(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2020년12월23일
(11) 등록번호 10-2193551
(24) 등록일자 2020년12월15일

(51) 국제특허분류(Int. Cl.)
H04L 9/00 (2006.01) *H04L 9/32* (2006.01)
(52) CPC특허분류
H04L 9/008 (2013.01)
H04L 9/3218 (2013.01)
(21) 출원번호 10-2019-7022196
(22) 출원일자(국제) 2018년12월21일
심사청구일자 2019년08월13일
(85) 번역문제출일자 2019년07월26일
(65) 공개번호 10-2020-0079217
(43) 공개일자 2020년07월02일
(86) 국제출원번호 PCT/CN2018/122573
(87) 국제공개번호 WO 2019/072302
국제공개일자 2019년04월18일
(56) 선행기술조사문헌
CN108764874 A
CN109035029 A
US20160358165 A1

(73) 특허권자
어드밴스드 뉴 테크놀로지스 씨오., 엘티디.
케이만 군도, 그랜드 케이만 케이와이1-9008, 조지 타운, 27 하스피탈 로드, 케이만 코포레이트 센터
(72) 발명자
장 웬빈
중국 저지앙 311121 항저우 유 항 디스트릭트 웨스트 웬 이 로드 넘버 969 빌딩 3 알리바바 그룹 리갈 디파트먼트 5층
마 바올리
중국 저지앙 311121 항저우 유 항 디스트릭트 웨스트 웬 이 로드 넘버 969 빌딩 3 알리바바 그룹 리갈 디파트먼트 5층
마 후안유
중국 저지앙 311121 항저우 유 항 디스트릭트 웨스트 웬 이 로드 넘버 969 빌딩 3 알리바바 그룹 리갈 디파트먼트 5층
(74) 대리인
김태홍, 김진희

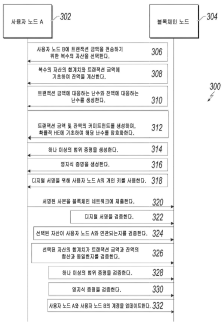
전체 청구항 수 : 총 27 항 심사관 : 양종필

(54) 발명의 명칭 **제네릭 계정 모델 및 준동형 암호화에 기반한 블록체인 데이터 보호**

(57) 요 약

본 명세서의 실시예는 상기 트랜잭션과 연관된 트랜잭션 데이터를 수신하는 단계로서, 트랜잭션 데이터는, 복수의 자산을 나타내는 데이터, 제1 난수와 트랜잭션의 트랜잭션 금액을 숨기는 제1 커미트먼트, 제2 난수와 잔액을 숨기는 제2 커미트먼트, 선형 결정적 준동형 암호화(HE) 스킴에 기초하여 제2 노드의 공개 키에 의해 양자 모두 암호화된 트랜잭션 금액 및 제3 난수, 선형 결정적 HE 스킴에 기초하여 제1 노드의 공개 키에 의해 양자 모두 암호화된 잔액 및 제4 난수, 및 영지식 증명(ZKP)을 포함하는 것인, 수신하는 단계; ZKP에 기초하여, 제1 난수가 제3 난수와 동일하고, 제2 난수가 제4 난수와 동일하며, 제1 커미트먼트에 숨겨진 트랜잭션 금액이 제 2 노드의 공개 키에 의해 암호화된 트랜잭션 금액과 동일한지를 결정하는 것에 기초하여, 트랜잭션이 유효한지를 결정하는 단계를 포함한다.

대 표 도



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

명 세 서

청구범위

청구항 1

블록체인 네트워크 내의 제1 노드와 제2 노드 사이의 트랜잭션(transaction)을 확인(validating)하기 위해 합의 노드(consensus node)에 의해 수행되는 컴퓨터 구현(computer-implemented) 방법에 있어서,

상기 트랜잭션과 연관된 트랜잭션 데이터를 수신하는 단계 - 상기 트랜잭션 데이터는 복수의 자산을 나타내는 데이터, 제1 난수(random number)와 상기 트랜잭션의 트랜잭션 금액(amount)을 숨기는 제1 커미트먼트(commitment), 제2 난수와 상기 복수의 자산의 합계치로부터 상기 트랜잭션 금액을 차감하는 것에 기초하여 계산된 잔액(change)을 숨기는 제2 커미트먼트, 선형 결정적 준동형 암호화(homomorphic encryption: HE) 스킴에 기초하여 상기 제2 노드의 공개 키에 의해 양자 모두 암호화된 상기 트랜잭션 금액 및 제3 난수, 상기 선형 결정적 HE 스킴에 기초하여 상기 제1 노드의 공개 키에 의해 양자 모두 암호화된 상기 잔액 및 제4 난수, 하나 이상의 범위 증명(range proof), 영지식 증명(zero-knowledge proof: ZKP), 및 상기 제1 노드의 공개 키에 대응하는 개인 키에 기초하여 생성된 디지털 서명을 포함함 - ;

상기 제1 노드의 공개 키에 기초하여 상기 디지털 서명을 검증하는 단계;

상기 하나 이상의 범위 증명이 상기 트랜잭션 금액과 상기 잔액 각각이 0 이상임을 증명한다고 결정하는 단계;

상기 복수의 자산의 합계치가 상기 트랜잭션 금액과 상기 잔액의 합산(sum)과 같다고 결정하는 단계; 및

상기 ZKP에 기초하여, 상기 제1 난수가 상기 제3 난수와 동일하고, 상기 제2 난수가 상기 제4 난수와 동일하며, 상기 제1 커미트먼트에 숨겨진 상기 트랜잭션 금액이 상기 제 2 노드의 공개 키에 의해 암호화된 상기 트랜잭션 금액과 동일하다고 결정함으로써, 상기 트랜잭션이 유효하다고 결정하는 단계

를 포함하는, 컴퓨터 구현 방법.

청구항 2

제1항에 있어서,

상기 트랜잭션은 상기 제1 노드와 연관된 계정과 상기 제2 노드와 연관된 계정 사이에 행해지며,

상기 방법은,

상기 트랜잭션이 유효하다고 결정한 후에, 상기 트랜잭션 금액과 상기 잔액에 기초하여 상기 제1 노드와 연관된 계정과 상기 제2 노드와 연관된 계정을 업데이트하는 단계

를 더 포함하는, 컴퓨터 구현 방법.

청구항 3

제1항에 있어서,

상기 복수의 자산 각각은 자산 유형, 커미트먼트에 숨겨진 자산 값, 및 상기 커미트먼트를 생성하는데 사용되는 난수 중 하나 이상과 연관되는 것인, 컴퓨터 구현 방법.

청구항 4

제3항에 있어서,

상기 복수의 자산 각각이 동일한 자산 유형과 연관된다고 결정하는 단계

를 더 포함하는, 컴퓨터 구현 방법.

청구항 5

제3항에 있어서,

상기 제1 커미트먼트, 상기 제2 커미트먼트, 및 상기 자산 값을 숨기는 커미트먼트는 준동형(homomorphic)의 커미트먼트 스킴에 기초하여 생성되고,

상기 복수의 자산의 합계치가 상기 트랜잭션 금액과 상기 잔액의 합산과 같다고 결정하는 단계는, 상기 커미트먼트 스킴의 준동형사상(homomorphism)에 기초하여 행해지는 것인, 컴퓨터 구현 방법.

청구항 6

제1항에 있어서,

상기 선형 결정적 HE 스킴은, 확률적(probabilistic) HE 스킴과 연관된 난수를 고정된 수(fixed number)로 변경하는 것에 기초하여 상기 확률적 HE 스킴으로부터 도출되는 것인, 컴퓨터 구현 방법.

청구항 7

제1항에 있어서,

상기 ZKP는 제5 난수와 제6 난수를 숨기는 커미트먼트, 상기 선형 결정적 HE 스킴에 기초하여 상기 제2 노드의 공개 키에 의해 암호화된 상기 제5 난수와 상기 제6 난수의 암호문(cyphertext), 및 상기 선형 결정적 HE 스킴에 기초하여 상기 제1 노드의 공개 키에 의해 암호화된 상기 제5 난수와 제6 난수의 암호문을 포함하는 것인, 컴퓨터 구현 방법.

청구항 8

제1항에 있어서,

상기 ZKP는 상기 선형 결정적 HE 스킴의 특성에 기초하여 상기 트랜잭션이 유효하다고 결정하기 위해 생성 및 사용되는 것인, 컴퓨터 구현 방법.

청구항 9

제1항에 있어서,

상기 트랜잭션이 유효하다고 결정하는 단계는 상기 블록체인 네트워크의 외부를 통한 상기 제1 노드와 상기 제2 노드 사이의 상호작용 없이 상기 ZKP에 기초하여 행해지는 것인, 컴퓨터 구현 방법.

청구항 10

컴퓨터 시스템에 의해 동작들을 수행하도록 실행가능한 하나 이상의 명령어가 저장된, 비일시적 컴퓨터 판독 가능 저장 매체에 있어서,

상기 동작들은,

블록체인 네트워크 내의 제1 노드와 제2 노드 사이의 트랜잭션과 연관된 트랜잭션 데이터를 수신하는 동작 - 상기 트랜잭션 데이터는 복수의 자산을 나타내는 데이터, 제1 난수와 상기 트랜잭션의 트랜잭션 금액을 숨기는 제1 커미트먼트, 제2 난수와 상기 복수의 자산의 합계치로부터 상기 트랜잭션 금액을 차감하는 것에 기초하여 계산된 잔액을 숨기는 제2 커미트먼트, 선형 결정적 준동형 암호화(homomorphic encryption: HE) 스킴에 기초하여 상기 제2 노드의 공개 키에 의해 양자 모두 암호화된 상기 트랜잭션 금액 및 제3 난수, 상기 선형 결정적 HE 스킴에 기초하여 상기 제1 노드의 공개 키에 의해 양자 모두 암호화된 상기 잔액 및 제4 난수, 하나 이상의 범위 증명, 영지식 증명(zero-knowledge proof: ZKP), 및 상기 제1 노드의 공개 키에 대응하는 개인 키에 기초하여 생성된 디지털 서명을 포함함 - ;

상기 제1 노드의 공개 키에 기초하여 상기 디지털 서명을 검증하는 동작;

상기 하나 이상의 범위 증명이 상기 트랜잭션 금액과 상기 잔액 각각이 0 이상임을 증명한다고 결정하는 동작;

상기 복수의 자산의 합계치가 상기 트랜잭션 금액과 상기 잔액의 합산(sum)과 같다고 결정하는 동작; 및

상기 ZKP에 기초하여, 상기 제1 난수가 상기 제3 난수와 동일하고, 상기 제2 난수가 상기 제4 난수와 동일하며, 상기 제1 커미트먼트에 숨겨진 상기 트랜잭션 금액이 상기 제 2 노드의 공개 키에 의해 암호화된 상기 트랜잭션 금액과 동일하다고 결정함으로써, 상기 트랜잭션이 유효하다고 결정하는 동작

을 포함하는 것인, 비일시적 컴퓨터 판독 가능 저장 매체.

청구항 11

제10항에 있어서,

상기 트랜잭션은 상기 제1 노드와 연관된 계정과 상기 제2 노드와 연관된 계정 사이에 행해지며,

상기 동작들은, 상기 트랜잭션이 유효하다고 결정한 후에, 상기 트랜잭션 금액과 상기 잔액에 기초하여 상기 제1 노드와 연관된 계정과 상기 제2 노드와 연관된 계정을 업데이트하는 동작을 더 포함하는 것인, 비일시적 컴퓨터 판독 가능 저장 매체.

청구항 12

제10항에 있어서,

상기 복수의 자산 각각은 자산 유형, 커미트먼트에 숨겨진 자산 값, 및 상기 커미트먼트를 생성하는데 사용되는 난수 중 하나 이상과 연관되는 것인, 비일시적 컴퓨터 판독 가능 저장 매체.

청구항 13

제12항에 있어서,

상기 동작들은, 상기 복수의 자산 각각이 동일한 자산 유형과 연관된다고 결정하는 동작을 더 포함하는 것인, 비일시적 컴퓨터 판독 가능 저장 매체.

청구항 14

제12항에 있어서,

상기 제1 커미트먼트, 상기 제2 커미트먼트, 및 상기 자산 값을 숨기는 커미트먼트는 준동형의 커미트먼트 스킴에 기초하여 생성되고,

상기 복수의 자산의 합계치가 상기 트랜잭션 금액과 상기 잔액의 합산과 같다고 결정하는 동작은, 상기 커미트먼트 스킴의 준동형사상에 기초하여 행해지는 것인, 비일시적 컴퓨터 판독 가능 저장 매체.

청구항 15

제10항에 있어서,

상기 선형 결정적 HE 스킴은, 확률적 HE 스킴과 연관된 난수를 고정된 수로 변경하는 것에 기초하여 상기 확률적 HE 스킴으로부터 도출되는 것인, 비일시적 컴퓨터 판독 가능 저장 매체.

청구항 16

제10항에 있어서,

상기 ZKP는 제5 난수와 제6 난수를 숨기는 커미트먼트, 상기 선형 결정적 HE 스킴에 기초하여 상기 제2 노드의 공개 키에 의해 암호화된 상기 제5 난수와 상기 제6 난수의 암호문, 및 상기 선형 결정적 HE 스킴에 기초하여 상기 제1 노드의 공개 키에 의해 암호화된 상기 제5 난수와 제6 난수의 암호문을 포함하는 것인, 비일시적 컴퓨터 판독 가능 저장 매체.

청구항 17

제10항에 있어서,

상기 ZKP는 상기 선형 결정적 HE 스킴의 특성에 기초하여 상기 트랜잭션이 유효하다고 결정하기 위해 생성 및 사용되는 것인, 비일시적 컴퓨터 판독 가능 저장 매체.

청구항 18

제10항에 있어서,

상기 트랜잭션이 유효하다고 결정하는 동작은, 상기 블록체인 네트워크의 외부를 통한 상기 제1 노드와 상기 제2 노드 사이의 상호작용 없이 상기 ZKP에 기초하여 행해지는 것인, 비일시적 컴퓨터 판독 가능 저장 매체.

청구항 19

컴퓨터 구현 시스템에 있어서,

하나 이상의 컴퓨터; 및

상기 하나 이상의 컴퓨터와 상호작용 가능하게 결합되고, 상기 하나 이상의 컴퓨터에 의해 실행될 때 하나 이상의 동작을 수행하는 하나 이상의 명령어가 저장된 유형의(tangible) 비일시적 머신-판독가능 매체를 갖는 하나 이상의 컴퓨터 메모리 디바이스

를 포함하고,

상기 하나 이상의 동작은,

블록체인 네트워크 내의 제1 노드와 제2 노드 사이의 트랜잭션과 연관된 트랜잭션 데이터를 수신하는 동작 - 상기 트랜잭션 데이터는 복수의 자산을 나타내는 데이터, 제1 난수와 상기 트랜잭션의 트랜잭션 금액을 숨기는 제1 커미트먼트, 제2 난수와 상기 복수의 자산의 합계치로부터 상기 트랜잭션 금액을 차감하는 것에 기초하여 계산된 잔액을 숨기는 제2 커미트먼트, 선형 결정적 준동형 암호화(homomorphic encryption: HE) 스킴에 기초하여 상기 제2 노드의 공개 키에 의해 양자 모두 암호화된 상기 트랜잭션 금액 및 제3 난수, 상기 선형 결정적 HE 스킴에 기초하여 상기 제1 노드의 공개 키에 의해 양자 모두 암호화된 상기 잔액 및 제4 난수, 하나 이상의 범위 증명, 영지식 증명(zero-knowledge proof: ZKP), 및 상기 제1 노드의 공개 키에 대응하는 개인 키에 기초하여 생성된 디지털 서명을 포함함 - ;

상기 제1 노드의 공개 키에 기초하여 상기 디지털 서명을 검증하는 동작;

상기 하나 이상의 범위 증명이 상기 트랜잭션 금액과 상기 잔액 각각이 0 이상임을 증명한다고 결정하는 동작;

상기 복수의 자산의 합계치가 상기 트랜잭션 금액과 상기 잔액의 합산(sum)과 같다고 결정하는 동작; 및

상기 ZKP에 기초하여, 상기 제1 난수가 상기 제3 난수와 동일하고, 상기 제2 난수가 상기 제4 난수와 동일하며, 상기 제1 커미트먼트에 숨겨진 상기 트랜잭션 금액이 상기 제 2 노드의 공개 키에 의해 암호화된 상기 트랜잭션 금액과 동일하다고 결정함으로써, 상기 트랜잭션이 유효하다고 결정하는 동작

을 포함하는 것인, 컴퓨터 구현 시스템.

청구항 20

제19항에 있어서,

상기 트랜잭션은 상기 제1 노드와 연관된 계정과 상기 제2 노드와 연관된 계정 사이에 행해지며,

상기 동작은, 상기 트랜잭션이 유효하다고 결정한 후에, 상기 트랜잭션 금액과 상기 잔액에 기초하여 상기 제1 노드와 연관된 계정과 상기 제2 노드와 연관된 계정을 업데이트하는 동작을 더 포함하는 것인, 컴퓨터 구현 시스템.

청구항 21

제19항에 있어서,

상기 복수의 자산 각각은 자산 유형, 커미트먼트에 숨겨진 자산 값, 및 상기 커미트먼트를 생성하는데 사용되는 난수 중 하나 이상과 연관되는 것인, 컴퓨터 구현 시스템.

청구항 22

제21항에 있어서,

상기 동작은, 상기 복수의 자산 각각이 동일한 자산 유형과 연관된다고 결정하는 동작을 더 포함하는 것인, 컴퓨터 구현 시스템.

청구항 23

제21항에 있어서,

상기 제1 커미트먼트, 상기 제2 커미트먼트, 및 상기 자산 값을 숨기는 커미트먼트는 준동형의 커미트먼트 스킴에 기초하여 생성되고,

상기 복수의 자산의 합계치가 상기 트랜잭션 금액과 상기 잔액의 합산과 같다고 결정하는 동작은, 상기 커미트먼트 스킴의 준동형사상에 기초하여 행해지는 것인, 컴퓨터 구현 시스템.

청구항 24

제19항에 있어서,

상기 선형 결정적 HE 스킴은, 확률적 HE 스킴과 연관된 난수를 고정된 수로 변경하는 것에 기초하여 상기 확률적 HE 스킴으로부터 도출되는 것인, 컴퓨터 구현 시스템.

청구항 25

제19항에 있어서,

상기 ZKP는 제5 난수와 제6 난수를 숨기는 커미트먼트, 상기 선형 결정적 HE 스킴에 기초하여 상기 제2 노드의 공개 키에 의해 암호화된 상기 제5 난수와 상기 제6 난수의 암호문, 및 상기 선형 결정적 HE 스킴에 기초하여 상기 제1 노드의 공개 키에 의해 암호화된 상기 제5 난수와 제6 난수의 암호문을 포함하는 것인, 컴퓨터 구현 시스템.

청구항 26

제19항에 있어서,

상기 ZKP는 상기 선형 결정적 HE 스킴의 특성에 기초하여 상기 트랜잭션이 유효하다고 결정하기 위해 생성 및 사용되는 것인, 컴퓨터 구현 시스템.

청구항 27

제19항에 있어서,

상기 트랜잭션이 유효하다고 결정하는 동작은, 상기 블록체인 네트워크의 외부를 통한 상기 제1 노드와 상기 제2 노드 사이의 상호작용 없이 상기 ZKP에 기초하여 행해지는 것인, 컴퓨터 구현 시스템.

발명의 설명

기 술 분 야

[0001] 블록체인 네트워크는 블록체인 시스템, 합의 네트워크, 분산 원장(distributed ledger) 시스템 네트워크, 또는 블록체인이라고도 지칭되며, 참여 엔티티가 데이터를 안전하고 변경 불가하게 저장할 수 있게 한다. 블록체인은 트랜잭션(transaction)의 원장으로 기술될 수 있으며, 블록체인의 복수의 사본은 블록체인 네트워크 전체에 저장된다. 블록체인 형식의 예로는 공개 블록체인, 컨소시엄 블록체인, 및 비공개 블록체인이 포함될 수 있다. 공개 블록체인은 모든 엔티티가 블록체인을 사용할 수 있고 합의 프로세스에 참여할 수 있도록 개방되어 있다. 컨소시엄 블록체인은 합의 프로세스가 특정 조직 또는 기간과 같은 사전에 선택된 노드의 집합에 의해 제어되는 블록체인이다. 특정 엔티티에 읽기 및 쓰기 권한을 중앙에서 제어하는 비공개 블록체인이 제공된다.

배 경 기 술

[0002] 블록체인은 사용자간의 트랜잭션을 기록하기 위하 다양한 기록 관리 모델을 사용할 수 있다. 예시적인 기록 관리 모델에는 미사용 트랜잭션 출력(unspent transaction output: UTXO)과 계정 잔고 모델(account balance model)이 포함된다. UTXO 모델에서, 각 트랜잭션은 이전 트랜잭션의 출력을 소비하고, 후속 트랜잭션에서 소비될 수 있는 새로운 출력을 생성한다. 사용자의 미사용 트랜잭션은 추적되며, 소비할 수 있는 잔고는 미사용 트랜잭션의 합계로서 계산된다. 계정 잔고 모델에서, 각 사용자의 계정 잔고는 글로벌 상태(global state)로 추적된다. 각 트랜잭션에 대해, 소비 계정의 잔고가 트랜잭션 금액 이상임을 확실히 하기 위해 체크된다. 이는

전통적인 은행 업무와 유사하다.

[0003] 볼록체인은 일련의 블록을 포함하는데, 각 블록은 네트워크에서 실행되는 하나 이상의 트랜잭션을 포함한다. 각 블록은 원장의 페이지로 유추될 수 있는 한편, 블록체인 자체는 원장의 전체 사본이다. 각 트랜잭션이 확인되고는 블록에 추가되며, 이 블록은 블록체인에 추가된다. 블록체인의 사본은 네트워크의 전체 노드에 복제된다. 이러한 방식으로, 블록체인의 상태에 대한 글로벌 합의가 있게 된다. 또한, 적어도 공용 네트워크의 경우에는, 블록체인은 모든 노드가 볼 수 있도록 개방되어 있다. 블록체인 사용자의 프라이버시를 보호하기 위해, 암호화 기술이 구현된다.

[0004] 계정 잔고 모델 하에서는, 트랜잭션의 양방 당사자가 커미트(commit)하는 값을 숨기기 위해 커미트먼트 스킴이 사용될 수 있다. 커미트먼트 스킴은 당사자가 선택(choice) 또는 값을 커미트하고 나중에 그 값을 다른 관련 당사자에게 전달할 필요성에서 생겨난다. 예를 들어, 상호작용식 페더슨 커미트먼트(Pedersen commitment: PC) 스킴에서, 제1 사용자는 난수 값(random value) r에 기초하여 생성된 커미트먼트 값 PC(t,r)을 전송함으로써 트랜잭션 금액 t에 커미트할 수 있다. 커미트먼트 값이 생성되며, 제2 사용자는 그 난수 값 r을 취득하는 것에 의해서만 트랜잭션 금액 t를 밝힐 수 있다. 트랜잭션 금액이 유효하다는 것을 확인하기 위해, 트랜잭션 금액이 0 이상이고 계정 잔고 이하라는 것을 증명하는 범위 증명(range proof)을 생성할 수 있다.

[0005] 몇몇 경우에는, 사용자로부터 복수의 트랜잭션이 이루어질 수 있다. 범위 증명은 계정의 잔고와 연관되어 있기 때문에, 복수의 트랜잭션은 블록체인에서 순차적으로 검증돼야 있다. 이와 같이, 해당 범위 증명은 각 트랜잭션 후에 계정의 잔고와 정확하게 연관될 수 있다. 하지만, 복수의 트랜잭션을 순차적으로 검증하는 것은 시간 소모적일 수 있다. 트랜잭션의 병렬 검증(parallel verification)을 가능케 하는 기록 관리 모델이 특히 시간에 민감한 태스크게 유리할 수 있다.

발명의 내용

[0006] 본 명세서의 실시예는 블록체인 트랜잭션의 비상호작용식 프라이버시 보호 검증을 위한 컴퓨터 구현 방법을 포함한다. 보다 상세하게는, 본 명세서의 실시예는 트랜잭션 금액, 계정 잔고, 또는 커미트먼트를 생성하기 위한 난수와 같은 프라이버시 정보를 다른 블록체인 노드에 드러내지 않으면서, 커미트먼트 스킴과 준동형 암호화에 기초하여, 블록체인 노드의 계정과 연관된 복수의 트랜잭션을 병렬로 확인(validating)할 수 있는 컴퓨터 구현 방법에 대한 것이다.

[0007] 몇몇 실시예에서, 동작은, 상기 트랜잭션과 연관된 트랜잭션 데이터를 수신하는 단계로서, 상기 트랜잭션 데이터는, 복수의 자산을 나타내는 데이터, 제1 난수와 상기 트랜잭션의 트랜잭션 금액을 숨기는 제1 커미트먼트, 제2 난수와 상기 복수의 자산의 합계치로부터 상기 트랜잭션 금액을 차감하는 것에 기초하여 계산된 잔액을 숨기는 제2 커미트먼트, 선형 결정적 준동형 암호화(homomorphic encryption: HE) 스킴에 기초하여 상기 제2 노드의 공개 키에 의해 양자 모두 암호화된 상기 트랜잭션 금액 및 제3 난수, 상기 선형 결정적 HE 스킴에 기초하여 상기 제1 노드의 공개 키에 의해 양자 모두 암호화된 상기 잔액 및 제4 난수, 하나 이상의 범위 증명; 영지식 증명(zero-knowledge proof: ZKP), 및 상기 제1 노드의 공개 키에 대응하는 개인 키에 기초하여 생성된 디지털 서명을 포함하는 것인, 상기 수신하는 단계; 상기 제1 노드의 공개 키에 기초하여 상기 디지털 서명을 검증하는 단계; 상기 하나 이상의 범위 증명이 상기 트랜잭션 금액과 상기 잔액 각각이 0 이상임을 증명한다고 결정하는 단계; 상기 복수의 자산의 합계치가 상기 트랜잭션 금액과 상기 잔액의 합산과 같다고 결정하는 단계; 상기 ZKP에 기초하여, 상기 제1 난수가 상기 제3 난수와 동일하고, 상기 제2 난수가 상기 제4 난수와 동일하며, 상기 제1 커미트먼트에 숨겨진 상기 트랜잭션 금액이 상기 제 2 노드의 공개 키에 의해 암호화된 상기 트랜잭션 금액과 동일하다고 결정함으로써, 상기 트랜잭션이 유효하다고 결정하는 단계를 포함한다. 다른 실시예는 컴퓨터 저장 장치에 인코딩된 방법의 동작을 수행하도록 구성된, 대응하는 시스템, 장치, 및 컴퓨터 프로그램을 포함한다.

[0008] 이들 및 다른 실시예는 각각 다음의 특징들 중 하나 이상을 선택적으로 포함할 수 있다: 상기 트랜잭션은 상기 제1 노드와 연관된 계정과 상기 제2 노드와 연관된 계정 사이에 행해지며, 상기 방법은 상기 트랜잭션이 유효하다고 결정한 후에, 상기 트랜잭션 금액과 상기 잔액에 기초하여 상기 제1 노드와 연관된 계정과 상기 제2 노드와 연관된 계정을 업데이트하는 단계를 더 포함하고; 상기 복수의 자산 각각은 자산 유형, 커미트먼트에 숨겨진 자산 값, 및 커미트먼트를 생성하는데 사용되는 난수 중 하나 이상과 연관되며; 상기 방법은 상기 복수의 자산 각각이 동일한 자산 유형과 연관된다고 결정하는 단계를 더 포함하고; 상기 제1 커미트먼트, 상기 제2 커미트먼트, 및 상기 자산 값을 숨기는 커미트먼트는 준동형(homomorphic)의 커미트먼트 스킴에 기초하여 생성되고, 상기 복수의 자산의 합계치가 상기 트랜잭션 금액과 상기 잔액의 합산과 같다고 결정하는 단계는 상기 커미트먼트 스킴의 준동형사상(homomorphism)에 기초하여 행해지며; 상기 선형 결정적 HE 스킴은 확률적 HE 스킴과 연관된

난수를 고정된 수(fixed number)로 변경하는 것에 의해 상기 확률적 HE 스킴으로부터 도출되고; 상기 ZKP는 제5 난수와 제6 난수를 숨기는 커미트먼트, 상기 선형 결정적 HE 스킴에 기초하여 상기 제2 계정의 공개 키에 의해 암호화된 상기 제5 난수와 상기 제6 난수의 암호문, 및 상기 선형 결정적 HE 스킴에 기초하여 상기 제1 계정의 공개 키에 의해 암호화된 상기 제5 난수와 제6 난수의 암호문을 포함하며; 상기 ZKP는 상기 선형 결정적 HE의 특성에 기초하여 상기 트랜잭션이 유효하다고 결정하기 위해 생성 및 사용되고; 상기 트랜잭션이 유효하다고 결정하는 단계는 상기 블록체인 네트워크의 외부를 통한 상기 제1 노드와 상기 제2 노드 사이의 상호작용 없이 상기 ZKP에 기초하여 행해진다.

[0009] 본 명세서는 하나 이상의 프로세서에 결합되며, 상기 하나 이상의 프로세서에 의해 실행될 때 상기 하나 이상의 프로세서로 하여금 본 명세서에 제공된 방법의 실시예에 따른 동작을 실행하게 하는 명령어들이 저장된, 하나 이상의 비일시적 컴퓨터 판독 가능 저장 매체를 또한 제공한다.

[0010] 본 명세서는 제공된 방법을 구현하기 위한 시스템을 또한 제공한다. 상기 시스템은: 하나 이상의 프로세서; 및, 하나 이상의 프로세서에 결합되며, 상기 하나 이상의 프로세서에 의해 실행될 때 상기 하나 이상의 프로세서로 하여금 본 명세서에 제공된 방법의 실시예에 따른 동작을 실행하게 하는 명령어들이 저장된, 컴퓨터 판독 가능 저장 매체를 포함한다.

[0011] 본 명세서에 기재된 주제의 실시예는 특정 이점 또는 기술적 효과를 실현하도록 구현될 수 있다. 예를 들어, 본 명세서의 실시예는 트랜잭션 중에 블록체인 노드의 계정 잔고와 트랜잭션 금액을 사적화할 수 있게 한다. 자금 이체의 수령자는 커미트먼트를 검증하기 위해 트랜잭션을 확인하거나 난수를 사용할 필요가 없으며, 트랜잭션 확인은 비상호작용식일 수 있다. 블록체인 노드는 영지식 증명(zero-knowledge proof: ZKP)이 가능하도록 HE와 커미트먼트에 기초하여 트랜잭션을 확인할 수 있다.

[0012] 설명된 방법은 다양한 모바일 컴퓨팅 디바이스의 계정/데이터 보안을 강화할 수 있게 해준다. 계정의 잔고와 트랜잭션 금액은 HE에 기초하여 암호화될 수 있으며, 커미트먼트 스킴에 의해 숨겨질 수 있다. 이와 같이, 합의 노드는 계정의 실제 계정 잔고를 공개하지 않으면서 HE의 특성에 기초하여 트랜잭션 후에 원장의 계정 잔고를 업데이트할 수 있다. 트랜잭션을 확인하기 위해 난수가 수신자에게 전송될 필요가 없기 때문에, 데이터 누출 위험이 저감될 수 있고, 난수를 관리하기 위해 컴퓨팅 및 메모리 자원이 더 적게 사용될 수 있다.

[0013] 본 명세서에 따른 방법은 본 명세서에 기재된 양태 및 특징의 임의의 조합을 포함할 수 있음을 알 수 있다. 즉, 본 명세서에 따른 방법은 본 명세서에 구체적으로 기재된 양태 및 특징의 조합에 국한되지 않고, 제공된 양태 및 특징의 임의의 조합도 또한 포함한다.

[0014] 본 명세서의 하나 이상의 실시예의 상세 내용은 첨부된 도면과 이하의 설명에 기재되어 있다. 본 명세서의 다른 특징과 이점은 설명과 도면으로부터, 및 특허청구범위로부터 자명해질 것이다.

도면의 간단한 설명

[0015] 도 1은 본 명세서의 실시예를 실행하는데 사용될 수 있는 환경의 일례를 도시하는 도면.

도 2는 본 명세서의 실시예에 따른 개념적 아키텍처의 일례를 도시하는 도면.

도 3은 준동형 암호화에 기초한 블록체인 트랜잭션의 프라이버시 보호된 확인 프로세스의 일례를 도시하는 도면.

도 4는 본 명세서의 실시예에 따른 블록체인 트랜잭션의 일례를 도시하는 도면.

도 5는 준동형 암호화에 기초한 블록체인 트랜잭션의 프라이버시 보호된 확인 프로세스의 다른 예를 도시하는 도면.

도 6은 본 명세서의 실시예에 따라 실행될 수 있는 방법의 일례를 도시하는 도면.

도 7은 본 명세서의 실시예에 따라 실행될 수 있는 방법의 다른 예를 도시하는 도면.

도 8은 본 명세서의 실시예에 따른 프로세스를 수행할 수 있는 블록체인 노드의 일례를 도시하는 도면.

다양한 도면에서 동일 참조 부호는 동일 요소를 나타낸다.

발명을 실시하기 위한 구체적인 내용

[0016] 본 명세서의 실시예는 블록체인 트랜잭션의 비상호작용식 프라이버시 보호 검증을 위한 컴퓨터 구현 방법을 포함한다. 보다 상세하게는, 본 명세서의 실시예는 트랜잭션 금액, 계정 잔고, 또는 커미트먼트를 생성하기 위한 난수와 같은 프라이버시 정보를 다른 블록체인 노드에 드러내지 않으면서, 커미트먼트 스킴과 준동형 암호화에 기초하여, 블록체인 노드의 계정과 연관된 복수의 트랜잭션을 병렬로 확인할 수 있는 컴퓨터 구현 방법에 대한 것이다. 몇몇 실시예에서, 동작은, 상기 트랜잭션과 연관된 트랜잭션 데이터를 수신하는 단계로서, 상기 트랜잭션 데이터는, 복수의 자산을 나타내는 데이터, 제1 난수와 상기 트랜잭션의 트랜잭션 금액을 숨기는 제1 커미트먼트, 제2 난수와 상기 복수의 자산의 합계치로부터 상기 트랜잭션 금액을 차감하는 것에 기초하여 계산된 잔액을 숨기는 제2 커미트먼트, 선형 결정적 HE 스킴에 기초하여 상기 제2 노드의 공개 키에 의해 양자 모두 암호화된 상기 트랜잭션 금액 및 제3 난수, 상기 선형 결정적 준동형 암호화(HE) 스킴에 기초하여 상기 제1 노드의 공개 키에 의해 양자 모두 암호화된 상기 잔액 및 제4 난수, 하나 이상의 범위 증명, 영지식 증명(ZKP), 및 상기 제1 노드의 공개 키에 대응하는 개인 키에 기초하여 생성된 디지털 서명을 포함하는 것인, 상기 수신하는 단계; 상기 제1 노드의 공개 키에 기초하여 상기 디지털 서명을 검증하는 단계; 상기 하나 이상의 범위 증명이 상기 트랜잭션 금액과 상기 잔액 각각이 0 이상임을 증명한다고 결정하는 단계; 상기 복수의 자산의 합계치가 상기 트랜잭션 금액과 상기 잔액의 합산과 같다고 결정하는 단계; 상기 ZKP에 기초하여, 상기 제1 난수가 상기 제3 난수와 동일하고, 상기 제2 난수가 상기 제4 난수와 동일하며, 상기 제1 커미트먼트에 숨겨진 상기 트랜잭션 금액이 상기 제 2 노드의 공개 키에 의해 암호화된 상기 트랜잭션 금액과 동일하다고 결정함으로써, 상기 트랜잭션이 유효하다고 결정하는 단계를 포함한다. 다른 실시예는 컴퓨터 저장 장치에 인코딩된 방법의 동작을 수행하도록 구성된, 대응하는 시스템, 장치, 및 컴퓨터 프로그램을 포함한다.

[0017] 본 명세서의 실시예의 다른 문맥을 제공하기 위해서 및 위에서 언급한 바와 같이, (예를 들면, P2P 노드로 구성된) 합의 네트워크 및 블록체인 네트워크라고도 지칭될 수 있는 분산 원장 시스템(distributed ledger system: DLS)은 참여 엔티티가 안전하고 변경 불가하게 트랜잭션을 수행하고 데이터를 저장할 수 있게 한다. 본 명세서에서는 블록체인이 특정 사용 사례를 참조하지 않고 일반적으로 DLS를 지칭하는데 사용된다.

[0018] 블록체인은 트랜잭션이 변경 불가하며 나중에 검증될 수 있는 방식으로 트랜잭션을 저장하는 데이터 구조이다. 블록체인은 하나 이상의 블록을 포함한다. 체인 내의 각 블록은 이전 블록의 암호화 해시를 포함함으로써 체인 내의 바로 직전의 이전 블록과 링크된다. 각 블록은 타임스탬프, 그 자체의 암호화 해시, 및 하나 이상의 트랜잭션을 또한 포함한다. 블록체인 네트워크의 노드에 의해 이미 검증된 트랜잭션은 해시되고, 머클 트리(Merkle tree)에 인코딩된다. 머클 트리는 트리의 리프 노드(leaf node)에 있는 데이터가 해시되고, 트리의 각 브랜치의 모든 해시가 브랜치의 루트에서 연결되는(concatenated) 데이터 구조이다. 이 프로세스는 전체 트리의 루트까지 트리를 계속하며, 이는 트리 내의 모든 데이터를 나타내는 해시를 저장한다. 트리에 저장된 트랜잭션의 것으로 여겨지는 해시는 이 해시가 트리의 구조와 일치하는지 여부를 판정함으로써 신속하게 검증될 수 있다.

[0019] 블록체인은 트랜잭션을 저장하는 데이터 구조지만, 블록체인 네트워크는 하나 이상의 블록체인을 관리, 업데이트, 및 유지하는 컴퓨팅 노드의 네트워크이다. 위에서 언급한 바와 같이, 블록체인 네트워크는 공개 블록체인 네트워크, 비공개 블록체인 네트워크, 또는 컨소시엄 블록체인 네트워크로 제공될 수 있다.

[0020] 공개 블록체인에서, 합의 프로세스는 합의 네트워크의 노드에 의해 제어된다. 예를 들면, 수백, 수천, 심지어는 수백만의 엔티티가 공개 블록체인에 참여할 수 있으며, 공개 블록체인 각각은 공개 블록체인 내에 적어도 하나의 노드를 운영한다. 따라서, 공개 블록체인은 참여 엔티티와 관련된 공개 네트워크로 생각될 수 있다. 몇몇 예에서, 블록이 유효하고 블록체인에 추가되도록 하기 위해서는 엔티티(노드)의 다수가 모든 블록에 서명해야 한다. 예시적인 공개 블록체인 네트워크에는 블록체인이라 불리는 분산 원장을 이용하는 P2P 지불 네트워크가 포함된다. 하지만, 위에서 언급한 바와 같이, 블록체인이라는 용어는 어떤 특정 블록체인 네트워크에 대한 특별한 언급 없이 분산 원장을 일반적으로 지칭하는데 사용된다.

[0021] 일반적으로 공개 블록체인은 공개 트랜잭션을 지원한다. 공개 트랜잭션은 블록체인 내의 모든 노드와 공유되며, 블록체인은 모든 노드에 걸쳐서 복제된다. 즉, 모든 노드는 블록체인에 대해 완벽한 합의 상태에 있게 된다. 합의(예를 들면, 블록체인에 대한 블록의 추가에 대한 합의)를 달성하기 위해, 블록체인 네트워크 내에 합의 포로토콜이 구현된다. 예시적인 합의 프로토콜로는, 제한없이, 작업 증명(proof-of-work: POW), 지분 증명(proof-of-stake: POS), 및 권위 증명(proof-of-authority: POA)가 포함된다. POW는 본 명세서에서 비한정적인 예로서 더 언급된다.

[0022] 본 명세서의 실시예는 블록체인 트랜잭션의 비상호작용식 프라이버시 보호 검증을 위한 컴퓨터 구현 방법을 포함한다. 보다 상세하게는, 본 명세서의 실시예는 트랜잭션 금액, 계정 잔고, 또는 커미트먼트를 생성하기 위한

난수와 같은 프라이버시 정보를 다른 블록체인 노드에 드러내지 않으면서, 커미트먼트 스킴과 준동형 암호화에 기초하여, 블록체인 노드의 계정과 연관된 복수의 트랜잭션을 병렬로 확인할 수 있는 컴퓨터 구현 방법에 대한 것이다.

[0023] 본 명세서의 실시예에 따르면, 블록체인 노드는 기록 관리(record-keeping) 방법으로서 병렬 트랜잭션 검증을 지원할 수 있는 제네릭 계정 모델(generic account model)을 사용할 수 있다. 계정 잔고 모델과 비교하여, 제네릭 계정 모델을 채용하는 블록체인 노드는 계정 잔고 대신에 복수의 자산의 기록을 유지할 수 있다. 복수의 자산 각각은 자산 유형, 자산 ID, 또는 자산 값 중 적어도 하나와 연관될 수 있다. 제네릭 계정 모델 하의 자산은 화폐형(monetary) 또는 고정형(fixed)과 같은 임의의 형태 또는 유형일 수 있다. 자산은 실화폐와 암호화폐를 포함할 수 있다. 몇몇 실시예에서, 고정 자산은 화폐 금액과 결부된 화폐성 자산으로 변환될 수 있다. 이 화폐 금액은 그리고 나서 블록체인 네트워크의 계정들 사이에서 트랜잭션을 수행하는데 사용될 수 있다. 예시 목적으로, 본 명세서의 실시예에 기재된 자산은 동일한 유형의 화폐로 변환되어서는 제네릭 계정 모델 하의 블록체인 계정에 저장되는 것으로 가정한다.

[0024] 데이터 프라이버시를 보호하기 위해, 트랜잭션은 블록체인 사용자 계정과 연관된 트랜잭션 금액 또는 금액 정보를 드러내지 않으면서, 커미트먼트에 기초하여 블록체인(원장)에 기록될 수 있다. 난수를 사용하여 트랜잭션 금액의 커미트먼트를 생성하기 위해 커미트먼트 스킴이 사용될 수 있다. 예시적인 커미트먼트 스킴은 PC 스킴을 포함하나, 이에 국한되지 않는다. 트랜잭션 금액은 커미트먼트 내에 숨겨지기 때문에, 트랜잭션 금액이 블록체인 사용자 계정의 값을 초과하지 않는다는 것을 증명하기 위해 하나 이상의 범위 증명이 사용될 수 있다.

[0025] 계정 잔고 모델 하에서, 범위 증명은 계정 잔고와 연관된다. 2개 이상의 트랜잭션이 이루어지지만 트랜잭션 모두가 확인되고 블록체인에 기록되지 않으면, 범위 증명은 부정확한 계정 잔고와 연관될 수 있으며, 그래서 무효한 것일 수 있다. 이에 비해, 제네릭 계정 모델 하에서는, 계정 값이 복수의 자산의 총합으로 계산될 수 있다. 트랜잭션 금액이 블록체인 사용자 계정들 사이에서 전송될 때, 트랜잭션 금액 이상의 결합 값을 갖는 복수의 자산 중 적어도 일부가 트랜잭션 금액을 커버하기 위해 사용될 수 있다. 잔여 자산이 전송 예정 금액보다 큰 합산 값을 갖는 조건 하에서 추가적인 전송이 이루어질 수 있다. 트랜잭션이 확인되지 않고 블록체인에 기록되지 않은 경우에도, 잔여 자산의 합산 값이 트랜잭션 금액 이상임을 보여주는 범위 증명은 여전히 유효할 수 있다. 그래서 제네릭 계정 모델 하에서는 2개 이상의 트랜잭션 검증이 병렬로 수행될 수 있다.

[0026] 본 명세서의 실시예에 따르면, 블록체인 트랜잭션은 트랜잭션 계정 잔고, 트랜잭션 금액, 또는 커미트먼트를 생성하는데 사용되는 난수를 드러내지 않으면서, 커미트먼트에 기초하여 확인되어 블록체인(원장)에 기록될 수 있다. PC 스킴과 같은 커미트먼트 스킴은 난수에 기초하여 트랜잭션 금액의 커미트먼트를 생성하는데 사용될 수 있다. 트랜잭션 금액과 난수는 확률적 또는 선형 결정적 HE를 사용하여 암호화될 수 있다. 트랜잭션 금액과 난수는 사용되는 HE 스킴의 특성에 기초하여 트랜잭션을 확인하기 위한 ZKP로서 한 세트의 값을 생성하기 위해서도 또한 사용될 수 있다. 트랜잭션 금액의 커미트먼트, 암호화된 트랜잭션 금액과 난수, 및 ZKP는 계정 잔고, 트랜잭션 금액, 또는 난수를 드러내지 않으면서 트랜잭션이 유효한지를 검증하기 위해 블록체인 노드에 의해 사용될 수 있다.

[0027] 도 1은 본 명세서의 실시예를 실행하는데 사용될 수 있는 환경(100)의 일례를 도시한다. 몇몇 예에서, 예시적인 환경(100)은 엔티티가 공개 블록체인(102)에 참여할 수 있게 한다. 예시적인 환경(100)은 컴퓨팅 시스템(106, 108)과, 네트워크(110)를 포함한다. 몇몇 예에서, 네트워크(110)는 LAN(local area network), WAN(wide area network), 인터넷, 또는 이들의 조합을 포함하며, 웹 사이트, 사용자 디바이스(예를 들면, 컴퓨팅 디바이스), 및 백엔드 시스템을 연결한다. 몇몇 예에서, 네트워크(110)는 유선 및/또는 무선 통신 링크를 통해서 액세스될 수 있다.

[0028] 도시된 예에서, 컴퓨팅 시스템(106, 108)은 각각 공개 블록체인(102)에서 노드로서 참여할 수 있게 하는 임의의 적절한 컴퓨팅 시스템을 포함한다. 예시적인 컴퓨팅 디바이스에는 서버, 데스크탑 컴퓨터, 랩탑 컴퓨터, 태블릿 컴퓨팅 디바이스, 및 스마트폰이 포함되나 이에 국한되지 않는다. 몇몇 예에서, 컴퓨팅 시스템(106, 108)은 공개 블록체인(102)과 상호작용하기 위한 하나 이상의 컴퓨터 구현 서비스를 호스팅할 수 있다. 예를 들면, 컴퓨팅 시스템(106)은 제1 엔티티(예를 들면, 사용자 A)가 하나 이상의 다른 엔티티(예를 들면, 다른 사용자)와의 그 트랜잭션을 관리하는데 사용하는 트랜잭션 관리 시스템과 같은, 제1 엔티티의 컴퓨터 구현 서비스를 호스팅할 수 있다. 컴퓨팅 시스템(108)은 제2 엔티티(예를 들면, 사용자 B)가 하나 이상의 다른 엔티티(예를 들면, 다른 사용자)와의 그 트랜잭션을 관리하는데 사용하는 트랜잭션 관리 시스템과 같은, 제2 엔티티의 컴퓨터 구현 서비스를 호스팅할 수 있다. 도 1의 예에서, 공개 블록체인(102)은 노드들의 P2P 네트워크로 표현되고, 컴퓨팅

시스템(106, 108)은 공개 블록체인(102)에 참여하는 제1 엔티티 및 제2 엔티티 각각의 노드를 제공한다.

[0029] 도 2는 본 명세서의 실시예에 따른 개념적 아키텍처(200)의 일례를 도시한다. 예시적인 개념적 아키텍처(200)는 엔티티 계층(202), 호스트 서비스 계층(204), 및 공개 블록체인 계층(206)을 포함한다. 도시된 예에서, 엔티티 계층(202)은 3개의 엔티티, 엔티티_1(E1), 엔티티_2(E2), 및 엔티티_3(E3)을 포함하는데, 각 엔티티는 각각의 트랜잭션 관리 시스템(208)을 구비한다.

[0030] 도시된 예에서, 호스트 서비스 계층(204)은 각 트랜잭션 관리 시스템(208)을 위한 블록체인 인터페이스(210)를 포함한다. 몇몇 예에서, 각각의 트랜잭션 관리 시스템(208)은 통신 프로토콜(예를 들면, HTTPS(hypertext transfer protocol secure))을 사용하여 네트워크(예를 들면, 도 1의 네트워크(110))를 통해서 각각의 블록체인 인터페이스(210)와 통신한다. 몇몇 예에서, 각 블록체인 인터페이스(210)는 각각의 트랜잭션 관리시스템(208)과 블록체인 계층(206)의 사이에 통신 연결을 제공한다. 보다 상세하게는, 각 블록체인 인터페이스(210)는 각 엔티티가 블록체인 계층(206)의 블록체인 네트워크(212)에 기록된 트랜잭션을 수행할 수 있게 한다. 몇몇 예에서, 블록체인 인터페이스(210)와 블록체인 계층(206) 사이의 통신은 원격 절차 호출(remote procedure call: RPC)를 사용하여 수행된다. 몇몇 예에서, 블록체인 인터페이스(210)는 각각의 트랜잭션 관리 시스템(208)을 위한 블록체인 노드를 "호스트"한다. 예를 들어, 블록체인 인터페이스(210)는 블록체인 네트워크(212)에 액세스하기 위한 애플리케이션 프로그래밍 인터페이스(application programming interface: API)를 제공한다.

[0031] 본 명세서에 기재된 바와 같이, 블록체인 네트워크(212)는 블록체인(216)에 정보를 변경 불가하게 기록하는 복수의 노드(214)를 포함하는 P2P 네트워크로 제공된다. 단일 블록체인(216)이 개략적으로 도시되어 있으나, 블록체인 네트워크(216)의 복수의 복사본이 블록체인 네트워크(212)에 걸쳐서 제공 및 유지된다. 예를 들어, 각 노드(214)는 블록체인(216)의 복사본을 저장한다. 몇몇 실시예에서, 블록체인(216)은 공개 블록체인에 참여하는 2개 이상의 엔티티들 사이에 수행되는 트랜잭션과 연관된 정보를 저장한다.

[0032] 도 3은 준동형 암호화(homomorphic encryption: HE)에 기초한 블록체인 트랜잭션의 프라이버시 보호된 확인 프로세스(300)의 일례를 도시한다. 상위 레벨에서, 프로세스(300)는 사용자 노드 A(302), 사용자 노드 B(도 3에는 도시하지 않음), 및 합의 노드라고도 불리는 블록체인 노드(304)에 의해 수행된다. 사용자 노드 A(302)의 계정과 사용자 노드 B의 계정 양자 모두는 제네릭 계정 모델에 기초하여 한 기록 관리 모델을 구비할 수 있다. 즉, 사용자 노드 A(302)와 사용자 노드 B의 계정 기록은 복수의 자산으로 유지된다. 값의 전송과 같은, 트랜잭션은 사용자 노드 A(302)로부터 사용자 노드 B로 이루어질 수 있다. 사용자 노드 A(302)는 트랜잭션을 커버하기 위해 트랜잭션 금액 이상의 합계치를 갖는 하나 이상의 계정 자산을 선택할 수 있다. 하나 이상의 자산의 합계치와 트랜잭션 금액 사이의 차는 사용자 노드 A(302)에 남은 트랜잭션의 잔액으로 여겨질 수 있다.

[0033] 계정 프라이버시를 보호하기 위해, 사용자 노드 A(302)는 트랜잭션을 커버하는데 사용되는 자산 값의 커미트먼트를 생성할 수 있다. 사용자 노드 A(302)는 트랜잭션의 트랜잭션 금액의 커미트먼트를 또한 생성할 수 있다. 사용자 노드 A(302)는 트랜잭션 금액, 잔액, 및 커미트먼트를 생성하는데 사용되는 난수를 암호화하기 위해 HE를 또한 사용할 수 있다. 트랜잭션의 유효성을 검증하기 위해, 블록체인 노드(304)는 커미트먼트에 숨겨진 트랜잭션 금액, 잔액, 및 난수와 ZKP에 기초하여 한 HE에 의해 암호화된 트랜잭션 금액, 잔액, 및 난수를 비교할 수 있다. 트랜잭션 금액, 잔액, 및 난수가 일치하면, 트랜잭션은 블록체인 노드(304)에 의해서 유효하다고 결정된다. 프로세스(300)의 보다 상세한 사항은 도 3에 관한 이하의 설명에서 논의된다.

[0034] 306에서, 사용자 노드 A(302)는 사용자 노드 B에 트랜잭션 금액을 전송하기 위한 복수의 자산을 선택한다. 사용자 노드 A(302)와 사용자 노드 B는 합의 프로세스에 참여하지 않으면서 블록체인 네트워크를 사용하는 사용자 노드 또는 블록체인 합의 노드일 수 있다. 앞서 논의된 바와 같이, 사용자 노드 A(302)는 기록을 유지하기 위해 제네릭 계정 모델을 사용할 수 있다. 기록을 위한 계정 잔고를 계정 잔고 모델 하에서 유지하는 대신에, 사용자 노드 A(302)의 계정 값은 계정이 보유한 자산의 합계치로 측정된다. 사용자 노드 A(302)는 트랜잭션 금액을 커버하기 위해 충분한 값을 갖는 복수의 자산을 선택할 수 있다. 예를 들어, 트래잭션 금액이 $7.5(미화)이면, 사용자 노드 A(302)는 트랜잭션 금액을 커버하기 위해 각각 $5, $2, 및 $1의 값을 갖는 3개의 자산을 선택할 수 있다.

[0035] 몇몇 실시예에서, 각 자산은 해당 자산을 식별하는 트랜잭션 어드레스 또는 자산 ID와 연관될 수 있다. 자산 ID는 자산 정보의 해싱(hashing)이 될 수 있다. 선택된 k개의 자산의 자산 ID는 ID_1, ..., ID_k로 표현될 수 있다.

[0036] 308에서, 사용자 노드 A(302)는 복수의 자산의 합계치와 트랜잭션 금액에 기초하여 잔액을 계산한다. 자산은

트랜잭션 금액보다 더 큰 합계치를 갖도록 선택되기 때문에, 잔액은 선택된 자산의 합계치에서 트랜잭션 금액을 차감한 것으로 계산될 수 있다. t를 사용하여 트랜잭션 금액을 나타내고 t_0를 사용하여 잔액을 나타내면, 잔액의 계산은 $t_0 = a_1 + \ldots + a_k - t$로 표현될 수 있는데, 여기서 $a_1, \ldots, a_k$는 각각, 트랜잭션 금액 t를 커버하기 위해 사용자 노드 A(302)에 의해 선택된 k개의 자산의 자산 값들이다.

[0037] 310에서, 사용자 노드 A(302)는 트랜잭션 금액에 대응하는 난수(random number)와 잔액에 대응하는 난수를 생성한다. 트랜잭션 금액 t에 대응하는 난수는 r로 나타낼 수 있다. 잔액 t_0에 대응하는 난수는 r_0로 나타낼 수 있다. 몇몇 실시예에서는, 자산 값의 커미트먼트를 생성하기 위해 복수의 난수들이 생성될 수 있다. 예를 들어, $a_1, \ldots, a_k$를 자산 값이라 가정하면, 이들 자산 값에 대응하는 난수는 $r_{a1}, \ldots, r_{ak}$로 표현될 수 있다.

[0038] 몇몇 실시예에서, 난수 r_0는 무작위로 생성되는 대신에 계산될 수도 있다. 이 계산은 $r_0 = r_{a1} + \ldots + r_{ak} - r$과 같이 표현될 수 있는데, 여기서 r은 트랜잭션 금액 t에 대한 커미트먼트를 산출하기 위해 생성된 난수이다. 계산된 난수 r_0를 사용함으로써, 사용자 노드 A(302)는 전송된 자산의 합계치가 수신된 자산 합계치와 동일함을 증명하기 위해 추가적인 ZKP를 생성할 필요가 없다. 몇몇 실시예에서, 다른 난수 r'은 ZKP를 지원하기 위해 $r' = r_1 + \ldots + r_k - r - r_0$와 같이 계산될 수 있다.

[0039] 단계 312에서, 사용자 노드 A(302)는 트랜잭션 금액과 잔액의 커미트먼트를 생성하며, 확률적 HE에 기초하여 해당 난수들을 암호화한다. 몇몇 실시예에서는, 커미트먼트를 생성하기 위해 PC와 같은 준동형 커미트먼트 스킴 사용될 수 있다. PC를 비한정적인 예로 사용하면, 트랜잭션 금액 t의 PC는 난수 r을 사용하여 생성될 수 있으며, 이는 $PC(r, t) = g^r h^t$와 같이 표현될 수 있는데, 여기서 g와 h는 타원 곡선의 생성자일 수 있고, PC(r, t)는 곡선 점의 스칼라 곱셈이다. 유사하게, 잔액 t_0의 PC는 $PC(r_0, t_0) = g^{r0} h^{t0}$와 같이 표현될 수 있다.

[0040] 난수 r은 OU(Okamoto-Uchiyama) 암호화 스킴과 같은, 확률적 HE 스킴에 기초하여 사용자 노드 B의 공개 키를 사용하여 암호화될 수 있다. Boneh-Goh-Nissim과 같은 다른 HE 스킴도 또한 사용될 수 있음을 이해해야 한다. OU를 비한정적인 예로 사용하면, 난수는 트랜잭션 금액 t를 난수로 취급함으로써 OU에 기초하여 암호화될 수 있으며, 이는 $OU_B(r, t) = u^r v^t$, 또는 간단히 $OU_B(t)$로 표현될 수 있는데, 여기서 u는 $v = u^n \bmod n$, 및 $n = p \times q$ 조건을 만족하는 $(Z/nZ)^*$의 생성자이며, 여기서 p와 q는 2개의 소수(prime number)이다. 확률적 OU는 $OU(a + b) = OU(a) \times OU(b)$ 특성을 충족시킬 수 있으며, 여기서 a와 b는 OU에 사용되는 평문(plaintext)이다.

[0041] 난수 r_0는 사용자 노드 A(302)의 공개 키를 사용하여 암호화될 수 있다. 난수는 잔액 t_0를 난수로 취급함으로써 OU에 기초하여 암호화될 수 있으며, 이는 $OU_A(r_0, t_0)$와 같이 표현될 수 있다.

[0042] 그러면 트랜잭션 금액의 암호문은 $T = (PC(t, r), OU_B(r, t))$와 같이 표현될 수 있고, 잔액의 암호문은 $T_0 = (PC(t_0, r_0), OU_A(r_0, t_0))$와 같이 표현될 수 있다. 유사하게, 선택된 k개의 자산의 암호문은 $T_i = (PC(t_i, r_i), OU_A(r_i, t_i))$와 같이 표현될 수 있는데, 여기서 $i = 1, \ldots, k$이다.

[0043] 314에서, 사용자 노드 A(302)는 하나 이상의 범위 증명을 생성한다. 몇몇 실시예에서, 제1 범위 증명 RP_1은 트랜잭션 금액 $t \geq 0$임을 증명하기 위해 생성될 수 있다. 제2 범위 증명 RP_2는 잔액 $t_0 \geq 0$, 즉 복수의 자산의 합계치가 트랜잭션 금액 이상임을 증명하기 위해 생성될 수 있다.

[0044] 316에서, 사용자 노드 A(302)는 ZKP를 생성한다. ZKP는 PC(r,t)에 숨겨진 난수와 트랜잭션 금액이 $OU_B(r,t)$에 암호화된 난수와 트랜잭션 금액과 동일하고, $PC(r_0,t_0)$에 숨겨진 난수와 트랜잭션 금액이 $OU_A(r_0, t_0)$에 암호화된 난수와 트랜잭션 금액과 동일함을 증명하는데 사용될 수 있다. ZKP를 생성하기 위해, 2개의 난수 t'_1과 r'_1이 선택될 수 있다. 이들 2개의 난수는 3개의 값, 즉 $P = PC(t'_1, r'_1)$, $P' = OU_B(r'_1, t'_1)$, $P'' = OU_A(r'_1, t'_1)$를 생성하는데 사용될 수 있다. 그리고 나서 이들 3개의 값은 $x = Hash(P, P', P'')$로 표현되는 해시를 생성하는데 사용될 수 있다. 이 해시 값 x는 $t'_2 = t'_1 + xt$, $r'_2 = r'_1 + xr$, $t'_3 = t'_1 + xt$, 및 $r'_3 = r'_1 + xr_0$를 계산하는데 사용될 수 있다. 그러면, ZKP는 $(P, P', t'_2, r'_2, P'', t'_3, r'_3)$와 같이 표현될 수 있다.

[0045] 318에서, 사용자 노드 A(302)는 트랜잭션 데이터에 서명하기 위한 디지털 서명을 생성하기 위해 개인 키를 사용

한다. 몇몇 실시예에서, 트랜잭션 데이터는 선택된 k개의 자산의 자산 ID(ID_1, ..., ID_k), 트랜잭션 금액의 암호문(T), 잔액의 암호문(T_0), 범위 증명(RP_1 및 RP_2), 난수 r', 및 ZKP를 포함할 수 있다.

[0046] 320에서, 사용자 노드 A(302)는 트랜잭션 데이터의 디지털 서명된 사본을 블록체인 네트워크에 제출한다.

[0047] 322에서, 블록체인 노드(304)는 디지털 서명을 검증한다. 디지털 서명의 검증은 트랜잭션 데이터가 사용자 노드 A(302)에 의해 전송되는 것을 보장하기 위해 행해질 수 있다. 몇몇 실시예에서, 볼록체인 노드(304)는 트랜잭션이 이미 수행되었는지를 검증할 수 있는 이중 지출 방지(anti-double spending) 메커니즘을 포함한다. 만약 그렇다면, 블록체인 노드(304)는 트랜잭션을 거부할 수 있다.

[0048] 324에서, 블록체인 노드(304)는 선택된 자산이 사용자 노드 A의 계정과 연관되는지를 검증한다. 검증은 자산의 자산 ID에 기초하여 할 수 있다.

[0049] 326에서, 블록체인 노드(304)는 선택된 복수의 자산의 합계치가 트랜잭션 금액과 잔액의 합산과 동일한지를 검증한다. 환언하면, 블록체인은 $a_1 + ... + a_k = t + t_0$ 인지를 검증한다. 앞서 논의된 바와 같이, 제네릭 계정 모델 하에서는, 데이터 프라이버시를 보호하기 위해 자산이 PC로서 블록체인에 보관될 수 있다. PC의 준동형사상에 따르면, $PC(r_{a1}, a_1) \times ... \times PC(r_{ak}, a_k) = PC(r_{a1} + ... + r_{ak}, a_1 + ... + a_k)$, 및 $PC(r, t) \times PC(r_0, t_0) = PC(r + r_0, t + t_0)$이다. 그래서, $PC(r_{a1}, a_1) \times ... \times PC(r_{ak}, a_k) = PC(r, t) \times PC(r_0, t_0) \times g^{r'}$를 증명함으로써, $a_1 + ... + a_k = t + t_0$가 증명될 수 있다.

[0050] 328에서, 블록체인 노드(304)는 하나 이상의 범위 증명을 검증한다.

[0051] 330에서, 블록체인 노드(304)는 ZKP를 검증한다. 위에서 논의한 바와 같이, 사용자 노드 B의 공개 키를 사용하여 암호화된 트랜잭션 금액에 대응하는 난수가 PC에 의해 숨겨진 해당 난수와 동일한지를 검증하고, 사용자 노드 A(302)의 공개 키를 사용하여 암호화된 잔액에 대응하는 난수가 PC에 의해 숨겨진 해당 난수와 동일한지를 검증하기 위해 ZKP가 생성될 수 있다. 몇몇 실시예에서는, ZKP를 검증하기 위해, 블록체인 노드(304)가 먼저 해시 값 x를 x = Hash(P, P', P'')와 같이 계산할 수 있다. 블록체인 노드(304)는 그리고 나서 $PC(t'_2, r'_2) = P \times PC(t, r)^x$, $OU_B(r'_2, t'_2) = P' \times OU_B(r, t)^x$, $PC(t'_3, r'_3) = P \times PC(t_0, r_0)^x$, 및 $OU_A(r'_3, t'_3) = P'' \times OU_A(r_0, t_0)^x$ 이 모두 참인지를 검증할 수 있다. 모두 참이면, 예시적인 프로세스(300)는 332로 진행한다. 그렇지 않으면, 블록체인 노드(304)는 트랜잭션을 거부할 수 있다.

[0052] 332에서, 블록체인 노드(304)는 사용자 노드 A(302)와 사용자 노드 B의 계정을 업데이트한다. 사용자 노드 A(302)와 사용자 노드 B의 계정은 제네릭 계정 모델 하에서 자산을 기록으로 보존하기 때문에, 트랜잭션 후에, 사용자 노드 A(302)로부터 전송된 복수의 자산은 사용자 노드 A(302)의 계정으로부터 삭제될 수 있다. 잔액은 사용자 노드 A(302)의 계정에 도로 추가될 수 있다. 트랜잭션 금액 및 대응하는 자산 ID는 사용자 노드 B의 계정에 새로운 자산으로 추가될 수 있다. 몇몇 실시예에서, 업데이트는 사용자 노드 A(302)와 사용자 노드 B의 대응하는 계정에 의해 유지되는 업데이트 자산 목록에 기초하여 행해질 수 있다. 몇몇 실시예에서, 업데이트는 트랜잭션 금액과 잔액의 암호문을 사용자 노드 A(302)와 사용자 노드 B에 의해 유지되는 암호화된 자산 값에 추가하는 것에 기초하여 수행될 수 있다. 계정의 업데이트는 도 4를 참조하여 본 명세서에서 보다 상세히 기재된다.

[0053] 도 4는 본 명세서의 실시예에 따른 블록체인 트랜잭션(400)의 일례를 도시한다. 예시적인 블록체인 트랜잭션(400)에 도시된 바와 같이, 사용자 노드 A(402)는 사용자 노드 B(404)에 트랜잭션 금액 t를 전송한다. 트랜잭션 전에, 사용자 노드 A(404)는 (ID_1, T_1), (ID_2, T_2), (ID_n, T_n)을 포함하는 n개의 자산을 갖고 있다.

[0054] 도 3을 참조하여 기재된 커미트먼트 스킴, 암호화 스킴, 및 트랜잭션 프로세스를 예로 사용하면, 사용자 노드 A(402)는 선택된 k개의 자산의 자산 ID, 즉 ID_1, ID_2, ..., ID_k를 포함할 수 있는 트랜잭션 데이터(408)를 생성할 수 있다. 트랜잭션 데이터(408)는 T_0, T, RP_1, RP_2, r', 및 ZKP를 더 포함할 수 있다. 트랜잭션 데이터(408)가 생성된 후에, 사용자 노드 A(402)는 그 디지털 서명을 추가하고는 디지털 서명된 트랜잭션 데이터를 합의를 위해 블록체인 네트워크(406)에 제출할 수 있다.

[0055] 트랜잭션 후에, 선택된 k개의 자산은 사용자 자산 A(402)로부터 삭제될 수 있다. 잔액은 사용자 노드 A(402)에

도로 추가될 수 있다. 그래서, 사용자 노드 A(402)는 다음의 (ID_k+1, T_{k+1}), (ID_{k+2}, T_{k+2}), ..., (ID_n, T_n), (ID_0, T_0)로 표현되는 자산을 가질 수 있으며, 여기서 ID_0는 잔액 t_0의 자산 ID를 나타낸다.

[0056] 트랜잭션 전에, 사용자 노드 B(404)는 $(ID_{1'}, T_{1'})$, $(ID_{2'}, T_{2'})$, $(ID_{m'}, T_{m'})$과 같이 표현될 수 있는 m개의 자산을 갖고 있다. 트랜잭션 후에는, 트랜잭션 금액이 사용자 노드 B(404)에 추가될 수 있다. 사용자 노드 B(404)는 다음의 $(ID_{1'}, T_{1'})$, $(ID_{2'}, T_{2'})$, $(ID_{m'}, T_{m'})$, $(ID_{t,T})$로 표현되는 자산을 가질 수 있으며, 여기서 ID_t는 트랜잭션 금액 t의 자산 ID를 나타낸다.

[0057] 도 5는 HE에 기초한 블록체인 트랜잭션의 프라이버시 보호된 확인 프로세스(500)의 일례를 도시한다. 상위 레벨에서, 예시적인 프로세스(500)는 사용자 노드 A(502), 사용자 노드 B(도 5에는 도시하지 않음), 및 합의 노드라고도 불리는 블록체인 노드(504)에 의해 수행된다. 사용자 노드 A(502)의 계정과 사용자 노드 B의 계정 양자 모두는 제네릭 계정 모델에 기초하여 할 수 있다. 값의 전송과 같은, 트랜잭션은 사용자 노드 A(502)로부터 사용자 노드 B로 이루어질 수 있다. 사용자 노드 A(502)는 트랜잭션을 커버하기 위해 트랜잭션 금액 이상의 합계치를 갖는 하나 이상의 계정 자산을 선택할 수 있다. 하나 이상의 자산의 합계치와 트랜잭션 금액 사이의 차는 사용자 노드 A(502)에 남은 트랜잭션의 잔액으로 여겨질 수 있다.

[0058] 계정 프라이버시를 보호하기 위해, 사용자 노드 A(502)는 PC와 같은 커미트먼트 스킴을 사용하여, 트랜잭션을 커버하는데 사용되는 자산의 값 및 트랜잭션의 금액의 커미트먼트를 생성할 수 있다. 사용자 노드 A(502)는 커미트먼트를 생성하는데 사용되는 난수를 암호화하기 위해 선형 결정적 HE를 또한 사용할 수 있다. 선형 결정적 HE는 다음의 특성을 가질 수 있다: $HE(s + t) = HE(s) \times HE(t)$, 및 $HE(kt) = HE(t)^k$. 트랜잭션의 유효성을 검증하기 위해, 블록체인 노드(504)는 커미트먼트에 숨겨진 난수와 ZKP에 기초하여 한 HE에 의해 암호화된 난수를 비교할 수 있다. 난수가 일치하면, 트랜잭션은 블록체인 노드(504)에 의해 유효하다고 결정될 수 있다. 프로세스(500)의 보다 상세한 사항은 도 5에 관한 이하의 설명에서 논의된다.

[0059] 506에서, 사용자 노드 A(502)는 사용자 노드 B에 트랜잭션 금액을 전송하기 위한 복수의 자산을 선택한다. 사용자 노드 A(502)와 사용자 노드 B는 합의 프로세스에 참여하지 않으면서 블록체인 네트워크를 사용하는 사용자 노드 또는 블록체인 합의 노드일 수 있다. 사용자 노드 A(502)는 트랜잭션 금액을 커버하기 위해 충분한 값을 갖는 복수의 자산을 선택할 수 있다.

[0060] 몇몇 실시예에서, 각 자산은 해당 자산을 식별하는 트랜잭션 어드레스 또는 자산 ID와 연관될 수 있다. 자산 ID는 자산 정보의 해싱이 될 수 있다. 선택된 k개의 자산의 자산 ID는 ID_1, ..., ID_k로 표현될 수 있다.

[0061] 508에서, 사용자 노드 A(502)는 복수의 자산의 합계치와 트랜잭션 금액에 기초하여 잔액을 계산한다. 자산은 트랜잭션 금액보다 더 큰 합계치를 갖도록 선택되기 때문에, 잔액은 선택된 자산의 합계치에서 트랜잭션 금액을 차감한 것으로 계산될 수 있다. t를 사용하여 트랜잭션 금액을 나타내고 t_0를 사용하여 잔액을 나타내면, 잔액의 계산은 $t_0 = a_1 + \ldots + a_k - t$ 로 표현될 수 있는데, 여기서 a_1, ..., a_k는 각각, 트랜잭션 금액 t를 커버하기 위해 사용자 노드 A(502)에 의해 선택된 k개의 자산의 자산 값들이다.

[0062] 510에서, 사용자 노드 A(502)는 트랜잭션 금액에 대응하는 난수와 잔액에 대응하는 난수를 생성한다. 트랜잭션 금액 t에 대응하는 난수는 r로 나타낼 수 있다. 잔액 t_0에 대응하는 난수는 r_0로 나타낼 수 있다. 몇몇 실시예에서는, 자산 값의 커미트먼트를 생성하기 위해 복수의 난수들이 생성될 수 있다. 예를 들어, a_1, ..., a_k를 자산 값이라 가정하면, 이들 자산 값에 대응하는 난수는 r_{a1}, ..., r_{ak}로 표현될 수 있다.

[0063] 몇몇 실시예에서, 난수 r_0는 무작위로 생성되는 대신에 계산될 수도 있다. 이 계산은 $r_0 = r_{a1} + \ldots + r_{ak} - r$ 과 같이 표현될 수 있는데, 여기서 r은 트랜잭션 금액 t에 대한 커미트먼트를 산출하기 위해 생성된 난수이다. r_0를 계산함으로써, 사용자 노드 A(502)는 전송된 자산의 합계치가 수신된 자산 합계치와 동일함을 증명하기 위해 추가적인 ZKP를 생성할 필요가 없다. 몇몇 실시예에서, 난수 r'은 $r' = r_1 + \ldots + r_k - r - r_0$와 같이 계산될 수 있다.

[0064] 단계 512에서, 사용자 노드 A(502)는 트랜잭션 금액과 잔액의 커미트먼트를 생성하며, 결정적 HE에 기초하여 해당 난수를 암호화한다. 몇몇 실시예에서는, 커미트먼트를 생성하기 위해 PC와 같은 준동형 커미트먼트 스킴이 사용될 수 있다. PC를 비한정적인 예로 사용하면, 트랜잭션 금액 t의 PC는 난수 r을 사용하여 생성될 수 있으

며, 이는 $PC(r, t) = g^{r}h^{t}$와 같이 표현될 수 있는데, 여기서 g와 h는 타원 곡선의 생성자일 수 있고, PC(r, t)는 곡선 점의 스칼라 곱셈이다. 유사하게, 잔액 t_0의 PC는 $PC(r_0, t_0) = g^{r0}h^{t0}$와 같이 표현될 수 있다.

[0065] 난수 r은 선형 결정적 HE에 기초하여 사용자 노드 B의 공개 키를 사용하여 암호화될 수 있다. 선형 결정적 HE는 HE 스킴의 난수를 0 또는 1 또는 다른 적절한 수로 고정함으로써, Paillier, Benaloh, OU, Naccache-Stern, Boneh-Goh-Nissim, Damgard-Jurik과 같은 확률적 HE 또는 등확률(equal-probability) HE로부터 취득될 수 있다. 암호화된 난수는 HE(r)로 표현될 수 있다.

[0066] 난수 r_0는 사용자 노드 A의 공개 키를 사용하여 암호화될 수 있다. 난수는 선형 결정적 HE에 기초하여 암호화될 수 있다. 암호화된 난수는 $HE(r^0)$로 표현될 수 있다.

[0067] 그러면 트랜잭션 금액 t의 암호문은 $T = (g^{r}h^{t}, HE_B(r))$와 같이 표현될 수 있고, 잔액의 암호문은 $T_0 = (g^{r0}h^{t0}, HE_A(r_0))$와 같이 표현될 수 있다. 유사하게, 선택된 k개의 자산의 암호문은 $T_i = (g^{ri}h^{ti}, HE(r_i)$와 같이 표현될 수 있는데, 여기서 i = 1, ..., k이다.

[0068] 514에서, 사용자 노드 A(502)는 하나 이상의 범위 증명을 생성한다. 몇몇 실시예에서, 제1 범위 증명 RP_1은 트랜잭션 금액 $t \geq 0$임을 증명하기 위해 생성될 수 있다. 제2 범위 증명 RP_2는 잔액 $t_0 \geq 0$, 즉 복수의 자산의 합계치가 트랜잭션 금액 이상임을 증명하기 위해 생성될 수 있다.

[0069] 516에서, 사용자 노드 A(502)는 ZKP를 생성한다. ZKP는 PC(r,t)에 숨겨진 난수가 HE(r)에 암호화된 난수와 동일하고, $PC(r_0,t_0)$에 숨겨진 난수가 $HE(r_0)$에 암호화된 난수와 동일함을 증명하는데 사용될 수 있다. ZKP를 생성하기 위해, 2개의 난수 t'_1과 r'_1이 선택될 수 있다. 이들 2개의 난수는 3개의 값, 즉 $P = g^{r'1}h^{t'1}$, $P' = HE_B(r'_1)$, $P'' = HE_A(r'_1)$를 생성하는데 사용될 수 있다. 그리고 나서 이들 3개의 값은 x = Hash(P, P', P'')로 표현되는 해시를 생성하는데 사용될 수 있다. 이 해시 값 x는 $t'_2 = t'_1 + xt$, $r'_2 = r'_1 + xr$, $t'_3 = t'_1 + xt$, 및 $r'_3 = r'_1 + xr_0$를 계산하는데 사용될 수 있다. 그러면, ZKP는 $(P, P', t'_2, r'_2, P'', t'_3, r'_3)$와 같이 표현될 수 있다.

[0070] 518에서, 사용자 노드 A(502)는 트랜잭션 데이터에 서명하기 위한 디지털 서명을 생성하기 위해 개인 키를 사용한다. 몇몇 실시예에서, 트랜잭션 데이터는 선택된 k개의 자산의 자산 ID(ID_1, ..., ID_k), 트랜잭션 금액의 암호문(T), 잔액의 암호문(T_0), 범위 증명(RP_1 및 RP_2), 난수 r', 및 ZKP를 포함할 수 있다.

[0071] 520에서, 사용자 노드 A(502)는 트랜잭션 데이터의 디지털 서명된 사본을 블록체인 네트워크에 제출한다.

[0072] 522에서, 블록체인 노드(504)는 디지털 서명을 검증한다. 디지털 서명의 검증은 트랜잭션 데이터가 사용자 노드 A(502)에 의해 전송되는 것을 보장하기 위해 행해질 수 있다. 몇몇 실시예에서, 볼록체인 노드(504)는 트랜잭션이 이미 수행되었는지를 검증할 수 있는 이중 지출 방지 메커니즘을 포함한다. 만약 그렇다면, 블록체인 노드(504)는 트랜잭션을 거부할 수 있다.

[0073] 524에서, 블록체인 노드(504)는 선택된 자산이 사용자 노드 A의 계정과 연관되는지를 검증한다. 검증은 자산의 자산 ID에 기초하여 할 수 있다.

[0074] 526에서, 블록체인 노드(504)는 선택된 복수의 자산의 합계치가 트랜잭션 금액과 잔액의 합산과 동일한지를 검증한다. 환언하면, 블록체인 노드(504)는 $a_1 + ... + a_k = t + t_0$ 인지를 검증한다. 앞서 논의된 바와 같이, 제네릭 계정 모델 하에서는, 데이터 프라이버시를 보호하기 위해 자산이 PC로서 블록체인에 보관될 수 있다. PC의 준동형사상에 따르면, $PC(r_{a1}, a_1) \times ... \times PC(r_{ak}, a_k) = PC(r_{a1} + ... + r_{ak}, a_1 + ... + a_k)$, 및 $PC(r, t) \times PC(r_0, t_0) = PC(r + r_0, t + t_0)$이다. 그래서, $PC(r_{a1}, a_1) \times ... \times PC(r_{ak}, a_k) = PC(r, t) \times PC(r_0, t_0) \times g^{r'}$을 증명함으로써, $a_1 + ... + a_k = t + t_0$가 증명될 수 있다.

[0075] 528에서, 블록체인 노드(504)는 하나 이상의 범위 증명을 검증한다.

[0076] 530에서, 블록체인 노드(504)는 ZKP를 검증한다. 이전에 논의한 바와 같이, 사용자 노드 B의 공개 키를 사용하

여 암호화된 트랜잭션 금액에 대응하는 난수가 PC에 의해 숨겨진 해당 난수와 동일한지를 검증하고, 사용자 노드 A(502)의 공개 키를 사용하여 암호화된 잔액에 대응하는 난수가 PC에 의해 숨겨진 해당 난수와 동일한지를 검증하기 위해, ZKP가 생성될 수 있다. 몇몇 실시예에서는, ZKP를 검증하기 위해, 블록체인 노드(504)가 먼저 해시 값 x를 x = Hash(P, P', P'')와 같이 계산할 수 있다. 블록체인 노드(504)는 그리고 나서 $g^{r'2}h^{t'2} = P \times (g^{r}h^{t})^{x}$, $HE_B(r') = P' \times HE(r)^{x}$, $g^{r'3}h^{t'3} = P \times (g^{r0}h^{t0})^{x}$, 및 $HE_A(r'_3) = P'' \times HE_A(r_0)^{x}$ 이 모두 참인지를 검증할 수 있다. 모두 참이면, 예시적인 프로세스(500)는 532로 진행한다. 그렇지 않으면, 블록체인 노드(504)는 트랜잭션을 거부할 수 있다.

[0077] 532에서, 블록체인 노드(504)는 사용자 노드 A(502)와 사용자 노드 B의 계정을 업데이트한다. 사용자 노드 A(502)와 사용자 노드 B의 계정은 제네릭 계정 모델 하에서 자산을 기록으로 보존하기 때문에, 트랜잭션 후에, 사용자 노드 A(502)로부터 전송된 복수의 자산은 사용자 노드 A(502)의 계정으로부터 삭제될 수 있다. 잔액은 사용자 노드 A(502)의 계정에 도로 추가될 수 있다. 트랜잭션 금액 및 대응하는 자산 ID는 사용자 노드 B의 계정에 새로운 자산으로 추가될 수 있다. 몇몇 실시예에서, 업데이트는 사용자 노드 A(502)와 사용자 노드 B의 대응하는 계정에 의해 유지되는 업데이트 자산 목록에 기초하여 행해질 수 있다. 몇몇 실시예에서, 업데이트는 트랜잭션 금액과 잔액의 암호문을 사용자 노드 A(502)와 사용자 노드 B에 의해 유지되는 암호화된 자산 값에 추가하는 것에 기초하여 수행될 수 있다. 예시적인 블록체인 트랜잭션(400)과 그 대응하는 계정 업데이트가 도 4의 설명에 기재되어 있다.

[0078] 도 6은 본 명세서의 실시예에 따라 실행될 수 있는 프로세스(600)의 일례를 도시한다. 제시를 명확히 하기 위해, 아래의 설명은 본 설명의 다른 도면들의 문맥에서 방법(600)을 기술한다. 하지만, 예시적인 프로세스(600)는 예를 들면, 임의의 시스템, 환경, 소프트웨어, 및 하드웨어, 또는 시스템, 환경, 소프트웨어, 및 하드웨어의 조합에 의해 적절히 수행될 수 있음을 이해할 것이다. 몇몇 실시예에서는, 예시적인 프로세스(600)의 단계들이 병렬로, 조합하여, 루프 형태로, 또는 임의의 순서로 실행될 수 있다.

[0079] 602에서, 합의 노드는 트랜잭션과 연관된 트랜잭션 데이터를 수신한다. 몇몇 예에서, 트랜잭션 데이터는, 복수의 자산을 나타내는 데이터, 제1 난수와 트랜잭션의 트랜잭션 금액을 숨기는 제1 커미트먼트, 제2 난수와 상기 복수의 자산의 합계치로부터 상기 트랜잭션 금액을 차감하는 것에 기초하여 계산된 잔액을 숨기는 제2 커미트먼트, 확률적 HE 스킴에 기초하여 제2 노드의 공개 키에 의해 양자 모두 암호화된 상기 트랜잭션 금액 및 제3 난수, 확률적 HE 스킴에 기초하여 제1 노드의 공개 키에 의해 양자 모두 암호화된 상기 잔액 및 제4 난수, 하나 이상의 범위 증명, ZKP, 및 제1 노드의 공개 키에 대응하는 개인 키에 기초하여 생성된 디지털 서명을 포함한다.

[0080] 몇몇 실시예에서, 복수의 자산 각각은 자산 유형, 커미트먼트에 숨겨진 자산 값 및 커미트먼트를 생성하는데 사용되는 난수 중 하나 이상과 연관된다. 몇몇 실시예에서, 합의 노드는 복수의 자산 각각이 동일한 자산 유형과 연관된다고 결정한다. 몇몇 실시예에서, 제1 커미트먼트, 제2 커미트먼트, 및 자산 값을 숨기는 커미트먼트는 준동형의 커미트먼트 스킴에 기초하여 생성된다.

[0081] 몇몇 실시예에서, 제3 난수는 트랜잭션 금액을 난수로 취급함으로써 확률적 HE 스킴에 기초하여 암호화되고, 제4 난수는 잔액을 난수로 취급함으로써 확률적 HE 스킴에 기초하여 암호화된다. 몇몇 실시예에서, 제1 커미트먼트와 제2 커미트먼트는 페더슨 커미트먼트 스킴에 기초하여 생성되고, 확률적 HE 스킴은 OU 암호화 스킴이다.

[0082] 몇몇 실시예에서, ZKP는 제5 난수와 제6 난수를 숨기는 페더슨(Pedersen) 커미트먼트, OU 암호화 스킴에 기초하여 제2 계정의 공개 키에 의해 암호화된 제5 난수와 제6 난수의 암호문, 및 OU 암호화 스킴에 기초하여 제1 계정의 공개 키에 의해 암호화된 제5 난수와 제6 난수의 암호문을 포함한다.

[0083] 604에서, 합의 노드는 제1 노드의 공개 키에 기초하여 디지털 서명을 검증한다.

[0084] 606에서, 합의 노드는 하나 이상의 범위 증명이 트랜잭션 금액과 잔액 각각이 0 이상임을 증명한다고 결정한다.

[0085] 608에서, 합의 노드는 복수의 화폐의 합계치가 트랜잭션 금액과 잔액의 합산과 같다고 결정한다. 몇몇 실시예에서, 복수의 자산의 합계치가 트랜잭션 금액과 잔액의 합산과 같다고 결정하는 것은 커미트먼트 스킴의 준동형 사상에 기초하여 행해진다.

[0086] 610에서, 합의 노드는 ZKP에 기초하여, 제1 난수가 제3 난수와 동일하고, 제2 난수가 제4 난수와 동일하며, 제1 커미트먼트에 숨겨진 트랜잭션 금액이 제2 노드의 공개 키에 의해 암호화된 트랜잭션 금액과 동일하다고 결정함

으로써, 트랜잭션이 유효하다고 결정한다.

[0087] 몇몇 실시예에서, 트랜잭션은 제1 노드와 연관된 계정과 제2 노드와 연관된 계정 사이에 행해지며, 본 방법은 트랜잭션이 유효하다고 결정한 후에, 트랜잭션 금액과 잔액에 기초하여 제1 노드와 연관된 계정과 제2 노드와 연관된 계정을 업데이트하는 것을 더 포함한다. 몇몇 실시예에서, ZKP는 확률적 HE의 특성에 기초하여 트랜잭션이 유효하다고 결정하기 위해 생성 및 사용된다. 몇몇 실시예에서, 트랜잭션이 유효하다고 결정하는 것은 블록체인 네트워크의 외부를 통한 제1 노드와 제2 노드 사이의 상호작용 없이 ZKP에 기초하여 행해진다.

[0088] 도 7은 본 명세서의 실시예에 따라 실행될 수 있는 예시적인 프로세스(700)를 도시한다. 제시를 명확히 하기 위해, 아래의 설명은 본 설명의 다른 도면들의 문맥에서 방법(700)을 기술한다. 하지만, 예시적인 프로세스(700)는 예를 들면, 임의의 시스템, 환경, 소프트웨어, 및 하드웨어, 또는 시스템, 환경, 소프트웨어, 및 하드웨어의 조합에 의해 적절히 수행될 수 있음을 이해할 것이다. 몇몇 실시예에서는, 예시적인 프로세스(700)의 단계들이 병렬로, 조합하여, 루프 형태로, 또는 임의의 순서로 실행될 수 있다.

[0089] 702에서, 합의 노드는 트랜잭션과 연관된 트랜잭션 데이터를 수신한다. 몇몇 예에서, 트랜잭션 데이터는, 복수의 자산을 나타내는 데이터, 제1 난수와 트랜잭션의 트랜잭션 금액을 숨기는 제1 커미트먼트, 제2 난수와 상기 복수의 자산의 합계치로부터 상기 트랜잭션 금액을 차감하는 것에 기초하여 계산된 잔액을 숨기는 제2 커미트먼트, 선형 결정적 HE 스킴에 기초하여 제2 노드의 공개 키에 의해 양자 모두 암호화된 상기 트랜잭션 금액 및 제3 난수, 선형 결정적 HE 스킴에 기초하여 제1 노드의 공개 키에 의해 양자 모두 암호화된 상기 잔액 및 제4 난수, 하나 이상의 범위 증명, ZKP, 및 제1 노드의 공개 키에 대응하는 개인 키에 기초하여 생성된 디지털 서명을 포함한다.

[0090] 몇몇 실시예에서, 복수의 자산 각각은 자산 유형, 커미트먼트에 숨겨진 자산 값, 및 커미트먼트를 생성하는데 사용되는 난수 중 하나 이상과 연관된다. 몇몇 실시예에서, 합의 노드는 복수의 자산 각각이 동일한 자산 유형과 연관된다고 결정한다. 몇몇 실시예에서, 제1 커미트먼트, 제2 커미트먼트, 및 자산 값을 숨기는 커미트먼트는 준동형의 커미트먼트 스킴에 기초하여 생성된다.

[0091] 몇몇 실시예에서, 선형 결정적 HE 스킴은 확률적 HE 스킴과 연관된 난수를 고정된 수로 변경하는 것에 의해 확률적 HE 스킴으로부터 도출된다.

[0092] 몇몇 실시예에서, ZKP는 제5 난수와 제6 난수를 숨기는 커미트먼트, 선형 결정적 HE 스킴에 기초하여 제2 계정의 공개 키에 의해 암호화된 제5 난수와 제6 난수의 암호문, 및 선형 결정적 HE 스킴에 기초하여 제1 계정의 공개 키에 의해 암호화된 제5 난수와 제6 난수의 암호문을 포함한다.

[0093] 704에서, 합의 노드는 제1 노드의 공개 키에 기초하여 디지털 서명을 검증한다.

[0094] 706에서, 합의 노드는 하나 이상의 범위 증명이 트랜잭션 금액과 잔액 각각이 0 이상임을 증명한다고 결정한다.

[0095] 708에서, 합의 노드는 복수의 화폐의 합계치가 트랜잭션 금액과 잔액의 합산과 같다고 결정한다. 몇몇 실시예에서, 복수의 자산의 합계치가 트랜잭션 금액과 잔액의 합산과 같다고 결정하는 것은 커미트먼트 스킴의 준동형 사상에 기초하여 행해진다.

[0096] 710에서, 합의 노드는 ZKP에 기초하여, 제1 난수가 제3 난수와 동일하고, 제2 난수가 제4 난수와 동일하며, 제1 커미트먼트에 숨겨진 트랜잭션 금액이 제 2 노드의 공개 키에 의해 암호화된 트랜잭션 금액과 동일하다고 결정함으로써, 트랜잭션이 유효하다고 결정한다.

[0097] 몇몇 실시예에서, 트랜잭션은 제1 노드와 연관된 계정과 제2 노드와 연관된 계정 사이에 행해지며, 본 방법은 트랜잭션이 유효하다고 결정한 후에, 트랜잭션 금액과 잔액에 기초하여 제1 노드와 연관된 계정과 제2 노드와 연관된 계정을 업데이트하는 것을 더 포함한다. 몇몇 실시예에서, ZKP는 선형 결정적 HE의 특성에 기초하여 트랜잭션이 유효하다고 결정하기 위해 생성 및 사용된다. 몇몇 실시예에서, 트랜잭션이 유효하다고 결정하는 것은 블록체인 네트워크의 외부를 통한 제1 노드와 제2 노드 사이의 상호작용 없이 ZKP에 기초하여 행해진다.

[0098] 도 8은 본 명세서의 실시예에 따른 프로세스를 수행할 수 있는 블록체인 노드(800)의 일례를 도시한다. 상위 레벨에서, 블록체인 노드(800)는 수신 유닛(802), 검증 유닛(804), 제1 결정 유닛(806), 제2 결정 유닛(808), 및 제3 결정 유닛(810)을 포함한다.

[0099] 몇몇 실시예에서, 수신 유닛(802)은 트랜잭션과 연관된 트랜잭션 데이터를 수신하도록 동작할 수 있다. 몇몇 예에서, 트랜잭션 데이터는, 복수의 자산을 나타내는 데이터, 제1 난수와 트랜잭션의 트랜잭션 금액을 숨기는

제1 커미트먼트, 제2 난수와 상기 복수의 자산의 합계치로부터 상기 트랜잭션 금액을 차감하는 것에 기초하여 계산된 잔액을 숨기는 제2 커미트먼트, 확률적 HE 스킴에 기초하여 제2 노드의 공개 키에 의해 양자 모두 암호화된 상기 트랜잭션 금액 및 제3 난수, 확률적 HE 스킴에 기초하여 제1 노드의 공개 키에 의해 양자 모두 암호화된 상기 잔액 및 제4 난수, 하나 이상의 범위 증명, ZKP, 및 제1 노드의 공개 키에 대응하는 개인 키에 기초하여 생성된 디지털 서명을 포함한다.

[0100] 몇몇 실시예에서, 수신 유닛(802)은 트랜잭션과 연관된 트랜잭션 데이터를 수신하도록 동작할 수 있으며, 트랜잭션 데이터는, 복수의 자산을 나타내는 데이터, 제1 난수와 트랜잭션의 트랜잭션 금액을 숨기는 제1 커미트먼트, 제2 난수와 상기 복수의 자산의 합계치로부터 상기 트랜잭션 금액을 차감하는 것에 기초하여 계산된 잔액을 숨기는 제2 커미트먼트, 선형 결정적 HE 스킴에 기초하여 제2 노드의 공개 키에 의해 양자 모두 암호화된 상기 트랜잭션 금액 및 제3 난수, 선형 결정적 HE 스킴에 기초하여 제1 노드의 공개 키에 의해 양자 모두 암호화된 상기 잔액과 제4 난수, 하나 이상의 범위 증명, ZKP, 및 제1 노드의 공개 키에 대응하는 개인 키에 기초하여 생성된 디지털 서명을 포함한다.

[0101] 몇몇 실시예에서, 복수의 자산 각각은 자산 유형, 커미트먼트에 숨겨진 자산 값, 및 커미트먼트를 생성하는데 사용되는 난수 중 하나 이상과 연관된다. 몇몇 실시예에서, 블록체인 노드(800)는 복수의 자산 각각이 동일한 자산 유형과 연관된다고 결정한다. 몇몇 실시예에서, 제1 커미트먼트, 제2 커미트먼트, 및 자산 값을 숨기는 커미트먼트는 준동형의 커미트먼트 스킴에 기초하여 생성된다. 몇몇 실시예에서, 선형 결정적 HE 스킴은 확률적 HE 스킴과 연관된 난수를 고정된 수로 변경하는 것에 의해 확률적 HE 스킴으로부터 도출된다.

[0102] 몇몇 실시예에서, 제3 난수는 트랜잭션 금액을 난수로 취급함으로써 확률적 HE 스킴에 기초하여 암호화되고, 제4 난수는 잔액을 난수로 취급함으로써 확률적 HE 스킴에 기초하여 암호화된다. 몇몇 실시예에서, 제1 커미트먼트와 제2 커미트먼트는 페더슨 커미트먼트 스킴에 기초하여 생성되고, 확률적 HE 스킴은 OU 암호화 스킴이다.

[0103] 몇몇 실시예에서, ZKP는 제5 난수와 제6 난수를 숨기는 페더슨 커미트먼트, OU 암호화 스킴에 기초하여 제2 계정의 공개 키에 의해 암호화된 제5 난수와 제6 난수의 암호문, 및 OU 암호화 스킴에 기초하여 제1 계정의 공개 키에 의해 암호화된 제5 난수와 제6 난수의 암호문을 포함한다. 몇몇 실시예에서, ZKP는 제5 난수와 제6 난수를 숨기는 커미트먼트, 선형 결정적 HE 스킴에 기초하여 제2 계정의 공개 키에 의해 암호화된 제5 난수와 제6 난수의 암호문, 및 선형 결정적 HE 스킴에 기초하여 제1 계정의 공개 키에 의해 암호화된 제5 난수와 제6 난수의 암호문을 포함한다.

[0104] 검증 유닛(804)은 제1 노드의 공개 키에 기초하여 디지털 서명을 검증하도록 동작할 수 있다.

[0105] 제1 결정 유닛(806)은 하나 이상의 범위 증명이 트랜잭션 금액과 잔액 각각이 0 이상임을 증명한다고 결정하도록 동작할 수 있다.

[0106] 제2 결정 유닛(808)은 복수의 화폐의 합계치가 트랜잭션 금액과 잔액의 합산과 같다고 결정하도록 동작할 수 있다. 몇몇 실시예에서, 복수의 자산의 합계치가 트랜잭션 금액과 잔액의 합산과 같다고 결정하는 것은 커미트먼트 스킴의 준동형사상에 기초하여 행해진다.

[0107] 제3 결정 유닛(810)은 ZKP에 기초하여, 제1 난수가 제3 난수와 동일하고, 제2 난수가 제4 난수와 동일하며, 제1 커미트먼트에 숨겨진 트랜잭션 금액이 제 2 노드의 공개 키에 의해 암호화된 트랜잭션 금액과 동일하다고 결정함으로써, 트랜잭션이 유효하다고 결정하도록 동작할 수 있다.

[0108] 몇몇 실시예에서, 트랜잭션은 제1 노드와 연관된 계정과 제2 노드와 연관된 계정 사이에 행해지며, 블록체인 노드(800)는 제3 결정 유닛(810)이 트랜잭션이 유효하다고 결정한 후에, 트랜잭션 금액과 잔액에 기초하여 제1 노드와 연관된 계정과 제2 노드와 연관된 계정을 업데이트하도록 동작 가능한 업데이트 유닛을 포함할 수 있다. 몇몇 실시예에서, ZKP는 확률적 HE의 특성에 기초하여 트랜잭션이 유효하다고 결정하기 위해 생성 및 사용된다. 몇몇 실시예에서, ZKP는 선형 결정적 HE의 특성에 기초하여 트랜잭션이 유효하다고 결정하기 위해 생성 및 사용된다. 몇몇 실시예에서, 트랜잭션이 유효하다고 결정하는 것은 블록체인 네트워크의 외부를 통한 제1 노드와 제2 노드 사이의 상호작용 없이 ZKP에 기초하여 행해진다.

[0109] 본 명세서에 기재된 주제의 실시예는 특정 이점 또는 기술적 효과를 실현하도록 구현될 수 있다. 예를 들어, 본 명세서의 실시예는 트랜잭션 중에 블록체인 노드의 계정 잔고와 트랜잭션 금액을 사적화(private)할 수 있게 한다. 자금 이체의 수령자는 커미트먼트를 검증하기 위해 트랜잭션을 확인하거나 난수를 사용할 필요가 없으며, 트랜잭션 확인은 비상호작용식일 수 있다. 블록체인 노드는 영지식 증명이 가능하도록 HE와 커미트먼

트에 기초하여 트랜잭션을 확인할 수 있다.

[0110] 설명된 방법은 다양한 모바일 컴퓨팅 디바이스의 계정/데이터 보안을 강화할 수 있게 해준다. 계정의 잔고와 트랜잭션 금액은 HE에 기초하여 암호화될 수 있으며, 커미트먼트 스킴에 의해 숨겨질 수 있다. 이와 같이, 합의 노드는 계정의 실제 계정 잔고를 밝히지 않으면서 HE의 특성에 기초하여 트랜잭션 후에 원장의 계정 잔고를 업데이트할 수 있다. 트랜잭션을 확인하기 위해 난수가 수신자에게 전송될 필요가 없기 때문에, 데이터 누출 위험이 저감될 수 있고, 난수를 관리하기 위해 컴퓨팅 및 메모리 자원이 더 적게 사용될 수 있다.

[0111] 본 명세서에 기재된 실시예와 동작은 본 명세서에 개시된 구조를 포함하는 디지털 전자 회로, 또는 컴퓨터 스프트웨어, 펌웨어, 또는 하드웨어 또는 이들의 하나 이상의 조합으로 구현될 수 있다. 동작은 하나 이상의 컴퓨터 판독 가능 저장 장치에 저장되거나 다른 다른 소스로부터 수신되는 데이터에 대해 데이터 처리 장치에 의해 수행되는 동작으로 구현될 수 있다. 데이터 처리 장치, 컴퓨터, 또는 컴퓨팅 디바이스는, 예로서 프로그램 가능 프로세서, 컴퓨터, SOC(system on a chip), 전술한 것들의 복수 형태 또는 조합을 포함하는, 데이터를 처리하는 장치, 디바이스, 및 기계를 포함할 수 있다. 장치는 특수 목적 논리 회로, 예를 들면 CPU(central processing unit), FPGA(field programmable gate array), 또는ASIC(application-specific integrated circuit)을 포함할 수 있다. 장치는 해당 컴퓨터 프로그램을 위한 실행 환경을 생성하는 코드, 예를 들면, 프로세서 펌웨어, 프로토콜 스택, 데이터베이스 관리 시스템, 운영체계(예를 들면, 단일 운영체계 또는 여러 운영체계의 조합), 크로스-플랫폼 런타임 환경, 가상머신, 또는 이들의 하나 이상의 조합을 구성하는 코드를 또한 포함할 수 있다. 장치와 실행 환경은 웜 서비스, 분산 컴퓨팅 및 그리드 컴퓨팅 인프라스트럭처와 같은 다양한 상이한 컴퓨팅 모델 인프라스트럭처를 실현할 수 있다.

[0112] 컴퓨터 프로그램(예를 들면, 프로그램, 소프트웨어, 소프트웨어 애플리케이션, 소프트웨어 모듈, 소프트웨어 유닛, 스크립트, 또는 코드라고도 알려짐)은 컴파일러형 또는 해석형 언어, 선언형 또는 절차형 언어를 포함하는 임의의 형태의 프로그래밍 언어로 작성될 수 있으며, 독립형 프로그램 또는 컴퓨팅 환경에서 사용하는데 적합한 모듈, 컴포넌트, 서브루틴, 객체, 또는 다른 유닛을 포함하는 임의의 형태로 전개(deploy)될 수 있다. 프로그램은 다른 프로그램 또는 데이터를 보유한 파일의 일부(예를 들면, 마크업 언어 문서에 저장된 하나 이상의 스크립트)에, 해당 프로그램 전용의 단일 파일에, 또는 복수의 연계 파일(coordinated files)(예를 들면, 하나 이상의 모듈, 서브프로그램, 또는 코드의 일부를 저장한 파일)에 저장될 수 있다. 컴퓨터 프로그램은 단일 컴퓨터 상에서 또는 한 지점에 배치되거나 또는 복수의 지점에 걸쳐 분산되어 통신 네트워크로 상호 연결된 복수의 컴퓨터 상에서 실행될 수 있다.

[0113] 컴퓨터 프로그램을 실행하기 위한 프로세서는, 예로서 범용 및 전용 마이크로프로세서 양자 모두, 및 임의의 종류의 디지털 컴퓨터의 임의의 하나 이상의 프로세서를 포함한다. 일반적으로, 프로세서는 판독 전용 메모리 또는 랜덤 액세스 메모리 또는 양자 모두로부터 명령어들 및 데이터를 수신할 수 있다. 컴퓨터의 필수 요소는 명령에 따라 동작을 수행하는 프로세서와 명령들 및 데이터를 저장하는 하나 이상의 메모리 디바이스이다. 일반적으로, 컴퓨터는 또한 데이터를 저장하기 위한 하나 이상의 대용량 저장장치를 포함하거나 또는 이에 데이터를 송신 또는 수신 또는 송수신하기 위해 동작 가능하게 결합될 수 있다. 또한, 컴퓨터는 다른 디바이스, 예를 들면 휴대폰, 모바일 디바이스, PDA(personal digital assistant), 게임콘솔, GPS(Global Positioning System) 수신기, 또는 이동형 저장장치에 내장될 수도 있다. 컴퓨터 프로그램 명령어들 및 데이터를 저장하는데 적합한 디바이스는, 예로서 반도체 메모리 디바이스, 자기 디스크, 및 자기-광 디스크를 포함하는 비휘발성 메모리, 매체 및 메모리 장치를 포함한다. 프로세서와 메모리에는 전용 로직 회로가 부가되거나 또는 프로세서와 메모리가 이에 병합될 수 있다.

[0114] 모바일 디바이스는 핸드셋, UE(user equipment), 휴대 전화기(예를 들면, 스마트폰), 태블릿, 웨어러블 디바이스(예를 들면, 스마트워치 및 스마트 아이글라스), 인체 내에 임플란트된 기기(예를 들면, 바이오센서, 인공와우 임플란트), 또는 다른 유형의 모바일 디바이스를 포함할 수 있다. 모바일 디바이스는 다양한 통신 네트워크(후술함)에 (예를 들면, RF(radio frequency) 신호를 사용하여) 무선으로 통신할 수 있다. 모바일 디바이스는 이 모바일 디바이스의 현재 환경의 특성을 판단하는 센서를 포함할 수 있다. 이들 센서들은 카메라, 마이크로폰, 근접 센서, GPS 센서, 동작 센서, 가속도계, 주변광(ambient light) 센서, 수분 센서, 자이로스코프, 나침반, 기압계, 지문 센서, 안면인식 시스템, RF 센서(예를 들면, Wi-Fi 및 셀뮬러 무선), 감온 센서, 또는 다른 유형의 센서를 포함할 수 있다. 예를 들어, 카메라는 이동식 또는 고정식 렌즈를 갖는 전방 또는 후방 카메라와, 플래시, 이미지 센서, 및 이미지 프로세서를 포함할 수 있다. 카메라는 안면 및/또는 홍채 인식을 위해 미세부분을 촬상할 수 있는 메가픽셀 카메라일 수 있다. 카메라는 데이터 프로세서 및 메모리에 저장되거나 원격으로 액세스되는 인증 정보와 함께 안면인식 시스템을 형성한다. 안면인식 시스템 또는 하나 이상의 센서, 예

를 들어 마이크로폰, 동작 센서, 가속도계, GPS 센서, 또는 RF 센서가 사용자 인증에 사용될 수 있다.

[0115] 사용자와의 상호작용을 제공하기 위해, 실시예들은 디스플레이 장치와 입력 장치, 예를 들면 사용자에게 정보를 디스플레이 하기 위한 LCD(liquid crystal display) 또는 OLED(organic light-emitting diode)/VR(virtual-reality)/AR(augmented reality) 디스플레이, 및 사용자가 컴퓨터에 입력을 제공할 수 있게 해주는 터치스크린, 키보드, 및 포인팅 디바이스를 구비한 컴퓨터 상에서 구현될 수 있다. 다른 종류의 디바이스도 사용자와의 상호작용을 제공하는데 사용될 수 있다: 예를 들어, 사용자에게 제공되는 피드백은 임의의 형태의 감각 피드백, 예를 들면 시각 피드백, 청각 피드백, 또는 촉각 피드백일 수 있으며; 사용자로부터의 입력은 음향, 음성언어(speech), 또는 촉각 입력을 포함하여 임의의 형태로 수신될 수 있다. 또한, 컴퓨터는 사용자에 의해 사용되는 디바이스에 문서를 송신 및 수신함으로써, 예를 들면 웹 브라우저로부터 수신된 요청에 응답하여 사용자의 클라이언트 디바이스 상의 웹 브라우저에 웹 페이지를 전송함으로써 사용자와 상호작용할 수 있다.

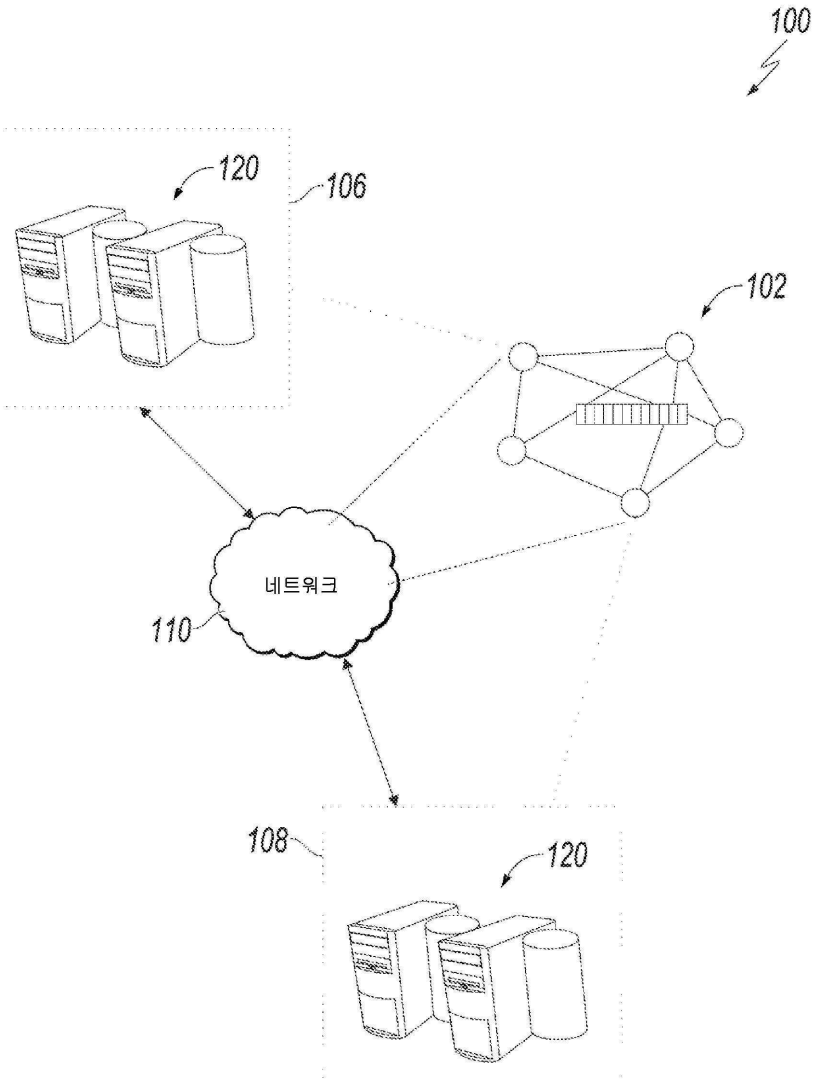
[0116] 실시예들은 임의의 형태 또는 매체의 유선 또는 무선 디지털 데이터 통신(또는 그 조합), 예를 들면 통신 네트워크에 의해 상호 연결된 컴퓨팅 디바이스를 사용하여 구현될 수 있다. 상호 연결된 디바이스의 예로는 전형적으로 통신 네트워크를 통하여 상호 작용하며 일반적으로 서로 멀리 떨어진 클라이언트와 서버가 있다. 클라이언트, 예를 들어 모바일 디바이스는, 예를 들면 구매, 판매, 지불, 수여, 송부, 또는 대출 트랜잭션을 수행하거나 또는 이를 인가하는 서버와, 또는 서버를 통하여 트랜잭션 자체를 수행할 수 있다. 이러한 트랜잭션은 동작과 응답이 시간적으로 근접해 있도록 실시간일 수 있는데; 예를 들어, 개인은 그 동작과 응답이 실질적으로 동시에 발생한다고 인식하며; 개인의 동작에 따른 응답에 걸리는 그 시간차는 1ms(밀리초) 미만이거나 1초 미만이고; 응답은 시스템의 처리 한계를 고려하여 의도적인 지연이 없다.

[0117] 통신 네트워크의 예로는 LAN(local area network), RAN(radio access network), MAN(metropolitan area network), 및 WAN(wide area network)이 포함된다. 통신 네트워크에는 인터넷 전부 또는 일부, 다른 통신 네트워크, 또는 통신 네트워크들의 조합이 포함될 수 있다. LTE(Long Term Evolution), 5G, IEEE 802, IP(Internet Protocol), 또는 다른 프로토콜 또는 프로토콜들의 조합을 포함하는 다양한 프로토콜 및 표준에 따라 통신 네트워크 상에서 정보가 전송될 수 있다. 통신 네트워크는 연결된 컴퓨팅 디바이스들 사이에서 음성, 비디오, 바이오메트릭, 또는 인증 데이터, 또는 다른 정보를 전송할 수 있다.

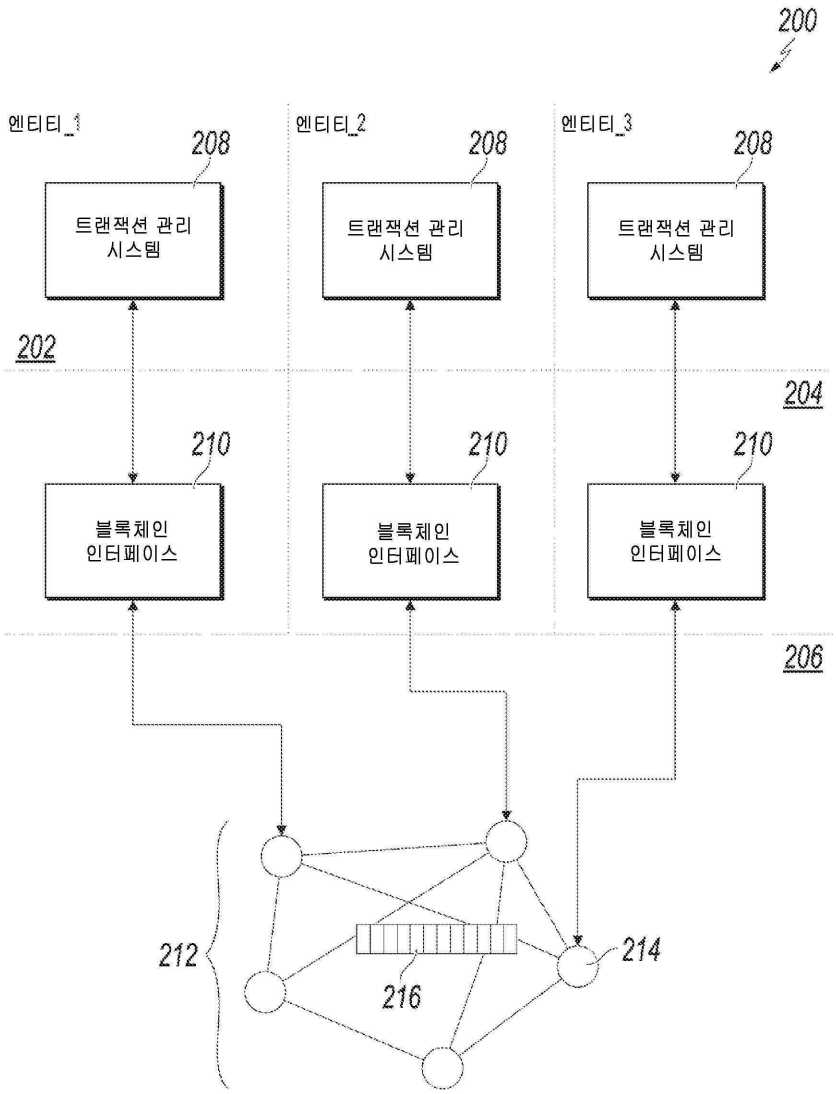
[0118] 개별 실시예로 기재된 특징들은 조합 형태로 단일 실시예로 구현될 수도 있는 한편, 단일 실시예로 기재된 특징들은 개별적으로 또는 임의의 적절한 하부 조합(sub-combination) 형태로 복수의 실시예로 구현될 수도 있다. 특성 순서로 기재되고 특허청구된 동작들을 그 특정 순서, 또는 예시된 모든 동작들이 수행되어야 함이 요구되는 것으로 이해되어서는 안 된다(어떤 동작들은 선택적일 수 있다). 적절한 경우에는, 멀티태스킹 또는 병렬처리(또는 멀티태스킹과 병렬처리의 조합)가 수행될 수도 있다.

도면

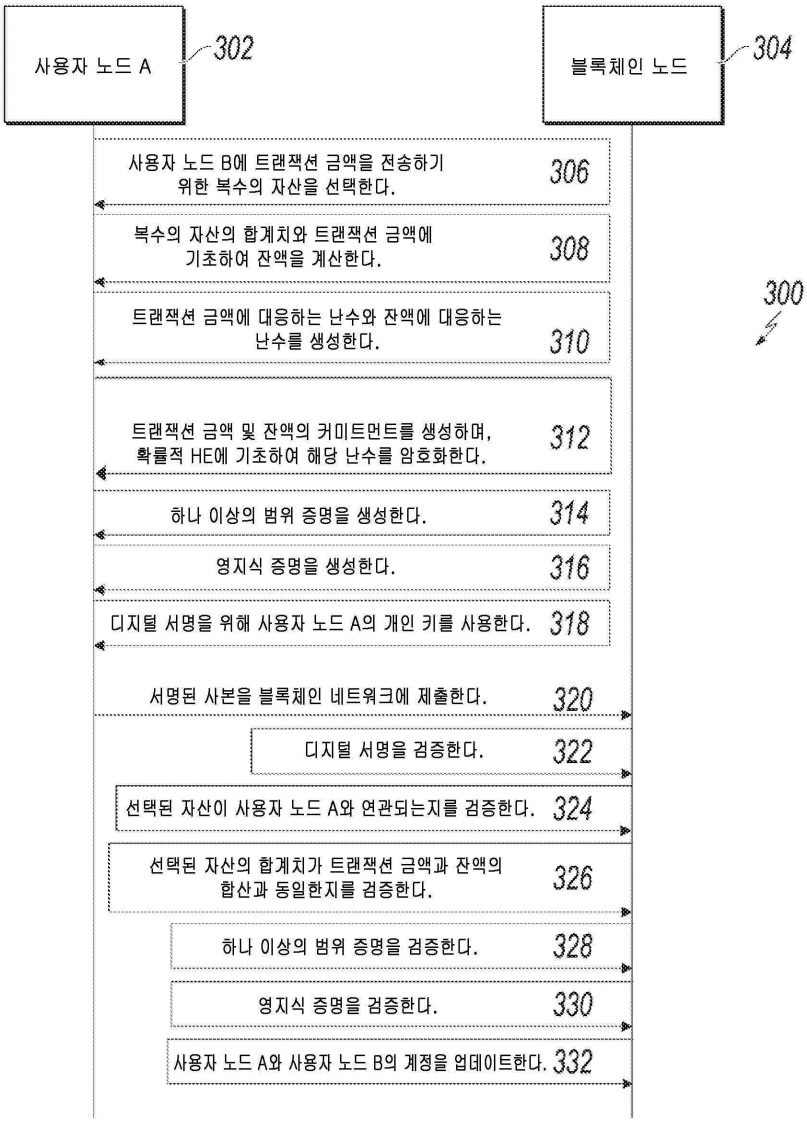
도면1



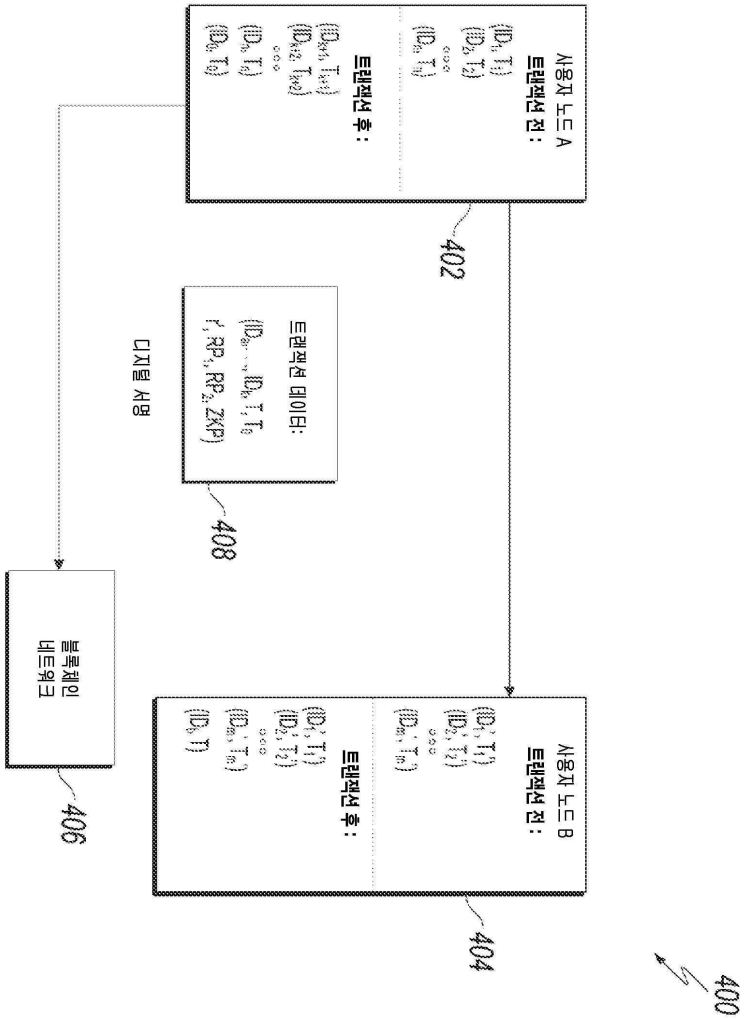
도면2


200
엔티티_1
엔티티_2
엔티티_3
208
208
208
트랜잭션 관리 시스템
트랜잭션 관리 시스템
트랜잭션 관리 시스템
202
204
210
210
210
블록체인 인터페이스
블록체인 인터페이스
블록체인 인터페이스
206
212
214
216

도면3


사용자 노드 A
302
블록체인 노드
304
300
사용자 노드 B에 트랜잭션 금액을 전송하기 위한 복수의 자산을 선택한다.
306
복수의 자산의 합계치와 트랜잭션 금액에 기초하여 잔액을 계산한다.
308
트랜잭션 금액에 대응하는 난수와 잔액에 대응하는 난수를 생성한다.
310
트랜잭션 금액 및 잔액의 커미트먼트를 생성하며, 확률적 HE에 기초하여 해당 난수를 암호화한다.
312
하나 이상의 범위 증명을 생성한다.
314
영지식 증명을 생성한다.
316
디지털 서명을 위해 사용자 노드 A의 개인 키를 사용한다.
318
서명된 사본을 블록체인 네트워크에 제출한다.
320
디지털 서명을 검증한다.
322
선택된 자산이 사용자 노드 A와 연관되는지를 검증한다.
324
선택된 자산의 합계치가 트랜잭션 금액과 잔액의 합산과 동일한지를 검증한다.
326
하나 이상의 범위 증명을 검증한다.
328
영지식 증명을 검증한다.
330
사용자 노드 A와 사용자 노드 B의 계정을 업데이트한다.
332

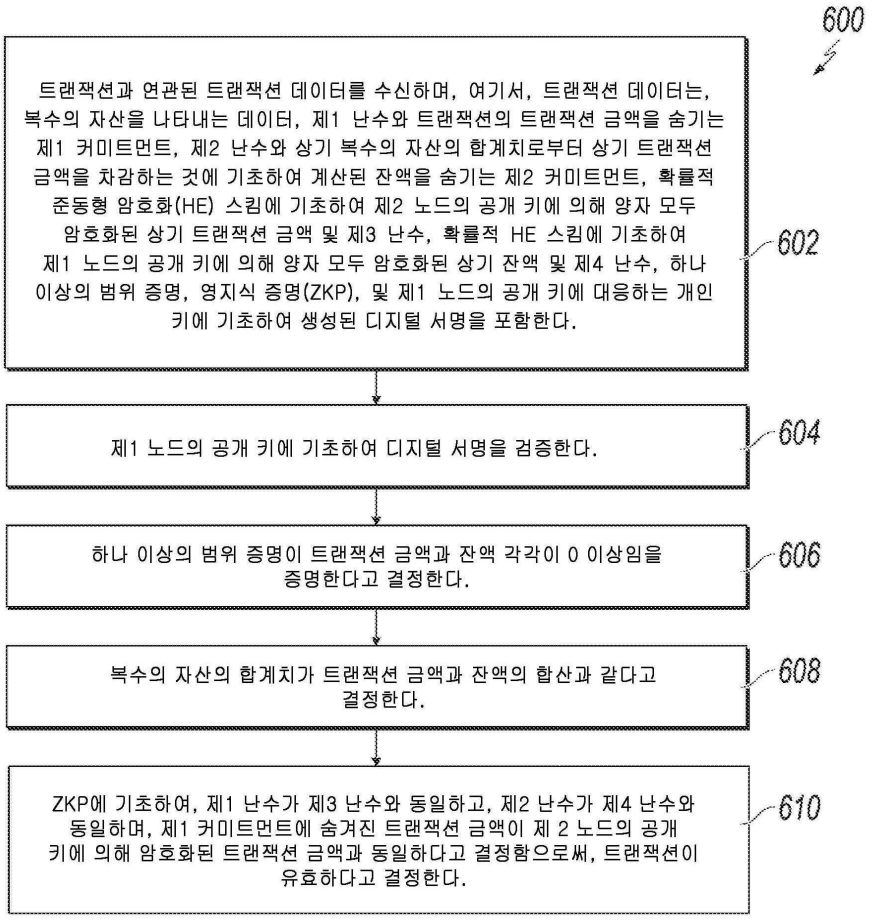
도면4


사용자 노드 A
트랜잭션 전 :
트랜잭션 후 :
사용자 노드 B
트랜잭션 전 :
트랜잭션 후 :
트랜잭션 데이터:
디지털 서명
블록체인 네트워크
402
404
406
408
400

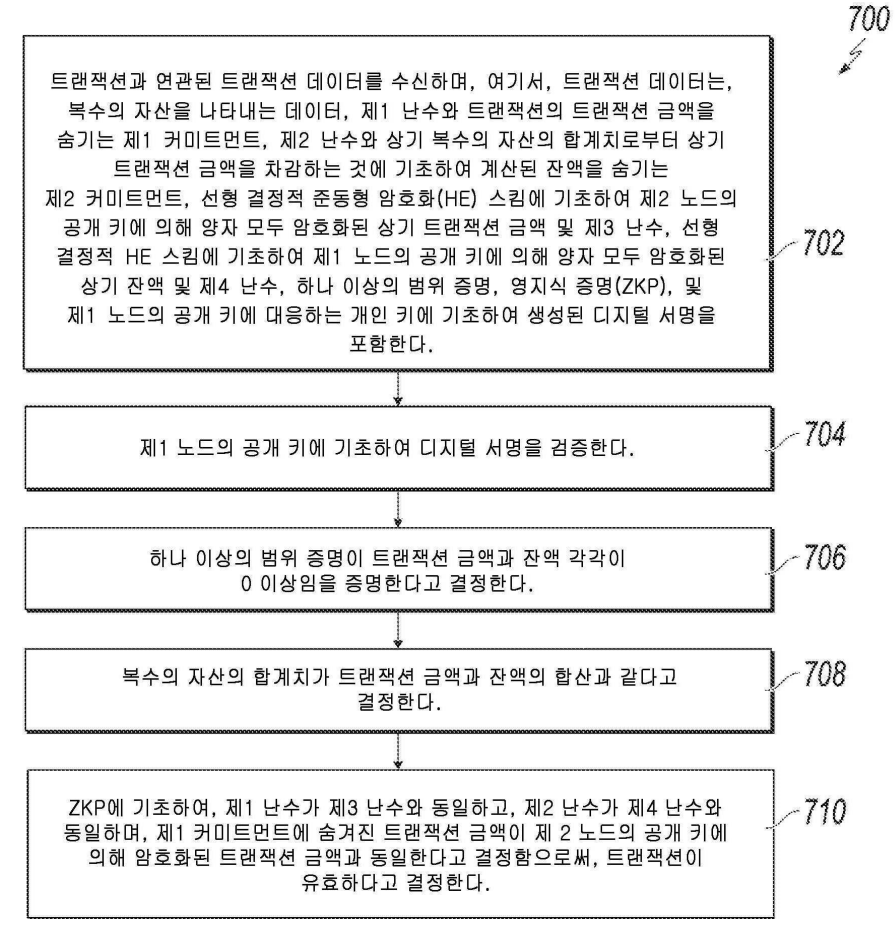
도면5


사용자 노드 A
502
블록체인 노드
504
500
사용자 노드 B에 트랜잭션 금액을 전송하기 위한 복수의 자산을 선택한다. 506
복수의 자산의 합계치와 트랜잭션 금액에 기초하여 잔액을 계산한다. 508
트랜잭션 금액에 대응하는 난수와 잔액에 대응하는 난수를 생성한다. 510
트랜잭션 금액 및 잔액의 커미트먼트를 생성하며, 결정적 HE에 기초하여 해당 난수를 암호화한다. 512
하나 이상의 범위 증명을 생성한다. 514
영지식 증명을 생성한다. 516
디지털 서명을 위해 사용자 노드 A의 개인 키를 사용한다. 518
서명된 사본을 블록체인 네트워크에 제출한다. 520
디지털 서명을 검증한다. 522
선택된 자산이 사용자 노드 A와 연관되는지를 검증한다. 524
선택된 자산의 합계치가 트랜잭션 금액과 잔액의 합산과 동일한지를 검증한다. 526
하나 이상의 범위 증명을 검증한다. 528
영지식 증명을 검증한다. 530
사용자 노드 A와 사용자 노드 B의 계정을 업데이트한다. 532

도면6


600
트랜잭션과 연관된 트랜잭션 데이터를 수신하며, 여기서, 트랜잭션 데이터는, 복수의 자산을 나타내는 데이터, 제1 난수와 트랜잭션의 트랜잭션 금액을 숨기는 제1 커미트먼트, 제2 난수와 상기 복수의 자산의 합계치로부터 상기 트랜잭션 금액을 차감하는 것에 기초하여 계산된 잔액을 숨기는 제2 커미트먼트, 확률적 준동형 암호화(HE) 스킴에 기초하여 제2 노드의 공개 키에 의해 양자 모두 암호화된 상기 트랜잭션 금액 및 제3 난수, 확률적 HE 스킴에 기초하여 제1 노드의 공개 키에 의해 양자 모두 암호화된 상기 잔액 및 제4 난수, 하나 이상의 범위 증명, 영지식 증명(ZKP), 및 제1 노드의 공개 키에 대응하는 개인 키에 기초하여 생성된 디지털 서명을 포함한다.
602
제1 노드의 공개 키에 기초하여 디지털 서명을 검증한다.
604
하나 이상의 범위 증명이 트랜잭션 금액과 잔액 각각이 0 이상임을 증명한다고 결정한다.
606
복수의 자산의 합계치가 트랜잭션 금액과 잔액의 합산과 같다고 결정한다.
608
ZKP에 기초하여, 제1 난수가 제3 난수와 동일하고, 제2 난수가 제4 난수와 동일하며, 제1 커미트먼트에 숨겨진 트랜잭션 금액이 제 2 노드의 공개 키에 의해 암호화된 트랜잭션 금액과 동일하다고 결정함으로써, 트랜잭션이 유효하다고 결정한다.
610

도면7


700
트랜잭션과 연관된 트랜잭션 데이터를 수신하며, 여기서, 트랜잭션 데이터는, 복수의 자산을 나타내는 데이터, 제1 난수와 트랜잭션의 트랜잭션 금액을 숨기는 제1 커미트먼트, 제2 난수와 상기 복수의 자산의 합계치로부터 상기 트랜잭션 금액을 차감하는 것에 기초하여 계산된 잔액을 숨기는 제2 커미트먼트, 선형 결정적 준동형 암호화(HE) 스킴에 기초하여 제2 노드의 공개 키에 의해 양자 모두 암호화된 상기 트랜잭션 금액 및 제3 난수, 선형 결정적 HE 스킴에 기초하여 제1 노드의 공개 키에 의해 양자 모두 암호화된 상기 잔액 및 제4 난수, 하나 이상의 범위 증명, 영지식 증명(ZKP), 및 제1 노드의 공개 키에 대응하는 개인 키에 기초하여 생성된 디지털 서명을 포함한다.
702
제1 노드의 공개 키에 기초하여 디지털 서명을 검증한다.
704
하나 이상의 범위 증명이 트랜잭션 금액과 잔액 각각이 0 이상임을 증명한다고 결정한다.
706
복수의 자산의 합계치가 트랜잭션 금액과 잔액의 합산과 같다고 결정한다.
708
ZKP에 기초하여, 제1 난수가 제3 난수와 동일하고, 제2 난수가 제4 난수와 동일하며, 제1 커미트먼트에 숨겨진 트랜잭션 금액이 제 2 노드의 공개 키에 의해 암호화된 트랜잭션 금액과 동일한다고 결정함으로써, 트랜잭션이 유효하다고 결정한다.
710

도면8

