(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2019-0058255
(43) 공개일자 2019년05월29일

(51) 국제특허분류(Int. Cl.)
G06Q 20/36 (2012.01) *G06Q 20/06* (2012.01)
G06Q 20/38 (2012.01)
(52) CPC특허분류
G06Q 20/3678 (2013.01)
G06Q 20/065 (2013.01)
(21) 출원번호 10-2018-0064368
(22) 출원일자 2018년06월04일
심사청구일자 2018년06월04일
(30) 우선권주장
1020170154923 2017년11월20일 대한민국(KR)

(71) 출원인
충남대학교산학협력단
대전광역시 유성구 대학로 99 (궁동, 충남대학교)
(72) 발명자
최훈
대전광역시 서구 만년로 25, 104동 503호 (만년동, 강변아파트)
김민호
전라북도 전주시 덕진구 신복5길 13-1, 201호 (팔복동1가)
김수진
경기도 평택시 중앙2로 94, 208동 606호 (합정동, 주공아파트)
(74) 대리인
유미특허법인

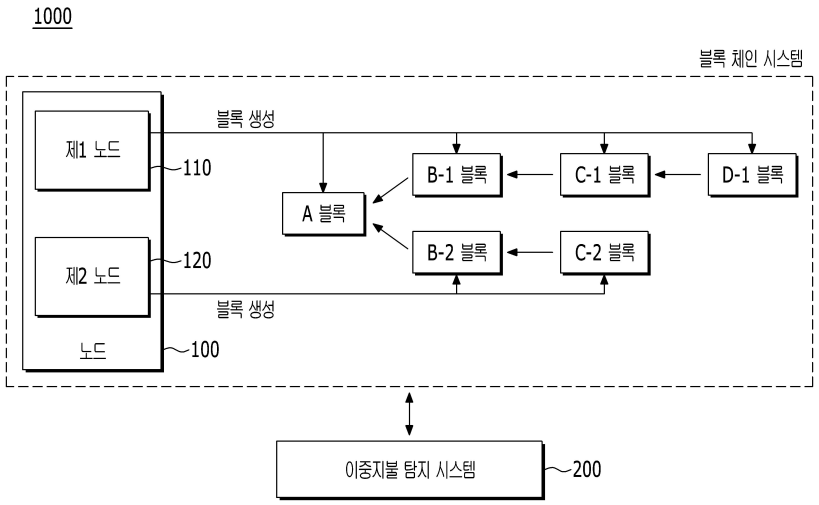
전체 청구항 수 : 총 10 항

(54) 발명의 명칭 **블록체인 이중지불 탐지 시스템 및 방법**

(57) 요 약

블록체인에 발생한 이중지불을 탐지하는 시스템으로서, 블록체인을 구성하는 복수의 블록들의 구조를 분석하여, 상기 블록체인 내에 발생한 분기점을 검색하는 분기점 검색부, 분기점이 검색된 경우, 상기 검색된 분기점을 형성하는 제1 블록 및 제2 블록을 결정하는 블록 결정부, 상기 제1 블록 및 상기 제2 블록에 포함된 거래정보들을 상호 비교하여, 상기 블록체인에 이중지불이 발생하였는지 결정하는 이중지불 발생 결정부 그리고 상기 블록체인에 이중지불이 발생한 경우, 상기 블록체인을 구성하는 복수의 블록들을 공유하는 노드들에 경고메시지를 전송하는 경고메시지 전송부를 포함한다.

대 표 도



(52) CPC특허분류
G06Q 20/382 (2013.01)

이 발명을 지원한 국가연구개발사업
과제고유번호 2015-0-00930
부처명 과학기술정보통신부
연구관리전문기관 정보통신기술진흥센터
연구사업명 SW전문인력양성/정보통신창의인재양성
연구과제명 2018년 SW중심대학 지원사업_충남대
기 여 율 1/1
주관기관 충남대학교 산학협력단
연구기간 2018.01.01 ~ 2018.12.31

명 세 서

청구범위

청구항 1

블록체인에 발생한 이중지불을 탐지하는 시스템으로서,

블록체인을 구성하는 복수의 블록들의 구조를 분석하여, 상기 블록체인 내에 발생한 분기점을 검색하는 분기점 검색부,

분기점이 검색된 경우, 상기 검색된 분기점을 형성하는 제1 블록 및 제2 블록을 결정하는 블록 결정부, 그리고

상기 제1 블록 및 상기 제2 블록에 포함된 거래정보들을 상호 비교하여, 상기 블록체인에 이중지불이 발생하였는지 결정하는 이중지불 발생 결정부

를 포함하는 이중지불 탐지 시스템.

청구항 2

제1항에서,

상기 이중지불 발생 결정부는

상기 제1 블록에 포함된 거래정보들과 상기 제2 블록에 포함된 거래정보들을 상호 비교하여 이전 거래정보가 동일하나 현재 거래정보가 상이한 제1 이중지불 거래정보들이 존재하는지 결정하고, 상기 제1 이중지불 거래정보들이 존재하는지에 따라 상기 블록체인 내에서 이중지불이 발생하였는지를 결정하는 이중지불 탐지 시스템.

청구항 3

제2항에서,

상기 이중지불 발생 결정부는

상기 제1 블록 및 상기 제2 블록에 포함된 거래정보들 중 이전 거래정보를 포함하지 않는 최초 거래정보를 제외하고, 상기 제1 블록에 포함된 거래정보들과 상기 제2 블록에 포함된 거래정보들을 상호 비교하는 이중지불 탐지 시스템.

청구항 4

제2항에서,

상기 이중지불 발생 결정부는

상기 제1 이중지불 거래정보들이 존재하는 경우, 상기 블록체인 내에서 이중지불이 발생하였다고 결정하고,

상기 제1 이중지불 거래정보들이 존재하지 않는 경우, 상기 제1 블록의 자식 블록인 제3 블록에 포함된 거래정보들과 상기 제2 블록의 자식 블록인 제4 블록에 포함된 거래정보들을 상호 비교하여, 이전 거래정보가 동일하나 현재 거래정보가 상이한 제2 이중지불 거래정보들이 존재하는지 결정하고, 상기 제2 이중지불 거래정보들이 존재하는지에 따라 상기 블록체인 내에서 이중지불이 발생하였는지를 결정하는 이중지불 탐지 시스템.

청구항 5

제1항에서,

상기 블록체인에 이중지불이 발생한 경우, 상기 블록체인을 구성하는 복수의 블록들을 공유하는 노드들에 경고 메시지를 전송하는 경고메시지 전송부

를 더 포함하는 이중지불 탐지 시스템.

청구항 6

복수의 블록들로 구성된 블록체인에 발생한 이중지불을 탐지하는 방법으로서,

블록체인 내에 분기점이 발생된 경우, 상기 발생된 분기점을 형성하는 제1 블록 및 제2 블록을 결정하는 단계,

상기 제1 블록 및 상기 제2 블록에 포함된 거래정보들을 추출하는 단계, 그리고

상기 추출한 거래정보들을 상호 비교하여, 상기 블록체인에 이중지불이 발생하였는지를 결정하는 단계

를 포함하는 이중지불 탐지 방법.

청구항 7

제6항에서,

상기 이중지불이 발생하였는지를 결정하는 단계는

상기 제1 블록에 포함된 거래정보들과 상기 제2 블록에 포함된 거래정보들을 상호 비교하여, 이전 거래정보가 동일하나 현재 거래정보가 상이한 제1 이중지불 거래정보들이 존재하는지 결정하는 단계, 그리고

상기 제1 이중지불 거래정보들이 존재하는지에 따라, 상기 블록체인 내에서 이중지불이 발생하였는지를 결정하는 단계

를 포함하는 이중지불 탐지 방법.

청구항 8

제7항에서,

상기 제1 이중지불 거래정보들이 존재하는지에 따라, 상기 블록체인 내에서 이중지불이 발생하였는지를 결정하는 단계는

상기 제1 이중지불 거래정보들이 존재하는 경우, 상기 블록체인 내에서 이중지불이 발생하였다고 결정하고,

상기 제1 이중지불 거래정보들이 존재하지 않는 경우, 상기 제1 블록의 자식 블록인 제3 블록과 상기 제2 블록의 자식 블록인 제4 블록을 결정하고, 상기 제3 블록 및 상기 제4 블록에 포함된 거래정보들을 추출하고, 상기 제3 블록에 포함된 거래정보들과 상기 제4 블록에 포함된 거래정보들을 상호 비교하여, 이전 거래정보가 동일하나 현재 거래정보가 상이한 제2 이중지불 거래정보들이 존재하는지 결정하고, 상기 제2 이중지불 거래정보들이 존재하는지에 따라 상기 블록체인 내에서 이중지불이 발생하였는지를 결정하는 이중지불 탐지 방법.

청구항 9

제7항에서,

상기 이중지불이 발생하였는지를 결정하는 단계는

상기 제1 블록 및 상기 제2 블록에 포함된 거래정보들 중 이전 거래정보를 포함하지 않는 최초 거래정보를 결정하는 단계를 더 포함하고,

상기 제1 이중지불 거래정보들이 존재하는지 결정하는 단계는

상기 제1 블록에 포함된 거래정보들과 상기 제2 블록에 포함된 거래정보들 중 상기 최초 거래정보를 제외한 거래정보들을 상호 비교하는 이중지불 탐지 방법.

청구항 10

제6항에서,

상기 블록체인에 이중지불이 발생한 경우, 상기 블록체인을 구성하는 복수의 블록들을 공유하는 노드들에 경고 메시지를 전송하는 단계

를 더 포함하는 이중지불 탐지 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 블록체인에서 이중지불을 탐지하기 위한 시스템 및 방법에 관한 것이다.

배 경 기 술

[0002] 블록체인은 비트코인 전자화폐시스템의 기반이 되는 기술로서, 전자화폐를 통해 거래가 수행된 경우 거래정보가 포함된 블록을 P2P(Peer-to-Peer) 통신 방식을 통해 네트워크에 연결된 모든 노드들에 전파하고, 각 노드들은 수신한 블록을 중복 저장한다. 블록체인을 이용한 전자화폐시스템은 거래내역을 여러 노드들에 분산시켜 저장하기 때문에, 중앙서버에 거래정보가 일괄적으로 저장되는 기존의 전자화폐 방식에 비해 보안을 획기적으로 강화할 수 있다는 장점이 있다.

[0003] 한편, 이러한 장점은 하나의 전자화폐로 반드시 한 번의 거래가 발생해야함을 전제로 한다. 그러나, 비트코인 전자화폐시스템 내에서 조작을 통해 하나의 전자화폐로 두 번 이상의 거래를 발생시킬 수가 있는데, 이를 이중지불이라 하며 불법거래에 해당한다. 시스템에서 이중지불이 발생하는 경우, 정상 거래에 대한 거래정보를 기록한 블록체인과 중복된 지불에 대한 거래정보를 기록한 블록체인이 공존하게 되며, 일정시간 경과 후 중복 지불 여부와 무관하게 길이가 더 긴 블록체인이 채택되고 짧은 것은 무시되어 폐기된다. 그러나, 단순히 길이가 더 긴 블록체인을 선택하는 경우, 중복된 지불에 대한 거래정보를 포함한 체인이 길어질 수 있는 확률이 존재하기 때문에 이중지불을 완벽하게 방지할 수 없다는 문제가 존재할 수 밖에 없다.

[0004] 이와 같은 문제를 해결하기 위해, 전자화폐를 통한 거래 이전에 해당 거래가 합당한지 제3 엔티티를 통해 확인하는 방식이 있었으나, 이러한 방식은 블록체인이 P2P 통신 방식을 사용하는 것과 맞지 않는 접근 방식이라는 문제가 있었다.

발명의 내용

해결하려는 과제

[0005] 본 발명이 해결하고자 하는 과제는 블록에 포함된 거래정보를 통해 블록체인 내에서 발생한 이중지불을 탐색하는 기술을 제공하는 것이다.

[0006] 또한, 본 발명이 해결하고자 하는 과제는 이중지불이 탐색된 경우, 이중지불이 탐색된 노드와 네트워크를 통해 연결된 타 노드들에게 이중지불 발생을 알리는 기술을 제공하는 것이다.

과제의 해결 수단

[0007] 본 발명의 일 실시예에 따른 블록체인에 발생한 이중지불을 탐지하는 시스템은 블록체인을 구성하는 복수의 블록들의 구조를 분석하여, 상기 블록체인 내에 발생한 분기점을 검색하는 분기점 검색부, 분기점이 검색된 경우, 상기 검색된 분기점을 형성하는 제1 블록 및 제2 블록을 결정하는 블록 결정부, 그리고 상기 제1 블록 및 상기 제2 블록에 포함된 거래정보들을 상호 비교하여, 상기 블록체인에 이중지불이 발생하였는지 결정하는 이중지불 발생 결정부를 포함한다.

[0008] 상기 이중지불 발생 결정부는 상기 제1 블록에 포함된 거래정보들과 상기 제2 블록에 포함된 거래정보들을 상호 비교하여 이전 거래정보가 동일하나 현재 거래정보가 상이한 제1 이중지불 거래정보들이 존재하는지 결정하고, 상기 제1 이중지불 거래정보들이 존재하는지에 따라 상기 블록체인 내에서 이중지불이 발생하였는지를 결정한다.

[0009] 상기 이중지불 발생 결정부는 상기 제1 블록 및 상기 제2 블록에 포함된 거래정보들 중 이전 거래정보를 포함하지 않는 최초 거래정보를 제외하고, 상기 제1 블록에 포함된 거래정보들과 상기 제2 블록에 포함된 거래정보들을 상호 비교한다.

[0010] 상기 이중지불 발생 결정부는 상기 제1 이중지불 거래정보들이 존재하는 경우, 상기 블록체인 내에서 이중지불이 발생하였다고 결정하고, 상기 제1 이중지불 거래정보들이 존재하지 않는 경우, 상기 제1 블록의 자식 블록인 제3 블록에 포함된 거래정보들과 상기 제2 블록의 자식 블록인 제4 블록에 포함된 거래정보들을 상호 비교하여, 이전 거래정보가 동일하나 현재 거래정보가 상이한 제2 이중지불 거래정보들이 존재하는지 결정하고, 상기 제2 이중지불 거래정보들이 존재하는지에 따라 상기 블록체인 내에서 이중지불이 발생하였는지를 결정한다.

[0011] 상기 이중지불 탐지 시스템은 상기 블록체인에 이중지불이 발생한 경우, 상기 블록체인을 구성하는 복수의 블록

들을 공유하는 노드들에 경고메시지를 전송하는 경고메시지 전송부를 더 포함한다.

[0012] 본 발명의 일 실시예에 따른 복수의 블록들로 구성된 블록체인에 발생한 이중지불을 탐지하는 방법은 블록체인 내에 분기점이 발생된 경우, 상기 발생된 분기점을 형성하는 제1 블록 및 제2 블록을 결정하는 단계, 상기 제1 블록 및 상기 제2 블록에 포함된 거래정보들을 추출하는 단계, 그리고 상기 추출한 거래정보들을 상호 비교하여, 상기 블록체인에 이중지불이 발생하였는지를 결정하는 단계를 포함한다.

[0013] 상기 이중지불이 발생하였는지를 결정하는 단계는 상기 제1 블록에 포함된 거래정보들과 상기 제2 블록에 포함된 거래정보들을 상호 비교하여, 이전 거래정보가 동일하나 현재 거래정보가 상이한 제1 이중지불 거래정보들이 존재하는지 결정하는 단계, 그리고 상기 제1 이중지불 거래정보들이 존재하는지에 따라, 상기 블록체인 내에서 이중지불이 발생하였는지를 결정하는 단계를 포함한다.

[0014] 상기 제1 이중지불 거래정보들이 존재하는지에 따라, 상기 블록체인 내에서 이중지불이 발생하였는지를 결정하는 단계는 상기 제1 이중지불 거래정보들이 존재하는 경우, 상기 블록체인 내에서 이중지불이 발생하였다고 결정하고, 상기 제1 이중지불 거래정보들이 존재하지 않는 경우, 상기 제1 블록의 자식 블록인 제3 블록과 상기 제2 블록의 자식 블록인 제4 블록을 결정하고, 상기 제3 블록 및 상기 제4 블록에 포함된 거래정보들을 추출하고, 상기 제3 블록에 포함된 거래정보들과 상기 제4 블록에 포함된 거래정보들을 상호 비교하여, 이전 거래정보가 동일하나 현재 거래정보가 상이한 제2 이중지불 거래정보들이 존재하는지 결정하고, 상기 제2 이중지불 거래정보들이 존재하는지에 따라 상기 블록체인 내에서 이중지불이 발생하였는지를 결정한다.

[0015] 상기 이중지불이 발생하였는지를 결정하는 단계는 상기 제1 블록 및 상기 제2 블록에 포함된 거래정보들 중 이전 거래정보를 포함하지 않는 최초 거래정보를 결정하는 단계를 더 포함하고, 상기 제1 이중지불 거래정보들이 존재하는지 결정하는 단계는 상기 제1 블록에 포함된 거래정보들과 상기 제2 블록에 포함된 거래정보들 중 상기 최초 거래정보를 제외한 거래정보들을 상호 비교한다.

[0016] 상기 이중지불 탐지 방법은 상기 블록체인에 이중지불이 발생한 경우, 상기 블록체인을 구성하는 복수의 블록들을 공유하는 노드들에 경고메시지를 전송하는 단계를 더 포함한다.

발명의 효과

[0017] 본 발명에 따르면, 정상거래에 의한 거래정보가 블록에 포함된 후에 이중지불이 발생하는 경우 또는 정상거래에 의해 발생한 거래정보와 이중지불에 의해 발생한 거래정보가 서로 다른 블록에 포함되는 경우라도 블록체인 내 발생한 이중지불을 탐지할 수 있다.

[0018] 또한, 본 발명에 따르면, 이중지불이 발생한 경우 블록체인 시스템 내 모든 노드들에 해당 내용이 전파되는바, 블록체인 시스템에서 빠르게 조치하여 이중지불로 인한 피해를 감소시킬 수 있다.

도면의 간단한 설명

[0019] 도 1 및 도 2는 본 발명의 실시예에 따른 블록체인 이중지불 탐지 시스템이 구현되는 환경을 도시한 도면이다.

도 3은 이중지불 탐지 시스템의 구조를 설명하는 도면이다.

도 4는 블록에 포함된 거래정보들을 이용하여 이중지불 발생여부를 결정하는 방법을 설명하는 도면이다.

도 5는 이중지불 탐지 시스템이 블록체인에 발생한 이중지불을 탐지하는 방법을 설명하는 도면이다.

발명을 실시하기 위한 구체적인 내용

[0020] 아래에서는 첨부한 도면을 참고로 하여 본 발명의 실시예에 대하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시예에 한정되지 않는다. 그리고 도면에서 본 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였으며, 명세서 전체를 통하여 유사한 부분에 대해서는 유사한 도면 부호를 붙였다.

[0021] 명세서 전체에서, 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있는 것을 의미한다.

[0022] 도 1 및 도 2는 본 발명의 실시예에 따른 블록체인 이중지불 탐지 시스템이 구현되는 환경을 도시한 도면이다.

[0023] 도 1을 참고하면, 블록체인 이중지불 탐지 시스템이 구현되는 환경(1000)은 블록체인 시스템을 구성하는 노드들(100) 및 이중지불 탐지 시스템(200)을 포함한다.

[0024] 노드들(100)은 P2P(Peer-to-Peer) 네트워크를 통해 상호 연결되고, 각 노드들(110 및 120)은 전자화폐를 통해 거래가 수행된 경우 거래정보가 포함된 블록을 각각 저장한다.

[0025] 구체적으로, 전자화폐를 통해 거래가 수행된 경우, 제1 노드(110)는 해당 거래와 관련된 거래정보를 수신하고, 해당 거래의 유효성을 검증한 후 유효한 경우 해당 거래정보를 포함하는 A 블록을 생성한다. 이후, 제1 노드(110)는 P2P 네트워크로 연결된 제2 노드(120)로 생성한 A 블록을 전송하며, 제2 노드(120)는 자신의 블록체인에 수신한 A 블록을 저장한다. 이를 통해, 노드들(100)은 동일한 거래정보를 포함하는 블록을 각각 자신의 블록체인에 저장하게 된다.

[0026] 한편, 제2 노드(120)가 이중지불 공격자인 경우, 특정 거래정보를 포함하는 블록이 제1 노드(110) 및 제2 노드(120)에서 동시에 생성될 수 있다. 예를 들면, 제1 노드(110)가 A 블록에 포함된 현재 거래정보를 이전 거래정보로 포함하는 B-1 블록을 생성하였으나, 이중지불 공격자인 제2 노드(120)가 A 블록에 포함된 현재 거래정보를 이전 거래정보로 포함하되, B-1 블록과 다른 현재 거래정보를 가진 B-2 블록을 동시에 생성할 수 있다.

[0027] 이 경우, 제1 노드(110)가 생성한 B-1 블록은 제2 노드(120)로 전송되고, 제2 노드(120)가 생성한 B-2 블록은 제1 노드(110)로 전송되며, 각 노드들(110 및 120)은 수신한 블록을 일단 자신의 블록체인 내 A 블록의 자식 블록으로 연결하는바, 각 노드들(110 및 120)의 블록체인 내에서 이중지불에 따른 분기점이 발생한다.

[0028] 이와 같이, 이중지불이 발생하는 경우 블록체인 내에서 분기점이 발생하므로, 이중지불 탐지 시스템(200)은 블록체인 시스템의 블록체인 내에서 분기점이 발생한 경우, 해당 분기점을 형성하는 블록들을 결정하고, 결정한 블록들에 포함된 거래정보들을 상호 비교하여 블록체인에 이중지불이 발생하였는지를 결정할 수 있다.

[0029] 한편, 도 1에서는 이중지불 탐지 시스템(200)이 블록체인 시스템 내 노드들(100)의 외부에 구현된 독립적인 엔티티로 도시되었으나, 블록체인 시스템 내 각각의 노드 내에 구현될 수도 있다.

[0030] 구체적으로, 도 2를 참고하면, 블록체인 이중지불 탐지 시스템이 구현되는 다른 환경(2000)에서, 제1 이중지불 탐지 시스템(300)은 제1 노드(110) 내에 구현되고 제2 이중지불 탐지 시스템(400)은 제2 노드(120) 내에 구현될 수 있다. 이 경우 제1 노드(110) 및 제2 노드(120)는 각각에 구비된 이중지불 탐지 시스템을 통해 하기 기능을 수행할 수 있다.

[0031] 이하, 이중지불 탐지 시스템(200)이 블록체인에 발생한 이중지불을 탐지하는 기술에 대해 자세히 설명한다.

[0032] 도 3은 이중지불 탐지 시스템의 구조를 설명하는 도면이고, 도 4는 블록에 포함된 거래정보들을 이용하여 이중지불 발생여부를 결정하는 방법을 설명하는 도면이다.

[0033] 도 3을 참고하면, 이중지불 탐지 시스템(200)은 분기점 검색부(210), 블록 결정부(220), 이중지불 발생 결정부(230) 및 경고메시지 전송부(240)를 포함한다.

[0034] 분기점 검색부(210)는 블록체인을 구성하는 복수의 블록들의 구조를 분석하여, 블록체인 내에 발생한 분기점을 검색한다.

[0035] 구체적으로, 분기점 검색부(210)는 블록체인 시스템 내 노드들(100)에 저장된 블록데이터에 접근하여 노드들(100)의 블록체인 구조를 확인하고, 블록체인 구조 내에 동일한 부모 블록에 서로 다른 자식 블록이 연결된 구조가 존재하는지 검색한다.

[0036] 블록 결정부(220)는 분기점이 검색된 경우, 검색된 분기점을 형성하는 제1 블록 및 제2 블록을 결정한다.

[0037] 예를 들면, 도 1에서, 분기점 검색부(210)에 의해 블록체인 내 B-1 블록 및 B-2 블록에 의한 분기점이 검색된 경우, 블록 결정부(220)는 검색된 분기점에 직접 연결된 2 이상의 자식 블록들 즉, B-1 블록 및 B-2 블록을 검색된 분기점을 형성하는 제1 블록 및 제2 블록으로 각각 결정할 수 있다. 한편, 비록 도 1에서는 하나의 부모 블록에 2개의 서로 다른 자식 블록이 연결된 것으로 도시되었으나, 하나의 부모 블록에 3 이상의 서로 다른 자식 블록이 연결될 수도 있다.

[0038] 이중지불 발생 결정부(230)는 제1 블록 및 제2 블록에 포함된 거래정보들을 상호 비교하여, 블록체인에 이중지불이 발생하였는지 결정한다.

[0039] 도 4를 참고하면, 제1 블록 및 제2 블록은 각각 복수의 거래정보들을 포함한다. 상기 설명한 바와 같이, 각각의

거래정보는 전자화폐를 통해 거래가 수행된 경우 발생하고, 블록의 첫번째 거래정보가 아닌 한, 각 거래정보는 현재 수행된 거래에 의해 발생한 현재 거래정보뿐만 아니라, 현재 거래 이전에 발생한 거래에 의해 생성된 이전 거래정보를 포함한다.

[0040] 예를 들면, 제1 블록이 전자화폐를 통한 사용자 A와 사용자 B 사이의 제1 거래 및 제1 거래 이후 발생한 전자화폐를 통한 사용자 B와 사용자 C 사이의 제2 거래에 대한 정보를 포함한다고 가정하면, 제1 블록은 제1 거래에 의해 발생한 제1 거래정보 및 제2 거래에 의해 발생한 제2 거래정보를 포함한다.

[0041] 이 경우, 제1 거래는 제1 블록의 첫번째 거래로서 코인베이스 트랜잭션으로 정의될 수 있으며, 제1 거래정보는 제1 거래에 의해 발생한 거래정보를 현재 거래정보로 포함하되, 첫번째 거래이므로 이전 거래정보를 포함하지 않는다. 반면, 제2 거래정보는 제1 거래에 의해 발생한 거래정보를 이전 거래정보로 포함하고, 제2 거래에 의해 생성된 거래정보를 현재 거래정보로 포함한다.

[0042] 한편, 제1 블록 및 제2 블록에 포함된 거래 정보는 서로 다른 블록에 포함된 거래정보를 이전 거래정보로 포함할 수도 있다.

[0043] 예를 들면, 제1 블록에 포함된 제1 거래정보가 코인베이스 트랜잭션에 의해 발생한 거래정보이고 제2 거래정보가 사용자 A와 사용자 B 사이의 거래에 의해 발생한 거래정보이며, 제2 블록에 포함된 제1 거래정보가 코인베이스 트랜잭션에 의해 발생한 거래정보이고 제2 거래정보가 사용자 B와 사용자 C 사이의 거래에 의해 발생한 거래정보라 할 때, 사용자 B와 사용자 C 사이의 거래 이전에 사용자 A와 사용자 B 사이의 거래가 발생한 경우이므로, 제2 블록의 제2 거래정보는 제1 블록의 제2 거래정보를 이전 거래정보로 포함한다.

[0044] 여기서, 거래정보는 트랜잭션 ID(Transaction Identifier, TXID)를 지칭할 수 있다.

[0045] 우선, 이중지불 발생 결정부(230)는 제1 블록에 포함된 거래정보들과 제2 블록에 포함된 거래정보들을 상호 비교하여 이전 거래정보가 동일하나 현재 거래정보가 상이한 이중지불 거래정보들이 존재하는지 결정한다.

[0046] 이 경우, 이중지불 발생 결정부(230)는 제1 블록 및 제2 블록에 포함된 거래정보들 중 이전 거래정보를 포함하지 않는 최초 거래정보를 제외하고, 제1 블록에 포함된 거래정보들과 제2 블록에 포함된 거래정보들을 상호 비교할 수 있다. 예를 들면, 도 4에서, 이중지불 발생 결정부(230)는 제1 블록에 포함된 제1 거래정보 및 제2 블록에 포함된 제1 거래정보는 이전 거래정보를 포함하지 않는바, 이를 제외한 나머지 거래정보들을 상호 비교할 수 있다.

[0047] 이후, 이중지불 발생 결정부(230)는 이중지불 거래정보들이 존재하는지에 따라 블록체인 내에서 이중지불이 발생하였는지 결정한다.

[0048] 예를 들면, 도 4를 참고하면, 이중지불 발생 결정부(230)는 제1 블록에 포함된 제2 거래정보와 제2 블록에 포함된 제2 거래정보의 이전 거래정보가 "16eab763"으로 동일하고, 현재 거래정보가 각각 "496bac12c" 및 "59b9ea8"로 상이한 경우, 하나의 전자화폐로 2 이상의 거래를 수행 즉, 이중지불이 수행되어 이중지불 거래정보들이 존재하는 경우이므로, 블록체인 내에서 이중지불이 발생한 것으로 결정한다.

[0049] 한편, 도 4와 달리 제1 블록에 포함된 거래정보들과 제2 블록에 포함된 거래정보들을 상호 비교하였으나 이중지불 거래정보들이 존재하지 않는 경우, 이중지불 발생 결정부(230)는 제1 블록의 자식 블록인 제3 블록에 포함된 거래정보와 제2 블록의 자식 블록인 제4 블록에 포함된 거래정보에서 이중지불 거래정보들이 존재할 수 있음을 알리는 플래그를 설정할 수 있다.

[0050] 이후, 이중지불 발생 결정부(230)는 제3 블록에 포함된 거래정보들과 제4 블록에 포함된 거래정보들을 상호 비교하여, 이전 거래정보가 동일하나 현재 거래정보가 상이한 제2 이중지불 거래정보들이 존재하는지 결정하고, 상기 제2 이중지불 거래정보들이 존재하는지에 따라 상기 블록체인 내에서 이중지불이 발생하였는지 결정한다.

[0051] 경고메시지 전송부(240)는 블록체인에 이중지불이 발생한 경우, 블록체인을 구성하는 복수의 블록들을 공유하는 노드들에 경고메시지를 전송한다.

[0052] 구체적으로, 경고메시지 전송부(240)는 블록체인에 이중지불이 발생한 경우 블록체인 시스템 내 노드들(100)에게 경고메시지를 전송할 수 있으며, 만일 이중지불 탐지 시스템(200)이 블록체인 시스템 내 노드 중 하나인 경우 이중지불 탐지 시스템(200)과 P2P 네트워크를 통해 상호 연결된 다른 노드들에게 경고메시지를 전송할 수 있다.

[0053] 도 5는 이중지불 탐지 시스템이 블록체인에 발생한 이중지불을 탐지하는 방법을 설명하는 도면이다.

[0054] 도 5를 참고하면, 이중지불 탐지 시스템(200)은 블록체인을 구성하는 복수의 블록들의 구조를 분석하여, 블록체인 내에 발생한 분기점을 검색한다(S100).

[0055] 예를 들면, 도 1에서, 이중지불 탐지 시스템(200)은 블록체인 시스템을 구성하는 노드들(100)에 접속하여 해당 노드들의 블록체인의 구조를 분석하고, 블록체인 내에 발생한 분기점을 검색할 수 있다.

[0056] 다른 실시예에서, 도 2와 같이 만일 이중지불 탐지 시스템(300 및 400)이 블록체인 시스템 의 노드 내에 구현된 경우, 이중지불 탐지 시스템이 구현된 노드에 저장된 블록체인의 구조를 분석하여, 분기점을 검색할 수 있다.

[0057] 이중지불 탐지 시스템(200)은 블록체인 내에 분기점이 발생된 경우, 발생된 분기점을 형성하는 제1 블록 및 제2 블록을 결정한다(S110).

[0058] 이중지불 탐지 시스템(200)은 제1 블록 및 제2 블록에 포함된 거래정보들을 각각 추출한다(S120).

[0059] 구체적으로, 상기 설명한 바와 같이, 제1 블록 및 제2 블록은 전자화폐를 통해 거래가 수행된 경우 생성된 거래정보를 하나 이상 포함하는바, 이중지불 탐지 시스템(200)은 분기점을 형성하는 복수의 블록들에 포함된 거래정보를 추출한다.

[0060] 이중지불 탐지 시스템(200)은 추출한 거래정보들을 상호 비교하여, 블록체인에 이중지불이 발생하였는지를 결정한다.

[0061] 구체적으로, 이중지불 탐지 시스템(200)은 상기 제1 블록에 포함된 거래정보들과 상기 제2 블록에 포함된 거래정보들을 상호 비교하여, 이전 거래정보가 동일하나 현재 거래정보가 상이한 제1 이중지불 거래정보들이 추출된 거래정보들에 존재하는지 결정한다(S130).

[0062] 이 경우, 이중지불 탐지 시스템(200)은 제1 블록 및 제2 블록에 포함된 거래정보들 중 이전 거래정보를 포함하지 않는 최초 거래정보를 결정하고, 제1 블록에 포함된 거래정보들과 제2 블록에 포함된 거래정보들 중 최초 거래정보를 제외한 거래정보들만을 상호 비교할 수 있다.

[0063] 만일 제1 이중지불 거래정보들이 존재하는 경우 이중지불이 수행된 경우이므로, 이중지불 탐지 시스템(200)은 블록체인 내에서 이중지불이 발생하였다고 결정하고, 블록체인을 구성하는 복수의 블록들을 공유하는 노드들(100)에 경고메시지를 전송한다(S131). 만일 이중지불 탐지 시스템(200)이 블록체인 시스템 내 노드 중 하나인 경우 이중지불 탐지 시스템(200)과 P2P 네트워크를 통해 상호 연결된 다른 노드들에게 경고메시지를 전송할 수 있다.

[0064] 만일 제1 이중지불 거래정보들이 존재하지 않는 경우, 이중지불 탐지 시스템(200)은 제1 블록의 자식 블록인 제3 블록과 제2 블록의 자식 블록인 제4 블록을 결정한다(S140).

[0065] 이중지불 탐지 시스템(200)은 제3 블록 및 제4 블록에 포함된 거래정보들을 각각 추출한다(S150).

[0066] 이중지불 탐지 시스템(200)은 제3 블록에 포함된 거래정보들과 제4 블록에 포함된 거래정보들을 상호 비교하여, 이전 거래정보가 동일하나 현재 거래정보가 상이한 제2 이중지불 거래정보들이 존재하는지 결정하고, 상기 제2 이중지불 거래정보들이 존재하는지에 따라 상기 블록체인 내에서 이중지불이 발생하였는지를 결정한다(S160).

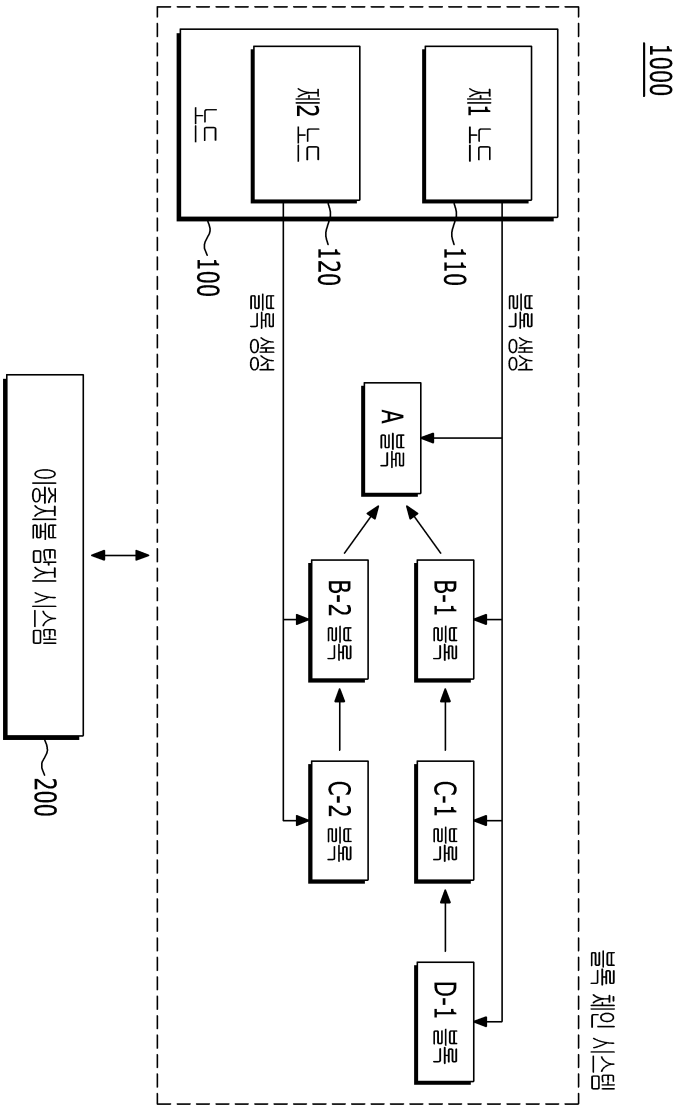
[0067] 본 발명에 따르면, 정상거래에 의한 거래정보가 블록에 포함된 후에 이중지불이 발생하는 경우 또는 정상거래에 의해 발생한 거래정보와 이중지불에 의해 발생한 거래정보가 서로 다른 블록에 포함되는 경우라도 블록체인 내 발생한 이중지불을 탐지할 수 있다.

[0068] 또한, 본 발명에 따르면, 이중지불이 발생한 경우 블록체인 시스템 내 모든 노드들에 해당 내용이 전파되는바, 블록체인 시스템에서 빠르게 조치하여 이중지불로 인한 피해를 감소시킬 수 있다.

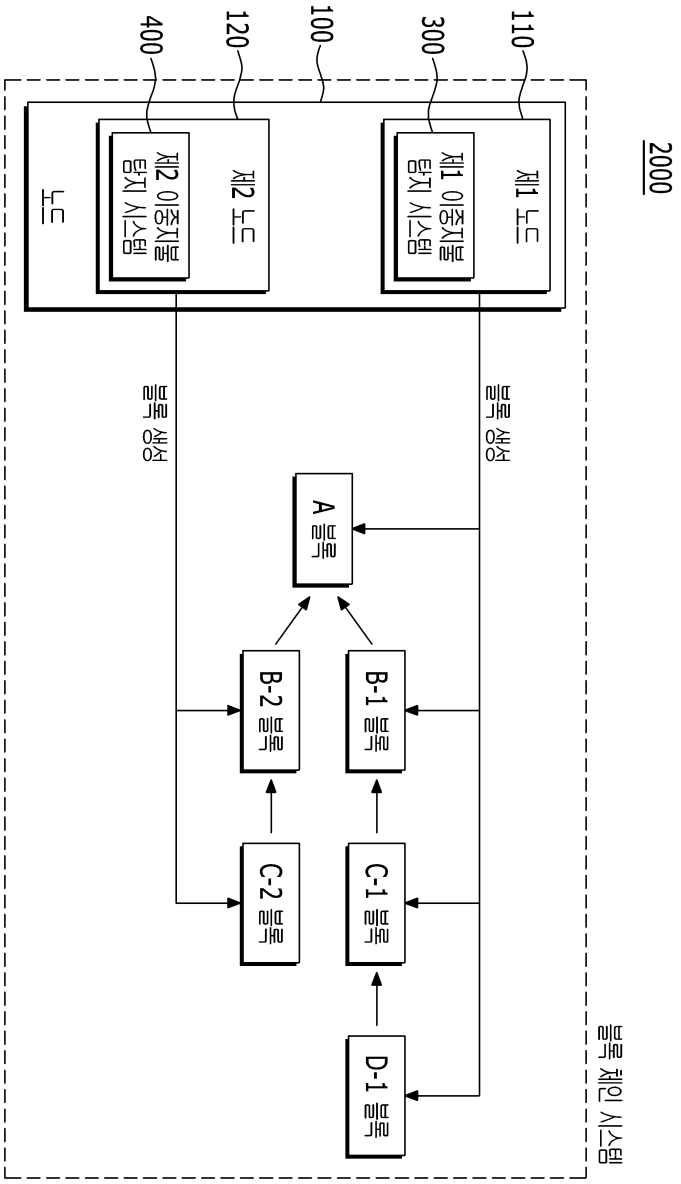
[0069] 이상에서 본 발명의 실시예에 대하여 상세하게 설명하였지만 본 발명의 권리범위는 이에 한정되는 것은 아니고 다음의 청구범위에서 정의하고 있는 본 발명의 기본 개념을 이용한 당업자의 여러 변형 및 개량 형태 또한 본 발명의 권리범위에 속하는 것이다.

도면

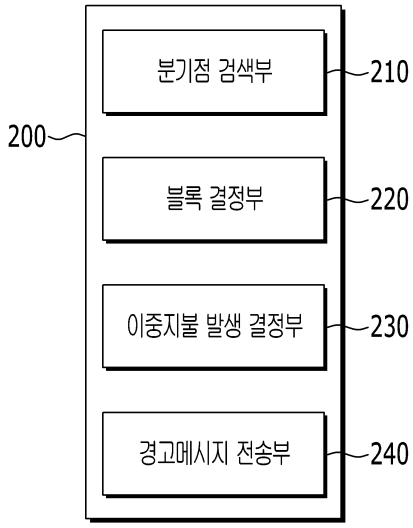
도면1


1000
노드
제1 노드
제2 노드
100
110
120
블록 생성
블록 생성
A 블록
B-1 블록
B-2 블록
C-1 블록
C-2 블록
D-1 블록
블록 체인 시스템
이중지불 탐지 시스템
200

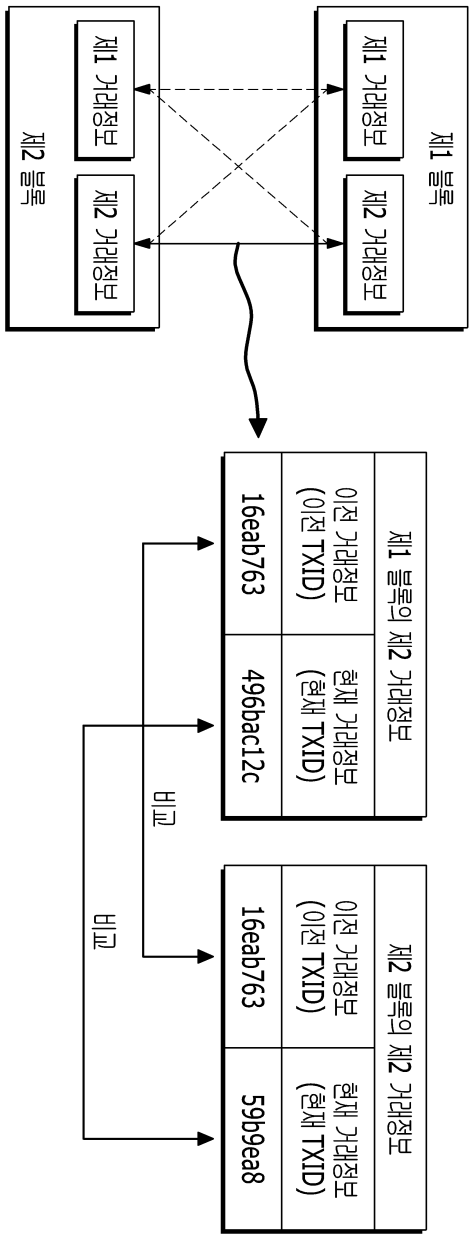
도면2


2000
110
300
100
120
400
노드
제1 노드
제1 이중지불 탐지 시스템
제2 노드
제2 이중지불 탐지 시스템
블록 생성
블록 생성
A 블록
B-1 블록
B-2 블록
C-1 블록
C-2 블록
D-1 블록
블록 체인 시스템

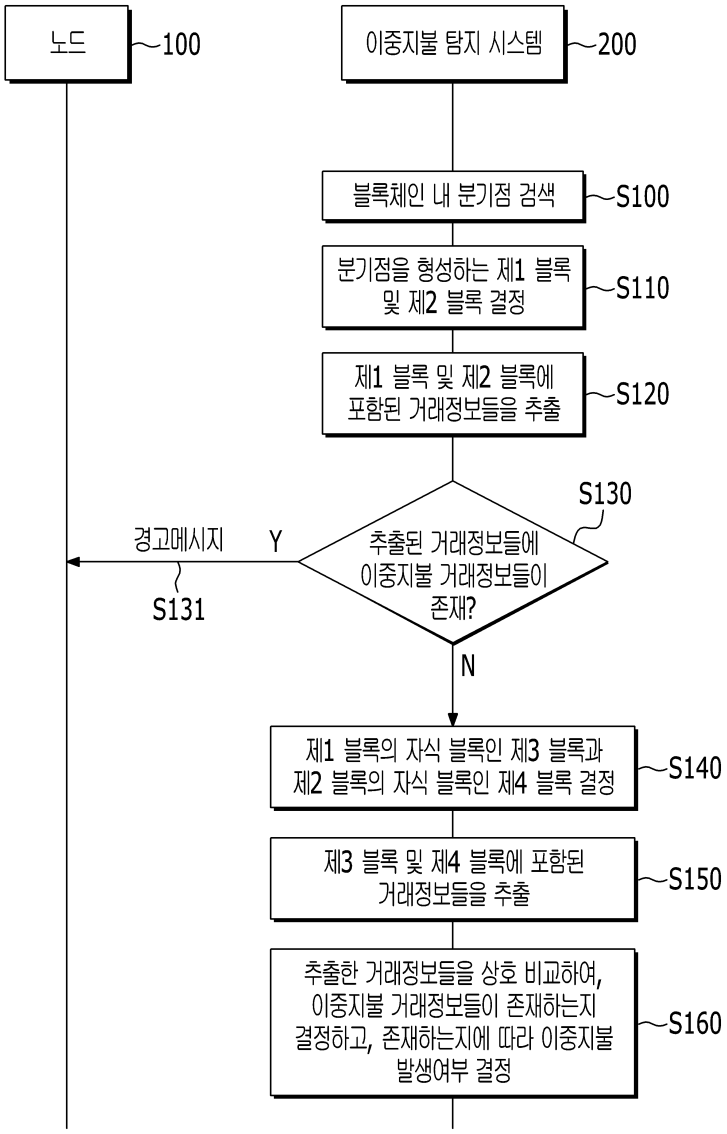
도면3



도면4


제1 블록
제1 거래정보
제2 거래정보
제2 블록
제1 거래정보
제2 거래정보
제1 블록의 제2 거래정보
이전 거래정보 (이전 TXID)
16eab763
현재 거래정보 (현재 TXID)
496bac12c
제2 블록의 제2 거래정보
이전 거래정보 (이전 TXID)
16eab763
현재 거래정보 (현재 TXID)
59b9ea8
비교
비교

도면5


노드
100
이중지불 탐지 시스템
200
블록체인 내 분기점 검색
S100
분기점을 형성하는 제1 블록 및 제2 블록 결정
S110
제1 블록 및 제2 블록에 포함된 거래정보들을 추출
S120
S130
추출된 거래정보들에 이중지불 거래정보들이 존재?
Y
경고메시지
S131
N
제1 블록의 자식 블록인 제3 블록과 제2 블록의 자식 블록인 제4 블록 결정
S140
제3 블록 및 제4 블록에 포함된 거래정보들을 추출
S150
추출한 거래정보들을 상호 비교하여, 이중지불 거래정보들이 존재하는지 결정하고, 존재하는지에 따라 이중지불 발생여부 결정
S160