(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2023년04월24일
(11) 등록번호 10-2525157
(24) 등록일자 2023년04월19일

(51) 국제특허분류(Int. Cl.)
G06Q 50/34 (2012.01) *G07C 15/00* (2021.01)
(52) CPC특허분류
G06Q 50/34 (2013.01)
G07C 15/006 (2013.01)
(21) 출원번호 10-2017-0170038
(22) 출원일자 2017년12월12일
심사청구일자 2020년12월11일
(65) 공개번호 10-2019-0078668
(43) 공개일자 2019년07월05일
(56) 선행기술조사문헌
JP2017157910 A*
KR1020160150278 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
포항공과대학교 산학협력단
경상북도 포항시 남구 청암로 77 (지곡동)
(72) 발명자
박찬익
경상북도 포항시 남구 지곡로 155, 6동 1105호
조용래
울산광역시 북구 호계로 371, 101동 1310호
(74) 대리인
특허법인이상

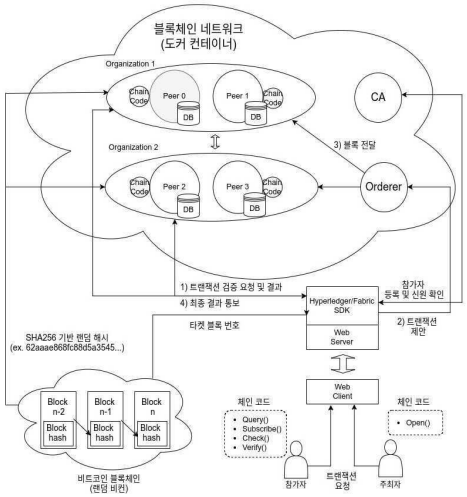
전체 청구항 수 : 총 16 항 심사관 : 황유진

(54) 발명의 명칭 **검증가능한 추첨을 위한 장치 및 방법**

(57) 요 약

추첨 시스템에 록체인(Blockchain)을 도입하여 참가자와 주최자 간의 신뢰 문제를 해결한 검증가능한 추첨을 위한 장치 및 방법이 개시된다.

대 표 도 - 도1



이 발명을 지원한 국가연구개발사업

과제고유번호	1711125876
과제번호	2020-0-00936-002
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기획평가원
연구사업명	블록체인융합기술개발(R&D)
연구과제명	5G 초저지연 서비스를 위한 무선 단말용 블록체인 기술 개발
기 여 율	30/100
과제수행기관명	포항공과대학교 산학협력단
연구기간	2021.01.01 ~ 2021.12.31

이 발명을 지원한 국가연구개발사업

과제고유번호	1711193875
과제번호	2021-0-00484-003
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기획평가원
연구사업명	데이터경제를위한블록체인기술개발(R&D)
연구과제명	노드 간 메시지 전달과 합의를 위한 최적 경로 네트워크 프로토콜 기술개발
기 여 율	30/100
과제수행기관명	포항공과대학교 산학협력단
연구기간	2023.01.01 ~ 2023.12.31

이 발명을 지원한 국가연구개발사업

과제고유번호	1711193306
과제번호	2018-0-01441-006
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기획평가원
연구사업명	정보통신방송혁신인재양성
연구과제명	크로스 도메인 호환성을 위한 블록체인 플랫폼 및 비즈모델 개발
기 여 율	40/100
과제수행기관명	포항공과대학교 산학협력단
연구기간	2023.01.01 ~ 2023.12.31

명 세 서

청구범위

청구항 1

블록체인 네트워크 내 스마트 컨트랙트의 동작에 의해 참가자 및 주최자 간의 검증 가능한 추첨을 수행하는 방법에 있어서,

상기 블록체인 네트워크에 의하여 실행되는 Open 트랜잭션에 의해 상기 스마트 컨트랙트를 호출하여 주최자로부터 입력된 추첨 행사의 추첨 정보를 추첨 네트워크 상에 등록하는 단계;

상기 블록체인 네트워크에 의하여 실행되는 Subscribe 트랜잭션에 의해 상기 스마트 컨트랙트를 호출하여 참가자를 상기 추첨 행사의 참가자 목록에 추가하는 단계;

상기 블록체인 네트워크에 의하여 실행되는 Check 트랜잭션에 의해 상기 스마트 컨트랙트를 호출하여, 현재 시간이 발표일에 도달한 경우 사전 발행된 타겟 블록의 해시 값을 랜덤 소스로 사용하는 당첨자 결정 알고리즘에 의해 당첨자 및 당첨 결과를 도출하는 단계;

상기 블록체인 네트워크에 의하여 실행되는 상기 Check 트랜잭션에 의해 상기 당첨자를 상기 추첨 행사의 당첨자 필드에 기록하는 단계;

상기 블록체인 네트워크에 의하여 실행되는 상기 Check 트랜잭션에 의해 상기 추첨 정보의 무결성을 검증하기 위한 제1 검증 키를 생성하는 단계; 및

상기 블록체인 네트워크에 의하여 실행되는 Verify 트랜잭션에 의해 상기 스마트 컨트랙트를 호출하여, 상기 추첨 네트워크 상에 등록된 상기 추첨 정보를 이용하여 제2 검증 키를 생성하고, 상기 제2 검증 키를 상기 제1 검증 키와 비교함으로써 상기 당첨 결과의 무결성을 검증하는 단계를 포함하는, 검증 가능한 추첨을 위한 방법.

청구항 2

청구항 1에 있어서,

상기 추첨 행사의 추첨 정보를 추첨 네트워크 상에 등록하는 단계에서는,

상기 추첨 행사의 이름, 발행일, 마감일, 상기 발표일, 타겟 블록 번호, 참가자 수, 당첨자 수, 랜덤 키 및 참가자 이름 중 적어도 하나의 상기 추첨 정보를 상기 추첨 네트워크 상에 등록하는 것을 포함하되,

상기 타겟 블록 번호는 비트 코인 블록 체인의 블록 생성 속도를 산출하여 상기 발표일에 인접한 타겟 블록의 번호를 예측한 것이고,

상기 랜덤 키는 적어도 하나의 추첨 행사를 구별하기 위한 것인, 검증 가능한 추첨을 위한 방법.

청구항 3

청구항 1에 있어서,

상기 추첨 행사의 참가자 목록에 추가하는 단계는,

상기 추첨 네트워크 상에 등록된 참가자를 CA 데이터 베이스에 등록하는 단계;

상기 CA 데이터 베이스로부터 공개 키를 할당 받는 단계; 및

상기 공개 키에 따른 해시 값을 통해 상기 참가자들의 신원을 확인하여 구분하는 단계를 포함하는, 검증 가능한 추첨을 위한 방법.

청구항 4

삭제

청구항 5

청구항 1에 있어서,

상기 당첨자 결정 알고리즘은,

참가자에게 개별 부여된 각 정수마다 랜덤 해시 값을 할당하고,

상기 랜덤 해시 값을 기준으로 상기 정수를 재정렬하여, 재정렬된 순서에 따라 당첨자를 결정하는, 검증 가능한 추첨을 위한 방법.

청구항 6

청구항 5에 있어서,

상기 랜덤 해시 값은,

랜덤 키 및 상기 타겟 블록의 해시 값을 SHA256-HMAC의 키와 데이터로 사용하여 임시 값을 산출하고,

상기 임시 값을 문자열로 변환한 후 상기 문자열의 끝에 정수 인덱스를 결합한 값을 SHA256의 입력으로 사용하여 산출된 해시 값인, 검증 가능한 추첨을 위한 방법.

청구항 7

청구항 1에 있어서,

상기 제1 검증 키는,

상기 타겟 블록 및 상기 타겟 블록의 직전 블록들의 해시 값 및 랜덤 키를 HMAC 함수로 만든 값 및 추첨 정보를 SHA256 함수로 만든 해시 값을 결합하여 생성된 것인, 검증 가능한 추첨을 위한 방법.

청구항 8

청구항 7에 있어서,

상기 제2 검증 키는,

상기 추첨 네트워크 상에 등록된 상기 추첨 정보를 바탕으로, 상기 제1 검증 키와 동일하게 산출되는, 검증 가능한 추첨을 위한 방법.

청구항 9

청구항 1에 있어서,

상기 블록체인 네트워크는 허가형 블록체인(Permissioned Blockchain)인, 검증 가능한 추첨을 위한 방법.

청구항 10

블록체인 네트워크 내 스마트 컨트랙트의 동작에 의해 참가자 및 주최자 간의 검증 가능한 추첨을 수행하는 장치에 있어서,

상기 스마트 컨트랙트를 호출하는 적어도 하나의 트랜잭션 명령을 저장하는 메모리(memory); 및

상기 메모리에 저장된 적어도 하나의 트랜잭션 명령을 실행하는 프로세서(processor)를 포함하되,

상기 적어도 하나의 트랜잭션 명령은,

주최자로부터 입력된 추첨 행사의 추첨 정보를 추첨 네트워크 상에 등록하도록 하는 명령,

참가자를 상기 추첨 행사의 참가자 목록에 추가하도록 하는 명령,

현재 시간이 발표일에 도달한 경우, 사전 발행된 타겟 블록의 해시 값을 랜덤 소스로 사용하는 당첨자 결정 알고리즘을 실행함으로써 당첨자 및 당첨 결과를 도출하도록 하는 명령,

상기 당첨자를 상기 추첨 행사의 당첨자 필드에 기록하도록 하는 명령,

상기 추첨 정보의 무결성을 검증하기 위한 제1 검증 키를 생성하도록 하는 명령, 및

상기 추첨 네트워크 상에 등록된 상기 추첨 정보를 이용하여 제2 검증 키를 생성하고, 상기 제2 검증 키를 상기

제1 검증 키와 비교함으로써 상기 당첨 결과의 무결성을 검증하도록 하는 명령을 포함하는, 검증 가능한 추첨을 위한 장치.

청구항 11

청구항 10에 있어서,

상기 추첨 행사의 추첨 정보를 추첨 네트워크 상에 등록하도록 하는 명령에서는,

상기 추첨 행사의 이름, 발행일, 마감일, 상기 발표일, 타겟 블록 번호, 참가자 수, 당첨자 수, 랜덤 키 및 참가자 이름 중 적어도 하나의 상기 추첨 정보를 상기 추첨 네트워크 상에 등록하는 것을 포함하되,

상기 타겟 블록 번호는 비트 코인 블록 체인의 블록 생성 속도를 산출하여 상기 발표일에 인접한 타겟 블록의 번호를 예측한 것이고,

상기 랜덤 키는 적어도 하나의 추첨 행사를 구별하기 위한 것인, 검증 가능한 추첨을 위한 장치.

청구항 12

청구항 10에 있어서,

상기 추첨 행사의 참가자 목록에 추가하도록 하는 명령은,

상기 추첨 네트워크 상에 등록된 참가자를 CA 데이터 베이스에 등록하도록 하는 명령,

상기 CA 데이터 베이스로부터 공개 키를 할당 받도록 하는 명령, 및

상기 공개 키에 따른 해시 값을 통해 상기 참가자들의 신원을 확인하여 구분하도록 하는 명령을 포함하는, 검증 가능한 추첨을 위한 장치.

청구항 13

삭제

청구항 14

청구항 10에 있어서,

상기 당첨자 결정 알고리즘은,

참가자에게 개별 부여된 각 정수마다 랜덤 해시 값을 할당하고,

상기 랜덤 해시 값을 기준으로 상기 정수를 재정렬하여, 재정렬된 순서에 따라 당첨자를 결정하는, 검증 가능한 추첨을 위한 장치.

청구항 15

청구항 14에 있어서,

상기 랜덤 해시 값은,

랜덤 키 및 상기 타겟 블록의 해시 값을 SHA256-HMAC의 키와 데이터로 사용하여 임시 값을 산출하고,

상기 임시 값을 문자열로 변환한 후 상기 문자열의 끝에 정수 인덱스를 결합한 값을 SHA256의 입력으로 사용하여 산출된 해시 값인, 검증 가능한 추첨을 위한 장치.

청구항 16

청구항 10에 있어서,

상기 제1 검증 키는,

상기 타겟 블록 및 상기 타겟 블록의 직전 블록들의 해시 값 및 랜덤 키를 HMAC 함수로 만든 값 및 추첨 정보를 SHA256 함수로 만든 해시 값을 결합하여 생성된 것인, 검증 가능한 추첨을 위한 장치.

청구항 17

청구항 16에 있어서,

상기 제2 검증 키는,

상기 추첨 네트워크 상에 등록된 상기 추첨 정보를 바탕으로, 상기 제1 검증 키와 동일하게 산출되는, 검증 가능한 추첨을 위한 장치.

청구항 18

청구항 10에 있어서,

상기 블록체인 네트워크는 허가형 블록체인(Permissioned Blockchain)인, 검증 가능한 추첨을 위한 장치.

발명의 설명

기 술 분 야

[0001] 본 발명은 추첨 시스템에서 참가자와 주최자간의 신뢰 문제를 블록체인(Blockchain)을 도입하여 해결한 것으로, 추첨을 위한 컴퓨터 소프트웨어 장치 및 방법에 관한 것이다.

배 경 기 술

[0002] 기존의 추첨 프로그램은 중앙 집중식(Centralized) 을 따라 구현되어 단일한 컴퓨터에서 실행된다. 추첨 실행시 사용되는 랜덤 값이 가지는 불규칙성에 따라서 추첨 시스템의 공평성이 결정되며, 모든 정보들이 중앙 집중되고 관리자 권한을 가지는 경우 모든 정보를 임의로 수정 가능하므로 이는 추첨 시스템의 신뢰성 문제를 제기한다. 랜덤 값의 불규칙성을 보장받는 기술은 대부분 미국 NIST 에서 제공하는 공공 랜덤 서비스 비콘을 사용하여 대응할 수 있으나, 중앙 집중 서버 관리자에 전적으로 의존해야 하는 문제는 여전히 해결하지 못하고 있다. 이러한 관리자 권한 문제를 해결하기 위해, 누구나 추첨 결과에 대해서 검증할 수 있게 하는 기법을 고안하는 것이 필요하다. 즉, 랜덤 값의 불규칙성은 그대로 유지하면서도, 향후 누구나 예상하고 동의하는 시점에 생성되는 랜덤 값을 사용하는 추첨시스템을 구성함으로써, 추첨 시스템의 공평성을 지원하면서도 추첨 결과에 대한 검증이 가능하게 구성한다.

[0003] 비트코인 블록체인은 기본적으로 전세계 분포되어 있는 블록 마이너 노드들이 경쟁적으로 암호학적 해쉬 퍼즐을 풀고 이를 통해 블록들 간의 체인을 구성하고 있다. 이러한 블록체인 구성을 위해 진행되는 암호학적 해쉬 퍼즐을 푸는 과정에는 기본적으로 많은 불규칙성에 기반한 과정이 내포되어 있으며, 매번 블록 마이너들이 블록을 생성할 때 마다 새로운 랜덤 값을 생성하는 것과 유사하다. 이러한 특징을 활용하면서, 추첨 시스템 동작 자체를 스마트 컨트랙트라고 불리는 블록체인상 실행되는 프로그램으로 구성함으로써 블록체인 기반 검증 가능한 추첨시스템을 구성할 수 있다.

[0004] 블록체인의 형태는 공개 블록체인, 허가형 블록체인, 그리고 컨소시움 블록체인 등으로 구별되며, 본 발명에서는 특정 형태의 블록체인을 가정하지 않지만, 설명의 편의성을 위해 허가형 블록체인 상황을 가정하고 서술한다.

[0005] 리눅스 재단(Linux foundation) 산하의 오픈 소스(open source) 블록체인 플랫폼인 하이퍼레저 패브릭(Hyperledger Fabric)은 허가형 블록체인(permissioned Blockchain)을 사용하여 기업들간의 투명한 거래를 가능하게 한다.

발명의 내용

해결하려는 과제

[0006] 기존의 중앙 집중식으로 구현된 추첨 시스템은 신뢰성 문제를 포함하고 있으며, 이러한 추첨 시스템은 다음 3가지 주요한 문제를 가지고 있다.

[0007] * 예측가능성(Predictability)

[0008] * 조작성(Modifiability)

[0009] * 정보의 비공개성(Information hiding)

[0010] 예측 가능성은 당첨자를 사전에 미리 예측할 수 있을 경우를 의미하고, 조작성은 추첨과 관련된 정보를 임의로 수정할 수 있음을 나타내며, 정보의 비공개성은 추첨과 관련된 정보를 참가자에 공개하지 않음을 뜻한다.

[0011] 이를 해결하기 위해 본 발명에서는 신뢰성 있는 추첨 시스템 장치 및 방법을 고안하였으며, 이 발명은 추첨시스템이 공평성(fairness), 불변성(immutability), 투명성(transparency), 검증가능성(verifiability) 속성을 가지도록 지원함으로써 기존 추첨시스템이 가지고 있는 3가지 주요 문제들을 해결한다.

[0012] 공평성은 사전에 당첨자를 예측할 수 없음을 의미하고, 불변성은 한 번 기록된 추첨 정보는 이후의 임의적 수정이 불가능함을 나타내며, 투명성은 추첨과 관련된 정보가 참가자들에 공개되어야 함을 뜻한다. 그리고 검증가능성은 추첨 시스템이 위와 같은 속성을 만족시키는지 검증이 가능해야 함을 뜻한다.

[0013] 본 발명은 이를 반영하여, 기존의 중앙 집중식으로 구현된 추첨 프로그램을 블록체인 플랫폼을 사용하여 구현함으로써, 공정성, 불변성, 투명성, 검증가능성 속성을 갖는 신뢰할 수 있는 추첨 프로그램을 개발하는 것이다. 보다 자세하게는, 추첨 서비스를 제공하는 블록체인 기반의 신뢰할 수 있는 추첨 프로그램을 개발하는 것과 관련된다.

과제의 해결 수단

[0014] 본 발명은 블록체인 플랫폼을 사용하여, 공평성, 불변성, 투명성, 검증가능성 속성을 갖는 신뢰성 있는 추첨 장치 및 방안을 제안한다.

[0015] 본 발명에서 공평성의 실현을 위해 사용한 랜덤 값은 2가지로 구분 된다. 미래에 생성될 비트 코인 블록 체인의 블록 해시와 암호학적으로 안전한 유사 난수 생성기(cryptographically secure pseudo random number generator)에 의해 생성된 랜덤 값이다. 이 둘을 조합한 값을 바탕으로 당첨자가 결정된다.

[0016] 투명성과 불변성은 블록체인으로 구현된 분산 복제 장부(distributed replicated ledger)에 의해 실현된다. 추첨과 관련된 트랜잭션들은 분산되어 있는 피어 노드들에 기록됨으로써 투명성이 확보되고, 블록 체인 형식으로 저장되기 때문에 불변성이 확보된다.

[0017] 본 발명에서 제안한 추첨 시스템의 결과 검증은 분산된 환경에서 동작하는 피어 노드들이 실행하는 스마트 컨트랙트와 관련된다. 각 피어 노드들에서 독립적으로 실행되는 스마트 컨트랙트는 당첨자가 결정될 당시의 생성된 검증 키를 다시 만들고 이를 비교함으로써 추첨 결과를 검증한다.

[0018] 스마트 컨트랙트(Smart contract)는 분산 복제 장부(Distributed replicated ledger)와의 입/출력을 수행하는 프로그램이다. 본 발명에서 사용한 하이퍼레저 패브릭에서는 이를 체인코드(Chain code)라 부르기도 한다.

[0019] 참가자를 CA에 의해 할당 받은 공개 키의 해시로 구분하여 참가자들의 익명성을 보장하는 기법을 제공한다.

[0020] 본 발명은 블록체인을 도입하여 기존의 중앙 집중식이 아닌 탈 집중화(Decentralized) 된 방식의 추첨 시스템을 제안하여 신뢰성 문제를 해결한다.

[0021] 리눅스 재단(Linux foundation) 산하의 오픈 소스 블록체인 플랫폼인 하이퍼레저 패브릭(Hyperledger Fabric)을 사용하여 추첨과 관련된 서비스를 제공하는 웹 기반의 프로그램을 제공한다.

발명의 효과

[0022] 본 발명은 신뢰할 수 있는 추첨 시스템을 제시하고 이를 블록체인을 도입함으로써 부정직한 추첨 행사로 인한 사회적 비용을 줄일 수 있다.

[0023] 기존의 중앙 집중식을 따르는 추첨 시스템을 신뢰할 수 있도록 만드는 기법들이 제시가 되었지만 여전히 단일 장애점 문제(single point of failure) 등의 문제가 있고 이들은 구현을 복잡하고 어렵게 만든다. 하지만 블록체인 플랫폼을 사용하면 신뢰성 문제가 쉽게 해결되고 효율적인 구현이 가능하다.

도면의 간단한 설명

[0024] 도1 은 본 발명에서 제안된 전체 시스템 구조도이다.

도 2는 시간 순에 따른 추첨 행사의 상태 변화와 가용한 체인 코드(스마트 컨트랙트) 개념도이다.

도 3은 검증을 위해 사용되는 검증 키 도출 과정의 블록 구성도이다.

발명을 실시하기 위한 구체적인 내용

[0025] 본 발명은 다양한 변경을 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 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다. 각 도면을 설명하면서 유사한 참조부호를 유사한 구성요소에 대해 사용하였다.

[0026] 제1, 제2, A, B 등의 용어는 다양한 구성요소들을 설명하는 데 사용될 수 있지만, 상기 구성요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 사용된다. 예를 들어, 본 발명의 권리 범위를 벗어나지 않으면서 제1 구성요소는 제2 구성요소로 명명될 수 있고, 유사하게 제2 구성요소도 제1 구성요소로 명명될 수 있다. "및/또는"이라는 용어는 복수의 관련된 기재된 항목들의 조합 또는 복수의 관련된 기재된 항목들 중의 어느 항목을 포함한다.

[0027] 어떤 구성요소가 다른 구성요소에 "연결되어" 있다거나 "접속되어" 있다고 언급된 때에는, 그 다른 구성요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성요소가 존재할 수도 있다고 이해되어야 할 것이다. 반면에, 어떤 구성요소가 다른 구성요소에 "직접 연결되어" 있다거나 "직접 접속되어" 있다고 언급된 때에는, 중간에 다른 구성요소가 존재하지 않는 것으로 이해되어야 할 것이다.

[0028] 본 출원에서 사용한 용어는 단지 특정한 실시예를 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 출원에서, "포함하다" 또는 "가지다" 등의 용어는 명세서상에 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.

[0029] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가지고 있다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥 상 가지는 의미와 일치하는 의미를 가지는 것으로 해석되어야 하며, 본 출원에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[0030] 이하, 첨부한 도면들을 참조하여, 본 발명의 바람직한 실시예를 보다 상세하게 설명하고자 한다. 본 발명을 설명함에 있어 전체적인 이해를 용이하게 하기 위하여 도면상의 동일한 구성요소에 대해서는 동일한 참조부호를 사용하고 동일한 구성요소에 대해서 중복된 설명은 생략한다. 이하, 본 발명에 따른 바람직한 실시예를 첨부된 도면을 참조하여 상세하게 설명한다.

[0032] 도 1은 본 발명에서 제안된 전체 시스템 구조도이다.

[0033] 도 1에서, 블록 체인 네트워크는 도커 기반의 컨테이너 형태로 구현이 되어 있고 두 개의 조직과 각 조직 당 두 개의 피어로 구성된다. 피어(Peer)는 트랜잭션을 스마트 컨트랙트 형식(체인코드)으로 실행하고 그에 대한 기록을 블록체인에 기록한다. 체인 코드 역시 독립된 컨테이너로 구현되어 있으며 피어 노드에 의해 실행된다. DB는 couchDB를 사용하였으며 분산 데이터 베이스의 일종인 블록 체인을 저장하고 관리하는 역할을 한다. 오더러(Orderer)는 웹 서버(SDK)로부터 요청 받은 트랜잭션에 순서를 정하고 블록을 형성하여 피어 노드에 전달한다. 하이퍼레저 패브릭에서의 CA(Certificate Authority)는 블록 체인 네트워크를 이루는 구성 요소들의 신원을 관리한다. 그리고 추첨을 위한 참가자들의 신원 역시 CA에 의해 관리된다.

[0034] 웹 서버 및 하이퍼레저/패브릭 SDK(Software development kit)는 사용자(웹 클라이언트)와 블록 체인 네트워크와의 상호작용을 수행한다. 즉, 사용자의 요청을 받으면 구현된 프로토콜을 따라 블록 체인 네트워크의 구성 노드들에 전달하고 그 결과를 사용자에게 알려준다. 또한 비트 코인 기반의 랜덤 비콘으로부터 랜덤 소스로 사용할 타겟 블록 번호를 가져오는 역할도 수행한다.

[0035] 웹 클라이언트 및 사용자는 실 사용자에 따라 참여자와 주최자로 구분된다. 이들이 수행할 수 있는 트랜잭션의 종류는 다음과 같이 다섯 가지로 구분된다. 참여자는 추첨 행사 목록을 조회할 수 있는 query 트랜잭션, 추첨 행사에 대한 참여를 실행하는 subscribe 트랜잭션, 추첨 결과(당첨자 결정)를 확인하는 check 트랜잭션, 추첨 검증을 수행하는 verify 트랜잭션으로 구성된다. 주최자는 open 트랜잭션을 통해 추첨 행사를 등록할 수 있다.

위 트랜잭션들은 모두 블록 체인 네트워크에서 스마트 컨트랙트 형식으로 구현된다.

[0036] 비트코인 블록체인은 랜덤 수치를 제공하는 비콘으로서의 기능을 수행한다. 비트코인의 블록들은 각 이전 블록의 해시를 갖고 있고 해시 값은 해시 특성 상 예측하기가 거의 불가능하다. 따라서 당첨자를 결정하기 위한 알고리즘은 아직 형성되지 않은 미래의 블록의 해시를 랜덤 소스로 사용한다.

[0038] 도 2는 시간 순에 따른 추첨 행사의 상태 변화와 가용한 체인 코드(스마트 컨트랙트) 개념도이다.

[0039] 도 2 는 추첨 행사의 시간 순에 따른 상태 변화와 가용한 체인 코드 연산을나타낸다.

[0040] 추첨 행사는 시간적으로 발행일 (Issue date), 마감일 (Due date), 그리고 발표일(Announce date)로 나뉜다. 발행일은 추첨 행사를 일으킨 날이다. 발행일과 마감일 사이에 참여자들은 등록된 행사에 참여할 수 있다. 그리고 발표일 이후에 결과를 확인하고 검증할 수 있다. 체인코드 연산 중 하나인 query는 시간 순에 상관 없이 언제든 호출가능하기 때문에 그림에서 생략하였다.

[0041] open 트랜잭션은 추첨 행사를 등록한다. 입력으로 행사 이름, 발행일, 마감일, 발표일, 타겟 블록 번호, 참여 멤버 수, 우승자 수, 랜덤 키, 멤버 이름을 받아 요청된 행사를 추첨 네트워크에 등록시킨다. 타겟 블록 번호는 비트 코인 블록 체인의 최근 블록 생성 속도를 계산하여 발표일에 인접한 블록 번호를 예측하여 선택된다. 랜덤 키는 각 행사를 구별하기 위한 고유 번호를 제공한다.

[0042] subscribe 트랜잭션은 참가자를 선택된 추첨 행사의 참가자 목록에 추가한다. subscribe 트랜잭션은 또한 관련된 체인 코드를 호출하기 전에 등록한 참가자를 CA의 데이터 베이스에 등록하고 CA로부터 공개 키를 할당 받는다. 그리고 공개 키의 해시 값을 통해 참가자를 구분한다. 해시 함수의 단방향(one-way) 특성에 의해 역변환이 불가능하므로 익명성이 보장 되고, 결과가 나왔을 경우 당첨자는 안전하게 당첨된 사실을 증명할 수 있다.

[0043] check 트랜잭션은 현재 시간이 발표일이 되었을 때 호출 가능하며, 당첨자를 결정하는 체인코드를 호출한다. check 트랜잭션이 호출될 때에는 반드시 랜덤 소스로 사용될 타겟 블록이 발행이 되어야 한다. 그렇지 않을 경우에는 실패한다. 타겟 블록이 발행이 되었다면, 해당 블록의 해시 값을 읽어와 이를 랜덤 소스를 사용한 당첨자 결정 알고리즘을 호출한다. 당첨자 결정 알고리즘은 랜덤 소스가 정해지면 결정적인(Deterministic) 방식으로 동작한다. 본 구현에서는 다음과 당첨자가 결정된다.

[0044] 1. [0, 1, ... , 참가자 수 - 1] 에 속한 각 정수에 랜덤 해시 값(X_i)을 할당한다. (키, 값) 쌍에서 키가 정수에 해당하고, 값이 해시에 해당한다.

[0045] 2. 1의 X_i 는 다음과 같이 계산된다. 추첨 행사 등록 시 할당된 랜덤 키와 타겟 블록 해시를 각 SHA256-HMAC의 키와 데이터로 사용하여 계산된 값을 Y라 하자. Y를 문자열로 변환한 값의 마지막에 정수 값의 인덱스(i)를 이어 붙인(concatenated) 값을 SHA256의 입력으로 사용하여 계산된 해시 값이 X_i 에 할당된다.

[0046] 3. 할당된 (해시) 값을 기준으로 정렬한다. 그리고 그 결과를 배열에 저장한다.

[0047] 4. 배열의 인덱스 순서 번호로 당첨자 순위를 가려낸다. 예를 들어 당첨자 수가 2명일 경우, 첫번째 인덱스 번호가 1등, 두번째 인덱스 번호가 2등이 된다.

[0048] 5. 참가자들은 초기에 참가한 순서대로 번호가 할당된다.

[0049] 위 방식으로 당첨자가 결정되면 스마트 컨트랙트는 추첨 행사의 당첨자 필드에 당첨자를 기록한다.

[0050] check 트랜잭션은 또한 추후 검증을 위한 검증 키를 생성한다.

[0052] 도 3은 검증을 위해 사용되는 검증 키 도출 과정의 블록 구성도이다.

[0053] 도 3을 참조하면, 랜덤 소스와 추첨 정보의 무결성을 위해 타겟 블록과 직전 3개 블록의 해시 값과 추첨 등록 당시 제공된 랜덤 키를 HMAC 함수로 만든 값과 추첨 정보를 SHA256 함수로 만든 해시 값을 이어 붙인(concatenated) 값에 대한 해시를 만들어낸다. 그리고 이렇게 생성된 검증 키(VerifiableRandomKey)는 추첨 정보의 검증 키 필드에 기록되고 verify 트랜잭션에 의해 사용된다.

[0054] verify 트랜잭션은 기록된 추첨 정보의 무결성과 추첨 결과를 재현하여 당첨자가 일치하는지 여부를 검증한다.

[0055] 도 3의 검증 키 도출 과정을 따라 검증 키를 생성하고 check 트랜잭션으로 기록된 검증 키를 비교한다.

[0056] 검증 키는 최종적으로 HMAC과 SHA256의 결과 문자열을 연결하여 구성됨. HMAC의 키로는 초기의 랜덤 키를 사용

하고, 해시 함수는 SHA256, 메시지로 사용될 데이터는 타겟 블록과 직전 3개 해시일 수 있다. Lottery information에 속하는 내용은 추첨 행사의 이름, 행사 등록 시 사용된 랜덤 키, 발행일, 마감일, 등록일, 당첨자 수, 당첨자 명단, 참가자 수, 참가자 명단, 타겟 블록 번호, 당첨자 결정 알고리즘의 소스 코드가 포함된다.

[0058] 본 발명의 실시예에 따른 방법의 동작은 컴퓨터로 읽을 수 있는 기록매체에 컴퓨터가 읽을 수 있는 프로그램 또는 코드로서 구현하는 것이 가능하다. 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 시스템에 의해 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록장치를 포함한다. 또한 컴퓨터가 읽을 수 있는 기록매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어 분산 방식으로 컴퓨터로 읽을 수 있는 프로그램 또는 코드가 저장되고 실행될 수 있다.

[0059] 또한, 컴퓨터가 읽을 수 있는 기록매체는 롬(rom), 램(ram), 플래시 메모리(flash memory) 등과 같이 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치를 포함할 수 있다. 프로그램 명령은 컴파일러(compiler)에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터(interpreter) 등을 사용해서 컴퓨터에 의해 실행될 수 있는 고급 언어 코드를 포함할 수 있다.

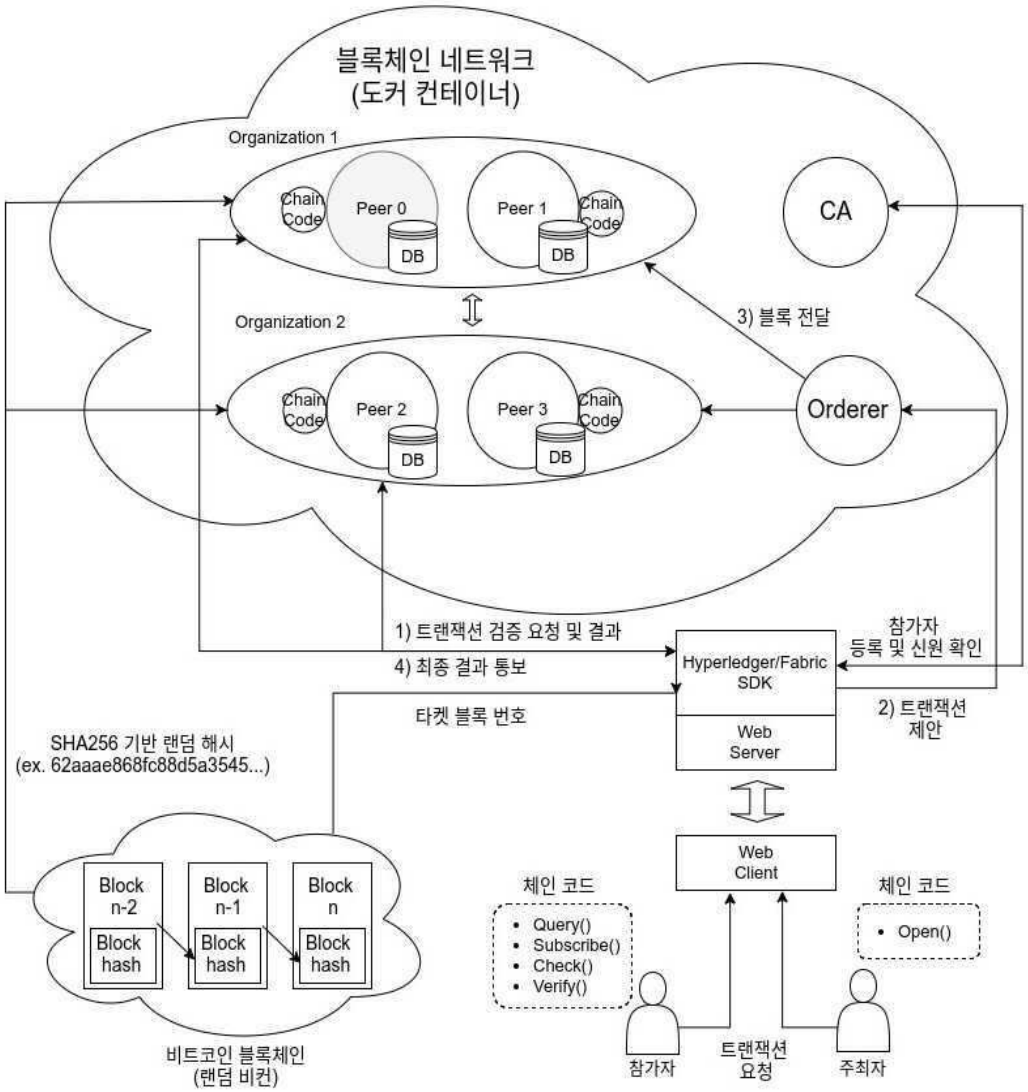
[0060] 본 발명의 일부 측면들은 장치의 문맥에서 설명되었으나, 그것은 상응하는 방법에 따른 설명 또한 나타낼 수 있고, 여기서 블록 또는 장치는 방법 단계 또는 방법 단계의 특징에 상응한다. 유사하게, 방법의 문맥에서 설명된 측면들은 또한 상응하는 블록 또는 아이템 또는 상응하는 장치의 특징으로 나타낼 수 있다. 방법 단계들의 몇몇 또는 전부는 예를 들어, 마이크로프로세서, 프로그램 가능한 컴퓨터 또는 전자 회로와 같은 하드웨어 장치에 의해(또는 이용하여) 수행될 수 있다. 몇몇의 실시예에서, 가장 중요한 방법 단계들의 하나 이상은 이와 같은 장치에 의해 수행될 수 있다.

[0061] 실시예들에서, 프로그램 가능한 로직 장치(예를 들어, 필드 프로그머블 게이트 어레이)가 여기서 설명된 방법들의 기능의 일부 또는 전부를 수행하기 위해 사용될 수 있다. 실시예들에서, 필드 프로그머블 게이트 어레이는 여기서 설명된 방법들 중 하나를 수행하기 위한 마이크로프로세서와 함께 작동할 수 있다. 일반적으로, 방법들은 어떤 하드웨어 장치에 의해 수행되는 것이 바람직하다.

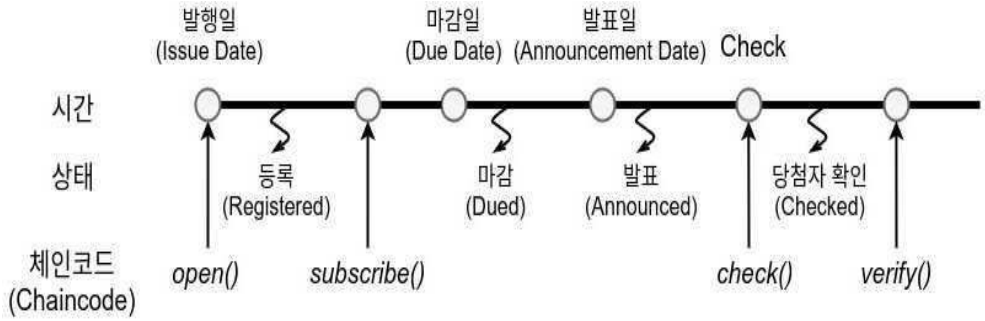
[0062] 이상 본 발명의 바람직한 실시예를 참조하여 설명하였지만, 해당 기술 분야의 숙련된 당업자는 하기의 특허 청구의 범위에 기재된 본 발명의 사상 및 영역으로부터 벗어나지 않는 범위 내에서 본 발명을 다양하게 수정 및 변경시킬 수 있음을 이해할 수 있을 것이다.

도면

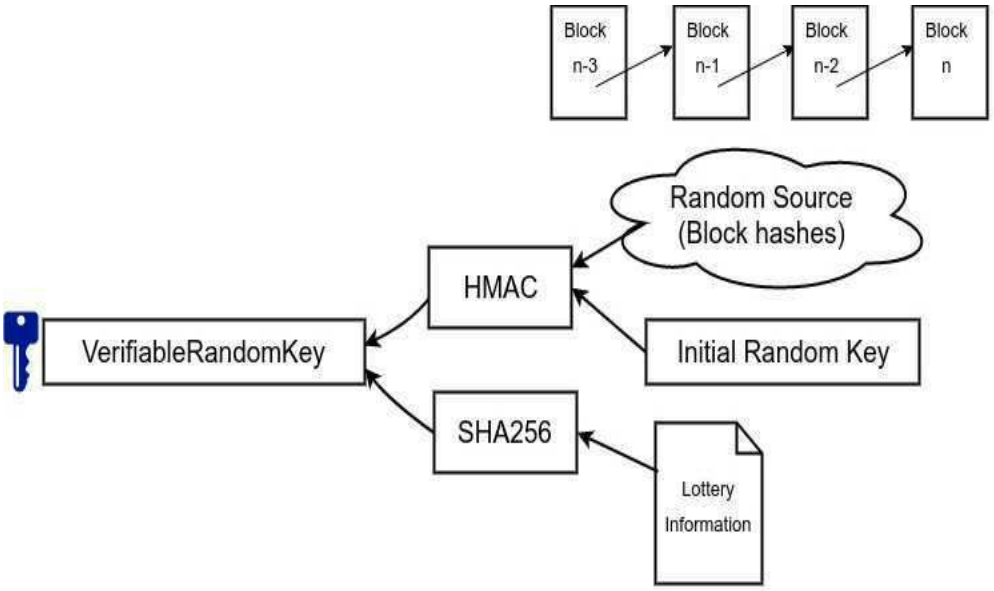
도면1


블록체인 네트워크
(도커 컨테이너)
Organization 1
Chain Code
Peer 0
DB
Peer 1
Chain Code
DB
CA
Organization 2
3) 블록 전달
Chain Code
Peer 2
DB
Peer 3
Chain Code
DB
Orderer
1) 트랜잭션 검증 요청 및 결과
4) 최종 결과 통보
참가자
등록 및 신원 확인
Hyperledger/Fabric SDK
Web Server
2) 트랜잭션 제안
타켓 블록 번호
SHA256 기반 랜덤 해시
(ex. 62aaae868fc88d5a3545...)
Block n-2
Block hash
Block n-1
Block hash
Block n
Block hash
Web Client
체인 코드
Query()
Subscribe()
Check()
Verify()
체인 코드
Open()
참가자
트랜잭션 요청
주최자
비트코인 블록체인
(랜덤 비컨)

도면2


발행일
(Issue Date)
마감일
(Due Date)
발표일
(Announcement Date)
Check
시간
상태
등록
(Registered)
마감
(Dued)
발표
(Announced)
당첨자 확인
(Checked)
체인코드
(Chaincode)
open()
subscribe()
check()
verify()

도면3


Block
n-3
Block
n-1
Block
n-2
Block
n
Random Source
(Block hashes)
HMAC
VerifiableRandomKey
Initial Random Key
SHA256
Lottery
Information