(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2020년12월24일
(11) 등록번호 10-2194078
(24) 등록일자 2020년12월16일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *G06F 16/182* (2019.01)
G06Q 20/06 (2012.01) *G06Q 20/10* (2012.01)
G06Q 20/22 (2012.01) *G06Q 20/36* (2012.01)
H04L 9/06 (2006.01) *H04L 9/30* (2006.01)
(52) CPC특허분류
H04L 9/3218 (2013.01)
G06F 16/1824 (2019.01)
(21) 출원번호 10-2019-7032098
(22) 출원일자(국제) 2019년01월31일
심사청구일자 2019년12월02일
(85) 번역문제출일자 2019년10월29일
(65) 공개번호 10-2020-0096722
(43) 공개일자 2020년08월13일
(86) 국제출원번호 PCT/CN2019/074057
(87) 국제공개번호 WO 2019/072317
국제공개일자 2019년04월18일
(56) 선행기술조사문헌
CN108335106 A
US20180189877 A1
WO2018140830 A1
WO2018186874 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
레이 하오
중국 저지앙 311121 항저우 유 항 디스트릭트 웨스트 웬 이 로드 넘버 969 빌딩 3 알리바바 그룹 리갈 디파트먼트 5층
(뒷면에 계속)
(74) 대리인
김태홍, 김진희

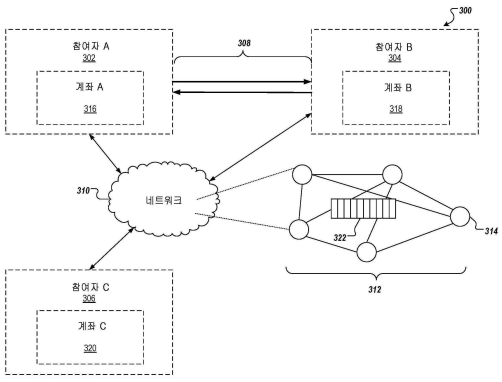
전체 청구항 수 : 총 13 항 심사관 : 양종필

(54) 발명의 명칭 **블록체인 네트워크 내 교차 자산 거래**

(57) 요 약

구현은 블록체인 네트워크에서 교차 자산 트레이딩에 관한 것이며, 제1 값, 제2 값 및 제2 노드의 환율에 기초하여 거래 정보를 제공하는 제1 노드를 포함하고, 제2 노드로부터 제1 증거 세트, 제1 범위 증명 및 제2 노드의 디지털 서명을 수신하고, 제1 범위 증명, 제2 범위 증명, 제1 증거 세트, 제2 증거 세트, 제1 노드의 디지털 서명 및 제2 노드의 디지털 서명에 기초하여 검증을 위한 거래를 제출하고, 거래는 제1 노드의 밸런스를 제1 값만큼 감소시키고, 제2 노드의 제1 밸런스를 제1 값만큼 증가시키고, 제2 노드의 제2 밸런스를 제2 값만큼 증가시키고, 제3 노드의 밸런스를 제2 값만큼 증가시키도록 실행된다.

대 표 도



(52) CPC특허분류
G06Q 20/0658 (2013.01)
G06Q 20/10 (2013.01)
G06Q 20/223 (2013.01)
G06Q 20/36 (2013.01)
H04L 9/0618 (2013.01)
H04L 9/0643 (2013.01)
H04L 9/30 (2013.01)
H04L 9/3239 (2013.01)
H04L 9/3247 (2013.01)

(72) 발명자
리 리춘
중국 저지앙 311121 항저우 유 항 디스트릭트 웨스트 웬 이 로드 넘버 969 빌딩 3 알리바바 그룹 리갈 디파트먼트 5층

후앙 장지에
중국 저지앙 311121 항저우 유 항 디스트릭트 웨스트 웬 이 로드 넘버 969 빌딩 3 알리바바 그룹 리갈 디파트먼트 5층

명 세 서

청구범위

청구항 1

블록체인 네트워크에서 프라이빗 교차 자산 트레이딩(private cross-asset trading)을 위한 컴퓨터 구현 방법(500)에 있어서,

상기 방법은 하나 이상의 프로세서에 의해 실행되고,

상기 블록체인 네트워크 내의 제1 노드에 의해 그리고 Boneh-Goh-Nissim(BGN) 암호화를 이용하여, 제1 값 및 제2 값에 기초하여 암호문을 생성하는 단계(506) - 상기 제2 값은 상기 제1 값의 동형 곱셈(homomorphic multiplication) 및 상기 블록체인 네트워크 내의 제2 노드에 의해 제공되는 암호화된 환율에 기초하여 결정되고, 상기 암호문 및 상기 암호화된 환율은 동일 타원 곡선(elliptic curve) 상에 있음 - ;

상기 제1 노드에 의해 상기 제2 노드에, 상기 제1 값 및 상기 암호문을 송신하는 단계(508);

상기 제1 노드에 의해 그리고 상기 제2 노드로부터, 상기 환율을 드러냄이 없이 영지식 증명(ZKP; zero-knowledge proof) 루틴에서 상기 환율을 검증하기 위해 사용될 수 있는 데이터의 세트를 포함하는 제1 증거 세트를 수신하는 단계(510);

상기 제1 노드에 의해, 상기 ZKP 루틴을 이용하여, 상기 암호문이 상기 제1 노드의 BGN 퍼블릭 키에 의해 암호화되는 것을 검증하기 위해 사용될 수 있는 데이터의 세트를 포함하는 제2 증거 세트를 생성하는 단계(512);

상기 제1 노드에 의해, 상기 제1 노드로부터 상기 제2 노드로의 상기 제1 값의 전달을 위한 상기 제1 노드와 상기 제2 노드 사이의 제1 거래, 및 상기 제2 노드로부터 제3 노드로의 상기 제2 값의 전달을 위한 상기 제2 노드와 상기 제3 노드 사이의 제2 거래를 포함하는 거래를 정의하는 단계; 및

상기 제1 노드에 의해, 상기 거래의 검증 및 실행을 위해 상기 블록체인 네트워크의 적어도 하나의 합의 노드에 상기 거래를 송신하는 단계(514) - 상기 거래는 상기 제1 증거 세트 및 상기 제2 증거 세트에 기초하여 검증되고, 상기 거래를 검증하는 것에 응답하여, 상기 제1 노드의 밸런스를 상기 제1 값만큼 감소시키고, 상기 제2 노드의 제1 밸런스를 상기 제1 값만큼 증가시키고, 상기 제2 노드의 제2 밸런스를 상기 제2 값만큼 감소시키고, 상기 제3 노드의 밸런스를 상기 제2 값만큼 증가시키도록, 상기 제1 거래 및 상기 제2 거래를 실행함 -

를 포함하는, 컴퓨터 구현 방법.

청구항 2

제1항에 있어서,

상기 제1 증거 세트는, 상기 제1 값, 상기 제1 노드에 의해 제공되는 한 쌍의 난수, 및 상기 암호문에 기초하여, 상기 제2 노드에 의해 제공되는 것인, 컴퓨터 구현 방법.

청구항 3

제1항에 있어서,

상기 적어도 하나의 합의 노드에 의해 상기 거래를 검증하는 것은, 상기 제1 노드의 디지털 서명 및 상기 제2 노드의 디지털 서명을 검증하는 것을 포함하는 것인, 컴퓨터 구현 방법.

청구항 4

제1항에 있어서,

상기 적어도 하나의 합의 노드에 의해 상기 거래를 검증하는 것은, 상기 제1 노드에 의해 제공되는 제1 범위 증명 및 상기 제2 노드에 의해 제공되는 제2 범위 증명을 검증하는 것을 포함하는 것인, 컴퓨터 구현 방법.

청구항 5

제4항에 있어서,

상기 제1 범위 증명은, 상기 제1 값이 0보다 크고, 상기 제1 노드의 밸런스가 상기 제1 값보다 크거나 같음을 증명하기 위해 ZKP를 포함하는 것인, 컴퓨터 구현 방법.

청구항 6

제4항에 있어서,

상기 제2 범위 증명은, 상기 제2 노드의 제2 밸런스가 상기 제2 값보다 크거나 같음을 증명하기 위해 ZKP를 포함하는 것인, 컴퓨터 구현 방법.

청구항 7

제1항에 있어서,

상기 거래는, BGN 암호화를 이용하여 생성된 암호문의 세트를 포함하는 데이터 세트를 더 포함하고, 상기 데이터 세트는 상기 적어도 하나의 합의 노드에 의해 상기 거래를 검증하기 위해 사용되는 것인, 컴퓨터 구현 방법.

청구항 8

제1항에 있어서,

상기 제1 노드에 의해, 상기 블록체인 네트워크의 서브 체인 채널을 통해 상기 제2 노드로부터 상기 환율을 수신하는 단계를 더 포함하는, 컴퓨터 구현 방법.

청구항 9

제1항에 있어서,

상기 암호문 중 적어도 하나의 암호문은 페더슨 커밋먼트(Pedersen Commitment)를 이용하여 제공되는 것인, 컴퓨터 구현 방법.

청구항 10

제1항에 있어서,

상기 제1 증거 세트의 데이터의 세트는 제1 데이터 값 및 제2 데이터 값을 포함하고, 상기 제1 데이터 값 및 상기 제2 데이터 값의 각각은 상기 제2 노드의 BGN 퍼블릭 키를 생성하기 위해 사용되는 파라미터에 기초하여 결정되는 것인, 컴퓨터 구현 방법.

청구항 11

제1항에 있어서,

상기 제2 증거 세트의 데이터의 세트는 암호문의 세트 및 값의 세트를 포함하고, 상기 값의 세트에서의 각 값은 상기 암호문의 세트의 해시에 기초하는 것인, 컴퓨터 구현 방법.

청구항 12

블록체인 네트워크에서 프라이빗 교차 자산 트레이딩(private cross-asset trading)을 위한 명령어를 저장한 컴퓨터 판독가능 저장 매체에 있어서,

상기 명령어는, 하나 이상의 프로세서에 의해 실행 가능하고 상기 하나 이상의 프로세서로 하여금, 제1항 내지 제11항 중 어느 한 항에 따른 방법을 수행하게 하는 것인, 컴퓨터 판독가능 저장 매체.

청구항 13

시스템에 있어서,

하나 이상의 프로세서; 및

상기 하나 이상의 프로세서와 결합되고, 블록체인 네트워크에서 프라이빗 교차 자산 트레이딩(private cross-

asset trading)을 위한 명령어가 저장된 하나 이상의 컴퓨터 판독가능 메모리

를 포함하고,

상기 명령어는, 제1항 내지 제11항 중 어느 한 항에 따른 방법을 수행하기 위해, 상기 하나 이상의 프로세서에 의해 실행 가능한 것인, 시스템.

청구항 14

삭제

청구항 15

삭제

청구항 16

삭제

청구항 17

삭제

청구항 18

삭제

청구항 19

삭제

청구항 20

삭제

청구항 21

삭제

청구항 22

삭제

청구항 23

삭제

청구항 24

삭제

청구항 25

삭제

청구항 26

삭제

청구항 27

삭제

청구항 28

삭제

청구항 29

삭제

청구항 30

삭제

청구항 31

삭제

청구항 32

삭제

청구항 33

삭제

발명의 설명

기 술 분 야

배 경 기 술

[0001] 합의 네트워크(consensus network) 및/또는 블록체인 네트워크로서 또한 지칭될 수 있는, 분산 원장 시스템(DLS; distributed ledger system)은 참여 엔티티들이 데이터를 안전하고 불변적으로 저장할 수 있게 한다. DLS는 일반적으로 임의의 특정 사용 사례를 참조함이 없이 블록체인 네트워크로서 지칭된다. 블록체인 네트워크의 예시적인 유형은 퍼블릭 블록체인 네트워크(public blockchain network), 프라이빗 블록체인 네트워크(private blockchain network) 및 컨소시엄 블록체인 네트워크(consortium blockchain network)를 포함할 수 있다. 퍼블릭 블록체인 네트워크는 DLS를 사용하고, 합의 프로세스에 참여하도록 모든 엔티티에 대해 공개된다. 프라이빗 블록체인 네트워크는, 읽기 및 쓰기 허가를 중앙적으로 제어하는 특정 엔티티에 대해 제공된다. 컨소시엄 블록체인 네트워크는, 합의 프로세스를 제어하고 액세스 제어 계층(access control layer)을 포함하는 엔티티의 선택 그룹에 대해 제공된다.

[0002] 블록체인 네트워크는 통화(currency)와 같은 디지털 자산의 전달 및 교환을 통해 트레이딩 가치를 위해 사용될 수 있다. 디지털 자산의 여러가지 상이한 유형은, 디지털 자산을 블록체인 네트워크의 하나의 노드로부터 다른 노드로 전달함으로써 블록체인 네트워크 내에서 교환될 수 있다. 일부 사례에서, 블록체인 네트워크 내에서 디지털 자산을 전달하는 것은 환율에 기초하여 제1 유형의 디지털 자산을 제2 유형의 디지털 자산으로 교환하는 것을 수반한다.

[0003] 그러나, 블록체인 네트워크의 참여자들은, 합의 노드를 포함하는 다른 참여자들이 거래의 세부 사항(예를 들어, 거래 금액, 환율)을 알지 못하도록 그들의 거래에서 프라이버시를 원할 수 있다. 프라이버시를 제공하기 위해 암호화 방법(encryption schemes)이 사용될 수 있다. 그러나, 일부 암호화 방법은 동형 곱셈(homomorphic multiplication)과 같은 곱셈 연산을 지원하지 않는다. 이러한 곱셈 연산을 지원하기 위한 일부 암호화 방법이 지만, 이들은 오로지 단일 곱셈 연산으로만 제한된다. 이는 환율의 프라이버시를 유지하기 위해 예를 들어, 환율을 포함하는 교차 자산 거래에서의 참여자들의 능력을 억제한다.

발명의 내용

[0004] 본 명세서의 구현은 블록체인 네트워크 내에서 통화를 전달하기 위한 컴퓨터 구현 방법을 포함한다. 보다 구체적으로, 본 명세서의 구현은 암호화된 거래 데이터 및 암호화된 환율을 이용하는 블록체인 네트워크 내의 교차 자산 거래에 관한 것이다.

[0005] 일부 구현에서, 작용들은 블록체인 네트워크 내의 제1 노드에 의해 그리고 Boneh-Goh-Nissim(BGN) 암호화를 이용하여, 제1 값 및 제2 값에 기초하여 암호문을 생성하는 단계로서, 제2 값은 제1 값 및 블록체인 네트워크 내의 제2 노드에 의해 제공되는 환율에 기초하여 결정되고, 제1 노드에 의해 제2 노드에, 제1 값 및 암호문을 송신하는 단계, 제1 노드에 의해 그리고 제2 노드로부터, 환율을 드러냄이 없이 영지식 증명(ZKP; zero-knowledge proof) 루틴에서 환율을 검증하기 위해 사용될 수 있는 데이터의 세트를 포함하는 제1 증거 세트를 수신하는 단계, 제1 노드에 의해, ZKP 루틴을 이용하여, 암호문이 제1 노드의 BGN 퍼블릭 키에 의해 암호화되는 것을 검증하기 위해 사용될 수 있는 데이터의 세트를 포함하는 제2 증거 세트를 생성하는 단계, 제1 노드에 의해, 제1 노드로부터 제2 노드에 제1 값의 전달을 위한 제1 노드와 제2 노드 사이의 제1 거래, 및 제2 노드로부터 제3 노드에 제2 값의 전달을 위한 제2 노드와 제3 노드 사이의 제2 거래를 포함하는 거래를 정의하는 단계, 제1 노드에 의해, 거래의 검증 및 실행을 위해 블록체인 네트워크의 적어도 하나의 합의 노드에 거래를 송신하는 단계로서, 거래는 제1 증거 세트 및 제2 증거 세트에 기초하여 검증되고, 거래를 검증하는 것에 응답하여, 제1 노드의 밸런스(balance)를 제1 값만큼 감소시키고, 제2 노드의 제1 밸런스를 제1 값만큼 증가시키고, 제2 노드의 제2 밸런스를 제2 값만큼 감소시키고, 제3 노드의 밸런스를 제2 값만큼 증가시키도록 제1 거래 및 제2 거래를 실행한다. 다른 구현은 컴퓨터 저장 디바이스 상에 인코딩된, 방법의 작용을 수행하도록 구성된, 대응하는 시스템, 장치 및 컴퓨터 프로그램을 포함한다.

[0006] 이들 및 다른 구현은 다음 특징 중 하나 이상을 각각 선택적으로 포함할 수 있다: 제1 증거 세트는 제1 값, 제1 노드에 의해 제공되는 한 쌍의 난수 및 암호문에 기초하여 제2 노드에 의해 제공되고; 적어도 하나의 합의 노드에 의해 거래를 검증하는 것은 제1 노드의 디지털 서명 및 제2 노드의 디지털 서명을 검증하는 단계를 포함하고; 적어도 하나의 합의 노드에 의해 거래를 검증하는 것은 제1 노드에 의해 제공되는 제1 범위 증명 및 제2 노드에 의해 제공되는 제2 범위 증명을 검증하는 단계를 포함하고; 제1 범위 증명은, 제1 값이 0보다 크고, 제1 노드의 밸런스가 제1 값보다 크거나 같음을 증명하기 위해 ZKP를 포함하고; 제2 범위 증명은 제2 노드의 제2 밸런스가 제2 값보다 크거나 같음을 증명하기 위해 ZKP를 포함하고; 거래는, BGN 암호화에 적어도 부분적으로 기초하여 생성된 암호문의 세트를 포함하는 데이터 세트를 더 포함하고, 데이터 세트는 적어도 하나의 합의 노드에 의해 거래를 검증하기 위해 사용되고; 작용은, 제1 노드에 의해, 블록체인 네트워크의 서브 체인 채널을 통해 제2 노드로부터 환율을 수신하는 단계를 더 포함하고; 암호문 중 적어도 하나의 암호문은 페더슨 커밋먼트(Pedersen Commitment)를 이용하여 제공되고; 제1 증거 세트의 데이터의 세트는 제1 데이터 값 및 제2 데이터 값을 포함하고, 제1 데이터 값 및 제2 데이터 값의 각각은 제2 노드의 BGN 퍼블릭 키를 생성하기 위해 사용되는 파라미터에 기초하여 결정되고; 제2 증거 세트의 데이터의 세트는 암호문의 세트 및 값의 세트를 포함하고, 값의 세트에서의 각 값은 암호문의 세트의 해시에 적어도 부분적으로 기초한다.

[0007] 본 명세서는 또한, 하나 이상의 프로세서에 결합되고, 하나 이상의 프로세서에 의해 실행될 때, 하나 이상의 프로세서로 하여금 본 명세서에서 제공되는 방법의 구현에 따른 동작을 수행하게 하는 저장된 명령어를 가지는 하나 이상의 비 일시적 컴퓨터 판독가능 저장 매체를 제공한다.

[0008] 본 명세서는 또한 본 명세서에서 제공되는 방법을 구현하기 위한 시스템을 제공한다. 시스템은 하나 이상의 프로세서, 및 하나 이상의 프로세서에 의해 실행될 때, 하나 이상의 프로세서로 하여금 본 명세서에서 제공되는 방법의 구현에 따른 동작을 수행하게 하는 저장된 명령어를 가지는 하나 이상의 프로세서에 결합된 컴퓨터 판독가능 저장 매체를 포함한다.

[0009] 본 명세서에 따른 방법은 본 명세서에 설명된 양태 및 특징의 임의의 조합을 포함할 수 있다는 것이 이해된다. 즉, 본 명세서에 따른 방법은 본 명세서에 명확하게 설명된 양태 및 특징의 조합으로 제한되지 않을 뿐만 아니라, 제공되는 양태 및 특징의 임의의 조합을 포함한다.

[0010] 본 명세서의 하나 이상의 구현의 세부 사항은 첨부 도면 및 이하의 설명에 제시되어 있다. 본 명세서의 다른 특징 및 장점은 상세한 설명 및 도면으로부터, 그리고 청구 범위로부터 명백해질 것이다.

도면의 간단한 설명

[0011] 도 1은 본 명세서의 구현을 실행하는데 사용될 수 있는 환경의 예를 도시한다.

도 2는 본 명세서의 구현에 따른 개념적 아키텍처의 예를 도시한다.

도 3은 본 명세서의 구현에 따른 교차 자산 트레이딩 플랫폼의 예를 도시한다.

도 4는 본 명세서의 구현에 따라 교차 자산 거래를 실행하기 위한 신호 다이어그램의 예를 도시한다.

도 5는 본 명세서의 구현에 따라 실행될 수 있는 프로세스의 예를 도시한다.

도 6은 본 명세서의 구현에 따른 장치의 모듈의 예를 도시한다.

다양한 도면에서 유사한 참조 번호는 유사한 요소를 나타낸다.

발명을 실시하기 위한 구체적인 내용

[0012] 본 명세서의 구현은 블록체인 네트워크 내에서 자산을 전달하기 위한 컴퓨터 구현 방법을 포함한다. 보다 구체적으로, 본 명세서의 구현은 암호화된 거래 데이터 및 암호화된 환율을 이용하는 블록체인 네트워크 내의 교차 자산 거래에 관한 것이다.

[0013] 본 명세서의 구현을 위한 추가적인 맥락을 제공하기 위해, 그리고 상술한 바와 같이, 합의 네트워크(예를 들어, 피어-투-피어(peer-to-peer) 노드로 구성됨) 및 블록체인 네트워크로서 또한 지칭될 수 있는, 분산 원장 시스템(DLS; distributed ledger system)은 참여 엔티티가 안전하고 불변적으로 거래를 수행하고, 데이터를 저장할 수 있게 한다. 블록체인이라는 용어는 일반적으로 특정 네트워크 및/또는 사용 사례들과 연관되지만, 블록체인은 일반적으로 임의의 특정 사용 사례를 참조함이 없이 DLS를 지칭하기 위해 여기에서 사용된다.

[0014] 블록체인은 거래가 불변인 방식으로 거래를 저장하는 데이터 구조이다. 따라서, 블록체인 상에 기록된 거래는 신뢰할 수 있고 신용할 수 있다. 블록체인은 하나 이상의 블록을 포함한다. 체인에서 각 블록은, 이전 블록의 암호화 해시(cryptographic hash)를 포함함으로써 체인에서 그것의 바로 전의 이전 블록에 연결된다. 각 블록은 또한, 타임스탬프(timestamp), 자체 암호화 해시 및 하나 이상의 거래를 포함한다. 블록체인 네트워크의 노드에 의해 이미 검증된 거래는 해싱되고 머클 트리(Merkle tree)로 인코딩된다. 머클 트리는 트리의 리프 노드(leaf node)에 있는 데이터가 해싱되는 데이터 구조이고, 트리의 각 브랜치(branch)에 있는 모든 해시는 브랜치의 루트(root)에 연쇄(concatenate)된다. 이러한 프로세스는 트리에서 모든 데이터를 나타내는 해시를 저장하는, 전체 트리의 루트까지 트리를 계속한다. 트리에 저장된 거래로 주장되는 해시는 트리의 구조와 일치하는지 여부를 결정함으로써 신속하게 검증될 수 있다.

[0015] 블록체인이 거래를 저장하기 위해 분산되거나 적어도 부분적으로 분산되는 데이터 구조인 반면, 블록체인 네트워크는 거래를 브로드캐스팅하고, 검증하며 유효화하는 등에 의해 하나 이상의 블록체인을 관리, 업데이트 및 유지하는 컴퓨팅 노드의 네트워크이다. 컨소시엄 블록체인 네트워크는 참여 엔티티들 사이에서 프라이빗이다. 컨소시엄 블록체인 네트워크에서, 합의 프로세스는 노드의 승인된 세트에 의해 제어되고, 하나 이상의 노드는 각각의 엔티티(예를 들어, 금융기관, 보험 회사)에 의해 운영된다. 예를 들어, 열(10)개의 엔티티(예를 들어, 금융기관, 보험 회사)의 컨소시엄이 컨소시엄 블록체인 네트워크를 운영할 수 있으며, 이들의 각각은 컨소시엄 블록체인 네트워크 내의 적어도 하나의 노드를 운영한다. 따라서, 컨소시엄 블록체인 네트워크는 참여 엔티티와 관련하여 프라이빗 네트워크로 간주될 수 있다. 일부 예들에서, 각 엔티티(노드)는, 유효화되고 블록체인에 추가되는 블록을 위해 매 블록을 사인(sign)해야 한다. 일부 예들에서, 적어도 엔티티(노드)(예를 들어, 적어도 7개의 엔티티)의 서브세트는, 유효화되고 블록체인에 추가되는 블록을 위해 매 블록을 사인해야 한다.

[0016] 상술한 바와 같이, 블록체인 네트워크는 퍼블릭 블록체인 네트워크, 프라이빗 블록체인 네트워크, 또는 컨소시엄 블록체인 네트워크로서 제공될 수 있다. 본 명세서의 구현은 컨소시엄 블록체인 네트워크를 참조하여 여기에서 더 상세히 설명된다. 그러나, 본 명세서의 구현은 블록체인 네트워크의 임의의 적절한 유형에서 실현될 수 있는 것으로 고려된다. 본 명세서에서 설명된 기술은 컨소시엄 블록체인 네트워크와 관련이 있는 것으로 나타나지만, 기술은 퍼블릭 블록체인 네트워크 및 프라이빗 블록체인 네트워크를 포함하는 다른 유형의 블록체인 네트워크에서 변경과 함께 또는 변경 없이 또한 사용될 수 있다.

[0017] 일반적으로, 컨소시엄 블록체인 네트워크는 참여하는 엔티티들 사이에서 프라이빗이다. 컨소시엄 블록체인 네트워크에서, 합의 프로세스는 합의 노드로서 지칭될 수 있는 노드의 허가된 세트에 의해 제어되고, 하나 이상의 합의 노드는 각각의 엔티티(예를 들어, 금융기관, 보험 회사)에 의해 운영된다. 예를 들어, 열(10)개 엔티티(예를 들어, 금융기관, 보험 회사)의 컨소시엄은 컨소시엄 블록체인 네트워크를 운영할 수 있고, 이들의 각각은 컨소시엄 블록체인 네트워크 내의 적어도 하나의 노드를 운영한다.

[0018] 일부 예들에서, 컨소시엄 블록체인 네트워크 내에서, 글로벌 블록체인은 모든 노드에 걸쳐 복제되는 블록체인으로서 제공된다. 즉, 모든 합의 노드는 글로벌 블록체인과 관련하여 완벽한 상태 합의에 있다. 합의(예를 들어, 블록체인에 대한 블록 추가 약정)를 달성하기 위해, 합의 프로토콜이 컨소시엄 블록체인 네트워크 내에서 구현된다. 예시적인 합의 프로토콜은, 제한 없이, 실용 비잔틴 장애 허용(PBFT; practical Byzantine fault

tolerance), 작업 증명(POW; proof-of-work), 지분 증명 (POS; proof-of-stake) 및 권한 증명 (POA; proof-of-authority)을 포함한다.

[0019] 컨소시엄 블록체인 네트워크는 디지털 자산의 전달 및 교환을 수행하는데 사용될 수 있다. 일부 예에서, 디지털 자산은 현실 세계 자산을 나타낼 수 있다. 일부 사례에서, 디지털 자산은 가상 자산을 나타낼 수 있다. 예를 들어, 가상 자산은 현실 세계 가치를 나타낼 수 있고, 제품 및/또는 서비스를 구매하는데 사용될 수 있다. 가상 자산은 현실 세계, 물리적 자산(예를 들어, 중국 RMB, 미국 달러)에 대한 대안으로서 제공된다. 컨소시엄 블록체인 네트워크 내에서 거래를 수행하는 것은, 컨소시엄 블록체인 네트워크가 거래를 검증하고, 불변적으로 기록함에 따라, 추가적인 보안을 제공한다. 본 명세서의 구현들은 통화들(예를 들어, RMB, USD)을 참조하여 본 명세서에서 더 상세히 설명된다. 그러나, 구현은 임의의 적절한 디지털 자산으로 실현될 수 있다는 것이 고려된다.

[0020] 도 1은 본 명세서의 구현을 실행하는데 사용될 수 있는 환경(100)의 예를 도시한다. 일부 예에서, 환경(100)은 엔티티가 컨소시엄 블록체인 네트워크(102)에 참여하는 것을 가능하게 한다. 환경(100)은 컴퓨팅 디바이스(106, 108) 및 네트워크(110)를 포함한다. 일부 예에서, 네트워크(110)는 근거리 네트워크(LAN; local area network), 원거리 네트워크(WAN; wide area network), 인터넷, 또는 이들의 조합을 포함하고, 웹 사이트, 사용자 디바이스(예를 들어, 컴퓨팅 디바이스), 및 백-엔드 시스템을 연결한다. 일부 예에서, 네트워크(110)는 유선 및/또는 무선 통신 링크를 통해 액세스될 수 있다.

[0021] 도시된 예에서, 컴퓨팅 시스템(106, 108)은 각각 컨소시엄 블록체인 네트워크(102)에서 노드로서의 참여를 가능하게 하는 임의의 적절한 컴퓨팅 시스템을 포함할 수 있다. 예시적인 컴퓨팅 디바이스는, 제한 없이, 서버, 데스크탑 컴퓨터, 랩탑 컴퓨터, 태블릿 컴퓨팅 디바이스 및 스마트폰을 포함한다. 일부 예에서, 컴퓨팅 시스템(106, 108)은 컨소시엄 블록체인 네트워크(102)와 상호작용하기 위한 하나 이상의 컴퓨터 구현 서비스를 호스팅(host)한다. 예를 들어, 컴퓨팅 시스템(106)은, 제1 엔티티가 하나 이상의 다른 엔티티(예를 들어, 다른 사용자)와의 거래를 관리하기 위해 사용하는 거래 관리 시스템과 같은, 제1 엔티티(예를 들어, 사용자 A)의 컴퓨터 구현 서비스들을 호스팅할 수 있다. 컴퓨팅 시스템(108)은, 제2 엔티티가 하나 이상의 다른 엔티티(예를 들어, 다른 사용자)와의 거래를 관리하기 위해 사용하는 거래 관리 시스템과 같은, 제2 엔티티(예를 들어, 사용자 B)의 컴퓨터 구현 서비스를 호스팅할 수 있다. 도 1의 예에서, 컨소시엄 블록체인 네트워크(102)는 노드의 피어-투-피어 네트워크로서 표현되고, 컴퓨팅 시스템(106, 108)은 컨소시엄 블록체인 네트워크(102)에 참여하는 제1 엔티티 및 제2 엔티티 각각의 노드를 제공한다.

[0022] 도 2는 본 명세서의 구현에 따른 개념적 아키텍처(200)의 예를 도시한다. 개념적 아키텍처(200)는 엔티티 계층(202), 호스팅된 서비스 계층(204), 및 블록체인 네트워크 계층(206)을 포함한다. 도시된 예에서, 엔티티 계층(202)은 세 참여자, 즉 참여자 A, 참여자 B 및 참여자 C를 포함하고, 각 참여자는 각각의 거래 관리 시스템(208)을 가진다.

[0023] 도시된 예에서, 호스팅된 서비스 계층(204)은 각 거래 관리 시스템(210)에 대한 인터페이스(210)를 포함한다. 일부 예에서, 각각의 거래 관리 시스템(208)은 프로토콜(예를 들어, 하이퍼텍스트 전송 프로토콜 보안(HTTPS; hypertext transfer protocol secure))을 사용하는 네트워크(예를 들어, 도 1의 네트워크(110))를 통해 각각의 인터페이스(210)와 통신한다. 일부 예에서, 각 인터페이스(210)는 각각의 거래 관리 시스템(208)과 블록체인 네트워크 계층(206) 사이의 통신 접속을 제공한다. 보다 구체적으로, 인터페이스(210)는 블록체인 네트워크 계층(206)의 블록체인 네트워크(212)와 통신한다. 일부 예에서, 인터페이스(210)와 블록체인 네트워크 계층(206) 사이의 통신은 원격 프로시저 호출(RPC; remote procedure call)을 이용하여 수행된다. 일부 예에서, 인터페이스(210)는 각각의 거래 관리 시스템(208)에 대한 블록체인 네트워크 노드를 "호스팅"한다. 예를 들어, 인터페이스(210)는 블록체인 네트워크(212)에 액세스하기 위해 애플리케이션 프로그래밍 인터페이스(API; application programming interface)를 제공한다.

[0024] 본 명세서에서 설명된 바와 같이, 블록체인 네트워크(212)는 블록체인(216)에 정보를 불변적으로 기록하는 복수의 노드(214)를 포함하는 피어-투-피어 네트워크로서 제공된다. 단일 블록체인(216)이 개략적으로 도시되어 있지만, 블록체인(216)의 다수의 사본이 제공되고, 블록체인 네트워크(212)에 걸쳐 유지된다. 예를 들어, 각 노드(214)는 블록체인의 사본을 저장한다. 일부 구현에서, 블록체인(216)은 컨소시엄 블록체인 네트워크에 참여하는 둘 이상의 엔티티 사이에서 수행되는 거래와 연관된 정보를 저장한다.

[0025] 블록체인(예를 들어, 도 2의 블록체인(216))은 블록들의 체인으로 구성되며, 각 블록은 데이터를 저장한다. 예시적인 데이터는 둘 이상의 참여자들 간의 거래를 나타내는 거래 데이터를 포함한다. 거래가 비-제한적인 예로서 본 명세서에서 사용되지만, 임의의 적절한 데이터가 블록체인(예를 들어, 문서, 이미지, 비디오, 오디오)에

저장될 수 있다는 것이 고려된다. 예시적인 거래는, 제한 없이, 가치가 있는 것(예를 들어, 자산, 제품, 서비스, 통화)의 교환을 포함할 수 있다. 거래 데이터는 블록체인 내에 불변적으로 저장된다. 즉, 거래 데이터는 변경될 수 없다.

[0026] 블록에 저장하기 전에, 거래 데이터는 해싱(hash)된다. 해싱은 거래 데이터(문자열 데이터로서 제공됨)를 고정된 길이의 해시 값(또한 문자열 데이터로서도 제공됨)으로 변환하는 프로세스이다. 거래 데이터를 획득하기 위해 해시 값을 언-해싱(un-hash)하는 것은 불가능하다. 해싱은 거래 데이터에서 약간의 변화조차도 완전히 상이한 해시 값을 초래하는 것을 보장한다. 또한, 앞서 언급한 바와 같이, 해시 값은 고정된 길이이다. 즉, 거래 데이터의 크기와 관계없이, 해시 값의 길이는 고정된다. 해싱은 해시 값을 생성하도록 해시 함수를 통해 거래 데이터를 처리하는 것을 포함한다. 해시 함수의 예는, 제한 없이, 256-비트 해시 값을 출력하는 안전한 해시 알고리즘(SHA; secure hash algorithm)(SHA)-256을 포함한다.

[0027] 복수의 거래의 거래 데이터는 하나의 블록에서 해싱되고 저장된다. 예를 들어, 두 거래의 해시 값이 제공되고, 다른 해시를 제공하도록 그들 자체가 해싱된다. 이러한 프로세스는 블록에 저장될 모든 거래에 대해, 단일 해시 값이 제공될 때까지 반복된다. 이러한 해시 값은 머클 루트 해시(Merkle root hash)로서 지칭되며, 블록의 헤더에 저장된다. 임의의 거래의 변화는 그의 해시 값의 변화를 초래할 것이고, 궁극적으로, 머클 루트 해시의 변화를 초래할 것이다.

[0028] 블록들은 합의 프로토콜을 통해 블록체인에 추가된다. 블록체인 네트워크 내의 다수의 노드는 합의 프로토콜에 참여하고, 블록체인에 추가된 블록을 가지도록 작업을 수행한다. 이러한 노드는 합의 노드로서 지칭된다. 앞서 설명된 PBFT는 합의 프로토콜의 비제한적인 예로서 사용된다. 합의 노드는 블록체인에 거래를 추가하도록 합의 프로토콜을 실행한다.

[0029] 보다 구체적으로, 합의 노드는 블록 헤더를 생성하고, 블록에서의 모든 거래들을 해싱하며, 단일 해시 값이 블록에서의 모든 거래에 대해 제공될 때까지 추가적인 해시 값을 생성하도록 해시 값을 쌍으로 결합한다(머클 루트 해시). 이러한 해시는 블록 헤더에 추가된다. 합의 노드는 또한 블록체인에서의 가장 최근의 블록(즉, 블록체인에 부가된 가장 마지막 블록)의 해시 값을 결정한다. 합의 노드는 또한 넌스 값(nonce value) 및 타임스탬프를 블록 헤더에 추가한다.

[0030] 일반적으로, PBFT는 비잔틴 장애(예를 들어, 기능장애 노드, 악성 노드)를 용인하는 실용 비잔틴 상태 기계 복제(practical Byzantine state machine replication)를 제공한다. 이는 장애가 발생할 것이라고 가정함으로써 PBFT에서 달성된다(예를 들어, 독립 노드 장애, 및/또는 합의 노드에 의해 전송된 조작된 메시지들의 존재를 가정). PBFT에서, 합의 노드는 일차 합의 노드(primary consensus node) 및 백업 합의 노드(backup consensus nodes)를 포함하는 시퀀스에서 제공된다. 일차 합의 노드는 주기적으로 변경되며, 거래는 블록체인 네트워크의 세계 상태에 대한 약정에 도달하는 블록체인 네트워크 내의 모든 합의 노드에 의해 블록체인에 추가된다. 이러한 프로세스에서, 메시지는 합의 노드들 간에 송신되며, 각 합의 노드는 메시지가 특정 피어 노드로부터 수신되었음을 증명하고, 메시지가 송신 중에 수정되지 않았음을 검증한다.

[0031] PBFT에서, 합의 프로토콜은 동일한 상태에서 시작하는 모든 합의 노드를 가지는 다수의 양상으로 제공된다. 시작하기 위해, 클라이언트는 서비스 동작을 호출(invoke)(예를 들어, 블록체인 네트워크 내에서 거래를 실행)하도록 요청을 일차 합의 노드에 전송한다. 요청을 수신한 것에 응답하여, 일차 합의 노드는 요청을 백업 합의 노드에 멀티캐스트(multicast)한다. 백업 합의 노드는 요청을 실행하고, 각각은 클라이언트에 응답을 전송한다. 클라이언트는 응답의 임계 수가 수신될 때까지 기다린다. 일부 예에서, 클라이언트는 수신될 $f+1$ 응답을 기다리는데, 여기서 f 는 블록체인 네트워크 내에서 용인될 수 있는 장애 합의 노드의 최대 수이다. 최종 결과는 충분한 수의 합의 노드가 블록체인에 추가될 기록의 순서에 대해 약정하는 것이고, 기록은 수락되거나 거절된다.

[0032] 일부 블록체인 네트워크에서, 암호화는 거래의 프라이버시를 유지하기 위해 구현된다. 예를 들어, 두 개의 노드가 거래 프라이빗을 유지하기를 원하는 경우, 블록체인 네트워크 내의 다른 노드가 거래의 세부 사항을 파악할 수 없으면, 노드는 거래 데이터를 암호화할 수 있다. 예시적인 암호화는, 제한 없이, 대칭 암호화(symmetric encryption) 및 비대칭 암호화(asymmetric encryption)를 포함한다. 대칭 암호화는 암호화(평문으로부터 암호문 생성) 및 복호화(암호문으로부터 평문 생성) 모두에 대해 단일 키를 사용하는 암호화 프로세스를 지칭한다. 대칭 암호화에서, 동일한 키는 다수의 노드에서 이용 가능하며, 따라서 각 노드는 거래 데이터를 암호화/복호화할 수 있다.

[0033] 비대칭 암호화는 각각 프라이빗 키 및 퍼블릭 키를 포함하는 키 쌍을 이용하며, 프라이빗 키는 각각의 노드에만 알려져 있고, 퍼블릭 키는 블록체인 네트워크 내의 임의의 또는 모든 다른 노드에 알려져 있다. 노드는 데이터를 암호화하도록 다른 노드의 퍼블릭 키를 이용할 수 있고, 암호화된 데이터는 다른 노드의 프라이빗 키를 이용하여 복호화될 수 있다. 예를 들어, 도 2를 다시 참조하면, 참여자 A는 데이터를 암호화하도록 참여자 B의 퍼블릭 키를 사용할 수 있고, 암호화된 데이터를 참여자 B에 전송할 수 있다. 참여자 B는 암호화된 데이터(암호문)를 복호화하고 원본 데이터(평문)를 추출하도록 그의 프라이빗 키를 사용할 수 있다. 노드의 퍼블릭 키로 암호화된 메시지는 오로지 노드의 프라이빗 키만을 사용하여 복호화될 수 있다.

[0034] 비대칭 암호화는 디지털 서명을 제공하는데 이용되며, 이는 거래에서 참여자가 거래에서 다른 참여자를 확인할 수 있게 할 뿐만 아니라, 거래의 유효성을 확인할 수 있게 한다. 예를 들어, 노드는 메시지를 디지털적으로 사인할 수 있고, 다른 노드는 메시지가 참여자 A의 디지털 서명에 기초하여 노드에 의해 전송된 것을 확인할 수 있다. 디지털 서명은 또한 메시지가 송신 시 조작되지 않는 것을 보장하는데 이용될 수 있다. 예를 들어, 다시 도 2를 참조하면, 참여자 A는 메시지를 참여자 B에 전송하는 것이다. 참여자 A는 메시지의 해시를 생성하고, 이어서 그의 프라이빗 키를 이용하여, 암호화된 해시로서 디지털 서명을 제공하도록 해시를 암호화한다. 참여자 A는 디지털 서명을 메시지에 첨부하고, 디지털 서명을 가지는 메시지를 참여자 B에 전송한다. 참여자 B는 참여자 A의 퍼블릭 키를 이용하여 디지털 서명을 복호화하고, 해시를 추출한다. 참여자 B는 메시지를 해싱하고 그 해시들을 비교한다. 해시들이 동일하다면, 참여자 B는 메시지가 참여자 A로부터 실제로 왔고, 조작되지 않았음을 확인할 수 있다.

[0035] 현실 세계, 물리적 통화를 전달하는 것 같이, 통화의 디지털 표현을 효과적으로 전달하는 것은 때때로 양수인이 제1 유형의 통화를 제2 유형의 통화로 교환하는 것을 요구한다. 예를 들어, 오로지 제1 유형의 통화(예를 들어, 미국 달러($))만을 가지는 컨소시엄 블록체인 네트워크의 제1 멤버(예를 들어, 참여자 A)는 통화를 제2 유형의 통화(예를 들어, 중국 RMB)로 컨소시엄 블록체인 네트워크의 제2 멤버(예를 들어, 참여자 C)에 전달하는 것을 원할 수 있다. 참여자 A가 값을 참여자 C에 전달하기 위해, 제1 유형의 통화의 금액이 참여자 C에 전달 전에 제2 유형의 통화의 동등한 값으로 교환된다.

[0036] 본 명세서의 구현들에 따르면, 본 명세서에서 더욱 상세하게 설명되는 바와 같이, 통화의 유형을 교환하는 것은 중개자로서 컨소시엄 블록체인 네트워크의 제3 멤버(예를 들어, 참여자 B)를 통해 달성될 수 있다. 예를 들어, 참여자 A는 제1 유형의 통화의 금액을 참여자 B에 전달할 수 있고, 참여자 B는 참여자 B에 의해 사용된 환율(ER; exchange rate)에 기초하여 동등한 값을 가지는 제2 유형의 통화의 금액을 참여자 C에 전달할 수 있다. 일부 예에서, 참여자 B는 통화 교환 서비스를 컨소시엄 블록체인 네트워크의 멤버들에 제공하는 금융기관이다.

[0037] 블록체인 네트워크 내의 통화 교환에 수반된 당사자들의 프라이버시를 보장하기 위해, 교환의 기본이 되는 거래 데이터는 블록체인 네트워크 내의 교환의 검증 및 공개 전에 암호화된다. 일부 예에서, 거래 데이터는 제1 통화의 전달된 금액(t_1) 및 제1 금액에 대한 교환으로 제공된 제2 통화의 금액(t_2)을 포함한다. 전형적으로, 검증을 위해 블록체인에 제출되는 거래 데이터는 BGN(Boneh-Goh-Nissim) 암호화와 같은 동형 암호화 방법을 이용하여 암호화된다. 동형 암호화 방법 하에서, 암호화된 데이터의 둘 이상의 아이템은 제한 없이 함께 추가될 수 있다. 다른 암호화 방법(예를 들어, Paillier 퍼블릭 키 암호화 (PKE))과는 달리, BGN 암호화는 두 암호문(예를 들어, 암호화 된 β와 암호화된 t_1의 곱셈)에 걸쳐 동형 곱셈을 가능하게 한다. 하지만, 동형 암호화를 이용하는 암호화된 데이터 아이템은 단일 곱으로 제한된다. 이는, 동형 암호화를 이용하는 암호화된 두 데이터 아이템의 곱셈 쌍이 암호화된 승수와 상이한 순서의 암호화된 곱을 생성하기 때문이다.

[0038] 아래의 식은 곱셈 동형의 일회적 특성을 보여주는데, 이는 통상적으로 타원 곡선 $\mathcal{G}$ 상에서 페어링(pairing)으로 불린다:

$$e: \mathcal{G} \times \mathcal{G} \rightarrow \mathcal{G}_1$$

[0039]

[0040] 여기서, 곱해지는 암호화된 데이터 아이템의 각각은 $\mathcal{G}_1$ 상에 있는 곱셈의 곱과 상이한 타원 곡선 $\mathcal{G}$ 상에 있다. 곱셈 동형에 의해 생성된 암호화된 데이터 아이템은 기본이 되는 타원 곡선의 이러한 변화로 인해 더 곱해지거나 나눠질 수 없다. 또한, 곱셈 동형에 의해 생성된 암호화된 데이터 아이템은 직접 동형 암호화(direct

homomorphic encryption)에 의해 생성된 데이터 아이템과 비교될 수 없다. 예를 들어, 동일한 타원곡선 $\mathcal{G}$ 상의 상기 식에서의 처음 두 개의 암호화된 데이터 아이템은 서로 비교될 수 있지만, 기본이 되는 타원곡선 $\mathcal{G}$ 및 $\mathcal{G}_1$ 에서의 차이로 인해, 곱셈 동형에 의해 생성된 타원곡선 $\mathcal{G}_1$ 상에서 세 번째로 암호화된 데이터 아이템과 비교될 수 없다.

[0041] BGN 암호화에 있어서, BGN 암호화를 사용할 각 참여자 i는 키 생성 프로세스를 통해 BGN 퍼블릭 키(PK; public key), 프라이빗 키(SK; private key) 쌍(예를 들어, PK_{BGN_i}, SK_{BGN_o})이 제공된다. 키 생성 프로세스를 통해 다음이 제공된다:

$$PK_{BGN_i} = \{N, \mathcal{G}, \mathcal{G}_1, e, P, Q\}_i$$

[0042]

$$SK_{BGN_i} = p$$

[0043]

[0044] 여기서:

[0045] $N = pq$

[0046] p, q 는 큰 소수

[0047] $\mathcal{G}$ 는 N 차 타원 곡선

[0048] $e: \mathcal{G} \times \mathcal{G} \rightarrow \mathcal{G}_1$ 은 페어링

[0049] $P \in \mathcal{G}$ 은 생성기

[0050] $Q = q\alpha P$ (차수가 P 인 $\mathcal{G}$ 의 서브그룹의 랜덤 생성기)

[0051] $\alpha < N$

[0052] 본 명세서의 맥락에서, 동형 암호화 방식 하에서, 퍼블릭 환율을 수반하는 교환 거래는 전달되는 금액 및/또는 교환되는 금액을 드러내거나 공개함이 없이 컨소시엄 블록체인 네트워크에 의해 검증되고 기록될 수 있다. 예를 들어, 참여자 A에 의해 교환 서비스 제공자인 참여자 B에 전달되는 제1 통화의 금액(t_1) 및 제1 금액에 대한 교환 시 참여자 B에 의해 제공되는 제2 통화의 금액(t_2)은 모두 동형 암호화를 이용하여 암호화될 수 있다. 이러한 방법 하에서, 암호화된 t_1 및 암호화된 t_2 모두는 타원 곡선 $\mathcal{G}$ 상에 있다. 암호화된 전송 금액 t_1은, t_1에 대한 교환 시 참여자 B에 의해 제공되어야 하는 제2 통화의 금액을 결정하도록 참여자 B의 퍼블릭 환율에 의해 곱해질 수 있다. 참여자 B의 환율은 이러한 예에서 퍼블릭이고, 비 암호화된 값이기 때문에, t_1과 퍼블릭 환율의 곱은 t_1과 동일한 타원 곡선 $\mathcal{G}$ 인 암호화된 데이터 아이템이다. 참여자 A와 참여자 B 사이의 교환 거래는 t_1 과 퍼블릭 환율의 암호화된 곱을 암호화된 데이터 아이템 t_2와 비교함으로써 블록체인 네트워크에 의해 검증될 수 있다. 퍼블릭 환율에 의해 곱해지는 t_1의 암호화된 곱이 암호화된 데이터 아이템 t_2와 동일하면, 이어서 거래는 검증되고, 블록체인 상에 기록된다.

[0053] 이러한 검증 방법은 퍼블릭 환율을 수반하는 교환 거래를 검증하기 위한 효과적인 수단을 제공하는 반면, 통화 교환 서비스를 제공하는 블록체인 네트워크 멤버는 종종 다른 이러한 공급자와 경쟁하고 있다. 결과적으로, 이

들은 블록체인 네트워크 내에서 그들의 환율을 공개하기를 원하지 않는다. 따라서, 환율뿐만 아니라 거래 데이터는 블록체인 네트워크 내에서 수행되고 블록체인 네트워크에 의해 검증되는 교환 거래들에 대해 암호화되는 것이 바람직하다.

[0054] 그러나, 앞서 설명된 검증을 이용하면, 동형 암호화에 대한 일회적 곱셈의 제한은 교환 거래의 검증에 대한 장벽을 만들며, 이 때 거래 데이터와 환율은 모두 동형 암호화를 이용하여 암호화된다. 예를 들어, 참여자 A에 의해 교환 서비스 제공자인 참여자 B에 전달되는 제1 통화의 금액(t_1), 제2 통화의 금액(t_2), 여기서 제2 통화의 금액(t_2)에 대한 제1 통화의 전달된 금액은 참여자 B에 의해 교환되었고, 참여자 B의 환율(β)은 각각 동형 암호화를 이용하여 암호화될 수 있다. 이러한 방법 하에서, 암호화된 t_1, 암호화된 t_2 및 암호화된 β는 모두 동일한 타원 곡선 $\mathcal{G}$ 상에 있다.

[0055] 앞서 논의된 바와 같이, 교환 거래에 수반된 환율이 퍼블릭일 때마다, 교환 거래는 t_1과 퍼블릭 환율의 곱을 암호화된 데이터 아이템 t_2와 비교함으로써 블록체인 네트워크에 의해 검증될 수 있다. 그러나, 환율이 암호화(β)될 때, t_1과 암호화된 환율(β)의 곱은 t_2의 기본이 되는 곡선 $\mathcal{G}$와 상이한 타원 곡선 $\mathcal{G}_1$상에 있다. 곱셈 동형으로부터 초래된 차수에서의 차이에 기초하여, 암호화된 환율(β)에 의해 곱해지는 t_1의 곱은 t_2와 비교될 수 없다. 그 결과, 현재의 검증 방법 하에서, 거래 데이터와 환율 모두의 암호화를 수반하는 교환 거래의 검증은 블록체인 네트워크 내에서 수행될 수 없다.

[0056] 상술한 맥락에 비추어, 그리고 본 명세서에서 더 상세히 설명되는 바와 같이, 본 명세서의 구현은 암호화된 거래 데이터 및 암호화된 환율을 이용하는 블록체인 네트워크 내의 교차 자산 트레이딩에 관한 것이다. 보다 구체적으로, 본 명세서의 교차 자산 트레이딩 플랫폼은 프라이빗(암호화된) 환율 검증으로 수행될 수 있는 거래를 가능하게 한다.

[0057] 도 3은 본 명세서의 구현에 따른 교차 자산 트레이딩 플랫폼(300)의 예를 도시한다. 도시된 예에서, 예시적인 교차 자산 트레이딩 플랫폼(300)은 각각의 디바이스(302, 304, 306)와 연관된 세 참여자들, 즉 참여자 A, 참여자 B 및 참여자 C를 포함한다. 예시적인 교차 자산 트레이딩 플랫폼(300)은 또한 서브 체인 채널(308), 네트워크(310) 및 컨소시엄 블록체인 네트워크(312)를 포함한다.

[0058] 일부 예에서, 네트워크(310)는 근거리 네트워크(LAN), 원거리 네트워크(WAN), 인터넷, 또는 이들의 조합을 포함하고, 웹 사이트, 사용자 디바이스(예를 들어, 컴퓨팅 디바이스), 및 백-엔드 시스템을 연결한다. 일부 예에서, 네트워크(110)는 유선 및/또는 무선 통신 링크를 통해 액세스될 수 있다.

[0059] 본 명세서에서 설명된 바와 같이, 블록체인 네트워크(312)는 블록체인(322)에서 정보를 불변적으로 기록하는 복수의 노드(314)를 포함하는 피어-투-피어 네트워크로서 제공된다. 단일 블록체인(322)이 개략적으로 도시되어 있지만, 블록체인(322)의 다수의 사본들이 제공되고, 블록체인 네트워크(312)에 걸쳐 유지된다. 예를 들어, 각 노드(314)는 블록체인(322)의 사본을 저장한다. 일부 구현에서, 블록체인(322)은 컨소시엄 블록체인 네트워크(312)에 참여하는 둘 이상의 엔티티들 사이에서 수행되는 거래와 연관된 정보를 저장한다. 일부 예에서, 디바이스(302, 304, 306)는 컨소시엄 블록체인 네트워크(312)에서의 각각의 노드(314)의 일부이다.

[0060] 일부 구현에서, 디바이스(302), 디바이스(304) 및 디바이스(306)는 각각의 계좌, 즉 계좌 A(316), 계좌 B(318) 및 계좌 C(320)를 포함한다. 일부 예에서, 계좌 A(316), 계좌 B(318) 및 계좌 C(320)는 금융 자산을 저장한다. 일부 예에서, 계좌 A(316), 계좌 B(318) 및 계좌 C(320)는 하나 이상의 유형의 통화의 금액을 저장한다.

[0061] 일부 구현에서, 서브 체인 채널(308)은 컨소시엄 블록체인 네트워크(312)의 두 멤버들 사이에서 블록체인 네트워크(312) 외부의 정보를 전달하기 위해 사용될 수 있다. 일부 예에서, 프라이빗 금융 정보는 서브 체인 채널(308)을 통해 컨소시엄 블록체인 네트워크(312)의 일 멤버로부터 블록체인 네트워크(312) 외부의 컨소시엄 블록체인 네트워크(312)의 다른 멤버로 전달될 수 있다. 예를 들어, 디바이스(304)는 서브 체인 채널(308)을 통해 환율을 송신함으로써 프라이빗 환율(β)을 블록체인 네트워크(312) 외부의 디바이스(302)에 전달할 수 있다.

[0062] 일부 예에서, 컨소시엄 블록체인 네트워크(312)의 둘 이상의 멤버들 간의 거래는 검증 및 기록을 위해 블록체인 네트워크(312)에 제출될 수 있다. 일부 예에서, 컨소시엄 블록체인 네트워크(312)의 둘 이상의 멤버들 간의 자산(예를 들어, 통화) 교환 거래는 교환의 검증을 위해 블록체인 네트워크(312)에 제출될 수 있다. 일부 예에서, 블록체인 네트워크(312)에 제출되는 거래 정보는 암호화된다. 일부 예에서, 블록체인 네트워크(312)에 제출되는

거래 정보는 동형 암호화를 이용하여 암호화된다. 일부 예에서, 거래 정보는 환율, 전달될 제1 금액 및 전달될 제2 금액을 포함한다. 일부 예에서, 전달될 제2 금액은 환율에 의해 곱해지는 제1 금액의 곱과 동일하다.

[0063] 도 4는 본 명세서의 구현에 따라 교차 자산 거래를 실행하기 위한 신호 다이어그램(400)의 예를 도시한다. 도 4의 신호 다이어그램(400)은 계좌 A(402)(예를 들어, 블록체인 네트워크 내의 노드), 계좌 B(404)(예를 들어, 블록체인 네트워크 내의 노드) 및 블록체인 네트워크의 합의 노드(406)를 포함한다. 일부 예에서, 계좌 A(402) 및 계좌 B(404)는 블록체인 네트워크에서 참여자들(예를 들어, 각각의 참여자 A 및 참여자 B)의 자산을 관리하기 위해 사용된다. 일부 예에서, 계좌 A(402) 및 계좌 B(404)는 각각의 참여자 A 및 참여자 B의 디지털 자산을 저장한다. 일부 예에서, 참여자 B는 금융기관이다.

[0064] 교차 자산 거래의 예는 도 4를 참조하여 본 명세서에서 더 상세하게 설명된다. 예시적인 거래에서, 제1 통화(예를 들어, USD)에서 금액(t_1)은 계좌 A로부터 제2 통화(예를 들어, RMB)에서 금액 (t_2)에서 블록체인 네트워크에서 다른 참여자(예를 들어, 참여자 C)의 계좌에 전달된다. 금액(t_1)은 중개자인 계좌 B(404)를 이용하여 전달되는데, 이는 제1 통화와 제2 통화 사이의 프라이빗 환율(β)을 제공한다. 계좌 A(402)는 계좌 A(402)가 이용가능한 제1 통화에서의 밸런스의 값인 밸런스 금액(s_A)를 포함한다. 계좌 B(404)는 계좌 B(404)가 이용가능한 제1 통화에서의 밸런스의 값인 제1 밸런스 금액(s_{B1})), 및 계좌 B(404)가 이용가능한 제2 통화에서의 밸런스의 값인 제2 밸런스 금액(s_{B2}))을 포함한다.

[0065] 예시적인 교차 자산 거래에서, 프라이빗 환율(β)은 계좌 B(404)로부터 계좌 A(402)에 송신된다(408). 프라이빗 환율을 운반하는 메시지는 네트워크를 통해 송신될 수 있다. 일부 예에서, 프라이빗 환율을 운반하는 메시지는 서브 체인 채널(예를 들어, 도 3의 서브 체인 채널(308))을 통해 송신된다.

X_1, Y_1, Z_1

[0066] 계좌 A(402)는 두 난수(r_1, r_2)를 생성한다(410). 계좌 A(402)는 교환 금액(t_2) 및 암호문 ( )와 X_2, Y_2, Z_2 ( )의 세트를 계산한다(412). 일부 구현에서, 교환 금액(t_2)은 아래 나타난 바와 같이 전달될 금액(t_1)과 프라이빗 환율(β)의 곱과 같다:

$$t_2 = \beta t_1$$

[0067]

[0068] 일부 구현에서, 암호문 (X_1, Y_1, Z_1)와 (X_2, Y_2, Z_2)의 세트는 커밋먼트 방법(commitment scheme) 및 암호화 방법에 기초하여 결정된다. 커밋먼트 방법의 예는, 제한 없이, 페더슨 커밋먼트 (PC; Pedersen Commitment)를 포함한다. 암호화 방법은 예는, 제한 없이, BGN 암호화를 포함한다. BGN 암호화를 위해, 각 참여자는 BGN 퍼블릭 키(PK), 프라이빗 키(SK) 쌍을 포함한다. 예를 들어, 계좌 A(402)는 그에 할당된 BGN PK-SK 쌍(예를 들어, PK_{BGN_A}, SK_{BGN_A})을 가지고, 계좌 B(404)는 그에 할당된 BGN PK-SK 쌍(예를 들어, PK_{BGN_B}, SK_{BGN_B})을 가지고, 계좌 C(도 4에 도시되지 않음)는 그에 할당된 BGN PK-SK 쌍(예를 들어, PK_{BGN_C}, SK_{BGN_C})을 가진다.

[0069] 일부 구현에서, 암호문 (X_1, Y_1, Z_1)와 (X_2, Y_2, Z_2)의 세트들은 다음과 같이 각각 결정된다:

[0070] $$(X_1, Y_1, Z_1) = (PC(t_1, r_1), BGN_A(t_1, r_1), BGN_B(t_1, r_1))$$

[0071] $$(X_2, Y_2, Z_2) = (PC(t_2, r_2), BGN_B(t_2, r_2), BGN_C(t_2, r_2))$$

[0072] 표기법 $PC(t,r)$은 블라인드 팩터(blind factor)로서 난수 r을 가지는 t의 페더슨 커밋먼트를 나타낸다. 표기법 BGN_A은 계좌 A(402)의 퍼블릭 키를 이용하는 BGN 암호화를 나타내고, 표기법 BGN_B은 계좌 B(404)의 퍼블릭 키를 이용하는 BGN 암호화를 나타내며, 표기법 BGN_C은 계좌 C의 퍼블릭 키를 이용하는 BGN 암호화를 나타낸다. 일부 예에서, 계좌 A(402)는 밸런스 암호문을 다음과 같이 제공한다.

$$\left(PC(s_A,\bar{r}_A),BGN_A(s_A,\bar{r}_A)\right)$$

[0073]

[0074] 여기서, $\bar{r}_A$는 계좌 A(402)에 의해 생성된 난수이다.

[0075] 암호문 (X_1,Z_1)와 (X_2,Y_2)의 서브 세트, 난수(r_1, r_2), 및 금액(t_1)은 계좌 A(402)로부터 계좌 B(404)에 전송된다(414). 일부 구현에서, 계좌 A(402)로부터 계좌 B(404)로의 메시지는 (예를 들어, 상술한 비대칭 암호화를 이용하여) 암호화된 메시지이다. 일부 예에서, 메시지는 서브 체인 채널(예를 들어, 도 3의 서브 체인 채널(308))을 통해 송신된다. 일부 예에서, (암호화된) 메시지는 데이터 세트 $[t_1,r_1,r_2,X_1,Z_1,X_2,Y_2]$를 포함한다.

[0076] 계좌 B는 데이터(예를 들어, $[t_1,r_1,r_2,X_1,Z_1,X_2,Y_2]$)가 드러나도록 메시지를 복호화한다. 암호문 데이터는 계좌 B(404)에 의해 검증된다(416). 일부 예에서, 계좌 B(404)는 계좌 A(402)에 의해 제공된 t_1, r_1, r_2에 기초하여 암호문 X_1,Z_1,X_2,Y_2이 정확한지 여부를 검사함으로써 암호문 데이터를 검증한다. 즉, 계좌 B는 X_1,Z_1,X_2,Y_2를 다시 계산하고, 이들이 계좌 A(402)로부터 수신된 것과 동일한지 여부를 결정한다. 암호문이 동일하지 않으면, 에러가 계좌 A로 전송될 수 있고, 거래가 종료된다.

[0077] 암호문이 검증되면, 계좌 B(404)는 범위 증명(RP_B)을 생성한다(418). 일부 구현에서, 범위 증명(RP_B)은 계좌 B(404)가 교환 거래를 수행하는데 충분한 자금을 가지는지 여부를 확인하는데 사용될 수 있는 영지식 증명(ZKP; zero-knowledge proof)이다. 예를 들어, 범위 증명(RP_B)은 다음을 증명하기 위해 생성될 수 있다:

$$s_{B_2}-t_2\geq 0$$

[0078]

[0079] 일부 예에서, 계좌 B(404)는 제1 밸런스 암호문 및 제2 밸런스 암호문을 각각 다음과 같이 제공한다:

$$\left(PC(s_{B_1},\bar{r}_{B_1}),BGN_B(s_{B_1},\bar{r}_{B_1})\right)$$

[0080]

$$\left(PC(s_{B_2},\bar{r}_{B_2}),BGN_B(s_{B_2},\bar{r}_{B_2})\right)$$

[0081]

[0082] 여기서 $\bar{r}_{B_1}$ 및 $\bar{r}_{B_2}$는 계좌 B(404)에 의해 제공되는 난수이다. 일부 예에서, 계좌 B(404)는 교환 암호문을 다음과 같이 제공한다.

$$(E',E'')=\left(PC(\beta,\gamma),BGN_B(\beta,\gamma)\right)$$

[0083]

[0084] 여기서, γ는 계좌 B(404)에 의해 생성된 난수이고, 다른 계좌들과 공유된다(예를 들어, 환율(β)을 가지는 계좌 A(402)에 제공).

[0085] 증거 세트(EX)가 생성되며(420), 이는 프라이빗 환율(β)을 검증하기 위해 사용될 수 있다. 일부 구현에서, 환율의 증거 세트(EX)는 다음과 같이 제공된다:

$$EX=(U,V,t'',\tilde{r}'',\hat{r}'')$$

[0086]

[0087] 일부 예에서, U 및 V는 다음과 같이 각각 계산된다.

$$U = e(P_B, P_B)^{t\prime} e(P_B, Q_B)^{\tilde{r}\prime} \qquad V = e(P_B, P_B)^{t\prime} e(P_B, Q_B)^{\hat{r}\prime}$$

[0088] 및

[0089] 여기서, P_B 및 Q_B는 PK_{BGN_A}에 제공되고 t', $\tilde{r}'$, 및 $\hat{r}'$은 계좌 B(404)에 의해 생성된 난수이다. 일부 예에서, $t'', \tilde{r}'', \hat{r}''$은 다음과 같이 각각 계산된다:

$$t'' = t' + yt_2$$

[0090]

$$\tilde{r}'' = \tilde{r}' + y\tilde{r}$$

[0091]

$$\hat{r}'' = \hat{r}' + y\hat{r}$$

[0092]

[0093] 여기서 $y = Hash(U, V)$ 및, $\tilde{r}$ 및 $\hat{r}$은 다음과 같이 각각 계산된다:

$$\tilde{r} = \beta t_1 + t_1\gamma + \gamma r_1 q_B \alpha_B$$

[0094]

$$\hat{r} = 2t_2 + r_2 q_B \alpha_B$$

[0095]

[0096] 일부 예에서, $Hash$는 블록체인 네트워크(예를 들어, SHA-256)에서 합의 노드를 포함하는, 참여자에게 공개적으로 알려진 임의의 적절한 해싱 함수로서 제공될 수 있다.

[0097] 일부 구현에서, 계좌 B(404)는 암호화된 메시지를 계좌 A(402)에 다시 리턴하고(422), 이는 다음의 예시적인 데이터 세트를 포함한다:

$$(X_1, Z_1, X_2, Y_2; RP_B, EX; Sig_B)$$

[0098]

[0099] 여기서, Sig_B는 계좌 B(404)의 디지털 서명이다. 일부 예에서, 메시지는 서브 체인 채널(예를 들어, 도 3의 서브 체인 채널(308))을 통해 송신된다.

[0100] 계좌 A(402)는 거래가 어떤 값에 대한 것이고, 계좌 A(402)가 거래를 수행하기에 충분한 자산을 가지는 ZKP로서 기능하는 범위 증명(RP_A)을 생성한다(424). 달리 말하면, 범위 증명(RP_A)은 다음을 증명하는 데 사용될 수 있다:

$$t_1 \geq 0 \qquad s_A - t_1 \geq 0$$

[0101] , 및

[0102] 계좌 A(404)는 금액(t_1)에 대한 계좌 A(402)로부터 계좌 B(404)로의 제1 서브 거래, 및 금액(t_2)에 대한 계좌 B(404)로부터 계좌 C로의 제2 서브 거래를 포함하는 서브 거래를 생성한다(426). 일부 예에서, 계좌 A는 난수(t', r')를 생성하고, 암호문의 세트를 다음과 같이 제공한다:

$$(X', Y', Z') = \left(PC(t', r'), BGN_A(t', r'), BGN_B(t', r')\right)$$

[0103]

[0104] 계좌 A는 데이터 세트(*PF*)를 다음과 같이 제공한다:

$$PF = (X', Y', Z'; t_1', r_1', t_2', r_2')$$

[0105]

[0106] 여기서:

[0107] $t_1' = t' + xt_1$, $r_1' = r' + xr_2$, $t_2' = t' + xt_2$, 및 $r_2' = r' + xr_2$

[0108] 여기서:

[0109] $$x = Hash(X', Y', Z')$$

[0110] 계좌 A(402)는 각각 제1 및 제2 서브 거래를 다음과 같이 제공한다:

[0111] $$A,B:X_1,Y_1,Z_1$$

[0112] $$B,C:X_2,Y_2,Z_2$$

[0113] 여기서, A는 계좌 A(402)의 식별자이고, B는 계좌 B(404)의 식별자이며, C는 계좌 C의 식별자이다(예를 들어, 식별자들은 블록체인 네트워크 내의 각각의 어드레스로서 제공됨). 제1 및 제2 서브 거래, 범위 증명 및 지원 증거 세트를 포함하는 거래가 제공된다. 예를 들어, 거래는 다음과 같이 제공된다:

[0114] $$A,B:X_1,Y_1,Z_1;B,C:X_2,Y_2,Z_2;RP_A,PF;RP_B,EX$$

[0115] 거래는 계좌 A(402)에 의해 디지털 서명되고(428), 계좌 A(402)(Sig_A)의 서명 및 계좌 B(404)(Sig_B)의 서명 모두를 포함한다. 계좌 A(402)는 서명된 거래를 합의 노드(406)에 제출한다(430). 서명된 거래는 다음과 같이 제공될 수 있다:

[0116] $$(A,B:X_1,Y_1,Z_1;B,C:X_2,Y_2,Z_2;RP_A,PF;RP_B,EX;Sig_A,Sig_B)$$

[0117] 합의 노드(406)는 계좌 A(402)의 서명 및 계좌 B(404)의 서명을 검증한다(432). 서명이 검증되지 않으면, 거래는 종료되며, 에러 메시지가 계좌 A(402)에 제공될 수 있다. 서명이 검증되면, 범위 증명(RP_A)) 및 범위 증명(RP_B)은 합의 노드(406)에 의해 검증된다(434). 범위 증명이 ZKP이기 때문에, 각각은 기본이 되는 평문 데이터를 드러냄이 없이 참으로 증명되거나 거짓을 리턴할 수 있다. 범위 증명이 검증되지 않으면, 거래는 종료되며, 에러 메시지가 계좌 A(402)에 제공될 수 있다. 범위 증명이 검증되면, 거래 금액이 0보다 크고, 계좌 A(402) 및 계좌 B(404) 모두가 거래를 수행하기 위한 각각의 통화에서 충분한 자산을 가지는 것으로 결정된다.

[0118] 일부 실시예에서, 합의 노드(406)는 데이터 세트(*PF*) 및 증거 세트(*EX*)에서의 증거를 이용함으로써 거래를 검증한다(436). 일부 예에서, 합의 노드(406)는 다음의 관계가 참인지 여부를 검증한다.

$$PC(t_1', r_1') = X' + xX_1$$

[0119]

$$BGN_A(t_1', r_1') = Y' + xY_1$$

[0120]

$$BGN_B(t_1', r_1') = Z' + xZ_1$$

[0121]

$$PC(t_2', r_2') = X' + xX_2$$

[0122]

$$BGN_B(t_2', r_2') = Y' + xY_2$$

[0123]

$$BGN_C(t_2', r_2') = Z' + xZ_2$$

[0124]

[0125] 여기서, $x = Hash(X', Y', Z')$ 이다. 상기 관계가 참이면, 암호문(BGN 암호문)이 적절한 퍼블릭 키로 암호화되고, 거래의 금액이 정확하다는 것이 확인된다.

[0126] 거래는 공개된(하지만 암호화된) 환율에서 수행됨을 또한 검증한다. 예를 들어, 합의 노드(406)는 데이터 세트(*EX*)의 증거를 이용함으로써 환율을 검증한다. 일부 예에서, 합의 노드(406)는 $y = Hash(U, V)$ 를 계산하고 다음의 관계들이 참인지 여부를 검증하기 위해 y를 사용한다:

$$e(P_B, P_B)^{t''} e(P_B, Q_B)^{\hat{r}''} = U * e(E_2, Z_1)^y$$

[0127]

$$e(P_B, P_B)^{t''} e(P_B, Q_B)^{\hat{r}''} = V * e(BGN_B(1,1), Y_2)^y$$

[0128]

[0129] 만약 관계가 참이 아니라면, 거래 및/또는 환율이 검증되지 않고, 거래는 종료되며, 에러 메시지가 계좌 A(402)에 제공될 수 있다. 관계가 참이 아니라면, 합의 노드(406)는 거래가 컨소시엄 블록체인 네트워크에 기록되는 것을 기록하고(438), 계좌 A(402), 계좌 B(404) 및 계좌 C의 계좌 밸런스들이 업데이트된다. 예를 들어, 계좌 A(402)의 밸런스(s_A)는 금액(t_1)만큼 감소하고, 계좌 B(404)의 밸런스(s_{B1})는 금액(t_1)만큼 증가하고, 계좌 B(404)의 밸런스(s_{B2})는 금액(t_2)만큼 감소하고, 계좌 C의 밸런스는 금액(t_2)만큼 증가한다.

[0130] 도 5는 본 명세서의 구현들에 따라 실행될 수 있는 프로세스(500)의 예를 도시한다. 일부 구현에서, 예시적인 프로세스(500)는 하나 이상의 컴퓨팅 디바이스를 이용하여 실행되는 하나 이상의 컴퓨터 실행가능 프로그램을 이용하여 수행될 수 있다. 일부 예에서, 예시적인 프로세스(500)는 블록체인 네트워크 내의 교차 자산 거래들을 수행하기 위해 컨소시엄 블록체인 네트워크의 노드들에 의해 수행될 수 있다.

[0131] 환율이 수신된다(502). 예를 들어, 환율은 블록체인 네트워크 내의 제1 참여자와 연관된 제1 노드(예를 들어, 블록체인 네트워크의 노드)에 의해, 블록체인 네트워크 내의 제2 참여자와 연관된 제2 노드(예를 들어, 블록체인 네트워크의 노드)로부터 수신된다. 일부 예에서, 환율은 서브 체인 채널을 통해 수신된다. 일부 예에서, 환율은 제2 참여자의 프라이빗 환율이다. 일부 구현에서, 제2 참여자는 금융기관이다. 일부 구현에서, 환율은 제2 참여자가 제2 유형의 통화에 대해 제1 유형의 통화를 교환하는 비율을 특정한다. 예를 들어, 환율은 제2 참여자가 RMB에 대해 USD를 교환할 것에 대한 비율을 특정할 수 있다.

[0132] 제1 난수 및 제2 난수가 제1 노드에 의해 생성된다(504). 제1 금액 및 제2 금액은 각각, 제1난수 및 제2난수를 이용하는 암호문의 제1 세트 및 암호문의 제2 세트 내에서 각각 암호화된다(506). 일부 예에서, 제1 금액은 교환을 위해 제1 참여자에 의해 참여자 멤버에 전달될 제1 자산 유형의 금액이다. 일부 예에서, 제2 금액은 제1 금액에 대해 교환될 제2 자산 유형의 금액이다. 일부 예에서, 제2 금액은 제2 참여자의 환율에 의해 곱해지는 제1 금액의 곱과 동일하다.

[0133] 일부 예에서, 암호문의 제1 세트는 제1 금액 및 제1 난수의 난수 커밋먼트와, 제1 금액 및 제1 난수의 두 개의 동형 암호화를 포함한다. 일부 예에서, 암호문의 제2 세트는 제2 금액 및 제2 난수의 난수 커밋먼트와, 제2 금액 및 제2 난수의 두 개의 동형 암호화를 포함한다. 일부 예에서, 암호문의 제1 세트는 각각, 제1 금액 및 제1 난수의 PC와, 제1 참여자의 BGN 퍼블릭 키 및 제2 참여자의 BGN 퍼블릭 키를 이용하는 제1 금액 및 제1 난수의 BGN 암호화를 포함한다. 일부 예에서, 암호문의 제2 세트는 각각, 제2 금액 및 제2 난수의 PC와, 제2 참여자의 BGN 퍼블릭 키 및 제3 참여자의 BGN 퍼블릭 키를 이용하는 제2 금액 및 제2 난수의 BGN 암호화를 포함한다.

[0134] 제1 금액, 제1 난수, 제2 난수, 암호문의 제1 세트의 적어도 일부(서브 세트) 및 암호문의 제2 세트의 적어도 일부(서브 세트)는 제1 노드로부터 제2 노드에 송신된다(508). 일부 구현에서, 제1 금액, 제1 난수, 제2 난수, 암호문의 제1 세트의 적어도 일부 및 암호문의 제2 세트의 적어도 일부는 서브 체인 채널을 통해 송신된다.

[0135] 제1 범위 증명, 환율의 증거 세트 및 제1 서명이 수신된다(510). 일부 구현에서, 제1 범위 증명, 환율의 증거 세트 및 제1 서명은 서브 체인 채널을 통해 제2 노드로부터 제1 노드에 의해 수신된다. 일부 예에서, 제1 디지

털 서명은 비대칭 암호화 방법에 기초한 제2 참여자의 디지털 서명이다. 일부 예에서, 제1 범위 증명은 제2 멤버와 연관된 계좌가 제2 금액에 대한 제1 금액을 교환하기 위해 제2 금액과 동일한 자산 유형의 충분한 자금을 가진다는 증거를 제공한다.

[0136] 데이터 세트, 제2범위 증명, 및 제2 디지털 서명이 생성된다(512). 일부 예에서, 데이터 세트는 교차 자산 거래의 진위성을 적어도 부분적으로 확인하기 위해 블록체인 네트워크 내에서 사용된다. 일부 예에서, 제2 디지털 서명은 비대칭 암호화 방법에 기초한 제1 참여자의 디지털 서명이다. 일부 예에서, 제2 범위 증명은, 제1 참여자와 연관된 계좌가 제1 금액을 제2 참여자에 전달하기 위해 제1 금액과 동일한 자산 유형의 충분한 자금을 가지고, 제1 금액이 마이너스가 아니라는 증거를 제공한다.

[0137] 거래는 검증을 위해 블록체인 네트워크에 제출된다(514). 일부 구현에서, 제1 노드에 의해 블록체인 네트워크에 제출된 거래는 암호문의 제1 세트, 암호문의 제2 세트, 제1 범위 증명, 데이터 세트, 제2 범위 증명, 환율의 증거 세트, 제1 디지털 서명, 및 제2 디지털 서명을 포함한다. 일부 구현에서, 블록체인 네트워크 내의 적어도 하나의 합의 노드는 서명들 및 범위 증명을 검증한다. 일부 구현에서, 적어도 하나의 합의 노드는 거래 데이터(예를 들어, 제1 금액, 제2 금액, 환율)가 드러남이 없이 거래를 검증한다. 일부 구현에서, 거래의 성공적인 검증에 응답하여, 거래는 블록체인 네트워크 내에서 실행된다. 일부 예에서, 제1 참여자 및 제2 참여자의 계좌들은 교환된 자산들을 반영하도록 블록체인 상에서 업데이트된다. 일부 예에서, 제3 참여자의 계좌는 제2 금액의 수신을 반영하도록 업데이트된다.

[0138] 도 6은 본 명세서의 구현에 따른 장치(600)의 모듈의 일 예에 대한 도면이다. 장치(600)는 블록체인 네트워크에서 프라이빗 교차 자산 트레이딩에 참여하도록 구성된 블록체인 노드의 예시적인 구현일 수 있고, 블록체인 네트워크는 컨소시엄 블록체인 네트워크이다. 장치(600)는 앞서 설명된 구현에 대응할 수 있고, 장치(600)는 다음을 포함한다:

[0139] 생성 유닛(602)은 BGN 암호화를 이용하여, 제1 값 및 제2 값에 기초한 암호문을 생성하고, 제2 값은 제1 값 및 블록체인 네트워크 내의 제2 노드에 의해 제공되는 환율에 기초하여 결정된다. 송신 유닛(604)은 제1 값 및 암호문을 제2 노드에 송신한다. 수신 유닛(606)은 환율을 드러냄이 없이 ZKP 루틴에서 환율을 검증하기 위해 사용될 수 있는 데이터의 세트를 포함하는 제1 증거 세트를 수신한다. 생성 유닛(602)은 ZKP 루틴을 이용하여, 암호문이 BGN 퍼블릭 키에 의해 암호화되는 것을 검증하기 위해 사용될 수 있는 데이터의 세트를 포함하는 제2 증거 세트를 생성한다.

[0140] 거래 정의 유닛(608)은 제1 노드로부터 제2 노드에 제1 값의 전달을 위한 제1 노드와 제2 노드 사이의 제1 거래, 및 제2 노드로부터 제3 노드에 제2 값의 전달을 위한 제2 노드와 제3 노드 사이의 제2 거래를 포함하는 거래를 정의한다. 송신 유닛(604)은 거래의 검증 및 실행을 위해 거래를 블록체인 네트워크의 적어도 하나의 합의 노드에 송신한다. 본 명세서에서 설명된 바와 같이, 거래는 제1 증거 세트 및 제2 증거 세트에 기초하여 검증될 수 있다. 거래의 검증에 응답하여, 합의 노드는 제1 노드의 밸런스를 제1 값만큼 감소시키고, 제2 노드의 제1 밸런스를 제1 값만큼 증가시키고, 제2 노드의 제2 밸런스를 제2 값만큼 감소시키고, 제3 노드의 밸런스를 제2 값만큼 증가시키도록 제1 거래 및 제2 거래를 실행한다.

[0141] 선택적인 구현에서, 제1 증거 세트는 제1 값, 제1 노드에 의해 제공되는 한 쌍의 난수 및 암호문에 기초하여 제2 노드에 의해 제공된다.

[0142] 선택적 구현에서, 합의 노드에 의해 거래를 검증하는 것은 제1 노드의 디지털 서명 및 제2 노드의 디지털 서명을 검증하는 것을 포함한다.

[0143] 선택적인 구현에서, 합의 노드에 의해 거래를 검증하는 것은 제1 노드에 의해 제공되는 제1 범위 증명 및 제2 노드에 의해 제공되는 제2 범위 증명을 검증하는 것을 포함한다.

[0144] 선택적인 구현에서, 제1 범위 증명은 제1 값이 0보다 크고, 제1 노드의 밸런스가 제1 값보다 크거나 같음을 증명하기 위해 ZKP를 포함한다.

[0145] 선택적인 구현에서, 제2 범위 증명은 제2 노드의 제2 밸런스가 제2 값보다 크거나 같음을 증명하기 위해 ZKP를 포함한다.

[0146] 선택적인 구현에서, 거래는 BGN 암호화에 적어도 부분적으로 기초하여 생성된 암호문의 세트를 포함하는 데이터 세트를 더 포함하고, 데이터 세트는 적어도 하나의 합의 노드에 의해 거래를 검증하는데 사용된다.

[0147] 선택적 구현에 있어서, 수신 유닛(606)는 블록체인 네트워크의 서브체인 채널을 통해 제2 노드로부터 환율을 수

신한다.

[0148] 선택적인 구현에서, 암호문의 적어도 하나의 암호문은 PC를 이용하여 제공된다.

[0149] 선택적 구현에서, 제1 증거 세트의 데이터의 세트는 제1 데이터 값 및 제2 데이터 값을 포함하고, 제1 데이터 값 및 제2 데이터 값의 각각은 제2 노드의 BGN 퍼블릭 키를 생성하기 위해 사용되는 파라미터에 기초하여 결정된다.

[0150] 선택적인 구현에서, 제2 증거 세트의 데이터의 세트는 암호문의 세트 및 값의 세트를 포함하며, 값의 세트에서의 각 값은 암호문의 세트의 해시에 적어도 부분적으로 기초한다.

[0151] 이전의 구현들에서 설명된 시스템, 장치, 모듈 또는 유닛은 컴퓨터 칩 또는 엔티티를 이용함으로써 구현될 수 있고, 또는 특정 기능을 가지는 제품을 이용함으로써 구현될 수 있다. 전형적인 구현 디바이스는 컴퓨터이고, 컴퓨터는 개인용 컴퓨터, 랩톱 컴퓨터, 셀룰러 폰, 카메라 폰, 스마트폰, 개인 휴대 정보 단말기(PDA), 미디어 플레이어, 네비게이션 디바이스, 이메일 수신 및 전송 디바이스, 게임 콘솔, 태블릿 컴퓨터, 웨어러블 디바이스, 또는 이들 디바이스의 임의의 조합일 수 있다.

[0152] 장치에서 각 유닛의 기능 및 역할의 구현 프로세스를 위해, 참조들이 이전 방법에서 대응하는 단계들의 구현 프로세스에 이루어질 수 있다. 세부 내용은 간소화를 위해 생략된다.

[0153] 장치 구현은 기본적으로 방법 구현에 대응하기 때문에, 관련된 부분에 대해, 참조들이 방법 구현에서의 관련된 설명에 이루어질 수 있다. 앞서 설명된 장치 구현은 하나의 예에 불과하다. 별개의 부분으로서 설명된 유닛은 물리적으로 분리되어 있거나 분리되어 있지 않을 수도 있으며, 유닛으로서 표시되는 부분은 물리적인 유닛이거나 물리적인 유닛이 아닐 수도 있고, 하나의 위치에 위치할 수 있거나, 다수의 네트워크 유닛 상에 분산되어 있을 수 있다. 일부 또는 모든 모듈은 본 명세서의 솔루션의 목표를 달성하기 위해 실제적인 요구에 기초하여 선택될 수 있다. 본 기술 분야에서 통상의 지식을 가진 자는 창의적인 노력 없이 이 애플리케이션의 구현을 이해하고 구현할 수 있다.

[0154] 다시 도 6을 참조하면, 프라이빗 교차 자산 트레이딩 장치의 내부 기능 모듈 및 구조를 나타내는 것으로 해석될 수 있다. 프라이빗 교차 자산 트레이딩 장치는 블록체인 네트워크 내에서 프라이빗 교차 자산 트레이딩에 참여하도록 구성된 블록체인 노드의 일례일 수 있다. 본질적으로 실행 바디는 전자 디바이스일 수 있으며, 전자 디바이스는 다음: 하나 이상의 프로세서; 및 하나 이상의 프로세서의 실행 가능한 명령어를 저장하도록 구성된 메모리를 포함한다.

[0155] 본 명세서에 설명된 동작 및 대상과 작용의 구현은 디지털 전자 회로로, 유형의 구체화된 컴퓨터 소프트웨어 또는 펌웨어로, 본 명세서에 개시된 구조 및 그 구조적 등가물을 포함하는 컴퓨터 하드웨어로, 또는 이들 중 하나 이상의 조합으로 구현될 수 있다. 본 명세서에 설명된 대상의 구현은 하나 이상의 컴퓨터 프로그램, 예를 들어, 컴퓨터 프로그램 캐리어 상에 인코딩된, 컴퓨터 프로그램 명령어의 하나 이상의 모듈로서, 데이터 프로세싱 장치에 의한 실행을 위해 또는 데이터 프로세싱 장치의 동작을 제어하기 위해 구현될 수 있다. 예를 들어, 컴퓨터 프로그램 캐리어는 인코딩되거나 저장된 명령어를 가지는 하나 이상의 컴퓨터 판독 가능 저장 매체를 포함할 수 있다. 캐리어는 자기, 광 자기 또는 광 디스크, 솔리드 스테이트 드라이브, 랜덤 액세스 메모리(RAM), 판독 전용 메모리(ROM), 또는 다른 유형의 매체와 같은 유형의(tangible) 비 일시적 컴퓨터 판독 가능 매체일 수 있다. 대안적으로, 또는 추가적으로, 캐리어는 인공적으로 생성된 전파 신호, 예를 들어 데이터 프로세싱 장치에 의해 실행을 위해 적합한 수신기 장치로 전송하기 위한 정보를 인코딩하기 위해 생성되는 기계 생성된 전기적, 광학적 또는 전자기적 신호일 수 있다. 컴퓨터 저장 매체는 기계 판독 가능 저장 디바이스, 기계 판독 가능 저장 기판, 랜덤 또는 직렬 액세스 메모리 디바이스, 또는 이들 중 하나 이상의 조합일 수 있거나 그 일부일 수 있다. 컴퓨터 저장 매체는 전파된 신호가 아니다.

[0156] 프로그램, 소프트웨어, 소프트웨어 애플리케이션, 앱, 모듈, 소프트웨어 모듈, 엔진, 스크립트 또는 코드로서 또한 지칭되거나 설명될 수 있는 컴퓨터 프로그램은 컴파일링 또는 해석된 언어, 또는 선언적이거나 절차적 언어를 포함하는 임의의 형태의 프로그래밍 언어로 쓰여질 수 있고; 자립형 프로그램 또는 컴퓨팅 환경에서 실행하기에 적합한 모듈, 컴포넌트, 엔진, 서브루틴 또는 기타 유닛을 포함하는 임의의 형태로 배치될 수 있으며, 이 환경은 하나 이상의 위치에서 데이터 통신 네트워크에 의해 상호 연결된 하나 이상의 컴퓨터를 포함할 수 있다.

[0157] 컴퓨터 프로그램은 파일 시스템의 파일에 대응할 수 있지만, 반드시 그럴 필요는 없다. 컴퓨터 프로그램은 다른 프로그램 또는 데이터, 예를 들어 마크업 언어 문서에 저장된 하나 이상의 스크립트를 보유하는 파일의 일부에,

해당 프로그램에 전용인 단일 파일에, 또는 다수의 조정된 파일에, 예를 들어, 하나 이상의 모듈, 서브 프로그램 또는 코드 부분을 저장하는 파일에 저장될 수 있다.

[0158] 컴퓨터 프로그램의 실행을 위한 프로세서는, 예로서, 범용 마이크로 프로세서 및 특수 목적의 마이크로 프로세서, 및 임의의 종류의 디지털 컴퓨터의 임의의 하나 이상의 프로세서를 포함한다. 일반적으로, 프로세서는 프로세서에 결합된 비 일시적 컴퓨터 판독 가능 매체로부터의 데이터뿐만 아니라 실행을 위한 컴퓨터 프로그램의 명령을 수신할 것이다.

[0159] 용어 "데이터 프로세싱 장치"는 예로서 프로그래밍 가능한 프로세서, 컴퓨터, 또는 다수의 프로세서 또는 컴퓨터를 포함하는 데이터를 프로세싱하기 위한 모든 종류의 장치, 디바이스 및 기계를 포함한다. 데이터 프로세싱 장치는 특수 목적의 논리 회로, 예를 들어 FPGA(field programmable gate array), ASIC(application specific integrated circuit) 또는 GPU(graphics processing unit)를 포함할 수 있다. 장치는 또한 하드웨어 외에 컴퓨터 프로그램을 위한 실행 환경을 생성하는 코드, 예를 들어 프로세서 펌웨어를 구성하는 코드, 프로토콜 스택, 데이터베이스 관리 시스템, 운영 체제, 또는 이들 중 하나 이상의 조합을 포함할 수 있다.

[0160] 본 명세서에 설명된 프로세스 및 논리 흐름은 입력 데이터를 조작하고 출력을 생성함으로써 동작을 수행하도록 하나 이상의 컴퓨터 프로그램을 실행하는 하나 이상의 컴퓨터 또는 프로세서에 의해 수행될 수 있다. 프로세스 및 논리 흐름은 또한 예를 들어, FPGA, ASIC 또는 GPU와 같은 특수 목적 논리 회로 또는 특수 목적 논리 회로와 하나 이상의 프로그래밍된 컴퓨터의 조합에 의해 수행될 수 있다.

[0161] 컴퓨터 프로그램의 실행에 적합한 컴퓨터는 범용 또는 특수 목적의 마이크로프로세서 또는 둘 다 또는 임의의 다른 종류의 중앙 처리 유닛(CPU; central processing unit)에 기초할 수 있다. 일반적으로, 중앙 처리 유닛은 판독 전용 메모리 또는 랜덤 액세스 메모리 또는 둘 다로부터 명령어 및 데이터를 수신할 것이다. 컴퓨터의 요소는 명령어를 실행하기 위한 중앙 처리 유닛과 명령어 및 데이터를 저장하기 위한 하나 이상의 메모리 디바이스를 포함할 수 있다. 중앙 처리 유닛 및 메모리는 특수 목적 논리 회로에 의해 보충되거나 특수 목적 논리 회로에 통합될 수 있다.

[0162] 일반적으로, 컴퓨터는 또한 하나 이상의 저장 디바이스로부터 데이터를 수신하거나 하나 이상의 저장 디바이스에 데이터를 전달하도록 동작적으로 결합될 것이다. 저장 디바이스는 예를 들어, 자기, 자기 광학 또는 광학 디스크, 솔리드 스테이트 드라이브, 또는 임의의 다른 유형의 비 일시적 컴퓨터 판독 가능 매체일 수 있다. 그러나 컴퓨터에는 이러한 디바이스들이 필요하지 않다. 따라서, 컴퓨터는 로컬 및/또는 원격인 하나 이상의 메모리와 같은 하나 이상의 저장 디바이스에 결합될 수 있다. 예를 들어, 컴퓨터는 컴퓨터의 필수 구성 요소인 하나 이상의 로컬 메모리를 포함할 수 있거나, 컴퓨터는 클라우드 네트워크에 있는 하나 이상의 원격 메모리에 결합될 수 있다. 게다가, 컴퓨터는 다른 장치, 예를 들어 몇 가지만 말하자면, 이동 전화, PDA(personal digital assistant), 모바일 오디오 또는 비디오 플레이어, 게임 콘솔, GPS(global positioning system) 수신기 또는 휴대용 저장 디바이스, 예를 들면 USB(universal serial bus) 플래쉬 드라이브에 내장될 수 있다.

[0163] 구성 요소들은 직접적으로 또는 하나 이상의 중간 구성 요소들을 통해 서로 전기적으로 또는 광학적으로 연결된 것과 같이 상호적으로써 서로에게 "결합되어" 있을 수 있다. 구성 요소는 또한 구성 요소 중 하나가 다른 하나에 통합되면 서로 "결합될" 수도 있다. 예를 들어, 프로세서 내로 통합되는 저장 컴포넌트(예를 들어, L2 캐시 컴포넌트)는 프로세서에 "결합된다".

[0164] 사용자와의 상호 작용을 제공하기 위해, 본 명세서에 설명된 대상의 구현은 사용자에게 정보를 디스플레이하기 위한 디스플레이 장치, 예를 들어 LCD(liquid crystal display) 모니터 및 사용자가 컴퓨터에 입력을 제공할 수 있는 입력 장치, 예를 들어 키보드 및 포인팅 장치, 예를 들어 마우스, 트랙볼 또는 터치 패드를 가지는 컴퓨터 상에서 구현되거나 이와 통신하도록 구성될 수 있다. 다른 종류의 디바이스가 또한 사용자와의 상호 작용을 제공하기 위해 사용될 수도 있다; 예를 들어, 사용자에게 제공되는 피드백은 임의의 형태의 감각 피드백, 예를 들어 시각 피드백, 청각 피드백 또는 촉각 피드백일 수 있으며; 사용자로부터의 입력은 음향, 음성 또는 촉각 입력을 포함하는 임의의 형태로 수신될 수 있다. 또한, 컴퓨터는 사용자에 의해 사용되는 디바이스로부터 문서를 전송하고 문서를 수신함으로써; 예를 들어, 웹 브라우저로부터 수신된 요청에 대한 응답으로 웹 페이지를 사용자의 디바이스 상의 웹 브라우저로 전송함으로써, 또는 사용자 디바이스, 예를 들어, 스마트폰 또는 전자 태블릿 상에서 실행되는 앱과 상호 작용함으로써, 사용자와 상호작용할 수 있다. 또한, 컴퓨터는 문자 메시지 또는 다른 형태의 메시지를 개인용 디바이스, 예를 들어 메시지 애플리케이션을 실행하는 스마트폰에 전송하고, 리턴으로 응답 메시지를 사용자로부터 수신함으로써 사용자와 상호 작용할 수 있다.

[0165] 본 명세서는 시스템, 장치 및 컴퓨터 프로그램 컴포넌트와 관련하여 "구성된다"라는 용어를 사용한다. 특정 동작 또는 작용을 수행하도록 하나 이상의 컴퓨터의 시스템을 구성하기 위해서는, 동작 시 시스템으로 하여금 동작 또는 작용을 수행하도록 시스템이 소프트웨어, 펌웨어, 하드웨어 또는 이들의 조합을 설치하였음을 의미한다. 특정 동작 또는 작용을 수행하도록 구성되는 하나 이상의 컴퓨터 프로그램을 구성하기 위해서는, 하나 이상의 프로그램이 데이터 프로세싱 장치에 의해 실행될 때, 장치로 하여금 동작 또는 작용을 수행하게 하는 명령어를 포함한다는 것을 의미한다. 특수 목적 논리 회로가 특정 동작 또는 작용을 수행하도록 구성된다는 것은 회로가 동작 또는 작용을 수행하는 전자 논리를 가지는 것을 의미한다.

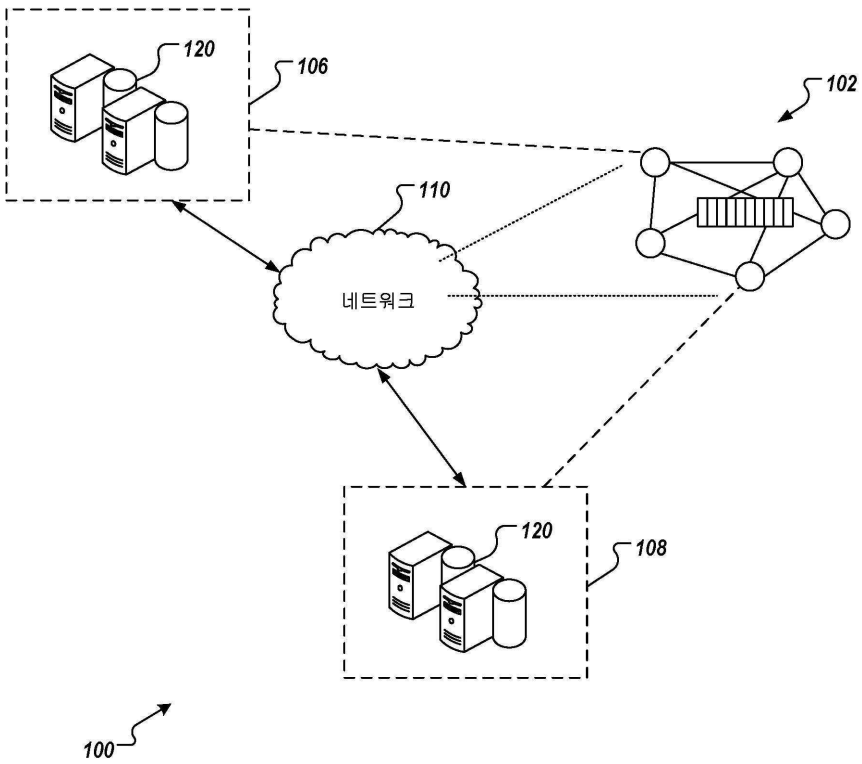
[0166] 본 명세서는 많은 특정 구현 세부 사항을 포함하지만, 이들은 청구범위 자체에 의해 정의되는 청구 대상의 범위에 대한 제한으로 해석되어서는 안되고, 특정 구현에 특정될 수 있는 특징의 설명으로 해석되어야 한다. 별도의 구현의 맥락에서 본 명세서에 설명된 특정 특징은 또한 단일 구현으로 조합하여 실현될 수도 있다. 반대로, 단일 구현의 맥락에서 설명되는 다양한 특징들은 또한 다수의 구현에서 개별적으로 또는 임의의 적절한 하위 조합으로 실현될 수 있다. 또한, 특징들이 특정 조합으로 작업하는 것으로 위에서 설명되고 심지어 초기에 그렇게 청구될 수 있지만, 청구된 조합으로부터의 하나 이상의 특징은 경우에 따라 조합으로부터 제외될 수 있고, 청구범위는 하위 조합 또는 하위 조합의 변형에 관한 것일 수 있다.

[0167] 유사하게, 동작들이 도면들에 도시되고 청구범위에 특정 순서로 기재되었지만, 이는 그러한 동작들이 바람직한 결과를 달성하기 위해, 도시된 특정한 순서 또는 순차적인 순서로 수행되도록 요구하거나, 또는 모든 예시된 동작이 수행되도록 요구되는 것으로 이해해서는 안된다. 특정 상황에서, 멀티태스킹 및 병렬 프로세싱이 유리할 수 있다. 또한, 상술한 구현에서 다양한 시스템 모듈들 및 컴포넌트들의 분리는 모든 구현에서 그러한 분리를 요구하는 것으로 이해되어서는 안되며, 설명된 프로그램 컴포넌트들 및 시스템들은 일반적으로 단일 소프트웨어 제품으로 통합되거나 또는 다수의 소프트웨어 제품으로 패키징된다는 것을 이해해야 한다.

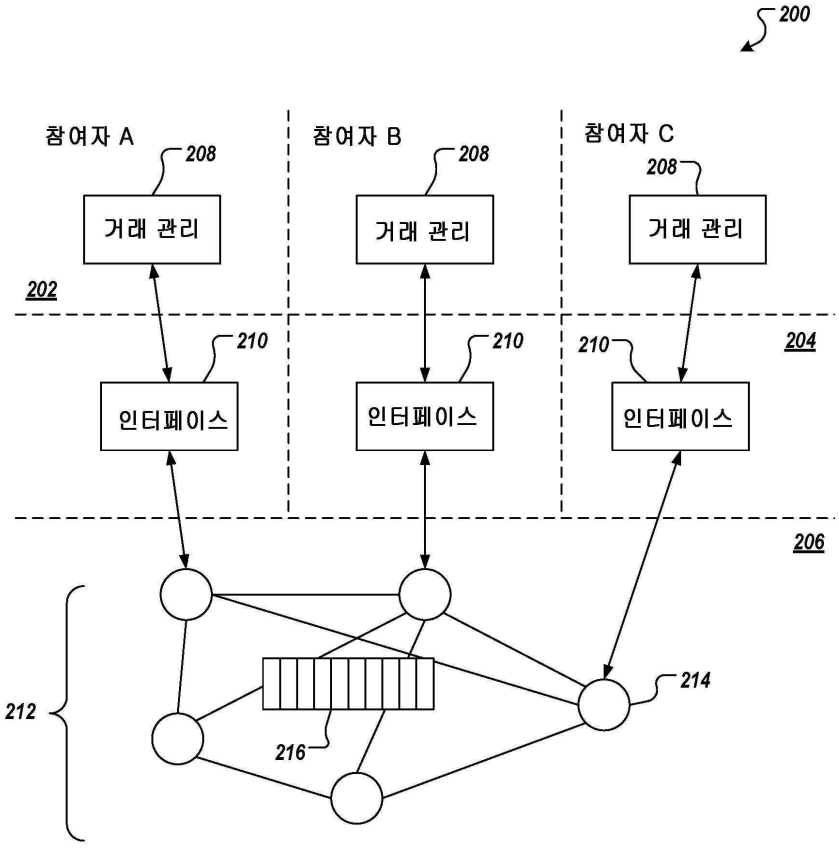
[0168] 대상의 특정 구현이 설명되었다. 다른 구현들은 다음의 청구범위의 범위 내에 있다. 예를 들어, 청구범위에 기재된 작용은 상이한 순서로 수행될 수 있으며 여전히 바람직한 결과를 달성할 수 있다. 일 예로서, 첨부 도면에 도시된 프로세스는 바람직한 결과를 달성하기 위해 도시된 특정 순서 또는 순차적 순서를 반드시 요구할 필요는 없다. 일부 경우에, 멀티태스킹 및 병렬 프로세싱이 유리할 수 있다.

도면

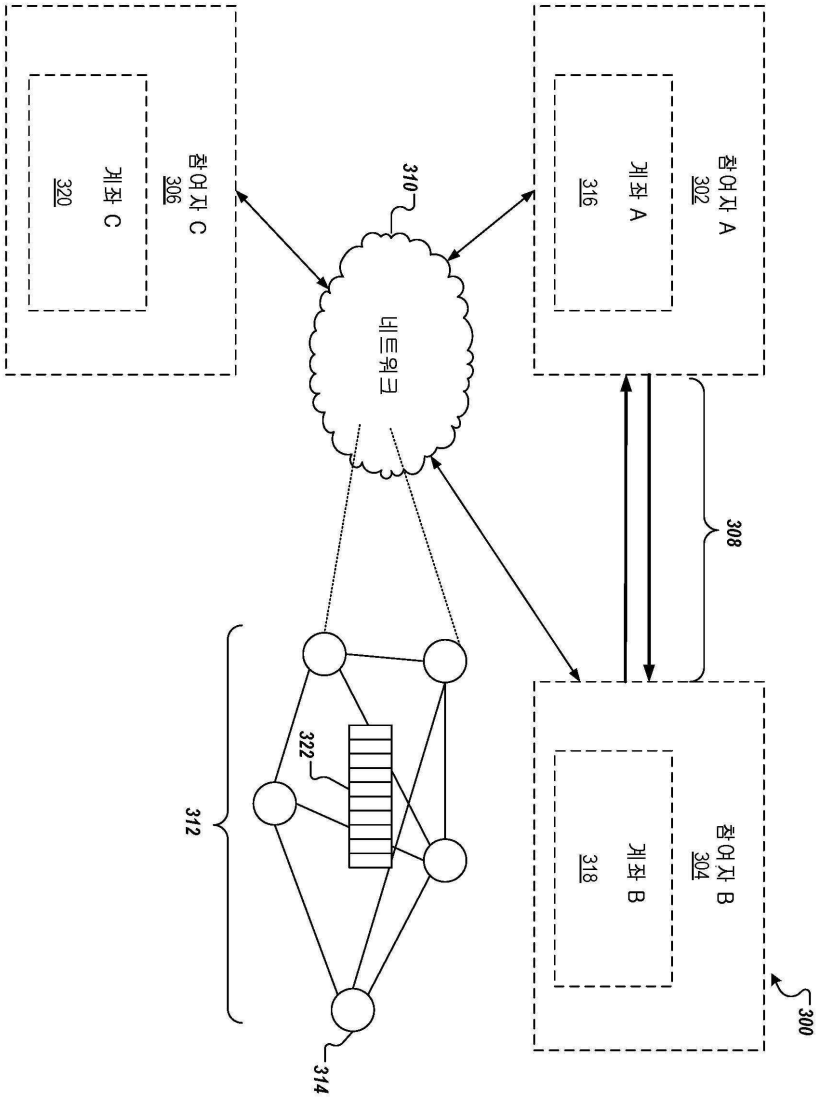
도면1



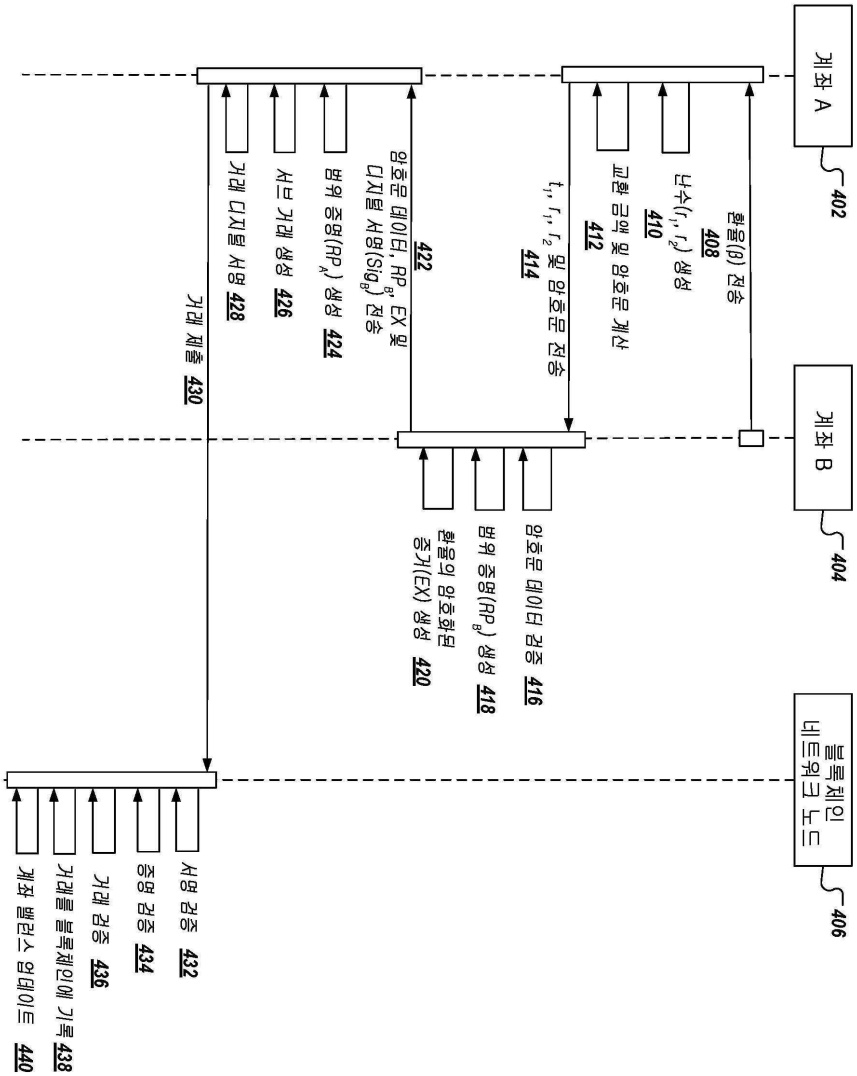
도면2


200
참여자 A
참여자 B
참여자 C
208
208
208
거래 관리
거래 관리
거래 관리
202
204
206
210
210
210
인터페이스
인터페이스
인터페이스
212
214
216

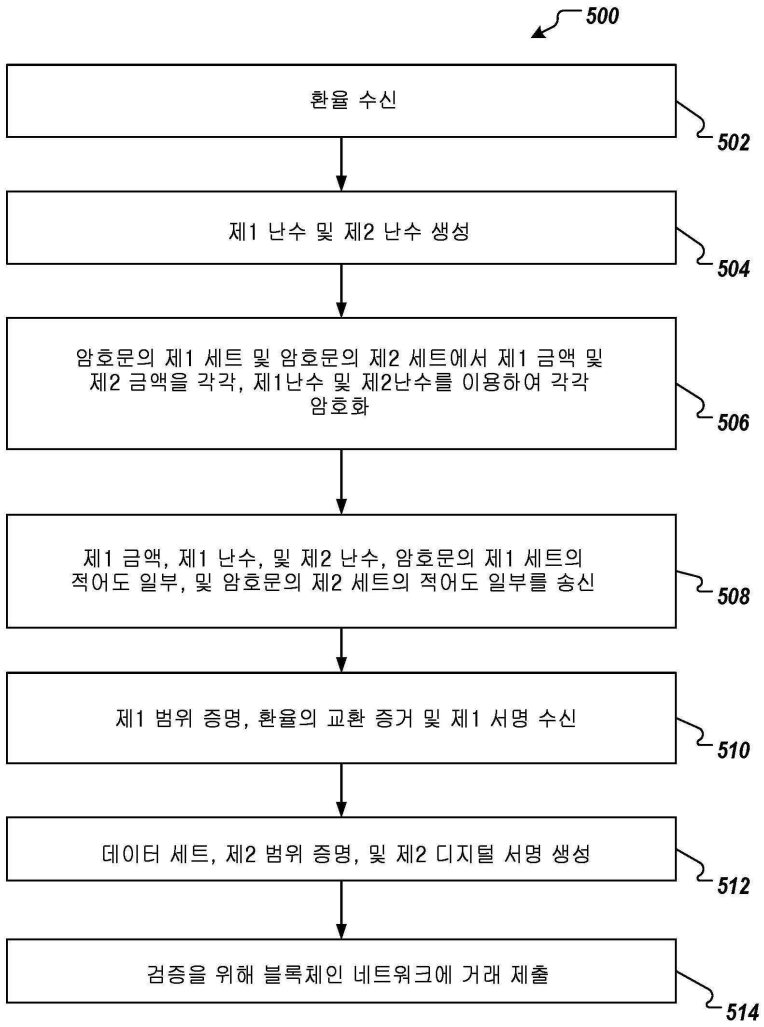
도면3


참여자 A
302
계좌 A
316
참여자 C
306
계좌 C
320
310
네트워크
308
참여자 B
304
계좌 B
318
300
312
322
314

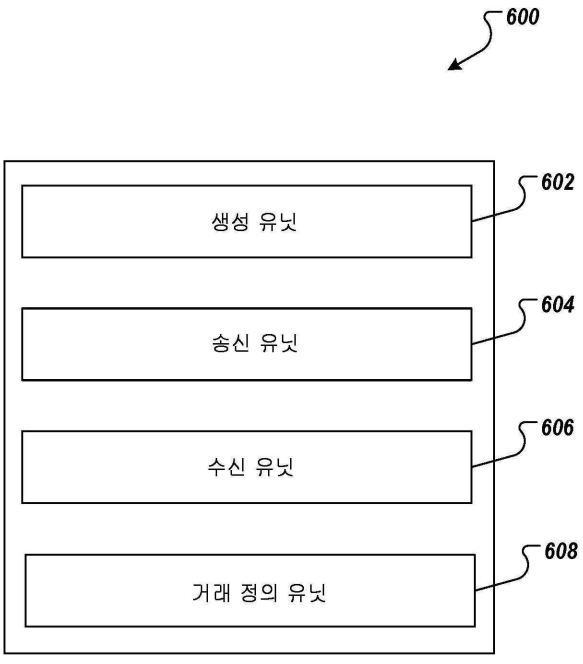
도면4


계좌 A
402
환율(β) 전송
408
난수(r_1, r_2) 생성
410
교환 금액 및 암호문 계산
412
t_1, r_1, r_2 및 암호문 전송
414
계좌 B
404
암호문 데이터 검증 416
범위 증명(RP_B) 생성 418
환율의 암호화된 증거(EX) 생성 420
암호문 데이터, RP_B, EX 및 디지털 서명(Sig_B) 전송
422
범위 증명(RP_A) 생성 424
서브 거래 생성 426
거래 디지털 서명 428
거래 제출 430
블록체인 네트워크 노드
406
서명 검증 432
증명 검증 434
거래 검증 436
거래를 블록체인에 기록 438
계좌 밸런스 업데이트 440

도면5


500
환율 수신
502
제1 난수 및 제2 난수 생성
504
암호문의 제1 세트 및 암호문의 제2 세트에서 제1 금액 및 제2 금액을 각각, 제1난수 및 제2난수를 이용하여 각각 암호화
506
제1 금액, 제1 난수, 및 제2 난수, 암호문의 제1 세트의 적어도 일부, 및 암호문의 제2 세트의 적어도 일부를 송신
508
제1 범위 증명, 환율의 교환 증거 및 제1 서명 수신
510
데이터 세트, 제2 범위 증명, 및 제2 디지털 서명 생성
512
검증을 위해 블록체인 네트워크에 거래 제출
514

도면6


600
생성 유닛
602
송신 유닛
604
수신 유닛
606
거래 정의 유닛
608

【심사관 직권보정사항】

【직권보정 1】

【보정항목】 청구범위

【보정세부항목】 청구항 12

【변경전】

블록체인 네트워크에서 프라이빗 교차 자산 트레이딩(private cross-asset trading)을 위한 명령어로 인코딩된 하나 이상의 컴퓨터 판독가능 저장 매체에 있어서,

상기 명령어는, 하나 이상의 프로세서에 의해 실행 가능하고 상기 하나 이상의 프로세서로 하여금, 제1항 내지 제11항 중 어느 한 항에 따른 방법을 수행하게 하는 것인, 하나 이상의 컴퓨터 판독가능 저장 매체.

【변경후】

블록체인 네트워크에서 프라이빗 교차 자산 트레이딩(private cross-asset trading)을 위한 명령어를 저장한 컴퓨터 판독가능 저장 매체에 있어서,

상기 명령어는, 하나 이상의 프로세서에 의해 실행 가능하고 상기 하나 이상의 프로세서로 하여금, 제1항 내지 제11항 중 어느 한 항에 따른 방법을 수행하게 하는 것인, 컴퓨터 판독가능 저장 매체.