 발행 장치에서 가상 화폐의 발행, 이체 또는 소각에 대한 기록은 블록 체인 기술을 이용한 공공 거래 장부에 기입된다.

【0097】 기존의 은행권의 거래 방식은 사용자 사이의 자금의 이체를 중앙에서 은행이 책임지고 모든 장부를 관리하여 통일된 거래 내역을 만드는 방식이었으나, 본 발명의 바람직한 실시 예에 따른 카드 매출 채권 기반 가상 화폐 발행 방법 및 카드 매출 채권 기반 가상 화폐 발행 장치는 대규모의 노드(node)들 사이에서 각 노드에 분산 저장된 장부의 데이터를 항상 최신 버전으로 유지할 수 있도록 하는 합의 수렴 알고리즘(algorithm)인 블록 체인으로 장부를 운영함으로써 가상 화폐를 이용하는 모든 사용자 사이에 신뢰를 형성할 수 있는 동시에 가상 화폐 네트

위크가 해킹(hacking)되는 것을 방지할 수 있는 효과를 달성할 수 있다.

【0098】 도면 10도는 본 발명의 바람직한 실시 예에 따른 카드 매출 채권 기반 가상 화폐 발행 방법 및 카드 매출 채권 기반 가상 화폐 발행 장치가 발행하는 가상 화폐에 부여되는 스마트 컨트랙트를 간략하게 개념으로 보여주는 도면이다.

【0099】 스마트 컨트랙트라 함은 블록 체인 기술을 기반으로 사용자가 가상 화폐에 직접 계약 조건과 내용을 코딩(coding)할 수 있는 기술로서, 계약 조건이 사람에 의해 수행되는 것이 아니라 전산적으로 자동화되어 수행될 수 있는 것을 특징으로 한다. 일 예로, 도면과 같이 가상 화폐를 이체하면서 송신자와 수신자를 지정하고 해당 가상 화폐가 쓰여야 할 용도 등을 스마트 컨트랙트로 기술하면, 해당 가상 화폐를 특정 용도로 밖에 사용하지 못하도록 제한할 수 있으며, 즉각 이행을 담보할 수 있다.

【0100】 본 발명의 바람직한 실시 예에 따른 카드 매출 채권 기반 가상 화폐 발행 방법 및 카드 매출 기반 가상 화폐 발행 장치는 결제 승인 정보에 기반하여 가상 화폐를 발행하여 계정(10)의 전자 지급으로 이체하는 과정 및 음의 가상 화폐가 발행되어 이체되는 과정에서 이러한 스마트 컨트랙트 기술을 사용할 수 있으며, 그 조건으로 기설정된 일정 기간 이내에 가상 화폐가 사용되는 경우에 대한 이자율, 변제의 충당 순서 등이 기입할 수 있다.

【0101】 정리하면, 뱅사(20)로부터 수신된 결제 승인 정보에 따른 결제액은 실제로는 카드사로부터는 약 2일 내지 9일이 경과되어야 입금되나, 결제액에 상응하는 금액의 가상 화폐는 결제 승인 정보가 수신되는대로 발행되어 계정(10)으로

입금된다. 따라서, 결제액의 입금 이전의 사용은 결제액이 카드 매출 채권 기반 가상 화폐 발행 장치(100)의 은행 계좌로 입금되기 이전의 사용이므로 단기 대출이 되어야 한다. 그러나, 카드 매출 채권 기반 가상 화폐 발행 장치(100)의 은행 계좌로 결제액이 입금된 이후의 사용은 정상적으로 발행 또는 구입한 가상 화폐의 사용이므로, 해당 가상 화폐의 사용에 대하여 이자 등을 지급할 필요가 없다.

【0102】 본 발명의 바람직한 실시 예에 따른 카드 매출 채권 기반 가상 화폐 발행 방법 및 카드 매출 채권 기반 가상 화폐 발행 장치는 이러한 조건을 스마트 콘트랙트로 구현함으로써, 가상 화폐의 사용, 이자 발생, 회수 등의 과정을 조건에 따라 자동으로 진행시킬 수 있는 효과를 달성할 수 있다.

【0103】 이를 기존의 카드 매출 대금 즉시 결제 서비스와 비교하면, 기존의 카드 매출 대금 즉시 결제 서비스는 가맹점 회원이 실제 사용할지 여부를 불문하고 결제 승인 정보를 수신하면 해당 금액을 가맹점 회원의 은행 계좌로 입금하고 수수료 또는 이자를 청구하였으나, 본 발명은 가맹점 회원이 실제 결제액의 입금일 이전에 이체된 가상 화폐를 사용하는 경우에만 수수료 또는 이자가 발생하므로, 기존의 카드 매출 대금 즉시 결제 서비스와 동등한 효과를 누리면서도 수수료 부담이 훨씬 줄어드는 효과를 달성할 수 있다.

【0104】 도면 11도는 본 발명의 바람직한 실시 예에 따른 카드 매출 채권 기반 가상 화폐 발행 방법에서 뱅크의 결제 승인 정보 없이 현금이 입금되었을 때 가상 화폐가 발행되는 방식을 보여주는 순서도이다.

【0105】 본 발명의 바람직한 실시 예에 따른 카드 매출 채권 기반 가상 화폐

발행 방법은 뱅사(20)로부터 수신되는 결제 승인 정보를 기반으로 가상 화폐가 발행되는 것을 원칙으로 하나, 이러한 결제 승인 정보가 없이도 카드 매출 채권 기반 가상 화폐 발행 장치(100)의 은행 계좌로 이체되는 현금에 근거하여 가상 화폐를 발행할 수도 있다.

【0106】 이를 위하여, 먼저 본 발명의 바람직한 실시 예에 따른 카드 매출 채권 기반 가상 화폐 발행 방법은 계정(10)의 은행 계좌로부터 카드 매출 채권 기반 가상 화폐 발행 장치(100)의 은행 계좌로 결제 승인 정보에 근거함이 없이 현금이 이체되었는지 여부를 확인하는 과정을 수행할 수 있다.(S11-1) 이체가 확인되는 경우, 카드 매출 채권 기반 가상 화폐 발행 장치(100)는 이체된 현금에 상응하는 금액의 가상 화폐를 발행하여 카드 매출 채권 기반 가상 화폐 발행 장치(100)의 전자 지갑에 저장하고(S11-2), 이체된 현금에 상응하는 금액의 가상 화폐를 카드 매출 채권 기반 가상 화폐 발행 장치(100)의 전자 지갑으로부터 계정(10)의 전자 지갑으로 이체하는 과정을 수행할 수 있다(S11-3)

【0107】 이러한 상황은 사용자가 현금 보유 보다는 가상 화폐의 소유를 더 원하는 경우에 발생할 수 있으며, 본 발명의 바람직한 실시 예에 따른 카드 매출 채권 기반 가상 화폐 발행 방법은 이러한 상황에 대응하여서도 가상 화폐를 발행할 수 있으므로 가상 화폐의 더 빠른 보급이 가능해지는 효과를 달성할 수 있다.

【0108】 도면 12도는 본 발명의 바람직한 실시 예에 따른 카드 매출 채권 기반 가상 화폐 발행 장치의 내부 구성을 블럭도로 보여주는 도면이다.

【0109】 본 발명의 바람직한 실시 예에 따른 카드 매출 채권 기반 가상 화폐

발행 장치(100)는 전자 지갑(121), 결제 승인 정보 수신 모듈(110), 가상 화폐 발행 모듈(131), 가상 화폐 이체 담당 모듈(132)을 포함하여 구성될 수 있으며, 추가로 은행 계좌(122), 계정 정보 저장 모듈(140), 현금 이체 관리 모듈(151), 미이체금 관리 모듈(152), 가상 화폐 회수 모듈(133), 가상 화폐 소각 모듈(134), 화폐 전환 요청 수신 모듈(160)을 더 포함하여 구성될 수 있다.

【0110】 카드 매출 채권 기반 가상 화폐 발행 장치(100)의 각 구성 요소의 역할을 더 자세히 살펴보면, 전자 지갑(121)은 가상 화폐를 저장하는 역할을 수행하고, 결제 승인 정보 수신 모듈(110)은 뱅크(20) 서버로부터 결제 승인 정보를 수신하는 역할을 수행하며, 가상 화폐 발행 모듈(131)은 결제 승인 정보 수신 모듈(110)로부터 결제 승인 정보를 전달받아 결제 승인 정보의 결제액에 상응하는 금액의 가상 화폐를 발행하여 전자 지갑(121)에 저장하는 역할을 수행할 수 있다. 그리고, 가상 화폐 이체 담당 모듈(132)은 결제 승인 정보 수신 모듈(110)이 전달한 결제 승인 정보내의 계정(10) 및 결제액을 계정의 전자 지갑, 은행 계좌를 포함한 정보를 저장하고 있는 계정 정보 저장 모듈(140)의 도움을 받아 파악하고, 해당 계정(10)의 전자 지갑으로 가상 화폐를 이체하거나 이체받는 것을 담당하는 역할을 수행할 수 있다. 또한, 현금 이체 관리 모듈(151)은 은행 계좌(122)와 계정(10)의 은행 계좌 사이의 현금의 이체를 담당하는 역할을 수행할 수 있으며, 미이체금 관리 모듈(152)은 현금 이체 관리 모듈(151)의 미이체 신호 출력에 따라 이체되지 않은 잔여 금액과 그에 대한 이자를 기설정된 일정 주기로 해당 계정의 은행 계좌에 청구하여 미이체된 금액을 관리하는 역할을 수행할 수 있다. 더 나아가 가상 화폐 회

수 모듈(133)도 현금 이체 관리 모듈(151)이 미이체 신호를 출력하는 경우, 이체되지 않은 결제액에 상응하는 금액의 가상 화폐를 해당 계정의 전자 지갑으로부터 이체받는 역할을 수행하며, 가상 화폐 소각 모듈(134)는 가상 화폐 회수 모듈(133)이 회수한 가상 화폐를 소각하거나, 회수되지 않은 잔여 가상 화폐에 상당하는 금액의 가상 화폐를 전자 지갑(121)에서 소각하는 역할을 수행할 수 있다. 마지막으로, 화폐 전환 요청 수신 모듈(160)은 계정(10)의 요청에 따라 가상 화폐에서 현금으로, 현금에서 가상 화폐로의 일 대 일 매칭 전환을 담당하는 역할을 수행하며, 이러한 과정은 가상 화폐 이체 담당 모듈(132) 및 현금 이체 관리 모듈(151)의 협조를 통하여 이루어질 수 있다.

【0111】 본 발명의 바람직한 실시 예에 따른 카드 매출 채권 기반 가상 화폐 발행 장치(100)는 이러한 구성을 통하여 기존의 작업 증명 방식이나 지분 증명 방식의 가상 화폐가 가지고 있는 문제점을 해결하는 동시에, 가상 화폐가 화폐로서의 기능을 수행하는데 필요한 유통량을 신속히 확보할 수 있는 효과를 달성할 수 있다.

【0112】 마지막으로, 본 발명인 카드 매출 채권 기반 가상 화폐 발행 장치(100)의 내부 구성요소의 설명에서 모듈은 반드시 물리적 장치만을 지칭하는 것이 아니고, 특정한 기능을 수행하는 소프트웨어(software) 또는 프로그램(program)적 함수 등을 지칭하는 것으로도 이해될 수 있음을 유의해야 한다.

【0113】 상술한 바와 같이, 본 발명의 바람직한 실시예들을 참조하여 설명하였지만 해당 기술 분야의 숙련된 당업자라면 하기의 특허 청구의 범위에 기재된 본

발명의 사상 및 영역으로부터 벗어나지 않는 범위 내에서 본 발명을 다양하게 수정 및 변경시킬 수 있음을 이해할 수 있을 것이다.

【부호의 설명】

【0115】 2 : 카드 매출 결제 대금 즉시 결제 서비스를 제공하는 서버

10 : 계정

20 : 뱅카

30 : 카드사

100 : 카드 매출 채권 기반 가상 화폐 발행 장치

110 : 결제 승인 정보 수신 모듈

121 : 전자 지갑

122 : 은행 계좌

131 : 가상 화폐 발행 모듈

132 : 가상 화폐 이체 담당 모듈

133 : 가상 화폐 회수 모듈

134 : 가상 화폐 소각 모듈

140 : 계정 정보 저장 모듈

151 : 현금 이체 관리 모듈

152 : 미이체금 관리 모듈

160 : 화폐 전환 요청 수신 모듈

【청구범위】

【청구항 1】

카드 매출 채권 기반 가상 화폐 발행 장치가 뱅(van, value added network) 사 서버(server)로부터 결제 승인 정보를 수신하는 단계;

상기 카드 매출 채권 기반 가상 화폐 발행 장치가 상기 결제 승인 정보의 결제액에 상응하는 금액의 가상 화폐를 발행하여 상기 카드 매출 채권 기반 가상 화폐 발행 장치의 전자 지갑에 저장하는 단계;

상기 카드 매출 채권 기반 가상 화폐 발행 장치가 상기 결제 승인 정보의 계정을 파악하는 단계;

상기 카드 매출 채권 기반 가상 화폐 발행 장치가 상기 결제 승인 정보의 결제액에 상응하는 금액의 가상 화폐를 상기 카드 매출 채권 기반 가상 화폐 발행 장치의 전자 지갑으로부터 상기 계정의 전자 지갑으로 이체하는 단계;

상기 카드 매출 채권 기반 가상 화폐 발행 장치가 기설정된 일정 기간 경과 후 상기 계정의 은행 계좌로부터 상기 결제 승인 정보의 결제액을 상기 카드 매출 채권 기반 가상 화폐 발행 장치의 은행 계좌로 이체받는 단계;를 더 포함하며,

상기 카드 매출 채권 기반 가상 화폐 발행 장치가 기설정된 일정 기간 경과 후 상기 계정의 은행 계좌로부터 상기 결제 승인 정보의 결제액을 상기 카드 매출 채권 기반 가상 화폐 발행 장치의 은행 계좌로 이체받는 단계에서, 상기 은행 계좌는 상기 계정이 상기 가상 화폐 발행 서버에 회원 가입시 자동 이체를 동의하여 신

고한 은행 계좌인 것을 특징으로 하는 카드 매출 채권 기반 가상 화폐 발행 방법.

【청구항 2】

가상 화폐를 저장하는 전자 지갑;

뱅크 서버로부터 결제 승인 정보를 수신하는 결제 승인 정보 수신 모듈 (module);

상기 결제 승인 정보 수신 모듈로부터 상기 결제 승인 정보를 전달 받아 상기 결제 승인 정보의 결제액에 상응하는 금액의 가상 화폐를 발행하여 상기 전자 지갑에 저장하는 가상 화폐 발행 모듈;

상기 결제 승인 정보 수신 모듈로부터 상기 결제 승인 정보를 전달 받아 계정 및 결제액을 파악하고, 해당 계정의 전자 지갑으로 결제액에 상응하는 가상 화폐를 이체하는 가상 화폐 이체 담당 모듈;

현금을 저장하는 은행 계좌;

계정의 전자 지갑, 은행 계좌를 포함하는 정보를 저장하는 계정 정보 저장 모듈;

상기 결제 승인 정보 수신 모듈로부터 상기 결제 승인 정보를 전달 받아 계정 및 결제액을 파악하고, 기설정된 일정 기간 경과 후 해당 계정의 은행 계좌로부터 결제액의 이체를 요청하며 미이체시 미이체 신호를 출력하는 현금 이체 관리 모듈;을 포함하고,

상기 계정 정보 저장 모듈에 저장된 계정의 은행 계좌는 해당 계정이 자동 이체를 동의하여 신고한 은행 계좌인 것을 특징으로 하는 카드 매출 채권 기반 가상 화폐 발행 장치.

【요약서】**【요약】**

본 발명은 카드 매출 채권 기반 가상 화폐 발행 방법 및 카드 매출 채권 기반 가상 화폐 발행 장치에 관한 것으로, 카드 결제시 발생하는 결제 승인 정보를 바탕으로 가상 화폐가 발행되도록 하여 신속한 유동량 확보뿐 아니라 화폐로서의 가격 안전성을 확보할 수 있는 카드 매출 채권 기반 가상 화폐 발행 방법 및 카드 매출 채권 기반 가상 화폐 발행 장치에 관한 발명이다.

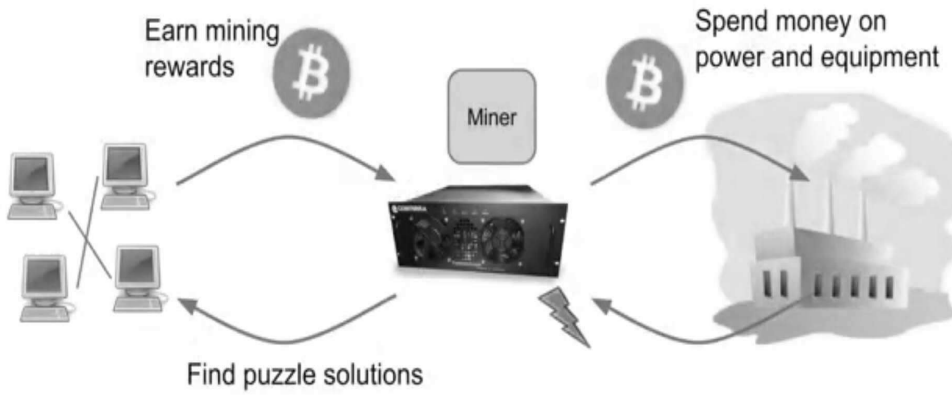
【대표도】

도 4

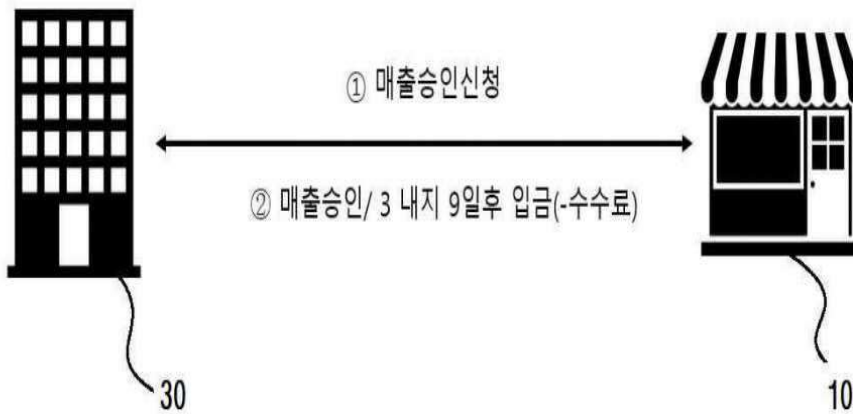
【도면】

【도 1】

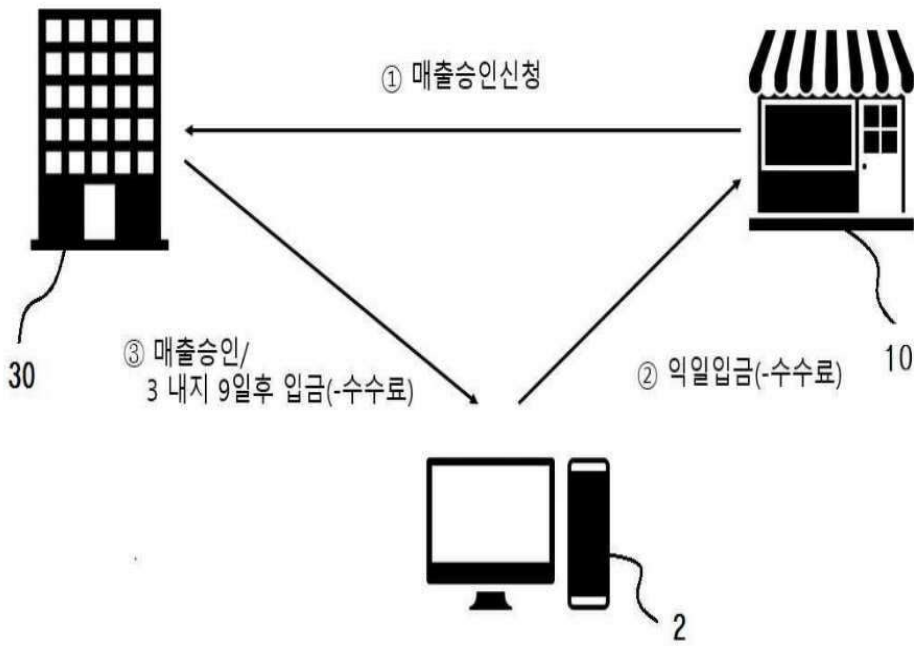
Proof-of-Work Mining:



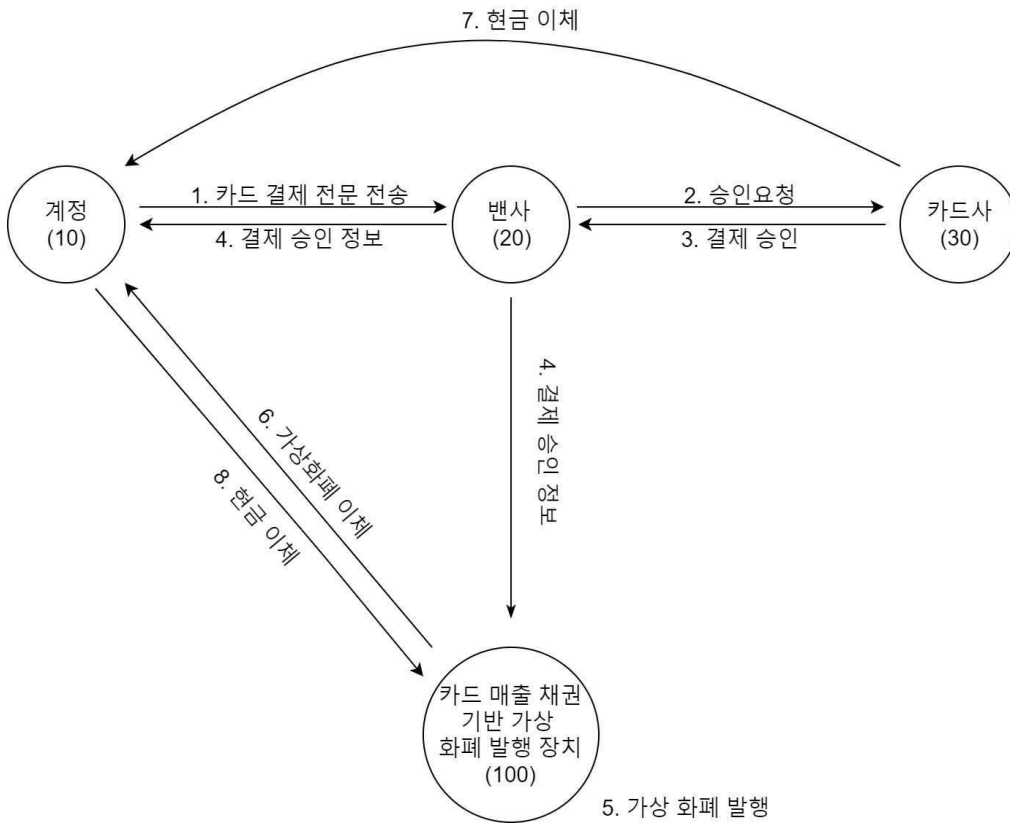
【도 2】



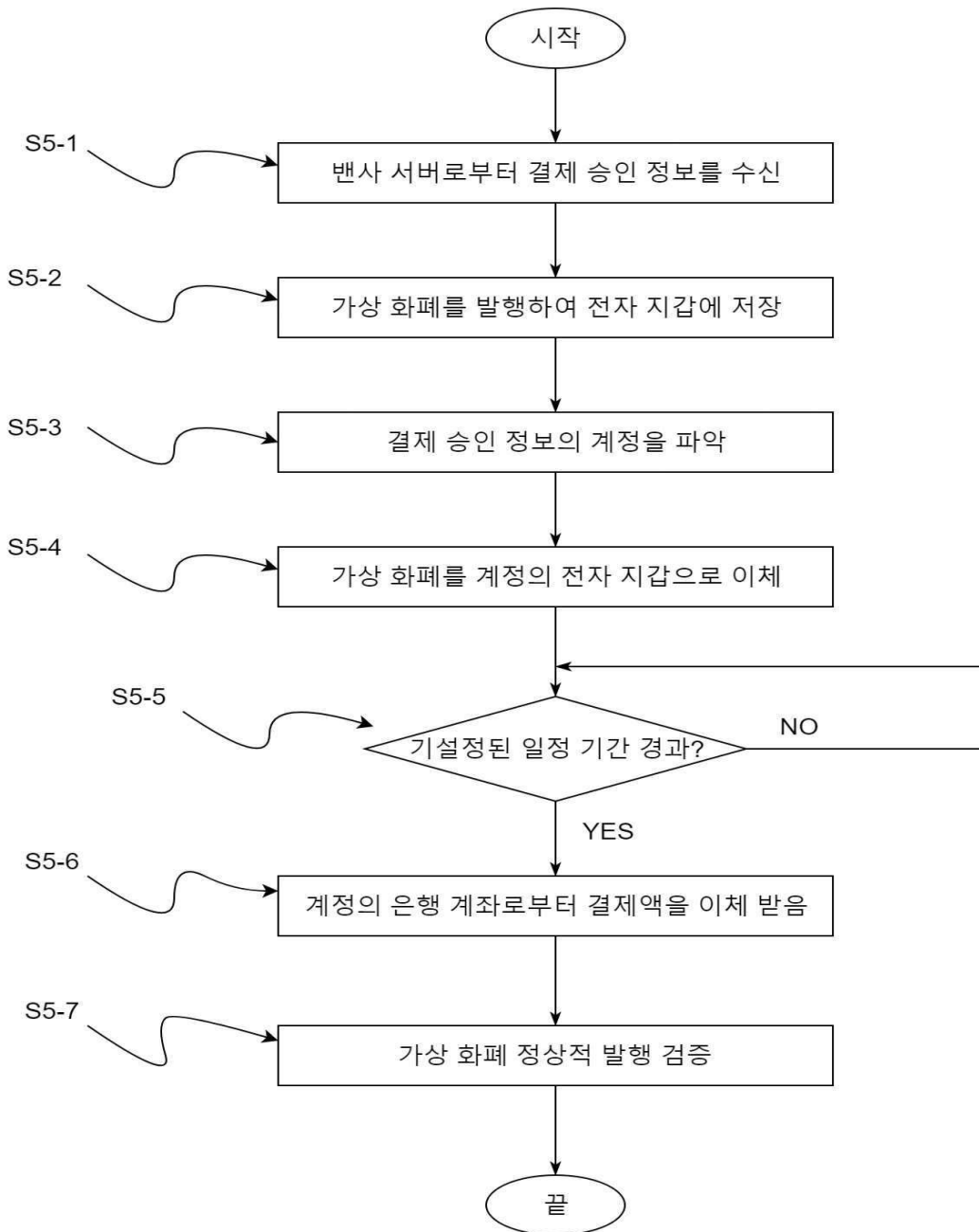
【도 3】



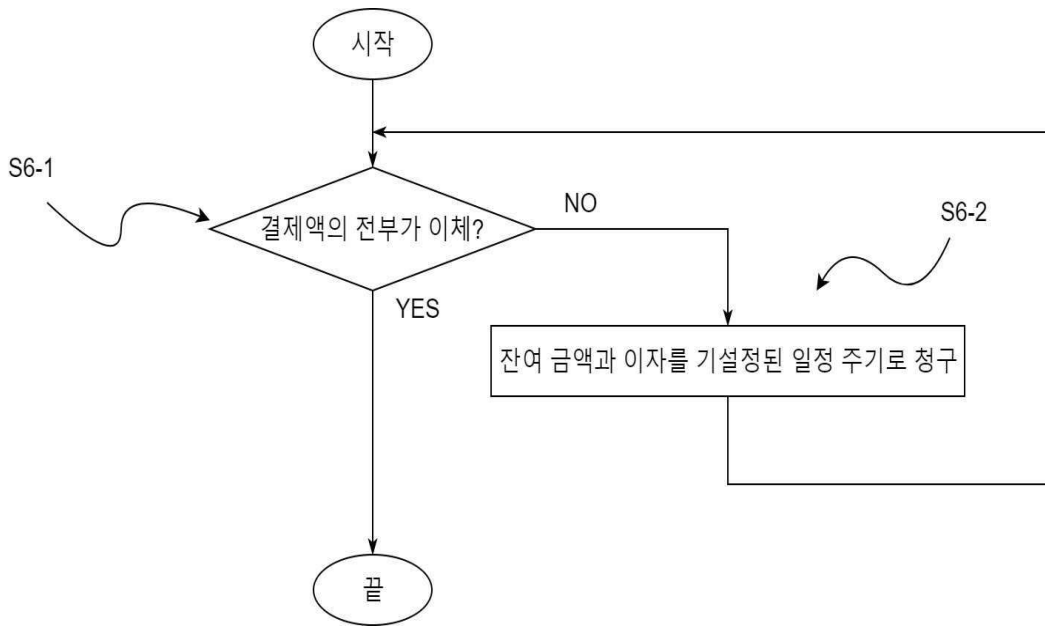
【도 4】



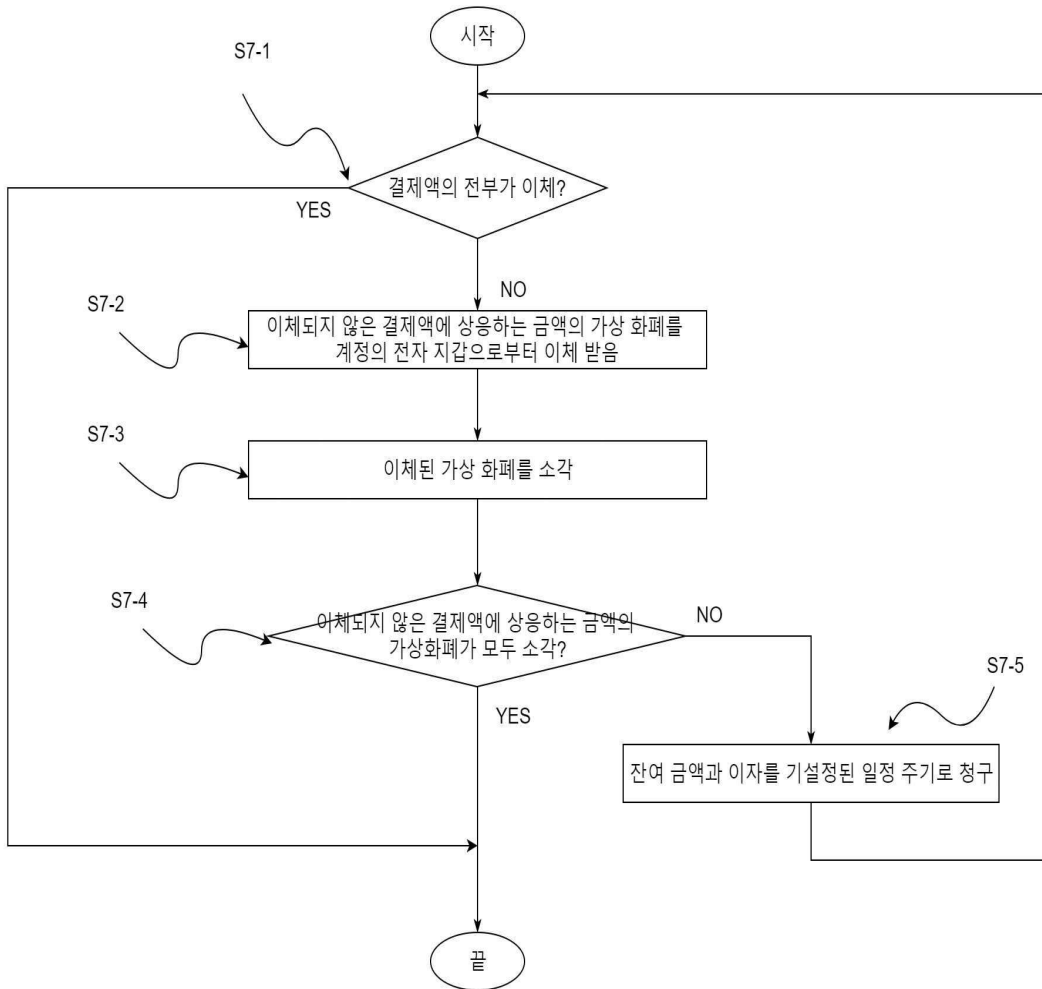
【도 5】



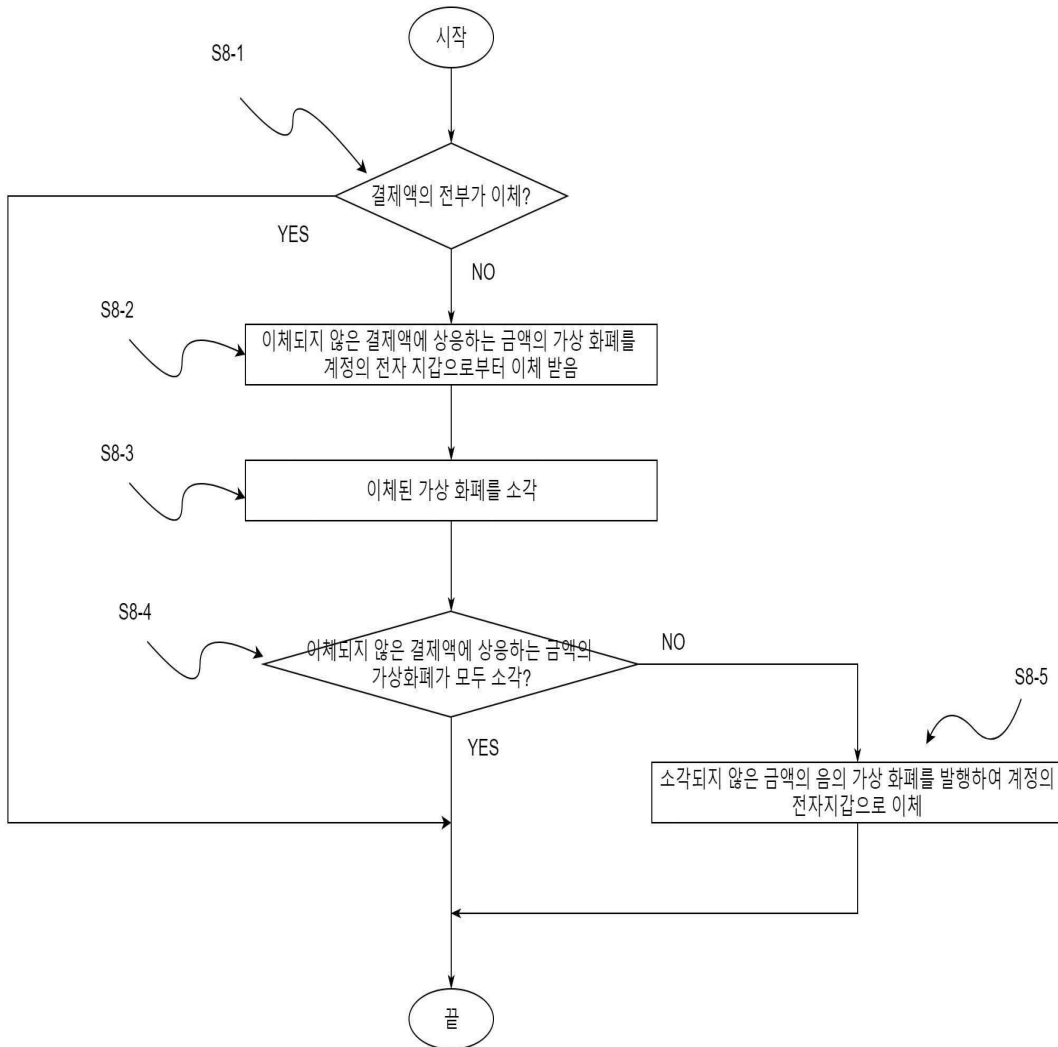
【도 6】



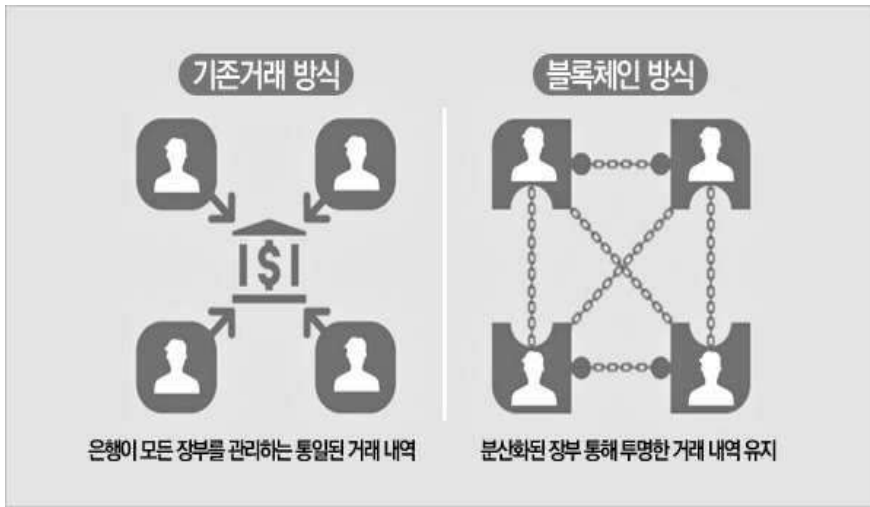
【도 7】



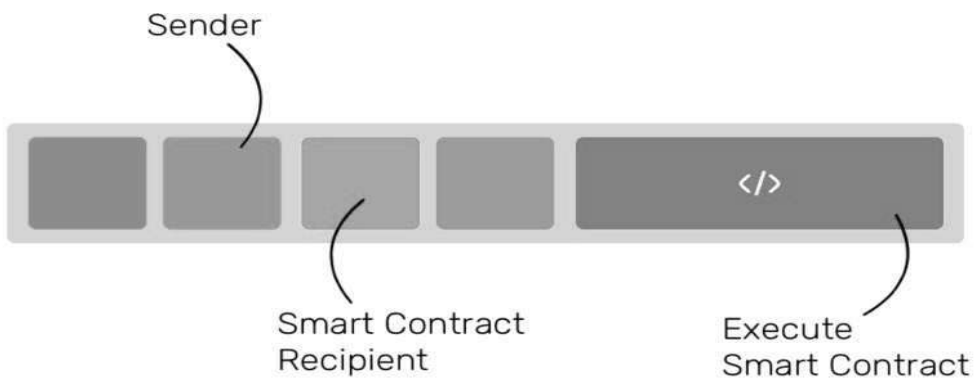
【도 8】



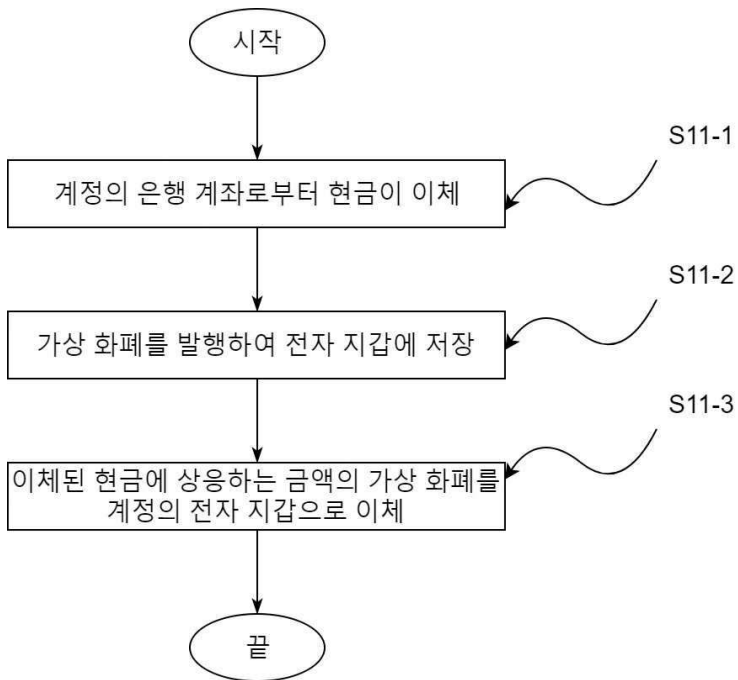
【도 9】



【도 10】



【도 11】



【도 12】

