



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2020-0084162
(43) 공개일자 2020년07월10일

(51) 국제특허분류(Int. Cl.)
G06Q 20/22 (2012.01) G06Q 20/38 (2012.01)
G06Q 40/02 (2012.01) H04L 9/06 (2006.01)
(52) CPC특허분류
G06Q 20/223 (2013.01)
G06Q 20/382 (2013.01)
(21) 출원번호 10-2019-0000224
(22) 출원일자 2019년01월02일
심사청구일자 2019년01월02일

(71) 출원인
서강대학교산학협력단
서울특별시 마포구 백범로 35 (신수동, 서강대학교)
(72) 발명자
장주욱
서울특별시 서대문구 가재울미래로 2, 206동 202호 (남가좌제1동, DMC파크뷰자이)
정준우
서울특별시 금천구 금하로 9길 4-22
최성석
서울특별시 양천구 월정로 9길 20, 203동 104호(신월동, 양천벽산블루밍2단지)
(74) 대리인
이지연

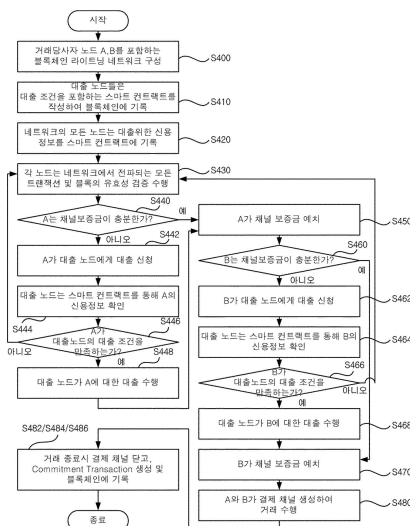
전체 청구항 수 : 총 12 항

(54) 발명의 명칭 **블록체인 라이트닝 네트워크를 기반으로 한 사용자간 거래 활성화를 위한 결제 시스템 및 결제 방법**

(57) 요약

본 발명은 블록체인 라이트닝 네트워크를 기반으로 한 결제 시스템에 관한 것이다. 상기 결제 시스템은, 참여 노드의 요청에 따라, 참여 노드에게 결제 채널 생성을 위한 채널 보증금에 대한 대출을 수행하거나, 결제를 위하여 선지불을 수행해야 되는 참여 노드에게 자본금에 대한 대출을 수행하는 대출 노드;를 구비한다. 상기 참여 노드 중 거래 당사자 노드들은 P2P 거래를 위하여 채널 보증금을 예치하고 P2P 결제 채널을 생성하고, 거래 당사자 노드들은 P2P 결제 채널을 통해 P2P 거래를 수행하거나, 상기 참여 노드들 중 중개 노드들은 결제를 위한 대금에 대한 선지불을 수행한다. 채널 보증금이 부족한 거래 당사자 노드 또는 선지불을 위한 자본금이 부족한 중개 노드는 상기 대출 노드에게 대출 신청하여 대출 노드로부터 채널 보증금 또는 자본을 대출받도록 하여, 사용자간의 거래를 활성화시킬 수 있게 된다.

대표도 - 도2



(52) CPC특허분류

G06Q 40/025 (2013.01)

H04L 9/06 (2013.01)

H04L 2209/56 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호 NRF-2016R1D1A1B01009027

부처명 교육부

연구관리전문기관 한국연구재단

연구사업명 이공학개인지초연구지원사업

연구과제명 블록체인 알고리즘의 개선 및 차세대 활용 기법의 연구

기 여 율 1/1

주관기관 서강대학교

연구기간 2018.03.01 ~ 2019.02.28

명세서

청구범위

청구항 1

다수의 참여 노드들을 구비하는 블록체인 라이트닝 네트워크에서의 결제 시스템에 있어서,

참여 노드의 요청에 따라, 참여 노드에게 결제 채널 생성을 위한 채널 보증금에 대한 대출을 수행하거나, 결제를 위하여 선지불을 수행해야 되는 참여 노드에게 자본금에 대한 대출을 수행하는 대출 노드;를 구비하고,

상기 참여 노드 중 거래 당사자 노드들은 P2P(peer to peer) 거래를 위하여 채널 보증금을 예치하고 P2P(peer to peer) 결제 채널을 생성하고, 거래 당사자 노드들은 P2P 결제 채널을 통해 P2P 거래를 수행하는 것을 특징으로 하며,

채널 보증금이 부족한 거래 당사자 노드는 상기 대출 노드에게 대출 신청하여 대출 노드로부터 채널 보증금을 대출받도록 하여, 사용자간의 거래를 활성화시킬 수 있도록 구성된 것을 특징으로 하는 블록체인 라이트닝 네트워크를 기반으로 한 결제 시스템.

청구항 2

제1항에 있어서, 거래 당사자 노드들이 중개 노드를 통해 P2P 거래하는 경우, 상기 중개 노드는 결제를 위한 대금에 대한 선지불을 수행하는 것을 특징으로 하며,

선지불을 위한 자본이 부족한 노드는 상기 대출 노드에게 대출 신청하여 대출 노드로부터 선지불을 위한 자본을 대출받도록 하여, 사용자간의 거래를 활성화시킬 수 있도록 구성된 것을 특징으로 하는 블록체인 라이트닝 네트워크를 기반으로 한 결제 시스템.

청구항 3

제1항에 있어서, 상기 참여 노드는,

자신의 신용 정보를 포함하는 트랜잭션을 생성하여 스마트 컨트랙트에 업로드하고,

대출이 필요한 경우, 스마트 컨트랙트를 열람하여 스마트 컨트랙트에 기록된 대출 노드의 대출 정보를 확인하고, 차용 노드(Borrower node)로서 대출 노드에게 대출 신청하는 것을 특징으로 하는 블록체인 라이트닝 네트워크를 기반으로 한 결제 시스템.

청구항 4

제1항에 있어서, 상기 대출 노드는,

대출 정보를 포함하는 트랜잭션을 생성하고, 상기 트랜잭션을 포함하는 스마트 컨트랙트를 작성하여 사전 설정된 합의 알고리즘에 따라 블록체인에 기록하고,

차용 노드로부터 대출 신청이 발생하면, 스마트 컨트랙트에 차용 노드에 대한 정보를 요청하고, 스마트 컨트랙트로부터 해당 차용 노드에 대한 정보를 담은 트랜잭션을 열람하고, 대출 노드의 대출 조건과 차용 노드의 신용 정보를 비교하여 확인하고, 차용 노드의 신용 정보가 대출 조건을 충족하는 경우 차용 노드에게 대출을 수행하는 것을 특징으로 하는 블록체인 라이트닝 네트워크를 기반으로 한 결제 시스템.

청구항 5

제1항에 있어서, 상기 대출 노드의 대출 정보는,

대출 조건, 대출 가능 금액, 상환 일자, 대출 이자, 대출 수수료를 포함하는 것을 특징으로 하는 블록체인 라이트닝 네트워크를 기반으로 한 결제 시스템.

청구항 6

제1항에 있어서, 상기 차용 노드의 신용 정보는,

신뢰도, 자본 정보, 대출 기록, 대출 노드와의 홉(Hop) 수를 포함하는 것을 특징으로 하는 블록체인 라이트닝 네트워크를 기반으로 한 결제 시스템.

청구항 7

제1항에 있어서, 상기 거래 당사자 노드들은

채널 보증금을 예치하는 펀딩 트랜잭션(Funding Transaction)을 생성하여 사전 설정된 합의 알고리즘에 따라 블록체인에 기록하고,

거래 당사자 노드간의 P2P 거래를 위한 P2P 결제 채널을 생성하고,

P2P 결제 채널을 통해 상기 P2P 거래의 과정에서 발생하는 복수의 마이크로 결제(micro payment)에 대한 모든 데이터를 채널에 기록하고 상기 P2P 거래가 종료되면 P2P 결제 채널을 닫고, 상기 채널에 기록된 모든 거래 내역 정보를 포함하는 단일의 Commitment 트랜잭션(Commitment Transaction)을 생성하고, 거래 당사자 노드들의 개인키로 상기 트랜잭션을 다중 서명하고 사전 설정된 합의 알고리즘에 따라 블록체인에 기록하는 것을 특징으로 하는 블록체인 라이트닝 네트워크를 기반으로 한 결제 시스템.

청구항 8

제7항에 있어서, 상기 채널 보증금은, 거래 당사자 노드들의 추후 거래 과정에서 악의적인 시도가 발생하는 경우 페널티로 사용되는 것을 특징으로 하는 블록체인 라이트닝 네트워크를 기반으로 한 결제 시스템.

청구항 9

제2항에 있어서, 상기 중개 노드는 거래 당사자 노드들과 각각 결제 채널을 형성하고 있는 노드로서, 거래 당사자 노드들로부터 사전 설정된 기준 홉(Hop)수 이하이며 수수료가 가장 낮은 노드인 것을 특징으로 하는 블록체인 라이트닝 네트워크를 기반으로 한 결제 시스템.

청구항 10

다수의 참여 노드들과 대출 노드들을 구비하는 블록체인 라이트닝 네트워크에서의 결제 방법에 있어서,

(a) 대출 노드가 대출 정보를 포함하는 트랜잭션을 생성하고, 상기 트랜잭션을 포함하는 스마트 컨트랙트를 작성하여 사전 설정된 합의 알고리즘에 따라 블록체인에 기록하는 단계;

(b) 참여 노드들 중 거래 당사자 노드들이 자신의 신용 정보를 포함하는 트랜잭션을 생성하여 스마트 컨트랙트에 업로드하고, 대출이 필요한 경우, 스마트 컨트랙트를 열람하여 스마트 컨트랙트에 기록된 대출 노드의 대출 정보를 확인하고, 차용 노드(Borrower node)로서 대출 노드에게 대출 신청하는 단계;

(c) 대출 노드는, 차용 노드로부터 대출 신청이 발생하면, 스마트 컨트랙트에 차용 노드에 대한 정보를 요청하고, 스마트 컨트랙트로부터 해당 차용 노드에 대한 정보를 담은 트랜잭션을 열람하고, 대출 노드의 대출 조건과 차용 노드의 신용 정보를 비교하여 확인하고, 차용 노드의 신용 정보가 대출 조건을 충족하는 경우 차용 노드에게 대출을 수행하는 단계;

(d) 참여 노드들 중 거래 당사자 노드들이 P2P(peer to peer) 거래를 위하여 채널 보증금을 예치하고 P2P(peer to peer) 결제 채널을 생성하고, 거래 당사자 노드들이 P2P 결제 채널을 통해 P2P 거래를 수행하는 단계;

를 구비하여, 블록체인 라이트닝 네트워크에서 사용자간의 거래를 활성화시킬 수 있도록 구성된 것을 특징으로 하는 블록체인 라이트닝 네트워크를 기반으로 한 결제 방법.

청구항 11

제10항에 있어서, 상기 블록체인 라이트닝 네트워크를 기반으로 한 결제 방법은,

(e) 거래 당사자 노드들이 중개 노드를 통해 P2P 거래하는 경우, 상기 중개 노드는 결제를 위한 대금에 대한 선지불을 위한 자본이 부족하면, 상기 대출 노드에게 대출 신청하여 대출 노드로부터 선지불을 위한 자본을 대출 받는 단계; 및

(f) 상기 중개 노드는 대금에 대한 선지불을 수행하고 거래 당사자 노드들의 거래를 중개하는 단계;
를 더 구비하는 것을 특징으로 하는 블록체인 라이트닝 네트워크를 기반으로 한 결제 시스템.

청구항 12

제1항에 있어서, 상기 (d) 단계는,

거래 당사자 노드들이 채널 보증금을 예치하는 펀딩 트랜잭션(Funding Transaction)을 생성하여 사전 설정된 합의 알고리즘에 따라 블록체인에 기록하고,

거래 당사자 노드간의 P2P 거래를 위한 P2P 결제 채널을 생성하고,

P2P 결제 채널을 통해 상기 P2P 거래의 과정에서 발생하는 복수의 마이크로 결제(micro payment)에 대한 모든 데이터를 채널에 기록하고 상기 P2P 거래가 종료되면 P2P 결제 채널을 닫고, 상기 채널에 기록된 모든 거래 내역 정보를 포함하는 단일의 Commitment 트랜잭션(Commitment Transaction)을 생성하고, 거래 당사자 노드들의 개인키로 상기 트랜잭션을 다중 서명하고 사전 설정된 합의 알고리즘에 따라 블록체인에 기록하는 것을 특징으로 하는 블록체인 라이트닝 네트워크를 기반으로 한 결제 시스템.

발명의 설명

기술 분야

[0001] 본 발명은 블록체인 라이트닝 네트워크를 기반으로 한 결제 시스템 및 방법에 관한 것으로서, 더욱 구체적으로는 블록체인 라이트닝 네트워크에서 거래 당사자 노드들이 채널 보증금이 부족하거나 HTLC 방식에서의 중개 노드들이 선지불을 수행을 위한 자본이 부족한 경우에 대출 노드를 이용하여 이들에게 대출할 수 있도록 하여, 사용자간의 거래를 활성화시킬 수 있도록 하는 블록체인 라이트닝 네트워크를 기반으로 한 사용자간 거래 활성화를 위한 결제 시스템 및 결제 방법에 관한 것이다.

배경 기술

[0002] 블록체인은 해시 함수를 이용한 데이터 암호화 및 머클트리 구조를 이용한 데이터 무결성을 보장하고 거래장부인 블록체인의 공유를 통해 데이터 위변조 여부 파악이 가능한 peer-to-peer (P2P) 기반의 분산형 컴퓨팅 기술이다.

[0003] 그러나, 기존의 블록체인을 이용한 결제시스템은 각각의 세부 거래 과정마다 트랜잭션이 발생하고 합의 알고리즘을 통해 블록에 기록되어야 하므로 거래 속도가 매우 낮은 문제점이 있다. 특히, 종래의 페이팔, 비자카드 등과 같은 결제시스템과의 거래 속도와 비교하였을 때, 블록체인을 이용한 결제 시스템은 실생활에서 이용하기 어려울 정도로 거래 속도가 매우 낮은 문제점이 있다. 또한, 매 거래마다 트랜잭션을 생성하여 블록체인에 기록하므로 사용자가 많아질수록 전체 블록체인의 용량이 크게 증가하는 확장성 문제가 발생하게 된다.

[0004] 결제 시스템에서의 이러한 문제점들을 극복하기 위하여 비트코인에서는 블록체인 라이트닝 네트워크 기술을 적용하는 방안이 제시되고 있다. 라이트닝 네트워크는 거래 당사자들이 지불, 환불, 송금 등 모든 세부 거래 과정을 매번 트랜잭션을 통해 블록체인에 기록하는 것이 아니라, 거래 당사자간에 off-chain을 통한 1대1 결제 채널(Payment Channel)을 생성하고, 상기 생성된 payment channel을 통해 거래 당사자간의 모든 micro payment를 진행하고 모든 거래 과정의 데이터를 기록하며, 거래가 끝나면 payment channel을 종료한 후, 각자의 개인키를 이용한 다중 서명(Multi Signature)을 통해 모든 거래 내역을 하나의 Commitment Transaction으로 만들어 블록체인에 기록하게 된다. 그 결과, 거래 속도를 높이고 확장성 문제를 해결할 수 있게 된다. 또한, 기존의 결제 시스템에서는 동일한 거래자들 사이에 복수의 micro payment를 할 경우 매 송금마다 암호화페에 대한 송금 수수료가 발생하게 되는 문제가 발생하게 되나, 전술한 라이트닝 네트워크에서는 모든 거래를 수행하고 최종적으로 하나의 트랜잭션을 전파하므로 송금 수수료를 크게 낮출 수 있게 된다.

[0005] 한편, P2P payment channel을 생성하기 위하여 거래 당사자인 노드들은 일정 금액을 채널 보증금으로 예치하는 Funding Transaction을 생성하여야 하며, 거래 당사자들은 이 채널 보증금의 범위내에서 복수의 일대일 micro payment가 가능하게 된다. 또한, 이 채널 보증금에 의해 추후 거래 과정에서 악의적인 시도를 한 이용자에게 페널티 부과가 가능하게 된다.

- [0006] 하지만, 거래 당사자들이 예치할 채널 보증금이 없거나 모자라는 경우에는 Payment Channel 을 생성할 수 없게 되어, 전술한 라이트닝 네트워크를 형성할 수 없게 되는 문제점이 발생하게 된다.
- [0007] 또한, P2P 결제 시스템에서 라이트닝 네트워크가 유지되기 위해서는 HTLC(Hashed Time Locked Contracts) 방식이 필요하다. HTLC 방식은, 예를 들어 설명하면, 노드 A,B,C에서 A와 B, B와 C 사이에는 결제 채널이 형성되어 있지만 A와 C 사이에는 직접적인 결제 채널이 형성되어 있지 않을 경우에도 B를 매개로 하여 A와 C의 사이에 완전한 데이터 교환 및 거래가 가능하게 만드는 방식이다. 이러한 HTLC 방식을 이용하면 A와 C의 사이에 홉(Hop) 수가 높더라도 n개의 중개노드를 거쳐서 A와 C 사이의 채널을 통한 거래가 가능하게 된다.
- [0008] 하지만, HTLC 알고리즘은 A가 C에게 지불할 금액을 B가 C에게 먼저 지불하고, 후에 해시 함수 알고리즘을 통해 B가 A에게서 상기 금액을 받게 되는 선지불 방식이다. 따라서, 다수의 거래로 인해 B가 거래 대금에 해당하는 여유 자본이 없는 경우에는 선지불이 어려우므로 HTLC 방식을 제대로 적용할 수 없게 되는 문제가 발생한다.
- [0009] 또한, 라이트닝 네트워크에서 노드 수가 확장되는 경우 A와 C 사이의 Hop 수가 매우 커지게 되어 n개의 중개 노드를 거쳐서 A와 C가 거래를 해야 하는 경우도 발생한다. 네트워크의 참여 노드가 많아지고 거래가 활성화될수록 1개의 노드가 중개 노드로서 역할을 수행하는 횟수도 많아지게 되므로 중개 노드가 부담해야 하는 선지불 금액의 총 크기는 매우 커지게 되는 문제점이 있다.
- [0010] 이와 같이, 라이트닝 네트워크에서 중개 노드가 선지불할 수 있을 만큼의 자본을 갖고 있지 않거나 특정 노드가 P2P 결제 채널을 생성할 수 있을 정도의 채널 보증금이 없는 경우에는 라이트닝 네트워크에서의 결제가 수행될 수 없게 되고, 그 결과 거래도 활성화될 수 없게 되는 것이다.

선행기술문헌

특허문헌

- [0011] (특허문헌 0001) 한국등록특허공보 제 10-1628007호
(특허문헌 0002) 한국공개특허공보 제 10-2018-0079847호

발명의 내용

해결하려는 과제

- [0012] 전술한 문제점을 해결하기 위한 본 발명은 블록체인 라이트닝 네트워크에 참여하는 거래 노드들에게 P2P 결제 채널을 형성하기 위한 채널 보증금을 대출하거나 중개 노드들에게 HTLC 방식에 따른 선지불 요청에 응하기 위한 자본을 대출할 수 있도록 하여 거래를 활성화시킬 수 있도록 하는 블록체인 라이트닝 네트워크에서의 결제 시스템 및 결제 방법을 제공하는 것을 목적으로 한다.

과제의 해결 수단

- [0013] 전술한 기술적 과제를 달성하기 위한 본 발명의 특징에 따른 블록체인 라이트닝 네트워크를 기반으로 한 결제 시스템은, 다수 개의 참여 노드들을 구비하는 블록체인 라이트닝 네트워크에서의 결제 시스템으로서, 참여 노드의 요청에 따라, 참여 노드에게 결제 채널 생성을 위한 채널 보증금에 대한 대출을 수행하거나, 결제를 위하여 선지불을 수행해야 되는 참여 노드에게 자본금에 대한 대출을 수행하는 대출 노드;를 구비하고,
- [0014] 상기 참여 노드 중 거래 당사자 노드들은 P2P(peer to peer) 거래를 위하여 채널 보증금을 예치하고 P2P(peer to peer) 결제 채널을 생성하고, 거래 당사자 노드들은 P2P 결제 채널을 통해 P2P 거래를 수행하거나, 상기 참여 노드들 중 중개 노드들은 결제를 위한 대금에 대한 선지불을 수행하는 것을 특징으로 하며,
- [0015] 채널 보증금이 부족한 거래 당사자 노드 또는 선지불 요청을 수행하기 위한 자본금이 부족한 중개 노드는 상기 대출 노드에게 대출 신청하여 대출 노드로부터 채널 보증금 또는 자본을 대출받도록 하여, 사용자간의 거래를 활성화시킬 수 있도록 구성된다.
- [0016] 전술한 특징에 따른 블록체인 라이트닝 네트워크를 기반으로 한 결제 시스템에 있어서, 상기 참여 노드는, 자신의 신용 정보를 포함하는 트랜잭션을 생성하여 스마트 컨트랙트에 업로드하고, 대출이 필요한 경우, 스마트 컨트랙트를 열람하여 스마트 컨트랙트에 기록된 대출 노드의 대출 정보를 확인하고, 차용 노드(Borrower node)로

서 대출 노드에게 대출 신청하는 것이 바람직하다.

- [0017] 전술한 특징에 따른 블록체인 라이트닝 네트워크를 기반으로 한 결제 시스템에 있어서, 상기 대출 노드는, 대출 정보를 포함하는 트랜잭션을 생성하고, 상기 트랜잭션을 포함하는 스마트 컨트랙트를 작성하여 사전 설정된 합의 알고리즘에 따라 블록체인에 기록하고, 차용 노드로부터 대출 신청이 발생하면, 스마트 컨트랙트에 차용 노드에 대한 정보를 요청하고, 스마트 컨트랙트로부터 해당 차용 노드에 대한 정보를 담은 트랜잭션을 열람하고, 대출 노드의 대출 조건과 차용 노드의 신용 정보를 비교하여 확인하고, 차용 노드의 신용 정보가 대출 조건을 충족하는 경우 차용 노드에게 대출을 수행하는 것이 바람직하다.
- [0018] 전술한 특징에 따른 블록체인 라이트닝 네트워크를 기반으로 한 결제 시스템에 있어서, 상기 대출 노드의 대출 정보는, 대출 조건, 대출 가능 금액, 상환 일자, 대출 이자, 대출 수수료를 포함하며, 상기 차용 노드의 신용 정보는, 신뢰도, 자본 정보, 대출 기록, 대출 노드와의 홉(Hop) 수를 포함하는 것이 바람직하다.
- [0019] 전술한 특징에 따른 블록체인 라이트닝 네트워크를 기반으로 한 결제 시스템에 있어서, 상기 거래 당사자 노드들은 채널 보증금을 예치하는 펀딩 트랜잭션(Funding Transaction)을 생성하여 사전 설정된 합의 알고리즘에 따라 블록체인에 기록하고, 거래 당사자 노드간의 P2P 거래를 위한 P2P 결제 채널을 생성하고, P2P 결제 채널을 통해 상기 P2P 거래의 과정에서 발생하는 복수의 마이크로 결제(micro payment)에 대한 모든 데이터를 채널에 기록하고 상기 P2P 거래가 종료되면 P2P 결제 채널을 닫고, 상기 채널에 기록된 모든 거래 내역 정보를 포함하는 단일의 Commitment 트랜잭션(Commitment Transaction)을 생성하고, 거래 당사자 노드들의 개인키로 상기 트랜잭션을 다중 서명하고 사전 설정된 합의 알고리즘에 따라 블록체인에 기록하는 것이 바람직하다.
- [0020] 전술한 특징에 따른 블록체인 라이트닝 네트워크를 기반으로 한 결제 시스템에 있어서, 상기 채널 보증금은, 거래 당사자 노드들의 추후 거래 과정에서 악의적인 시도가 발생하는 경우 패널티로 사용되는 것이 바람직하다.

발명의 효과

- [0021] 본 발명에 따른 블록체인 라이트닝 네트워크를 기반으로 한 결제 시스템은, 대출 노드를 더 구비하고, 거래 당사자 노드들이 P2P 결제 채널을 생성하기 위하여 필요한 채널 보증금이 부족하거나, 중개 노드들이 HTLC 방식에 따라 대금을 선지불해야 되는 경우 자본금이 부족한 경우에, 대출 노드로부터 채널 보증금이나 선지불을 위한 자본금을 대출받을 수 있도록 한다.
- [0022] 그 결과, 거래 당사자 노드들이 채널 보증금이 부족하거나 중개 노드가 선지불을 위한 자본금이 부족하더라도 스마트 컨트랙트와 대출 노드를 이용하여 대출할 수 있도록 함으로써, 블록체인 라이트닝 네트워크를 안정적으로 유지할 수 있을 뿐만 아니라 사용자간의 거래를 원활하게 수행할 수 있게 된다.

도면의 간단한 설명

- [0023] 도 1은 본 발명의 제1 실시예에 따른 블록체인 라이트닝 네트워크를 기반으로 한 결제 시스템을 전체적으로 도시한 구성도이다.
- 도 2는 본 발명의 제1 실시예에 따른 블록체인 라이트닝 네트워크를 기반으로 한 결제 시스템에 있어서, 채널 보증금을 대출할 수 있도록 하여 사용자간의 거래 활성화시킨 결제 과정을 순차적으로 도시한 흐름도이다.
- 도 3은 본 발명의 제1 실시예에 따른 블록체인 라이트닝 네트워크를 기반으로 한 결제 시스템에 있어서, 거래 당사자 노드들이 대출 노드로부터 채널 보증금을 대출하는 과정을 도시한 모식도이다.
- 도 4는 본 발명의 제1 실시예에 따른 블록체인 라이트닝 네트워크를 기반으로 한 결제 시스템에 있어서, 거래 당사자 노드들이 P2P 결제 채널(Payment Channel)을 통해 거래하는 것을 도시한 모식도이며, 도 5는 P2P 결제 채널에 의해 생성된 거래 내역들을 포함하는 Commitment transaction을 생성하는 것을 도시한 모식도이다.
- 도 6은 본 발명의 제2 실시예에 따른 블록체인 라이트닝 네트워크를 기반으로 한 결제 시스템에 있어서, HTLC 방식에 의한 중개 노드가 선지불할 자본금을 대출할 수 있도록 하여 사용자간의 거래 활성화시킨 결제 과정을 순차적으로 도시한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

- [0024] 이하, 첨부된 도면을 참조하여 본 발명의 바람직한 제1 실시예에 따른 블록체인 라이트닝 네트워크를 기반으로 한 사용자간의 거래를 활성화시킬 수 있는 결제 시스템 및 결제 방법에 대하여 구체적으로 설명한다.

- [0025] 도 1은 본 발명의 제1 실시예에 따른 블록체인 라이트닝 네트워크를 기반으로 한 결제 시스템을 전체적으로 도시한 구성도이다.
- [0026] 도 1을 참조하면, 본 발명의 제1 실시예에 따른 블록체인 라이트닝 네트워크를 기반으로 한 결제 시스템은, 다수의 참여 노드들과 다수의 대출 노드들을 포함하는 블록체인 라이트닝 네트워크(Blockchain Lightning Network)를 구성한다. 다수의 참여 노드들 중 2개의 노드는 거래 당사자 노드로서 지불, 환불, 송금 등의 거래를 수행하게 된다.
- [0027] 도 2는 본 발명의 제1 실시예에 따른 블록체인 라이트닝 네트워크를 기반으로 한 결제 시스템에 있어서, 채널 보증금을 대출할 수 있도록 하여 사용자간의 거래 활성화시킨 결제 과정을 순차적으로 도시한 흐름도이다. 이하, 도 1 및 도 2를 참조하여 본 발명의 제1 실시예에 따른 결제 시스템에 있어서 거래 당사자 노드에게 채널 보증금을 대출하여 P2P 결제 채널을 이용하여 OFF-Chain 에서 거래할 수 있도록 하는 결제 방법에 대하여 구체적으로 설명한다.
- [0028] 도 1 및 도 2를 참조하면, 본 실시예에 따른 결제 시스템은 먼저 거래 당사자들인 A 및 B를 참여 노드로 하고 적어도 하나 이상의 대출 노드(Lender node)를 포함하는 블록체인 라이트닝 네트워크를 구성한다(단계 400).
- [0029] 각 대출 노드들은 대출 정보를 포함하는 트랜잭션을 생성하고, 상기 트랜잭션을 포함하는 스마트 컨트랙트를 작성하고, 블록체인 라이트닝 네트워크의 다른 노드들에게 전파하고 사전 설정된 합의 알고리즘에 따라 합의 절차를 거친 후 상기 스마트 컨트랙트를 블록체인에 기록한다(단계 410). 상기 대출 정보는 대출 조건, 대출 가능 금액, 상환 일자, 대출 이자, 대출 수수료를 포함하는 것이 바람직하다.
- [0030] 상기 블록체인 라이트닝 네트워크를 구성하는 모든 참여 노드들은 대출을 위하여 필요한 자신의 신용 정보를 포함하는 트랜잭션을 생성하고 스마트 컨트랙트에 기록한다(단계 420). 상기 신용 정보는 신도, 자본 정보, 대출 기록, 대출 노드와의 홉(Hop) 수를 포함하는 것이 바람직하다.
- [0031] 상기 블록체인 라이트닝 네트워크를 구성하는 모든 노드들은 네트워크에서 전파되는 모든 트랜잭션 및 블록들에 대하여 사전 설정된 합의 알고리즘에 따라 유효성을 검증하게 된다(단계 430). 상기 합의 알고리즘은 작업 증명(POW) 등이 사용될 수 있다.
- [0032] 다음, 거래를 수행하고자 하는 거래 당사자 노드들인 제1 및 제2 노드는 채널 보증금을 예치한다. 도 3을 참조하여, 거래 당사자 노드들이 채널 보증금을 예치하는 과정을 보다 구체적으로 설명한다.
- [0033] 도 3은 본 발명의 제1 실시예에 따른 블록체인 라이트닝 네트워크를 기반으로 한 결제 시스템에 있어서, 거래 당사자 노드들이 대출 노드로부터 채널 보증금을 대출하는 과정을 도시한 모식도이다.
- [0034] 먼저, 도 3을 참조하면, 거래 당사자 노드들 중 제1 노드는 결제 채널 생성을 위한 채널 보증금을 예치하는 트랜잭션을 생성하고, 네트워크에 전파하여 사전 설정된 합의 알고리즘에 따라 블록체인에 기록한다. 이때, 제1 노드는 결제 채널 생성을 위한 채널 보증금이 충분한지 여부를 판단한다(단계 440). 만약 채널 보증금이 부족하지 않으면, 제1 노드는 채널 보증금을 예치하기 위한 트랜잭션을 생성하여 네트워크에 전파하고, 사전 설정된 합의 알고리즘에 따라 블록체인에 기록한다(단계 450).
- [0035] 만약 제1 노드가 제2 노드와의 결제 채널 생성을 위한 채널 보증금이 부족한 경우, 스마트 컨트랙트를 열람하여 스마트 컨트랙트에 기록된 대출 노드의 대출 정보를 확인하고, 차용 노드(Borrower node)로서 대출 노드에게 대출 신청을 하게 된다(단계 442). 다음, 대출 노드는 대출 신청에 따라, 스마트 컨트랙트에 차용 노드에 대한 정보를 요청하고, 스마트 컨트랙트로부터 해당 차용 노드에 대한 정보를 담은 트랜잭션을 열람하고(단계 444), 대출 노드의 대출 조건과 차용 노드의 신용 정보를 비교하여 확인하고, 차용 노드의 신용 정보가 대출 조건을 충족하는 경우(단계 446) 차용 노드에게 대출을 수행한다(단계 448). 다음, 제1 노드는 대출받은 채널 보증금을 예치하기 위한 트랜잭션을 생성하여 네트워크에 전파하고, 사전 설정된 합의 알고리즘에 따라 블록체인에 기록한다(단계 450).
- [0036] 한편, 거래 당사자 노드들 중 제2 노드도 결제 채널 생성을 위한 채널 보증금을 예치하는 트랜잭션을 생성하고, 네트워크에 전파하여 사전 설정된 합의 알고리즘에 따라 블록체인에 기록한다. 이때, 제2 노드는 결제 채널 생성을 위한 채널 보증금이 충분한지 여부를 판단한다(단계 460). 만약 채널 보증금이 부족하지 않으면, 제2 노드는 채널 보증금을 예치하기 위한 펀딩 트랜잭션(Funding Transaction)을 생성하여 네트워크에 전파하고, 사전 설정된 합의 알고리즘에 따라 블록체인에 기록한다(단계 470).
- [0037] 만약 제2 노드는 제1 노드와의 결제 채널 생성을 위한 채널 보증금이 부족한 경우, 스마트 컨트랙트를 열람하여

스마트 컨트랙트에 기록된 대출 노드의 대출 정보를 확인하고, 차용 노드(Borrower node)로서 대출 노드에게 대출 신청을 하게 된다(단계 462). 다음, 대출 노드는 대출 신청에 따라, 스마트 컨트랙트에 차용 노드에 대한 정보를 요청하고, 스마트 컨트랙트로부터 해당 차용 노드에 대한 정보를 담은 트랜잭션을 열람하고(단계 464), 대출 노드의 대출 조건과 차용 노드의 신용 정보를 비교하여 확인하고, 차용 노드의 신용 정보가 대출 조건을 충족하는 경우(단계 466) 차용 노드에게 대출을 수행한다(단계 468). 다음, 제2 노드는 대출받은 채널 보증금을 예치하기 위한 펀딩 트랜잭션(Funding Transaction)을 생성하여 네트워크에 전파하고, 사전 설정된 합의 알고리즘에 따라 블록체인에 기록한다(단계 470).

[0038] 한편, 거래 당사자 노드인 제1 노드 또는 제2 노드가 대출을 받지 못하여 채널 보증금이 부족하여 이를 예치하지 못하는 경우 P2P 결제 채널을 생성할 수 없게 되므로, 해당 거래는 무효가 된다.

[0039] 다음, 채널 보증금을 예치한 거래 당사자 노드들인 제1 및 제2 노드는 P2P 결제 채널(Payment channel)을 생성하고 상기 결제 채널을 통해 거래를 수행하게 된다(단계 480). 도 4 내지 도 5를 참조하여, 거래 당사자 노드들이 결제 채널을 생성하고 거래를 수행하는 과정을 보다 구체적으로 설명한다.

[0040] 도 4는 본 발명의 제1 실시예에 따른 블록체인 라이트닝 네트워크를 기반으로 한 결제 시스템에 있어서, 거래 당사자 노드들이 P2P 결제 채널(Payment Channel)을 통해 거래하는 것을 도시한 모식도이며, 도 5는 P2P 결제 채널에 의해 생성된 거래 내역들을 포함하는 Commitment transaction을 생성하는 것을 도시한 모식도이다.

[0041] 전술한 과정에 의해 거래 당사자인 제1 및 제2 노드가 모두 채널 보증금을 예치하면, OFF-chain인 제1 및 제2 노드간의 P2P 결제 채널을 생성하고(단계 480), P2P 결제 채널을 통해 상기 P2P 거래의 과정에서 발생하는 복수의 마이크로 결제(micro payment)에 대한 모든 데이터를 채널에 기록하고 상기 P2P 거래가 종료되면 P2P 결제 채널을 닫고(단계 482), 상기 채널에 기록된 모든 거래 내역 정보를 포함하는 단일의 Commitment 트랜잭션(Commitment Transaction)을 생성하고(단계 484), 거래 당사자 노드들의 개인키로 상기 트랜잭션을 다중 서명하고 사전 설정된 합의 알고리즘에 따라 블록체인에 기록하게 된다(단계 486).

[0042] 한편, 상기 채널 보증금은, 거래 당사자 노드들의 추후 거래 과정에서 악의적인 시도가 발생하는 경우 패널티로 사용된다.

[0043] 이하, 도 6을 참조하여 본 발명의 제2 실시예에 따른 결제 시스템에 있어서 참여 노드가 HTLC 방식에 따른 선지불을 위한 자본금을 대출할 수 있도록 하여 P2P 결제 채널을 이용한 거래에서의 중개 노드 역할을 수행할 수 있도록 하는 결제 방법에 대하여 구체적으로 설명한다.

[0044] 도 6은 본 발명의 제2 실시예에 따른 블록체인 라이트닝 네트워크를 기반으로 한 결제 시스템에 있어서, HTLC 방식에 의한 중개 노드가 선지불할 자본금을 대출할 수 있도록 하여 사용자간의 거래 활성화시킨 결제 과정을 순차적으로 도시한 흐름도이다. 도 6을 참조하면, 본 실시예에 따른 결제 시스템은 먼저 A, B 및 C를 참여 노드로 하고 적어도 하나 이상의 대출 노드(Lender node)를 포함하는 블록체인 라이트닝 네트워크를 구성한다(단계 800).

[0045] 각 대출 노드들은 대출 정보를 포함하는 트랜잭션을 생성하고, 상기 트랜잭션을 포함하는 스마트 컨트랙트를 작성하고, 블록체인 라이트닝 네트워크의 다른 노드들에게 전파하고 사전 설정된 합의 알고리즘에 따라 합의 절차를 거친 후 상기 스마트 컨트랙트를 블록체인에 기록한다(단계 810). 상기 대출 정보는 대출 조건, 대출 가능 금액, 상환 일자, 대출 이자, 대출 수수료를 포함하는 것이 바람직하다.

[0046] 상기 블록체인 라이트닝 네트워크를 구성하는 모든 참여 노드들은 대출을 위하여 필요한 자신의 신용 정보를 포함하는 트랜잭션을 생성하고 스마트 컨트랙트에 기록한다(단계 820). 상기 신용 정보는 신뢰도, 자본 정보, 대출 기록, 대출 노드와의 홉(Hop) 수를 포함하는 것이 바람직하다.

[0047] 상기 블록체인 라이트닝 네트워크를 구성하는 모든 노드들은 네트워크에서 전파되는 모든 트랜잭션 및 블록들에 대하여 사전 설정된 합의 알고리즘에 따라 유효성을 검증하게 된다(단계 830).

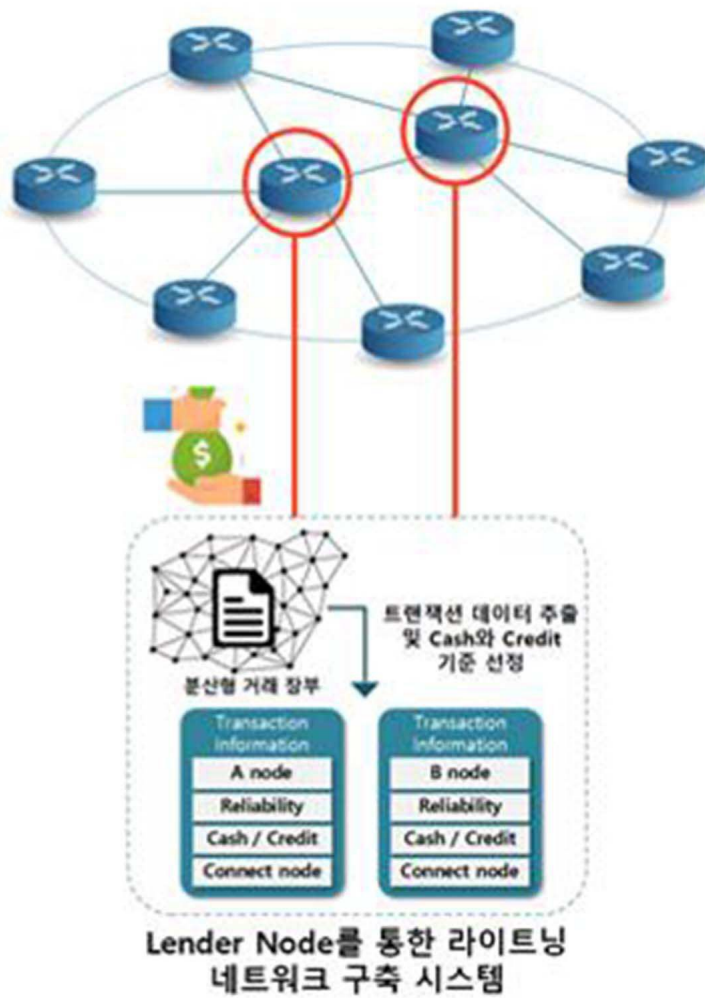
[0048] 다음, 거래를 수행하고자 하는 거래 당사자 노드들인 제1 및 제2 노드(A,C)는 블록체인 네트워크에서의 Hop 수를 계산한다(단계 840). 제1 및 제2 노드의 사이의 Hop 수가 사전 설정된 기준값(m) 이상인지 여부를 판단한다(단계 850).

[0049] 만약, 거래 당사자인 제1 및 제2 노드 사이의 Hop 수가 기준값보다 작으면, 전술한 제1 실시예의 방법에 따라 제1 및 제2 노드의 사이에 P2P Payment Channel을 생성하고 거래를 수행한다(단계 860).

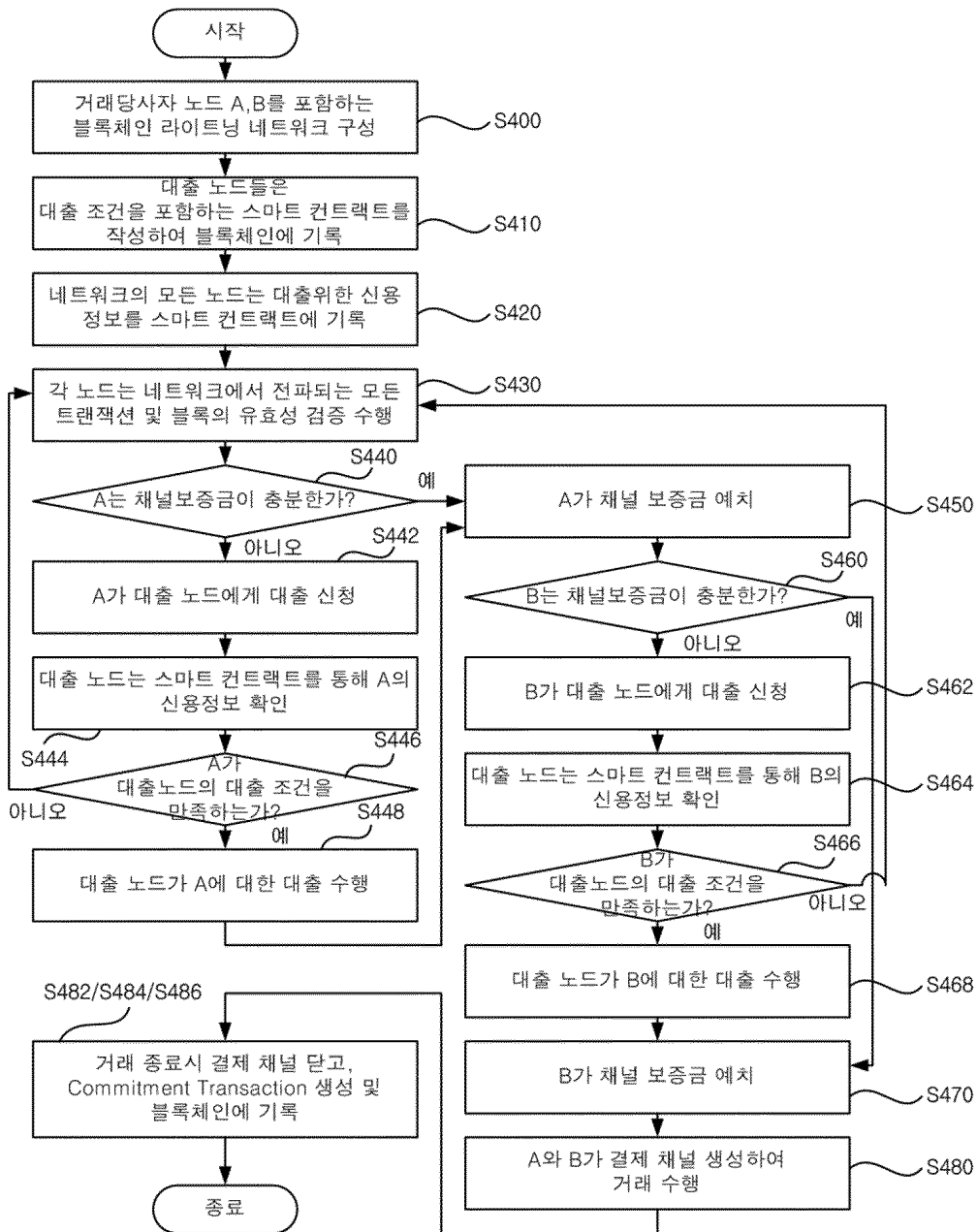
- [0050] 만약, 거래 당사자인 제1 및 제2 노드의 사이의 Hop 수가 기준값 이상이면, 제1 및 제2 노드는 자신들과 거래 채널을 형성하고 있는 노드들을 탐색하고(단계 870), 탐색된 노드들 중에서 제1 및 제2 노드로부터 기준 Hop수 (n) 이하이며 수수료가 가장 낮은 노드를 중개 노드(B)로 선정한다(단계 872).
- [0051] 다음, 중개 노드(B)가 HTLC 방식에 의한 선지불을 위한 자본이 충분한지 여부를 판단한다(단계 874).
- [0052] 만약 중개 노드가 선지불을 위한 자본이 충분하면, 제1 노드(A)와 중개노드(B)의 결제 채널과, 중개노드(B)와 제2 노드(C)의 결제 채널을 통해, 제1 노드(A)와 제2 노드(C)는 거래를 수행하게 된다(단계 890).
- [0053] 만약 중개 노드가 선지불을 위한 자본이 부족하면, 중개 노드는 스마트 컨트랙트를 열람하여 스마트 컨트랙트에 기록된 대출 노드의 대출 정보를 확인하고, 차용 노드(Borrower node)로서 대출 노드에게 대출 신청을 한다(단계 880). 다음, 대출 노드는 대출 신청에 따라, 스마트 컨트랙트에 차용 노드에 대한 정보를 요청하고, 스마트 컨트랙트로부터 해당 차용 노드에 대한 정보를 담은 트랜잭션을 열람하고(단계 882), 대출 노드의 대출 조건과 차용 노드의 신용 정보를 비교하여 확인하고, 차용 노드의 신용 정보가 대출 조건을 충족하는 경우(단계 884) 차용 노드에게 대출을 수행한다(단계 886). 다음, 제1 노드(A)와 중개노드(B)의 결제 채널과, 중개노드(B)와 제2 노드(C)의 결제 채널을 통해, 제1 노드(A)와 제2 노드(C)는 거래를 수행하게 된다(단계 890).
- [0054] 한편, 중개 노드가 대출 노드로부터 대출받지 못하거나 선지불할 자본금이 부족한 경우에는 P2P 결제 채널을 유지할 수 없게 되어 거래는 무효가 된다.
- [0055] 이상에서 본 발명에 대하여 그 바람직한 실시예를 중심으로 설명하였으나, 이는 단지 예시일 뿐 본 발명을 한정하는 것이 아니며, 본 발명이 속하는 분야의 통상의 지식을 가진 자라면 본 발명의 본질적인 특성을 벗어나지 않는 범위에서 이상에 예시되지 않은 여러 가지의 변형과 응용이 가능함을 알 수 있을 것이다. 그리고, 이러한 변형과 응용에 관계된 차이점들은 첨부된 청구 범위에서 규정하는 본 발명의 범위에 포함되는 것으로 해석되어야 할 것이다.

도면

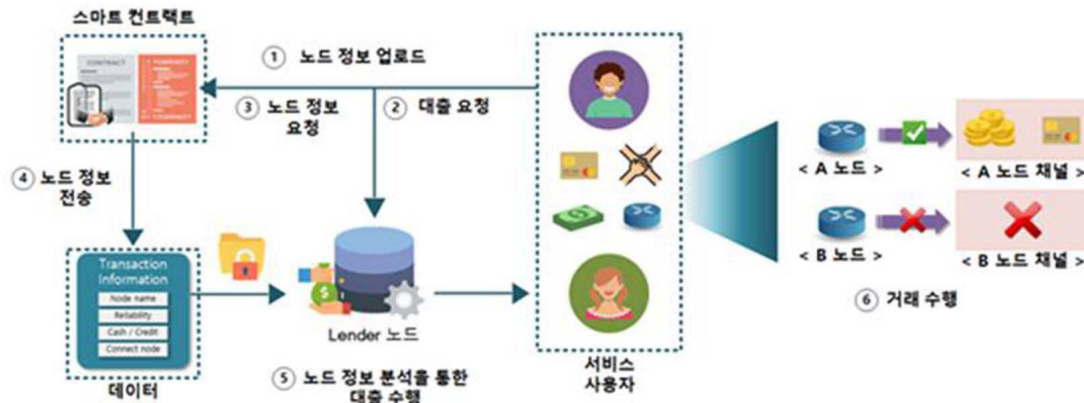
도면1



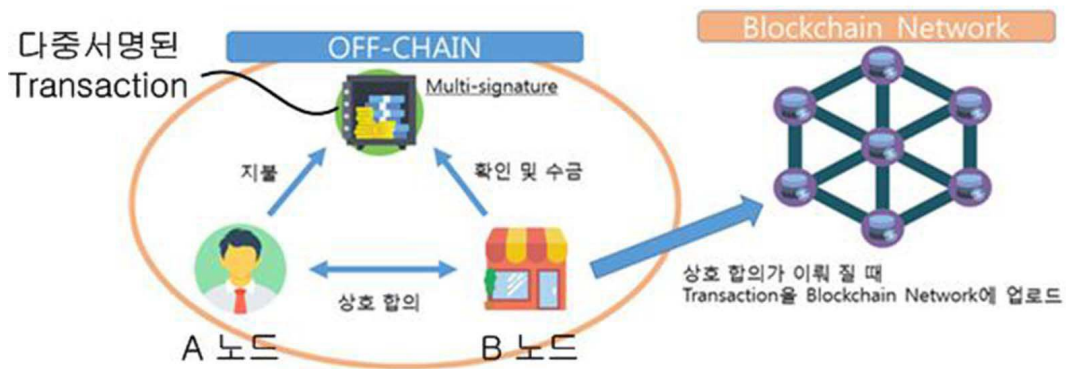
도면2



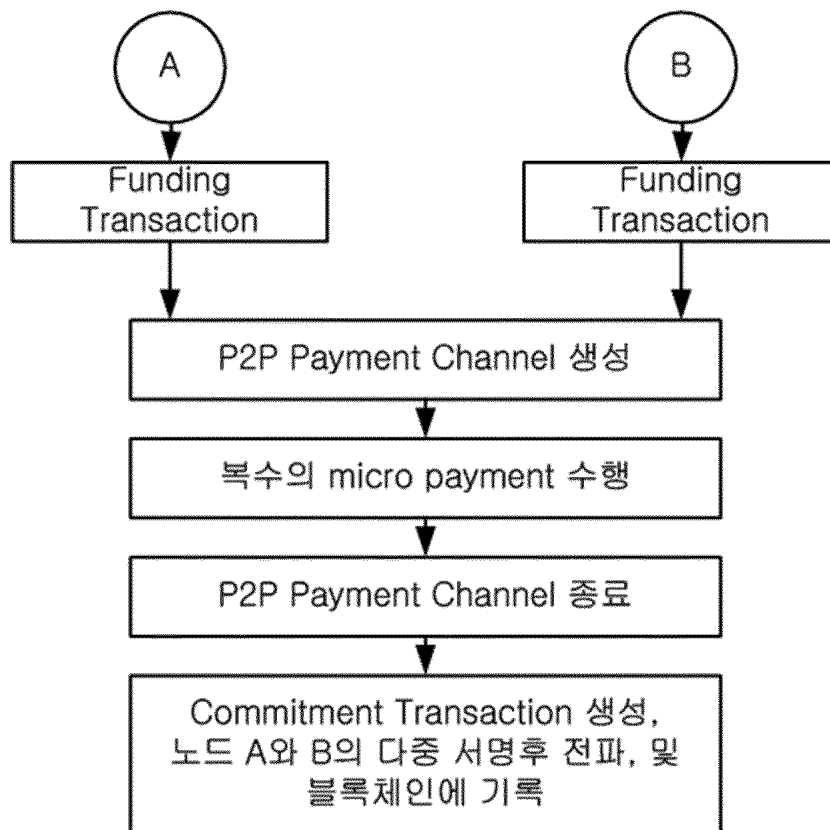
도면3



도면4



도면5



도면6

