(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2021-0020606
(43) 공개일자 2021년02월24일

(51) 국제특허분류(Int. Cl.)
G06Q 30/02 (2012.01) *G06Q 50/34* (2012.01)
(52) CPC특허분류
G06Q 30/0212 (2013.01)
G06Q 50/34 (2013.01)
(21) 출원번호 10-2019-0100301
(22) 출원일자 2019년08월16일
심사청구일자 2019년08월16일

(71) 출원인
서강대학교산학협력단
서울특별시 마포구 백범로 35 (신수동, 서강대학교)
(72) 발명자
장주욱
서울특별시 서대문구 가재울미래로 2, 206동 202호 (남가좌제1동, DMC파크뷰자이)
박인환
서울특별시 마포구 백범로 35 리찌과학관(R관) 805호
(74) 대리인
이지연

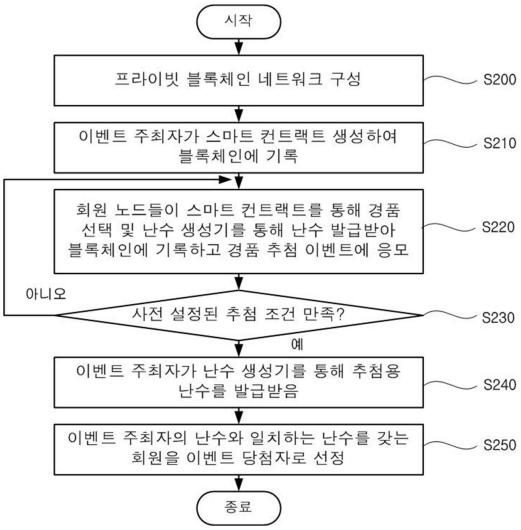
전체 청구항 수 : 총 10 항

(54) 발명의 명칭 **블록체인을 기반으로 한 경품 추첨 이벤트 관리 시스템 및 방법**

(57) 요 약

본 발명은 블록체인을 기반으로 한 경품 추첨 이벤트 관리 시스템 및 방법에 관한 것이다. 상기 경품 추첨 이벤트 관리 시스템은, 인증기관의 단말기, 이벤트 주최자의 단말기 및 회원 단말기들이 각각 노드로서 참가하는 프라이빗 블록체인 네트워크(Private Blockchain Network)를 구성하고, 상기 이벤트 주최자 노드는 이벤트/경품 선택기 및 난수 생성기를 기록한 스마트 컨트랙트를 생성하여 블록체인에 기록하는 것을 특징으로 하며, 상기 회원 노드는, 스마트 컨트랙트의 경품 선택기를 통해 경품을 선택하고, 스마트 컨트랙트의 난수 생성기를 통해 난수를 발급받고, 상기 발급된 난수를 블록의 형태로 블록체인에 기록하여, 이벤트에 응모하는 것을 특징으로 하며, 상기 이벤트 주최자 노드는 사전 설정된 경품 추첨 상태가 되면, 스마트 컨트랙트의 난수 생성기를 통해 난수를 생성하고, 상기 생성된 난수와 일치하는 난수를 블록체인에 기록한 회원 노드를 당첨자로 선택한다.

대 표 도 - 도2



이 발명을 지원한 국가연구개발사업

과제고유번호	R17XA05-44
부처명	한국전력공사
과제관리(전문)기관명	전력연구원
연구사업명	전력산업기초연구
연구과제명	블록체인과 IoT를 결합한 마이크로그리드 기반 신재생에너지 거래 플랫폼
기 여 율	1/1
과제수행기관명	서강대학교 산학협력단
연구기간	2017.05.01 ~ 2020.04.30

명 세 서

청구범위

청구항 1

인증기관의 단말기, 이벤트 주최자의 단말기 및 회원 단말기들이 각각 노드로서 참가하는 프라이빗 블록체인 네트워크(Private Blockchain Network)를 구성하고,

상기 이벤트 주최자 노드는 이벤트/경품 선택기 및 난수 생성기를 기록한 스마트 컨트랙트를 생성하여 블록체인에 기록하는 것을 특징으로 하며,

상기 회원 노드는, 스마트 컨트랙트의 경품 선택기를 통해 경품을 선택하고, 스마트 컨트랙트의 난수 생성기를 통해 난수를 발급받고, 상기 발급된 난수를 블록의 형태로 블록체인에 기록하여, 이벤트에 응모하는 것을 특징으로 하며,

상기 이벤트 주최자 노드는 사전 설정된 경품 추첨 상태가 되면, 스마트 컨트랙트의 난수 생성기를 통해 난수를 생성하고, 상기 생성된 난수와 일치하는 난수를 블록체인에 기록한 회원 노드를 당첨자로 선택하는 것을 특징으로 하는 블록체인을 기반으로 한 경품 추첨 이벤트 관리 시스템.

청구항 2

제1항에 있어서, 상기 스마트 컨트랙트의 경품 선택기는,

이벤트 정보 및 경품 정보를 포함하고,

회원 노드로부터 이벤트 참가 신청되고 경품이 선택되면, 이벤트 응모 노드 정보, 이벤트 참가 신청 정보 및 경품 선택 정보를 포함하는 블록을 생성하여 블록체인에 기록하는 것을 특징으로 하는 블록체인을 기반으로 한 경품 추첨 이벤트 관리 시스템.

청구항 3

제1항에 있어서, 이벤트 참가 신청한 회원 노드인 이벤트 응모 노드는 자신의 공개키를 이용하여 스마트 컨트랙트의 난수 생성기를 열고,

상기 스마트 컨트랙트의 난수 생성기는, 인증기관으로부터 난수 시드의 발급 요청이 발생되면, 스마트 컨트랙트가 난수 시드(Seed)를 생성하여 인증 기관 노드에 발급하는 것을 특징으로 하며,

상기 인증 기관 노드는 스마트 컨트랙트로부터 발급된 난수 시드를 이용하여 난수를 생성하여 이벤트 응모 노드에게 제공하는 것을 특징으로 하는 블록체인을 기반으로 한 경품 추첨 이벤트 관리 시스템.

청구항 4

제3항에 있어서, 상기 인증 기관 노드는 임의의 문자열을 생성하고, 상기 생성된 문자열과 난수 시드의 발급 요청을 포함하는 블록을 생성하여 블록체인에 기록하고,

스마트 컨트랙트는 인증 기관 노드가 생성한 문자열과 난수 시드 발급 요청을 포함하는 블록이 생성된 시간을 포함하는 메시지를 생성하고,

이벤트 응모 노드는 상기 생성된 메시지를 개인키로 서명하고,

스마트 컨트랙트는 상기 서명된 메시지의 유효성을 검증하고, 유효성이 검증되면 난수 시드를 생성하여 인증 기관 노드에 발급하는 것을 특징으로 하는 블록체인을 기반으로 한 경품 추첨 이벤트 관리 시스템.

청구항 5

제1항에 있어서, 상기 이벤트 주최자 노드는,

사전 설정된 이벤트 응모자의 개수가 충족되거나 사전 설정된 시간이 만료되면, 사전 설정된 경품 추첨 상태가 된 것으로 판단하고, 스마트 컨트랙트의 난수 생성기를 통해 난수를 생성하고, 상기 생성된 난수와 동일한 난수

를 블록체인에 기록한 회원 노드를 당첨자로 선택하는 것을 특징으로 하는 블록체인을 기반으로 한 경품 추첨 이벤트 관리 시스템.

청구항 6

제1항에 있어서, 상기 회원 단말기는,

이벤트 주최자 노드로부터 응모권을 제공받고, 상기 응모권의 정보 및 회원 정보를 토대로 하여 상기 인증 기관 노드로부터 인증되면, 인증 기관 노드로부터 개인키, 공개키를 지급받고 프라이빗 블록체인 네트워크의 노드로 참가하는 것을 특징으로 하는 블록체인을 기반으로 한 경품 추첨 이벤트 관리 시스템.

청구항 7

인증기관의 단말기, 이벤트 주최자의 단말기 및 회원 단말기들이 각각 노드로서 참가하는 프라이빗 블록체인 네트워크(Private Blockchain Network)를 이용한 경품 추첨 방법에 있어서,

상기 이벤트 주최자 노드가 이벤트/경품 선택기 및 난수 생성기를 기록한 스마트 컨트랙트를 생성하여 블록체인에 기록하는 단계;

상기 회원 노드가, 스마트 컨트랙트의 이벤트/경품 선택기를 통해 이벤트 참가 신청 및 경품 선택을 하여 이벤트 응모 노드가 되고, 이벤트 응모 노드가 스마트 컨트랙트의 난수 생성기를 통해 난수를 발급받고, 상기 발급된 난수를 블록의 형태로 블록체인에 기록하는 단계;

사전 설정된 경품 추첨 상태가 되면, 상기 이벤트 주최자 노드가, 스마트 컨트랙트의 난수 생성기를 통해 난수를 생성하고, 상기 생성된 난수와 동일한 난수를 블록체인에 기록한 회원 노드를 당첨자로 선택하는 단계;

를 구비하는 것을 특징으로 하는 블록체인을 기반으로 한 온라인 이벤트 경품 추첨 방법.

청구항 8

제7항에 있어서, 상기 스마트 컨트랙트의 경품 선택기는,

이벤트 정보 및 경품 정보를 포함하고,

회원 노드로부터 이벤트 참가 신청되고 경품이 선택되면, 이벤트 참가 신청 정보 및 경품 선택 정보를 포함하는 블록을 생성하여 블록체인에 기록하는 것을 특징으로 하는 블록체인을 기반으로 한 경품 추첨 방법.

청구항 9

제7항에 있어서, 상기 회원 노드가 난수를 블록체인에 기록하는 단계는,

이벤트 응모하고자 하는 노드가 자신의 공개키를 이용하여 스마트 컨트랙트의 난수 생성기를 여는 단계;

상기 스마트 컨트랙트의 난수 생성기는, 인증기관으로부터 발생된 난수 시드 발급 요청에 따라, 스마트 컨트랙트가 난수 시드(Seed)를 생성하여 인증 기관 노드에 발급하는 단계;

상기 인증 기관 노드가 스마트 컨트랙트로부터 발급된 난수 시드를 이용하여 난수를 생성하여 이벤트 참가 신청 노드에게 제공하는 단계;를 구비하는 것을 특징으로 하는 블록체인을 기반으로 한 경품 추첨 방법.

청구항 10

제9항에 있어서, 스마트 컨트랙트가 난수 시드를 생성하는 단계는,

상기 인증 기관 노드가 임의의 문자열을 생성하고, 상기 생성된 문자열과 난수 시드 발급 요청을 포함하는 블록을 생성하여 블록체인에 기록하고,

스마트 컨트랙트가 인증 기관 노드가 생성한 문자열과 난수 시드 발급 요청을 포함하는 블록이 블록체인에 기록된 시간을 포함하는 메시지를 생성하고,

이벤트 참가 신청 노드가 상기 생성된 메시지를 개인키로 서명하고,

스마트 컨트랙트가 상기 서명된 메시지의 유효성을 검증하고, 유효성이 검증되면 난수 시드를 생성하여 인증 기관 노드에 발급하는 것을 특징으로 하는 블록체인을 기반으로 한 경품 추첨 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 블록체인을 기반으로 한 경품 추첨 이벤트 관리 시스템 및 방법에 관한 것으로서, 더욱 구체적으로는 인증 기관, 이벤트 주최자 노드 및 회원 노드들이 프라이빗 블록체인 네트워크를 구성하고, 블록체인의 스마트 컨트랙트에 난수 생성기를 기록하고, 난수 생성기를 통해 스마트 컨트랙트가 발급한 난수 시드를 이용하여 인증 기관이 난수를 생성하고, 이를 토대로 하여 경품 추첨을 수행하는 것을 특징으로 하는 블록체인을 기반으로 한 경품 추첨 이벤트 관리 시스템 및 방법에 관한 것이다.

배 경 기 술

[0002] 경품을 추첨하여 제공하는 다양한 형태의 이벤트들이 여러 분야에서 많이 진행되고 있다. 이때, 이벤트 주최자들은 많은 응모자들을 모집하고, 사전 설정된 경품들을 제공하기 위하여 추첨하고, 추첨 결과에 따라 사전 공지한 경품들을 당첨자에게 제공하게 된다.

[0003] 하지만, 응모자들의 응모 행위, 이벤트 주최자의 추첨 행위 및 당첨자에 대한 경품 제공 행위 등이 모두 공정하게 진행되어야 하나, 이 모든 단계들을 정확하면서도 공정하게 감시하는 것은 실제로 매우 어려운 작업이다. 따라서, 이 과정들 중에 불공정 행위나 불법 행위들이 많이 발생하게 되는 문제점이 있다.

[0004] 또한, 종래의 경품 추첨 시스템은 경품의 지급 및 경품의 종류가 기존에 공지된 그대로 진행되지 않거나, 단순히 이용자들을 모으기 위한 수단으로 사용되는 경우가 왕왕 발생하고, 이벤트 주최자가 임의로 당첨자를 조작하여 이벤트 주최자와 관련된 사람이 경품을 수령하는 등의 문제가 발생하게 됨에 따라, 이벤트의 공정성 및 신뢰성이 완전하게 보장되지 않는다.

[0005] 이에 따라, 본 발명은 난수를 이용하여 블록체인을 기반으로 한 공정한 경품 추첨 이벤트 관리 시스템을 제안하고자 한다. 하지만, 블록체인 네트워크에서도 난수를 생성한 다양한 방법이 제안되고 있으나, 대부분의 방법들이 각각의 문제점들이 내포되어 있는 실정이다.

[0006] 난수 생성 방법 중 하나는 블록체인에서 블록의 상태값을 활용하여 난수를 생성하는 방식으로서, 해당 트랜잭션에 따라 매번 달라지는 블록의 해쉬값을 이용하게 된다. 하지만, 이 방식은 블록에 어떤 트랜잭션이 포함될지 알 수 없기 때문에 난수를 생성하는 것이 합리적으로 보이기는 하나, 작업 증명(Proof of Work;PoW) 방식으로 블록을 생성한 마이너(miner)가 블록의 트랜잭션의 순서를 바꿔 마이너가 원하는 해쉬값을 만들어 낼 가능성이 존재한다. 따라서, 이 난수 생성 방법은 공정한 난수를 생성하지 못할 수 있는 문제점이 있다.

[0007] 난수를 생성하는 다른 방식은, 스마트 컨트랙트 생성자가 여러 개의 해싱 시드(Hashing Seed)를 넣어 스마트 컨트랙트를 생성하는 것이다. 이때 난수 요청자는 스마트 컨트랙트의 해싱 시드들 중 하나를 선택하고, 선택된 해싱 시드를 대신하여 다른 해싱 시드를 스마트 컨트랙트에게 제공한다. 해싱 시드는 각 참여자가 중복으로 선택할 수 없도록 하고, 스마트 컨트랙트는 선택된 해싱 시드와 새로이 제공된 시드를 조합하여 난수를 생성하게 된다. 하지만, 이러한 난수 생성 방법은 스마트 컨트랙트 생성자가 컨트랙트를 생성할 때 해싱 시드가 무엇인지 알고 있기 때문에 검증 기관의 인증을 받더라도 경품 추첨 이벤트 관리 시스템에서 공정하지 못한 방법으로 난수를 제공할 가능성이 존재하는 문제점이 있다. 또한, 다수의 이벤트 참가자가 발생하는 경우, 스마트 컨트랙트의 해싱 시드들이 더 많이 필요하게 되고, 이 경우 스마트 컨트랙트의 저장 용량이 증가되어야 하므로 확장성을 고려하기 어려운 문제점도 발생하게 된다.

[0008] 또 다른 난수 생성 방법은, 스마트 컨트랙트 생성자가 해싱 시드를 대신하여 자신의 공개키를 스마트 컨트랙트에 올리면 난수 요청자는 시드를 제공하고, 스마트 컨트랙트 생성자의 공개키에 상응하는 개인키로 시드를 서명하고, 서명 정보로 난수를 생성하는 방법이다. 하지만 이 난수 생성 방법은, 난수 요청자가 제공한 시드가 중복되면 안되므로, 사용한 시드를 저장하여 중복을 방지하여야 하므로 스마트 컨트랙트의 저장 용량이 증가하게 되는 문제점이 발생한다. 또한, 요청한 시드가 많아질수록 중복 확인에 필요한 시간이 많이 소요되는 문제점이 있다.

선행기술문헌

특허문헌

[0009] (특허문헌 0001) 한국등록특허공보 제 10-1887964호

(특허문헌 0002) 한국등록특허공보 제 10-1928087호

발명의 내용

해결하려는 과제

[0010] 전술한 문제점을 해결하기 위한 본 발명의 목적은 난수 생성시에 스마트 컨트랙트의 서명을 통한 유효성 검증을 통해 스마트 컨트랙트가 난수 시드를 발급하고, 이에 따라 인증기관이 난수를 발급함으로써 스마트 컨트랙트의 저장 용량 문제와 불공정 문제를 해결할 수 있도록 하는 블록체인 네트워크를 기반으로 하여 경품 추첨 이벤트 관리 시스템 및 방법을 제공하는 것이다.

[0011] 또한, 본 발명의 다른 목적은 블록체인의 인증, 부인 방지, 데이터 무결성 특성에 의하여 악의적인 공격자의 데이터 위/변조가 원천적으로 방지되고, 이벤트 진행시 정확하고 공정하게 경품을 지급할 수 있도록 하는 경품 추첨 이벤트 관리 시스템 및 방법을 제공하는 것이다.

과제의 해결 수단

[0012] 전술한 기술적 과제를 달성하기 위한 본 발명의 제1 특징에 따른 블록체인을 기반으로 한 경품 추첨 이벤트 관리 시스템은, 인증기관의 단말기, 이벤트 주최자의 단말기 및 회원 단말기들이 각각 노드로서 참가하는 프라이빗 블록체인 네트워크(Private Blockchain Network)를 구성하고,

[0013] 상기 이벤트 주최자 노드는 이벤트/경품 선택기 및 난수 생성기를 기록한 스마트 컨트랙트를 생성하여 블록체인에 기록하는 것을 특징으로 하며, 상기 회원 노드는, 스마트 컨트랙트의 경품 선택기를 통해 경품을 선택하고, 스마트 컨트랙트의 난수 생성기를 통해 난수를 발급받고, 상기 발급된 난수를 블록의 형태로 블록체인에 기록하여, 이벤트에 응모하는 것을 특징으로 하며, 상기 이벤트 주최자 노드는 사전 설정된 경품 추첨 상태가 되면, 스마트 컨트랙트의 난수 생성기를 통해 난수를 생성하고, 상기 생성된 난수와 동일한 난수를 블록체인에 기록한 회원 노드를 당첨자로 선택한다.

[0014] 전술한 제1 특징에 따른 블록체인을 기반으로 한 경품 추첨 이벤트 관리 시스템에 있어서, 상기 스마트 컨트랙트의 경품 선택기는, 이벤트 정보 및 경품 정보를 포함하고, 회원 노드로부터 이벤트 참가 신청되고 경품이 선택되면, 이벤트 응모 노드 정보, 이벤트 참가 신청 정보 및 경품 선택 정보를 포함하는 블록을 생성하여 블록체인에 기록하는 것이 바람직하다.

[0015] 전술한 제1 특징에 따른 블록체인을 기반으로 한 경품 추첨 이벤트 관리 시스템에 있어서, 이벤트 참가 신청한 회원 노드인 이벤트 응모 노드는 자신의 공개키를 이용하여 스마트 컨트랙트의 난수 생성기를 열고, 상기 스마트 컨트랙트의 난수 생성기는, 인증기관으로부터 난수 시드의 발급 요청이 발생되면, 스마트 컨트랙트가 난수 시드(Seed)를 생성하여 인증 기관 노드에 발급하는 것을 특징으로 하며, 상기 인증 기관 노드는 스마트 컨트랙트로부터 발급된 난수 시드를 이용하여 난수를 생성하여 이벤트 응모 노드에게 제공하는 것이 바람직하다.

[0016] 전술한 제1 특징에 따른 블록체인을 기반으로 한 경품 추첨 이벤트 관리 시스템에 있어서, 상기 인증 기관 노드는 임의의 문자열을 생성하고, 상기 생성된 문자열과 난수 시드의 발급 요청을 포함하는 블록을 생성하여 블록체인에 기록하고, 스마트 컨트랙트는 인증 기관 노드가 생성한 문자열과 난수 시드 발급 요청을 포함하는 블록이 생성된 시간을 포함하는 메시지를 생성하고, 이벤트 응모 노드는 상기 생성된 메시지를 개인키로 서명하고, 스마트 컨트랙트는 상기 서명된 메시지의 유효성을 검증하고, 유효성이 검증되면 난수 시드를 생성하여 인증 기관 노드에 발급하는 것이 바람직하다.

[0017] 전술한 제1 특징에 따른 블록체인을 기반으로 한 경품 추첨 이벤트 관리 시스템에 있어서, 상기 이벤트 주최자 노드는, 사전 설정된 이벤트 응모자의 개수가 충족되거나 사전 설정된 시간이 만료되면, 사전 설정된 경품 추첨 상태가 된 것으로 판단하고, 스마트 컨트랙트의 난수 생성기를 통해 난수를 생성하고, 상기 생성된 난수와 동일한 난수를 블록체인에 기록한 회원 노드를 당첨자로 선택하는 것이 바람직하다.

[0018] 전술한 제1 특징에 따른 블록체인을 기반으로 한 경품 추첨 이벤트 관리 시스템에 있어서, 상기 회원 단말기는,

이벤트 주최자 노드로부터 응모권을 제공받고, 상기 응모권의 정보 및 회원 정보를 토대로 하여 상기 인증 기관 노드로부터 인증되면, 인증 기관 노드로부터 개인키, 공개키를 지급받고 프라이빗 블록체인 네트워크의 노드로 참가하는 것이 바람직하다.

[0019] 본 발명의 제2 특징에 따른 블록체인을 기반으로 한 경품 추첨 이벤트 관리 방법은, 인증기관의 단말기, 이벤트 주최자의 단말기 및 회원 단말기들이 각각 노드로서 참가하는 프라이빗 블록체인 네트워크(Private Blockchain Network)를 이용한 경품 추첨 방법에 관한 것으로서, 상기 이벤트 주최자 노드가 이벤트/경품 선택기 및 난수 생성기를 기록한 스마트 컨트랙트를 생성하여 블록체인에 기록하는 단계, 상기 회원 노드가, 스마트 컨트랙트의 이벤트/경품 선택기를 통해 이벤트 참가 신청 및 경품 선택을 하여 이벤트 응모 노드가 되고, 이벤트 응모 노드가 스마트 컨트랙트의 난수 생성기를 통해 난수를 발급받고, 상기 발급된 난수를 블록의 형태로 블록체인에 기록하는 단계; 사전 설정된 경품 추첨 상태가 되면, 상기 이벤트 주최자 노드가, 스마트 컨트랙트의 난수 생성기를 통해 난수를 생성하고, 상기 생성된 난수와 동일한 난수를 블록체인에 기록한 회원 노드를 당첨자로 선택하는 단계를 구비한다.

발명의 효과

[0020] 전술한 구성을 갖는 본 발명에 따른 경품 추첨 이벤트 관리 시스템은 프라이빗 블록체인 네트워크와 스마트 컨트랙트 기술을 결합한 것으로서, 경품 추첨 시스템에서 추첨에 관한 모든 사항을 블록체인에 기록함으로써, 데이터의 무결성 및 보안성을 보장할 수 있고, 스마트 컨트랙트를 통해 계약 이행의 강제성과 자동성을 보장할 수 있게 된다. 본 발명에 따른 경품 추첨 이벤트 관리 시스템은 블록체인 네트워크를 기반으로 하고, 경품 선택 및 난수 생성을 위한 트랜잭션 등 모든 트랜잭션은 각 노드가 작업 증명 과정을 통해 블록을 생성하게 되고, 이렇게 생성된 블록은 과반수 노드에게 유효성을 검증받고 해당 시점까지 모인 트랜잭션을 모두 포함하는 (n+1)번째 블록을 생성하여 블록체인에 기록된다. 블록체인에 기록되는 모든 트랜잭션 및 데이터는 무결성을 보장받고 블록체인 내 모든 노드들은 이 기록들을 공유하게 된다. 또한, 악의적인 공격자에 의한 데이터 위/변조가 원천적으로 방지된다.

[0021] 이벤트 참여자는 이벤트 주체자로부터 응모권을 받아 프라이빗 블록체인 네트워크에 참여하는 동시에 인증기관으로부터 개인 정보의 인증을 받음으로써, 블록체인에 악의적인 노드가 참여하는 것을 미연에 방지할 수 있다. 또한, 본 발명에 따른 시스템은 모든 데이터들이 블록체인에 분산되어 보관되기 때문에, 경품의 당첨 조작 및 데이터 위변조 시도를 원천적으로 차단할 수 있을 뿐만 아니라 데이터의 투명성이 보장되므로 당첨자를 확인할 수 있다.

[0022] 또한, 본 발명에 따른 시스템에 있어서, 스마트 컨트랙트를 통해 계약의 이행이 보장되어 경품의 지급 및 지급일자에 관련된 문제를 방지할 수 있으며, 스마트 컨트랙트에서 안전한 난수 생성 방법을 제시함으로써, 추첨의 조작이 불가능하게 된다.

[0023] 본 발명에 따른 경품 추첨 이벤트 관리 시스템에서는 인증기관이 난수를 생성하도록 함으로써, 인증 기관이 무한대로 난수를 생성할 수 있을 뿐만 아니라, 난수를 생성하는 과정에서 인증 기관이 무작위 배열을 생성하도록 함으로써 응모권을 가진 회원의 선택에 대해 독립적으로 작동하게 된다. 한편, 무작위 배열이 재사용 된다 하더라도, 인증기관과 응모권을 가진 회원에 어떠한 영향도 받지 않는 블록 시간을 추가적인 변수로 넣고 난수 생성 시에 블록 시간이 결정됨으로써, 마이너가 임의로 시간을 조작할 수 없기 때문에 포크 어택(Fork Attack)을 예방할 수 있게 된다.

[0024] 또한, 본 발명에 따른 방법은 난수를 생성하는 어떤 데이터도 스마트 컨트랙트에 저장되지 않기 때문에, 데이터 저장 용량의 문제도 해결할 수 있게 된다 .

도면의 간단한 설명

[0025] 도 1은 본 발명의 바람직한 실시예에 따른 경품 추첨 이벤트 관리 시스템을 설명하기 위하여 도시한 모식도이다.

도 2는 본 발명의 바람직한 실시예에 따른 경품 추첨 이벤트 관리 시스템에 있어서, 전체적으로 경품 추첨 이벤트가 진행되는 과정을 순차적으로 도시한 흐름도이다.

도 3은 본 발명의 바람직한 실시예에 따른 경품 추첨 이벤트 관리 시스템에 있어서, 프라이빗 블록체인 네트워크를 구성하는 과정을 순차적으로 도시한 흐름도이다.

도 4는 본 발명의 바람직한 실시예에 따른 경품 추첨 이벤트 관리 시스템에 있어서, 회원 노드가 스마트 컨트랙트의 난수 생성기를 통해 난수를 발급받는 과정을 구체적으로 설명한다.

도 5는 본 발명의 바람직한 실시예에 따른 경품 추첨 이벤트 관리 시스템에 있어서, 이벤트 주최자가 이벤트 관련 정보를 포함하는 스마트 컨트랙트를 작성하여 블록체인에 기록하는 과정을 순차적으로 도시한 흐름도이다.

도 6은 본 발명의 바람직한 실시예에 따른 경품 추첨 이벤트 관리 시스템에 있어서, 회원 노드가 경품 추첨 이벤트에 응모하여 블록체인에 기록하는 과정을 순차적으로 도시한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0026] 본 발명에 따른 경품 추첨 이벤트 관리 시스템은 인증 기관, 이벤트 주최자 및 회원의 단말기들이 노드로 참가하는 프라이빗 블록체인 네트워크를 구성하고, 스마트 컨트랙트를 통해 회원 노드가 이벤트 및 경품 추첨 참가에 따른 난수를 발급받고, 이벤트 주최자 노드가 난수와 동일한 난수를 갖는 회원 노드를 당첨자로 결정하는 것을 특징으로 한다.

[0027] 이하, 첨부된 도면을 참조하여 본 발명의 바람직한 실시예에 따른 블록체인 네트워크를 기반으로 한 경품 추첨 이벤트 관리 시스템 및 방법에 대하여 구체적으로 설명한다.

[0028] 도 1은 본 발명의 바람직한 실시예에 따른 경품 추첨 이벤트 관리 시스템을 설명하기 위하여 도시한 모식도이다. 도 1을 참조하면, 본 발명에 따른 경품 추첨 이벤트 관리 시스템(1)은 인증 기관(10), 이벤트 주최자(20) 및 회원들(30)의 단말기는 노드로서 참가하여 프라이빗 블록체인 네트워크(Private Blockchain Network)를 구성하고, 각 노드들은 블록체인을 기록하고 관리한다.

[0029] 도 2는 본 발명의 바람직한 실시예에 따른 경품 추첨 이벤트 관리 시스템에 있어서, 전체적으로 경품 추첨 이벤트가 진행되는 과정을 순차적으로 도시한 흐름도이다. 도 2를 참조하면, 본 발명에 따른 경품 추첨 이벤트 관리 시스템에서의 경품 추첨 과정은 먼저 인증 기관, 이벤트 주최자 및 응모권을 가진 회원들이 노드로서 참가하여 프라이빗 블록체인 네트워크를 구성한다(단계 200).

[0030] 다음, 이벤트 주최자는 난수 생성기, 경품의 종류 및 지급 방식, 제세 공과금 등의 사항을 스마트 컨트랙트에 기록하고, 이벤트 주최자의 개인키로 서명한 후, 서명의 유효성이 검증되면 블록체인에 기록한다(단계 210).

[0031] 다음, 회원 노드들은 각각 스마트 컨트랙트를 통해 경품의 종류 및 지급 방식을 선택하고, 제세 공과금 등의 필요 사항들을 선택한 후, 난수 생성기를 이용하여 난수를 발급받고, 발급된 난수를 포함하는 블록을 생성하여 블록체인에 기록함으로써, 경품 추첨 이벤트에 응모한다(단계 220).

[0032] 다음, 사전 설정된 이벤트 응모자의 수가 충족되었거나 사전 설정된 응모 기간이 만료되면(단계 230), 이벤트 주최자는 스마트 컨트랙트의 난수 생성기를 통해 난수를 생성한다(단계 240). 이벤트 주최자의 난수와 일치하는 난수를 가진 회원이 있으면, 이벤트 당첨자로 선정된다(단계 250). 한편, 이벤트 주최자 노드가 생성한 난수와 일치하는 난수를 갖는 회원이 없다면, 이벤트 주최자 노드는 일치하는 난수를 갖는 회원이 나올 때 까지 난수 생성 과정을 수회 반복하게 된다.

[0033] 이벤트 주최자의 추첨을 위한 난수와 일치하는 난수를 가진 회원 노드에게는 이벤트 당첨자임을 나타내는 메시지를 전송하고, 스마트 컨트랙트를 통해 경품의 지급 절차를 진행하게 되며(단계 260), 난수와 일치하지 않는 난수를 가진 회원 노드에게는 이벤트 당첨이 실패되었음을 나타내는 메시지를 전송한다.

[0034] 이하, 전술한 각 단계에 대하여 보다 구체적으로 설명한다.

[0035] 먼저, 도 3을 참조하여 본 발명에 따라 프라이빗 블록체인 네트워크를 구성하는 과정을 구체적으로 설명한다. 도 3은 본 발명의 바람직한 실시예에 따른 경품 추첨 이벤트 관리 시스템에 있어서, 프라이빗 블록체인 네트워크를 구성하는 과정을 순차적으로 도시한 흐름도이다.

[0036] 도 3을 참조하면, 먼저 이벤트 주최자(20)는 자신의 정보를 인증 기관에 제출하고(단계 300), 인증 기관으로부터 인증을 받고(단계 310/단계 320) 프라이빗 블록체인 네트워크에 하나의 노드로서 참가하게 된다.

[0037] 또한, 각 회원들은 이벤트 주최자로부터 응모권을 제공받고, 응모권을 가진 회원은 이벤트 주최자 노드에 의해 프라이빗 블록체인 네트워크에 초대되고(단계 330), 상기 초대된 회원은 자신의 개인 정보, 예컨대 이름, 전화번호, 주민등록번호 등을 인증 기관에 제출하고 인증을 요청하며(단계 340), 이에 따라 인증 기관은 회원의 정보 타당성을 검토하고 신뢰성을 확인하여 인증하며(단계 350), 공개키와 개인키를 제공함으로써(단계 360), 해

당 회원 노드는 프라이빗 블록체인 네트워크의 노드로서 참가할 수 있게 된다(단계 370).

[0038] 이하, 도 4를 참조하여 본 발명에 따른 시스템에 있어서 회원 노드가 스마트 컨트랙트의 난수 생성기를 이용하여 경품 추첨 이벤트에 응모하기 위하여 난수를 발급받는 과정을 설명한다.

[0039] 도 4는 본 발명의 바람직한 실시예에 따른 경품 추첨 이벤트 관리 시스템에 있어서, 회원 노드가 스마트 컨트랙트의 난수 생성기를 통해 난수를 발급받는 과정을 구체적으로 설명한다. 도 4를 참조하면, 경품 추첨 이벤트에 응모하는 회원 노드는 스마트 컨트랙트의 난수 생성기를 자신의 공개키로 열고(단계 400), 인증기관은 임의의 문자열을 생성하고, 문자열과 함께 난수 시드 생성을 요청하며(단계 410), 인증기관의 난수 시드 생성 요청은 블록으로 생성되어 블록체인에 기록된다(단계 420). 스마트 컨트랙트는 인증 기관이 생성한 문자열과 상기 난수 시드 생성 요청을 포함하는 블록이 생성된 시간을 포함한 메시지를 생성한다(단계 430). 상기 회원 노드는 자신의 개인키로 서명을 하고, 위의 스마트 컨트랙트의 메시지에 상기 서명을 넣는다(단계 440). 다음, 스마트 컨트랙트는 상기 회원 노드의 공개키, 개인키 서명, 및 스마트 컨트랙트가 생성한 메시지에 대한 유효성을 검증하고(단계 450), 유효성이 검증되면 스마트 컨트랙트는 난수 생성을 위한 난수 시드를 생성하여 인증기관으로 발급한다(단계 460). 상기 인증기관은 스마트 컨트랙트로부터 난수 시드를 제공받고, 이를 이용하여 난수를 생성하여 회원 노드에게 발급한다(단계 470). 한편, 인증기관으로부터 난수를 발급받은 회원 노드는 해당 난수를 포함하는 블록을 생성하여 블록체인에 기록한다(단계 480).

[0040] 전술한 과정을 통하여, 난수를 생성하면 인증기관이 무한대로 난수를 생성할 수 있고, 난수를 생성하는 과정에서 인증 기관이 무작위 배열을 생성하도록 함으로써 응모권을 가진 회원의 선택에 독립적으로 작동하도록 한다. 그리고, 무작위 배열이 재사용된다 하더라도, 인증 기관과 응모권을 가진 회원에게 어떠한 영향도 받지 않는 블록 시간을 추가적인 변수로 사용하고, 응모권을 가진 회원이 난수를 생성할 때 블록 시간이 결정됨으로써, 마이너가 임의로 시간을 조작할 수 없도록 하여 포크 어택(Fork Attack)을 예방할 수 있다. 또한, 전술한 본 발명에 따른 방법은 난수 생성하는 어떠한 데이터도 스마트 컨트랙트에 저장되지 않기 때문에 데이터 저장 용량의 문제들도 해결될 수 있다.

[0041] 이하, 도 5를 참조하여 본 발명에 따른 경품 추첨 이벤트 관리 시스템에 있어서, 이벤트 주최자가 스마트 컨트랙트를 작성하여 블록체인에 기록하는 과정(도 2의 단계 210)을 설명한다.

[0042] 도 5는 본 발명의 바람직한 실시예에 따른 경품 추첨 이벤트 관리 시스템에 있어서, 이벤트 주최자가 이벤트 관련 정보를 포함하는 스마트 컨트랙트를 작성하여 블록체인에 기록하는 과정을 순차적으로 도시한 흐름도이다. 도 5를 참조하면, 이벤트 주최자는 경품의 종류, 지급날짜 및 지급 정보, 제세 공과금 관련 정보, 난수 생성기를 포함하는 스마트 컨트랙트를 작성한다(단계 500). 스마트 컨트랙트를 이벤트 주최자의 개인키로 서명한 후, 사전 설정된 작업 증명 과정(PoW)을 거쳐 블록을 생성한다(단계 510), 다음, 상기 스마트 컨트랙트를 포함하는 블록을 블록체인에 기록하여 추가함으로써, 블록체인 네트워크를 구성하는 노드들이 공유하게 된다(단계 520).

[0043] 이하, 도 6을 참조하여 본 발명에 따른 경품 추첨 이벤트 관리 시스템에 있어서, 회원 노드가 경품 추첨 이벤트에 응모하여 난수를 발급받아 블록체인에 기록하는 과정을 설명한다.

[0044] 도 6은 본 발명의 바람직한 실시예에 따른 경품 추첨 이벤트 관리 시스템에 있어서, 회원 노드가 경품 추첨 이벤트에 응모하여 블록체인에 기록하는 과정을 순차적으로 도시한 흐름도이다. 도 6을 참조하면, 경품 추첨 이벤트에 응모하고자 하는 회원 노드는 프라이빗 블록체인 네트워크에 참여한 후 스마트 컨트랙트를 호출하고(단계 600), 스마트 컨트랙트를 통해 경품의 종류, 수량, 지급 방식 등을 선택하고, 난수 생성기를 통해 인증 기관으로부터 난수를 발급받아 트랜잭션에 추가한다(단계 610).

[0045] 회원 노드는 상기 트랜잭션을 자신의 개인키로 서명한 후 프라이빗 블록체인 네트워크에 전파하고(단계 620), 작업 증명(PoW) 과정을 거쳐 트랜잭션에 대한 블록을 생성하고 해당 블록을 네트워크에 전파하며(단계 630), 각 노드들이 블록을 검증하고(단계 640), 과반수 이상의 노드들이 해당 블록에 대하여 승인하면(단계 650), 각 노드들은 상기 승인된 블록을 블록체인에 기록하게 되고 그 결과 모든 노드들이 해당 블록을 공유할 수 있게 된다(단계 660).

[0046] 이상에서 본 발명에 대하여 그 바람직한 실시예를 중심으로 설명하였으나, 이는 단지 예시일 뿐 본 발명을 한정하는 것이 아니며, 본 발명이 속하는 분야의 통상의 지식을 가진 자라면 본 발명의 본질적인 특성을 벗어나지 않는 범위에서 이상에 예시되지 않은 여러 가지의 변형과 응용이 가능함을 알 수 있을 것이다. 그리고, 이러한 변형과 응용에 관계된 차이점들은 첨부된 청구 범위에서 규정하는 본 발명의 범위에 포함되는 것으로 해석되어

야 할 것이다.

부호의 설명

[0047] 1 : 경품 추첨 이벤트 관리 시스템

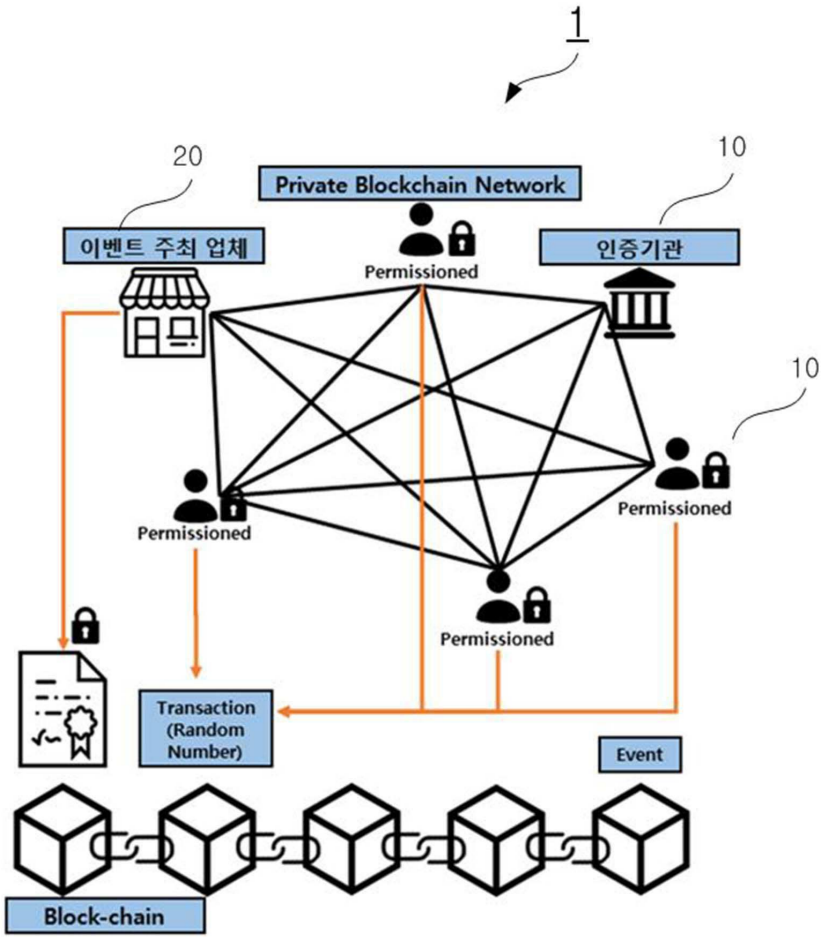
10 : 인증 기관 노드

20 : 이벤트 주최자 노드

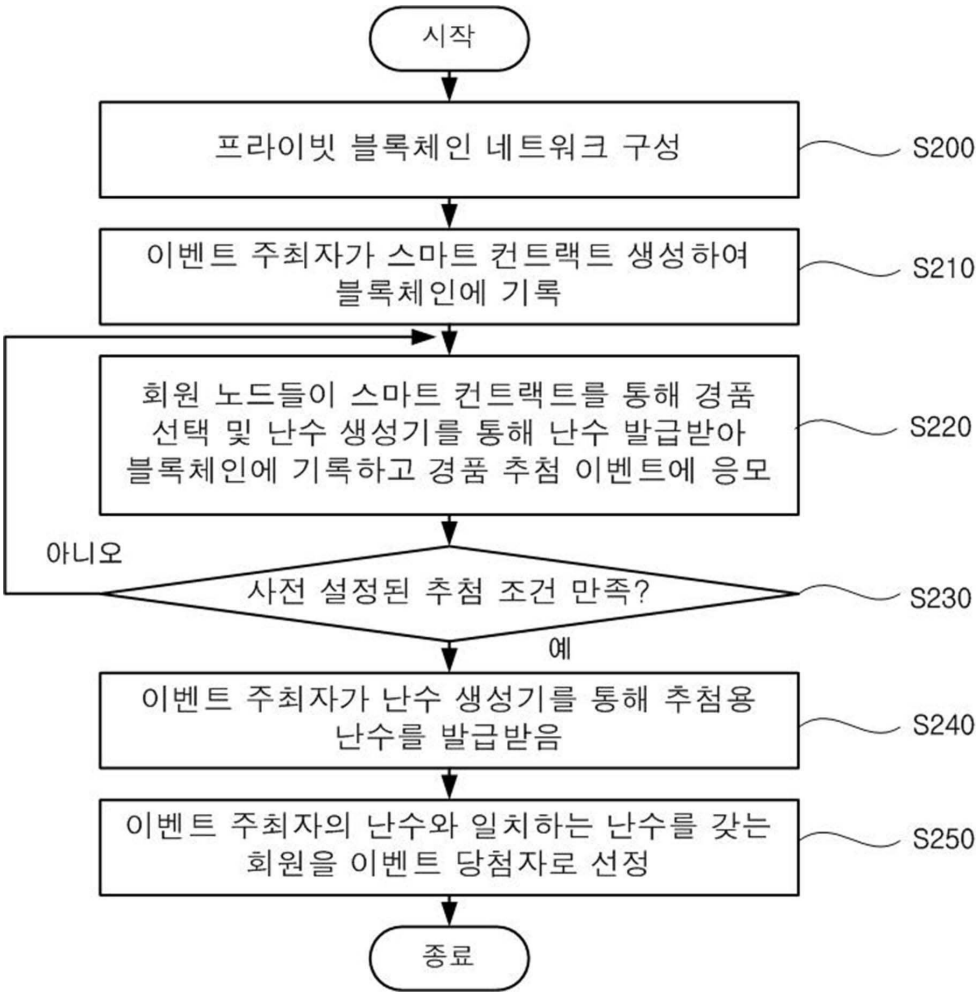
30 : 회원 노드

도면

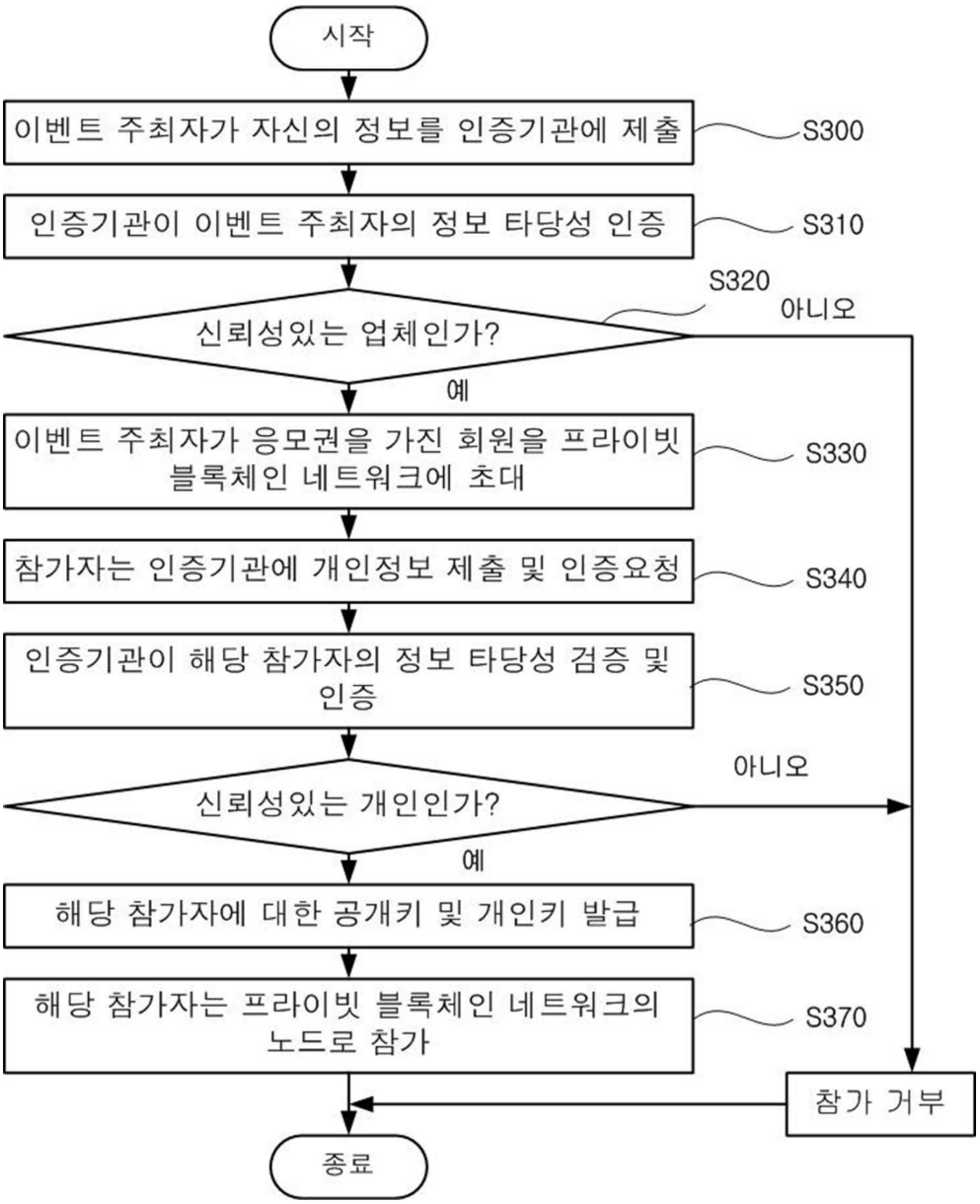
도면1



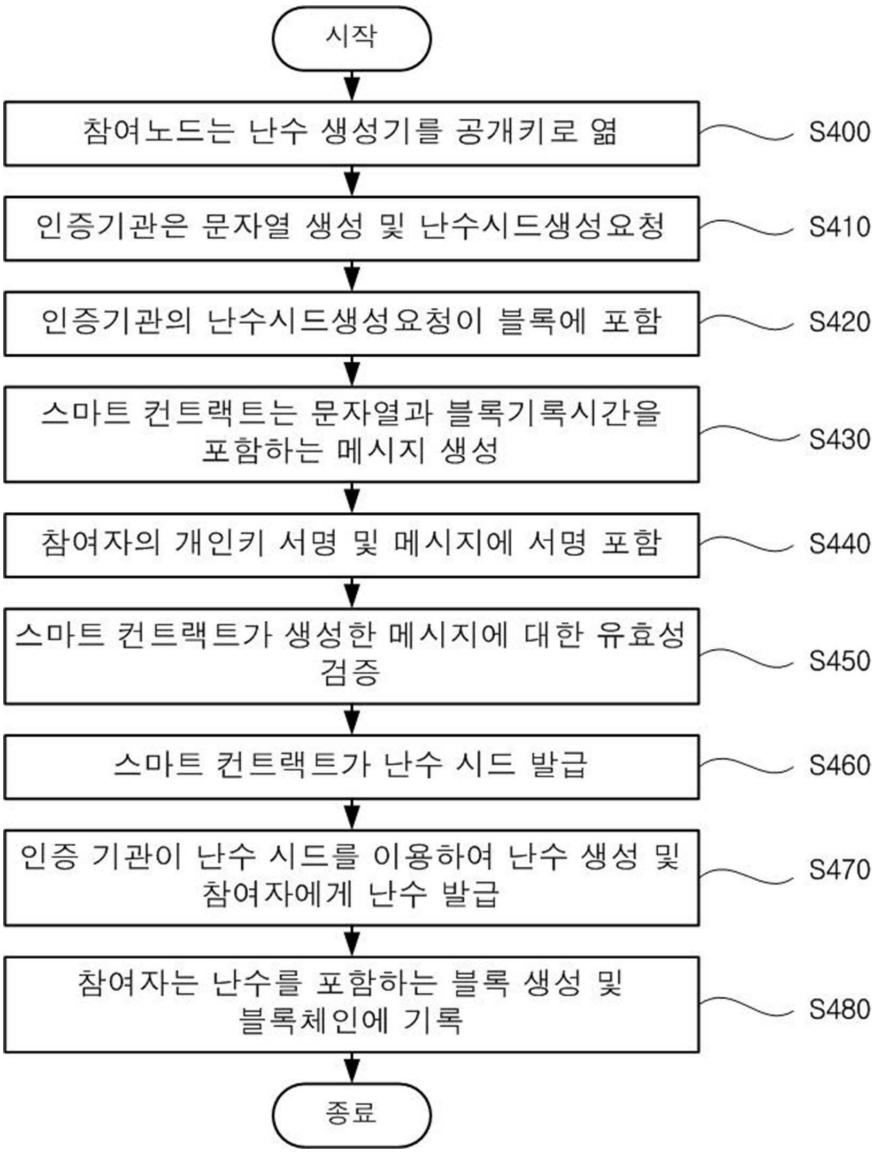
도면2


시작
프라이빗 블록체인 네트워크 구성
S200
이벤트 주최자가 스마트 컨트랙트 생성하여 블록체인에 기록
S210
회원 노드들이 스마트 컨트랙트를 통해 경품 선택 및 난수 생성기를 통해 난수 발급받아 블록체인에 기록하고 경품 추첨 이벤트에 응모
S220
아니오
사전 설정된 추첨 조건 만족?
S230
예
이벤트 주최자가 난수 생성기를 통해 추첨용 난수를 발급받음
S240
이벤트 주최자의 난수와 일치하는 난수를 갖는 회원을 이벤트 당첨자로 선정
S250
종료

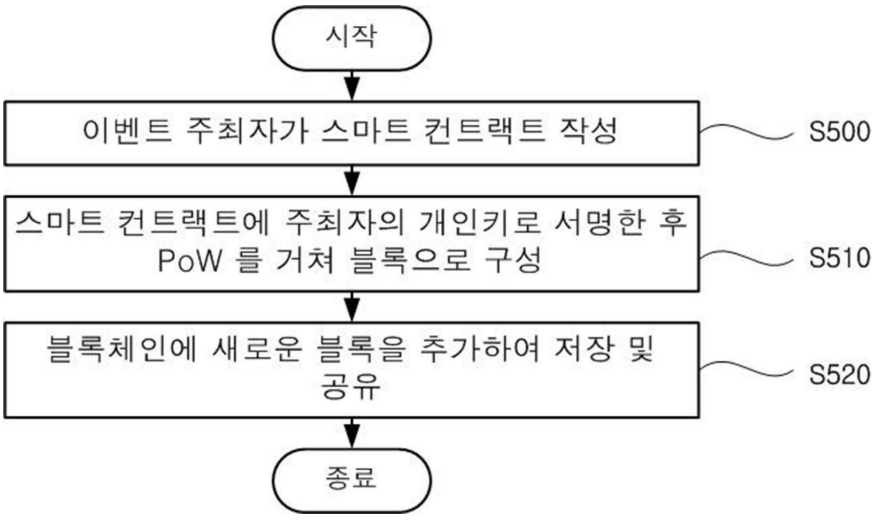
도면3


시작
이벤트 주최자가 자신의 정보를 인증기관에 제출
S300
인증기관이 이벤트 주최자의 정보 타당성 인증
S310
S320
신뢰성있는 업체인가?
아니오
예
이벤트 주최자가 응모권을 가진 회원을 프라이빗 블록체인 네트워크에 초대
S330
참가자는 인증기관에 개인정보 제출 및 인증요청
S340
인증기관이 해당 참가자의 정보 타당성 검증 및 인증
S350
신뢰성있는 개인인가?
아니오
예
해당 참가자에 대한 공개키 및 개인키 발급
S360
해당 참가자는 프라이빗 블록체인 네트워크의 노드로 참가
S370
참가 거부
종료

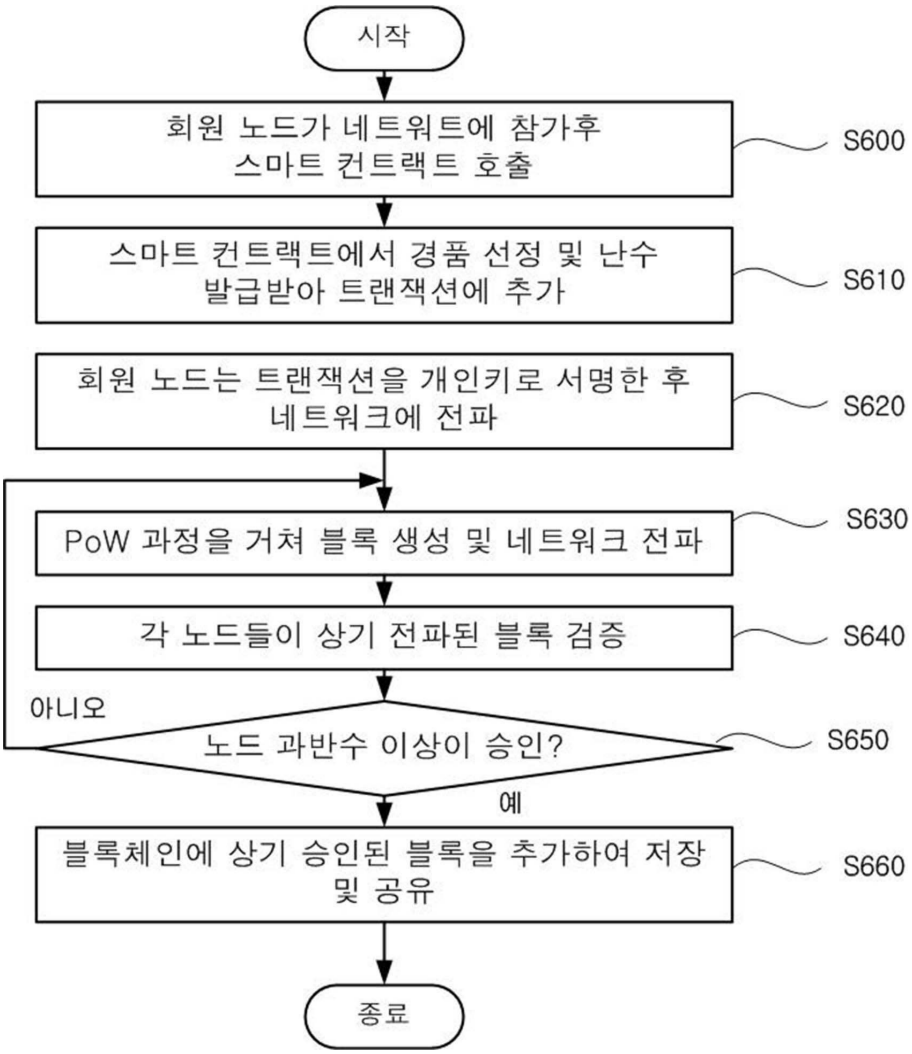
도면4


시작
참여노드는 난수 생성기를 공개키로 엶
S400
인증기관은 문자열 생성 및 난수시드생성요청
S410
인증기관의 난수시드생성요청이 블록에 포함
S420
스마트 컨트랙트는 문자열과 블록기록시간을 포함하는 메시지 생성
S430
참여자의 개인키 서명 및 메시지에 서명 포함
S440
스마트 컨트랙트가 생성한 메시지에 대한 유효성 검증
S450
스마트 컨트랙트가 난수 시드 발급
S460
인증 기관이 난수 시드를 이용하여 난수 생성 및 참여자에게 난수 발급
S470
참여자는 난수를 포함하는 블록 생성 및 블록체인에 기록
S480
종료

도면5


시작
이벤트 주최자가 스마트 컨트랙트 작성
S500
스마트 컨트랙트에 주최자의 개인키로 서명한 후 PoW 를 거쳐 블록으로 구성
S510
블록체인에 새로운 블록을 추가하여 저장 및 공유
S520
종료

도면6


시작
회원 노드가 네트워트에 참가후
스마트 컨트랙트 호출
S600
스마트 컨트랙트에서 경품 선정 및 난수
발급받아 트랜잭션에 추가
S610
회원 노드는 트랜잭션을 개인키로 서명한 후
네트워크에 전파
S620
PoW 과정을 거쳐 블록 생성 및 네트워크 전파
S630
각 노드들이 상기 전파된 블록 검증
S640
아니오
노드 과반수 이상이 승인?
S650
예
블록체인에 상기 승인된 블록을 추가하여 저장
및 공유
S660
종료