(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2019년11월01일
(11) 등록번호 10-2039570
(24) 등록일자 2019년10월28일

(51) 국제특허분류(Int. Cl.)
G06Q 20/38 (2012.01)
(52) CPC특허분류
G06Q 20/3827 (2013.01)
G06Q 20/3825 (2013.01)
(21) 출원번호 10-2018-0025724
(22) 출원일자 2018년03월05일
심사청구일자 2018년03월05일
(65) 공개번호 10-2019-0105320
(43) 공개일자 2019년09월17일
(56) 선행기술조사문헌
KR1020170136724 A
KR1020130070500 A*
JP2015072689 A
KR1020160114749 A
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
주식회사 더블터
인천광역시 남구 인하로 100, 인하대학교 하이테크 1008호(용현동)
(72) 발명자
양대헌
서울특별시 서초구 서초중앙로 200, 17동 901호(서초동,삼풍아파트)
(74) 대리인
양성보

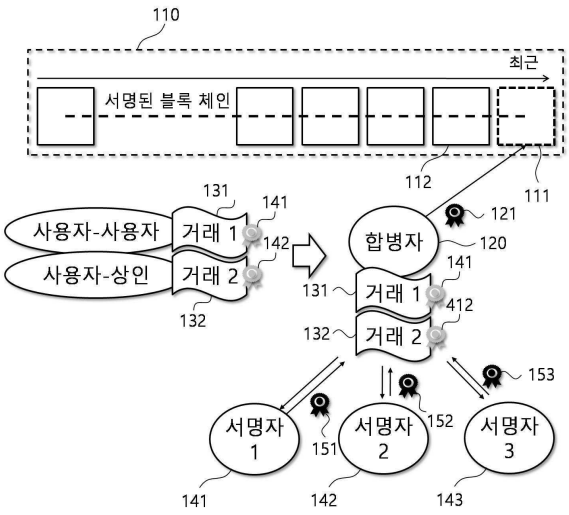
전체 청구항 수 : 총 10 항 심사관 : 권태헌

(54) 발명의 명칭 **암호화폐를 사용하지 않는 법정화폐용 P2P 장부**

(57) 요 약

암호화폐를 발행하지 않고도 법정화폐에 대한 보편적인 금융 플랫폼을 구현할 수 있는 p2p(peer-to-peer) 장부에 대한 기술을 개시한다. 본 발명의 실시예들에 따른 네트워크 시스템은 네트워크에 입장하고자 하는 복수의 사용자들 각각에 대해 실명으로 신원을 인증받아 상기 네트워크상에서의 사용자 식별자를 제공하는 금융 플랫폼; 상기 사용자들간의 거래에 대한 정보를 수집 및 병합하여 거래 블록을 생성하고, 상기 생성된 거래 블록을 위한 서명자들을 선택하여, 상기 선택된 서명자들의 상기 생성된 거래 블록에 대한 서명을 받아 상기 생성된 거래 블록을 서명된 블록 체인에 추가시키고자 시도하는 복수의 합병자 노드들; 및 상기 복수의 합병자 노드들 각각으로부터의 요청에 따라 상기 복수의 합병자 노드들 각각에서 생성된 거래 블록의 유효성을 확인하고, 상기 유효성이 확인된 거래 블록에 서명하는 복수의 서명자 노드들을 포함할 수 있다.

대 표 도 - 도1



(52) CPC특허분류
G06Q 20/389 (2013.01)

명 세 서

청구범위

청구항 1

블록체인 네트워크에 입장하고자 하는 복수의 사용자들 각각에 대해 실명으로 신원을 인증받아 상기 블록체인 네트워크상에서의 사용자 식별자를 제공하는 금융 플랫폼;

상기 실명으로 신원이 인증된 사용자들간의 법정화폐를 이용한 거래에 대한 정보를 수집 및 병합하여 거래 블록을 생성하고, 상기 생성된 거래 블록이 포함하는 거래에 대한 이해관계와 무관하게, 서명된 블록 체인의 완성된 마지막 블록의 거래에 기반하여 상기 생성된 거래 블록을 위한 서명자들을 선택하고, 상기 선택된 서명자들의 상기 생성된 거래 블록에 대한 서명을 받아 상기 생성된 거래 블록을 상기 서명된 블록 체인에 추가시키고자 시도하는 복수의 합병자 노드들; 및

상기 복수의 합병자 노드들 각각으로부터의 요청에 따라 상기 복수의 합병자 노드들 각각에서 생성된 거래 블록의 유효성을 확인하고, 상기 유효성이 확인된 거래 블록에 서명하는 복수의 서명자 노드들

을 포함하는 것을 특징으로 하는 네트워크 시스템.

청구항 2

제1항에 있어서,

상기 복수의 합병자 노드들은,

상기 복수의 서명자 노드들로부터 서명된 거래 블록들이 대응하는 합병자 노드들에 의해 각각 브로드캐스트됨에 따라, 상기 서명된 거래 블록들의 유효성을 확인하고, 상기 유효성이 확인된 상기 서명된 거래 블록들의 상기 서명된 블록 체인으로의 추가를 승인하는 것을 특징으로 하는 네트워크 시스템.

청구항 3

제1항에 있어서,

상기 복수의 합병자 노드들 각각에서 생성된 거래 블록이 추가된 블록 체인들 중 상기 복수의 서명자 노드들로부터 가장 많은 서명을 받은 거래 블록이 추가된 블록 체인이 선택되는 것을 특징으로 하는 네트워크 시스템.

청구항 4

제1항에 있어서,

상기 복수의 합병자 노드들 각각은,

상기 서명된 블록 체인에 추가시키고자 하는 거래 블록의 이전 거래 블록에 포함된 거래에 대한 정보들을 입력으로 가지면서 임의적(random)이어서 예측 불가능하지만 결정적(deterministic)이어서 입력에 따라 출력이 결정되는 함수를 통해 출력되는 해시 값을 생성하고, 상기 생성된 해시 값에 기반하여 상기 추가시키고자 하는 거래 블록을 위한 서명자들을 선택하며, 상기 선택된 서명자들에 대응하는 서명자 노드들로 상기 추가시키고자 하는 거래 블록에 대한 서명을 요청하는 것을 특징으로 하는 네트워크 시스템.

청구항 5

제1항에 있어서,

상기 복수의 서명자 노드들 각각은,

자신이 서명한 거래 블록의 블록 식별자를 관리하고, 상기 서명된 블록 체인에서 마지막으로 서명된 거래 블록이 완성되기 전에 생성된 거래 블록에 대한 서명 요청을 거절하는 것을 특징으로 하는 네트워크 시스템.

청구항 6

제1항에 있어서,

상기 복수의 서명자 노드들 각각은,

자신이 이미 서명한 거래 블록 상의 거래들에 대한 정보를 포함하는 다른 거래 블록에 대한 서명 요청을 무시하며, 상기 서명 요청의 무시에 대한 정보를 상기 다른 거래 블록에 대응하는 합병자 노드에게 통지하는 것을 특징으로 하는 네트워크 시스템.

청구항 7

제1항에 있어서,

상기 복수의 서명자 노드들 각각은,

서명된 것과 일치하지 않는 거래를 포함하는 블록에 대한 서명 요청을 상기 금융 플랫폼에 보고하고, 상기 서명 요청에 따른 합병자의 식별자 및 상기 일치하지 않는 거래의 송신자의 식별자를 상기 블록체인 네트워크상에 브로드캐스팅하는 것을 특징으로 하는 네트워크 시스템.

청구항 8

컴퓨터와 결합되어 서명 방법을 컴퓨터에 실행시키기 위해 컴퓨터 판독 가능한 기록매체에 저장된 컴퓨터 프로그램에 있어서,

상기 서명 방법은,

입장하고자 하는 복수의 사용자들에 대해 실명으로 신원이 인증된 블록체인 네트워크상의 합병자 노드로부터 상기 블록체인 네트워크를 통해 상기 합병자 노드가 상기 실명으로 신원이 인증된 사용자들간의 법정화폐를 이용한 거래에 대한 정보를 수집 및 병합하여 생성한 거래 블록에 대한 서명 요청을 수신하는 단계;

상기 서명 요청된 거래 블록의 유효성을 확인하는 단계; 및

상기 유효성이 확인된 거래 블록에 서명하는 단계

를 포함하고,

상기 서명 요청은, 해시 값에 기초하여 선택되는 상기 블록체인 네트워크상의 서명자 노드들에게 상기 합병자 노드에 의해 전송되고,

상기 해시 값은 서명된 블록 체인의 마지막 거래 블록이 포함하는 거래들에 대한 정보들을 입력으로 가지면서 임의적(random)이어서 예측 불가능하지만 결정적(deterministic)이어서 입력에 따라 출력이 결정되는 함수를 통해 출력되는 것을 특징으로 하는 컴퓨터 프로그램.

청구항 9

컴퓨터와 결합되어 거래 블록 추가 방법을 컴퓨터에 실행시키기 위해 컴퓨터 판독 가능한 기록매체에 저장된 컴퓨터 프로그램에 있어서,

상기 거래 블록 추가 방법은,

입장하고자 하는 복수의 사용자들에 대해 실명으로 신원이 인증된 블록체인 네트워크를 통해 상기 실명으로 신원이 인증된 사용자들간의 법정화폐를 이용한 거래에 대한 정보를 수집하는 단계;

상기 수집된 거래에 대한 정보를 병합하여 거래 블록을 생성하는 단계;

상기 생성된 거래 블록이 포함하는 거래에 대한 이해관계와 무관하게, 서명된 블록 체인의 완성된 마지막 블록의 거래에 기반하여 상기 생성된 거래 블록을 위한 서명자들을 선택하는 단계;

상기 선택된 서명자들의 상기 생성된 거래 블록에 대한 서명을 요청하는 단계; 및

상기 서명자들로부터 서명된 거래 블록을 상기 서명된 블록 체인에 추가시키기 위해, 상기 서명된 거래 블록을 상기 블록체인 네트워크상의 복수의 합병자 노드들로 전송하는 단계

를 포함하는 것을 특징으로 하는 컴퓨터 프로그램.

청구항 10

제8항 또는 제9항의 컴퓨터 프로그램이 기록되어 있는 것을 특징으로 하는 컴퓨터에서 판독 가능한 기록매체.

발명의 설명

기 술 분 야

[0001] 아래의 설명은 어떠한 암호화폐를 발행하지 않고도 법정화폐에 대한 보편적인 금융 플랫폼을 구현할 수 있는 p2p(peer-to-peer) 장부에 관한 것으로, 보다 자세하게는, 실명 네트워크 내에서의 법정화폐를 이용한 거래를 기록하기 위한 p2p 장부와, 상기 p2p 장부 기반의 네트워크 시스템, 서명자의 서명 방법 및 합병자의 거래 블록 추가 방법에 관한 것이다.

배 경 기 술

[0002] 사토시 나가모토(Satoshi Nakamoto)의 기발한 생각으로 인해, p2p 공개 장부는 익명의 네트워크 내에서 구현 가능한 것으로 보인다. 임의의 인터넷 유저는 네트워크에 참여하고 그들의 컴퓨팅 능력 또는 작업 증명(proof-of-work)를 제공함으로써 p2p 네트워크에 기여할 수 있다. 작업 증명은 익명의 참가자들에 의한 영리한 1 CPU 당 1표 구현이고, 이는 비트코인 장부가 불법적인 변형이 되지 않도록 한다. 그들의 작업에 대해 노드들을 보상하기 위하여, 비트코인이라 불리는 암호화폐가 발행되고 각 노드들에게 주어진다. 예를 들어, 한국공개특허 제10-2016-0024185호는 SE(Secure Element)를 이용하여 암호화폐를 관리하는 시스템 및 그 방법에 대해 개시하고 있다.

[0003] 그러나, 장부 및 암호화폐의 그 익명성은 그 기술이 법정화폐 경제에서 사용되는 것을 막는다. 암호화폐들은 자금 세탁 또는 조세 회피를 위해 사용될 지라도 추적 불가능하며, 암호화폐들의 가치는 안정적이지 않으며 격렬히 요동친다.

발명의 내용

해결하려는 과제

[0004] 실명 네트워크 내에서의 법정화폐를 이용한 거래를 기록하기 위한 p2p 장부와, 상기 p2p 장부 기반의 네트워크 시스템, 서명자의 서명 방법 및 합병자의 거래 블록 추가 방법을 제공한다.

과제의 해결 수단

[0005] 네트워크에 입장하고자 하는 복수의 사용자들 각각에 대해 실명으로 신원을 인증받아 상기 네트워크상에서의 사용자 식별자를 제공하는 금융 플랫폼; 상기 사용자들간의 거래에 대한 정보를 수집 및 병합하여 거래 블록을 생성하고, 상기 생성된 거래 블록을 위한 서명자들을, 상기 생성된 거래 블록이 포함하는 거래에 대한 이해관계와 무관하게, 서명된 블록 체인의 완성된 마지막 블록의 거래에 기반하여 선택하고, 상기 선택된 서명자들의 상기 생성된 거래 블록에 대한 서명을 받아 상기 생성된 거래 블록을 상기 서명된 블록 체인에 추가시키고자 시도하는 복수의 합병자 노드들; 및 상기 복수의 합병자 노드들 각각으로부터의 요청에 따라 상기 복수의 합병자 노드들 각각에서 생성된 거래 블록의 유효성을 확인하고, 상기 유효성이 확인된 거래 블록에 서명하는 복수의 서명자 노드들을 포함하는 것을 특징으로 하는 네트워크 시스템을 제공한다.

[0006] 일측에 따르면, 상기 복수의 합병자 노드들은, 상기 복수의 서명자 노드들로부터 서명된 거래 블록들이 대응하는 합병자 노드들에 의해 각각 브로드캐스팅됨에 따라, 상기 서명된 거래 블록들의 유효성을 확인하고, 상기 유효성이 확인된 상기 서명된 거래 블록들의 상기 서명된 블록 체인으로의 추가를 승인하는 것을 특징으로 할 수 있다.

[0007] 다른 측면에 따르면, 상기 복수의 합병자 노드들 각각에서 생성된 거래 블록이 추가된 블록 체인들 중 상기 복수의 서명자 노드들로부터 가장 많은 서명을 받은 거래 블록이 추가된 블록 체인이 선택되는 것을 특징으로 할 수 있다.

[0008] 또 다른 측면에 따르면, 상기 복수의 합병자 노드들 각각은, 상기 서명된 블록 체인에 추가시키고자 하는 거래 블록의 이전 거래 블록에 포함된 거래에 대한 정보들을 입력으로 가지면서 임의적(random)이어서 예측 불가능하지만 결정적(deterministic)이어서 입력에 따라 출력이 결정되는 함수를 통해 출력되는 해시 값을 생성하고, 상

기 생성된 해시 값에 기반하여 상기 추가시키고자 하는 거래 블록을 위한 서명자들을 선택하며, 상기 선택된 서명자들에 대응하는 서명자 노드들로 상기 추가시키고자 하는 거래 블록에 대한 서명을 요청하는 것을 특징으로 할 수 있다.

[0009] 또 다른 측면에 따르면, 상기 복수의 서명자 노드들 각각은, 자신이 서명한 거래 블록의 블록 식별자를 관리하고, 상기 서명된 블록 체인에서 마지막으로 서명된 거래 블록이 완성되기 전에 생성된 거래 블록에 대한 서명 요청을 거절하는 것을 특징으로 할 수 있다.

[0010] 또 다른 측면에 따르면, 상기 복수의 서명자 노드들 각각은, 자신이 이미 서명한 거래 블록 상의 거래들에 대한 정보를 포함하는 다른 거래 블록에 대한 서명 요청을 무시하며, 상기 서명 요청의 무시에 대한 정보를 상기 다른 거래 블록에 대응하는 합병자 노드에게 통지하는 것을 특징으로 할 수 있다.

[0011] 또 다른 측면에 따르면, 상기 복수의 서명자 노드들 각각은, 서명된 것과 일치하지 않는 거래를 포함하는 블록에 대한 서명 요청을 상기 금융 플랫폼에 보고하고, 상기 서명 요청에 따른 합병자의 식별자 및 상기 일치하지 않는 거래의 송신자의 식별자를 상기 네트워크상에 브로드캐스팅하는 것을 특징으로 할 수 있다.

[0012] 입장하고자 하는 복수의 사용자들에 대해 실명으로 신원이 인증된 네트워크상의 합병자 노드로부터 상기 네트워크를 통해 상기 합병자 노드가 생성한 거래 블록에 대한 서명 요청을 수신하는 단계; 상기 서명 요청된 거래 블록의 유효성을 확인하는 단계; 및 상기 유효성이 확인된 거래 블록에 서명하는 단계를 포함하고, 상기 서명 요청은 해시 값에 기초하여 선택되는 상기 네트워크상의 서명자 노드들에게 상기 합병자 노드에 의해 전송되고, 상기 해시 값은 서명된 블록 체인의 마지막 거래 블록이 포함하는 거래들에 대한 정보들을 입력으로 가지면서 임의적(random)이어서 예측 불가능하지만 결정적(deterministic)이어서 입력에 따라 출력이 결정되는 함수를 통해 출력되는 것을 특징으로 하는 서명 방법을 제공한다.

[0013] 입장하고자 하는 복수의 사용자들에 대해 실명으로 신원이 인증된 네트워크를 통해 상기 사용자들간의 거래에 대한 정보를 수집하는 단계; 상기 수집된 거래에 대한 정보를 병합하여 거래 블록을 생성하는 단계; 상기 생성된 거래 블록을 위한 서명자들을 상기 생성된 거래 블록이 포함하는 거래에 대한 이해관계와 무관하게, 서명된 블록 체인의 완성된 마지막 블록의 거래에 기반하여 선택하는 단계; 상기 선택된 서명자들의 상기 생성된 거래 블록에 대한 서명을 요청하는 단계; 및 상기 서명자들로부터 서명된 거래 블록을 서명된 블록 체인에 추가시키기 위해, 상기 서명된 거래 블록을 상기 네트워크상의 복수의 합병자 노드들로 전송하는 단계를 포함하는 것을 특징으로 하는 거래 블록 추가 방법을 제공한다.

[0014] 컴퓨터 장치와 결합되어 상기 방법을 컴퓨터 장치에 실행시키기 위해 컴퓨터 판독 가능한 기록매체에 저장된 컴퓨터 프로그램을 제공한다.

[0015] 상기 방법을 컴퓨터 장치에 실행시키기 위한 프로그램이 기록되어 있는 컴퓨터 판독 가능한 기록매체를 제공한다.

[0016] 컴퓨터 장치에서 판독 가능한 명령을 실행하도록 구현되는 적어도 하나의 프로세서를 포함하고, 상기 적어도 하나의 프로세서에 의해, 입장하고자 하는 복수의 사용자들에 대해 실명으로 신원이 인증된 네트워크상의 합병자 노드로부터 상기 네트워크를 통해 상기 합병자 노드가 생성한 거래 블록에 대한 서명 요청을 수신하고, 상기 서명 요청된 거래 블록의 유효성을 확인하고, 상기 유효성이 확인된 거래 블록에 서명하며, 상기 서명 요청은 해시 값에 기초하여 선택되는 상기 네트워크상의 서명자 노드들에게 상기 합병자 노드에 의해 전송되고, 상기 해시 값은 서명된 블록 체인의 마지막 거래 블록이 포함하는 거래들에 대한 정보들을 입력으로 가지면서 임의적(random)이어서 예측 불가능하지만 결정적(deterministic)이어서 입력에 따라 출력이 결정되는 함수를 통해 출력되는 것을 특징으로 하는 컴퓨터 장치를 제공한다.

[0017] 컴퓨터 장치에서 판독 가능한 명령을 실행하도록 구현되는 적어도 하나의 프로세서를 포함하고, 상기 적어도 하나의 프로세서에 의해, 입장하고자 하는 복수의 사용자들에 대해 실명으로 신원이 인증된 네트워크를 통해 상기 사용자들간의 거래에 대한 정보를 수집하고, 상기 수집된 거래에 대한 정보를 병합하여 거래 블록을 생성하고, 상기 생성된 거래 블록을 위한 서명자들을 상기 생성된 거래 블록이 포함하는 거래에 대한 이해관계와 무관하게, 서명된 블록 체인의 완성된 마지막 블록의 거래에 기반하여 선택하고, 상기 선택된 서명자들의 상기 생성된 거래 블록에 대한 서명을 요청하고, 상기 서명자들로부터 서명된 거래 블록을 서명된 블록 체인에 추가시키기 위해, 상기 서명된 거래 블록을 상기 네트워크상의 복수의 합병자 노드들로 전송하는 것을 특징으로 하는 컴퓨터 장치를 제공한다.

발명의 효과

[0018] 실명 네트워크 내에서의 법정화폐를 이용한 거래를 기록하기 위한 p2p 장부와, 상기 p2p 장부 기반의 네트워크 시스템, 서명자의 서명 방법 및 합병자의 거래 블록 추가 방법을 제공할 수 있다.

도면의 간단한 설명

[0019] 도 1은 본 발명의 일실시예에 따른 P2P 장부 프로토콜의 예를 도시한 도면이다.

도 2는 본 발명의 일실시예에 있어서, 서명된 블록 체인에 추가된 새로운 블록이 포함하는 정보의 예를 도시한 도면이다.

도 3은 본 발명의 일실시예에 있어서, 종전 블록에 기반하여 새로운 블록을 위한 서명자들이 선택하는 예를 도시한 도면이다.

도 4는 본 발명의 일실시예에 따른 p2p 장부가 블록 위조(forking a block)에 대한 보호되는 예를 도시한 도면이다.

도 5는 본 발명의 일실시예에 있어서, 네트워크 시스템의 동작 환경의 예를 도시한 도면이다.

도 6은 본 발명의 일실시예에 있어서, 컴퓨터 장치의 내부 구성의 예를 도시한 도면이다.

도 7은 본 발명의 일실시예에 있어서, 서명 방법의 예를 도시한 흐름도이다.

도 8은 본 발명의 일실시예에 있어서, 거래 블록 추가 방법의 예를 도시한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0020] 이하, 실시예를 첨부한 도면을 참조하여 상세히 설명한다.

[0021] 본 발명의 실시예들에서는 어떠한 암호화폐를 발행하지 않고도 법정화폐에 대한 보편적인 금융 플랫폼을 구현하는 p2p 장부에 대한 기술들을 설명한다. 이에 대해, 본 발명의 실시예들에서는 실명 신원에 기반하는 "인구 증명(Proof of Population)"이라는 새로운 개념을 도입한다. 그것은 은행들을 위한 p2p 장부로서 사용될 수 있고, 결제를 위한 영향력 있는 도구로서 사용될 수 있고, 임의의 금융 거래(transaction)들을 위해 사용될 수 있다. 나아가, 그것은 제3자에 의해 장악되었던 비용을 중앙 집중화될 수 없는 피어들에게 분산시킨다. 에너지 요구가 매우 낮기 때문에 본 발명의 실시예들에 따른 소프트웨어를 스마트폰이나 개인용 컴퓨터 상에 실행하는 것이 가능하다.

[0023] 1. 소개

[0024] 제3 신뢰 기관은 신뢰받은 방법으로 기록 거래를 하기 위하여 필요한 것으로 가정된다. 이 모델에서, 참가자들이 기록들이 변형되지 않는다는 것을 믿기 위해서는 신뢰가 필요가 필요하다. 신뢰를 제공하는 대신에, 제3 신뢰 기관은 참가자들로부터 거래 비용을 받는다. 이는 네트워크 내의 참가자들이 일반적으로 은행과 같은 제3 신뢰 기관을 운용하는 비용에 동의한다면 잘 이루어진다. 그러나, 기술적, 경제적, 정치적으로 거래를 보호하는 제3 신뢰 기관을 설치하는 것이 불가능하다면, 분산되지만 위조가 불가능한 온라인 거래 기록이 필요하다. 또한, 이미 제3 신뢰 기관이 존재하더라도, 제3 신뢰 기관을 유지하는 비용이 너무 커서 기술적 또는 경제적으로 불가피한 것이 아니라 부당한 이익을 창출할 때, 구현 가능하다면, 분산된 장부를 사용하는 것이 더 바람직하다. 분산된 장부를 제공하는 것과 제3 기관을 제거하는 것은 제3 기관에 의존하지 않는 또 다른 경쟁 기술을 제공함으로써 신뢰 기관에 의해 운영되는 시장에 큰 영향을 미친다.

[0025] 2009년, 비트코인은 중앙 집중화된 화폐 주조국을 제거하고 온라인 화폐 시스템에 대한 장부를 탈중앙화한다는 개념을 제공했다. 비트코인 네트워크에서 코인들은 피어들이 하나의 세계적인 불변 장부를 관리함으로써 분산된 방법으로 발행된다. 장부가 변하지 않도록 하기 위하여, 나카모토는 익명의 피어들의 투표에 의해 장부 내 불일치를 해결할 수 있는 새로운 투표 메커니즘을 개발했다. 인터넷 내의 노드들은 정확하게 구별될 수 없기 때문에, 1노드 당 1투표를 실현하기 위한 메커니즘이 요구된다. IP 주소와 같은 신원들은 쉽게 장악될 수 있으므로, 비트코인은 1CPU 당 1투표라는 추상적인 개념을 효과적으로 구현하기 위하여 소위 작업 증명(proof-of-work, PoW)을 사용한다.

[0026] 현재의 PoW 기반 암호화폐 시스템들에는 그것들이 거래를 위한 실물화폐로서 사용되지 못하게 하는 몇몇 기술적

인 한계들이 있다.

[0027] - 에너지: 디지코노미스트(Digiconomist)에 의한 비트코인 에너지 소비 지수에 따르면, 비트코인에 의해 전력을 공급받을 수 있는 미국 가정의 수는 4,049,860 가정이다.

[0028] - 느린 승인: 이론적으로 블록이 완성되는 데 적어도 60분이 걸리지만, 일반적으로 제한된 블록 크기 및 대량 거래에 실질적으로 더 의존한다.

[0029] - 확장 가능성: 초 당 처리될 수 있는 거래의 개수는 단지 4-20개이다. 이는 큰 스케일의 네트워크를 위한 후보군이 될 수 없다.

[0030] PoW를 사용하는 대신, 지분 증명(proof-of-stake, PoS)을 사용하는 암호화폐 시스템들이 있다. 지분 소유자들이 투표하기 위해 그들의 지분을 거는 PoS 기반 시스템은 이른바 상기 문제들을 해결한다. PoS 공격의 유효성에 대해 여전히 논란들이 있지만, 몇몇 체인들을 동시 위조하는 것이 가능하고, 심지어 수익성이 있다고 주장된다.

[0031] 이제 암호화폐의 다른 측면들인 익명성과 탈중앙화에 대해 알아본다.

[0032] - 비 투명성: 모든 거래들은 소유자가 확인될 수 없는 임의의 주소들 하에서 처리된다.

[0033] - 비 탈중앙화: 파워 또는 지분을 해싱하는 것은 소규모 그룹인 사람들에 의해 장악됐다.

[0034] 1.1. 투명성

[0035] 암호화폐들은 실물화폐만큼 추적 불가능하도록 온라인 화폐 시스템을 효율적으로 실현한다. 비트코인이 도입된 이후로, 암호화폐에 많은 초점이 쏠렸고, 이는 여러 가지의 암호화폐 시스템들의 홍수(암호화폐의 수는 약 1,300 여 개)를 촉발했다. 그러나, 블록 체인(block chain) 개념을 사용하는 거의 모든 암호화폐들은 추적이 불가능하다. 실세계에서의 현금이 자금 세탁 및 조세 회피와 같은 범죄에 사용될 때조차 추적하는 것이 쉽지 않은 것처럼, 암호화폐들은 거래소에서 실물화폐로 교환될 때를 제외하고는 추적할 수 없다. 그러나, 현대 사회는 신용 카드, 체크 카드 및 급여로 인하여 보다 투명한 경제로 나아간다. 현재의 현금 모델은 이러한 대안제들에 의해 점진적으로 사라지고 있다. 그러나, 비트코인으로 대표되는 암호화폐들은 우리가 나아가고 있는 방향과 반대로 나아간다. 그 불투명성을 보여주는 한 사례는 2017년 3월, 미국 증권거래위원회(US SEC)에서 거래의 불투명성 때문에 윙클보스 비트코인 트러스트(Winklevoss Bitcoin Trust)가 상장되지 않도록 결정한 것이다.

[0036] 1.2. 탈중앙화

[0037] 본 발명의 실시예들에 따른 p2p 플랫폼은 어떤 암호화폐도 생성하지 않기 때문에, 탈중앙화란 네트워크에 대한 기여와 보상이 참여자들에게 균일하게 분배되는 것을 의미한다. Bolckchain.info에 따르면, 상위 7개의 채굴 그룹들은 세계 해싱 파워의 70% 이상을 점유하고 있다. 최근에 암호화폐들은 처음 제안됐을 때 기대되었던 것만큼 탈중앙화되지는 않은 것으로 추측된다. 지분 증명은 또한 고지분 소유자들이 장부를 제어하도록 하며, 이중 지급(double spending)이 가능한 것으로 보고된다. 소규모 그룹인 사람들에 의한 중앙화를 방지하기 위하여, 1인-1투표만이 해결책이고 다른 대안들은 단지 유사한 것들에 불과하다.

[0038] 1.3. 적은 수의 그룹들에 의해 장악될 수 없는 고-탈중앙화된 공개 장부들 및 거래 상의 고-투명성 공개 장부들이라는 요구를 만족하기 위한 본 발명의 실시예들에 따른 아이디어는 실명 기반 투표를 사용하는 것이다. 금융 거래들이 실명으로 수행되어야 한다는 것을 고려할 때, 본 발명의 실시예들에서는 익명의 네트워크를 고수할 필요가 없다. 본 발명의 실시예들에서는 장부 상 프라이버시를 보호하는 반면, 진정한 탈중앙화 및 높은 수준의 투명성을 모두 성취할 수 있는 p2p 금융 플랫폼을 제안한다. 비효율적인 PoW 기반 투표를 사용하는 대신에, 본 발명의 실시예에 따른 시스템은 훨씬 더 안전하고, 빠르고, 확장 가능하며, 친환경적인 인구 증명(proof-of-population, PoP) 기반 투표를 사용한다.

[0039] 이제, 암호화폐에 대해 논의한다. 비트코인 설계자들의 목표는 거창하지만 비트코인은 화폐가 될 수 없다. 사람들은 상품을 구매하기 위해 그것을 사용하길 원하지 않고, 투기하는 것을 원하며, 이에 대한 여러 이유가 있다. 하나는 그것이 실물화폐에서 분리되어 독자적인 생태계에서 기능한다는 것이며, 다른 하나는 높은 채굴 비용이다.

[0040] - 폐쇄된 생태계: 화폐 장부 기술들은 채굴자들의 경제적인 인센티브를 안정적으로 유지하기 위하여 폐쇄된 생태계에 의존한다. 즉, 암호화폐는 보상이고 거래는 오직 암호화폐로 이루어진다.

[0041] - 채굴 비용: PoW 기반 장부들은 높은 채굴 비용 때문에 소액 거래를 처리하는 데 적합하지 않다.

[0042] 1.4. 암호화폐의 폐쇄된 생태계

[0043] 현재 암호화폐 네트워크들에서, 보상은 네트워크 내에서 암호화폐로 주어지며, 장부 상 거래들은 오직 같은 암호화폐로 이루어진다. 이러한 폐쇄된 생태계는 공격자들의 인센티브에 대한 가치를 매우 안정적으로 유지하는 효과를 주지만, 다른 한편 장부의 사용을 오직 암호화폐와 관련된 거래들로 제한한다. 장부 내 거래들을 위한 화폐와 보상에 대한 암호화폐가 다르다면, 경제적인 인센티브는 채굴자들을 유인할 수 없다. 비트코인 장부가 USD 거래들을 처리하고, 거래 비용 및 코인베이스(coinbase)를 포함하는 보상들은 비트코인으로 주어진다고 가정하자. 비트코인의 가치가 급락하고 보상들이 블록들 내 거래들보다 더 작아질 때, 이러한 화폐 분리는 명백하게 공격자들로 하여금 정직하게 채굴하지 않도록 할 것이고, 잘못된 행동(거래 블록들을 위조하는 것)을 하도록 장려한다. 가치가 매우 높을 때, 거래 비용은 너무 높아서 소액 거래들을 처리하기에 너무 높을 것이다. 이는 대부분의 암호화폐들이 그들의 네트워크에서 재귀적으로 정의되는 이유이다. 거래를 위한 화폐와 보상을 위한 화폐를 분리할 수 없음에도 불구하고, 채굴자들에게 실제의 경제적인 인센티브를 주기 위하여 화폐 가치를 평가하는 방법이 있음에 틀림없다. 암호화폐 거래소들은 이러한 목적을 위해 존재하지만, 암호화폐들의 가치는 투기에 의해 급변하고 있다.

[0044] 1.5. 채굴 비용

[0045] 다른 한편, PoW를 풀어내며 블록들을 채굴하기 위한 비용은 최근 매우 높아서 적은 양의 거래를 융통하는 데 사용하기가 어렵다. 예를 들어, 초대형 채굴 풀인 AntMiner S9에 의한 한 블록 채굴은 하드웨어 비용을 고려하지 않더라도 19,598.50 USD의 비용이 든다. https://grisha.org/blog/2017/09/28/electricity-cost-of-1-bitcoin/. 그러므로, 우리가 소액 거래를 처리하는 데 비트코인을 사용할 수 없다는 점은 꽤 명백하다.

[0046] 결과적으로, 실물 경제와 분리된 폐쇄된 생태계 및 높은 채굴 비용은 PoW/PoS 기반 암호화폐들이 실물 거래에 적용될 수 없게 한다. 이를 극복하기 위하여, 우리는 암호화폐 대신에 법정화폐(fiat currency) 사용을 제안한다. 이것 또한 장부 상 화폐의 재귀적인 사용이지만, 이러한 설계 선택은 폐쇄된 생태계 문제를 단순화한다. 본 발명의 실시예들에 따른 장부 상 화폐는 이미 현실의 바로 그 화폐(법정화폐)이다. 암호화폐를 법정화폐와 교환하기 위해서 어떠한 거래소도 필요하지 않다. 어떠한 암호화폐도 본 발명의 실시예들에 따른 시스템에서 생성되지 않는다. 본 발명의 실시예들에 따른 p2p 플랫폼(사실상, 임의의 암호화폐의 거래를 처리하기 위해 사용될 수 있는)이 특정 종류의 화폐에 제한되지 않을지라도, 본 발명의 실시예들에 따른 플랫폼 상에서 화폐에 대한 분산된 장부를 운영하는 방법을 보여줄 것이다. 장부 상에 법정화폐를 취급하기 때문에, 그것은 가치 변동과 상관없이 상업 및 온라인, 오프라인 지불을 위해 자유로이 사용될 수 있다. 블록을 만들기 위한 증명을 생성하는 비용은 PoW와 비교할 때 매우 평범한, 서명들을 생성하고 모으는 것이다. 그러므로, 채굴자들을 위한 경제적인 인센티브는 클 필요가 없으며, 이는 소액 거래들이 네트워크 상에서 효율적으로 처리될 수 있다는 것을 의미한다.

[0047] 전술한 모든 문제들을 해결함으로써, 본 발명의 실시예들에 따른 p2p 금융 플랫폼은 은행들이 금융 상품을 판매하도록 할 수 있으며, 소비자들로 하여금 중앙 서버에서 운영되지 않는 계좌를 개설하도록 할 수 있다.

[0049] 2. 배경

[0050] 비트코인에 의해 해결된 문제는 BGP(Byzantine Generals Problem)라고 불리며, 이는 불완전한 통신 네트워크 및 불완전한 대중들이라는 가정 하에서, 대중들 사이에서의 일치를 만드는 것이다. 비트코인은 인터넷 상의 '같지 않은' 익명의 사용자들 사이에서 BGP를 해결하기 위한 시도이다. 비트코인 네트워크는 인터넷으로 연결된 참여자들이 익명성을 유지한 채 네트워크에 자유롭게 참여하고 떠날 수 있는 인터넷상의 불변의 공개 장부를 만들기 위해 구축되었다. 심지어 더 심하게, 그들은 그들 고유의 이익을 찾기 위하여 공개 장부를 훼손(corrupt)시키려고 한다. 이때, 훼손에 의해 동시에 존재하는 다수의 장부들이 있을 가능성이 있다. 단일한 공개 장부에 합의를 하기 위한 명확한 방법은 투표이지만, 익명의 사용자들 사이에서 신뢰받고 안전한 방법으로 투표하는 것은 쉽게 수행될 수 없다. 단일한 장부를 위해 투표하는 방법은 인터넷 내 BGP와 관련된다. 비트코인은 1투표를 위한 1CPU를 효율적으로 구현하는 작업 증명(PoW)으로 문제를 해결한다. PoW와 함께 다수의 거래들을 보유하는 블록들은 블록 체인으로 구성되는 하나의 공개 장부에 연결된다. PoW는 "채굴자"라고 불리는 네트워크 참여자들에 의해 계산되고 채굴자들은 암호화폐의 형태로 거래 비용 및 코인베이스(coinbase)를 보상받는다. 장부를 변형하기 위하여, 공격자들은 현존 블록 체인에 다른 거래를 더하고, 현존 체인을 찾아내어(catch up) 치환(override)하는 PoW를 더함으로써 체인을 포크(fork)시킨다. 이것을 하기 위해, 공격자는 블록 체인에 대한

PoW를 계산하기 위하여 더 많은 컴퓨팅 파워를 가져야 한다. 만들어진 블록 체인이 현존 체인보다 길어지는 지점에 다다를 때, 공격자는 위조한 체인을 공개하고 이 새로운 체인으로 치환할 것을 요청한다. 공격자 또는 공격자들의 그룹은 공격을 성공하기 위하여 51% 또는 그 이상의 컴퓨팅 파워를 가져야 한다(51% 공격).

[0051] 익명의 네트워크 상 투표의 어려움은 비트코인의 PoW 기반 블록 체인의 가치이다. 그러나, 익명성은 자금 세탁 및 조세 회피 관점에서 실물 금융 플랫폼에 대한 블록 체인 기술의 적용을 방해한다. 그러므로, 금융 서비스 부문의 기구들은 '프라이빗 블록 체인(private block chain)' 및 '컨소시움 블록 체인(consortium block chain)' 기술에 흥미를 갖는다. 프라이빗/컨소시움 블록 체인 네트워크에서, 이해 관계가 있는 개체들은 프라이빗/컨소시움 블록 체인에 참여하고 훼손된 장부는 일부 개체에 손실을 주기 때문에, 개체들은 어떠한 '코인' 또는 '채굴' 보상 없이도 네트워크를 운영하는 것이 가능하다. 블록 체인의 진정한 의미는 이해 관계 없는 익명의 참여자들 사이에서 합의를 만들 수 있는 공개 장부에 있다는 관점에서, 참여 노드들의 신원이 서로에게 알려지고 노드들이 기구들에 의해 운영되는 프라이빗/컨소시움 블록 체인들은 단지 보안 목적을 위한 데이터베이스들의 중복된 분산으로 여겨질 수 있다. 본 발명의 실시예들에서는 프라이빗 또는 컨소시움 블록 체인 내 개체들이 실제 신원을 가지며, 서로 쉽게 신원 보장이 가능하고, 이에 따라 데이터베이스에서 불일치가 발생할 때 PoW/PoS 없이 쉽게 합의할 수 있다는 점에 주목한다. 프라이빗 또는 컨소시움 블록 체인에 기반하는 현재의 실험적인 프로젝트들은 이해관계를 갖는 개체들에 의한 중복 데이터베이스 관리에 의해 얻어지는 보안 및 분산 데이터베이스 시스템들 간 통일성(coherence)의 효율에 집중하고 있다. 이해관계가 있는 제 3자들 사이에서의 거래들을 다루기 위하여, PBFT(practical Byzantine fault tolerance protocols)의 변형들이 프라이빗 체인을 위해 채택되어 왔다. 그러나, 대부분의 PBFT 프로토콜들은 퍼블릭 체인 네트워크에서 사용되기에 충분할 정도로 확장 가능하지 않다. 그러므로, 프라이빗/컨소시움의 의미는 제한된다.

[0052] 현존 블록 체인들과는 달리, 우리의 블록 체인은 공개 장부(Public Block Chain)의 개방성 및 프라이빗 장부(Private Block Chain)의 높은 처리량 모두를 갖는다. 한편, 익명의 노드들이 아니라 실명 인증된 노드들에 의해 동작하기 때문에 프라이빗 블록 체인으로 보인다. 다른 한편, 노드들이 우리의 네트워크에 자유롭게 참여하고 떠날 수 있다는 점 및 블록들이 이해 관계없는 임의적인 노드들에 의해 서명된다는 점에서, 퍼블릭 체인으로도 보인다. 이는 익명의 네트워크가 아니지만 실명 인증된 피어들에 의해 작동되는 네트워크이므로, 기록되는 모든 거래들은 필요하다면 정부 당국에 의해 신원 확인이 가능하다. 새로운 장부는 실물화폐와 암호화폐를 포함하는 임의 유형의 자산을 다루는 궁극적인 P2P 금융 플랫폼으로서 작용할 수 있다. 이 플랫폼을 사용함으로써, 은행의 장부가 은행 서버가 아닌 스마트폰 및 컴퓨터들을 사용하여 피어들에 의해 운영되는 분산된 불변 장부 내에서 관리되는 P2P 은행이 생긴다. 은행의 역할은 그들의 소비자들을 매핑하고 네트워크 상에서 금융 상품들을 판매하는, 가명(pseudonym) 및 실제 신원 관리를 포함한다.

[0054] 3. 동기(motivation)

[0055] 퍼블릭 블록 체인의 혁신은 PoW에 의한 익명 투표를 가능하게 함으로써, 장부 불일치를 해결하는 것에 있다. 노드의 신원이 알려지지 않더라도, 하나의 노드에서 오는 두 개의 투표(중복 투표)인지 또는 다른 노드들에서 오는 두 개의 투표(2개의 유효한 투표)인지 구별하는 방법이 있다면, 장부 불일치를 해결하기 위하여 투표 수를 카운트할 수 있다. 중복 투표의 경우, 두 개의 투표 중 하나는 무시될 수 있다. 이 경우, 비싼 PoW 계산이 필요하지 않고 투표를 카운트할 수 있다. 실명 기반 식별자 및 그 디지털 서명은 이 목적을 위해 기능할 수 있다. 실명 식별은 단지 투표만을 위해서라면 과도하지만, 고-탈중앙화, 고-투명성 장부들을 위한 실명 추적 가능 플랫폼을 목적으로 하기 때문에, 본 발명의 실시예들에 따른 목적에 완벽히 부합한다.

[0056] 실명 기반 가명 및 디지털 서명을 사용하는 본 발명의 실시예들에 따른 p2p 장부는 블록이 명백한 과반수 투표에 의해 확인되는 프라이빗/컨소시움 블록 체인의 변형으로 보일 수 있다. 그러나, 본 발명의 실시예들에 따른 장부는 일단 실명으로 식별되면 누구라도 네트워크에 자유롭게 접근하고 떠날 수 있으며, 장부 접근은 누구에게도 제어되지 않고 블록은 임의적인 피어들에 의해 서명될 수 있다는 점에서 퍼블릭 블록 체인의 일종이다. 또한, 퍼블릭 체인의 작동 환경은 프라이빗 체인과 다르다. 서명자(signer)의 수는 많고, 과도한 포킹(forking)은 큰 네트워크 지연에 의해 빈번하게 발생한다. 그러므로, 우리는 하이퍼레저(Hyperledger)와 같은 프라이빗/컨소시움 블록 체인에서 취하는 PBFT 기반 과반수 투표 알고리즘과는 다른 전략이 필요하다.

[0057] 프라이빗/컨소시움 블록 체인에서는 블록에 이해 관계가 있는 서명자들이 블록에 서명해야 하는 반면, 본 발명의 실시예들에 따른 p2p 플랫폼에서 서명 기반 과반수 투표는 누가 블록에 서명했는지에 관심이 없고 얼마나 많은 투표자들이 블록에 서명했는지에만 관심이 있다. 그러므로, 서명들은 특정 수의 피어들이 블록에 투표했다는 사실을 증명하는 데 사용된다. 간단히 말하면, PoP는 채굴자(본 발명의 실시예들에서의 "합병자(merger)")

가 서명자의 신원과 상관없이 블록에 대해 N 개의 서명을 가장 빨리 모은다면, 보상을 얻는 게임이다. 이는 해시 퍼즐을 가장 빨리 푼 채굴자가 게임을 이기는 PoW와 유사하다. 블록을 추가하기 위하여, 참여자들 사이의 N명의 임의의 피어들은 그들의 서명을 블록에 추가함으로써 블록을 위한 투표를 한다. 여기서 $N \geq 1$이다. 체인이 길어질수록, 더 많은 투표자들이 체인을 지지한다. 그러므로, 장부 상 불일치가 발생할 때, 더 많은 투표자들을 갖는 체인 포크가 선택될 것이고, 이는 과반수 투표의 정확한 구현이다. 여기서 문제는 분산 p2p 네트워크에서 효율적이고, 안전하고 탈중앙화된 방법으로 서명 기반 과반수 투표를 구현하는 방법이다. 문제에 대한 우리의 접근은 1) 거래량, 거래 비용 및 완성 시간에 의한 공격자들의 이득과 손실을 신중하게 균형 잡는 것 및 2) 완전 추적성을 통해 장부를 위조하지 못하도록 공격자들을 방해하는 실명 기반 플랫폼의 장점을 취하는 것이다.

[0059] 4. P2P 장부 프로토콜

[0060] 새로운 블록 체인을 현실화하기 위하여, 디지털 서명을 사용하는 인구 증명(PoP)은 개인들에 의한 명백한 투표 실현인 PoW 또는 PoS(Proof of Stake) 대신 사용된다. 누적된 컴퓨팅 파워 및 지분의 양에 의존하는 PoW 및 PoS와는 달리, PoP는 블록을 지지하는 사람들의 누적된 수에 따라서 결정을 한다. 그러므로, 포킹(forking)이 여러 버전의 체인을 생성하는 공격 또는 비동기화에 의해 발생할 때, 더 많은 인구를 갖는 체인 또는 더 많은 투표자에 의해 지지되는 체인이 게임을 이기는 체인으로 선택된다.

[0061] 4.1. 노드: 서명자(Signer) 및 합병자(Merger)

[0062] PoP 네트워크에는 두 종류의 노드가 있다. 한 종류의 노드는 디지털적으로 블록에 서명함으로써 공개 장부를 유지하는 데 기여하고, 다른 종류의 노드는 다수의 거래를 하나의 블록으로 모으고, 블록에 대해 노드들에게 서명 요청을 하고, 서명(signature)들을 모아서, 이것을 현존하는 블록 체인에 연결함으로써 기여한다. 전자의 노드는 서명자라고 불리고 후자의 노드는 합병자라고 불린다. 서명자는 거래 블록에 대한 서명 요청을 받을 때 PoP 지갑이 서명을 생성해야 하는지 확인하는 메시지를 사용자에게 보여준다. 이는 자동적인 서명을 위한 사전 동의를 설정함으로써 자동적으로 수행될 수 있다. 본 발명의 실시예에서는 서명 모듈이 스마트폰과 같이 어플리케이션의 설치가 가능한 단말 상에서 실행되는 경우를 고려한다. 서명자는 자신의 단말에 본 발명의 실시예들에 따른 어플리케이션을 설치함으로써, 서명자는 블록에 서명하는 것에 대한 보상으로서 얼마의 돈을 벌 수 있다. 합병자는 거래 블록을 구성하기 위하여 특정한 수의 거래들을 수집하고 검증한다. 또한, 각 거래 블록에 대하여, 합병자는 서명자들로부터 블록에 대한 일정 수의 유효한 서명들을 수집하고 그것들을 블록에 삽입해야 한다. 합병자의 소프트웨어(유효한 서명들의 수집 및 삽입을 위한 모듈) 또한 스마트폰 또는 데스크탑/서버 컴퓨터와 같은 합병자의 단말 상에서 실행될 수 있다. 합병자 노드는 더 많은 서명자들이 그들의 네트워크에 참여하게 해서 필요한 만큼 많은 서명들을 빠르게 수집하기 위하여 스스로를 알리거나 프로모션을 해야 한다. 서명자가 네트워크에 참여할 때, 스스로를 합병자들에 등록할 것이고 합병자들은 서명자에게 블록에 서명하라고 요청할 것이다. 서명자가 다수의 합병자들에 참여할 때, 서명자는 합병자들 사이에서 우선순위를 설정해야 한다. PoP 네트워크에 참여하는 노드들은 네트워크를 유지하기 위하여 그들의 작업에 대한 보상을 받아야 한다. 합병자 노드들은 거래 수집/검증 및 이러한 거래를 위한 서명들을 수집하는 것에 대한 보상을 받고, 서명자 노드들은 서명을 생성한 그들의 기여에 대해 보상을 받는다. 이 보상은 장부 상의 그들의 계좌에 실제 화폐로 주어진다.

[0063] 도 1은 본 발명의 일실시예에 따른 P2P 장부 프로토콜의 예를 도시한 도면이다. 제1 점선박스(110)는 본 실시예에 따른 P2P 장부로서의 서명된 블록 체인의 예를 나타내고 있으며, 도 1은 합병자(120)가 사용자간의 거래들 및/또는 사용자와 상인들간의 거래들을 하나의 블록으로 합병하여 제1 점선박스(110)에 표시된 서명된 블록 체인의 새로운 블록(111)으로 추가하고자 하는 경우의 예를 나타내고 있다. 도 1에서는 거래 1(131)과 거래 2(132)를 도시하고 있으나 실제로는 새로이 추가하고자 하는 블록(111)의 종전 블록(112)이 승인된 이후에 발생되어 합병자(120)에게 전달된 복수의 거래들을 포함할 수 있다.

[0064] 예를 들어, 거래가 A에서 B로 발생할 때, 금액의 양, 날짜/시간, 거래 목적 및 그들(A와 B)의 ID들을 포함하는 거래 기록은 A 및 B의 개인 서명 키들을 이용하여 서명되고 A와 B 중 어느 하나에 의해 합병자들로 보내진다. 다시 말해, 도 1에서 사용자와 사용자간의 거래 1(131)은 금액의 양, 날짜/시간, 거래 목적에 대한 정보와 두 사용자들의 ID들을 포함할 수 있다. 또한, 거래 1(131)은 두 사용자들의 개인 서명 키들에 의해 서명(133)되어 합병자들에게 전송될 수 있다. 도 1에서는 하나의 합병자(120)를 대표적으로 도시하고 있으나, 실질적으로는 복수의 합병자들 각각으로 거래 기록이 전달될 수 있다. 이와 유사하게, 도 1에서 사용자와 상인간의 거래 2(132)는 금액의 양, 날짜/시간, 거래 목적에 대한 정보와 사용자의 ID 및 상인의 ID를 포함할 수 있다. 또한,

거래 2(132)는 사용자의 개인 서명 키와 상인의 개인 서명 키에 의해 서명(134)되어 합병자들에게 전송될 수 있다.

[0065] 이때, 거래들(131, 132)은 서명자들(141, 142, 143)에 의해 서명될 수 있다. 도 1에서는 대표적으로 세 명의 서명자들(141, 142, 143)이 합병자(120)의 요청에 따라 새로운 블록(111)을 위한 서명들(151, 152, 153)을 제공함에 대해 도시하고 있다. 이때, 새로운 블록(111)에 대한 서명에 참여할 서명자들은 이후 설명될 방식에 따라 선택될 수 있다.

[0066] 합병자(120)는 새로운 블록(111)에 서명(121)하여 모든 합병자들에게 브로드캐스팅할 수 있으며, 합병자들에 의해 승인된 새로운 블록(111)은 제1 점선박스(110)에 나타난 서명된 블록 체인의 마지막 블록으로 추가될 수 있다. 합병자들이 블록을 승인하는 방식에 대해서는 이후 더욱 자세히 설명한다.

[0067] 이처럼 본 발명의 실시예들에 따른 PoP 네트워크에서 거래는 계좌 소유자에 의해 서명되고 합병자에게 보내질 수 있으며, 다수의 거래를 포함하는 블록은 서명자들 및 합병자들에게 서명될 수 있다.

[0068] 도 2는 본 발명의 일실시예에 있어서, 서명된 블록 체인에 추가된 새로운 블록이 포함하는 정보의 예를 도시한 도면이다. 도 2는 도 1을 통해 설명한 서명된 블록 체인의 마지막에 추가되는 새로운 블록(111)이 서명(141)된 거래 1(131)과 서명(142)된 거래 2(132)를 포함하며, 이러한 새로운 블록(111)이 서명자들(141, 142, 143)에 의해 서명(151, 152, 153)되어 있음을 나타내고 있다. 또한, 합병자(120) 역시 새로운 블록(111)에 서명(121)하였음을 나타내고 있다.

[0069] 4.2. PoP 네트워크에 노드로서의 참여 및 계좌 개설

[0070] PoP 네트워크는 얼마나 많은 사람들이 블록을 지원하는지를 요구하기 때문에, 개인은 네트워크에 입장하기 전에 p2p 은행에 의해 실명으로 신원을 인증 받아야 한다. 사용자가 인증을 받으면, 스스로 고유의 공개 키(publickey)/비밀 키(private key) 쌍 및 가명(pseudonym)을 생성하고 p2p 은행으로부터 그 쌍에 대한 서명을 받는다. 그러므로, p2p 은행의 역할은 사용자를 인증하고 가명 및 공개 키 쌍에 대한 공개 키 인증서를 발행하는 것이다. 사용자는 이 모든 것을 전자 지갑에 저장하지만, p2p 은행에 의해 서명을 받은 공개 키 및 가명 쌍은 블록 체인에 등록되고 p2p 은행은 실명을 저장하며 공개 키 및 가명은 데이터베이스 내에 튜플(tuple)로 저장된다. 다수의 p2p 은행들에 의해 생성된 이 데이터베이스는 노드들을 구분하기 위하여 공유되어야 하거나 단일한 신뢰 당국에 의해 관리받을 수 있다. 여기서 당국의 역할이 실명 및 가명 쌍들의 관리에 제한되지만 거래 처리와는 관련이 없다. 공개 키는 필요하다면 장부 상에 새로운 공개 키 및 가명 쌍을 추가함으로써 업데이트 될 수 있다. 유사하게, 가명은 데이터베이스 내에 재등록함으로써 업데이트될 수 있지만 체인지 로그도 관리되어야 한다.

[0071] 장부 상에 인증을 성공적으로 등록받은 사용자는 서명자, 합병자 및/또는 원한다면 소비자로서 역할을 할 수 있다.

[0072] 4.3. p2p 은행에서의 거래 처리

[0073] 도 1을 통해 설명한 바와 같이, 거래가 A에서 B로 발생할 때, 금액의 양, 날짜/시간, 거래 목적 및 그들의 ID들을 포함하는 거래 기록은 A 및 B의 개인 서명 키들을 이용하여 서명되고 A와 B 중 어느 하나에 의해 합병자들로 보내진다. 합병자들은 지갑 내에 프로파일된 합병자들 순위에 따라 송신자에 의해 선택된다. 이제, 거래 기록을 받은 합병자는 그 기록의 유효성을 검증하고, 일부 기록들을 합병함으로써 거래 블록을 만든다. 블록이 구성될 때, 합병자는 블록을 체인에 추가하기 위하여 가능한 빠르게 미리 정해진(그러나 주기적으로 조정되는) 수의 서명들을 수집한다. 서명자와 합병자는 오직 그들이 네트워크에 참여한 후에 생성된 블록에 대해서만 서명을 만들 수 있다. 블록에 대한 서명자들은 합병자에 의해 임의로 선택되지 않고, 종전 블록의 거래 기록들의 임의적(random)이어서 예측 불가능하지만 결정적(deterministic)이어서 입력에 따라 출력이 결정되는 함수의 출력 결과인 해시 값에 의해 선택될 수 있다. 일례로, 해시 값은 합병자들 각각에서 미리 설정된 해시 함수를 통해 생성할 수 있다. 이때, 종전 블록의 거래 기록들로부터 추출되는 정보를 파라미터로 갖는 해시 함수를 통해 그 결과값인 해시 값에 따라 서명자들이 선택될 수 있다. 그러므로 공격을 위해 서명 그룹을 변화시키기 위해서는, 종전 블록의 거래들을 변화시켜 그들의 해시 값이 공격자들의 서명자 그룹을 선택하도록 하는 것이 필요하다. 이때, 이미 설명한 바와 같이 종전 블록의 거래들을 변화시키기 위해서는 그 이전 블록의 거래들을 변화시켜야만 한다. 결과적으로, 한 블록의 서명 그룹을 변화시키는 것은 선행하는 모든 블록들 및 모든 후속 블록들의 모든 서명 그룹을 변화시키는 것과 관련된다.

[0074] 도 3은 본 발명의 일실시예에 있어서, 종전 블록에 기반하여 새로운 블록을 위한 서명자들이 선택하는 예를 도

시한 도면이다. 도 3은 도 1을 통해 설명한 새로운 블록(111)과 새로운 블록의 종전 블록(112)을 도시하고 있다. 이때, 종전 블록(112)은 거래 a(310), 거래 b(320) 및 거래 c(330)에 대한 정보를 포함할 수 있으며, 도 2를 통해 설명한 바와 유사하게 서명자들의 서명들, 그리고 합병자의 서명을 포함할 수 있다. 또한, 앞서 설명한 바와 같이, 종전 블록(112)은 종전 블록(112)의 이전 블록에 기반하여 생성된 이전 해시 값(340)을 포함할 수 있다.

[0075] 합병자(일례로, 도 1을 통해 설명한 합병자(120))는 종전 블록(112)에 포함된 거래 a(310), 거래 b(320) 및 거래 c(330)에 대한 정보를 파라미터로 갖는 해시 함수(350)를 통해 새로운 블록(111)을 위한 해시 값을 생성할 수 있다. 새롭게 생성된 해시 값은 도 3에 도시된 이전 해시 값(360)과 같이 새로운 블록(111)에 포함될 수 있다. 한편, 합병자는 해시 함수(350)를 통해 생성된 해시 값에 기반하여 서명자들(370)을 선택할 수 있다. 예를 들어, 도 1의 서명자들(141, 142, 143)은 합병자(120)가 해시 값에 기반하여 계산된 서명자 ID들에 의해 선택될 수 있다.

[0076] 이후에는 도 1을 통해 설명한 바와 같이, 합병자가 서명자들(370)에게 새로운 블록(111)을 보내어 서명자들(370)의 서명들(151, 152, 153)을 받아 합병할 수 있다. 이처럼 본 발명의 실시예들에 따른 PoP 네트워크 내 블록은 서명자들 및 합병자들에게 서명될 수 있으며, 서명자 그룹은 종전 블록의 거래에 대한 해시 값에 의해 강제될 수 있다.

[0077] 1) 거래는 합병자의 네트워크에 브로드캐스트되고 합병자들은 일부 거래량이 수집될 때까지 기다린다.

[0078] 2) 합병자는 거래들을 블록에 수집하고, 서명자 ID를 계산하고, 합병자의 서명자 관리목록에 등록된 서명자들 중에서 가장 가까운 ID를 갖는 서명자들을 찾고, 그 서명자들에게 블록을 보낸다.

[0079] 3) 서명자는 블록의 유효성을 확인하고, 블록 상의 서명을 통해 합병자에게 응답한다.

[0080] 4) 합병자는 블록 상의 일부 서명들을 얻을 때까지 기다리고, 성공적으로 얻는다면 블록에 서명하고 모든 합병자들에게 복수 서명된 블록을 브로드캐스팅한다.

[0081] 5) 합병자들은 블록이 유효하고 중복 지급되지 않을 때만 블록을 승인한다.

[0082] 6) 합병자들은 종전 해시로서 승인된 블록의 해시를 사용하여, 체인에 다음 블록을 생성하는 작업을 함으로써 블록 승인을 통지한다.

[0083] 서명자는 서명한 모든 블록 ID들을 보유해야 한다. 서명자는 아래와 같은 내용을 확인한 후에 블록에 대한 서명을 한다.

[0084] - 블록 내 시간 스탬프는 분산된 네트워크 상의 시간 동기화 에러를 고려한 현재 시간과 매치되지 않으면, 당국에 보고하고 블록을 무시한다(예를 들어, 비트코인 네트워크에서, 블록은 타임 스탬프가 마지막 11개 블록의 중앙값보다 크면 유효한 것으로 승인된다).

[0085] - 서명 요청이 서명자가 네트워크에 참여하기 전에 생성된 블록에 대한 것이라면 무시한다.

[0086] - 요청이 마지막으로 서명된 블록이 완성되기 전에 생성된 블록에 대한 것이라면, 합병자로부터의 서명 요청은 자동적으로 거절될 것이다.

[0087] - 요청이 이미 서명된 블록 상의 거래들에 대한 정보를 포함하는 또 다른 블록에 대한 것이라면, 서명자는 요청을 무시하고 합병자에게 이를 통지한다. 이 통지는 "당신은 늦었습니다. 거래는 이미 추가되었습니다."라는 메시지를 합병자에게 신속하게 알리는 효과가 있다.

[0088] - 요청이 서명된 것과 일치하지 않는 거래를 포함하는 블록에 대한 것이라면, 해당 요청을 한 사용자를 네트워크 밖으로 쫓아내기 위하여 서명자는 당국에 보고하고 합병자 ID 및 송신자 ID를 네트워크에 브로드캐스팅한다. 이제, 이 공격자로부터의 모든 요청들은 무시될 것이다.

[0089] 서명자들은 거래 비용의 공평한 분배를 위해 합병자에 의하여 시간이 지나면 자격이 박탈될 수 있다.

[0090] 4.4. 다수의 투표자들을 갖는 포크

[0091] 블록이 체인(O)에 추가될 때, 새로운 체인(N)을 형성하기 위하여 결과를 전체적인 네트워크에 퍼뜨리는 데에는 수 초가 걸린다. 그러므로, 그 시간 동안, 또 다른 합병자는 또 다른 블록을 체인(O)에 추가하려고 할 수 있으며, 이는 또 다른 체인(N')을 만드는 체인 포킹을 유발한다. 체인 포킹은 명백히 해결되어야 하는 두 가지 버전의 장부가 존재하는 것을 의미한다. PoP 네트워크에서, 적절한 체인을 선택하는 것은 투표에 의해 수행된다.

둘 이상의 포크들이 주된 체인이 되기 위해 서로 경쟁할 때, 합병자들은 더 많이 누적된 수의 서명을 갖는 포크를 선택하며, 이는 더 많은 사람들이 체인을 지지한다는 것을 의미한다.

[0092] 4.5. 승인 레벨

[0093] 블록 B_i가 체인에 추가되고 다음 블록 B_{i+1}이 그 체인에 추가될 때 B_i는 네트워크로부터 하나의 승인을 받는다. 미리 결정된 수의 승인들이 있은 후, 블록은 영구적으로 체인에 추가되며, 이 영구적인 승인 후에는 또 다른 포킹 요청이 승인되지 않을 것이다. 그러므로, 합병자는 경합하는 포크 블록 체인들 중에서 최신의 영구적인 승인에 대한 가장 빠른 타임 스탬프를 갖는 하나를 선택해야 한다. 이는 최신의 영구적인 승인 이후의 시간 프레임 내로 포킹 논의를 제한시킨다.

[0094] 처리량(throughput)을 향상시키기 위하여, 본 발명의 실시예들에서는 GHOST(Greedy Heaviest-Observed Sub-Tree)를 채택할 수 있다. 개념은 경합하는 브랜치를 제거하는 것이 아니라 브랜치가 포크되어 나오는 블록을 지원하도록 브랜치를 남기는 것이다. 이제 가장 긴 체인을 선택하는 대신에, 우리는 가장 큰 인구가 지원하는 가장 무거운 체인을 선택한다.

[0095] 4.6. 서명자 그룹 선택

[0096] 블록 B_i에 대한 서명자 그룹은 종전 블록들 상 거래 내용과, 서명 및 체인 해시가 제외된 서명자 그룹 내 서명자들의 리스트를 해시함으로써 선택된다. 즉, 리스트는 $H(H(T_{N-1}),T_{N-2}),\cdots,T_{N-t})$에 의해 계산될 수 있으며, 여기서 T_i는 i번째 블록 상의 거래 및 서명자 리스트들이며, t(≥1)는 최종 임계 값이다. 서명 그룹의 이러한 소급성 및 적용되지만 예측 불가능한 선택은 장부의 훼손을 더 어렵게 만든다.

[0097] 4.7. 해밍 거리(Hamming distance) 내 가장 가까운 서명자 ID

[0098] 서명자가 아직 참여하지 않았거나 ID를 갖는 서명자가 활성화되지 않았을 수 있기 때문에 해시 값에 의해 선택된 서명자 ID는 유효하지 않을 수 있다. 이러한 경우, 해밍 거리 내 가장 가까운 ID가 선택될 것이고 가장 긴 체인을 선택하는 스코어는 아래 수학식 1과 같이 계산될 수 있다.

수학식 1

[0099]
$$\sum_{i=1}^{N}\left[S_i * 128 - 2 \times \sum_{j=1}^{S_i} H_{ij}\right]$$

[0100] 여기서 S_i는 블록 B_i 내 서명자들의 수이고, 128은 ID의 비트 길이의 예일 수 있고, H_ij는 j번째 서명자와 해시 출력 간의 해밍 거리이다.

[0101] 4.8. 난이도 조절: 서명자들의 수

[0102] 새로운 서명자들은 합병자들을 통해 네트워크에 참여하고, 그들은 다음 블록으로부터 서명 처리에 참여한다. *S*는 블록에 서명하기 위한 서명자들의 수이다. 매 2초는 *S*개의 서명을 수집하기 위한 기준점이다. 이는 1,800개의 블록 생성 시간을 측정함으로써 계산되고, 그 수는 블록에 기록된다. *S*개의 서명을 모으기에는 너무 느리다면, 최소인 *S*(예를 들어, 5)만 보안 목적을 위해 유지된다.

[0104] 5. 보안

[0105] 5.1. 블록 위조

[0106] 블록을 위조하기 위하여, 공격자는 두 가지 선택을 할 수 있다. 하나는 블록 내 서명들을 위조하는 것인데, 이는 서명의 EUF-CMA 보안성에 의해 실행 불가능하다. 암호 서명을 파괴하는 대신에, 블록의 서명 그룹을 매수할 수 있다. 이 방법은 서명자 그룹을 교체시키고 그들 소유 서명자 그룹의 서명들을 넣는 것이다.

[0107] 5.1.1. 서명자 그룹 교체

[0108] 공격자가 $B_i^{'}$ 를 얻기 위하여 한 블록 B_i 내 거래를 변형할 때, 서명자 그룹에 의해 서명된 $B_i^{'}$를 얻어야 한다. 서명을 위조하지 않으려면 (암호학적으로 불가능하므로), 서명자 그룹을 교체시켜야 한다. 이에 대해, 서명자 그룹은 $B_{i-1}^{'}$ 의 기록들에 의해 결정되기 때문에, 종전 블록 B_{i-1} 의 거래 기록들은 $B_{i-1}^{'}$로 변형되어야 한다. 이는 결국 변형된 블록 $B_{i-1}^{'}$ 의 재서명과 관련된다. 블록 B_{i-1} 의 서명자 그룹은 그들이 이미 시간 프레임 내에 서명되었기 때문에 $B_{i-1}^{'}$ 에 재서명하지 않을 것이고, 이에 따라 $B_{i-1}^{'}$ 에 대한 서명자 그룹은 변화되어야 한다. 결과적으로, 블록 B_i 의 변형은 B_{i-1} , B_{i-2} , …, B_1 의 역행 회귀 변형과 관련된다. 또한, B_i 내 거래를 변화시킴으로써, B_{i+1} 내 저장된 체인 해시 및 B_{i+1} 의 서명자 그룹 모두가 변화된다. 결과적으로, 하나의 블록을 변화시키는 것은 순행 및 역행 체인 모두의 변형과 관련된다.

[0109] 도 4는 본 발명의 일실시예에 따른 p2p 장부가 블록 위조(forking a block)에 대한 보호되는 예를 도시한 도면이다. 도 4는 서명된 블록 체인의 일부로서, 블록 Bi-1(411), 타겟 블록 Bi(412) 및 블록 Bi+1(413)을 나타내고 있으며, 타겟 블록 Bi(412)가 서명자 그룹 a(421)에 의해 서명되었고, 블록 Bi+1(413)가 서명자 그룹 b(422)에 의해 서명되는 경우를 나타내고 있다.

[0110] 이때, 타겟 블록 Bi(412)가 승인되기 이전에 위조자가 위조 블록 Bi'(431)에 대한 승인을 받고자 하는 경우를 고려할 수 있다. 이미 설명한 바와 같이 서명자 그룹 a(421)는 블록 Bi-1(411)의 거래에 대한 해시 값에 기반하여 선택되기 때문에 위조자는 다른 서명자 그룹을 활용하여 위조 블록 Bi'(431)에 대한 서명을 받기 위해서는 블록 Bi-1(411)의 거래 내용을 위조해야 한다. 이는 위조자에게 블록 Bi-1(411)의 이전 블록들을 순차적으로 모두 위조해야 할 것을 요구한다.

[0111] 또한, 위조자는 서명자들에 대한 공모를 시도할 수 있다. 그러나, 위조자가 공모자들을 모으기 위해서는 공개적으로 광고를 해야 한다는 부담이 있으며, 다음의 위조 블록 Bi+1'(432)에 서명을 받기 위한 서명자들이 위조 블록 Bi'(431)의 거래 내용에 의해 선택되기 때문에, 위조 블록 Bi+1'(432)를 위해 선택되는 서명자 그룹은 도 4에 도시된 바와 같이 서명자 그룹 x(441)로서 정상적인 블록 Bi+1(413)의 서명자 그룹 b(422)과 달라지게 된다. 다시 말해, 다음 위조 블록 Bi+1'(432) 뿐만 아니라, 이후에 새롭게 추가되어야 할 위조자의 모든 위조 블록들은 중복 서명에 의해 다수의 합병자들이 시도하는 정상적인 블록들과 지속적으로 경쟁해야만 하며, 이러한 경쟁은 서명된 블록 체인의 마지막 블록에 대해서까지 반복되어야만 한다.

[0112] 5.1.2. 매수로 훼손되거나 도난 키로 협상된 서명자 그룹

[0113] 블록을 위조하기 위하여 서명자 그룹을 매수하거나 키를 훔침으로써, 공격할 수 있다. 이렇게 하면, 현재 블록 B_i 에 대한 서명자 그룹이 변화되지 않아서 정확하지만 매수된 서명자 그룹에 의한 유효한 서명들이 부가되기 때문에, 공격자는 종전 블록들을 변화시킬 필요가 없다. 공격자는 오직 순행 위조에 대해서만 관심이 있다. 거래들 및 대응하는 서명들의 변화에 의해, 다음 블록 B_{i+1} 에 대한 서명자 그룹 및 체인 해시 값은 실제 체인 상의 블록의 것들과는 본질적으로 매치되지 않는다. 그러므로, 공격자는 블록 B_{i+1}에 서명하기 위하여 새로운 서명자 그룹을 다시 매수하거나 협상해야만 한다. 이제, 변형된 블록 $B_{i+1}^{'}$는 다른 서명자 그룹, 다른 체인 해시를 갖지만 같은 거래들을 가지며, 이는 다른 서명을 유발한다. B_{i+2} 에 대해, 블록에 서명한 서명자 그룹은 공격자들에게 매수되어야 하고, 이는 체인의 마지막 블록까지 반복된다. 확정 투표로 되돌아가기 위한 매수된 서명자들의 요구되는 수는 너무 커서 위조된 거래량에 의해 보상되지 않는다.

[0114] 5.2. 보안 경제, 포상금 및 벌금

[0115] 공격자들이 장부 위조에 참여하지 않도록 하는 다수의 장치가 있다.

[0116] 가장 중요한 첫 번째 장치는, 완전 추적 가능한 실명 기반 장부이다. 가장 강력한 동기는 모든 노드가 이미 실명 인증되었고 장부 상 모든 거래가 완전히 추적 가능하다는 사실로부터 온다. 그러므로, 네트워크 내 노드들

은 범죄가 완벽히 추적 가능하고 색출될 가능성이 높다는 것을 충분히 안다.

[0117] 두 번째 장치는, 비공개 포크가 불가능해서, 포킹을 위해서는 공개 광고가 불가피하다는 점이다. PoW 네트워크에서, 채굴자는 실제 체인(honest chain)을 치환하기 위하여 비공개 포크를 배포할 때까지 다른 채굴자들보다 빠르게 PoW를 계산함으로써 이중 지급에 대한 포크를 비밀리에 만들 수 있다. 그러나, PoP 네트워크에서, 포킹 체인을 만드는 것은 *R*개의 서명자 그룹이 약 *R*X*S*개(대략 200 서명자 또는 더 정확하게 $\sum_{i=1}^{R} S_i$)의 공모를 해야만 하기 때문에, 블록을 위조하는 합병자는 비공개 포킹을 할 수 없다. 그러나, 위조 합병자에 의해 제안받은 서명자들 중 적어도 하나는 블록이 이미 높은 확률로 완성되었다는 것을 알아야 한다(블록은 네트워크 거리의 시간 이후에 완성된다). 그러므로, 임의의 서명자는 당국에 이중 지급 시도를 신고할 것이다.

[0118] 세 번째 장치는, 각 공모 서명자에게 주어지는 인센티브가 거래 비용보다 적다는 점이다. *F*%를 거래 비용 부분으로, *TA*를 블록 당 최대량 한도라고 하자. 또한, 단일한 거래는 *TA*의 *M*% 미만으로 제한된다. 또한, S_i 및 *R*을 각각 블록에 대한 서명자 그룹 사이즈 및 확정을 위한 블록의 수라고 하자. 서명자들의 수 S_i는 네트워크 속도에 의해 결정되고, *R*은 네트워크 거리에 의해 결정된다. 명료성을 위하여, *S*를 한 블록에 대한 서명자들의 평균 수라고 가정하자. 이때, 공격자를 위한 최고의 시나리오는 막 확정된 블록을 위조하는 것이고 이는 블록들의 최소 개수만 재서명될 필요가 있기 때문이다. 공격자는 블록을 위조해서 화폐 소비에 대한 자신의 거래가 제거되도록 한다. 위조된 블록은 공격자의 이중 지급에 대해 *M*××*TA* 개의 거래를 잃고, 따라서 *M*××*F*××*TA*는 위조된 블록의 공모 서명자들에게 보상되어야 한다. 다음 블록에 대한 서명자 그룹은 이제 새로운 그룹으로 변화하고, 그들은 다음 블록을 위조된 것에 서명해야 한다. 거래들은 변화하지 않기 때문에 후속 블록들은 같은 서명자 그룹들에 의해 서명되고, 그들은 새로운 서명으로부터 추가 수입을 얻지 않는다. 이제, 후속 블록들에 대한 공모 서명자들은 중복 서명 행위라는 것을 알면서 같은 블록에 또 다시 서명하라는 요청을 받는다. 이때, 공모 서명자들은 공모에 참여할지 말지 선택해야 한다. 공모 서명자들은 두 가지를 고려한다. 하나는 네트워크 노드들에 의해 이중 서명 행위로 당국에 신고될 가능성이 높다는 점이다. 다른 하나는 공모 서명자들이 이중 서명 행위가 거래 비용을 얻을 기회를 잃게 만들 수 있다는 점을 공모 서명자들이 알고 있다는 것이다. 이는 공모 서명자들이 서명한 종전 체인이 공모 서명자들이 공모하려는 후속 체인보다 거래 비용을 벌어들일 더 많은 가능성을 갖기 때문이다. 요약하면, 공모 서명자가 얻을 수 있는 지분은, $(M \times TA - M \times F \times TA)/(R \times S)$와 같이 계산될 수 있으며, 거래 비용은 $F \times TA/S$와 같이 얻어질 수 있다.

[0119] 그러므로, 서명자는 $F \times TA/S$를 $((1-F) \times M \times TA)/(R \times S)$와 비교할 것이다. 간단한 대수에 의해, $F = M/(R+M)$가 얻어질 수 있다. 즉, *F*가 $M/(R+M)$이상일 때, 서명자는 공모에 참여하지 않고, 정직하게 행동할 것이다. *M* = 10%이고, *R* = 10으로 설정한다면, *F*를 1% 미만으로 설정할 수 있다. 이는 블록 상 단일한 거래의 최대 부분이 10%로 제한되고, 그 블록을 포함하는 10개의 블록이 더해진 후에 하나의 블록이 확인된다면, 거래 비용 1%가 공모 공격을 방지하기에 충분하다는 것을 의미한다.

[0120] 네 번째 장치로, 포상금 및 벌금을 고려할 수 있다. 네트워크를 보호하기 위하여, 본 발명의 실시예들에서는 이중 지급자의 신고자에게 주어지는 포상금 및 공격자에 대한 벌금을 도입할 수 있다. 공개적으로 광고되어야 하고 공모하기 위하여 서명자들을 모집해야 한다는 점을 고려할 때 위조에 의한 이익보다 벌금이 크다면, 잠재적인 공격자는 거의 장부를 위조하려고 하지 않을 것이다. 불법 위조에 공모할 때 얻을 수 있는 지분보다 포상금이 더 높게 설정되기 때문에 임의의 서명자는 이중 지급자를 보고할 가능성이 더 높다. 이를 위해, 포상금 및 벌금은 $((1-F) \times M \times TA)/(R \times S)$보다 높게 설정되어야 한다.

[0121] 마지막 장치를 위해, 공격에 의해 주어진 인센티브는 최대 거래 값(예를 들어, 블록 내 총합의 10%)을 설정하는 시스템 정책에 의해 제한될 수 있다. 거래의 가격이 높다면, 거래는 공격을 방해하기 위하여 많은 소규모 거래들로 분리시켜야 한다. 이렇게 함으로써, 공모자들이 얻는 최대 이익은 제한된다. 각 블록에 대해 *TA*를 작게 설정함으로써, 공격자들의 인센티브를 작게 한다. 예를 들어, *TA*를 USD 10,000으로, *S*를 10으로 각각 설정한다면, *R* = 10, *M* = 10% 및 *F* = 1%를 고려할 때, 각 공모자들에 대한 최대 이익은 단지 USD 9.9이다. USD 9.9는 완전 추적 가능한 네트워크 내에서 범죄에 가담할 정도로 충분하지는 않을 것이다.

[0122] 이처럼 블록 위조는 위조자가 공모자들을 모으기 위하여 공개적으로 광고해야 하고, 지분은 비용, 포상금 및 벌금에 비해 적기 때문에 유인이 적어진다.

[0124] 6. 기타

[0125] 6.1. 로컬 블록 체인들 및 보간(interpolation)에 의한 크기 확장가능성

[0126] PoP 체인의 확장가능성에 대해, 모든 영역 범위(regional area)는 자체의 로컬 블록 체인을 갖는다. 영역 내에서 발생하는 모든 거래들은 전술한 바와 같이 처리된다. 반면, 거래가 두 로컬 블록 체인들 사이에서 발생하는 경우를 고려할 수 있다. 예를 들어, 올랜도(Orlando)에 있는 로컬 체인 상의 A(이하, 'A@Orlando')가 페어팩스(Fairfax)에 있는 로컬 체인 상의 B(이하, 'B@Fairfax)에게로 USD 5를 보내길 원하는 경우를 고려할 수 있다. "A@Orlando가 B@Fairfax에 USD 5를 보낸다"는 거래는 잔액을 확인함으로써 처음으로 검증되고 페어팩스(Fairfax)에 있는 로컬 체인 상에서 처리될 수 있다. 그러므로, 더 많은 합병자들 및 서명자들과 관련되기 때문에 거래 간 비용은 로컬 내부의 거래 처리 비용보다 높을 것이다. B@Fairfax가 보스턴(Boston)에 있는 로컬 체인 상의 C(이하, 'C@Boston')에 얼마의 금액을 보내길 원할 때, B@Fairfax의 잔액은 페어팩스(Fairfax)에 있는 로컬 체인 상에서 처음 유효화될 수 있다.

[0127] 체인의 지역화(localization) 및 체인 간 상호 조작성(interoperability)은 크기와 속도 관점에서 장부가 관리 가능하도록 한다. 하나의 로컬 체인은 거래 규모 때문에 거래 처리는 지연되지 않고, 장부의 크기는 빠르게 증가하지 않으며, 오직 지역에서 발생하는 거래 기록들을 가지고 있다. 심지어 장부들을 작게 유지하면서, 상호 조작성에 의해 체인들 간 거래가 가능하다.

[0128] 6.2. 모든 잔액을 새로운 체인으로 이동시키는 시간 확장가능성

[0129] 체인들 간의 상호 조작성에 의해, 본 발명의 실시예들에 따른 시스템은 시간 확장이 가능해질 수 있다. 새로운 체인이 생성되고, 이는 오래된 체인을 사용하지 않도록 광고될 수 있으며, 오래된 체인 상의 모든 잔액들은 새로운 체인으로 이동될 수 있다. 이때, 오래된 체인은 피어들의 저장소(전체 노드들)에서 보관될 수 있다. 모든 잔액들이 새로운 체인으로 이동하지 않고 이후에 오래된 체인 상 거래 요청이 발생한다면, 보관된 체인은 여전히 새로운 체인으로 이동하는 데 사용될 수 있다.

[0130] 6.3. 금액에 대한 프라이버시

[0131] 다수의 주소들은 추적을 어렵게 하기 위하여 금액에 대한 프라이버시 기술이 거래들을 분리시키는 데 사용될 수 있다.

[0132] 6.4. 잔액 기반 장부

[0133] 거래 기록들 뿐만 아니라 각 계좌의 잔액은 계좌 잔액 확인을 더 빠르게 만들기 위해 장부 내에 저장될 수 있다.

[0134] 6.5. 블록 체인 상의 영수증

[0135] 오직 재산 이동 정보를 저장하는 대신에, 우리는 매수할 수 없는 온라인 영수증을 체인 상에 실현하는 것이 가능하도록 문맥 정보를 저장할 수 있다. 장부의 저장소를 절약하고 더 나은 프라이버시 보호를 위해, 오직 거래의 해시 값은 장부에 저장되지만 고유 거래 정보는 은행에 의해 별도로 저장된다.

[0136] 6.6. 종래 은행과의 거래

[0137] 소비자들이 종래 은행 계좌(T)에서 우리의 p2p 은행 계좌(P)로 소정의 금액을 이체할 때, T 내의 잔액은 줄어들고 T에서 P로의 이체를 나타내는 거래는 생성된다. 거래를 포함하는 블록이 성공적으로 블록 체인에 연결될 때, 거래 처리는 완료된다. P에서 T로의 거래는 양 쪽 계좌 내 잔액들을 조정함으로써 유사하게 처리될 수 있다.

[0138] 6.7. 국제 송금

[0139] 분명히 한 국가 내 한 체인에 있는 계좌로부터 다른 국가의 체인으로 돈을 국제적으로 송금하는 것은 가능하다. 환율을 적용함으로써, 출처 체인에 우선 거래를 기록하고 로컬 체인 상호 조작 절차를 사용하여 목적지 체인에 기록하는 것은 국제 송금을 완성시킨다.

[0141] 7. 현존하는 암호화폐 기술들과의 차이점

[0142] 7.1. 완전 추적 가능한 실명 온라인 금융 플랫폼

[0143] 본 발명의 실시예들에 따른 블록 체인은 실명으로 신원 확인된 사용자들(노드들)에 의해 실행되고 사용되며, 따라서 가명 및 실명 매핑 테이블이 주어질 때 모든 거래는 추적 가능하다. 이는 조세 회피, 자금 세탁에 대한 정부의 고민을 해소시킴으로써 장부의 발전을 용이하게 할 것이다.

[0144] 7.2. 진정한 탈중앙화

[0145] 한 명의 사용자가 하나의 투표를 할 수 있다는 점에서 PoW 및 PoS와 비교할 때 더 민주적이다. PoW 또는 PoS를 사용하는 익명의 네트워크에서, 큰 컴퓨팅 능력 소유자 또는 고-지분 소유자는 다른 이들보다 더 많이 투표할 수 있다. 이런 관점에서 보다 민주적이라는 것은 많은 것을 의미한다. 예를 들어, 보다 민주적이라는 것은 네트워크의 더 나은 보안, 공평성 및 민주적 제어를 의미할 수 있다. 현재 PoW/PoS 네트워크들은 탈중앙화가 요구되지만 그들은 사실 높은 해시 능력 그룹들, 큰 암호화폐 거래소들 및 개발자들에 의해 중앙화된다. 반면, 본 발명의 실시예들에 따른 PoP는 암호화폐, PoW, PoS가 아닌 탈중앙화를 제공할 수 있다.

[0146] 7.3. 또한, PoP는 역행 또는 순행 위조 가능성에 의한 더 높은 보안성을 제공할 수 있다.

[0147] 7.4. 높은 거래 처리 속도

[0148] 거래 처리량 및 에너지 소모의 관점에서, PoP는 PoW보다 낫다. 이는 PoP가 거래 처리를 위해 어떠한 거대한 계산도 유발하지 않기 때문이다. 결국, PoP 네트워크는 더 빠른 처리 속도 크기의 순서로 인해 PoW 네트워크에 비해 더 확장성이 있다. 현재 비트코인 네트워크의 처리 속도는 겨우 7 TPS(Transactions Per Second)이다.

[0149] 7.5. 실물화폐에 대한 프로토콜

[0150] 현재 암호화폐 네트워크에서, 보상은 네트워크 내의 암호화폐로 주어지고, 거래는 오직 암호화폐로 된다. 네트워크 내부의 이러한 재귀적인 사용은 암호화폐와 현실 세계의 가치 간의 분리를 유발한다. 그것은 암호화폐의 현실세계 가치에 대해 어떠한 기준도 제공하지 않으나, 암호화폐의 자산 가치를 불안정하게 만든다. 실물화폐(예를 들어, USD)와 암호화폐 사이를 얽는 가치는 오직 암호화폐 거래소 시장에서 발생한다. 그 곳들이 오직 암호화폐의 시장 가치가 결정되고 그 가치에 대한 어떠한 기준(또는 앵커)도 없는 장소들이기 때문에 현재 거래 시장에서의 문제들이 발생한다. 거래소에서의 불안정성 및 암호화폐 거래에 대한 재귀적인 사용은 암호화폐들이 현실 세계의 화폐의 역할을 제공하는 것을 막는다. PoP 기반 p2p 은행은 암호화폐 대신 실물화폐 이체를 다루고, 이에 따라 거래 비용은 실물화폐로 주어진다. 전체적으로, p2p 은행을 위한 프로토콜은 가상으로 개설된 금융 시스템이 아니라 실제 금융 시스템을 위해 동작한다.

[0151] 7.5. 디지털 서명

[0152] PoP 네트워크에 대해, 임의의 보안(EU-CMA 보안) 디지털 서명은 RSA-OAEP, ECDSA, DSA, 페어링 기반 서명 등과 같은 플랫폼에서 동시에 사용될 수 있다. 네트워크 대역폭이 충분하지 않으면, 집합 서명(aggregate signature)이 다수의 서명들을 압축하기 위해 사용될 수 있다.

[0153] 7.6. 다른 어플리케이션들

[0154] 금액 이체 뿐만 아니라 임의 형태의 거래들을 위해 취급될 수 있다. 예를 들어, 암호화폐는 PoP 네트워크 상에서 취급될 수 있다. 책 판매 기록들, 음악/노래 판매 기록들은 사업 처리를 투명하게 하기 위해 장부에 저장될 수 있다.

[0156] 도 5는 본 발명의 일실시예에 있어서, 네트워크 시스템의 동작 환경의 예를 도시한 도면이다. 도 5는 금융 플랫폼(510), 복수의 서명자 노드들(510) 및 복수의 합병자 노드들(530)을 나타내고 있다. 이때, 금융 플랫폼(510), 복수의 서명자 노드들(510) 각각, 그리고 복수의 합병자 노드들(530) 각각은, 일례로 이후 도 6을 통해 설명되는 컴퓨터 장치(600)와 같은, 물리적인 하드웨어 장치로 구현될 수 있으며, 실시예에 따라 둘 이상의 컴퓨터 장치들이 결합된 형태로 구현될 수도 있다.

[0157] 금융 플랫폼(510)은 앞서 설명한 p2p 은행에 대응할 수 있으며, 네트워크에 입장하고자 하는 복수의 사용자들 각각에 대해 실명으로 신원을 인증받아 상기 네트워크상에서의 사용자 식별자를 제공할 수 있다.

[0158] 복수의 합병자 노드들(520) 각각은 사용자들간의 거래에 대한 정보를 수집 및 병합하여 거래 블록을 생성하고, 생성된 거래 블록을 위한 서명자들을, 상기 생성된 거래 블록이 포함하는 거래에 대한 이해관계와 무관하게, 서명된 블록 체인의 완성된 마지막 블록의 거래에 기반하여 선택하고, 선택된 서명자들의 생성된 거래 블록에 대

한 서명을 받아 생성된 거래 블록을 서명된 블록 체인에 추가시키고자 시도할 수 있다. 복수의 합병자 노드들(520) 각각은 앞서 설명한 합병자의 단말에 대응할 수 있다.

[0159] 복수의 서명자 노드들(530) 각각은 복수의 합병자 노드들(520) 각각으로부터의 요청에 따라 복수의 합병자 노드들(520) 각각에서 생성된 거래 블록의 유효성을 확인하고, 유효성이 확인된 거래 블록에 서명할 수 있다. 복수의 서명자 노드들(530) 각각은 앞서 설명한 서명자의 단말에 대응할 수 있다.

[0160] 이때, 금융 플랫폼(510), 복수의 서명자 노드들(510) 각각, 그리고 복수의 합병자 노드들(520) 각각은, 도 5에 도시된 네트워크(540)를 통해 서로 통신할 수 있다.

[0161] 이미 설명한 바와 같이, 거래가 A에서 B로 발생할 때, 금액의 양, 날짜/시간, 거래 목적 및 그들의 ID들을 포함하는 거래 기록은 A 및 B의 개인 서명 키들을 이용하여 서명되고 A와 B 중 어느 하나(송신자)에 의해 합병자들로 보내진다. 합병자들은 지갑 내에 프로파일된 합병자들 순위에 따라 송신자에 의해 선택된다.

[0162] 이때, 복수의 합병자 노드들(520)은 선택된 합병자들의 단말들에 대응할 수 있으며, 복수의 합병자 노드들(520)은, 복수의 서명자 노드들(530)로부터 서명된 거래 블록들이 대응하는 합병자 노드들에 의해 각각 브로드캐스트됨에 따라, 서명된 거래 블록들의 유효성을 확인하고, 유효성이 확인된 서명된 거래 블록들의 서명된 블록 체인으로의 추가를 승인할 수 있다. 이미 설명한 바와 같이, PoP 네트워크는 블록을 지원하는 사람들의 누적된 수(서명 수)에 따라서 새로운 블록 체인을 선택 및 현실화한다. 이때, 새로운 블록 이전의 확정된 블록 체인에 대해서는 누적된 사람들의 수가 동일하기 때문에 결국 새롭게 블록 체인에 추가되는 거래 블록의 수에 따라 새로운 블록 체인이 선택될 수 있다. 복수의 서명자 노드들(530) 각각은 브로드캐스트되는 새로운 거래 블록들의 유효성을 확인하고, 유효성이 확인된 서명된 거래 블록들을 블록 체인에 추가하는 것을 승인할 수 있으며, 이때 거래 블록을 지원하는 사람들의 누적된 수(서명 수)가 가장 많은 거래 블록의 추가를 승인하거나 또는 유효성이 확인된 거래 블록들이 추가된 새로운 블록 체인들 중 거래 블록을 지원하는 사람들의 누적된 수(서명 수)가 가장 많은 거래 블록이 추가된 블록 체인을 선택할 수 있다.

[0163] 한편, 복수의 합병자 노드들(520) 각각은, 서명된 블록 체인에 추가시키고자 하는 거래 블록의 이전 거래 블록에 포함된 거래에 대한 정보들을 입력으로 가지면서 예측 불가능(random)하지만 입력에 따라 출력이 결정(deterministic)되는 함수를 통해 출력되는 해시 값을 생성하고, 생성된 해시 값에 기반하여 추가시키고자 하는 거래 블록을 위한 서명자들을 선택하며, 선택된 서명자들에 대응하는 서명자 노드들로 추가시키고자 하는 거래 블록에 대한 서명을 요청할 수 있다.

[0164] 이 경우, 복수의 서명자 노드들(530) 각각은 자신이 서명한 거래 블록의 블록 식별자를 관리하고, 서명된 블록 체인에서 마지막으로 서명된 거래 블록이 완성되기 전에 생성된 거래 블록에 대한 서명 요청을 거절할 수 있다. 또한, 복수의 서명자 노드들(530) 각각은 자신이 이미 서명한 거래 블록 상의 거래들에 대한 정보를 포함하는 다른 거래 블록에 대한 서명 요청을 무시하며, 서명 요청의 무시에 대한 정보를 다른 거래 블록에 대응하는 합병자 노드에게 통지할 수 있다. 또한, 복수의 서명자 노드들(530) 각각은 서명된 것과 일치하지 않는 거래를 포함하는 블록에 대한 서명 요청을 금융 플랫폼(510)에 보고하고, 서명 요청에 따른 합병자의 식별자 및 상기 일치하지 않는 거래의 송신자의 식별자를 네트워크상에 브로드캐스팅할 수 있다.

[0165] 도 6은 본 발명의 일실시예에 있어서, 컴퓨터 장치의 내부 구성의 예를 도시한 도면이다. 앞서 설명한 바와 같이, 금융 플랫폼(510), 복수의 서명자 노드들(510) 각각, 그리고 복수의 합병자 노드들(530) 각각은, 도 6의 컴퓨터 장치(600)와 같은, 물리적인 하드웨어 장치로 구현될 수 있으며, 실시예에 따라 둘 이상의 컴퓨터 장치들이 결합된 형태로 구현될 수도 있다.

[0166] 이러한 컴퓨터 장치(600)는 도 6에 도시된 바와 같이, 메모리(610), 프로세서(620), 통신 인터페이스(630) 그리고 입출력 인터페이스(640)를 포함할 수 있다. 메모리(610)는 컴퓨터에서 판독 가능한 기록매체로서, RAM(random access memory), ROM(read only memory) 및 디스크 드라이브와 같은 비소멸성 대용량 기록장치(permanent mass storage device)를 포함할 수 있다. 여기서 ROM과 디스크 드라이브와 같은 비소멸성 대용량 기록장치는 메모리(610)와는 구분되는 별도의 영구 저장 장치로서 컴퓨터 장치(600)에 포함될 수도 있다. 또한, 메모리(610)에는 운영체제와 적어도 하나의 프로그램 코드가 저장될 수 있다. 이러한 소프트웨어 구성요소들은 메모리(610)와는 별도의 컴퓨터에서 판독 가능한 기록매체로부터 메모리(610)로 로딩될 수 있다. 이러한 별도의 컴퓨터에서 판독 가능한 기록매체는 플로피 드라이브, 디스크, 테이프, DVD/CD-ROM 드라이브, 메모리 카드 등의 컴퓨터에서 판독 가능한 기록매체를 포함할 수 있다. 다른 실시예에서 소프트웨어 구성요소들은 컴퓨터에서 판독 가능한 기록매체가 아닌 통신 인터페이스(630)를 통해 메모리(610)에 로딩될 수도 있다. 예를

들어, 소프트웨어 구성요소들은 네트워크(540)를 통해 수신되는 파일들에 의해 설치되는 컴퓨터 프로그램에 기반하여 컴퓨터 장치(600)의 메모리(610)에 로딩될 수 있다.

[0167] 프로세서(620)는 기본적인 산술, 로직 및 입출력 연산을 수행함으로써, 컴퓨터 프로그램의 명령을 처리하도록 구성될 수 있다. 명령은 메모리(610) 또는 통신 인터페이스(630)에 의해 프로세서(620)로 제공될 수 있다. 예를 들어 프로세서(620)는 메모리(610)와 같은 기록 장치에 저장된 프로그램 코드에 따라 수신되는 명령을 실행하도록 구성될 수 있다.

[0168] 통신 인터페이스(630)은 네트워크(540)를 통해 컴퓨터 장치(600)가 다른 장치(일례로, 앞서 설명한 저장 장치들)와 서로 통신하기 위한 기능을 제공할 수 있다. 일례로, 컴퓨터 장치(600)의 프로세서(620)가 메모리(610)와 같은 기록 장치에 저장된 프로그램 코드에 따라 생성한 요청이나 명령, 데이터, 파일 등이 통신 인터페이스(630)의 제어에 따라 네트워크(540)를 통해 다른 장치들로 전달될 수 있다. 역으로, 다른 장치로부터의 신호나 명령, 데이터, 파일 등이 네트워크(540)를 거쳐 컴퓨터 장치(600)의 통신 인터페이스(630)를 통해 컴퓨터 장치(600)로 수신될 수 있다. 통신 인터페이스(630)를 통해 수신된 신호나 명령, 데이터 등은 프로세서(620)나 메모리(610)로 전달될 수 있고, 파일 등은 컴퓨터 장치(600)가 더 포함할 수 있는 저장 매체(상술한 영구 저장 장치)로 저장될 수 있다.

[0169] 입출력 인터페이스(640)는 입출력 장치(650)와의 인터페이스를 위한 수단일 수 있다. 예를 들어, 입력 장치는 마이크, 키보드 또는 마우스 등의 장치를, 그리고 출력 장치는 디스플레이, 스피커와 같은 장치를 포함할 수 있다. 다른 예로 입출력 인터페이스(640)는 터치스크린과 같이 입력과 출력을 위한 기능이 하나로 통합된 장치와의 인터페이스를 위한 수단일 수도 있다. 입출력 장치(650)는 컴퓨터 장치(600)와 하나의 장치로 구성될 수도 있다.

[0170] 또한, 다른 실시예들에서 컴퓨터 장치(600)는 도 6의 구성요소들보다 더 적은 혹은 더 많은 구성요소들을 포함할 수도 있다. 그러나, 대부분의 종래기술적 구성요소들을 명확하게 도시할 필요성은 없다. 예를 들어, 컴퓨터 장치(600)는 상술한 입출력 장치(650) 중 적어도 일부를 포함하도록 구현되거나 또는 트랜시버(transceiver), 데이터베이스 등과 같은 다른 구성요소들을 더 포함할 수도 있다.

[0171] 도 7은 본 발명의 일실시예에 있어서, 서명 방법의 예를 도시한 흐름도이다. 본 실시예에 따른 서명 방법은 일례로 앞서 설명한 서명자의 단말을 구현하는 컴퓨터 장치(600)에 의해 수행될 수 있다. 예를 들어, 컴퓨터 장치(600)의 프로세서(620)는 메모리(610)가 포함하는 운영체제의 코드나 적어도 하나의 프로그램의 코드에 따른 제어 명령(instruction)을 실행하도록 구현될 수 있다. 여기서, 프로세서(620)는 컴퓨터 장치(600)에 저장된 코드가 제공하는 제어 명령에 따라 컴퓨터 장치(600)가 도 7의 방법이 포함하는 단계들(710 내지 730)을 수행하도록 컴퓨터 장치(600)를 제어할 수 있다.

[0172] 단계(710)에서 컴퓨터 장치(600)는 입장하고자 하는 복수의 사용자들에 대해 실명으로 신원이 인증된 네트워크상의 합병자 노드로부터 네트워크를 통해 상기 합병자 노드가 생성한 거래 블록에 대한 서명 요청을 수신할 수 있다. 여기서, 컴퓨터 장치(600)는 복수의 사용자들 중 서명자로서 선택된 사용자의 단말에 대응할 수 있으며, 합병자 노드 역시 복수의 사용자들 중 합병자로 선택된 사용자의 단말에 대응할 수 있다. 이때, 서명 요청은 해시 값에 기초하여 선택되는 네트워크상의 서명자 노드들에게 합병자 노드에 의해 전송될 수 있으며, 여기서 해시 값은 서명된 블록 체인의 마지막 거래 블록이 포함하는 거래들에 대한 정보들을 입력으로 가지면서 임의적(random)이어서 예측 불가능하지만 결정적(deterministic)이어서 입력에 따라 출력이 결정되는 함수를 통해 출력될 수 있다.

[0173] 단계(720)에서 컴퓨터 장치(600)는 서명 요청된 거래 블록의 유효성을 확인할 수 있다. 서명자가 거래 블록의 유효성을 확인하는 과정에 대해서는 앞서 여러 번 설명하였기에 반복적인 설명은 생략한다.

[0174] 단계(730)에서 컴퓨터 장치(600)는 유효성이 확인된 거래 블록에 서명할 수 있다. 이때, 컴퓨터 장치(600)는 서명된 거래 블록을 합병자 노드로 전송할 수 있다. 합병자 노드에서의 동작에 대해서는 도 8을 통해 설명한다.

[0175] 도 8은 본 발명의 일실시예에 있어서, 거래 블록 추가 방법의 예를 도시한 흐름도이다. 본 실시예에 따른 거래 블록 추가 방법은 일례로 앞서 설명한 합병자의 단말을 구현하는 컴퓨터 장치(600)에 의해 수행될 수 있다. 예를 들어, 컴퓨터 장치(600)의 프로세서(620)는 메모리(610)가 포함하는 운영체제의 코드나 적어도 하나의 프로그램의 코드에 따른 제어 명령(instruction)을 실행하도록 구현될 수 있다. 여기서, 프로세서(620)는 컴퓨터 장치(600)에 저장된 코드가 제공하는 제어 명령에 따라 컴퓨터 장치(600)가 도 8의 방법이 포함하는 단계들(810

내지 850)을 수행하도록 컴퓨터 장치(600)를 제어할 수 있다.

[0176] 단계(810)에서 컴퓨터 장치(600)는 입장하고자 하는 복수의 사용자들에 대해 실명으로 신원이 인증된 네트워크를 통해 사용자들간의 거래에 대한 정보를 수집할 수 있다. 예를 들어, 거래가 사용자 A에서 사용자 B로 발생할 때, 금액의 양, 날짜/시간, 거래 목적 및 그들(사용자 A와 사용자 B)의 ID들을 포함하는 거래 기록은 사용자 A의 개인 서명 키 및 사용자 B의 개인 서명 키를 이용하여 서명되고 사용자 A와 사용자 B 중 어느 하나(송신자)에 의해 합병자들로 보내질 수 있다. 본 실시예에서 컴퓨터 장치(600)는 이러한 합병자들 중 하나의 단말일 수 있으며, 단계(810)에서와 같이 사용자들간의 거래에 대한 정보를 수집할 수 있다.

[0177] 단계(820)에서 컴퓨터 장치(600)는 수집된 거래에 대한 정보를 병합하여 거래 블록을 생성할 수 있다. 거래 블록은 적어도 하나의 송신자로부터 수신되는 거래에 대한 정보(앞선 예에서의 거래 기록)를 포함할 수 있다.

[0178] 단계(830)에서 컴퓨터 장치(600)는 생성된 거래 블록을 위한 서명자들을 생성된 거래 블록이 포함하는 거래에 대한 이해관계와 무관하게, 서명된 블록 체인의 완성된 마지막 블록의 거래에 기반하여 선택할 수 있다. 일례로, 도 3에서는 새로운 블록(111)의 종전 블록(112)이 포함하는 거래들(310, 320, 330)을 입력 파라미터로 갖는 해시 함수를 이용하여 계산되는 해시 값을 통해 새로운 블록(111)을 위한 서명자들(370)이 선택되는 예를 설명한 바 있다.

[0179] 단계(840)에서 컴퓨터 장치(600)는 선택된 서명자들의 생성된 거래 블록에 대한 서명을 요청할 수 있다. 이때, 서명자들 각각은 도 7을 통해 설명한 단계들(710 내지 730)을 통해 서명 요청을 수신하고, 거래 블록에 대한 유효성을 확인하여 유효한 거래 블록에 서명을 하여 도 8의 실시예에 따른 컴퓨터 장치(600)인 합병자 노드로 전송할 수 있다.

[0180] 단계(850)에서 컴퓨터 장치(600)는 서명자들로부터 서명된 거래 블록을 서명된 블록 체인에 추가시키기 위해, 서명된 거래 블록을 네트워크상의 복수의 합병자 노드들로 전송할 수 있다. 이때, 이미 설명한 바와 같이, 복수의 합병자 노드들 각각은 서명된 거래 블록의 유효성을 확인하고 유효성이 확인된 서명된 거래 블록을 서명된 블록 체인으로의 추가를 승인할 수 있다. 이 경우, 앞서 설명한 바와 같이 거래 블록을 지원하는 사람들의 누적된 수(서명 수)가 가장 많은 거래 블록의 추가를 승인하거나 또는 유효성이 확인된 거래 블록들이 추가된 새로운 블록 체인들 중 거래 블록을 지원하는 사람들의 누적된 수(서명 수)가 가장 많은 거래 블록이 추가된 블록 체인을 선택할 수 있다.

[0181] 도 5 내지 도 8에서 생략된 내용들은 그 앞의 설명들을 참고할 수 있으며, 이러한 네트워크 시스템이나 서명 방법 및 거래 블록 생성 방법이 갖는 효과들에 대해서도 앞서 자세히 설명한 바 있다.

[0182] 이상에서 설명된 시스템 또는 장치는 하드웨어 구성요소, 소프트웨어 구성요소 또는 하드웨어 구성요소 및 소프트웨어 구성요소의 조합으로 구현될 수 있다. 예를 들어, 실시예들에서 설명된 장치 및 구성요소는, 예를 들어, 프로세서, 콘트롤러, ALU(arithmetic logic unit), 디지털 신호 프로세서(digital signal processor), 마이크로컴퓨터, FPGA(field programmable gate array), PLU(programmable logic unit), 마이크로프로세서, 또는 명령(instruction)을 실행하고 응답할 수 있는 다른 어떠한 장치와 같이, 하나 이상의 범용 컴퓨터 또는 특수 목적 컴퓨터를 이용하여 구현될 수 있다. 처리 장치는 운영 체제(OS) 및 상기 운영 체제 상에서 수행되는 하나 이상의 소프트웨어 어플리케이션을 수행할 수 있다. 또한, 처리 장치는 소프트웨어의 실행에 응답하여, 데이터를 접근, 저장, 조작, 처리 및 생성할 수도 있다. 이해의 편의를 위하여, 처리 장치는 하나가 사용되는 것으로 설명된 경우도 있지만, 해당 기술분야에서 통상의 지식을 가진 자는, 처리 장치가 복수 개의 처리 요소(processing element) 및/또는 복수 유형의 처리 요소를 포함할 수 있음을 알 수 있다. 예를 들어, 처리 장치는 복수 개의 프로세서 또는 하나의 프로세서 및 하나의 콘트롤러를 포함할 수 있다. 또한, 병렬 프로세서(parallel processor)와 같은, 다른 처리 구성(processing configuration)도 가능하다.

[0183] 소프트웨어는 컴퓨터 프로그램(computer program), 코드(code), 명령(instruction), 또는 이들 중 하나 이상의 조합을 포함할 수 있으며, 원하는 대로 동작하도록 처리 장치를 구성하거나 독립적으로 또는 결합적으로(collectively) 처리 장치를 명령할 수 있다. 소프트웨어 및/또는 데이터는, 처리 장치에 의하여 해석되거나 처리 장치에 명령 또는 데이터를 제공하기 위하여, 어떤 유형의 기계, 구성요소(component), 물리적 장치, 가상 장치(virtual equipment), 컴퓨터 저장 매체 또는 장치에 구체화(embody)될 수 있다. 소프트웨어는 네트워크로 연결된 컴퓨터 시스템 상에 분산되어서, 분산된 방법으로 저장되거나 실행될 수도 있다. 소프트웨어 및 데이터는 하나 이상의 컴퓨터 판독 가능 기록매체에 저장될 수 있다.

[0184] 실시예에 따른 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판

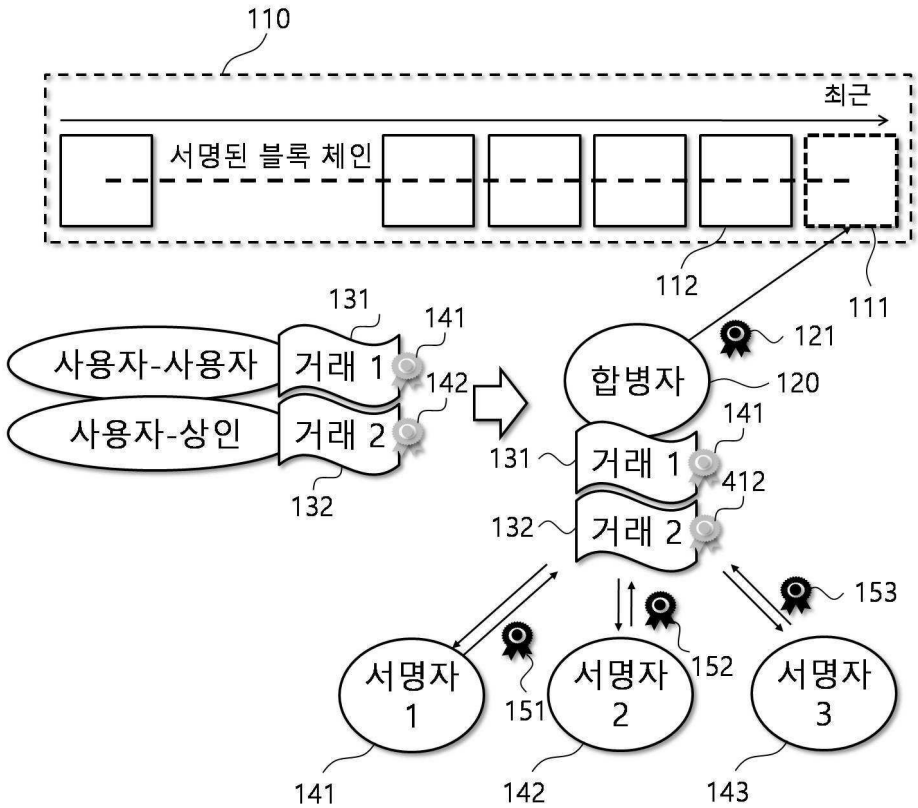
독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 실시예를 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 통상의 기술자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 이러한 기록매체는 단일 또는 수개 하드웨어가 결합된 형태의 다양한 기록수단 또는 저장수단일 수 있으며, 어떤 컴퓨터 시스템에 직접 접속되는 매체에 한정되지 않고, 네트워크 상에 분산 존재하는 것일 수도 있다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다.

[0185] 이상과 같이 실시예들이 비록 한정된 실시예와 도면에 의해 설명되었으나, 해당 기술분야에서 통상의 지식을 가진 자라면 상기의 기재로부터 다양한 수정 및 변형이 가능하다. 예를 들어, 설명된 기술들이 설명된 방법과 다른 순서로 수행되거나, 및/또는 설명된 시스템, 구조, 장치, 회로 등의 구성요소들이 설명된 방법과 다른 형태로 결합 또는 조합되거나, 다른 구성요소 또는 균등물에 의하여 대치되거나 치환되더라도 적절한 결과가 달성될 수 있다.

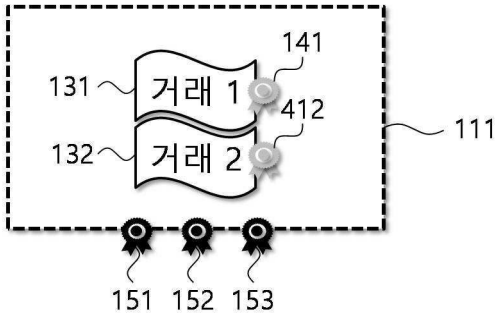
[0186] 그러므로, 다른 구현들, 다른 실시예들 및 청구범위와 균등한 것들도 후술하는 청구범위의 범위에 속한다.

도면

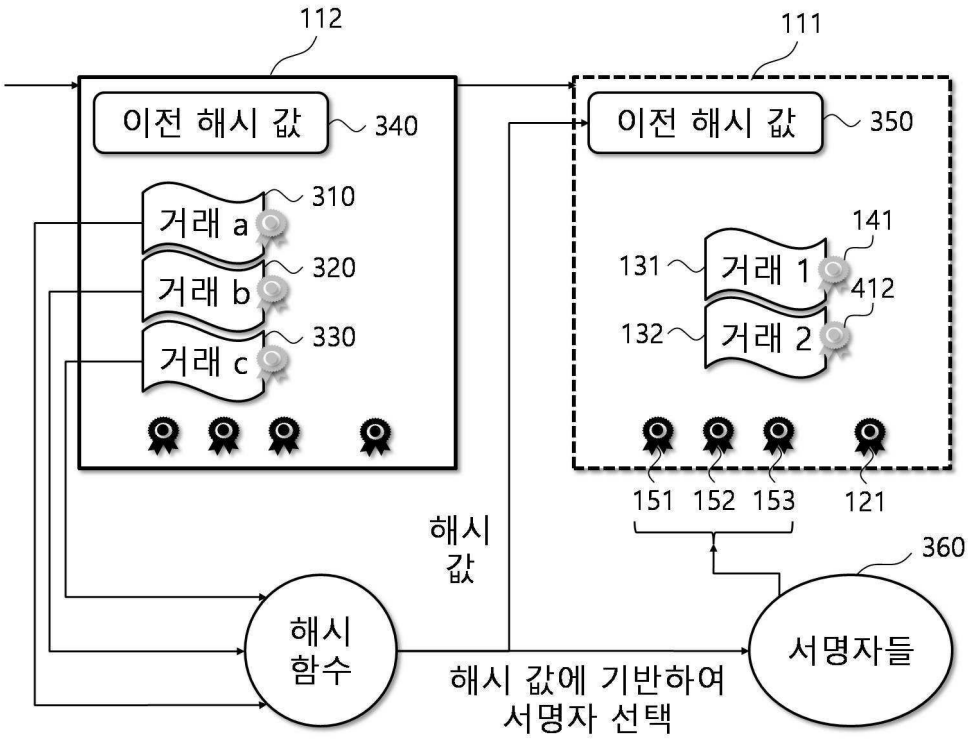
도면1



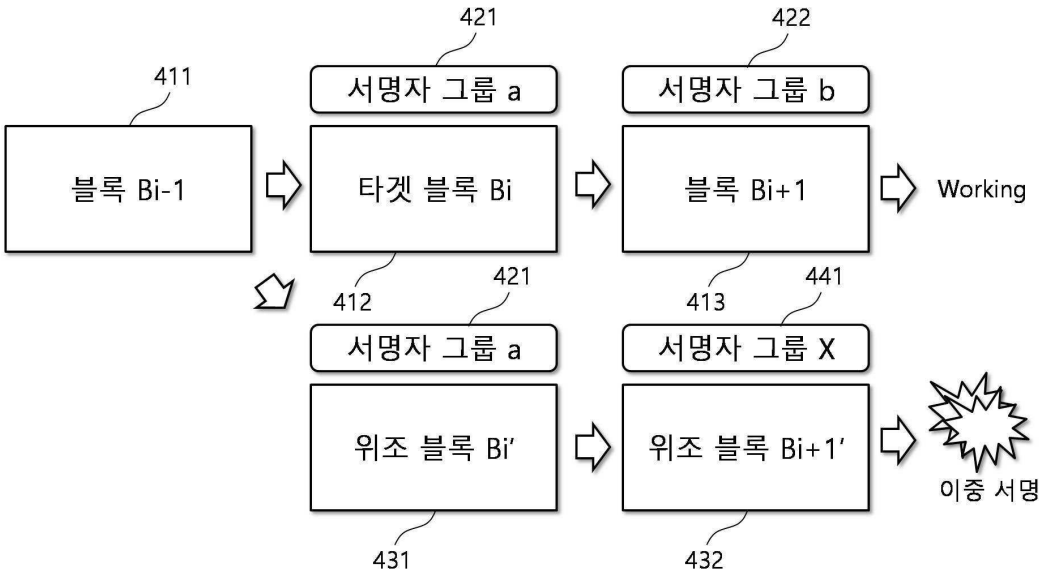
도면2


141
131
거래 1
412
111
132
거래 2
151
152
153

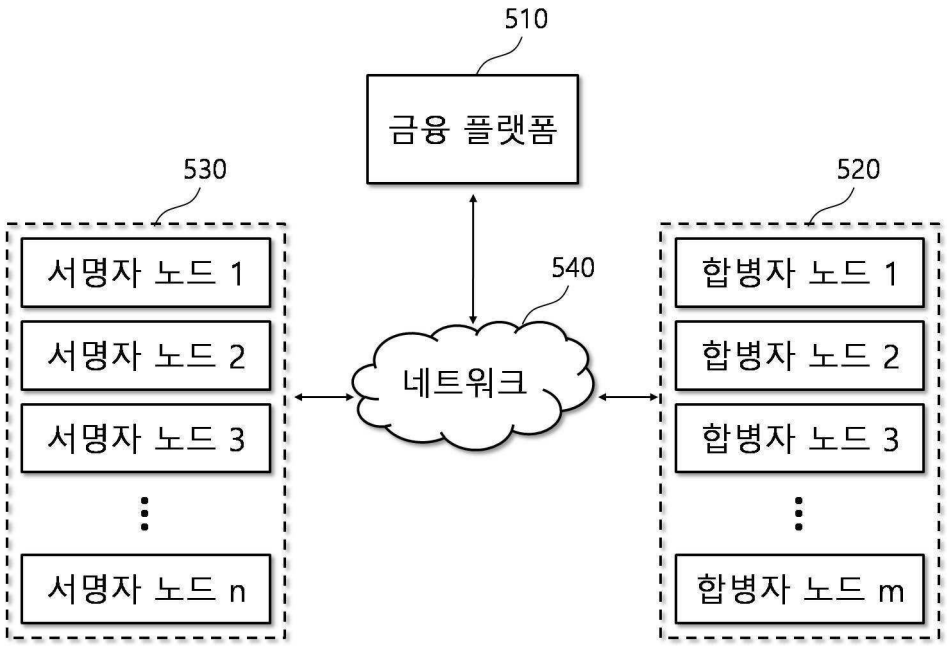
도면3


112
111
이전 해시 값
340
이전 해시 값
350
310
거래 a
320
거래 b
330
거래 c
141
131
거래 1
412
132
거래 2
151
152
153
121
해시
값
360
해시
함수
서명자들
해시 값에 기반하여
서명자 선택

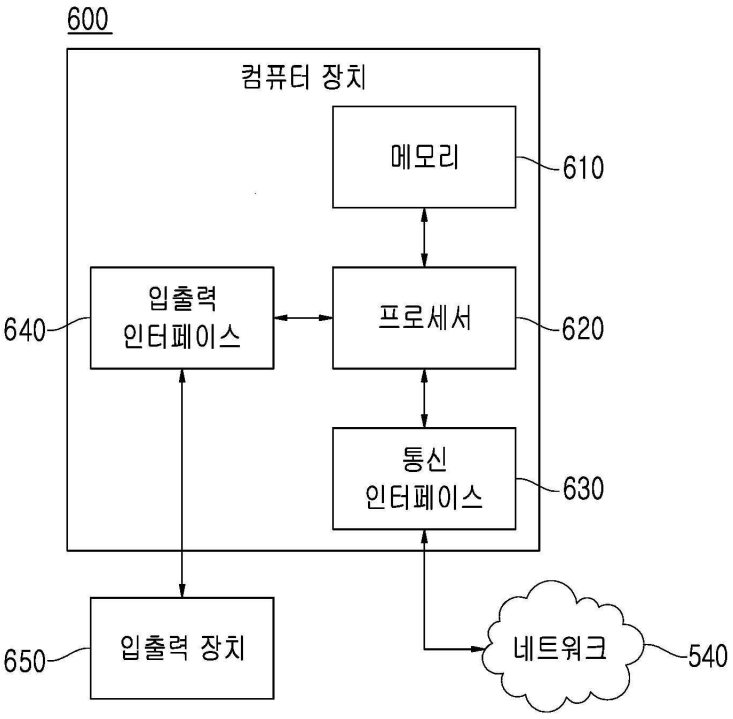
도면4


421
422
411
서명자 그룹 a
서명자 그룹 b
블록 Bi-1
타겟 블록 Bi
블록 Bi+1
Working
412
421
413
441
서명자 그룹 a
서명자 그룹 X
위조 블록 Bi'
위조 블록 Bi+1'
이중 서명
431
432

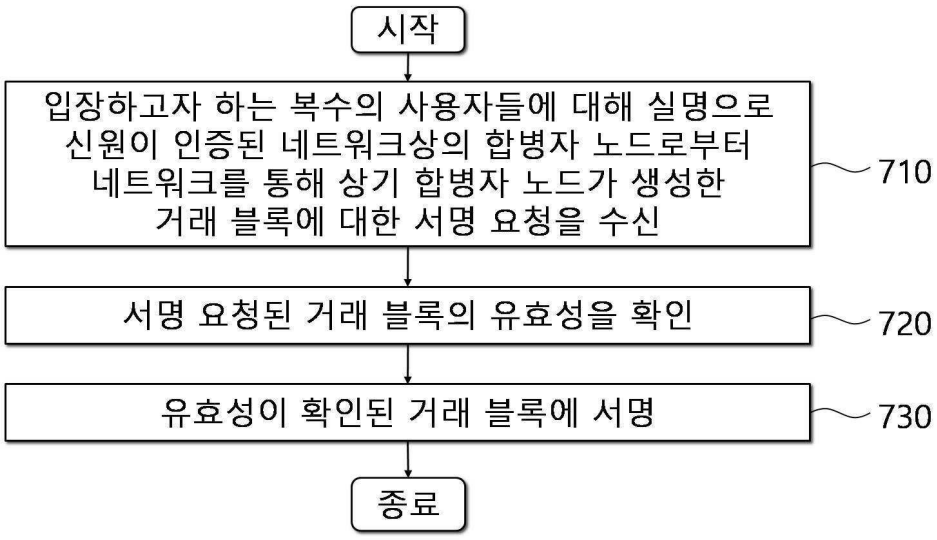
도면5


510
금융 플랫폼
530
520
540
서명자 노드 1
서명자 노드 2
서명자 노드 3
서명자 노드 n
네트워크
합병자 노드 1
합병자 노드 2
합병자 노드 3
합병자 노드 m

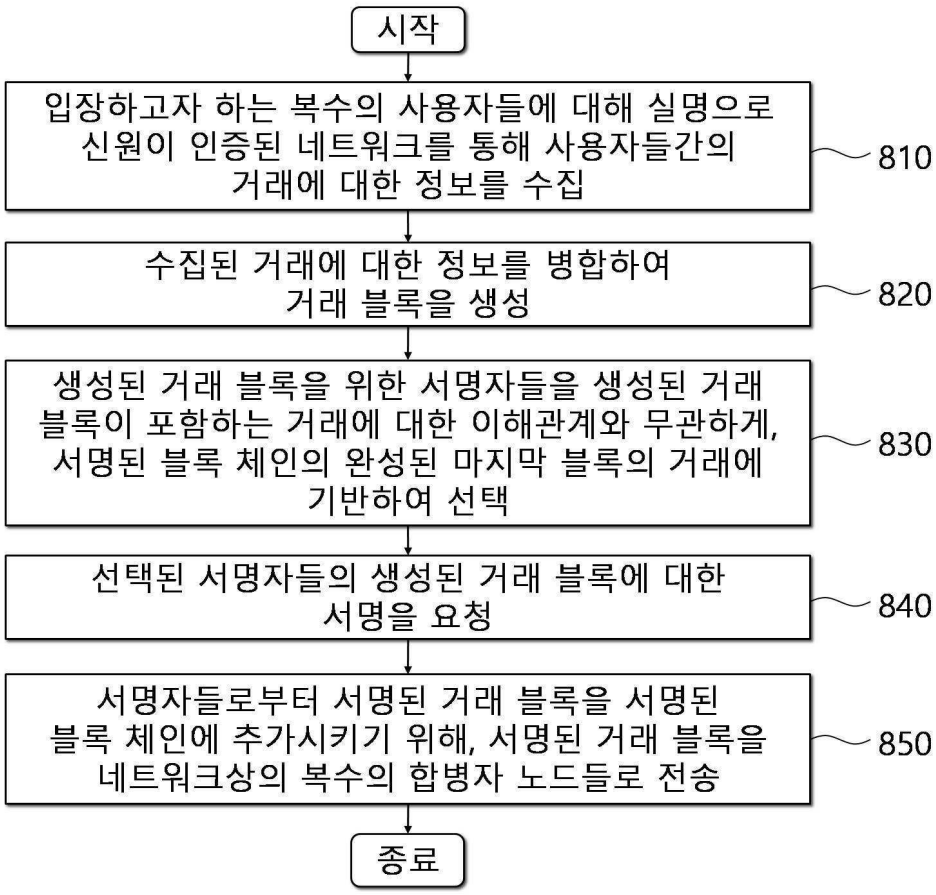
도면6


600
컴퓨터 장치
메모리
610
입출력
인터페이스
640
프로세서
620
통신
인터페이스
630
650
입출력 장치
네트워크
540

도면7


시작
입장하고자 하는 복수의 사용자들에 대해 실명으로 신원이 인증된 네트워크상의 합병자 노드로부터 네트워크를 통해 상기 합병자 노드가 생성한 거래 블록에 대한 서명 요청을 수신
710
서명 요청된 거래 블록의 유효성을 확인
720
유효성이 확인된 거래 블록에 서명
730
종료

도면8


시작
입장하고자 하는 복수의 사용자들에 대해 실명으로 신원이 인증된 네트워크를 통해 사용자들간의 거래에 대한 정보를 수집
810
수집된 거래에 대한 정보를 병합하여 거래 블록을 생성
820
생성된 거래 블록을 위한 서명자들을 생성된 거래 블록이 포함하는 거래에 대한 이해관계와 무관하게, 서명된 블록 체인의 완성된 마지막 블록의 거래에 기반하여 선택
830
선택된 서명자들의 생성된 거래 블록에 대한 서명을 요청
840
서명자들로부터 서명된 거래 블록을 서명된 블록 체인에 추가시키기 위해, 서명된 거래 블록을 네트워크상의 복수의 합병자 노드들로 전송
850
종료