(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2020-0096241
(43) 공개일자 2020년08월11일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *H04L 9/30* (2006.01)
(52) CPC특허분류
H04L 9/3247 (2013.01)
H04L 9/3066 (2013.01)
(21) 출원번호 10-2020-7017368
(22) 출원일자(국제) 2018년12월03일
심사청구일자 없음
(85) 번역문제출일자 2020년06월16일
(86) 국제출원번호 PCT/IB2018/059555
(87) 국제공개번호 WO 2019/111125
국제공개일자 2019년06월13일
(30) 우선권주장
1720389.4 2017년12월07일 영국(GB)

(71) 출원인
엔체인 홀딩스 리미티드
안티구아바부다 세인트존스, 처치 스트리트 44, 피츠제럴드 하우스
(72) 발명자
바르톨루치 실비아
영국 카디프 씨에프10 2에이치에이치 처칠 웨이 처칠 하우스 7 플로어 어커트-다이크 앤드 로드 엘엘피
베르나트 파울린
영국 카디프 씨에프10 2에이치에이치 처칠 웨이 처칠 하우스 7 플로어 어커트-다이크 앤드 로드 엘엘피
요셉 다니엘
영국 카디프 씨에프10 2에이치에이치 처칠 웨이 처칠 하우스 7 플로어 어커트-다이크 앤드 로드 엘엘피
(74) 대리인
제일특허법인(유)

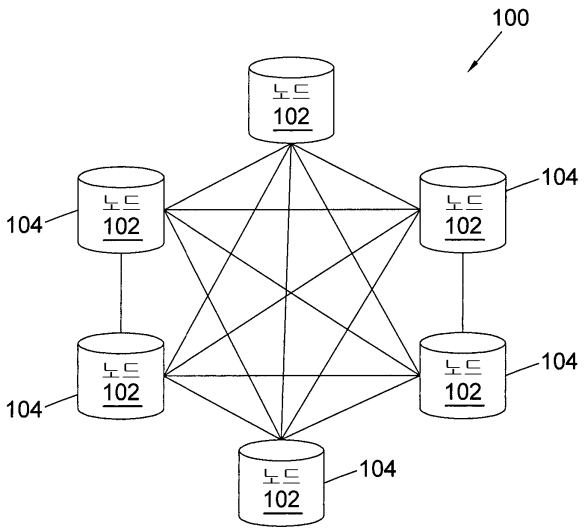
전체 청구항 수 : 총 15 항

(54) 발명의 명칭 **블라인드 결과 선택을 위한 블록체인 구현 보안 시스템 및 방법**

(57) 요 약

블록 체인 구현 보안 방법이 제공될 수 있다. 블록체인 네트워크를 사용하여 구현될 수 있다. 블록체인 구현 보안 방법의 실시예는 제 1 당사자와 제 2 당사자를 포함한다. 블록체인 구현 보안 방법은 제 1 당사자에 의해 생성된 제 1 복수의 *n*개 비밀의 암호화 버전과 제 2 당사자에 의해 생성된 제 2 복수의 *n*개 비밀의 암호화 버전의 조합에 기초하는 복수의 *n*개의 암호화 잠금을 생성한다. 제 1 당사자에 의해 생성된 제 1 복수의 *n*개 비밀에 속하는 하나의 비밀이 임의로 선택된다. 그리고, 복수의 *n*개의 암호화 잠금 중 특정 암호화 잠금을 잠금 해제하는 암호화 키가 생성되고, 여기서, 특정 암호화 잠금은 제 1 당사자에 의해 생성된 제 1 복수의 *n*개 비밀에 속하는 임의로 선택된 하나의 비밀에 대응한다.

대 표 도 - 도1a



(52) CPC특허분류
H04L 9/3239 (2013.01)
H04L 2209/38 (2013.01)
H04L 2209/56 (2013.01)

명 세 서

청구범위

청구항 1

제 1 당사자와 제 2 당사자를 포함하는 블록체인 구현 보안 방법으로서,

상기 제 1 당사자에 의해 생성된 제 1 복수의 *n*개 비밀의 암호화 버전과 상기 제 2 당사자에 의해 생성된 제 2 복수의 *n*개 비밀의 암호화 버전을 조합하여 복수의 *n*개의 암호화 잠금을 생성하는 단계와,

상기 제 1 당사자에 의해 생성된 상기 제 1 복수의 *n*개 비밀에 속하는 하나의 비밀을 임의로 선택하는 단계, 및

상기 복수의 *n*개의 암호화 잠금 중 특정 암호화 잠금을 잠금 해제하는 암호화 키를 생성하는 단계 - 상기 특정 암호화 잠금은, 상기 제 1 당사자에 의해 생성된 상기 제 1 복수의 *n*개 비밀에 속하는 상기 임의로 선택된 하나의 비밀에 대응함 -

를 포함하는 블록체인 구현 보안 방법.

청구항 2

제 1 항에 있어서,

상기 제 1 당사자에 의해 생성된 상기 제 1 복수의 *n*개 비밀의 상기 암호화 버전은, 상기 제 1 복수의 *n*개 비밀을 상기 제 1 당사자에게 공개하지 않은 채로 상기 제 2 당사자에게 전달되고/전달되거나,

상기 복수의 *n*개의 암호화 잠금은, 상기 제 1 당사자에 의해 생성된 상기 제 1 복수의 *n*개 비밀을 상기 제 2 당사자에게 공개하지 않은 채로 상기 제 2 당사자에 의해 생성되고/생성되거나,

상기 복수의 *n*개의 암호화 잠금은, 상기 복수의 *n*개의 암호화 잠금이 상기 제 1 당사자에 의해 생성된 상기 제 1 복수의 *n*개 비밀의 상기 암호화 버전과 상기 제 2 당사자에 의해 생성된 상기 제 2 복수의 *n*개 비밀의 상기 암호화 버전의 허용된 조합에 기초한다는 것을 보장하기 위해, 상기 제 2 당사자에 의해 생성되고 상기 제 1 당사자에 의해 검증되고/검증되거나,

상기 제 1 당사자에 의해 생성된 상기 제 1 복수의 *n*개 비밀에 속하는 상기 하나의 비밀은, 상기 제 1 당사자에 의해 임의로 선택되어 상기 제 2 당사자에게 안전하게 전달되고/전달되거나,

상기 암호화 키는, 상기 제 1 당사자에 의해 생성된 상기 제 1 복수의 *n*개 비밀을 상기 제 2 당사자에게 공개하지 않은 채로 상기 제 2 당사자에 의해 생성되는,

블록체인 구현 보안 방법.

청구항 3

제 1 항 또는 제 2 항에 있어서,

상기 복수의 *n*개의 암호화 잠금은, 상기 제 1 당사자에 의해 생성된 상기 제 1 복수의 *n*개 비밀의 상기 암호화 버전과 상기 제 2 당사자에 의해 생성된 상기 제 2 복수의 *n*개 비밀의 상기 암호화 버전의 선형 조합에 기초하는,

블록체인 구현 보안 방법.

청구항 4

제 3 항에 있어서,

상기 제 2 당사자에 의해, 적어도 하나의 트랜잭션 입력과 복수의 *n*개의 트랜잭션 출력을 포함하는 제 1 트랜잭션을 구성하는 단계 - 상기 제 1 트랜잭션의 상기 적어도 하나의 트랜잭션 입력은, 상기 제 2 당사자의 디지털 자산을 가리키고, 상기 제 1 트랜잭션의 상기 *n*개의 트랜잭션 출력은, 상기 제 2 당사자의 디지털 자산의 통제된 이전을 위해 상기 복수의 *n*개의 암호화 잠금 중 상이한 것에 기초한 잠금 스크립트를 포함함 - 와,

상기 제 1 당사자에 의해, 상기 제 2 당사자에 의해 생성된 상기 제 2 복수의 *n*개 비밀을 상기 제 1 당사자에게 공개하지 않은 채로, 상기 제 1 복수의 *n*개 비밀의 상기 암호화 버전과 상기 제 2 복수의 *n*개 비밀의 상기 암호화 버전으로부터 도출된 데이터를 사용하여 상기 제 1 트랜잭션을 검증하는 단계를 더 포함하고,

상기 제 1 당사자에 의해 생성된 상기 제 1 복수의 *n*개 비밀에 속하는 상기 하나의 비밀은, 상기 제 1 트랜잭션의 성공적인 검증에 응답하여 상기 제 1 당사자에 의해 임의로 선택되는,

블록체인 구현 보안 방법.

청구항 5

제 4 항에 있어서,

상기 제 2 당사자에 의해, 상기 제 1 당사자가 임의로 선택한 상기 하나의 비밀에 대응하는 상기 제 1 트랜잭션의 특정 트랜잭션 출력을 결정하는 단계와,

상기 제 2 당사자에 의해, 트랜잭션 입력과 적어도 하나의 트랜잭션 출력을 포함하는 제 2 트랜잭션을 구성하는 단계 - 상기 제 2 트랜잭션의 상기 트랜잭션 입력은, 상기 제 1 당사자에 의해 임의로 선택된 상기 하나의 비밀에 대응하는 상기 제 1 트랜잭션의 상기 특정 트랜잭션 출력을 가리키고 상기 제 1 트랜잭션의 상기 특정 트랜잭션 출력의 상기 암호화 잠금을 잠금 해제하는 상기 암호화 키에 기초한 잠금 해제 스크립트를 포함하며, 상기 제 2 트랜잭션의 상기 적어도 하나의 트랜잭션 출력은, 상기 제 2 당사자의 디지털 자산의 통제된 이전을 위한 잠금 스크립트 및 출력값을 포함함 -

를 더 포함하는 블록체인 구현 보안 방법.

청구항 6

제 4 항에 있어서,

상기 제 2 당사자에 의해, 상기 제 1 트랜잭션의 상기 *n*개의 트랜잭션 출력에 대한 수 *n*을 생성하는 단계와,

상기 제 2 당사자에 의해, 상기 수 *n*을 포함하는 메시지를 상기 제 1 당사자에게 송신하는 단계, 및

상기 제 1 당사자에 의해, 상기 수 *n*을 포함하는, 상기 제 1 당사자에 의해 송신된 상기 메시지를 수신하는 단계

를 더 포함하는 블록체인 구현 보안 방법.

청구항 7

제 4 항에 있어서,

상기 제 1 당사자에 의해, 상기 제 1 복수의 *n*개의 비밀을 생성하는 단계와,

상기 제 1 당사자에 의해, 타원 곡선 암호화를 이용하여 상기 제 1 복수의 *n*개 비밀을 암호화하여, 상기 제 1 복수의 *n*개 비밀의 상기 암호화 버전을 나타내는 *n*개의 결과 데이터 포인트를 획득하는 단계와,

상기 제 1 당사자에 의해, 상기 *n*개의 결과 데이터 포인트를 포함하는 메시지를 상기 제 2 당사자에게 송신하는 단계와,

상기 제 2 당사자에 의해, 상기 *n*개의 결과 데이터 포인트를 포함하는, 상기 제 1 당사자에 의해 송신된 상기 메시지를 수신하는 단계와,

상기 제 2 당사자에 의해, 상기 *n*개의 결과 데이터 포인트를 복구하는 단계와,

상기 제 2 당사자에 의해, 상기 제 2 복수의 *n*개 비밀을 생성하는 단계, 및

상기 제 2 당사자에 의해, 타원 곡선 암호화를 이용하여 상기 제 2 복수의 *n*개 비밀을 암호화하여, 상기 제 2 복수의 *n*개 비밀의 상기 암호화 버전을 나타내는 *n*개의 결과 데이터 포인트를 획득하는 단계

를 더 포함하고,

상기 제 2 당사자는, 상기 제 1 당사자에 의해 생성된 상기 제 1 복수의 *n*개 비밀의 상기 암호화 버전을 나타내는 상기 *n*개의 데이터 포인트와 상기 제 2 당사자에 의해 생성된 상기 제 2 복수의 *n*개 비밀의 상기 암호화 버

전을 나타내는 상기 *n*개의 데이터 포인트의 선형 조합에 기초하는 상기 복수의 *n*개의 암호화 잠금을 생성하는,

블록체인 구현 보안 방법.

청구항 8

제 5 항에 있어서,

상기 제 1 당사자에 의해, 상기 제 1 당사자가 임의로 선택한 상기 하나의 비밀을 포함하는 메시지를 상기 제 2 당사자에게 송신하는 단계와,

상기 제 2 당사자에 의해, 상기 제 1 당사자가 임의로 선택한 상기 하나의 비밀을 포함하는, 상기 제 1 당사자로부터 송신된 상기 메시지를 수신하는 단계와,

상기 제 2 당사자에 의해, 상기 제 1 당사자로부터 송신된 상기 메시지에 응답하여 상기 제 1 당사자가 임의로 선택한 상기 하나의 비밀에 대응하는 상기 제 1 트랜잭션의 상기 특정 트랜잭션 출력과 연관된 인덱스를 생성하는 단계, 및

상기 제 2 당사자에 의해, 상기 제 1 당사자가 임의로 선택한 상기 하나의 특정 비밀과 상기 제 1 트랜잭션의 상기 특정 트랜잭션 출력과 연관된 상기 인덱스에 기초하여 상기 암호화 키를 생성하는 단계

를 더 포함하고,

상기 제 2 당사자는 상기 제 2 트랜잭션의 상기 트랜잭션 입력을 구성할 때 상기 암호화 키와 상기 제 1 트랜잭션의 상기 특정 트랜잭션 출력과 연관된 상기 인덱스의 양쪽 모두를 사용하는,

블록체인 구현 보안 방법.

청구항 9

제 5 항에 있어서,

상기 제 1 트랜잭션의 상기 *n*개의 트랜잭션 출력의 상기 잠금 스크립트는, 상기 복수의 *n*개의 암호화 잠금 중 상이한 것에 대응하는 서명 및 (상기 제 2 당사자가 보유한 비공개키로부터 도출된 서명과 같은) 가능한 다른 필요 데이터를 제공하는 각각의 잠금 해제 스크립트에 의해 해제될 수 있고,

상기 제 2 트랜잭션의 상기 트랜잭션 입력은, 상기 트랜잭션 입력이 가리키는 상기 제 1 트랜잭션의 상기 특정 트랜잭션 출력의 상기 암호화 잠금에 대응하는 서명과 (상기 제 2 당사자가 보유하는 상기 비공개키로부터 도출된 서명과 같은) 가능한 다른 필요 데이터를 구비하는 잠금 해제 스크립트를 포함하며,

상기 특정 트랜잭션 출력의 상기 암호화 잠금에 대응하는 상기 서명은, 상기 제 1 당사자에 의해 임의로 선택된 상기 하나의 비밀에 기초하여 상기 제 2 당사자에 의해 생성된 상기 암호화 키로 구성되는,

블록체인 구현 보안 방법.

청구항 10

제 5 항에 있어서,

블록체인 네트워크의 블록체인 블록에 상기 제 1 트랜잭션을 저장하기 위해 상기 블록체인 네트워크에서 검증 및 채굴을 위해 상기 제 1 트랜잭션을 브로드캐스팅하는 단계, 및/또는

상기 블록체인 네트워크의 블록체인 블록에 상기 제 2 트랜잭션을 저장하기 위해 상기 블록체인 네트워크에서 검증 및 채굴을 위해 상기 제 2 트랜잭션을 브로드캐스팅하는 단계

를 더 포함하고,

상기 블록체인은, 작업 증명(proof-of-work) 블록체인 또는 지분 증명(proof-of-stake) 블록체인인,

블록체인 구현 보안 방법.

청구항 11

제 5 항에 있어서,

상기 제 2 당사자에 의해, 상기 제 1 트랜잭션의 검증 실패에 응답하여 적어도 하나의 제 3 트랜잭션을 구성하는 단계 - 상기 제 3 트랜잭션은, 적어도 하나의 트랜잭션 입력과 적어도 하나의 트랜잭션 출력을 포함하고, 상기 제 3 트랜잭션의 상기 적어도 하나의 트랜잭션 입력은, 상기 제 1 트랜잭션의 트랜잭션 출력을 가리키고, 상기 제 2 트랜잭션의 상기 적어도 하나의 트랜잭션 출력은, 상기 제 2 당사자에게 디지털 자산을 상환하기 위한 잠금 스크립트 및 출력값을 포함함 - 를 더 포함하고,

상기 적어도 하나의 제 3 트랜잭션은, 상기 제 1 트랜잭션의 상기 *n*개의 트랜잭션 출력을 참조하는 복수의 트랜잭션 입력을 구비하는 단일 트랜잭션을 포함하거나,

상기 적어도 하나의 제 3 트랜잭션은, 각각 상기 제 1 트랜잭션의 상기 *n*개의 트랜잭션 출력 중 상이한 것을 참조하는 트랜잭션 입력을 구비하는 *n*개의 개별 트랜잭션을 포함하는,

블록체인 구현 보안 방법.

청구항 12

제 11 항에 있어서,

비공개키와 공개키 쌍은, 상기 제 2 당사자와 연관되어 있고,

상기 제 1 트랜잭션의 상기 *n*개의 트랜잭션 출력의 상기 잠금 스크립트는, 상기 제 2 당사자의 상기 비공개키로부터 도출된 서명을 제공하는 잠금 해제 스크립트에 의해 해제될 수 있고,

상기 제 3 트랜잭션의 상기 적어도 하나의 트랜잭션 입력은, 상기 제 1 트랜잭션의 대응하는 트랜잭션 출력을 가리키고, 상기 제 2 당사자의 상기 비공개키로부터 도출된 서명을 제공하는 잠금 해제 스크립트를 포함하는,

블록체인 구현 보안 방법.

청구항 13

제 4 항에 있어서,

상기 제 1 당사자는, 상기 복수의 *n*개의 암호화 잠금이 상기 제 1 당사자에 의해 생성된 상기 제 1 복수의 *n*개 비밀의 암호화 버전과 상기 제 2 당사자에 의해 생성된 상기 제 2 복수의 *n*개 비밀의 암호화 버전의 허용된 선형 조합에 기초한다는 것을 보장하기 위해, 상기 제 1 트랜잭션을 검증하고/검증하거나,

상기 제 1 당사자는, 상기 제 2 당사자에 의해 생성된 상기 제 2 복수의 *n*개 비밀을 상기 제 1 당사자에게 공개하지 않은 채로, 상기 제 2 당사자에 의해 생성된 상기 제 2 복수의 *n*개 비밀의 상기 암호화 버전의 조합으로부터 도출된 데이터를 이용하여 상기 제 1 트랜잭션을 검증하고/검증하거나,

상기 제 1 트랜잭션의 상기 검증은, 다음 형식의 연산을 포함하고,

$$(k_B^{(1)}G + k_B^{(2)}G \ldots + k_B^{(n)}G) + (k_A^{(1)}G + k_A^{(2)}G \ldots + k_A^{(n)}G) \stackrel{?}{=} \left(k_A^{(1)} + k_B^{(1)}\right)G + \left(k_A^{(2)} + k_B^{(2)}\right)G \ldots + \left(k_A^{(n)} + k_B^{(n)}\right)G,$$

여기서, $k_A^{(1)}$, $k_A^{(2)}$, …, $k_A^{(n)}$는 상기 제 1 복수의 *n*개 비밀이고,

$k_B^{(1)}$, $k_B^{(2)}$, …, $k_B^{(n)}$는 상기 제 2 복수의 *n*개 비밀이고,

*G*는 타원 곡선의 포인트이고,

$k_A^{(1)}G$, $k_A^{(2)}G$, …, $k_A^{(n)}G$는 상기 제 1 복수의 *n*개 비밀의 암호화 버전이며,

$k_B^{(1)}G$, $k_B^{(2)}G$, …, $k_B^{(n)}G$는 상기 제 2 복수의 *n*개 비밀의 암호화 버전인,

블록체인 구현 보안 방법.

청구항 14

실행되는 경우, 프로세서가 제 1 항 내지 제 13 항 중 어느 한 항의 방법 중 임의의 부분을 수행하도록 구성하

는 컴퓨터 실행 가능 명령어를 포함하는 컴퓨터 판독 가능 저장 매체.

청구항 15

전자 장치로서,

인터페이스 장치와,

상기 인터페이스 장치에 커플링된 프로세서와,

상기 프로세서에 커플링된 메모리

를 포함하고,

상기 메모리는, 상기 프로세서가 제 1 항 내지 제 13 항 중 어느 한 항의 방법 중 임의의 부분을 수행하도록 구성하는 컴퓨터 실행 가능 명령어를 저장하는

전자 장치.

발명의 설명

기 술 분 야

[0001] 본 발명은 일반적으로 분산 시스템에 관한 것으로, 보다 상세하게는 블록체인에 유지되는 암호화된 자산(cryptographically-enforced assets)(암호 화폐 포함)의 신뢰성 및 유용성을 개선하기 위한 방법 및 시스템에 관한 것이다.

배 경 기 술

[0002] 본 명세서에서는 '블록체인'이라는 용어를 사용하는데, 이는 모든 형태의 전자, 컴퓨터 기반의 분산 원장을 포함한다. 이것에는 블록체인 및 트랜잭션 체인 기술, 허가 및 미허가 원장, 공유 원장 및 이들의 변형이 포함되지만, 이것으로 제한되는 것은 아니다. 다른 블록체인 구현예가 제안되고 개발되었지만, 가장 널리 알려진 블록체인 기술의 애플리케이션은 비트코인 원장이다. 편의 및 예시의 목적으로 비트코인이 본 명세서에서 참조될 수 있지만, 본 발명은 비트코인 블록체인에 사용되는 것으로만 제한되지 않고, 대안적인 블록체인 구현예 및 프로토콜이 본 발명의 범주 내에 속한다는 점에 유의해야 한다. 용어 "비트코인"이 본 명세서에 사용되어, 비트코인 프로토콜로부터 도출되는 모든 변형을 포함한다.

[0003] 블록체인은 합의 기반의(consensus-based) 전자 원장으로서, 컴퓨터에 기반하여 분산되고, 블록으로 구성된 분산형 시스템으로 구현되며, 이는 결국 트랜잭션 정보와 기타 정보로 구성된다. 비트코인의 경우, 각 트랜잭션은 블록체인 시스템 참여자 간의 디지털 자산의 통제권 양도를 인코딩하는 데이터 구조이며, 적어도 하나의 입력과 적어도 하나의 출력을 포함한다. 각 블록에는, 블록이 함께 체인화되어 초기부터 블록체인에 기입된 모든 트랜잭션에 대한 영구적이고 변경할 수 없는 기록을 생성하도록 이전 블록의 해시가 포함되어 있다. 트랜잭션에는 입력 및 출력에 포함된 스크립트로 알려진 작은 프로그램이 포함되어 있는데, 이는 트랜잭션의 출력에 액세스할 수 있는 방법과 대상을 특정한다. 비트코인 플랫폼에서 이들 스크립트는 스택 기반(stack-based) 스크립팅 언어를 이용하여 기입된다.

[0004] 트랜잭션이 블록체인에 기입되기 위해서는 "유효성 검증 완료(validated)"라야 한다. 일부 네트워크 노드는 채굴기 역할을 하고, 각 트랜잭션의 유효성 검증 작업을 수행하고, 네트워크에서는 유효하지 않은 트랜잭션이 거부된다. 예를 들어, 노드에 설치된 소프트웨어 클라이언트는 UTXO(unspent transaction output)를 참조하는 트랜잭션에 대해 이 유효성 검증 작업을 수행한다. 잠금 및 잠금 해제 스크립트를 실행하여 유효성 검증을 수행할 수 있다. 잠금 및 잠금 해제 스크립트의 실행이 TRUE로 평가되고, (충분한 채굴 비용 등을 포함하는) 다른 특정 조건들이 충족되면, 그 트랜잭션은 유효하며, 블록체인에 이 트랜잭션이 기입될 수 있다. 따라서, 트랜잭션을 블록체인에 기입하기 위해서는, i) 트랜잭션을 수신하는 노드에 의해 유효성이 검증되어야 하고 - 트랜잭션의 유효성이 검증되면, 노드는 네트워크의 다른 노드에 트랜잭션을 중계함 -, ii) 채굴기가 구축한 새로운 블록에 추가되어야 하고, iii) 채굴, 즉, 과거 트랜잭션의 공개 원장에 추가되어야 한다. 블록체인에 블록을 충분히 추가하여 사실상 트랜잭션을 되돌릴 수 없게 만들 때, 트랜잭션이 확인되는(confirmed) 것으로 간주된다.

[0005] 비공개키(private key)는, 블록체인에서 유지되는 암호화 화폐를 지출하는 것과 같이, 블록체인에서 유지되는 암호화 자산에 대한 액세스를 제어하는 데 일반적으로 사용된다. 보다 구체적으로, 사용자가 보유한 다른 암호

화 자산에 대한 암호화 코인이나 토큰을 송수신하기 위해 공개 어드레스와 비공개키가 사용자에게 통상 제공된다. 비공개키는 사용자가 보유한 암호화 코인이나 다른 암호화 자산이 지출, 인출되거나 또는 다른 방식으로 양도되거나 담보로 제공될 수 있게 하는 비밀 번호이다. 비트코인에서, 비공개키는 보통 256비트 수이다. 공개 어드레스는 사용자의 암호화 자산이 예치 및 수신되는 곳이다. 공개 어드레스는 수학적 알고리즘을 통해 비공개키로부터 생성된다. 그러나 공개 어드레스로부터 비공개키를 생성하여 프로세스를 반전시키는 것은 현실적으로 불가능하다.

[0006] 일반적으로 디지털 지갑은 사용자의 비공개키를 저장하는 데 사용된다. 사용자가 보유한 암호화 자산을 지출, 인출 또는 다른 방식으로 양도하거나 담보로 제공하기 위해 사용자에 의한 트랜잭션이 시작되면, 디지털 지갑은 비공개키로 트랜잭션을 처리함으로써 디지털 서명을 생성한다. 이는 어떤 트랜잭션에 대해 유효한 서명을 생성하는 유일한 방법은, 비공개키에 해당하는 공개 어드레스에 대해 트랜잭션의 서명이 유효하도록 그 비공개키를 사용하는 것이기 때문에, 시스템의 보안이 유지된다. 서명과 공개 어드레스는 트랜잭션이 (공개 어드레스에 해당하는 비공개키의 보유자인) 사용자로부터 왔는지 확인하고, (송금액이나 수취인 어드레스와 같은) 보안에 중요한 트랜잭션 요소가 브로드캐스트된 후에는 변경될 수 없도록 하는 데 사용된다. 이들 트랜잭션 요소가 변경되면, 사용자의 서명과 공개 어드레스에 기초한 트랜잭션의 검증이 실패할 것이다.

[0007] 사용자가 자신의 비공개키를 잃어버린 경우, 사용자는 더 이상 비공개키와 연관된 사용자의 암호화 자산을 지출, 인출 또는 다른 방식으로 양도하거나 담보로 제공할 수 없다. 따라서, 비공개키를 안전한 위치에 보관하는 것이 필수적이다. 디지털 지갑이 사용자의 비공개키를 저장할 수 있는 방법에는 여러 가지가 있다.

[0008] 일 예에서, 비공개키는 사용자의 비공개키로 트랜잭션이 체결되어야 할 때, 검색할 수 있도록 종이 양식이나 전자 문서에 인쇄될 수 있다. 예를 들어, 비공개키는, 사용자의 비공개키로 트랜잭션이 체결되어야 할 때, 스캔될 수 있는 QR 코드 형태로 인쇄될 수도 있다. 비공개키는 콜드 스토리지(cold-storage)나 하드웨어 지갑을 이용하여 저장될 수도 있는데, 일반적으로 사용자의 비공개키를 안전하게 저장하고 이 비공개키를 이용하여 오프라인에서 트랜잭션에 서명하는 스마트카드나 USB 장치가 사용된다. 다른 예에서, 비공개키는 핫 월렛(hot wallet)을 사용하여 저장될 수 있는데, 일반적으로 비공개키를 저장하고 인터넷에 어떤 방식으로 든 온라인으로 연결된 시스템을 사용하여 트랜잭션에 서명한다.

[0009] 비트코인의 사용자를 포함하여, 비트코인에 대한 일반적인 오해는 이 시스템이 완전히 익명이라는 오해이다. 모든 확인된 트랜잭션이 블록체인에 공개적으로 보인다는 점에서 익명성은 실제로 프로토콜 설계의 주안점은 아니었다. 원장의 투명성이 이중 지출의 위험성을 완화시키는 동시에 낮은 트랜잭션 비용과 수수료라는 매력을 제공하고, 기존의 은행 시스템에서와 같이 신뢰할 수 있는 중앙 집중식 시스템은 존재하지 않는다.

[0010] 트랜잭션에는 가명(pseudonyms)으로 작동하는 사용자의 입력 및 출력 공용 어드레스가 포함된다. 연관된 비공개키를 소유한 사용자만이 트랜잭션에 서명할 수 있다. 비트코인 프로토콜은 익명성(pseudonymity)을 제공하고, 이는 사용자 어드레스가 임의의 개인 정보에 명시적으로 결부되지 않는다는 것을 의미한다. 그러나 탈익명화 공격(de-anonymization attacks)은 비트코인 어드레스를 실제 ID(identity)와 연관지을 수 있는 사용자 정보를 찾는 것을 목표로 한다.

[0011] 탈익명화 단계 이전에 트랜잭션을 추적하고 그 트랜잭션을 공통 엔티티에 링크하기 위해 분석이 수행될 것이다. 예를 들어, 단일 트랜잭션의 입력으로 사용된 모든 어드레스를 하나의 ID로 그룹화할 수 있고, 이 정보를 사용하여 사용자 네트워크를 재구성할 수 있다.

[0012] 암호 화폐 사용자와 연관된 IP 어드레스(들)는 비트코인 네트워크 익명성을 훼손하는 데 사용될 수도 있다. 실제로 악의적인 공격자는 공개키를 IP 어드레스에 링크하여 특정 사용자가 제출한 모든 트랜잭션을 추적하는 데 성공할 수 있다. 더욱이, IP 정보는 실제 사용자의 ID를 검색하는 데 사용될 수 있고, 이 IP 정보를 다른 소스, 예컨대, 인터넷 포럼과 소셜 미디어와 결합함으로써 이 결과를 달성할 수 있다. 이러한 상황에서, 상이한 트랜잭션 세트에 대해 복수의 공개-비공개키 쌍을 생성하거나 운영의 익명성을 향상시키기 위해 편의상 혼합 서비스에 참여하는 것은 성공하지 못할 수 있다.

[0013] 비트코인 시스템 내(외)에서 코인 혼합 서비스의 개발은 코인 흐름의 추적 불가능성과 코인 소유자와의 트랜잭션의 링크 불가능성을 향상시키는 데 중점을 두고 있었다. 이들 혼합 서비스는 종종 신뢰할 수 있는 제 3 자가 참가자를 모집하고, P2P 네트워크(peer-to-peer network)에서 브로드캐스트될 트랜잭션을 생성해야 한다. 사용자 입력량과 출력량이 모두 동일하게 제공되는 경우, 코인 혼합 서비스는 추적 불가능성을 강화하는 가장 간단하고 효율적인 방법이다.

[0014] 이들 해법은 완벽한 것은 아니다. 신경망과 k-평균 클러스터(k-means cluster)를 이용하는 상이한 탈익명화 기술이 어드레스를 함께 클러스터링하고 그것을 사용자와 일치시키기 위해 존재한다. 예를 들어, 취약점 분석(taint analysis)은 다른 어드레스에서 수신한 특정 어드레스의 비트코인 비율을 측정하고, 트랜잭션의 입력량과 출력양 사이의 관계를 추론하려 한다.

[0015] 마지막으로 머신 러닝 알고리즘은 데이터를 분석하고 이벤트 체인에서 패턴을 찾는다. 비록 인간의 본성은 완전히 예측 가능하지는 않지만, 인간은 특정 상황에서 다른 사람들의 행동에 대한 이해를 바탕으로 하여 예측한다고 주장할 수 있다. 암호 화폐 시스템에서, 사용자는 표준 뱅킹 시스템에서와 마찬가지로, 이러한 기계 학습 알고리즘에 의해 추적되고 악용될 수 있는 패턴(모닝 커피, 월간 기부, 특정 조건에서 코인 혼합 서비스 사용 등)을 준수할 가능성이 높다. '활동 수준', '트랜잭션 타임스탬프' 또는 '교환 금액'과 같은 사용자 습관을 분석하면, 화폐의 탈익명화를 시도하는 공격자는 사용자 네트워크를 재구성할 수 있다. 이는 사용자의 행동이 공격자가 바로 사용할 수 있는 정보를 유출할 수 있음을 시사한다. 비트코인 시스템과 트랜잭션 이력의 공개 특성 때문에, 이러한 탈익명화 공격의 잠재성은 금융 규제 기관, 프로토콜 설계자 및 보안 분석가와 같은 많은 다른 당사자의 우려를 증가시킨다.

발명의 내용

[0016] 따라서, 본 발명에 따르면, 블록체인 구현된, 암호화된 보안 방법 및 장치가 제공된다. 이들은 제 1 당사자와 제 2 당사자가 관련될 수 있고, 제 1 당사자의 행동으로 제 2 당사자의 행동에 임의성(randomness)을 도입할 수 있다. 본 발명의 실시예는 악의적인 공격 및 보안 침해(compromises)를 감소시킴으로써 보안을 향상시킨다. 따라서, 본 발명의 실시예는 개선된 블록체인 네트워크를 제공한다.

[0017] 본 발명은 또한 블록체인에서 리소스의 잠금/잠금 해제를 제어하기 위해 암호화 기술을 사용하는 것으로 설명될 수 있고, 이는 사용자에게 향상된 보안을 제공한다.

[0018] 실시예에서, 블록체인 구현 보안 방법은, 복수의 *n*개의 암호화 잠금(locks)을 생성하기 위해, 제 1 당사자에 의해 생성된 제 1 복수의 *n*개 비밀(secrets)의 암호화 버전과 제 2 당사자에 의해 생성된 제 2 복수의 *n*개 비밀의 암호화 버전을 조합하는 단계와,

[0019] 제 1 당사자에 의해 생성된 제 1 복수의 *n*개 비밀에 속하는 하나의 비밀을 임의로 선택하는 단계, 및

[0020] 복수의 *n*개의 암호화 잠금 중 특정 암호화 잠금을 잠금 해제하는 암호화 키를 생성하는 단계 - 특정 암호화 잠금은 제 1 당사자에 의해 생성된 제 1 복수의 *n*개 비밀에 속하는 임의로 선택된 하나의 비밀에 대응함 - 를 포함할 수 있다.

[0021] 추가적으로 또는 대안적으로, 제 1 당사자에 의해 생성된 제 1 복수의 *n*개 비밀의 암호화 버전은 제 1 복수의 *n*개 비밀을 제 1 당사자에게 공개하지 않은 채로 제 2 당사자에게 전달될 수 있다.

[0022] 추가적으로 또는 대안적으로, 제 1 당사자에 의해 생성된 제 1 복수의 *n*개 비밀을 제 2 당사자에게 공개하지 않은 채로, 복수의 n개의 암호화 잠금이 제 2 당사자에 의해 생성될 수 있다.

[0023] 추가적으로 또는 대안적으로, 복수의 *n*개의 암호화 잠금은, 복수의 *n*개의 암호화 잠금이 제 1 당사자에 의해 생성된 제 1 복수의 *n*개 비밀의 암호화 버전과 제 2 당사자에 의해 생성된 제 2 복수의 n개 비밀의 암호화 버전의 허용된 조합에 기초한다는 것을 보장하기 위해, 제 2 당사자에 의해 생성되고 제 1 당사자에 의해 검증될 수 있다.

[0024] 추가적으로 또는 대안적으로, 제 1 당사자에 의해 생성된 제 1 복수의 n개 비밀에 속하는 하나의 비밀은 제 1 당사자에 의해 임의로 선택되어 제 2 당사자에게 안전하게 전달될 수 있다.

[0025] 추가적으로 또는 대안적으로, 복수의 n개의 암호화 잠금은 제 1 당사자에 의해 생성된 제 1 복수의 *n*개 비밀의 암호화 버전과 제 2 당사자에 의해 생성된 제 2 복수의 n개 비밀의 암호화 버전의 선형 조합에 기초할 수 있다.

[0026] 추가적으로 또는 대안적으로, 본 발명은 복수의 n개의 암호화 잠금을 사용하여, 제 2 당사자의 디지털 자산과 같은 디지털 자산의 이전을 제어할 수 있다. 이와 같은 실시예(들)에서, 제 1 복수의 *n*개 비밀에 속하는 하나의 비밀을 선택하는 데 있어 제 1 당사자의 임의의 동작은 블록체인 트랜잭션 출력을 임의로 선택하고/선택하거나 해당 블록체인 트랜잭션 출력에 대한 *n*개의 암호화 잠금 중 하나를 잠금 해제하는 암호화 키 구성과 같은, 제 2 당사자의 행동에 임의성을 도입한다.

[0027] 추가적으로 또는 대안적으로, 블록체인 구현 보안 방법은 논리적으로 초기화 단계, 커미트먼트 단계(commitment phase), 지불 단계 및 상환 단계의 4단계로 구분될 수 있다.

[0028] 초기화 단계에서, 제 2 당사자는 제 1 당사자에 의해 생성된 제 1 복수의 *n*개 비밀의 암호화 버전과 제 2 당사자에 의해 생성된 제 2 복수의 *n*개 비밀의 암호화 버전의 선형 조합에 기초하여 복수의 *n*개의 암호화 잠금을 생성할 수 있으며, 제 1 당사자에 의해 생성된 *n*개 비밀은 제 2 당사자에게 공개되지 않는다.

[0029] 커미트먼트 단계에서, 제 2 당사자는 적어도 하나의 트랜잭션 입력과 복수의 *n*개의 트랜잭션 출력을 포함하는 제 1 트랜잭션(또는 커미트먼트 트랜잭션)을 구성할 수 있으며, 여기서, 제 1 트랜잭션의 적어도 하나의 트랜잭션 입력은 제 2 당사자의 디지털 자산을 가리키고, 제 1 트랜잭션의 *n*개의 트랜잭션 출력은 복수의 *n*개의 암호화 잠금 중 상이한 것들에 기초한 잠금 스크립트를 포함한다. 제 1 당사자는 제 1 복수의 *n*개 비밀의 암호화 버전과 제 2 복수의 *n*개 비밀의 암호화 버전을 사용하여 제 1 트랜잭션을 검증하고, 제 2 당사자에 의해 생성된 *n*개 비밀은 제 1 당사자에게 공개되지 않는다. 제 1 트랜잭션의 성공적인 검증에 응답하여, 제 1 당사자는 제 1 당사자에 의해 생성된 제 1 복수의 비밀 중 하나의 특정 비밀을 임의로 선택하고, 제 1 당사자에 의해 임의로 선택된 하나의 특정 비밀을 제 2 당사자에게 송신한다. 제 2 당사자는 제 1 당사자가 임의로 선택한 하나의 특정 비밀에 대응하는 제 1 트랜잭션의 특정 트랜잭션 출력을 결정한다.

[0030] 지불 단계에서, 제 2 당사자는 트랜잭션 입력과 적어도 하나의 트랜잭션 출력을 포함하는 제 2 트랜잭션(또는 지불 트랜잭션)을 구성할 수 있는데, 여기서, 제 2 트랜잭션의 트랜잭션 입력은 제 1 당사자에 의해 임의로 선택된 하나의 특정 비밀에 대응하는 제 1 트랜잭션의 특정 트랜잭션 출력을 가리키고, 제 2 트랜잭션의 적어도 하나의 트랜잭션 출력은 제 2 당사자의 디지털 자산을 이전하기 위한 출력값 및 잠금 스크립트를 포함한다. 제 2 트랜잭션의 트랜잭션 입력은 또한 트랜잭션 입력에 의해 가리켜진 제 1 트랜잭션의 특정 트랜잭션 출력의 잠금 스크립트에 의해 제공되는 암호화 잠금에 대응하는 서명을 제공하는 잠금 해제 스크립트 및 제 1 트랜잭션의 특정 트랜잭션 출력의 잠금 스크립트에 의해 제공되는 방해물(encumbrance)을 해제하기 위한 가능한 다른 필요 데이터(예컨대, 제 2 당사자에 속하는 비공개키로부터 도출된 서명)를 포함할 수 있다.

[0031] 상환 단계에서, 제 2 당사자는 적어도 하나의 트랜잭션 입력과 적어도 하나의 트랜잭션 출력을 포함하는 적어도 하나의 제 3 트랜잭션(또는 상환 트랜잭션)를 구성할 수 있으며, 여기서, 제 3 트랜잭션의 적어도 하나의 트랜잭션 입력은 제 1 트랜잭션의 트랜잭션 출력을 가리키고, 제 3 트랜잭션의 적어도 하나의 트랜잭션 출력은 제 2 당사자에게 디지털 자산을 상환하기 위한 출력값과 잠금 스크립트를 포함한다. 제 3 트랜잭션의 트랜잭션 입력(들)은 트랜잭션 입력(들)에 의해 가리켜진 제 1 트랜잭션의 대응하는 트랜잭션 출력의 잠금 스크립트에 의해 제공되는 방해물을 해제하는 서명을 제공하는 잠금 해제 스크립트를 포함할 수도 있다.

[0032] 추가적으로 또는 대안적으로, 이 방법의 초기화 단계는 제 2 당사자가 제 1 트랜잭션의 *n*개의 트랜잭션 출력에 대해 수 *n*(여기서, *n*은 1보다 큰 정수)을 생성하여 수 *n*을 포함하는 메시지를 제 1 당사자에게 송신하는 단계를 더 포함할 수 있다.

[0033] 추가적으로 또는 대안적으로, 이 방법의 초기화 단계는, 제 1 당사자가 제 1 복수의 *n*개 비밀을 생성하는 단계와, 타원 곡선 암호화(elliptic curve cryptography)를 이용하여 제 1 복수의 *n*개 비밀을 암호화하여 제 1 복수의 *n*개 비밀의 암호화 버전을 나타내는 *n*개의 결과 데이터 포인트를 획득하는 단계, 및 *n*개의 결과 데이터 포인트를 포함하는 메시지를 제 2 당사자에게 송신하는 단계를 포함한다. 제 2 당사자는 *n*개의 결과 데이터 포인트를 복구하고, 제 2 복수의 *n*개 비밀을 생성하고, 타원 곡선 암호화를 이용하여 제 2 복수의 *n*개 비밀을 암호화하여 제 2 복수의 *n*개 비밀의 암호화 버전을 나타내는 *n*개의 결과 데이터 포인트를 획득하며, 제 1 복수의 *n*개 비밀의 암호화 버전을 나타내는 *n*개의 데이터 포인트와 제 2 복수의 *n*개 비밀의 암호화 버전을 나타내는 *n*개의 데이터 포인트의 선형 조합으로부터 *n*개의 암호화 잠금을 생성할 수 있다.

[0034] 추가적으로 또는 대안적으로, 이 방법은 제 1 당사자가 임의로 선택한 제 1 복수의 *n*개 비밀 중 하나의 특정 비밀을 포함하는 메시지를 제 1 당사자가 제 2 당사자에게 송신하는 단계를 포함할 수 있다. 제 2 당사자는 이 메시지를 수신하고, 제 1 당사자가 임의로 선택한 하나의 특정 비밀에 대응하는 제 1 트랜잭션의 특정 트랜잭션 출력과 연관된 인덱스를 결정하며, 제 1 당사자에 의해 임의로 선택되고 수신 메시지에 포함된 하나의 특정 비밀과 제 2 당사자에 의해 생성되고 제 1 트랜잭션의 특정 트랜잭션 출력에 대한 공개키 잠금을 도출하는 데 사용된 비밀을 추가함으로써 비공개키를 도출할 수 있다. 지불 단계에서, 제 2 당사자는 제 1 트랜잭션의 특정 트랜잭션 출력과 연관된 인덱스를 제 2 트랜잭션의 트랜잭션 입력을 구성하는 데 사용할 수 있다. 제 2 당사자는 또한 제 1 당사자 및 제 2 당사자에 의해 공동으로 생성된 비밀의 추가로부터 도출된 비공개키를 이용하여 제 1 트랜잭션의 특정 트랜잭션 출력의 잠금 스크립트에 의해 제공된 공개키 잠금에 대응하는 서명을 생성할 수

있다. 서명된 잠금 해제 스크립트는 제 2 트랜잭션의 트랜잭션 입력에 포함될 수 있다.

[0035] 추가적으로 또는 대안적으로, 블록체인 네트워크의 블록체인 블록에 제 1 트랜잭션을 저장하기 위해 제 1 트랜잭션을 블록체인 네트워크에서 브로드캐스트하여 검증 및 채굴할 수 있고, 블록체인 네트워크의 블록체인 블록에 제 2 트랜잭션을 저장하기 위해 제 2 트랜잭션을 블록체인 네트워크에서 브로드캐스트하여 검증 및 채굴할 수 있다. 블록체인은 작업 증명(proof-of-work) 블록체인 또는 지분 증명(proof-of-stake) 블록체인일 수 있다.

[0036] 추가적으로 또는 대안적으로, 비공개키와 공개키 쌍(pair)은 제 2 당사자와 연관될 수 있다. 커미트먼트 단계에서, 제 1 트랜잭션의 *n*개의 트랜잭션 출력의 잠금 스크립트는 제 2 당사자의 공개키뿐만 아니라, (제 1 당사자와 제 2 당사자에 의해 공동으로 생성된 2개의 비밀 세트로부터 도출된) *n*개의 암호화 잠금에 기초할 수 있다. 예를 들어, 제 1 트랜잭션의 *n*개의 트랜잭션 출력의 잠금 스크립트는, i) 트랜잭션 출력 옵션 각각의 암호화 잠금에 대응하는 서명과 제 2 당사자 자신의 비공개키에 기초하는 제 2 당사자의 서명을 제공하는 잠금 해제 스크립트, 또는 ii) 제 2 당사자 자신의 비공개키에 기초하는 제 2 당사자의 서명을 제공하는 잠금 해제 스크립트에 의해 해제될 수 있다.

[0037] 추가적으로 또는 대안적으로, 상기 상환 단계의 적어도 하나의 제 3 트랜잭션은 제 1 트랜잭션의 대응하는 잠금 스크립트에 의해 제공되는 방해물을 해제하기 위해 제 2 당사자 자신의 비공개키에 기초하여 제 2 당사자의 서명을 제공하는 잠금 해제 스크립트를 구비하는 트랜잭션 입력을 포함할 수 있다. 또한, 적어도 하나의 제 3 트랜잭션은 제 1 트랜잭션의 *n*개의 트랜잭션 출력을 참조하는 복수의 트랜잭션 입력을 구비하는 단일 트랜잭션일 수 있다. 대안적으로, 상환 단계의 적어도 하나의 제 3 트랜잭션은 제 1 트랜잭션의 *n*개의 트랜잭션 출력 중 다른 하나를 참조하는 트랜잭션 입력을 각각 구비하는 *n*개의 개별 트랜잭션을 포함할 수 있다.

[0038] 추가적으로 또는 대안적으로, 제 1 당사자는 복수의 *n*개의 암호화 잠금이 제 1 당사자에 의해 생성된 제 1 복수의 *n*개 비밀의 암호화 버전과 제 2 당사자에 의해 생성된 제 2 복수의 *n*개 비밀의 암호화 버전의 허용된 선형 조합에 기초한다는 것을 보장하기 위해, 제 1 트랜잭션을 검증할 수 있다.

[0039] 추가적으로 또는 대안적으로, 제 1 당사자는 제 2 당사자에 의해 생성된 제 2 복수의 *n*개 비밀의 암호화 버전의 조합을 나타내는 데이터를 이용하여 제 1 트랜잭션을 검증할 수 있고, 제 2 복수의 *n*개 비밀은 제 1 당사자에게 공개되지 않는다. 이 경우에, 제 2 당사자는 제 2 복수의 *n*개 비밀의 암호화 버전의 조합을 나타내는 데이터를 생성할 수 있고, 제 2 복수의 *n*개 비밀의 암호화 버전의 조합을 나타내는 데이터를 포함하는 메시지를 제 1 당사자에게 송신할 수 있다.

[0040] 추가적으로 또는 대안적으로, 제 1 트랜잭션의 검증은 다음 형식의 동작을 포함할 수 있다.

$$(k_B^{(1)}G + k_B^{(2)}G \ldots + k_B^{(n)}G) + (k_A^{(1)}G + k_A^{(2)}G \ldots + k_A^{(n)}G) \stackrel{?}{=} \left(k_A^{(1)} + k_B^{(1)}\right)G + \left(k_A^{(2)} +$$

[0041] $$k_B^{(2)}\Big)G \ldots + \left(k_A^{(n)} + k_B^{(n)}\right)G.$$

[0042] 여기서, $k_A^{(1)}$, $k_A^{(2)}$, …, $k_A^{(n)}$는 제 1 복수의 *n*개 비밀이고,

[0043] $k_B^{(1)}$, $k_B^{(2)}$, …, $k_B^{(n)}$은 제 2 복수의 *n*개 비밀이고,

[0044] G는 타원 곡선상의 포인트이고,

[0045] $k_A^{(1)}G$, $k_A^{(2)}G$, …, $k_A^{(n)}G$는 제 1 복수의 *n*개 비밀의 암호화 버전이며,

[0046] $k_B^{(1)}G$, $k_B^{(2)}G$, …, $k_B^{(n)}G$는 제 2 복수의 *n*개 비밀의 암호화 버전이다.

[0047] 본 발명에 따르면, 프로세서, 컴퓨터 메모리 및 네트워크 인터페이스 장치를 포함하는 전자 장치가 제공될 수 있다. 메모리는, 실행될 때, 본 명세서에 설명된 방법을 수행하도록 프로세서를 구성하는 컴퓨터 실행 가능 명령어를 저장한다.

[0048] 본 발명에 따르면, 컴퓨터 판독 가능 저장 매체가 제공될 수 있다. 컴퓨터 판독 가능 저장 매체는 컴퓨터 실행 가능 명령어를 포함하는 데, 이 명령어가 실행될 때, 본 명세서에 설명된 방법을 수행하도록 프로세서를 구성한다.

도면의 간단한 설명

[0049] 본 발명의 이들 및 다른 양태는 여기에 설명되는 실시예를 참조하여 명백해지고 명확해질 것이다. 본 발명의 실시예는 첨부 도면을 참조하여, 단지 예로서, 이하에 상세히 설명될 것이다.

도 1a는 예시적인 블록체인 네트워크의 블록도를 도시한다.

도 1b는 예시적인 블록체인 원장의 개략도이다.

도 1c는 비트코인 블록체인 환경에 대한 특정 블록체인 트랜잭션의 예를 나타낸다.

도 2는 제 1 당사자와 제 2 당사자간의 통신을 이용하여 제 2 당사자의 행동에 임의성을 도입하는 방식으로 제 2 당사자의 디지털 자산을 이전하기 위한 블록체인 트랜잭션을 생성하는 예시적인 방법의 상위 레벨 흐름도이다.

도 3a와 도 3b는 도 2의 초기화 단계의 예시적인 상세를 집합적으로 나타내는 흐름도이다.

그림 4a 내지 도 4c는 도 2의 커미트먼트 단계의 예시적인 상세를 집합적으로 나타내는 흐름도이다.

도 5는 도 2의 지불 단계의 예시적인 상세를 나타내는 흐름도이다.

도 6은 도 2의 상환 단계의 예시적인 상세를 나타내는 흐름도이다.

도 7은 도 2 내지 6의 방법론의 특정 동작의 개략적인 예시도이다.

도 8은 다양한 실시예가 구현될 수 있는 컴퓨팅 환경을 도시한다.

발명을 실시하기 위한 구체적인 내용

[0050] **블록체인 네트워크**

[0051] 먼저, 블록체인과 연관된 예시적인 블록체인 네트워크(100)를 블록도 형식으로 도시한 도 1a를 참조할 것이다. 블록체인 네트워크는 공개 블록체인 네트워크일 수 있으며, P2P(peer-to-peer) 공개 멤버십 네트워크는 초대없이 또는 다른 회원의 동의없이 누구나 참여할 수 있다. 블록체인 네트워크(100)가 작동하는 블록체인 프로토콜의 인스턴스를 실행하는 분산형 전자 장치는 블록체인 네트워크(100)에 참여할 수 있다. 이러한 분산형 전자 장치는 노드(102)로 지칭될 수 있다. 블록체인 프로토콜은, 예를 들어, 비트코인 프로토콜일 수 있다.

[0052] 블록체인 프로토콜을 실행하고 블록체인 네트워크(100)의 노드(102)를 형성하는 전자 장치는, 예를 들어, 데스크탑 컴퓨터, 랩톱 컴퓨터, 태블릿 컴퓨터, 서버, 스마트 폰과 같은 휴대기기, 스마트 워치나 기타 전자 장치와 같은 웨어러블 컴퓨터를 포함하는 다양한 유형일 수 있다.

[0053] 블록체인 네트워크(100)의 노드(102)는 유무선 통신 기술을 포함할 수 있는 적절한 통신 기술을 사용하여 서로 커플링된다. 이러한 통신은 블록체인과 연관된 프로토콜을 준수한다. 예를 들어, 블록체인이 비트코인 블록체인인 경우, 비트코인 프로토콜이 사용될 수 있다.

[0054] 노드(102)는, 도 1b에 도시된 바와 같이, 트랜잭션 블록의 분산 원장(1216)을 유지한다. 이 분산 원장(1216)은 종종 블록체인 원장 또는 블록체인으로 지칭된다. 작업 증명에 의해 확보된 블록체인 원장의 경우, 블록체인 원장에 영향을 미치는 노드(102)에 의한 트랜잭션은 다른 노드(102)에 의해 검증되어 블록체인 원장의 유효성이 유지된다. 또한, 블록체인 원장이 작업 증명 기반 블록체인인 경우, 블록과 함께 제출된 작업 증명을 확인하여 블록을 검증한다.

[0055] 블록체인 원장(1216)은 트랜잭션의 블록(예컨대, 블록(1221, 1222, 1223))에 대응하는 데이터를 포함한다. 예를 들어, 블록(1222)은 트랜잭션(1230(1)~(4))을 포함한다. 블록(1223)을 제외한 블록체인 원장(1216)의 블록들은, 어떤 블록이 불변(immutable)으로 될 때 그 블록에서 계산되는 값에 후속 블록이 좌우되고, 불변 블록에 대한 어떠한 수정이라도 다른 블록체인 노드에 의해 무효 블록으로 쉽게 인식될 수 있다는 점에서 암호화적으로 불변성(cryptographically immutable)이 있다. 열린 박스로서 도시된 블록(1223)은 변경 가능성이 있고 아직 블록체인 원장(1216)에 커미트되지 않은 트랜잭션의 스토리지를 나타낸다.

[0056] 블록체인 네트워크(100)의 각 노드(102)는 블록체인 원장(1216)의 완전한 사본이나 부분 사본을 저장할 수 있다. 일부 노드(102)에는 미지출(unspent) 트랜잭션만이 유지되고, 다른 노드에는 전체 블록체인 원장이 유지 관리될 수 있다. 이러한 방식으로, 각 노드가 그 자신의 사본을 가질 수 있으므로 블록체인 원장은 분산 원장

이다. 블록체인 네트워크(100)의 각 노드(102)는 프로토콜의 규칙에 따라 이러한 규칙을 완전히 따르는 모든 노드에 대해, 블록체인 원장의 사본을 수정하도록 구성될 수 있으며, 그들의 사본은 블록 및 트랜잭션에 대한 소정 전파 시간을 제외하고는 늘 다른 노드와 동일해야 한다. 각 노드(102)는 또한 그들이 수신한 블록과 그들 블록 내의 트랜잭션을 검증하도록 구성될 수 있다. 블록체인 프로토콜의 규칙은, 블록이나 트랜잭션이 무효라고 결정되면, 블록체인 노드가 블록이나 트랜잭션을 다른 노드로 전파하지 않아야 한다는 것이다. 이 규칙을 사용하면, 유효하고 유효한 것으로 검증된 블록 및 트랜잭션은 블록체인 네트워크를 전파하지만 무효인 블록 및 트랜잭션은 전파되지 않는다.

[0057] 블록체인 네트워크(100)의 노드(102) 중 적어도 일부는 블록체인 네트워크(100)의 채굴기(104)로서 동작한다. 도 1a의 블록체인 네트워크(100)가 작업 증명(proof-of-work) 블록체인인 경우, 채굴기(104)는 블록체인 원장에 다음 블록을 생성하기 위해 대량의 연산을 수행한다. 예를 들어, 작업 증명 블록체인은 채굴기가 암호화 문제를 해결하도록 요구할 수 있다. 비트코인에서, 채굴기(104)는 블록 헤더(block header)가, SHA-256을 이용하여, 현재 난이도(current difficulty)에 따라 정의된 값보다 작은 수로 해싱하도록 논스(nonce)를 찾는다. 작업 증명 알고리즘에 필요한 해싱 능력이란, 그 위에 어떤 수 이상의 블록이 채굴된 후에는, 트랜잭션이 사실상 불가역적인 것으로 간주된다는 것을 의미한다. 암호화 문제를 해결하는 채굴기(104)는 블록체인에 대한 신규 블록을 생성하고, 신규 블록을 다른 노드(102)에 브로드캐스트한다. 다른 노드(102)는 채굴기(104)가 실제로 암호화 문제를 해결했으며, 따라서 블록이 블록체인에 추가되어야 한다는 것을 수락하기 전에 작업 증명을 충분히 입증했는지를 검증한다. 블록은 노드(102)의 합의(consensus)에 의해 분산 블록체인 원장에 추가된다. 도 1a의 블록체인 네트워크(100)가 지분 증명(proof-of-stake) 블록체인인 경우, 채굴기(104)는 다음 블록을 생성하기 위해 경쟁하고, 승자는 각각의 채굴기(104)가 보유한 부(즉, 지분)에 의존하는 결정론적(의사 랜덤) 프로세스에 따라 선택된다.

[0058] 채굴기(104)에 의해 생성된 블록은 노드(102)에 의해 블록체인에 브로드캐스트된 트랜잭션을 포함한다. 예를 들어, 블록은 노드(102) 중 하나와 연관된 어드레스로부터 노드(102) 중 다른 하나와 연관된 어드레스로의 트랜잭션을 포함할 수 있다. 이러한 방식으로, 블록은 하나의 어드레스로부터 다른 어드레스로의 트랜잭션의 레코드로서 기능한다. 트랜잭션이 블록에 포함되도록 요청한 당사자는 그들의 공개키에 해당하는 비공개키를 이용하여 요청에 서명함으로써 이전 개시(예컨대, 비트코인의 경우, 비트코인을 소비할 수 있는) 권한이 있음을 증명한다. 이전은 요청이 유효하게 서명된 경우에만 블록에 추가될 수 있다.

[0059] 비트코인의 경우, 공개키와 어드레스 사이에 일대일 대응 관계가 있다. 즉, 각 공개키는 단일 어드레스와 연관된다. 따라서, 본 명세서에서 디지털 자산을 공개키로(또는 공개키로부터) 이전하는 것(예컨대, 공개키에 지불)과 디지털 자산을 그 공개키와 연관된 어드레스로(또는 어드레스로부터) 전송하는 것에 대한 언급은 공통의 동작을 지칭한다.

[0060] 일부 노드(102)는 유효성 검증 노드로서 참여할 수 있고, 또한 채굴기로서 동작할 수 있다(또는 동작하지 않을 수 있다). 유효성 검증 노드는 서명(들) 확인, 유효한 UTXO에 대한 참조 확인 등을 포함할 수 있는 트랜잭션의 유효성 검증을 수행한다.

[0061] 도 1a의 예는 6개의 노드(102)를 포함하고, 그 중 5개는 채굴기(104)로서 참여하고 있다. 실제로, 노드(102)나 채굴기(104)의 수는 상이할 수 있다. 많은 블록체인 네트워크에서, 노드(102)와 채굴기(104)의 수는 도 1a에 도시된 수보다 훨씬 많을 수 있다.

[0062] 도 1c는 비트코인 블록체인에 저장될 수 있는 트랜잭션(150)의 예를 도시한다. 유사한 기능의 다른 변형도 가능하다. 트랜잭션의 데이터 요소나 필드는 도 1c에 도시된 바와 같을 수 있고, 본 발명에서 설명된 것 이외의 추가 필드를 포함할 수 있다. 도시된 바와 같이, 트랜잭션(150)의 블록체인 프로토콜 버전을 나타내는 값을 포함하는 블록체인 버전 필드(152)가 존재한다. #vin 필드(154)는 트랜잭션(150)에 몇 개의 트랜잭션 입력(아래에 설명됨)이 존재하는지를 표시한다. 도시되지는 않았지만, 다른 필드들이 존재할 수 있고, 각각의 트랜잭션 입력(여기에서는 Vin[y](160)으로 예시됨)에 대해, 이전 트랜잭션의 트랜잭션 ID(TxID)(161), 이전 트랜잭션(트랜잭션 입력(160)과 일치하도록 트랜잭션 출력을 제공하는 트랜잭션)의 출력 중 하나에 대한 인덱스(162)를 포함하는 필드 세트가 존재하며, 여기서, TxID(161)와 인덱스(162)는 함께 이전 트랜잭션의 출력을 참조하는 포인터(163)를 형성한다. 본 명세서에서 사용되는 바와 같이, 현재 또는 현재 트랜잭션(current or present transaction)과 관련한 맥락에서 사용될 때, 용어 "이전 트랜잭션"은 현재 또는 현재 트랜잭션에 의해 참조된(및 "지출된") 트랜잭션 출력을 갖는 특정한 이전 트랜잭션(또는 트랜잭션)을 지칭한다. 예에서, 현재 또는 현재 트랜잭션은 "지출(spending) 트랜잭션"이라고 지칭될 수 있다.

[0063] 일부 블록체인 구현예에서는, 고유 TxID 값을 할당하기 위한 중앙 집중형 메커니즘이 없고, 대신 트랜잭션 자체 내용의 해시를 생성하는 것과 같이 트랜잭션에 대한 고유 TxID를 생성하기 위한 분산형 메커니즘이 존재한다. 유효 트랜잭션이 상이한 유효 트랜잭션과 완전히 동일한 내용을 모두 가질 수 없으므로, 각각의 유효 트랜잭션은 TxID에 대해 고유한 해시를 포함할 것이다(해시 충돌의 천문학적으로 낮은 확률은 제외). 그러나, 본 명세서에서는 각 트랜잭션이 고유한 트랜잭션 ID를 가지고 있다고 가정한다. 해싱의 특성상, 트랜잭션의 내용으로부터 TxID가 생성되면, 해당 내용의 어느 것도 변경할 수 없으며, TxID가 해당 트랜잭션에 대해 유효하게 유지되도록 한다.

[0064] 도 1c에 도시된 바와 같이, 트랜잭션 입력 Vin[y](160)에 대한 필드 세트는 또한 다음에 오는 잠금 해제 스크립트의 길이를 나타내는 Unlocking_Script_Length 필드(164)와, 포인터(163)에 의해 가리켜진 트랜잭션 출력의 대응하는 잠금 스크립트를 "잠금 해제"하는 Vin[y](160)에 대한 잠금 해제 스크립트(일반적으로 비트코인 프로토콜에서 "scriptSig"로 지칭됨)를 포함하는 Unlocking_Script 필드(165), 및 트랜잭션(150)을 제한하는 데 사용될 수 있는 Sequence# 필드(166)를 포함한다.

[0065] 도 1c는 하나의 트랜잭션 입력과 하나의 트랜잭션 출력만을 명시적으로 나타내지만, 각각은 하나보다 많을 수 있다. 트랜잭션 입력에 뒤이어, 트랜잭션(150)에 몇 개의 트랜잭션 출력(이하에 설명됨)이 존재하는 지를 나타내는 #vout 필드(170)가 존재한다. 각 트랜잭션 출력(여기서는 Vout[x](180)를 예로 들어 설명함)에는, 이 트랜잭션 출력 Vout[x](180)에 의해 제공된 트랜잭션 값(예컨대, 비트코인 수)을 나타내는 출력값 필드(181)와 뒤이어 오는 잠금 스크립트의 길이를 나타내는 Locking_Script_Length 필드(182), 및 이 트랜잭션 출력 Vout[x](180)에 대한 잠금 스크립트(일반적으로 비트코인 프로토콜에서 "scriptPubKey"로 지칭됨)를 포함하는 Locking_Script 필드(183)를 포함하는 필드 세트가 존재한다. 전술한 바와 같이, 이 트랜잭션 출력의 트랜잭션 값은, 잠금 해제 스크립트를 포함하는, 그 잠금 해제 스크립트와 잠금 스크립트를 사용하여 검증을 수행할 때 블록체인 노드가 TRUE로 검증할 트랜잭션 입력을 구비하는 지출 트랜잭션을 생성할 수 있는 사람이라면 누구나 "소비"할 수 있다. 트랜잭션(150)이 지정된 미래 시간 이전이나 지정된 미래 블록 이전에 활성화되지 않도록 제한할 수 있는 잠금 시간 필드(190)와 같은 다른 필드는 트랜잭션 출력 필드에 뒤따를 수 있다. 지출 트랜잭션의 각 트랜잭션 입력이 이전 트랜잭션 출력의 대응하는 트랜잭션 출력을 가리키고 이전 트랜잭션 출력이 트랜잭션 값을 포함하는 경우, 트랜잭션 입력은 그 트랜잭션 값을 나타내는 필드를 포함할 필요는 없다.

[0066] 이제 도 2 내지 도 6을 참조하면, 블록체인 트랜잭션에서 "패턴 형성"의 문제를 해결하는 방법이 도시되어 있다. 이러한 방법에서, 액터(당사자 A)는 액터를 대신하여 무작위로, 맹목적으로 옵션을 선택하는 에이전트로서의 역할을 하는 셀렉터(당사자 B)를 선택한다. 셀렉터의 선택에 따른 편중(biases)을 제거하기 위해, 이 프로세스는 서로 다른 트랜잭션 출력을 잠그기 위해 사용되는 비밀의 교환에 기초한다. 셀렉터는 액터가 블록체인에서 검증 및 저장을 위해 트랜잭션을 제출할 때까지 액터에게 어떤 옵션이 선택되어 있는지 알 수 없을 것이다. 일반적으로, 이 방법은 사용자가 랜덤 선택을 생성하고자 하는 모든 상황에 적용 가능할 수 있고, 랜덤 선택을 생성하는 것 외에 에이전트와 협력하여 랜덤 선택을 하는 것이다. 도 2에 도시된 바와 같이, 이 방법은 4개의 단계 수순, 즉, 초기화 단계(201), 커미트먼트 단계(203)(커미트먼트 트랜잭션을 포함함), 지불 단계(205)(지불 트랜잭션을 포함함) 및 상환 단계(207)(적어도 하나의 상환 트랜잭션을 포함함)로 논리적으로 구분될 수 있다.

[0067] 실시예에서, 이 방법은 타원 곡선에서 유한 필드 산술 연산을 사용하는 디지털 암호화와 디지털 서명을 이용한다. 실시예에서, 타원 곡선은 수학식 $y^2 \equiv x^3 + ax + b \ (mod\ p)$으로 기술된 포인트들의 집합인데, 여기서, $4a^3 + 27b^2 \neq 0 \ (mod\ p)$이고, p는 소수(prime)이다. 유한 필드 산술 연산은 '포인트 덧셈(point addition)' 연산과 '포인트 더블링(point doubling)' 연산을 포함할 수 있다. '포인트 덧셈' 연산에서, 타원 곡선 상의 새로운 포인트가 곡선의 교차점의 반전(negation)으로 계산된다. 이것은 $R = P+Q$로 설명될 수 있다. '포인트 더블링' 연산에서는, 타원 곡선 상의 새로운 포인트는 더블 포인트(point double)로 계산된다. 이것은 $R = P+P = 2P$로 설명될 수 있다. 보다 구체적으로, 타원 곡선상의 2개의 포인트, $P(x_1,y_1)$과 $Q(x_2,y_2)$이 주어지면, $P+Q = (x_3,y_3)$이고, 여기서, x_3,y_3 및 m은 다음과 같다.

수학식 1

[0068] $$x_3 = m^2 - x_1 - x_2 \bmod p$$

[0069] $y_3 = m(x_1 - x_3) - y_1 \bmod p$, 및

[0070] $$m = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} \bmod p : if\ P \neq Q\ (Point\ Addition) \\ \frac{3x_1^2 + a}{2y_1} \bmod p : if\ P = Q\ (Point\ Doubling) \end{cases}$$

[0071] 유한 필드 산술 연산에는 수학식 $nP = \underbrace{P + P + \cdots + P}_{n}$, 로 설명되는 '스칼라에 의한 포인트 곱셈' 연산도 포함될 수 있는데, 여기서, n은 자연수이고, P는 타원 곡선 상의 포인트이다. 타원 곡선에서 유한 필드 산술 연산을 사용하는 디지털 암호화와 디지털 서명의 이용은, (일반적으로는 아니지만) 본 발명을 위해, 다음과 같이 주어진 비공개-공개키 관계의 동형 특성에 기인한다.

수학식 2

[0072] $$E(m+n) = E(m) + E(n)$$

[0073] 여기서, $E(x)$는 암호화 함수 xG이고, x는 비공개키이고, G는 타원 곡선의 기준점이며, xG는 x에 대응하는 공개키이다.

[0074] 초기화 단계(201)는 도 3a 와 도 3b의 동작 301 내지 동작 327을 포함한다. 커미트먼트 단계(203)는 도 4a 내지 도 4c의 동작 401 내지 동작 433을 포함한다. 지불 단계(205)는 도 5의 동작 501 내지 동작 503을 포함한다. 상환 단계(207)는 도 6의 동작 601을 포함한다.

[0075] 액터(또는 이 예에서 당사자 B)가 대표적으로 수행하는 동작은 도 3a, 도 3b 및 도 4의 왼쪽에 도시되고, 셀렉터(또는 이 예에서 당사자 A)가 대표적으로 수행하는 동작은 도 3a, 도 3b 및 도 4의 오른쪽에 도시되어 있음에 주목한다. 액터(또는 이 예에서 당사자 B)가 대표적으로 수행하는 동작은 디지털 지갑의 일부로 구현될 수 있으며, 이는 본 명세서에 기술된 기능을 수행할 때 프로그램 제어 하에 완전 자동 또는 반자동 방식으로 동작하도록 구성될 수 있다. 셀렉터(또는 이 예에서 당사자 A)가 대표적으로 수행하는 동작은 에이전트 노드에 의해 수행될 수 있으며, 이는 본 명세서에 기술된 기능을 수행할 때 프로그램 제어 하에 완전 자동 또는 반자동 방식으로 동작하도록 구성될 수 있다. 액터(예컨대, 액터의 디지털 지갑) 및 셀렉터(예컨대, 셀렉터의 에이전트 노드)는 블록체인 네트워크(100)를 포함할 수 있는 네트워크화된 데이터 통신이나 다른 적절한 데이터 통신 네트워크를 통해 메시지 및 서로 다른 형태의 데이터를 통신할 수 있다고 가정한다.

[0076] 도 3a 및 도 3b는 초기화 단계(201)의 예시적인 상세를 도시한다. 액터(당사자 B)와 셀렉터(당사자 A)는 타원 곡선의 기준점(G)과 타원 곡선에 대한 큰 소수 차수(prime order)(n_c) 및 최대 키 크기(q)를 포함하는 타원 곡선과 연관 파라미터 세트에 합치하는 것으로 가정한다. 예를 들어, 비트코인(secp256k1)에 사용되는 표준화된 타원 곡선을 선택할 수 있다. 또한, 비공개키와 공개키 쌍(sk_{Ub}, sK_{Ub})은 액터(당사자 B)에 속하며, 비공개키와 공개키 쌍(sk_{Ua}, sK_{Ua})은 셀렉터(당사자 A)에 속한다.

[0077] 동작 301에서, 액터(당사자 B)는 이 방법에 사용할 트랜잭션 출력 옵션의 수 n을 결정한다.

[0078] 동작 303에서, 액터(당사자 B)는 셀렉터(당사자 A)에 수 n을 포함하는 비공개 메시지를 생성한다. 비공개 메시지는 셀렉터(당사자 A)의 공개키(sK_{Ua})를 사용하여 암호화될 수 있다.

[0079] 동작 305에서, 액터(당사자 B)는 동작 303의 비공개 메시지를 셀렉터(당사자 A)에게 송신한다.

[0080] 동작 307에서, 셀렉터(당사자 A)는 동작 303의 비공개 메시지를 수신한다.

[0081] 동작 309에서, 셀렉터(당사자 A)는 동작 307에서 수신한 비공개 메시지에 포함된 수 n을 복구한다. 셀렉터(당

사자 A)의 공개키(sK_{Ua})를 사용하여 암호화된 비공개 메시지로부터 수 n을 복구하기 위해, 셀렉터(당사자 A)는 셀렉터(당사자 A)의 비공개키(sk_{Ua})를 사용하여 비공개 메시지를 해독할 수 있다.

[0082] 동작 311에서, 셀렉터(당사자 A)는 트랜잭션 출력 옵션에 대응하는 n개의 비밀($k_A^{(1)}$, $k_A^{(2)}$, …, $k_A^{(n)}$)을 생성한다. 실시예에서, n개 비밀($k_A^{(1)}$, $k_A^{(2)}$, …, $k_A^{(n)}$)은 간격 [1, n_c-1] 내에서 선택될 수 있으며, 여기서, n_c는 타원 곡선의 큰 소수 차수(large prime order)이다.

[0083] 동작 313에서, 셀렉터(당사자 A)는 타원 곡선상의 기준점 G와 함께 타원 곡선 암호화를 이용하여 n개 비밀($k_A^{(1)}$, $k_A^{(2)}$, …, $k_A^{(n)}$)을 암호화하여, n개의 결과 데이터 포인트($k_A^{(1)}G$, $k_A^{(2)}G$, …, $k_A^{(n)}G$)를 획득한다. 이 동작에서, n개의 결과 데이터 포인트($k_A^{(1)}G$, $k_A^{(2)}G$, …, $k_A^{(n)}G$)는, 전술한 바와 같이, 스칼라에 의한 포인트 곱셈으로부터 도출될 수 있고, 여기서, 비밀의 값은 각각의 데이터 포인트를 도출하는 데 사용되는 스칼라이다.

[0084] 동작 315에서, 셀렉터(당사자 A)는 액터(당사자 B)에 동작 313의 n개의 데이터 포인트($k_A^{(1)}G$, $k_A^{(2)}G$, …, $k_A^{(n)}G$)를 포함하는 비공개 메시지를 생성한다. 비공개 메시지는 액터(당사자 B)의 공개키(sK_{Ub})를 사용하여 암호화될 수 있다.

[0085] 동작 317에서, 셀렉터(당사자 A)는 동작 315의 비공개 메시지를 액터(당사자 B)에게 송신한다.

[0086] 동작 319에서, 액터(당사자 B)는 동작 315의 비공개 메시지를 수신한다.

[0087] 동작 321에서, 액터(당사자 B)는 동작 315에서 수신된 비공개 메시지에 포함된 n개의 데이터 포인트($k_A^{(1)}G$, $k_A^{(2)}G$, …, $k_A^{(n)}G$)를 복구한다. 액터(당사자 B)의 공개키(sK_{Ub})를 사용하여 암호화된 비공개 메시지에 포함된 n개의 데이터 포인트($k_A^{(1)}G$, $k_A^{(2)}G$, …, $k_A^{(n)}G$)를 복구하기 위해, 액터(당사자 B)는 액터(당사자 B)의 비공개키(sk_{Ub})를 사용하여 비공개 메시지를 해독할 수 있다.

[0088] 동작 323에서, 액터(당사자 B)는 n개의 트랜잭션 출력 옵션에 대응하는 n개 비밀($k_B^{(1)}$, $k_B^{(2)}$, …, $k_B^{(n)}$)을 생성한다. 실시예에서, n개 비밀($k_B^{(1)}$, $k_B^{(2)}$, …, $k_B^{(n)}$)은 간격 [1, n_c-1] 내에서 선택될 수 있으며, 여기서, n_c는 타원 곡선의 큰 소수 차수이다. 동작 323에서 액터(당사자 B)에 의해 생성된 n개 비밀($k_B^{(1)}$, $k_B^{(2)}$, …, $k_B^{(n)}$)은 방법의 후속 동작에서 셀렉터(당사자 A)에게 공개되지 않는다는 점에 유의한다.

[0089] 동작 325에서, 액터(당사자 B)는 타원 곡선상의 기준점 G와 함께 타원 곡선 암호화를 이용하여 n개 비밀($k_B^{(1)}$, $k_B^{(2)}$, …, $k_B^{(n)}$)을 암호화하여 n개의 결과 데이터 포인트($k_B^{(1)}G$, $k_B^{(2)}G$, …, $k_B^{(n)}G$)를 획득한다. 이 동작에서, n개의 결과 데이터 포인트($k_B^{(1)}G$, $k_B^{(2)}G$, …, $k_B^{(n)}G$)는, 전술한 바와 같이, 스칼라에 의한 포인트 곱셈으로부터 도출될 수 있고, 여기서, 비밀의 값은 각각의 데이터 포인트를 도출하는 데 사용되는 스칼라이다.

[0090] 동작 327에서, 액터(당사자 B)는 동작 313의 n개의 데이터 포인트($k_A^{(1)}G$, $k_A^{(2)}G$, …, $k_A^{(n)}G$)와 동작 325의 n개의 데이터 포인트($k_B^{(1)}G$, $k_B^{(2)}G$, …, $k_B^{(n)}G$)의 선형 조합에 기초하여 n개의 트랜잭션 출력 옵션의 각각에 대해 n개의 공개키 잠금(s_1G, s_2G, …, s_nG)을 생성한다. 각각 n개의 공개키 잠금은 액터(당사자 B)가 생성한 암호화된 비밀을 나타내는 하나의 데이터 포인트와 셀렉터(당사자 A)가 생성한 암호화된 비밀을 나타내는 하나의 데이터 포인트를 합산하여 생성된다. 실시예에서, n개의 공개키 잠금(s_1G, s_2G, …, s_nG)은 다음과 같이 도출될 수 있다.

수학식 3

[0091] 트랜잭션 출력 옵션 1: $s_1G = (k_A^{(1)}G + k_B^{(1)}G) = (k_A^{(1)} + k_B^{(1)})G$ (a)

트랜잭션 출력 옵션 2: $s_2G = (k_A^{(2)}G + k_B^{(2)}G) = (k_A^{(2)} + k_B^{(2)})G$ (b)

…

트랜잭션 출력 옵션 n: $s_nG = (k_A^{(n)}G + k_B^{(n)}G) = (k_A^{(n)} + k_B^{(n)})G$ (n)

[0092] 각 옵션의 마지막 2개 항목에 대해 획득된 등가성은 그룹의 동형 특성을 기반으로 한다. 또한, 설명을 단순화하기 위해, 전술한 실시예는 데이터 포인트($k_A^{(i)}G$)와 데이터 포인트($k_B^{(i)}G$)의 선형 조합에 기초하여 각각의 트랜잭션 출력 옵션 i(1 내지 n에 속함)에 대한 공개키 잠금을 도출한다는 점에 유의한다. 액터(당사자 B)에 의해 생성된 그룹에서 가져온 하나의 데이터 포인트와 셀렉터(당사자 A)에 의해 생성된 그룹에서 가져온 다른 하나의 데이터 포인트로 이루어진 데이터 포인트 쌍의 임의의 조합은, 두 그룹 중 서로 다른 데이터 포인트 조합이 서로 다른 트랜잭션 출력에 사용되어 데이터 포인트가 두 번 사용되지 않는 한, n개의 트랜잭션 출력 옵션에 대한 공개키 잠금을 형성하기 위해 조합될 수 있다.

[0093] 동작 313의 n개의 데이터 포인트($k_A^{(1)}G$, $k_A^{(2)}G$, …, $k_A^{(n)}G$)와 동작 325의 n개의 데이터 포인트($k_B^{(1)}G$, $k_B^{(2)}G$, …, $k_B^{(n)}G$)의 선형 조합에 기초하여 n개의 트랜잭션 출력 옵션 각각에 대해 n개의 공개키 잠금(s_1G, s_2G, …, s_nG)을 생성하고, 동작 323에서 액터(당사자 B)에 의해 생성된 비밀($k_B^{(1)}$, $k_B^{(2)}$, …, $k_B^{(n)}$)을 셀렉터(당사자 A)에게 공개하지 않음으로써, 셀렉터(당사자 A)는, 동작 311에서, 셀렉터(당사자 A)에 의해 생성된 비밀($k_A^{(1)}$, $k_A^{(2)}$, …, $k_A^{(n)}$) 중 어느 것이 n개의 공개키 잠금 각각을 도출하는 데 사용되었는지 모를 것이라는 점에 유의한다. 또한 셀렉터(당사자 A)는 n개의 공개키 잠금을 재구성하거나 n개의 공개키 잠금 중 어느 하나를 해제하는 잠금 해제 스크립트를 생성할 수 없으며, 이는 액터(당사자 B)만으로, 아래에 설명하는 바와 같이, n개의 공개키 잠금 중 어느 하나를 해제하는 잠금 해제 스크립트를 생성할 수 있도록 한다.

[0094] 동작 327 이후에, 초기화 단계에서 액터(당사자 B)와 셀렉터(당사자 A)의 동작을 종료할 수 있다.

[0095] 도 4a 내지 도 4c는 커미트먼트 단계(203)의 예시적인 상세를 도시한다.

[0096] 동작 401에서, 액터(당사자 B)는 동작 327의 n개의 공개키 잠금(s_1G, s_2G, …, s_nG)과 액터(당사자 B)의 공개키(sK_{Ub})를 사용하여 n개의 트랜잭션 출력 옵션에 대한 n개의 잠금 스크립트를 생성한다. 각각의 특정 트랜잭션 출력 옵션에 대해 잠금 스크립트가 제공하는 잠금(방해물(encumbrance))은 i) 동작 327의 n개의 공개키 잠금 중 하나(s_1G, s_2G …, s_nG 중 하나)에 대응하는 서명(s_1, s_2, …, s_n 중 하나)과 액터(당사자 B)의 비공개키(sK_{Ub})로부터 도출된 서명, 또는 ii) 액터(당사자 B)의 비공개키(sK_{Ub})로부터 도출된 서명을 제공하는 잠금 해제 스크립트에 의해 해제되도록 구성될 수 있다.

[0097] 실시예에서, 각각의 n개의 트랜잭션 출력 옵션에 대한 n개의 잠금 스크립트는 다음과 같은 비트코인 스크립트 언어의 op_if 및 op_else opcode를 사용할 수 있다.

[0098]
```
OP_IF
    OP_2 <pubkey sK_Ub> <pubkey s_1G> OP_2 OP_CHECKMULTISIG
OP_ELSE
    <EXPIRY TIME T1> OP_CHECKSEQUENCVERIFY OP_DROP <pubkey
sK_Ub> OP_CHECKSIG
OP_ENDIF
```

[0099] 잠금 스크립트의 제 1 부분(IF)은 서명(s_1, s_2, …, s_n 중 하나)과 액터(당사자 B)의 비공개키(sk_{Ub})로부터 도출된 서명을 필요로 하는 n개 중 m개(2개 중 2개) 의 다중 서명 스크립트(m-of-n multisig script)이다. 이 경우의 잠금 해제 스크립트(아래에 설명하는 바와 같이, 지불 트랜잭션(T_P)의 일부임)는 다음과 같다.

[0100]
```
OP_0 <sig sk_Ub> <sig s_1> OP_TRUE
```

[0101] 이 잠금 해제 스크립트는, 필요한 서명(즉, 각 트랜잭션 출력에 대한 서명(s_1, s_2, …, s_n 중 하나)과 액터(당사자 B)의 비공개키(sk_{Ub})로부터 도출된 서명)을 제공하기 때문에, 커미트먼트 트랜잭션(T_C)의 각 트랜잭션 출력에 대한 잠금 스크립트의 제 1 옵션(케이스 i)을 잠금 해제할 수 있다.

[0102] 공개키에 대한 서명이 필요한 경우(이 경우, 액터의 공개키(sK_{Ub})), 잠금 스크립트(ELSE)의 제 2 부분은 표준 잠금 해제 스크립트이다. 프로토콜이 중단된 경우(즉, 셀렉터가 액터에게 비밀 값을 보내지 않은 경우), 향후 어느 시점 이후에 액터가 자금을 상환할 수 있도록 잠금 시간 값(T1)을 선택해야 한다. 잠금 시간 파라미터는 opcode OP_CHECKSEQUENCEVERIFY를 사용하여 정의된다. OP_CHECKSEQUENCEVERIFY는 BIP112에 도입되었으며, 이를 통해 소비 중인 출력의 연령에 따라 스크립트의 실행 경로를 제한할 수 있다는 점에 유의한다(https://github.com/bitcoin/bips/blob/master/bip-0112.mediawiki).

[0103] 이 경우의 (아래에 설명하는 바와 같이, 상환 트랜잭션(T_R)의 일부인) 잠금 해제 스크립트는 다음과 같다.

[0104]
```
<T1> <sig sk_Ub> OP_FALSE
```

[0105] 이 잠금 해제 스크립트는, 필요한 서명(즉, 액터(당사자 B)의 비공개키(sk_{Ub})로부터 도출된 서명)을 제공하기 때문에, 커미트먼트 트랜잭션(T_C)의 각 트랜잭션 출력의 잠금 스크립트의 제 2 옵션(케이스 ii)을 잠금 해제할 수 있다.

[0106] 동작 403에서, 액터(당사자 B)는 커미트먼트 트랜잭션(T_C)을 구성하는데, 여기에는 액터(당사자 B)의 자금이나 UTXO를 지정하는 하나 이상의 트랜잭션 입력과 트랜잭션 출력의 출력값을 잠그기 위해 동작 401에서 생성된 n개의 잠금 스크립트 중 하나를 가진 출력값(하나 이상의 트랜잭션 입력에 의해 지정된 액터의 자금의 일부임)을 각각 포함하는 n개의 트랜잭션 출력이 포함된다. 커미트먼트 트랜잭션(T_C)의 하나 이상의 트랜잭션 입력에 의해 지정된 액터(당사자 B)의 자금은 커미트먼트 트랜잭션(T_C)의 n개의 트랜잭션 출력의 출력값을 커버하기에 충분해야 한다는 점에 유의한다.

[0107] 동작 405에서, 액터(당사자 B)는 커미트먼트 트랜잭션(T_c)의 트랜잭션 출력에 지정된 액터의 자금을 액터의 동일 어드레스(또는 다른 어드레스)로 상환하기 위한 적어도 하나의 상환 트랜잭션(T_R)을 구성한다. 적어도 하나의 상환 트랜잭션(T_R)은 커미트먼트 트랜잭션(T_c)의 트랜잭션 출력을 가리키는 트랜잭션 입력을 포함하고, 여기서, 각 트랜잭션 입력에는 커미트 트랜잭션(T_c)의 대응하는 트랜잭션 출력 옵션에 대해 잠금 스크립트가 제공한 잠금(방해물(encumbrance))을 해제하기 위해 액터(당사자 B)의 비공개키(sk_{Ub})로부터 도출된 서명을 제공하는 잠금 해제 스크립트가 포함된다. 이 서명은 커미트먼트 트랜잭션(T_c)의 대응하는 트랜잭션 출력 옵션의 잠금 스크립트의 케이스 ii)를 충족한다. 적어도 하나의 상환 트랜잭션(T_R)은 또한 커미트먼트 트랜잭션(T_c)의 하나 이상의 트랜잭션 출력에 특정된 액터(당사자 B)의 자금을 액터의 동일 어드레스(또는 다른 어드레스)로 이전하는 출력값과 잠금 스크립트를 구비하는 하나 이상의 트랜잭션 출력을 포함할 수 있다.

[0108] 실시예에서, 상환 트랜잭션(T_R)에 대한 액터(당사자 B)의 비공개키(sk_{Ub})로부터 도출된 서명은 다음과 같이 타원곡선 암호화를 사용하여 생성할 수 있다. 상환 트랜잭션(T_R)의 일부는 해시되어 메시지(m)를 형성하고, 0<k<q의 범위에서 난수 k가 선택된다. 서명은 다음과 같이 2파트 (R, S)로 생성될 수 있다.

수학식 4

[0109] $$R = k \times G$$

[0110] $$S = k^{-1}(m + xr) \bmod n_c \quad \text{(b)}$$

[0111] 여기서, x는 액터의 비공개키(sk_{Ub})이고,

[0112] k^{-1}은, $k^{-1}k \equiv 1 \bmod n_c$와 같은 k mod n_c의 역수이다.

[0113] 실시예에서, 액터(당사자 B)는 커미트먼트 트랜잭션(T_c)의 n개의 상이한 트랜잭션 출력을 가리키는 n개의 트랜잭션 입력으로 단일 상환 트랜잭션(T_R)을 구성할 수 있다. 이 경우, 단일 상환 트랜잭션(T_R)에 대한 트랜잭션 출력(들)의 출력값(들)은 커미트먼트 트랜잭션(T_c)의 n개의 상이한 트랜잭션 출력에서 특정된 액터의 총 자금을 초과할 수 없다.

[0114] 다른 실시예에서, 액터(당사자 B)는 커미트먼트 트랜잭션(T_c)의 n개의 상이한 트랜잭션 출력을 가리키는 각각의 트랜잭션 입력으로 n개의 상환 트랜잭션(T_R)을 구성할 수 있다. 이 경우에, n개의 상환 트랜잭션(T_R)에 대한 트랜잭션 출력(들)의 출력값(들)은 커미트먼트 트랜잭션(T_c)의 n개의 상이한 트랜잭션 출력에서 특정된 액터의 총 자금을 초과할 수 없다.

[0115] 동작 407에서, 액터(당사자 B)는 검증 및 채굴을 위해 블록체인 네트워크(100)에서 동작 403의 커미트먼트 트랜잭션(T_c)을 브로드캐스트한다. 일단 검증되고 성공적으로 채굴되면, 커미트먼트 트랜잭션(T_c)은 블록체인 네트워크(100)에 의해 유지되는 분산된 블록체인 원장의 블록의 일부로 저장된다.

[0116] 실시예에서, 타원 곡선 암호화에 기초한 커미트먼트 트랜잭션(T_c)의 검증은 커미트먼트 트랜잭션(T_c)의 해싱 부분을 포함하여 메시지(m)을 형성할 수 있다. 액터(당사자 B)의 공개키(sK_{Ub})와 2파트 서명(R, S)은 커미트먼트 트랜잭션(T_c)이 제공된다. 2 파트 서명(R, S)은 다음과 같이 검증될 수 있다.

[0117] · $v = S^{-1}m \times G + S^{-1}R \times y$를 계산한다.

[0118] 여기서, S^{-1}은, $S^{-1}S \equiv 1 \bmod n_c$와 같이, S mod q의 역수이며, y는 액터의 공개키(sK_{Ub})이다.

[0119] · v == R인 경우에만, 2 파트 서명(R, S)이 유효임을 결정한다.

[0120] 2 파트 서명(R, S) 중 하나만 유효한 것으로 결정되면, 커미트먼트 트랜잭션(T_c)이 검증될 수 있다. 타원 곡선은 소수 차수(n_c)를 가지므로, 타원 곡선 포인트에 기준점(G)를 곱하면, S^{-1}의 mod n_c 부분이 사라진다는 점에 유의한다.

[0121] 동작 409에서, 액터(당사자 B)는 동작 325의 n개의 데이터 포인트($k_B^{(1)}G$, $k_B^{(2)}G$, …, $k_B^{(n)}G$)를 결합하여, 다음의 $s_BG = k_B^{(1)}G + k_B^{(2)}G + \cdots + k_B^{(n)}G$와 같은 결과 데이터 포인트($s_BG$)를 도출한다. 이 동작에서, 데이터 포인트(s_BG)는 동작 325의 n개의 데이터 포인트를 포함하는 일련의 포인트 추가 동작으로부터 도출될 수 있다.

[0122] 동작 411에서, 액터(당사자 B)는 동작 409의 데이터 포인트(s_BG)를 포함하는 비공개 메시지를 셀렉터(당사자 A)에 생성한다. 비공개 메시지는 셀렉터(당사자 A)의 공개키(sK_{Ua})를 사용하여 암호화된 형태일 수 있다.

[0123] 동작 413에서, 액터(당사자 B)는 동작 411의 비공개 메시지를 셀렉터(당사자 A)에게 송신한다.

[0124] 동작 415에서, 셀렉터(당사자 A)는 동작 409의 데이터 포인트(s_BG)를 포함하는 비공개 메시지를 수신한다.

[0125] 동작 417에서, 셀렉터(당사자 A)는 동작 409의 데이터 포인트(s_BG)를 복구하고, 커미트먼트 트랜잭션(T_C)의 정확

성을 검증하기 위해 데이터 포인트(s_BG)를 사용한다. 셀렉터(당사자 A)의 공개키(sK_{Ua})를 사용하여 암호화된 비공개 메시지에서 데이터 포인트(s_BG)를 복구하기 위해, 셀렉터(당사자 A)는 셀렉터(당사자 A)의 비공개키(sK_{Ua})를 사용하여 비공개 메시지를 해독할 수 있다.

[0126] 실시예에서, 동작 417의 검증은 합 s_BG+s_AG가 $(k_A^{(1)}+k_B^{(1)})G+k_A^{(2)}+k_B^{(2)})G \cdots+k_A^{(n)}+k_B^{(n)})G$의 합과 같은지를 결정하는 것을 포함한다. 이 경우에, s_AG는 동작 313의 n개의 데이터 포인트($k_A^{(1)}G$, $k_A^{(2)}G$, …, $k_A^{(n)}G$)로부터 $s_AG = k_A^{(1)}G+k_A^{(2)}G \cdots +k_A^{(n)}G$로 결정될 수 있다. 타원 곡선을 사용하는 암호화 기법의 동형 특성으로 인해, 이 검증 동작은 다음과 같이 표현될 수 있다.

수학식 5

[0127] $$(k_B^{(1)}G + k_B^{(2)}G \ldots + k_B^{(n)}G) + (k_A^{(1)}G + k_A^{(2)}G \ldots + k_A^{(n)}G) \doteq \left(k_A^{(1)} + k_B^{(1)}\right)G + \left(k_A^{(2)} + k_B^{(2)}\right)G \ldots + \left(k_A^{(n)} + k_B^{(n)}\right)G$$

[0128] 셀렉터(당사자 A)는 커미트먼트 트랜잭션(T_c)의 n개의 트랜잭션 출력 옵션의 잠금 스크립트로부터 수학식 (5)의 RHS에 대한 데이터 포인트를 검색할 수 있고, 그 후 수학식 (5)의 RHS에 제공되는 것과 같이 이들 데이터 포인트를 함께 조합할 수 있다. 이러한 검증은 액터(당사자 B)가 프로토콜을 준수하고 커미트먼트 트랜잭션(T_c)의 n개의 트랜잭션 출력 옵션에 대해 대응하는 n개의 잠금 스크립트의 일부인 n개의 공개키 잠금(s_1G, s_2G, …, s_nG)을 생성했는지 확인할 수 있고, 여기서, n개의 공개키 잠금(s_1G, s_2G, …, s_nG)은 동작 313의 n개의 데이터 포인트($k_A^{(1)}G$, $k_A^{(2)}G$, …, $k_A^{(n)}G$)와 동작 325의 n개의 데이터 포인트($k_B^{(1)}G$, $k_B^{(2)}G$, …, $k_B^{(n)}G$)의 허용된 선형 조합에 기초한다.

[0129] 동작 419에서, 셀렉터(당사자 A)는 커미트먼트 트랜잭션(T_C)이 검증되는지 여부를 확인하기 위해 동작 417의 결정 결과를 평가한다. 만약 '예'인 경우, 아래에 설명된 바와 같이, 동작 421 내지 동작 433으로 진행되고, '아니오'인 경우, 동작 421 내지 동작 433을 건너뛴다.

[0130] 동작 421에서, 셀렉터(당사자 A)는 동작 311에서 셀렉터(당사자 A)에 의해 생성된 비밀($k_A^{(1)}$, $k_A^{(2)}$, …, $k_A^{(n)}$) 중 하나를 임의로 선택한다.

[0131] 동작 423에서, 셀렉터(당사자 A)는 비공개 메시지를 액터(당사자 B)에 생성하고, 여기서, 비공개 메시지는 동작 421에서 임의로 선택된 비밀($k_A^{(1)}$, $k_A^{(2)}$, …, $k_A^{(n)}$ 중 하나)를 포함한다. 비공개 메시지는 액터(당사자 B)의 공개키(sK_{Ub})를 사용하여 암호화될 수 있다.

[0132] 동작 425에서, 셀렉터(당사자 A)는 비공개 메시지를 액터(당사자 B)에게 송신하고, 이는 동작 421에서 임의로 선택된 비밀($k_A^{(1)}$, $k_A^{(2)}$, …, $k_A^{(n)}$ 중 하나)을 포함하고, 커미트먼트 단계에서, 셀렉터(당사자 A)의 동작은 종료된다.

[0133] 동작 427에서, 액터(당사자 B)는 셀렉터(당사자 A)로부터 (동작 421에서 임의로 선택된 비밀($k_A^{(1)}$, $k_A^{(2)}$, …, $k_A^{(n)}$ 중 하나)을 포함하는) 비공개 메시지를 수신하고, 커미트먼트 트랜잭션(T_C)의 잠금 기간(Locktime Period)의 만료 내에 비공개 메시지가 수신되었는 지를 결정한다. '아니오'인 경우, 액터(당사자 B)의 동작은 도시한 바와 같이 상환 단계(도 6)로 계속된다. '예'인 경우, 동작은 동작 429로 계속된다. 액터(당사자 B)의 공개키(sK_{Ub})를 사용하여 암호화된 비공개 메시지에 포함된 비밀을 복구하기 위해, 액터(당사자 B)는 액터(당사자 B)의 비공개키(sK_{Ub})를 사용하여 비공개 메시지를 해독할 수 있다.

[0134] 단계 429에서, 액터(당사자 B)는 셀렉터(당사자 A)로부터 수신된 비공개 메시지에 포함된 비밀($k_A^{(1)}$, $k_A^{(2)}$, …, $k_A^{(n)}$ 중 하나)이, 동작 401에서, 커미트먼트 트랜잭션(T_C)의 n개의 트랜잭션 출력의 공개키 잠금을 구성하는 데 사용되는 동작 321의 데이터 포인트 중 어느 하나와 일치하는 지를 결정한다. 이러한 동작에는 결과 데이터 포인트(이것은 전술한 동작 313과 마찬가지임)를 얻기 위해 타원 곡선의 기준점(G)와 함께 타원 곡선 암호화를 이용하여 비밀($k_A^{(1)}$, $k_A^{(2)}$, …, $k_A^{(n)}$ 중 하나)을 암호화하는 것과 결과 데이터 포인트가 동작 319에서 셀렉터(당사자 A)로부터 수신되어 동작 321에서 액터(당사자 B)에 의해 복구된 데이터 포인트 중 어느 하나와 일치하는 지를 결정하는 것이 포함될 수 있다. 이 결정이 실패하면, 액터(당사자 B)의 동작은 도시된 바와 같이 상환 단계(도 6)로 계속될 수 있다. 이 결정이 성공하면, 동작은 동작 431 및 동작 433으로 계속된다.

[0135] 동작 431에서, 액터(당사자 B)는 셀렉터(당사자 A)로부터 수신된 비공개 메시지에 포함된 비밀($k_A^{(1)}$, $k_A^{(2)}$, …, $k_A^{(n)}$ 중 하나)과 동작 429에서 결정된 동작 321의 특정 데이터 포인트 사이의 일치하는 대응 관계를 이용하여, 공개키 잠금이 수신 메시지에 포함된 비밀($k_A^{(1)}$, $k_A^{(2)}$, …, $k_A^{(n)}$ 중 하나)로부터 도출되는 커미트먼트 트랜잭션 T_c의 특정 트랜잭션 출력을 식별하는 인덱스를 도출한다. 예를 들어, $k_A^{(2)}$가 비공개 메시지에 포함된 임의로 선택된 비밀이고, 수학식 3(b)의 예로 예시된 바와 같이, $k_A^{(2)}$ 가 커미트먼트 트랜잭션(T_c)의 트랜잭션 출력 2의 공개키 잠금(s_2G)을 구성하는 데 사용된 경우, 동작 431에서 도출된 인덱스는 커미트먼트 트랜잭션(T_c)의 트랜잭션 출력 2를 참조할 것이다.

[0136] 동작 433에서, 액터(당사자 B)는 수신 메시지에 포함된 비밀($k_A^{(1)}$, $k_A^{(2)}$, …, $k_A^{(n)}$ 중 하나)과, 동작 323에서 액터(당사자 B)에 의해 생성되고 동작 431의 인덱스에 의해 식별된 특정 트랜잭션 출력에 대한 공개키 잠금을 도출하는 데 사용되는 비밀($k_B^{(1)}$, $k_B^{(2)}$, …, $k_B^{(n)}$ 중 하나)을 추가함으로써 비공개키를 도출하고, 액터(당사자 B)의 동작은, 도 5에 도시된 바와 같이, 지불 단계로 계속된다.

[0137] 셀렉터(당사자 A)에 의해 선택된 임의의 비밀은, 셀렉터(당사자 A)가 이러한 임의의 비밀 선택의 효과를 모르는 상태에서, 후술하는 바와 같은 지불 트랜잭션을 위해 동작 433에서 비공개키를 구성하는 경우에 액터의 행동에 영향을 미친다는 점에 유의한다. 블록체인에서 액터(당사자 B)에 의해 지불 트랜잭션이 제출된 후에만 그 효과를 발견할 수 있다. 이 설정은 커미트먼트 트랜잭션의 n개의 트랜잭션 출력 옵션 중에서 선택하는 것이 완전히 무작위적이며 편중되지 않도록 보장한다. 또한 셀렉터(당사자 A)가 액터의 비밀의 합계(예컨대, $s_BG = k_B^{(1)}G+k_B^{(2)}G \cdots +k_B^{(n)}G$)에 대한 추가적인 정보에 액세스할 수 있음에도 불구하고, 셀렉터(당사자 A)는 어떤 비밀이 커미트먼트 트랜잭션(T_C)의 n개의 트랜잭션 출력 옵션 중 어느 하나를 잠금 해제하는지 유추할 수 없을 것이다. 또한, 셀렉터(당사자 A)는 액터의 비밀($k_B^{(1)}$, $k_B^{(2)}$, …, $k_B^{(n)}$)을 모르기 때문에, 셀렉터(A 당사자)는 지불 트랜잭션(T_P)을 제출하여도 액터로부터 자금을 훔칠 수 없게 되는 데, 이는 지불 트랜잭션(T_P) 역시 셀렉터가 재생할 수 없는 액터의 필수 서명(s_1, s_2, …, s_n 중 하나로부터 도출됨)을 필요로 하기 때문이다.

[0138] 도 5는 지불 단계(205)의 예시적인 상세를 도시한다. 셀렉터(당사자 A)는, 도 5의 동작으로부터 명백한 바와 같이, 지불 단계(205)에 참여할 필요가 없다. 지불 단계(205)에서, 액터(당사자 A)의 동작은 액터(당사자 B)가 셀렉터(당사자 A)로부터 비공개 메시지를 수신하는 것에 응답하여 수행되고, 이 비공개 메시지는 커미트먼트 트랜잭션(T_C)의 잠금 기간의 만료 내에 커미트먼트 트랜잭션(T_C)의 n개의 트랜잭션 출력 옵션 중 임의로 선택된 어느 하나에 해당하는, 셀렉터(당사자 A)에 의해 생성된 비밀($k_A^{(1)}$, $k_A^{(2)}$, …, $k_A^{(n)}$) 중 하나를 포함한다는 점에 유의한다.

[0139] 동작 501에서, 액터(당사자 B)는 동작 431에서 결정된 인덱스에 대응하는 커미트먼트 트랜잭션(T_C)의 특정 트랜잭션 출력을 가리키는 트랜잭션 입력을 포함하는 지불 트랜잭션(T_P)을 구성한다. 트랜잭션 입력에는 동작 433의 비공개키에 기초한 서명뿐만 아니라 트랜잭션 입력이 가리키는 커미트먼트 트랜잭션(T_c)의 특정 트랜잭션 출력의

잠금 스크립트에 의해 제공된 잠금(방해물)을 해제하는 액터(당사자 B)의 비공개키(sk_{Ub}) 기초한 서명을 제공하는 잠금 해제 스크립트도 포함된다. 이 서명은 커미트먼트 트랜잭션(T_C)의 대응하는 트랜잭션 출력 옵션의 잠금 스크립트의 케이스 i)를 충족한다. 지불 트랜잭션(T_P)은 또한 커미트먼트 트랜잭션(T_c)의 특정 트랜잭션 출력에서 특정된 액터의 자금의 일부 또는 전부를 수취인(액터나 몇몇 다른 수취인의 다른 어드레스일 수 있음)에게 이전하는 출력값과 잠금 스크립트를 구비하는 하나 이상의 트랜잭션 출력을 포함한다.

[0140] 실시예에서, 동작 433의 비공개키에 기초한 서명과 지불 트랜잭션(T_P)에 대한 액터(당사자 B)의 비공개키(sk_{Ub})로부터 도출된 서명은 다음과 같이 타원 곡선 암호화를 사용하여 생성될 수 있다. 지불 트랜잭션 T_P의 일부는 해시되어 메시지 m을 형성하고, 0<k<q의 범위에서 난수 k가 선택된다. 동작 433의 비공개키에 기초하는 서명은 다음과 같이 2 파트 ($R1$, $S1$)로 생성될 수 있다.

수학식 6

[0141] $$R1 = k \times G$$

[0142] $$S1 = k^{-1}(m + x1R1) \bmod n_c \quad \text{(b)}$$

[0143] 여기서, $x1$은 동작 433의 비공개키이고,

[0144] k^{-1}은, $k^{-1}k \equiv 1 \bmod n_c$와 같이, $k \bmod n_c$의 역수이다.

[0145] 액터(당사자 B)의 비공개키(sk_{Ub})부터 도출된 서명은 다음과 같이 2파트 ($R2$, $S2$)로 생성될 수 있다.

수학식 7

[0146] $$R2 = k \times G$$

[0147] $$S2 = k^{-1}(m + x2R2) \bmod n_c \quad \text{(b)}$$

[0148] 여기서, $x2$는 액터의 비공개키(sk_{Ub})이고,

[0149] k^{-1}은, $k^{-1}k \equiv 1 \bmod n_c$와 같은 $k \bmod n_c$의 역수이다.

[0150] 동작 503에서, 액터(당사자 B)는 검증 및 채굴을 위해 블록체인 네트워크(100)에서 지불 트랜잭션(T_P)을 브로드캐스트한다. 일단 검증되고 성공적으로 채굴되면, 지불 트랜잭션(T_P)은 블록체인 네트워크(100)에 의해 유지되는 분산된 블록체인 원장의 블록의 일부로 저장된다. 지불 트랜잭션(T_P)을 브로드캐스트한 후, 지불 단계(205)에서의 액터(당사자 B)의 동작이 종료된다.

[0151] 실시예에서, 타원 곡선 암호화에 기초한 지불 트랜잭션(T_P)의 검증은 지불 트랜잭션(T_P)의 일부를 해싱하여 메시지(m)를 형성하는 것을 포함할 수 있다. 커미트먼트 트랜잭션(T_C)의 트랜잭션 출력 옵션의 공개키 잠금과, 액터(당사자 B)의 공개키(sK_{Ub}), 및 2 파트 서명($R1$, $S1$), ($R2$, $S2$)은 지불 트랜잭션(T_P)과 함께 제공된다. 동작 433의 비공개키에 기초한 2 파트 서명($R1$, $S1$)은 다음과 같이 검증될 수 있다.

[0152] · $v1 = S1^{-1}m \times G + S1^{-1}R1 \times y1$를 계산한다.

[0153] 여기서, $S1^{-1}$은 $S1^{-1}S1 \equiv 1 \bmod n_c$와 같은 $S1 \bmod q$의 역수이며,

[0154] $y1$은 커미트먼트 트랜잭션(T_C)의 트랜잭션 출력 옵션의 공개키 잠금이다.

[0155] · $v1==R1$인 경우에만, 2 파트 서명($R1$, $S1$)이 유효임을 결정한다.

[0156] 액터의 비공개키(sk_{Ub})로부터 도출된 2 파트 서명($R2$, $S2$)은 다음과 같이 검증될 수 있다.

[0157] · $v2 = S2^{-1}m \times G + S2^{-1}R2 \times y2$를 계산한다.

[0158] 여기서, $S2^{-1}$은 $S2^{-1}S2 \equiv 1 \ mod \ n_c$와 같은 $S2$ mod q의 역수이며,

[0159] $y2$는 액터의 공개키(sK_{Ub})이다.

[0160] · $v2==R2$인 경우에만, 2 파트 서명($R2$, $S2$)가 유효임을 결정한다.

[0161] 지불 트랜잭션은 2 파트 서명($R1$, $S1$) 및 ($R2$, $S2$)의 양쪽 모두가 유효한 것으로 결정된 경우에만 검증될 수 있다. 두 경우 모두에서, 타원 곡선에는 소수 차수(n_c)가 있으므로, 타원 곡선 포인트에 기준점(G)을 곱하면, S^{-1}의 mod n_c 부분이 사라진다는 점에 유의한다.

[0162] 액터(당사자 B)가 지불 트랜잭션(T_P)의 자금의 수취인일 필요는 없다는 점에 유의한다. 즉, 액터가 자금을 그들의 어드레스 중 하나에서 그들이 비공개키를 소유한 새로운 어드레스로 옮기려고 하지 않는다. 이 경우, 수취인의 서명과 셀렉터가 제공한 비밀을 사용하여 자금을 잠금 해제할 수 있다.

[0163] 도 6은 상환 단계(207)의 예시적인 상세를 도시한다. 셀렉터(당사자 A)는, 도 6의 동작으로부터 명백한 바와 같이, 상환 단계(207)에 참여할 필요가 없다. 상환 단계(207)에서 액터(당사자 A)의 동작은, 지불 단계 이후에 수행될 수 있고, 또한, i) 액터(당사자 B)가 셀렉터(당사자 A)로부터 커미트먼트 트랜잭션(T_C)의 잠금 기간(Locktime Period)의 만료 내에 임의의 비밀($k_A^{(1)}$, $k_A^{(2)}$, …, $k_A^{(n)}$ 중 하나)을 포함하는 비공개 메시지를 수신하지 않거나, 또는 ii) 수신 메시지에 포함된 임의로 선택된 비밀이 동작 401에서 커미트먼트 트랜잭션(T_C)의 n개의 트랜잭션 출력의 공개키 잠금을 구성하는데 사용된 데이터 포인트 중 어느 하나와 일치하지 않는 것에 응답하여 수행될 수 있다.

[0164] 동작 601에서, 액터(당사자 B)는 검증 및 채굴을 위해 블록체인 네트워크(100)의 동작 405에서 구성된 적어도 하나의 상환 트랜잭션(T_R)을 브로드캐스트한다. 일단 검증되고 성공적으로 채굴되면, 적어도 하나의 상환 트랜잭션(T_R)은 블록체인 네트워크(100)에 의해 유지되는 분산된 블록체인 원장의 블록의 일부로서 저장된다. 적어도 하나의 상환 트랜잭션(T_R)을 브로드캐스트한 후, 상환 단계(207)에서의 액터(당사자 B)의 동작이 종료된다.

[0165] 실시예에서, 타원 곡선 암호화에 기초한 상환 트랜잭션(T_R)의 검증은 상환 트랜잭션(T_R)의 일부를 해싱하여 메시지(m)를 형성하는 것을 포함할 수 있다. 액터(당사자 B)의 공개키(sK_{Ub})와 액터의 비공개키(sk_{Ub})로부터 도출된 2 파트 서명(R, S)는 상환 트랜잭션(T_R)과 함께 제공된다. 2 파트 서명(R, S)는 다음과 같이 검증될 수 있다.

[0166] · $v = S^{-1}m \times G + S^{-1}R \times y$를 계산한다.

[0167] 여기서, S^{-1}은 $S^{-1}S \equiv 1 \ mod \ n_c$와 같은 S mod q의 역수이며,

[0168] y는 액터의 공개키(sK_{Ub})이다.

[0169] · $v==R$인 경우에만, 2 파트 서명(R, S)가 유효임을 결정한다.

[0170] 서명(R, S)이 유효한 것으로 결정되는 경우에만, 상환 트랜잭션(T_R)이 검증될 수 있다. 타원 곡선에는 소수 차수(n_c)가 있으므로, 타원 곡선 포인트에 기준점(G)을 곱하면, S^{-1}의 mod n_c 부분이 사라진다는 점에 유의한다.

[0171] 도 7은 도 2 내지 6의 방법론의 특정 동작을 나타낸다.

[0172] 상술한 예는 액터와 셀렉터 간에 정보를 통신하기 위해 비공개 메시지를 사용한다는 점에 유의한다. 이들 비공개 메시지는 표준 암호화 기술을 사용하여 암호문 메시지를 작성할 수 있다. 이는 임의 유형의 암호화 솔루션(예컨대, 타원 곡선, RSA 등)으로 수행할 수 있다. 기본적으로 메시지는 수취인이 보유하는 공개키로 (임의의 암호화 방식을 사용하여) 암호화될 수 있고, 암호문 메시지는 수취인에게 송신된다. 그러면 수취인은 수취인이 보유하는 비공개키를 사용하여 암호문 메시지를 해독할 수 있다. 수취인은 자신이 가지고 있는 비공개키를 사

용하여 암호문이 나타내는 정보를 결정/판독할 수 있기 때문에, 암호화는 제 3 자로부터 메시지에 포함된 정보를 숨기기 위해서만 수행된다는 점에 유의한다.

[0173] 대안적인 실시예에서, 액터와 셀렉터 사이에서 정보를 통신하는 하나 이상의 메시지는 암호화 기술을 포함하지 않고 원시 데이터를 공개적으로 통신하여 암호문을 생성할 수 있다. 이와 같은 암호화되지 않은 통신은 메시지(들)에 포함된 원시 데이터의 공개 통신으로 인한 보안 위험이 없는 경우에 적합할 수 있다.

[0174] 또한, 전술한 예는 특정 작업 증명 블록체인 네트워크(예컨대, 비트코인 블록체인 네트워크)를 참조했지만, 본 명세서에 설명된 방법은 다른 유형의 작업 증명 블록체인 네트워크 및 다른 가능한 지분 증명 블록체인 네트워크와 함께 사용될 수도 있다.

[0175] 도 8은 본 발명의 적어도 하나의 실시예를 실시하는 데 사용될 수 있는 컴퓨팅 장치(2600)의 예시적이고 단순화된 블록도이다. 다양한 실시예에서, 컴퓨팅 장치(2600)는 위에 예시되고 설명된 임의의 방법 및 시스템을 구현하는 데 사용될 수 있다. 예를 들어, 컴퓨팅 장치(2600)는 데이터 서버, 웹 서버, 휴대용 컴퓨팅 장치, 퍼스널 컴퓨터 또는 임의의 전자 컴퓨팅 장치로 사용되도록 구성될 수 있다. 도 8에 도시된 바와 같이, 컴퓨팅 장치(2600)는 버스 서브시스템(2604)을 통해 다수의 주변 서브시스템과 통신하도록 구성될 수 있고 동적으로 커플링되는 하나 이상의 프로세서(2602)를 포함할 수 있다. 프로세서(2602)는, 본 명세서에 기술된 바와 같이, 소비 트랜잭션의 유효성 검증의 일환으로서 잠금 해제 및 잠금 스크립트의 처리를 위해 이용될 수 있다. 이들 주변 서브시스템은 메모리 서브시스템(2608)과 파일/디스크 저장 서브시스템(2610)을 포함하는 저장 서브시스템(2606), 하나 이상의 사용자 인터페이스 입력 장치(2612), 하나 이상의 사용자 인터페이스 출력 장치(2614) 및 네트워크 인터페이스 서브시스템(2616)을 포함할 수 있다. 이러한 저장 서브시스템(2606)은 본 발명에서 설명된 트랜잭션과 연관된 상세와 같은 정보의 임시 저장이나 장기 저장을 위해 사용될 수 있다.

[0176] 버스 서브시스템(2604)은 컴퓨팅 장치(2600)의 다양한 구성 요소와 서브시스템이 의도한대로 서로 통신할 수 있게 하는 메커니즘을 제공할 수 있다. 버스 서브시스템(2604)은 단일 버스로서 개략적으로 도시되어 있지만, 버스 서브시스템의 대안적인 실시예는 다수의 버스를 이용할 수도 있다. 네트워크 인터페이스 서브시스템(2616)은 다른 컴퓨팅 장치와 네트워크에 대한 인터페이스를 제공할 수 있다. 네트워크 인터페이스 서브시스템(2616)은 컴퓨팅 장치(2600)로부터 데이터를 수신하고, 컴퓨팅 장치로부터 다른 시스템으로 데이터를 전송하기 위한 인터페이스로서 기능할 수 있다. 예를 들어, 네트워크 인터페이스 서브시스템(2616)은 데이터 기술자가 장치를 무선 네트워크에 연결하여, 데이터 기술자가 사용자 데이터 센터와 같은 원격 위치에 있는 동안 데이터를 송수신하게 할 수 있다. 버스 서브시스템(2604)은 본 발명의 감독 모델에 대한 상세, 검색어 등과 같은 데이터를 전달하기 위해 이용될 수 있고, 감독 모델의 출력을 하나 이상의 프로세서(2602)와 네트워크 인터페이스 서브시스템(2616)을 통한 판매자 및/또는 채권자에게 전달하는 데 이용될 수 있다.

[0177] 사용자 인터페이스 입력 장치(2612)는 키보드와 같은 하나 이상의 사용자 입력 장치와, 통합 마우스, 트랙볼, 터치 패드 또는 그래픽 태블릿과 같은 포인팅 장치와, 스캐너와, 바코드 스캐너와, 디스플레이에 통합된 터치스크린과, 음성 인식 시스템, 마이크와 같은 오디오 입력 장치, 및 다른 유형의 입력 장치를 포함할 수 있다. 일반적으로, 용어 "입력 장치"의 사용은 컴퓨팅 장치(2600)에 정보를 입력하기 위한 모든 가능한 유형의 장치와 메커니즘을 포함하도록 의도된다. 하나 이상의 사용자 인터페이스 출력 장치(2614)는 디스플레이 서브시스템, 프린터, 또는 오디오 출력 장치 등과 같은 비시각적 디스플레이를 포함할 수 있다. 디스플레이 서브시스템은 CRT(Cathode Ray Tube), LCD(Liquid Crystal Display), LED(Light Emitting Diode) 디스플레이 또는 프로젝션과 같은 평면 패널 장치나 다른 디스플레이 장치일 수 있다. 일반적으로, 용어 "출력 장치"의 사용은 컴퓨팅 장치(2600)로부터 정보를 출력하기 위한 모든 가능한 유형의 장치와 메커니즘을 포함하도록 의도된다. 하나 이상의 사용자 인터페이스 출력 장치(2614)는, 예를 들어, 그러한 상호 작용이 적절한 경우, 기술된 프로세스와 그의 변형을 수행하는 애플리케이션과의 사용자 상호 작용을 용이하게 하기 위한 사용자 인터페이스를 표시하기 위해 사용될 수 있다.

[0178] 저장 서브시스템(2606)은 본 발명의 적어도 하나의 실시예의 기능을 제공할 수 있는 기본 프로그래밍 및 데이터 구성을 저장하기 위한 컴퓨터 판독 가능 저장 매체를 제공할 수 있다. 하나 이상의 프로세서에 의해 실행될 때, 애플리케이션(프로그램, 코드 모듈, 명령어)은 본 발명의 하나 이상의 실시예의 기능을 제공할 수 있고, 저장 서브시스템(2606)에 저장될 수 있다. 이들 애플리케이션 모듈 또는 명령어는 하나 이상의 프로세서(2602)에 의해 실행될 수 있다. 저장 서브시스템(2606)은 본 발명에 따라 사용된 데이터를 저장하기 위한 저장소를 추가로 제공할 수 있다. 저장 서브시스템(2606)은 메모리 서브시스템(2608)과 파일/디스크 저장 서브시스템(2610)을 포함할 수 있다.

[0179] 메모리 서브시스템(2608)은 프로그램 실행 동안 명령어와 데이터를 저장하기 위한 메인 RAM(2618)과 고정 명령이 저장될 수 있는 ROM(2600)을 포함하는 다수의 메모리를 포함할 수 있다. 파일/디스크 저장 서브시스템(2610)은 프로그램과 데이터 파일을 위한 비일시적 영구(비휘발성) 스토리지를 제공할 수 있으며, 하드 디스크 드라이브, 플로피 디스크 드라이브와 관련 이동식 매체, CD-ROM 드라이브, 광학 드라이브, 이동식 미디어 카트리지 및 기타 유사한 저장 매체를 포함할 수 있다.

[0180] 컴퓨팅 장치(2600)는 적어도 하나의 로컬 시계(2624)를 포함할 수 있다. 로컬 시계(2624)는 특정 시작 날짜로부터 발생된 틱(tick)의 수를 나타내는 카운터일 수 있고, 컴퓨팅 장치(2600) 내에 일체로 내장될 수 있다. 로컬 시계(2624)는 컴퓨팅 장치(2600)와 거기에 포함된 모든 서브시스템에 대한 프로세서에서의 데이터 전송을 특정 클록 펄스로 동기화하는 데 사용될 수 있고, 컴퓨팅 장치(2600)와 데이터 센터 내의 다른 시스템간의 동기화 동작(synchronous operation)을 조정하는 데 사용될 수 있다. 일 실시예에서, 로컬 시계(2624)는 원자 시계(atomic clock)이다. 다른 실시예에서, 로컬 시계는 프로그램 가능 간격 타이머(programmable interval timer)이다.

[0181] 컴퓨팅 장치(2600)는 휴대용 컴퓨터 장치, 태블릿 컴퓨터, 워크 스테이션 또는 후술하는 임의의 다른 장치를 포함하는 다양한 유형일 수 있다. 또한, 컴퓨팅 장치(2600)는 하나 이상의 포트(예컨대, USB, 헤드폰 잭, 라이트닝 커넥터 등)를 통해 컴퓨팅 장치(2600)에 연결될 수 있는 다른 장치를 포함할 수 있다. 컴퓨팅 장치(2600)에 연결될 수 있는 장치는 광섬유 커넥터를 수용하도록 구성된 복수의 포트를 포함할 수 있다. 따라서, 이 장치는 광학 신호를, 프로세싱을 위해 장치를 컴퓨팅 장치(2600)에 연결하는 포트를 통해 전송할 수 있는 전기 신호로 변환하도록 구성될 수 있다. 컴퓨터와 네트워크의 끊임없이 변화하는 특성으로 인해, 도 8에 도시된 컴퓨팅 장치(2600)에 대한 설명은 장치의 바람직한 실시예를 설명하기 위한 목적의 특정 예로서만 의도된 것이다. 도 8에 도시된 시스템보다 더 많거나 적은 구성 요소를 구비하는 많은 다른 구성이 가능하다.

[0182] 따라서, 명세서 및 도면은 제한적인 의미가 아니라 예시적인 것으로 간주되어야 한다. 그러나, 청구 범위에 기재된 본 발명의 범주를 벗어나지 않고 다양한 수정 및 변경이 이루어질 수 있음이 명백할 것이다. 마찬가지로, 다른 변형예도 본 발명의 범주 내에 포함된다. 따라서, 본 발명의 기술은 다양한 수정과 대안적인 구성에 영향을 받을 수 있지만, 그 예시된 특정 실시예가 도면에 도시되어 있고 위에 상세하게 설명되어 있다. 그러나, 본 발명을 특정 형태나 개시된 형태로 한정하려는 의도는 없지만, 그 반대로, 첨부된 청구 범위에 정의되어 있는 바와 같은 본 발명의 범주 내에 포함되는 모든 변형, 대안적인 구성 및 등가물을 포괄하는 의도가 있음을 이해해야 한다.

[0183] 본 발명의 실시예를 설명하는 맥락에서(특히, 다음의 청구 범위의 맥락에서) 용어 "a" 및 "an" 및 "the" 및 유사한 지시어의 사용은, 문맥 상 달리 명시되거나 모순되지 않는 한, 단수와 복수를 모두 포함하는 것으로 해석되어야 한다. "구비하는", "갖는", "포함하는" 및 "함유하는"이라는 용어는, 달리 언급되지 않는 한, 개방형 용어(즉, "포함하지만 이것으로 제한되지 않는"을 의미함)로 해석되어야 한다. "연결된"이라는 용어는 물리적인 연결을 수정하지 않고 지칭할 때, 비록 어떤 간섭이 있더라도, 부분적으로 또는 전체적으로 함께 포함되거나, 연결되거나 결합되는 것으로 해석되어야 한다. 본 발명에서 값의 범위의 언급은, 달리 명시되지 않는 한, 그 범위 내에 속하는 각각의 개별 값을 개별적으로 지칭하는 속기법으로서 기능하고, 각각의 개별 값이 마치 개별적으로 인용되는 것처럼 명세서에 통합되는 것으로 의도된다. 용어 "세트"(예컨대, "아이템 세트") 또는 "서브세트"의 사용은, 문맥상 달리 언급되거나 모순되지 않는 한, 하나 이상의 멤버를 포함하는 비어 있지 않은 집합으로 해석되어야 한다. 또한, 대응하는 세트의 "서브세트"라는 용어는, 문맥상 달리 언급되거나 모순되지 않는 한, 반드시 대응하는 세트의 적절한 서브세트를 나타내는 것은 아니지만, 서브세트와 대응하는 세트는 동일할 수 있다.

[0184] 문맥상 명백하게 다르게 명시되거나 명백하게 모순되지 않는 한, "A, B, 및 C 중 적어도 하나" 또는 "A, B 및 C 중 적어도 하나"라는 형태의 어구와 같은 조합 언어는 아이템, 용어 등이 A 또는 B 또는 C이거나, A 및 B 및 C의 세트의 임의의 비어 있지 않은 서브세트일 수 있음을 제시하기 위해 일반적으로 사용되는 문맥에 따라 달리 이해된다. 예를 들어, 3개의 구성원으로 이루어진 세트의 예시적인 예에서, "A, B, 및 C 중 적어도 하나"와 "A, B 및 C 중 적어도 하나"와 같은 조합 문구는 {A}, {B}, {C}, {A, B}, {A, C}, {B, C}, {A, B, C}의 세트 중 임의의 것을 지칭한다. 따라서, 이러한 조합 언어는 일반적으로 특정 실시예가 A 중 적어도 하나, B 중 적어도 하나 및 C 중 적어도 하나가 각각 존재해야 함을 의미하는 것으로 의도되지 않는다.

[0185] 설명된 프로세스의 동작은, 문맥상 달리 표시되거나 달리 명확하게 모순되지 않는 한, 임의의 적합한 순서로 수행될 수 있다. 설명된 프로세스(또는 그의 변형 및/또는 조합)는 실행 가능한 명령어로 구성된 하나 이상의 컴

퓨터 시스템의 제어 하에 수행될 수 있고, 하드웨어 또는 이들의 조합에 의해, 하나 이상의 프로세서에서 집합적으로 실행하는 코드(예컨대, 실행 가능한 명령어, 하나 이상의 컴퓨터 프로그램 또는 하나 이상의 애플리케이션)로서 구현될 수 있다. 코드는, 예를 들어, 하나 이상의 프로세서에 의해 실행 가능한 복수의 명령어를 포함하는 컴퓨터 프로그램의 형태로 컴퓨터 판독 가능 저장 매체에 저장될 수 있다. 컴퓨터 판독 가능 저장 매체는 비일시적일 수 있다.

[0186] 제공된 임의의 및 모든 예나 예시적인 언어(예컨대, "예를 들어")의 사용은 단지 본 발명의 실시예를 더 잘 설명하기 위한 것이며, 달리 청구되지 않는 한 본 발명의 범주에 제한을 두려는 것은 아니다. 본 명세서의 어떤 언어도 본 발명의 실시에 필수적인 것으로서, 청구되지 않은 요소를 나타내는 것으로 해석되어서는 안 된다.

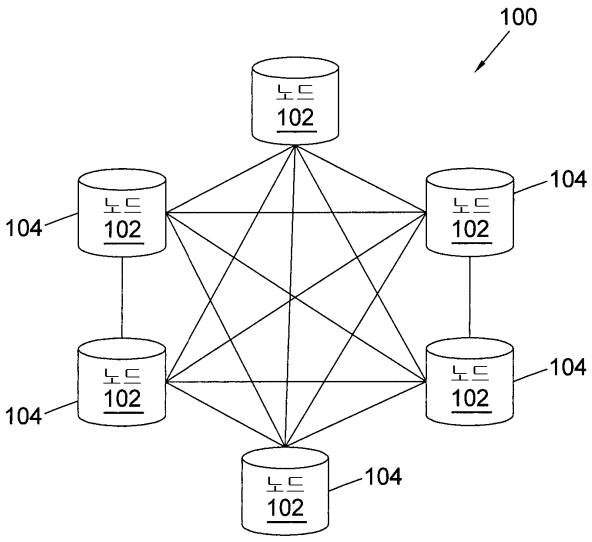
[0187] 본 발명을 수행하기 위해 본 발명자에게 알려진 최상의 모드를 포함하여 본 발명의 실시예들이 설명된다. 이들 실시예의 변형은 전술한 설명을 읽으면 당업자에게 명백해질 것이다. 본 발명자는 당업자가 적절한 변형을 채택할 것으로 기대하고, 또한 본 발명의 실시예에 대해 구체적으로 설명된 것과는 다르게 실시하고자 한다. 따라서, 본 발명의 범주는, 적용 가능한 법률에 의해 허용되는 바와 같이, 여기에 첨부된 청구 범위에 인용된 주제의 모든 수정과 등가물을 포함한다. 또한, 이들의 모든 가능한 변형에서, 상술한 요소들의 임의의 조합은, 달리 명시되거나 문맥상 명백하게 모순되지 않는 한, 본 발명의 범주에 포함된다.

[0188] 인용된 간행물, 특허 출원 및 특허를 포함한 모든 참고 문헌은 각각의 참고 문헌이 개별적, 구체적으로 통합되고, 전체적으로 명시되는 것과 동일한 정도로 참고로서 포함되며 전체적으로 설명되었다.

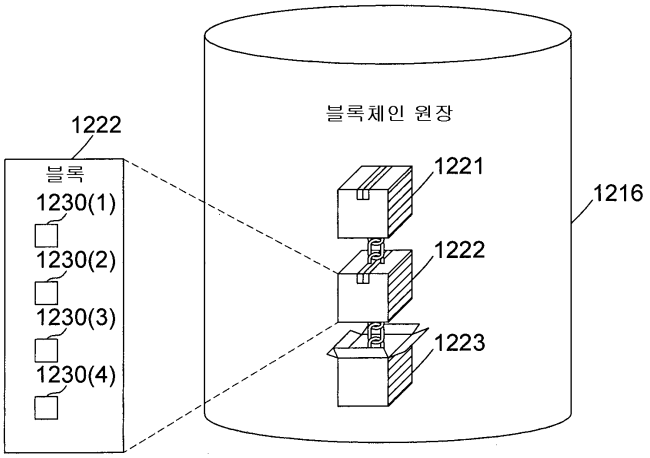
[0189] 위에 언급된 실시예는 본 발명을 제한하기보다는 예시하는 것이며, 당업자라면 첨부된 청구 범위에 의해 한정된 바와 같이, 본 발명의 범주를 벗어나지 않고도 많은 대안적인 실시예를 설계할 수 있다는 것에 주목해야 한다. 청구 범위에서, 괄호 안의 모든 참조 부호는 청구 범위를 제한하는 것으로 해석되지 않아야 한다. "포함하는(comprising)", "포함하다(comprises)" 등의 단어는 청구항 또는 명세서 전체에 열거된 것 이외의 요소나 단계의 존재를 배제하지 않는다. 본 명세서에서, "포함하다"는 "구성하다 또는 이루어지다"를 의미하고, "포함하는"은 "구성하는 또는 이루어지는"을 의미한다. 요소의 단일 참조는 그러한 요소의 복수 참조를 배제하지 않으며, 그 반대도 마찬가지이다. 본 발명은 몇 개의 별개의 요소를 포함하는 하드웨어와 적절히 프로그래밍된 컴퓨터에 의해 구현될 수 있다. 여러 수단을 열거하는 장치 청구항에서, 이들 수단 중 일부는 하나의 동일한 하드웨어 항목에 의해 구현될 수 있다. 특정 조치가 서로 다른 종속항에서 인용된다는 사실은 이들 조치의 조합이 유리하게 사용될 수 없다는 것을 나타내는 것은 아니다.

도면

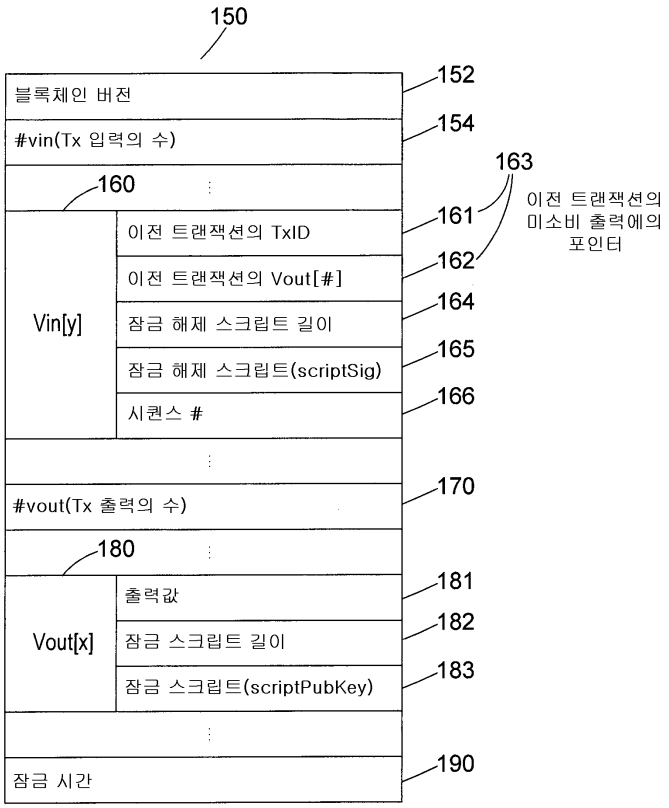
도면1a



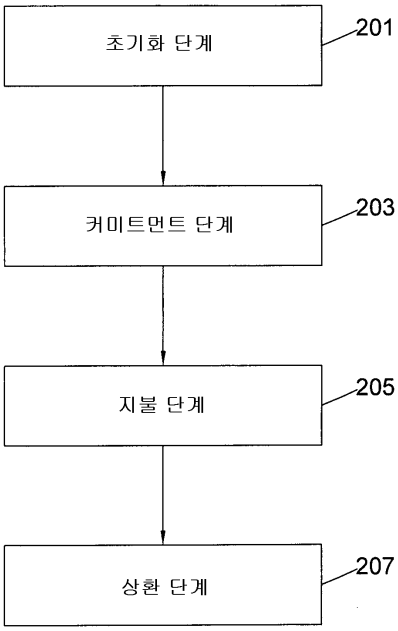
도면1b


블록체인 원장
1222
블록
1230(1)
1230(2)
1230(3)
1230(4)
1221
1222
1223
1216

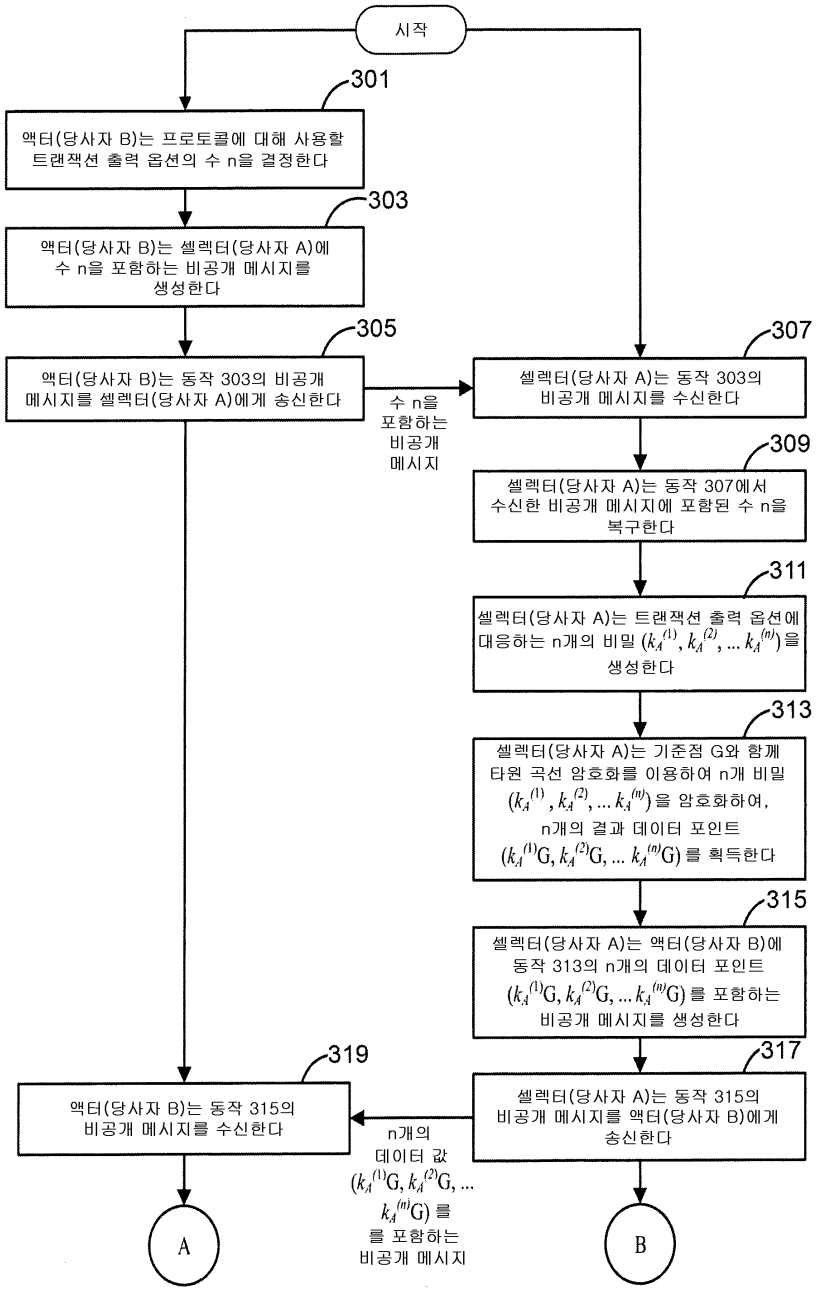
도면1c


150
블록체인 버전
152
#vin(Tx 입력의 수)
154
160
163
이전 트랜잭션의 미소비 출력에의 포인터
Vin[y]
이전 트랜잭션의 TxID
161
이전 트랜잭션의 Vout[#]
162
잠금 해제 스크립트 길이
164
잠금 해제 스크립트(scriptSig)
165
시퀀스 #
166
#vout(Tx 출력의 수)
170
180
Vout[x]
출력값
181
잠금 스크립트 길이
182
잠금 스크립트(scriptPubKey)
183
잠금 시간
190

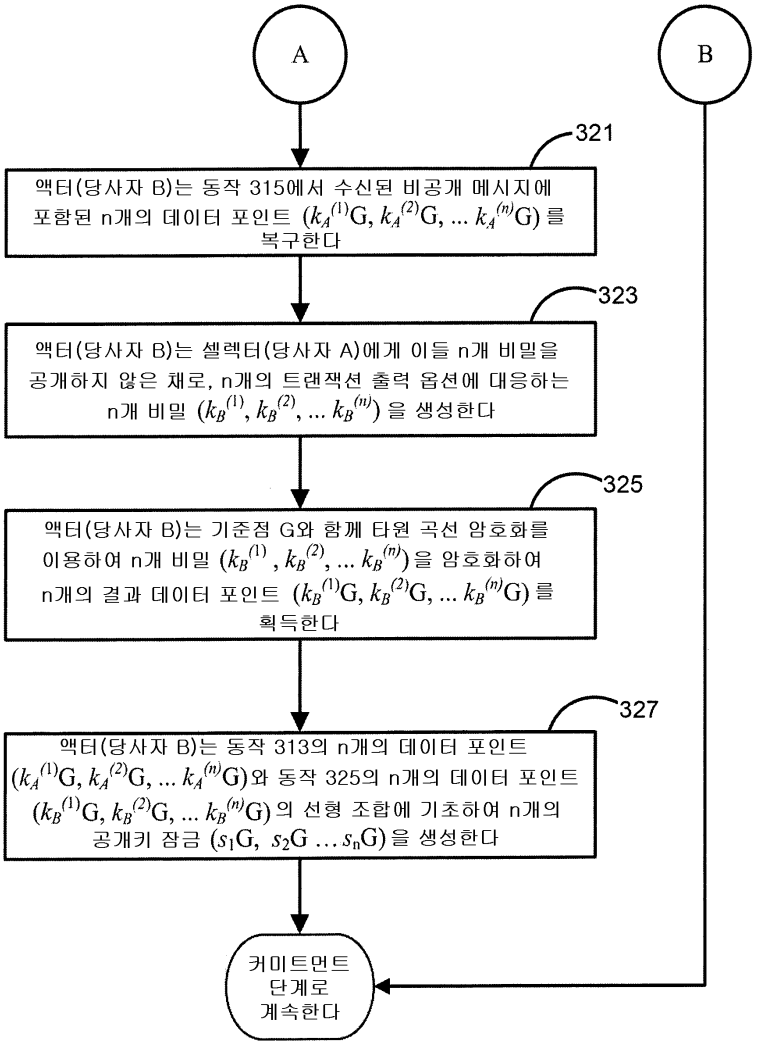
도면2



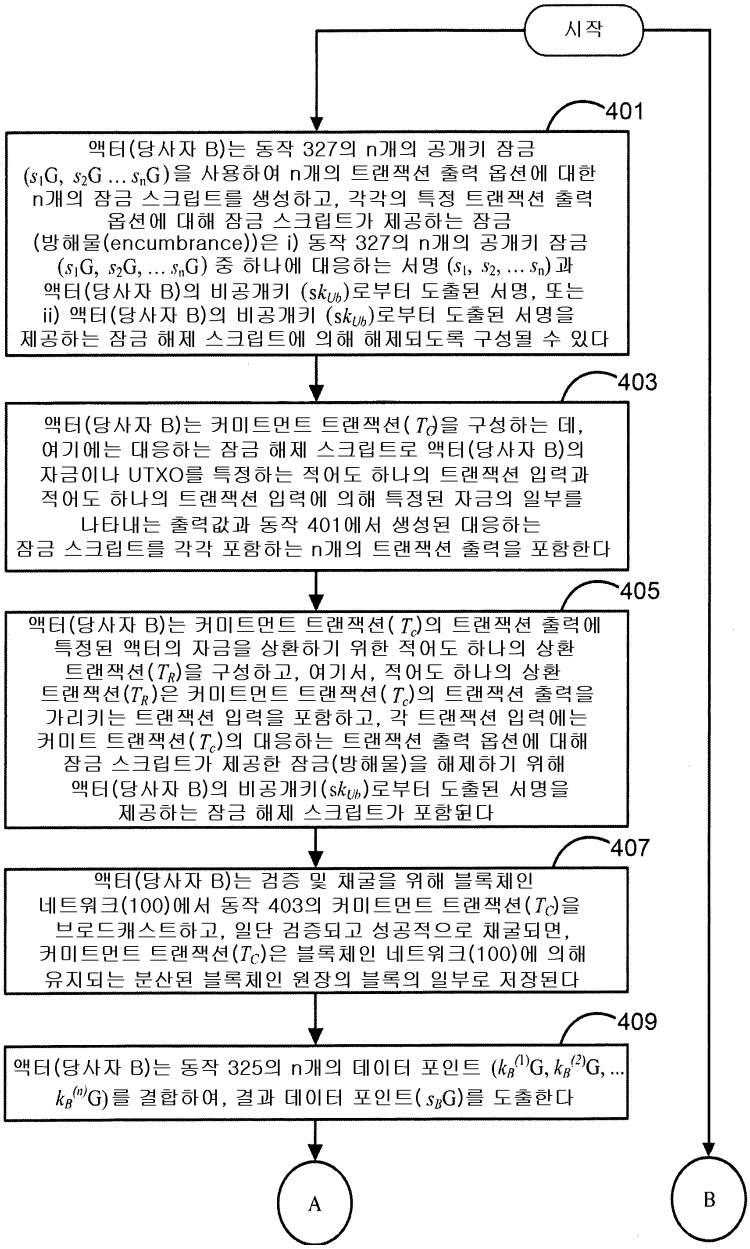
도면3a


시작
301
액터(당사자 B)는 프로토콜에 대해 사용할 트랜잭션 출력 옵션의 수 n을 결정한다
303
액터(당사자 B)는 셀렉터(당사자 A)에 수 n을 포함하는 비공개 메시지를 생성한다
305
액터(당사자 B)는 동작 303의 비공개 메시지를 셀렉터(당사자 A)에게 송신한다
수 n을 포함하는 비공개 메시지
307
셀렉터(당사자 A)는 동작 303의 비공개 메시지를 수신한다
309
셀렉터(당사자 A)는 동작 307에서 수신한 비공개 메시지에 포함된 수 n을 복구한다
311
셀렉터(당사자 A)는 트랜잭션 출력 옵션에 대응하는 n개의 비밀 $(k_A^{(1)}, k_A^{(2)}, \ldots k_A^{(n)})$을 생성한다
313
셀렉터(당사자 A)는 기준점 G와 함께 타원 곡선 암호화를 이용하여 n개 비밀 $(k_A^{(1)}, k_A^{(2)}, \ldots k_A^{(n)})$을 암호화하여, n개의 결과 데이터 포인트 $(k_A^{(1)}G, k_A^{(2)}G, \ldots k_A^{(n)}G)$를 획득한다
315
셀렉터(당사자 A)는 액터(당사자 B)에 동작 313의 n개의 데이터 포인트 $(k_A^{(1)}G, k_A^{(2)}G, \ldots k_A^{(n)}G)$를 포함하는 비공개 메시지를 생성한다
317
셀렉터(당사자 A)는 동작 315의 비공개 메시지를 액터(당사자 B)에게 송신한다
319
액터(당사자 B)는 동작 315의 비공개 메시지를 수신한다
n개의 데이터 값 $(k_A^{(1)}G, k_A^{(2)}G, \ldots k_A^{(n)}G)$를 를 포함하는 비공개 메시지
A
B

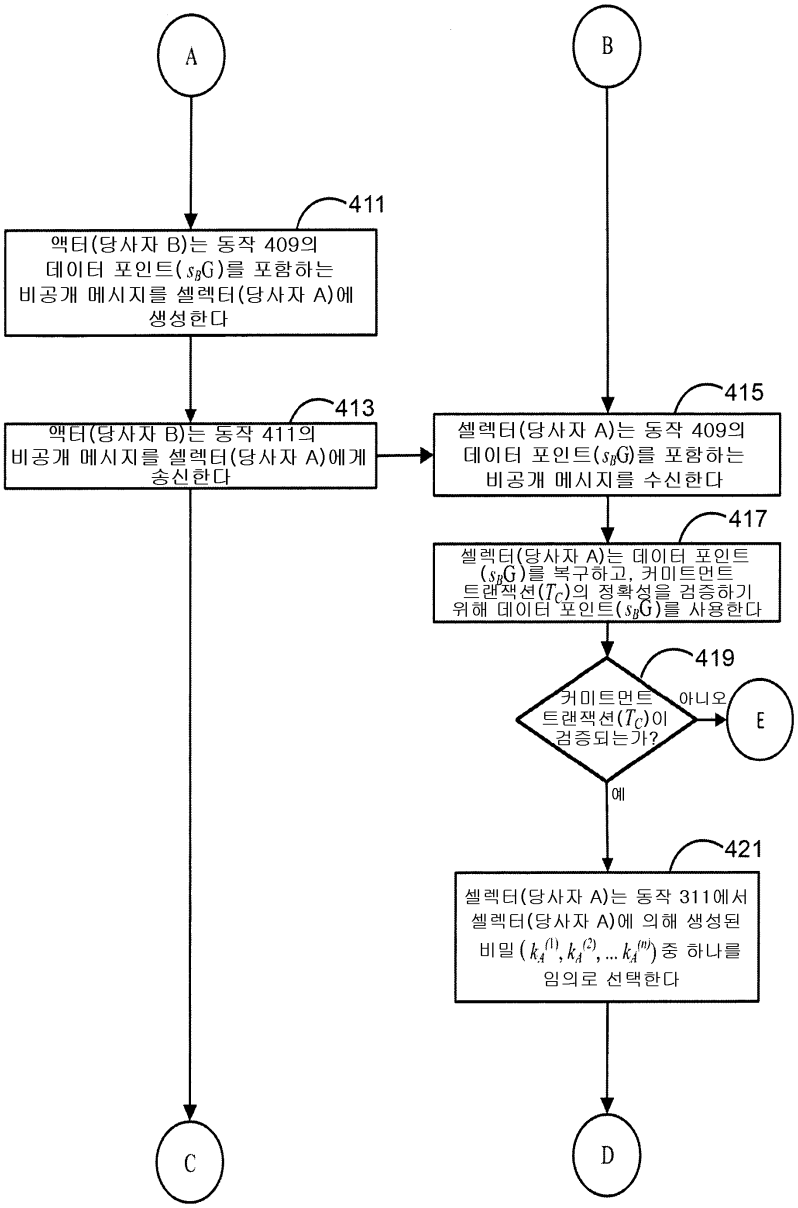
도면3b


A
B
321
액터(당사자 B)는 동작 315에서 수신된 비공개 메시지에 포함된 n개의 데이터 포인트 $(k_A^{(1)}G, k_A^{(2)}G, \ldots k_A^{(n)}G)$ 를 복구한다
323
액터(당사자 B)는 셀렉터(당사자 A)에게 이들 n개 비밀을 공개하지 않은 채로, n개의 트랜잭션 출력 옵션에 대응하는 n개 비밀 $(k_B^{(1)}, k_B^{(2)}, \ldots k_B^{(n)})$ 을 생성한다
325
액터(당사자 B)는 기준점 G와 함께 타원 곡선 암호화를 이용하여 n개 비밀 $(k_B^{(1)}, k_B^{(2)}, \ldots k_B^{(n)})$ 을 암호화하여 n개의 결과 데이터 포인트 $(k_B^{(1)}G, k_B^{(2)}G, \ldots k_B^{(n)}G)$ 를 획득한다
327
액터(당사자 B)는 동작 313의 n개의 데이터 포인트 $(k_A^{(1)}G, k_A^{(2)}G, \ldots k_A^{(n)}G)$ 와 동작 325의 n개의 데이터 포인트 $(k_B^{(1)}G, k_B^{(2)}G, \ldots k_B^{(n)}G)$ 의 선형 조합에 기초하여 n개의 공개키 잠금 $(s_1G, s_2G \ldots s_nG)$ 을 생성한다
커미트먼트 단계로 계속한다

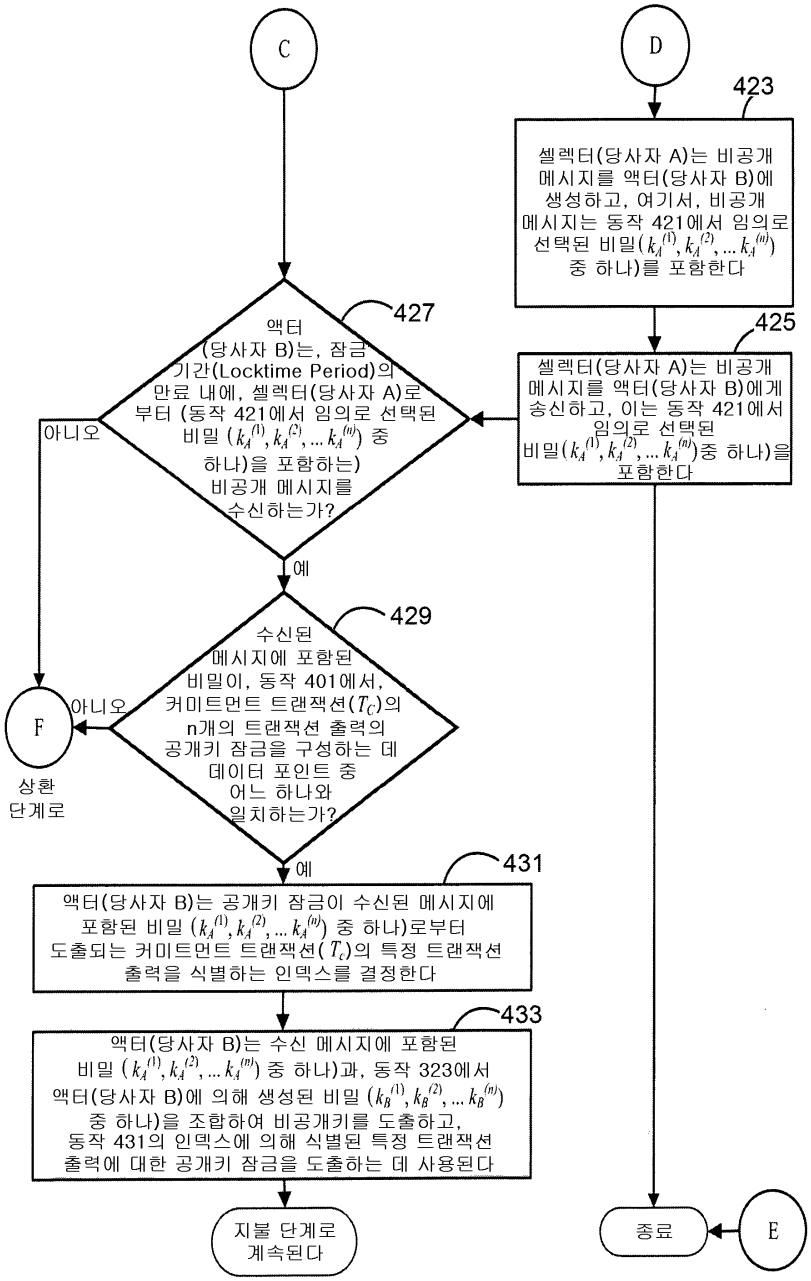
도면4a


시작
401
액터(당사자 B)는 동작 327의 n개의 공개키 잠금 (s_1G, s_2G ... s_nG)을 사용하여 n개의 트랜잭션 출력 옵션에 대한 n개의 잠금 스크립트를 생성하고, 각각의 특정 트랜잭션 출력 옵션에 대해 잠금 스크립트가 제공하는 잠금 (방해물(encumbrance))은 i) 동작 327의 n개의 공개키 잠금 (s_1G, s_2G, ... s_nG) 중 하나에 대응하는 서명 (s_1, s_2, ... s_n)과 액터(당사자 B)의 비공개키 (sk_{Ub})로부터 도출된 서명, 또는 ii) 액터(당사자 B)의 비공개키 (sk_{Ub})로부터 도출된 서명을 제공하는 잠금 해제 스크립트에 의해 해제되도록 구성될 수 있다
403
액터(당사자 B)는 커미트먼트 트랜잭션(T_C)을 구성하는 데, 여기에는 대응하는 잠금 해제 스크립트로 액터(당사자 B)의 자금이나 UTXO를 특정하는 적어도 하나의 트랜잭션 입력과 적어도 하나의 트랜잭션 입력에 의해 특정된 자금의 일부를 나타내는 출력값과 동작 401에서 생성된 대응하는 잠금 스크립트를 각각 포함하는 n개의 트랜잭션 출력을 포함한다
405
액터(당사자 B)는 커미트먼트 트랜잭션(T_c)의 트랜잭션 출력에 특정된 액터의 자금을 상환하기 위한 적어도 하나의 상환 트랜잭션(T_R)을 구성하고, 여기서, 적어도 하나의 상환 트랜잭션(T_R)은 커미트먼트 트랜잭션(T_c)의 트랜잭션 출력을 가리키는 트랜잭션 입력을 포함하고, 각 트랜잭션 입력에는 커미트 트랜잭션(T_c)의 대응하는 트랜잭션 출력 옵션에 대해 잠금 스크립트가 제공한 잠금(방해물)을 해제하기 위해 액터(당사자 B)의 비공개키(sk_{Ub})로부터 도출된 서명을 제공하는 잠금 해제 스크립트가 포함된다
407
액터(당사자 B)는 검증 및 채굴을 위해 블록체인 네트워크(100)에서 동작 403의 커미트먼트 트랜잭션(T_C)을 브로드캐스트하고, 일단 검증되고 성공적으로 채굴되면, 커미트먼트 트랜잭션(T_C)은 블록체인 네트워크(100)에 의해 유지되는 분산된 블록체인 원장의 블록의 일부로 저장된다
409
액터(당사자 B)는 동작 325의 n개의 데이터 포인트 ($k_B^{(1)}$G, $k_B^{(2)}$G, ... $k_B^{(m)}$G)를 결합하여, 결과 데이터 포인트(s_BG)를 도출한다
A
B

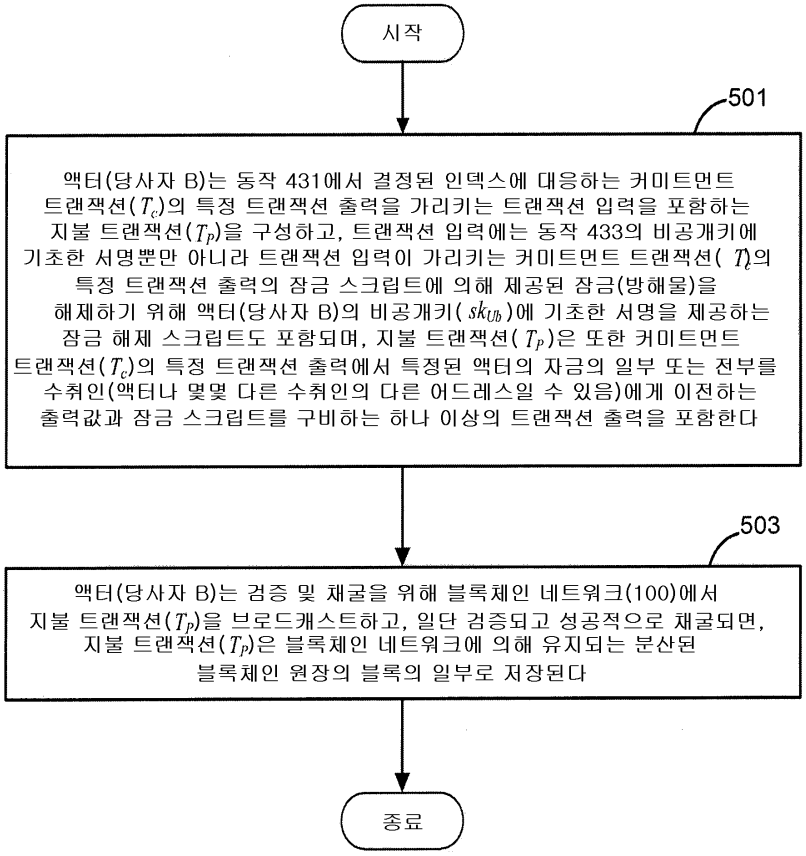
도면4b


A
B
411
액터(당사자 B)는 동작 409의 데이터 포인트(s_BG)를 포함하는 비공개 메시지를 셀렉터(당사자 A)에 생성한다
413
액터(당사자 B)는 동작 411의 비공개 메시지를 셀렉터(당사자 A)에게 송신한다
415
셀렉터(당사자 A)는 동작 409의 데이터 포인트(s_BG)를 포함하는 비공개 메시지를 수신한다
417
셀렉터(당사자 A)는 데이터 포인트(s_BG)를 복구하고, 커미트먼트 트랜잭션(T_C)의 정확성을 검증하기 위해 데이터 포인트(s_BG)를 사용한다
419
커미트먼트 트랜잭션(T_C)이 검증되는가?
아니오
E
예
421
셀렉터(당사자 A)는 동작 311에서 셀렉터(당사자 A)에 의해 생성된 비밀 ($k_A^{(1)}, k_A^{(2)}, \ldots k_A^{(m)}$) 중 하나를 임의로 선택한다
C
D

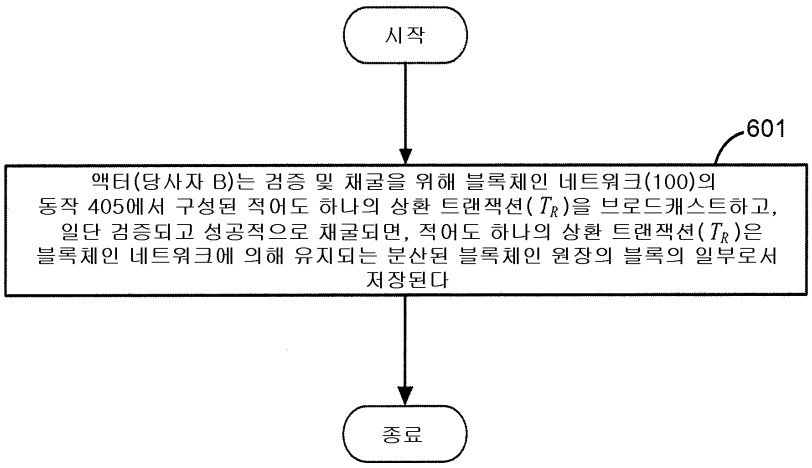
도면4c


C
D
423
셀렉터(당사자 A)는 비공개 메시지를 액터(당사자 B)에 생성하고, 여기서, 비공개 메시지는 동작 421에서 임의로 선택된 비밀($k_A^{(1)}, k_A^{(2)}, \ldots k_A^{(n)}$) 중 하나)를 포함한다
425
셀렉터(당사자 A)는 비공개 메시지를 액터(당사자 B)에게 송신하고, 이는 동작 421에서 임의로 선택된 비밀($k_A^{(1)}, k_A^{(2)}, \ldots k_A^{(n)}$)중 하나)을 포함한다
427
액터 (당사자 B)는, 잠금 기간(Locktime Period)의 만료 내에, 셀렉터(당사자 A)로부터 (동작 421에서 임의로 선택된 비밀 ($k_A^{(1)}, k_A^{(2)}, \ldots k_A^{(n)}$) 중 하나)을 포함하는) 비공개 메시지를 수신하는가?
아니오
예
429
수신된 메시지에 포함된 비밀이, 동작 401에서, 커미트먼트 트랜잭션(T_C)의 n개의 트랜잭션 출력의 공개키 잠금을 구성하는 데 데이터 포인트 중 어느 하나와 일치하는가?
아니오
F
상환 단계로
예
431
액터(당사자 B)는 공개키 잠금이 수신된 메시지에 포함된 비밀 ($k_A^{(1)}, k_A^{(2)}, \ldots k_A^{(n)}$) 중 하나)로부터 도출되는 커미트먼트 트랜잭션(T_c)의 특정 트랜잭션 출력을 식별하는 인덱스를 결정한다
433
액터(당사자 B)는 수신 메시지에 포함된 비밀 ($k_A^{(1)}, k_A^{(2)}, \ldots k_A^{(n)}$) 중 하나)과, 동작 323에서 액터(당사자 B)에 의해 생성된 비밀 ($k_B^{(1)}, k_B^{(2)}, \ldots k_B^{(n)}$) 중 하나)을 조합하여 비공개키를 도출하고, 동작 431의 인덱스에 의해 식별된 특정 트랜잭션 출력에 대한 공개키 잠금을 도출하는 데 사용된다
지불 단계로 계속된다
종료
E

도면5

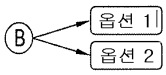

시작
501
액터(당사자 B)는 동작 431에서 결정된 인덱스에 대응하는 커미트먼트 트랜잭션(T_c)의 특정 트랜잭션 출력을 가리키는 트랜잭션 입력을 포함하는 지불 트랜잭션(T_p)을 구성하고, 트랜잭션 입력에는 동작 433의 비공개키에 기초한 서명뿐만 아니라 트랜잭션 입력이 가리키는 커미트먼트 트랜잭션(T_c)의 특정 트랜잭션 출력의 잠금 스크립트에 의해 제공된 잠금(방해물)을 해제하기 위해 액터(당사자 B)의 비공개키(sk_{cb})에 기초한 서명을 제공하는 잠금 해제 스크립트도 포함되며, 지불 트랜잭션(T_p)은 또한 커미트먼트 트랜잭션(T_c)의 특정 트랜잭션 출력에서 특정된 액터의 자금의 일부 또는 전부를 수취인(액터나 몇몇 다른 수취인의 다른 어드레스일 수 있음)에게 이전하는 출력값과 잠금 스크립트를 구비하는 하나 이상의 트랜잭션 출력을 포함한다
503
액터(당사자 B)는 검증 및 채굴을 위해 블록체인 네트워크(100)에서 지불 트랜잭션(T_p)을 브로드캐스트하고, 일단 검증되고 성공적으로 채굴되면, 지불 트랜잭션(T_p)은 블록체인 네트워크에 의해 유지되는 분산된 블록체인 원장의 블록의 일부로 저장된다
종료

도면6

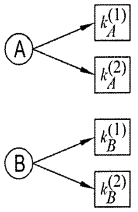

시작
601
액터(당사자 B)는 검증 및 채굴을 위해 블록체인 네트워크(100)의 동작 405에서 구성된 적어도 하나의 상환 트랜잭션(T_R)을 브로드캐스트하고, 일단 검증되고 성공적으로 채굴되면, 적어도 하나의 상환 트랜잭션(T_R)은 블록체인 네트워크에 의해 유지되는 분산된 블록체인 원장의 블록의 일부로서 저장된다
종료

도면7

301 - 당사자 B는 n개의 트랜잭션 출력 옵션의 숫자를 결정한다

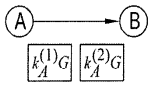


311 - 당사자 A는 n개의 트랜잭션 출력 옵션에 대한 n개의 비밀을 생성한다

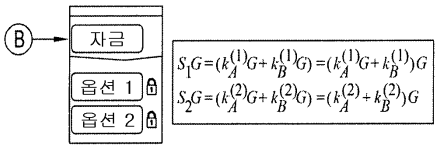


323 - 당사자 B는 n개의 트랜잭션 출력 옵션을 위한 n개의 비밀을 생성한다

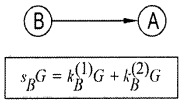
317 - 당사자 A는 동작 311에서 생성 n개의 비밀의 암호화 버전을 당사자 B로 송신한다



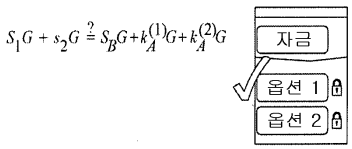
327 - 당사자 B는 비밀의 조합에 기초한 n개의 공개키 잠금을 준비한다



413 - 당사자 B는 동작 311에서 생성된 n개의 비밀의 암호화 조합을 당사자 A로 송신한다

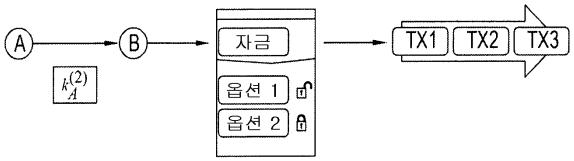


417-419 - 당사자 A는 블록체인에 저장된 커미트먼트 트랜잭션의 정확도를 확인한다



421-427 - 당사자 A는 동작 311에서 생성된 비밀 중 하나를 임의로 선택하고, 그 임의로 선택된 비밀을 당사자 B에게 송신한다

431-501 - 당사자 B는 비공개키를 사용하여 블록체인에 저장하기 위해 검증되고 채굴되는 지불 트랜잭션의 잠금 해제 스크립트에 대한 서명을 구성한다



도면8