(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2023-0071320
(43) 공개일자 2023년05월23일

(51) 국제특허분류(Int. Cl.)
G06Q 20/38 (2012.01) *G06Q 10/06* (2012.01)
G06Q 20/06 (2012.01) *G06Q 20/40* (2012.01)
(52) CPC특허분류
G06Q 20/386 (2023.05)
G06Q 10/0633 (2023.01)
(21) 출원번호 10-2021-0157386
(22) 출원일자 2021년11월16일
심사청구일자 2021년11월16일

(71) 출원인
포항공과대학교 산학협력단
경상북도 포항시 남구 청암로 77 (지곡동)
(72) 발명자
박찬익
경상북도 포항시 남구 지곡로 155, 6동 1105호
노용두
대전광역시 유성구 봉산로 39 , 203동 907호
(74) 대리인
특허법인이상

전체 청구항 수 : 총 20 항

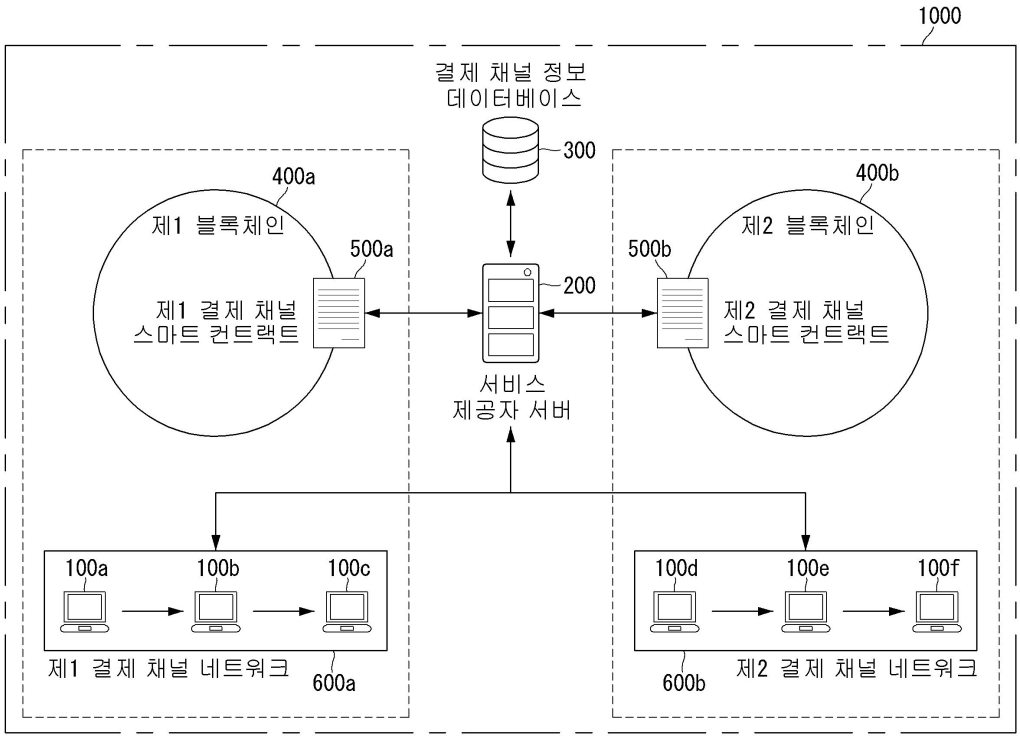
(54) 발명의 명칭 **하나 이상의 블록체인 환경에서의 자산 거래 시스템, 자산 거래 방법 및 장치**

(57) 요 약

본 발명에 의해 개시되는 복수의 블록체인들을 포함하는 크로스체인 간의 자산 거래 방법은 크로스체인 자산 거래 요청을 수신하는 단계; 상기 요청에 따라 블록체인 별로 결제 채널 네트워크를 개설하는 단계; 상기 결제 채널 네트워크들에 연관된 모든 사용자 단말들에게 준비 메시지를 생성 및 전송하는 단계; 자산 거래와 관련된 모

(뒷면에 계속)

대 표 도



든 사용자 단말들로부터 준비 완료 메시지를 수신하였는지 여부를 확인하고, 자산 거래와 관련된 모든 사용자 단말들에게 개별 결제 채널 네트워크 별로 커밋(COMMIT) 메시지와 함께 사용자 단말들로부터 수신한 모든 준비 완료 메시지들을 전송하는 단계; 상기 결제 채널 네트워크와 관련된 사용자 단말들에게 상기 결제 채널 네트워크와 관련된 사용자 단말들로부터 수신한 모든 커밋 완료 메시지와 함께 거래 승인(CONFIRM) 메시지를 생성 및 전송하는 단계; 및 결제 채널 네트워크와 관련된 사용자 단말로부터 수신하는 응답 메시지에 따라 거래 승인 메시지 또는 환불 승인 메시지를 송신하는 단계를 포함하고, 상기 거래 승인 메시지 또는 환불 승인 메시지를 송신하는 단계는, 상기 거래 승인 메시지 및 환불 승인 메시지 중 어느 하나의 메시지만 생성되도록 강제하는 것을 특징으로 한다.

(52) CPC특허분류

G06Q 20/065 (2013.01)
G06Q 20/407 (2013.01)
H04L 9/50 (2022.05)
H04L 2209/56 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호	1711126049
과제번호	2018-0-01441-004
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기획평가원
연구사업명	정보통신방송혁신인재양성
연구과제명	크로스 도메인 호환성을 위한 블록체인 플랫폼 및 비즈모델 개발
기 여 율	70/100
과제수행기관명	포항공과대학교 산학협력단
연구기간	2021.01.01 ~ 2021.12.31

이 발명을 지원한 국가연구개발사업

과제고유번호	1711125876
과제번호	2020-0-00936-002
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기획평가원
연구사업명	블록체인융합기술개발
연구과제명	5G 초저지연 서비스를 위한 무선 단말용 블록체인 기술 개발
기 여 율	30/100
과제수행기관명	포항공과대학교 산학협력단
연구기간	2021.01.01 ~ 2021.12.31

명 세 서

청구범위

청구항 1

프로세서가 실행하는 크로스체인 자산 거래 프로그램에 의해 실행되며, 서비스 제공자 서버를 활용하여 블록체인마다 개별적인 결제 채널 스마트 컨트랙트를 구비하고 있는 복수의 블록체인들을 포함하는 크로스체인 간의 자산 거래 방법으로서,

크로스체인 자산 거래 요청을 수신하는 단계;

상기 요청에 따라 블록체인 별로 결제 채널 네트워크를 개설하는 단계;

상기 결제 채널 네트워크들에 연관된 모든 사용자 단말들에게 준비 메시지를 생성 및 전송하는 단계;

자산 거래와 관련된 모든 사용자 단말들로부터 준비 완료 메시지를 수신하였는지 여부를 확인하고, 자산 거래와 관련된 모든 사용자 단말들에게 개별 결제 채널 네트워크 별로 커밋(COMMIT) 메시지와 함께 사용자 단말들로부터 수신한 모든 준비 완료 메시지들을 전송하는 단계;

상기 결제 채널 네트워크와 관련된 사용자 단말들에게 상기 결제 채널 네트워크와 관련된 사용자 단말들로부터 수신한 모든 커밋 완료 메시지와 함께 거래 승인(CONFIRM) 메시지를 생성 및 전송하는 단계; 및

결제 채널 네트워크와 관련된 사용자 단말로부터 수신하는 응답 메시지에 따라 거래 승인 메시지 또는 환불 승인 메시지를 송신하는 단계를 포함하고,

상기 거래 승인 메시지 또는 환불 승인 메시지를 송신하는 단계는,

상기 거래 승인 메시지 및 환불 승인 메시지 중 어느 하나의 메시지만 생성되도록 강제하는 것을 특징으로 하는,

자산 거래 방법.

청구항 2

청구항 1에 있어서,

상기 결제 채널 스마트 컨트랙트는,

결제에 관여하는 사용자 단말에 문제가 발생하였을 때 일관된 방식으로 분쟁 조절하는 것을 특징으로 하는,

자산 거래 방법.

청구항 3

청구항 2에 있어서,

상기 일관된 방식은,

결제에 관여하는 모든 상기 사용자 단말들의 결제 채널 상태가 결제 완료 이후의 상태를 가진 채로 종료하거나 또는 모든 상기 사용자 단말의 결제 채널 상태가 결제 이전의 상태를 가진 채로 종료하는 것을 특징으로 하는,

자산 거래 방법.

청구항 4

청구항 1에 있어서,

상기 사용자 단말은,

결제 채널이 사용되지 않는 IDLE,

크로스체인 자산 거래에 사용하기 위해 준비 완료됨을 의미하는 PREPARED, 및 크로스체인 자산 거래에 관여되는

모든 상기 사용자 단말들이 결제 채널 사용을 동의(준비)하고, 크로스체인 자산 거래가 완료되기를 대기하는 COMMITTED의 결제 채널 상태를 갖는 것을 특징으로 하는,

자산 거래 방법.

청구항 5

청구항 1에 있어서,

상기 요청에 따라 블록체인 별로 결제 채널 네트워크를 개설하는 단계는,

결제 채널 정보 데이터베이스에 저장된 결제 채널 정보를 토대로 블록체인 별로 결제 채널 네트워크를 개설하는 것을 특징으로 하는,

자산 거래 방법.

청구항 6

청구항 1에 있어서,

상기 서비스 제공자 서버는,

크로스체인 자산 거래 인스턴스가 생성 및 초기화된 상태인 NONE,

크로스체인 자산 거래에 관여되는 모든 사용자 단말들이 결제 채널 사용에 동의했음을 나타내는 PREPARED,

크로스체인 자산 거래에 관여되는 모든 사용자 단말들의 결제 채널의 상태가 커밋 완료임을 나타내는 COMMITTED, 및

크로스체인 자산 거래에 관여되는 사용자 단말들 중 하나 이상의 사용자 단말로부터 진행 중이던 크로스체인 자산 거래 취소 요청을 받은 상태인 REFUND AUTHORIZED 상태를 가지는 것을 특징으로 하는,

자산 거래 방법.

청구항 7

청구항 1에 있어서,

상기 결제 채널 네트워크에 연관된 모든 사용자 단말들에게 준비 메시지를 생성 및 전송하는 단계는,

블록체인 목록, 블록체인 별 송신자 단말 공개 주소, 블록체인 별 수신자 단말 공개 주소의 정보를 포함하는 크로스체인 자산 거래 요청 메시지를 함께 전송하는 것을 특징으로 하는,

자산 거래 방법.

청구항 8

청구항 6에 있어서,

상기 거래 승인 메시지 또는 환불 승인 메시지를 송신하는 단계는,

상기 REFUND AUTHORIZED 상태를 제외한 다른 상태에서, 모든 사용자 단말들로부터 자산 거래 COMMIT 메시지에 동의하는 메시지를 수신한 경우,

상기 거래 승인 메시지를 송신하고, 신뢰 실행 환경 상에서 송신자 단말의 크로스체인 자산 거래 예약금을 차감하며, 수신자 단말의 결제 채널 수신자 금액을 크로스체인 자산 거래 예약금만큼 증가시키는 단계를 더 포함하는 것을 특징으로 하는,

자산 거래 방법.

청구항 9

청구항 6에 있어서,

상기 거래 승인 메시지 또는 환불 승인 메시지를 송신하는 단계는,

상기 COMMITTED 상태를 제외한 상태에서, 하나 이상의 사용자 단말로부터 환불 메시지를 수신한 경우,

크로스체인 자산 거래에 관여되는 모든 사용자 단말들에게 환불 승인 메시지를 송신하는 단계를 더 포함하는 것을 특징으로 하는,

자산 거래 방법.

청구항 10

서비스 제공자 서버 및 블록체인마다 개별적인 결제 채널 스마트 컨트랙트를 구비하고 있는 복수의 블록체인들을 포함하는 크로스체인 간의 자산 거래 장치로서,

프로세서(processor); 및

상기 프로세서에 의해 실행되는 하나 이상의 명령들이 저장된 메모리(memory)를 포함하며,

상기 하나 이상의 명령들은,

크로스체인 자산 거래 요청을 수신하는 명령;

상기 요청에 따라 블록체인 별로 결제 채널 네트워크를 개설하는 명령;

상기 결제 채널 네트워크들에 연관된 모든 사용자 단말들에게 준비 메시지를 생성 및 전송하는 명령;

자산 거래와 관련된 모든 사용자 단말들로부터 준비 완료 메시지를 수신하였는지 여부를 확인하고, 자산 거래와 관련된 모든 사용자 단말들에게 개별 결제 채널 네트워크 별로 커밋(COMMIT) 메시지와 함께 사용자 단말들로부터 수신한 모든 준비 완료 메시지들을 전송하는 명령;

상기 결제 채널 네트워크와 관련된 사용자 단말들에게 상기 결제 채널 네트워크와 관련된 사용자 단말들로부터 수신한 모든 커밋 완료 메시지와 함께 거래 승인(CONFIRM) 메시지를 생성 및 전송하는 명령; 및

결제 채널 네트워크와 관련된 사용자 단말로부터 수신하는 응답 메시지에 따라 거래 승인 메시지 또는 환불 승인 메시지를 송신하는 명령을 포함하고,

상기 거래 승인 메시지 또는 환불 승인 메시지를 송신하는 명령은,

상기 거래 승인 메시지 및 환불 승인 메시지 중 어느 하나의 메시지만 생성하도록 강제하는 것을 특징으로 하는,

자산 거래 장치.

청구항 11

청구항 10에 있어서,

상기 결제 채널 스마트 컨트랙트는,

결제에 관여하는 사용자 단말에 문제가 발생하였을 때 일관된 방식으로 분쟁 조절하는 것을 특징으로 하는,

자산 거래 장치.

청구항 12

청구항 11에 있어서,

상기 일관된 방식은,

결제에 관여하는 모든 상기 사용자 단말들의 결제 채널 상태가 결제 완료 이후의 상태를 가진 채로 종료하거나 또는 모든 상기 사용자 단말의 결제 채널 상태가 결제 이전의 상태를 가진 채로 종료하는 것을 특징으로 하는,

자산 거래 장치.

청구항 13

청구항 10에 있어서,

상기 사용자 단말은,

결제 채널이 사용되지 않는 IDLE,

크로스체인 자산 거래에 사용하기 위해 준비 완료됨을 의미하는 PREPARED, 및

크로스체인 자산 거래에 관여되는 모든 상기 사용자 단말들이 결제 채널 사용을 동의(준비)하고, 크로스체인 자산 거래가 완료되기를 대기하는 COMMITTED의 결제 채널 상태를 갖는 것을 특징으로 하는,

자산 거래 장치.

청구항 14

청구항 10에 있어서,

상기 요청에 따라 블록체인 별로 결제 채널 네트워크를 개설하는 명령은,

결제 채널 정보 데이터베이스에 저장된 결제 채널 정보를 토대로 블록체인 별로 결제 채널 네트워크를 개설하는 것을 특징으로 하는,

자산 거래 장치.

청구항 15

청구항 10에 있어서,

상기 서비스 제공자 서버는,

크로스체인 자산 거래 인스턴스가 생성 및 초기화된 상태인 NONE,

크로스체인 자산 거래에 관여되는 모든 사용자 단말들이 결제 채널 사용에 동의했음을 나타내는 PREPARED,

크로스체인 자산 거래에 관여되는 모든 사용자 단말들의 결제 채널의 상태가 커밋 완료임을 나타내는 COMMITTED, 및

크로스체인 자산 거래에 관여되는 사용자 단말들 중 하나 이상의 사용자 단말로부터 진행 중이던 크로스체인 자산 거래 취소 요청을 받은 상태인 REFUND AUTHORIZED 상태를 가지는 것을 특징으로 하는,

자산 거래 장치.

청구항 16

청구항 10에 있어서,

상기 결제 채널 네트워크들에 연관된 모든 사용자 단말들에게 준비 메시지를 생성 및 전송하는 명령은,

블록체인 목록, 블록체인 별 송신자 단말 공개 주소, 블록체인 별 수신자 단말 공개 주소의 정보를 포함하는 크로스체인 자산 거래 요청 메시지를 함께 전송하는 것을 특징으로 하는,

자산 거래 장치.

청구항 17

청구항 15에 있어서,

상기 거래 승인 메시지 또는 환불 승인 메시지를 송신하는 명령은,

상기 REFUND AUTHORIZED 상태를 제외한 다른 상태에서, 모든 사용자 단말들로부터 자산 거래 COMMIT 메시지에 동의하는 메시지를 수신한 경우,

상기 거래 승인 메시지를 송신하고, 신뢰 실행 환경 상에서 송신자 단말의 크로스체인 자산 거래 예약금을 차감하며, 수신자 단말의 결제 채널 수신자 금액을 크로스체인 자산 거래 예약금만큼 증가시키도록 수행하는 명령을 더 포함하는 것을 특징으로 하는,

자산 거래 장치.

청구항 18

청구항 15에 있어서,

상기 거래 승인 메시지 또는 환불 승인 메시지를 송신하는 명령은,

상기 COMMITTED 상태를 제외한 상태에서, 하나 이상의 사용자 단말로부터 환불 메시지를 수신한 경우,

상기 크로스체인 자산 거래에 관여되는 모든 사용자 단말들에게 환불 승인 메시지를 송신하도록 하는 명령을 더 포함하는 것을 특징으로 하는,

자산 거래 장치.

청구항 19

서비스 제공자 서버를 활용하여 결제 채널 스마트 컨트랙트를 구비하는 동일한 블록체인 내의 멀티 홉 결제 방법으로서,

멀티 홉 결제 요청을 수신하는 단계;

상기 요청에 따라 블록체인 별로 결제 채널 네트워크를 개설하는 단계;

상기 결제 채널 네트워크에 연관된 모든 사용자 단말들에게 준비 메시지를 생성 및 전송하는 단계;

멀티 홉 결제와 관련된 모든 사용자 단말들로부터 준비 완료 메시지를 수신하였는지 여부를 확인하고, 멀티 홉 결제와 관련된 모든 사용자 단말들에게 개별 결제 채널 네트워크 별로 커밋(COMMIT) 메시지와 함께 사용자 단말들로부터 수신한 모든 준비 완료 메시지들을 전송하는 단계; 및

상기 결제 채널 네트워크와 관련된 사용자 단말들에게 상기 결제 채널 네트워크와 관련된 사용자 단말들로부터 수신한 모든 커밋 완료 메시지와 함께 거래 승인(CONFIRM) 메시지를 생성 및 전송하는 단계를 포함하는,

자산 거래 방법.

청구항 20

청구항 19에 있어서,

상기 사용자 단말은,

결제 진행 중 임의의 시점에 결제 채널 스마트 컨트랙트의 결제 채널 정산 모듈을 통하여 결제 채널 네트워크를 이탈할 수 있는 것을 특징으로 하는,

자산 거래 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 블록체인 환경에서의 자산 거래 시스템, 자산 거래 방법 및 장치에 관한 것으로, 보다 상세하게는, 하나 이상의 블록체인 환경에서 자산 거래 서비스를 실시간으로 빠르게 처리하기 위한 블록체인 환경에서의 자산 거래 시스템, 자산 거래 방법 및 장치에 관한 것이다.

배 경 기 술

[0002] 블록체인(Blockchain)은 사용자 단말 간 합의 알고리즘을 통해 데이터의 무결성 및 투명성을 보장하는 분산 시스템이다. 상기 블록체인 상에서 실행되는 스마트 컨트랙트(Smart Contract)는 모든 사용자 단말이 동일한 프로그램 로직을 수행하고 동일한 결과를 얻을 수 있도록 하는 분산 시스템 환경에서의 프로그램이다.

[0003] 상기 블록체인은 크게 두가지 문제점을 가지고 있다. 첫번째 단점은 블록체인에서 사용되는 코인 혹은 디지털 자산은 오직 해당 블록체인에서만 사용 가능하다는 제한이 있다는 것이다. 두번째 단점은 블록체인은 블록체인 네트워크에 참여하는 사용자 단말 수가 증가하면 증가할수록 합의 알고리즘 수행 시간 역시 늘어난다는 확장성의 문제가 있다는 점이다.

[0004] 상기 블록체인은 합의 알고리즘 모델, 결제 처리 특화 모델, 디지털 자산, 네트워크 참여 등 다양한 목적에 부합되도록 설계된다. 상기 다양한 블록체인들은 각각 독립적인 네트워크를 구성하기 때문에, 디지털 자산의 활용도를 극대화할 수 있도록 복수 개의 블록체인 간 효율적인 자산 거래 기법이 요구된다. 여기서, 크로스체인은 복수 개의 블록체인을 의미한다. 상기 크로스체인의 효율적인 자산거래 기법으로는 Atomic Cross-Chain Swaps (이하, ACCS), Tesseract, AC3WN 등이 있다.

[0005] 상기 ACCS는 비밀값을 제공하는 경우에만 컨트랙트가 수행될 수 있도록 강제하는 Hashed Timelock Contract(HTLC)를 이용하여 사용자 단말 간 크로스체인 자산 교환을 안전하게 달성하는 기법이다. 각 사용자 단말은 순차적으로, 반드시 비밀값을 제공하는 경우에만 상대방 사용자 단말로부터 디지털 자산의 소유권을 양도받을 수 있다.

[0006] 상기 Tesseract는 신뢰 실행 환경(Trusted Execution Environment)을 사용하여 실시간으로 크로스체인 자산 거래를 지원하는 시스템이다. 상기 신뢰 실행 환경은 미리 정해진 프로그램 코드의 실행만을 강제하여 사용자의 악의적인 행동을 차단하는 하드웨어 기술이다. 상기 Tesseract는 이러한 신뢰 실행 환경의 특징을 이용하여 오프체인상에서 크로스체인 자산 거래를 지원한다.

[0007] 상기 AC3WN은 크로스체인 자산 거래를 병렬로 수행하여 사용자 수에 상관없이 총 네 번의 블록체인 승인 기간을 요구하는 기법이다.

[0008] 하지만 상기의 3가지의 방법은 아래와 같은 문제점을 가지고 있다.

[0009] 상기 ACCS 프로토콜은 HTLC를 이용하여 크로스체인 자산 거래를 지원한다. 그러나 서로 다른 블록체인에 속한 각 사용자 단말은 자신들이 생성 및 전파한 트랜잭션이 블록체인에 완전히 포함될 때까지 충분한 승인 기간을 필수적으로 요구하므로, 거래 지연 시간은 사용자 수에 비례하여 증가한다는 문제점을 내포하고 있다.

[0010] 상기 Tesseract는 신뢰 실행 환경을 활용하여 오프체인상 실시간으로 크로스체인 자산 거래를 지원한다. 그러나, Tesseract는 사용자 단말 간 오직 일대일 거래만 지원 가능하다. 따라서, 제공 가능한 크로스체인 자산 거래의 범위가 한정적이라는 문제점이 있다.

[0011] 상기 AC3WN은 크로스체인 자산 거래의 성공 및 환불 여부가 총 네 번의 블록체인 승인 기간만을 요구하기 때문에 사용자 수에 상관없이 지연 시간이 증가하지 않는다는 장점이 있다. 그러나, 요구되는 네 번의 블록체인 승인 기간은 여전히 수 분 이상의 지연 시간이 소요된다는 문제가 있다.

발명의 내용

해결하려는 과제

[0012] 상기와 같은 문제점을 해결하기 위한 본 발명의 목적은 일대일 뿐만 아니라 다자간 크로스체인 자산 거래를 지원할 수 있고, 오프체인상 자산 거래를 지원하여 실시간 거래를 지원할 수 있는 자산 거래 방법을 제공하는데 있다.

[0013] 상기와 같은 문제점을 해결하기 위한 본 발명의 다른 목적은 일대일 뿐만 아니라 다자간 크로스체인 자산 거래를 지원할 수 있고, 오프체인상 자산 거래를 지원하여 실시간 거래를 지원할 수 있는 자산 거래 장치를 제공하는데 있다.

[0014] 상기와 같은 문제점을 해결하기 위한 본 발명의 또 다른 목적은 동일 블록체인에서 멀티 홉 결제를 지원할 수 있는 자산 거래 방법을 제공하는데 있다.

과제의 해결 수단

[0015] 상기 목적을 달성하기 위한 본 발명의 일 실시예에 따른 프로세서가 실행하는 크로스체인 자산 거래 프로그램에 의해 실행되며, 서비스 제공자 서버를 활용하여 블록체인마다 개별적인 결제 채널 스마트 컨트랙트를 구비하고 있는 복수의 블록체인들을 포함하는 크로스체인 간의 자산 거래 방법은 크로스체인 자산 거래 요청을 수신하는 단계; 상기 요청에 따라 블록체인 별로 결제 채널 네트워크를 개설하는 단계; 상기 결제 채널 네트워크들에 연관된 모든 사용자 단말들에게 준비 메시지를 생성 및 전송하는 단계; 자산 거래와 관련된 모든 사용자 단말들로부터 준비 완료 메시지를 수신하였는지 여부를 확인하고, 자산 거래와 관련된 모든 사용자 단말들에게 개별 결제 채널 네트워크 별로 커밋(COMMIT) 메시지와 함께 사용자 단말들로부터 수신한 모든 준비 완료 메시지들을 전송하는 단계; 상기 결제 채널 네트워크와 관련된 사용자 단말들에게 상기 결제 채널 네트워크와 관련된 사용자

단말들로부터 수신한 모든 커밋 완료 메시지와 함께 거래 승인(CONFIRM) 메시지를 생성 및 전송하는 단계; 및 결제 채널 네트워크와 관련된 사용자 단말로부터 수신하는 응답 메시지에 따라 거래 승인 메시지 또는 환불 승인 메시지를 송신하는 단계를 포함하고, 상기 거래 승인 메시지 또는 환불 승인 메시지를 송신하는 단계는, 상기 거래 승인 메시지 및 환불 승인 메시지 중 어느 하나의 메시지만 생성되도록 강제하는 것을 특징으로 한다.

[0016] 상기 결제 채널 스마트 컨트랙트는, 결제에 관여하는 사용자 단말에 문제가 발생하였을 때 일관된 방식으로 분쟁 조절하는 것을 특징으로 할 수 있다.

[0017] 상기 일관된 방식은, 결제에 관여하는 모든 상기 사용자 단말들의 결제 채널 상태가 결제 완료 이후의 상태를 가진 채로 종료하거나 또는 모든 상기 사용자 단말의 결제 채널 상태가 결제 이전의 상태를 가진 채로 종료하는 것을 특징으로 할 수 있다.

[0018] 상기 사용자 단말은, 결제 채널이 사용되지 않는 IDLE, 크로스체인 자산 거래에 사용하기 위해 준비 완료됨을 의미하는 PREPARED, 및 크로스체인 자산 거래에 관여되는 모든 상기 사용자 단말들이 결제 채널 사용을 동의(준비)하고, 크로스체인 자산 거래가 완료되기를 대기하는 COMMITTED의 결제 채널 상태를 갖는 것을 특징으로 할 수 있다.

[0019] 상기 요청에 따라 블록체인 별로 결제 채널 네트워크를 개설하는 단계는 결제 채널 정보 데이터베이스에 저장된 결제 채널 정보를 토대로 블록체인 별로 결제 채널 네트워크를 개설하는 것을 특징으로 할 수 있다.

[0020] 상기 서비스 제공자 서버는, 크로스체인 자산 거래 인스턴스가 생성 및 초기화된 상태인 NONE, 크로스체인 자산 거래에 관여되는 모든 사용자 단말들이 결제 채널 사용에 동의했음을 나타내는 PREPARED, 크로스체인 자산 거래에 관여되는 모든 사용자 단말들의 결제 채널의 상태가 커밋 완료임을 나타내는 COMMITTED, 및 크로스체인 자산 거래에 관여되는 사용자 단말들 중 하나 이상의 사용자 단말로부터 진행 중이던 크로스체인 자산 거래 취소 요청을 받은 상태인 REFUND AUTHORIZED 상태를 가지는 것을 특징으로 할 수 있다.

[0021] 상기 결제 채널 네트워크에 연관된 모든 사용자 단말들에게 준비 메시지를 생성 및 전송하는 단계는, 블록체인 목록, 블록체인 별 송신자 단말 공개 주소, 블록체인 별 수신자 단말 공개 주소의 정보를 포함하는 크로스체인 자산 거래 요청 메시지를 함께 전송하는 것을 특징으로 할 수 있다.

[0022] 상기 거래 승인 메시지 또는 환불 승인 메시지를 송신하는 단계는, 상기 REFUND AUTHORIZED 상태를 제외한 다른 상태에서, 모든 사용자 단말들로부터 자산 거래 COMMIT 메시지에 동의하는 메시지를 수신한 경우, 상기 거래 승인 메시지를 송신하고, 신뢰 실행 환경 상에서 송신자 단말의 크로스체인 자산 거래 예약금을 차감하며, 수신자 단말의 결제 채널 수신자 금액을 크로스체인 자산 거래 예약금만큼 증가시키는 단계를 더 포함할 수 있다.

[0023] 상기 거래 승인 메시지 또는 환불 승인 메시지를 송신하는 단계는 상기 COMMITTED 상태를 제외한 상태에서, 하나 이상의 사용자 단말로부터 환불 메시지를 수신한 경우, 크로스체인 자산 거래에 관여되는 모든 사용자 단말들에게 환불 승인 메시지를 송신하는 단계를 더 포함할 수 있다.

[0024] 상기 목적을 달성하기 위한 본 발명의 다른 실시예에 따른 서비스 제공자 서버 및 블록체인마다 개별적인 결제 채널 스마트 컨트랙트를 구비하고 있는 복수의 블록체인들을 포함하는 크로스체인 간의 자산 거래 장치는, 프로세서(processor); 및 상기 프로세서에 의해 실행되는 하나 이상의 명령들이 저장된 메모리(memory)를 포함하며, 상기 하나 이상의 명령들은, 크로스체인 자산 거래 요청을 수신하는 명령; 상기 요청에 따라 블록체인 별로 결제 채널 네트워크를 개설하는 명령; 상기 결제 채널 네트워크들에 연관된 모든 사용자 단말들에게 준비 메시지를 생성 및 전송하는 명령; 자산 거래와 관련된 모든 사용자 단말들로부터 준비 완료 메시지를 수신하였는지 여부를 확인하고, 자산 거래와 관련된 모든 사용자 단말들에게 개별 결제 채널 네트워크 별로 커밋(COMMIT) 메시지와 함께 사용자 단말들로부터 수신한 모든 준비 완료 메시지들을 전송하는 명령; 상기 결제 채널 네트워크와 관련된 사용자 단말들에게 상기 결제 채널 네트워크와 관련된 사용자 단말들로부터 수신한 모든 커밋 완료 메시지와 함께 거래 승인(CONFIRM) 메시지를 생성 및 전송하는 명령; 및 결제 채널 네트워크와 관련된 사용자 단말로부터 수신하는 응답 메시지에 따라 거래 승인 메시지 또는 환불 승인 메시지를 송신하는 명령을 포함하고, 상기 거래 승인 메시지 또는 환불 승인 메시지를 송신하는 명령은, 상기 거래 승인 메시지 및 환불 승인 메시지 중 어느 하나의 메시지만 생성하도록 강제하는 것을 특징으로 할 수 있다.

[0025] 상기 결제 채널 스마트 컨트랙트는, 결제에 관여하는 사용자 단말에 문제가 발생하였을 때 일관된 방식으로 분쟁 조절하는 것을 특징으로 할 수 있다.

[0026] 상기 일관된 방식은, 결제에 관여하는 모든 상기 사용자 단말들의 결제 채널 상태가 결제 완료 이후의 상태를

가진 채로 종료하거나 또는 모든 상기 사용자 단말의 결제 채널 상태가 결제 이전의 상태를 가진 채로 종료하는 것을 특징으로 할 수 있다.

[0027] 상기 사용자 단말은, 결제 채널이 사용되지 않는 IDLE, 크로스체인 자산 거래에 사용하기 위해 준비 완료됨을 의미하는 PREPARED, 및 크로스체인 자산 거래에 관여되는 모든 상기 사용자 단말들이 결제 채널 사용을 동의(준비)하고, 크로스체인 자산 거래가 완료되기를 대기하는 COMMITTED의 결제 채널 상태를 갖는 것을 특징으로 할 수 있다.

[0028] 상기 요청에 따라 블록체인 별로 결제 채널 네트워크를 개설하는 명령은, 결제 채널 정보 데이터베이스에 저장된 결제 채널 정보를 토대로 블록체인 별로 결제 채널 네트워크를 개설하는 것을 특징으로 할 수 있다.

[0029] 상기 서비스 제공자 서버는, 크로스체인 자산 거래 인스턴스가 생성 및 초기화된 상태인 NONE, 크로스체인 자산 거래에 관여되는 모든 사용자 단말들이 결제 채널 사용에 동의했음을 나타내는 PREPARED, 크로스체인 자산 거래에 관여되는 모든 사용자 단말들의 결제 채널의 상태가 커밋 완료임을 나타내는 COMMITTED, 및 크로스체인 자산 거래에 관여되는 사용자 단말들 중 하나 이상의 사용자 단말로부터 진행 중이던 크로스체인 자산 거래 취소 요청을 받은 상태인 REFUND AUTHORIZED 상태를 가지는 것을 특징으로 할 수 있다.

[0030] 상기 결제 채널 네트워크들에 연관된 모든 사용자 단말들에게 준비 메시지를 생성 및 전송하는 명령은, 블록체인 목록, 블록체인 별 송신자 단말 공개 주소, 블록체인 별 수신자 단말 공개 주소의 정보를 포함하는 크로스체인 자산 거래 요청 메시지를 함께 전송하는 것을 특징으로 할 수 있다.

[0031] 상기 거래 승인 메시지 또는 환불 승인 메시지를 송신하는 명령은, 상기 REFUND AUTHORIZED 상태를 제외한 다른 상태에서, 모든 사용자 단말들로부터 자산 거래 COMMIT 메시지에 동의하는 메시지를 수신한 경우, 상기 거래 승인 메시지를 송신하고, 신뢰 실행 환경 상에서 송신자 단말의 크로스체인 자산 거래 예약금을 차감하며, 수신자 단말의 결제 채널 수신자 금액을 크로스체인 자산 거래 예약금만큼 증가시키도록 수행하는 명령을 더 포함할 수 있다.

[0032] 상기 거래 승인 메시지 또는 환불 승인 메시지를 송신하는 명령은, 상기 COMMITTED 상태를 제외한 상태에서, 하나 이상의 사용자 단말로부터 환불 메시지를 수신한 경우, 상기 크로스체인 자산 거래에 관여되는 모든 사용자 단말들에게 환불 승인 메시지를 송신하도록 하는 명령을 더 포함할 수 있다.

[0033] 상기 목적을 달성하기 위한 본 발명의 또 다른 실시예에 따른 서비스 제공자 서버를 활용하여 결제 채널 스마트 컨트랙트를 구비하는 동일한 블록체인 내의 멀티 홉 결제 방법으로서, 멀티 홉 결제 요청을 수신하는 단계; 상기 요청에 따라 블록체인 별로 결제 채널 네트워크를 개설하는 단계; 상기 결제 채널 네트워크에 연관된 모든 사용자 단말들에게 준비 메시지를 생성 및 전송하는 단계; 멀티 홉 결제와 관련된 모든 사용자 단말들로부터 상기 준비 완료 메시지를 수신하였는지 여부를 확인하고, 멀티 홉 결제와 관련된 모든 사용자 단말들에게 개별 결제 채널 네트워크 별로 커밋(COMMIT) 메시지와 함께 사용자 단말들로부터 수신한 모든 준비 완료 메시지들을 전송하는 단계; 및 상기 결제 채널 네트워크와 관련된 사용자 단말들에게 상기 결제 채널 네트워크와 관련된 사용자 단말들로부터 수신한 모든 커밋 완료 메시지와 함께 거래 승인(CONFIRM) 메시지를 생성 및 전송하는 단계를 포함한다.

[0034] 상기 사용자 단말은, 결제 진행 중 임의의 시점에 결제 채널 스마트 컨트랙트의 결제 채널 정산 모듈을 통하여 결제 채널 네트워크를 이탈할 수 있는 것을 특징으로 할 수 있다.

발명의 효과

[0035] 본 발명에 의하면, 서비스 제공자 서버는 신뢰 실행 환경을 활용하여 승인 메시지와 환불 승인 메시지 중 단 한 종류의 메시지만 생성할 수 있도록 강제함으로써, 서비스 제공자 서버가 임의의 사용자 단말에게는 승인 메시지를 생성 및 전송하고, 동시에 다른 사용자 단말에게는 환불 승인 메시지를 생성 및 전송할 수 없음을 강제할 수 있다. 이를 통하여, 본 발명은 특정 사용자 단말이 자산을 잃는 상황이 발생하지 않음을 보장할 수 있고, 크로스체인 자산 거래에 참여하는 모든 사용자 단말에게 안전성을 제공할 수 있는 장점이 있다.

[0036] 본 발명에 의하면, 신뢰 실행 환경을 활용하여 오프체인상 크로스체인 자산 거래를 제공함으로써, 크로스체인 자산 거래 지연 시간을 대폭 감소할 수 있고, 일대일 크로스체인 거래뿐만 다자간 거래도 지원할 수 있으므로, 거래 가능한 범위를 확대할 수 있는 장점이 있다. 또한, 사용자 단말은 스마트 컨트랙트에 단 한 번의 예치금(deposit)을 통해 단일 블록체인 자산 거래 처리 기능과 크로스체인 자산 거래 처리 기능을 동시에 이용 가능함으로써, 사용자 단말의 예치금액 비용을 절감할 수 있다.

[0037] 본 발명에 의하면, 복수의 블록체인 상 크로스체인 자산 거래를 제공할 수 있으며, 또한 동일 블록체인 내 멀티 홉 결제 서비스 역시 지원할 수 있어, 사용자에게 폭넓은 서비스 제공이 가능할 수 있다.

도면의 간단한 설명

[0038] 도 1은 본 발명의 일 실시예에 따른 두 개의 블록체인 환경상 크로스체인 자산 거래 시스템의 구성도이다.

도 2는 본 발명의 일 실시예에 따른 사용자 단말의 블록도이다.

도 3은 본 발명의 실시예에 따른 결제 채널 스마트 컨트랙트의 구성도이다.

도 4a는 본 발명의 실시예에 따른 서비스 제공자 서버의 모듈 구성을 보여주는 구성도이다.

도 4b는 본 발명의 실시예에 따른 서비스 제공자 서버의 블록도이다.

도 5a 는 본 발명의 실시예에 따른 크로스 체인 자산 거래가 진행되는 과정을 보여주는 순서도다.

도 5b는 본 발명의 실시예에 따른 크로스 체인 자산 거래가 진행되는 과정을 보여주는 순서도다.

도 6은 본 발명의 실시예에 따른 크로스 체인 자산 거래가 환불되는 과정을 보여주는 순서도다.

도 7은 본 발명의 실시예에 따른 크로스 체인 자산 거래 이후 결제 채널 종료 과정을 나타내는 순서도이다.

발명을 실시하기 위한 구체적인 내용

[0039] 본 발명은 다양한 변경을 가할 수 있고 여러 가지 실시예를 가질 수 있는 바, 특정 실시예들을 도면에 예시하고 상세하게 설명하고자 한다. 그러나, 이는 본 발명을 특정한 실시 형태에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다.

[0040] 제1, 제2 등의 용어는 다양한 구성요소들을 설명하는데 사용될 수 있지만, 상기 구성요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 사용된다. 예를 들어, 본 발명의 권리 범위를 벗어나지 않으면서 제1 구성요소는 제2 구성요소로 명명될 수 있고, 유사하게 제2 구성요소도 제1 구성요소로 명명될 수 있다. 및/또는 이라는 용어는 복수의 관련된 기재된 항목들의 조합 또는 복수의 관련된 기재된 항목들 중의 어느 항목을 포함한다.

[0041] 본 출원의 실시예들에서, “A 및 B 중에서 적어도 하나”는 “A 또는 B 중에서 적어도 하나” 또는 “A 및 B 중 하나 이상의 조합들 중에서 적어도 하나”를 의미할 수 있다. 또한, 본 출원의 실시예들에서, “A 및 B 중에서 하나 이상”은 “A 또는 B 중에서 하나 이상” 또는 “A 및 B 중 하나 이상의 조합들 중에서 하나 이상”을 의미할 수 있다.

[0042] 어떤 구성요소가 다른 구성요소에 "연결되어" 있다거나 "접속되어" 있다고 언급된 때에는, 그 다른 구성요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성요소가 존재할 수도 있다고 이해되어야 할 것이다. 반면에, 어떤 구성요소가 다른 구성요소에 "직접 연결되어" 있다거나 "직접 접속되어" 있다고 언급된 때에는, 중간에 다른 구성요소가 존재하지 않는 것으로 이해되어야 할 것이다.

[0043] 본 출원에서 사용한 용어는 단지 특정한 실시예를 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 출원에서, "포함하다" 또는 "가지다" 등의 용어는 명세서상에 기재된 특징, 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0044] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가지고 있다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥 상 가지는 의미와 일치하는 의미를 가진 것으로 해석되어야 하며, 본 출원에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[0045] 블록체인은 비허가형 블록체인 네트워크의 모든 참여 단말들이 합의 알고리즘을 수행함에 따라서, 참여하는 사용자 단말 수가 증가하면 증가할수록 합의 알고리즘 수행 시간 역시 늘어난다는 확장성 문제점을 가진다. 이러한 문제점을 해결하기 위한 방안으로, 오프체인(off-chain) 기법, 합의 알고리즘(consensus algorithm) 개선,

혹은 전체 블록체인 네트워크를 여러 개의 작은 독립적인 네트워크로 분할 하는 샤딩(sharding) 기법 등이 있다.

[0046] 특히, 오프체인 기법 중 결제 채널 기술은 두 사용자 단말 간 결제 채널을 개설하고, 개설한 결제 채널을 이용하여 블록체인 외부에서 거래(transaction)를 진행한다. 진행된 하나 이상의 거래는 두 당사자 간의 합의만을 요구하며, 최종 거래 결과만을 블록체인에 기록하는 기법이다. 따라서, 거래 빈도수가 많아지더라도 신속하게 처리할 수 있다는 장점이 있다. 또한, 두 사용자 단말 간 직접적으로 결제 채널이 개설되어 있지 않은 경우에는 멀티 홉 결제 처리 기법을 통해 자산 전송을 가능하도록 한다. 여기서, 멀티 홉 결제 처리는 결제 채널 네트워크를 기반으로 원자적(atomic)으로 동작한다. 결제 채널 네트워크는 송신자 단말의 결제 채널과 최종 수신자 단말의 결제 채널에 이르기까지 하나 이상의 중간 사용자 단말의 결제 채널을 포함하는, 결제 채널 경로를 의미한다.

[0047] 이하, 첨부한 도면들을 참조하여, 본 발명의 바람직한 실시예를 보다 상세하게 설명하고자 한다. 본 발명을 설명함에 있어 전체적인 이해를 용이하게 하기 위하여 도면상의 동일한 구성요소에 대해서는 동일한 참조부호를 사용하고 동일한 구성요소에 대해서 중복된 설명은 생략한다.

[0048] 도 1은 본 발명의 일 실시예에 따른 두 개의 블록체인 환경상 크로스체인 자산 거래 시스템의 구성도이다.

[0049] 여기서, 두 개의 블록체인들은 임의의 하나의 블록체인을 제1 블록체인이라 하고, 다른 하나의 블록체인을 제2 블록체인이라 할 수 있다. 상기 크로스체인의 자산 거래 시스템은 둘 이상의 블록체인들 간의 자산 거래에도 적용하다.

[0050] 도 1을 참조하면, 크로스체인 자산 거래 시스템(1000)은 사용자 단말들(100a~100f), 서비스 제공자 서버(200), 결제 채널 정보 데이터베이스(300), 제1 블록체인(400a), 제2 블록체인(400b), 제1 결제 채널 스마트 컨트랙트(500a), 제2 결제 채널 스마트 컨트랙트(500b), 제1 결제 채널 네트워크, 및 제2 결제 채널 네트워크(600a~600b)를 포함한다.

[0051] 상기 사용자 단말(100a~100f)들은 멀티 홉 결제 서비스 및 크로스체인 자산 거래 서비스를 이용할 수 있다. 상기 사용자 단말(100a~100f)들은 데스크탑, 또은 모바일 장치일 수 있다. 여기서, 본 발명에서의 사용자 단말(100a~100f)들은 프로토콜을 위배하는 악의적인 행위를 할 수 없도록 신뢰 실행 환경(120)을 탑재한 단말일 수 있다. 상기 신뢰 실행 환경(120)에 대해서는 도 2를 참조하여 상세히 후술한다.

[0052] 상기 사용자 단말(100a~100f)들은 블록체인 공개 주소(public address)와 개인 키(private key)를 가질 수 있다. 상기 사용자 단말(100a~100f)들은 상기 블록체인 공개 주소와 개인 키를 기반으로 상기 블록체인의 결제 채널 스마트 컨트랙트(500a, 500b)로의 사용자 트랜잭션 생성이나, 크로스체인 자산 거래 프로토콜을 위한 메시지를 생성할 때 서명을 할 수 있다. 상기 사용자 단말(100a~100f)들은 신뢰 실행 환경(120) 내부에서 결제 채널을 개설하며, 개설된 결제 채널을 통해 크로스체인 자산 거래 및 오프체인 멀티 홉 결제 서비스를 이용할 수 있다.

[0053] 여기서, 크로스체인 자산 거래를 하는 두 사용자가 있을 수 있고, 임의로 제1 사용자와 제2 사용자로 구분할 수 있다. 복수개의 블록체인에서는 동일한 사용자라도 다른 주소을 가질 수 있다. 상기 제1 블록체인 상에서의 제1 사용자의 사용자 단말은 제1 사용자 단말A(100a)라하고, 상기 제2 블록체인 상에서의 제1 사용자의 사용자 단말을 제1 사용자 단말B(100f)일 수 있다. 또한, 상기 제1 블록체인 상에서의 제2 사용자의 사용자 단말은 제2 사용자 단말A(100c)라하고, 상기 제2 블록체인 상에서의 제2 사용자의 사용자 단말을 제2 사용자 단말B(100d)일 수 있다.

[0054] 상기 사용자 단말(100a~100f)들은 결제 채널을 개설하기 위해 다음과 같은 동작을 수행할 수 있다. 상기 사용자 단말(100a~100f)들은 신뢰 실행 환경(120) 내부에서 블록체인 공개 주소(public address)와 개인 키(private key)를 생성할 수 있다. 여기서, 상기 사용자 단말(100a~100f)들은 신뢰 실행 환경(120)이 생성한 개인 키를 알 수 없다. 상기 사용자 단말(100a~100f)들은 결제 채널을 개설하고 싶은 타 사용자 단말의 신뢰 실행 환경이 생성한 블록체인 공개 주소와, 결제 채널에서 사용할 금액을 신뢰 실행 환경(120)으로 전달할 수 있다. 상기 신뢰 실행 환경(120)은 전달 받은 블록체인 공개 주소와 금액을 포함하는 트랜잭션을 생성하며, 결제 채널 컨트랙트로 전송할 수 있다. 상기 결제 채널 스마트 컨트랙트는 결제 채널 개설 완료 이벤트를 결제 채널과 관련된 제1 사용자 단말(100a, 100f) 및 제2 사용자 단말(100c, 100d)에게 전달하며, 상기 제1 사용자 단말(100a, 100f) 및 제2 사용자 단말(100c, 100d)은 해당 이벤트를 신뢰 실행 환경(120)에게 전달한다. 이후, 각 사용자 단말들의 신뢰 실행 환경(120)은 결제 채널 상태를 초기화할 수 있다.

[0055] 상기 서비스 제공자 서버(200)는 제1 블록체인(400a) 또는 제2 블록체인(400b)내에서 결제 채널 네크워크상 사

용자 간 자산 거래뿐 아니라, 복수의 블록체인 간, 예를 들어 제1 블록체인(400a)과 제2 블록체인(400b) 간의 사용자 사이 크로스체인 자산 거래를 중계하는 장치일 수 있다. 상기 서비스 제공자 서버(200)는 크로스체인 자산 거래에 관여되는 모든 사용자 단말(100a~100f)들의 크로스체인 자산 거래 과정을 동기적으로 제어함으로써, 사용자 단말(100a~100f)들의 개별적 결제 채널 상태 업데이트를 병렬적으로 진행할 수 있다. 따라서 상기 서비스 제공자 서버(200)는 크로스체인 자산 거래를 신속하고 효율적으로 지원할 수 있다.

[0056] 또한, 상기 서비스 제공자 서버(200)는 악의적인 행동을 차단하기 위해 신뢰 실행 환경(280b)을 기반으로 할 수 있다. 복수의 블록체인들 간에 진행되는 크로스체인 자산 거래 프로토콜 상에서, 사용자 단말(100a~100f)들은 크로스체인 자산 거래프로토콜이 종료되기 전까지는 상기 결제 채널 스마트 컨트랙트(500)로 정산 및 분쟁 조정 요청을 할 수 없을 수 있다.

[0057] 상기 서비스 제공자 서버(200)는 제1 블록체인(400a)과 제2 블록체인(400b)들별 결제 채널 네트워크를 구성하며, 각각의 결제 채널 네트워크별로 사용자 단말(100a~100f)들 간 크로스체인 자산 거래를 지원할 수 있다. 상기 서비스 제공자 서버(200)는 결제 채널 네트워크상 송신자 단말은 수신자 단말에 이르는 중간 단말들의 결제 채널을 통해 수신자 단말로 자산을 송신할 수 있다. 도 1을 참조하여 예를 들면, 제1 결제 채널 네트워크의 결제 송신자 단말인, 제1 사용자 단말A(100a)는 중간 사용자 단말(100b)을 통하여 수신자 단말인 제2 사용자 단말A(100c)에 자산을 송신할 수 있다.

[0058] 본 명세서에서 크로스체인 자산 거래는, 특정 블록체인 내의 결제 채널 네트워크상 결제 채널을 통해 자산을 수신한 사용자 단말은 반드시 타 블록체인에서 결제 채널을 통해 다른 사용자 단말에게 자산을 송신하는 것을 의미할 수 있다. 즉, 본 발명의 시스템에서는 자산 거래 과정을 원자적으로 처리하는 것을 뜻할 수 있다.

[0059] 상기 서비스 제공자 서버(200)는 위와 같은 방식으로 하나의 동일 블록체인 상 결제 채널 네트워크를 구성하여 사용자 단말들 간 멀티 홉 결제 서비스 역시 지원 가능할 수 있다.

[0060] 상기 결제 채널 정보 데이터베이스(300)는 결제 채널 정보를 수신 및 저장한다. 상기 결제 채널 정보는 제1 블록체인(400a) 상 존재하는 제1 결제 채널 스마트 컨트랙트(500a) 및 제2 블록체인(400b) 상 존재하는 제2 결제 채널 스마트 컨트랙트(500b)가 유지, 관리하는 모든 사용자 단말들의 결제 채널 정보일 수 있다.

[0061] 상기 결제 채널 정보 데이터베이스(300)는 상기 블록체인별 결제 채널 스마트 컨트랙트(500a, 500b)가 유지 관리하는 모든 사용자 단말(100a~100f)들의 결제 채널 정보를 저장할 수 있다. 따라서, 상기 서비스 제공자 서버(200)는 결제 채널 네트워크 구성 시, 상기 결제 채널 정보 데이터베이스(300) 에 저장된 결제 채널 정보를 바탕으로 생성할 수 있다. 또한, 상기 서비스 제공자 서버(200)는 블록체인상 결제 채널 정보가 업데이트 되는 이벤트를 지속적으로 모니터링하면서 해당 정보를 상기 결제 채널 정보 데이터베이스(300)에 저장할 수 있다.

[0062] 상기 제1 블록체인(400a)은 상기 제1 스마트 컨트랙트(500a), 및 상기 사용자 단말들(100a~100c)을 포함하는 제1 결제 채널 네트워크(600a)를 포함하고, 상기 제2 블록체인(400b)은 상기 제2 스마트 컨트랙트(500b), 및 상기 사용자 단말들(100d~100f)을 포함하는 제2 결제 채널 네트워크(600b)를 포함할 수 있다.

[0063] 상기 제1 블록체인(400a) 및 제2 블록체인(400b)은 분산 컴퓨팅 기반의 데이터 위변조 방지 기술 및 분산 데이터 저장 기술을 의미한다. 상기 제1 블록체인(400a)의 사용자 단말(100a~100c)들은 크로스체인 자산 거래를 위해 제1 블록체인(400a)에서 제1 결제 채널 네트워크(600a)를 형성하고, 제2 블록체인(400b)의 사용자 단말(100d~100f)들 역시 제2 블록체인(400b)에서 제2 결제 채널 네트워크(600b)를 구성할 수 있다.

[0064] 상기 결제 채널 스마트 컨트랙트(500a, 500b)들은 상기 사용자 단말 (100a~100f)들의 요청에 따라 결제 채널 정보를 생성하고, 사용자 보증금을 관리함으로써, 결제 채널 종료시 블록체인 상 보증금을 기반으로 정산하는 과정 및 결제 채널 정산 과정에서의 사용자들간 분쟁 조정을 담당할 수 있다.

[0065] 상기 결제 채널 스마트 컨트랙트(500a, 500b)들은 블록체인 상에서 동작하는 프로그램일 수 있다. 상기 결제 채널 스마트 컨트랙트(500a, 500b)들은 사용자 단말(100)의 초기 결제 채널 정보를 유지 및 관리할 수 있다. 상기 결제 채널 스마트 컨트랙트(500a, 500b)들은 관리하는 정보를 바탕으로, 향후 멀티 홉 결제에 관여되는 여러 사용자 단말(100a~100f)들 간 분쟁이 발생하였을 경우 일관된 방식으로 분쟁을 조정할 수 있다.

[0066] 여기서, 일관된 방식이란, 멀티 홉 결제에 관여하는 모든 사용자 단말(100a~100f)들의 결제 채널 상태가 멀티 홉 결제 완료 이후의 상태를 가진 채로 종료하거나, 혹은 사용자 단말(100a~100f)들의 결제 채널 상태가 멀티 홉 결제 이전의 상태를 가진 채로 종료하는 것을 의미할 수 있다.

[0067] 상기 결제 채널 네트워크(600a~600b)들은 한 쌍의 사용자 단말에 대해 생성되는 결체 채널을 기반으로 직접 연

결되지 않는 사용자 단말간 결제 채널을 연결하는 임의의 경로로 구성될 수 있다.

[0068] 도 2는 본 발명의 일 실시예에 따른 사용자 단말의 구성도이다.

[0069] 도 2를 참조하면, 상기 사용자 단말(100)은 신뢰 실행 환경(Trusted Execution Environment, TEE)(120)을 탑재한 단말을 의미할 수 있다. 상기 신뢰 실행 환경(120)은 미리 정의한 동작만을 수행함으로써, 프로그램 로직의 무결성을 보장할 수 있다. 따라서, 상기 신뢰 실행 환경(120)은 악의적인 사용자 단말의 행동을 차단할 수 있다.

[0070] 상기 신뢰 실행 환경(120)은 블록체인 공개 주소(public address)와 개인 키(private key)를 생성한 후 신뢰 실행 환경(120) 내부에 저장할 수 있다. 따라서, 사용자 단말(100)의 비신뢰 실행 환경(110)에서는 신뢰 실행 환경(120)이 생성한 개인 키(private key) 정보를 알 수 없을 수 있다. 상기 사용자 단말(100)은 블록체인 사용자 트랜잭션 생성이나, 크로스체인 자산 거래 프로토콜을 위한 메시지를 생성할 때 반드시 개인키로 서명하며, 상기 신뢰 실행 환경(120) 내부에서 메시지 및 트랜잭션들에 대한 서명을 개인키를 기반으로 진행할 수 있다.

[0071] 여기서, 상기 사용자 단말(100)의 비신뢰 실행 환경(110)에 설치된 운영체제 소프트웨어는 외부 환경으로의 네크워크 통신을 담당할 수 있다. 상기 사용자 단말(100)의 크로스체인 자산 거래 프로토콜 통신 정보는 모두 신뢰 실행 환경(120)으로 전달할 수 있다. 상기 사용자 단말(100)의 크로스체인 자산 거래 프로토콜과 관련한 모든 동작은 신뢰 실행 환경(120) 내부에서 처리할 수 있다.

[0072] 도 3은 본 발명의 일 실시예에 따른 결제 채널 스마트 컨트랙트의 구성도이다.

[0073] 상기 결제 채널 스마트 컨트랙트(500)는 결제 채널 생성 모듈(510), 결제 채널 종료 모듈(520), 및 결제 채널 정산 모듈(530)을 포함한다.

[0074] 상기 결제 채널 생성 모듈(510)은 상기 사용자 단말(100)의 예치금(deposit)을 바탕으로 결제 채널을 생성하는 모듈이다. 결제 채널 생성 이후, 상기 결제 채널 생성 모듈(510)은 생성한 결제 채널에 관련된 둘 이상의 사용자 단말(100)들에게 결제 채널 생성 이벤트를 알릴 수 있다. 상기 둘 이상의 사용자 단말(100)들은 해당 이벤트를 신뢰 실행 환경(120)으로 전달할 수 있고, 상기 신뢰 실행 환경(120)은 결제 채널을 초기화할 수 있다.

[0075] 상기 결제 채널 종료 모듈(520)은 상기 결제 채널 생성 모듈(510)을 통해 생성했던 결제 채널을 종료하는 모듈이다. 상기 둘 이상의 사용자 단말(100)들 간 결제 채널 사용 결과를 바탕으로 둘 이상의 사용자 단말(100)들에게 기존 예치금을 분배하고 결제 채널을 종료할 수 있다.

[0076] 상기 결제 채널 정산 모듈(530)은 결제 채널 네트워크상 멀티 홉 결제를 진행 중인 사용자 단말(100)이 해당 결제 채널 네트워크를 이탈하는 경우 발생하는 분쟁을 조정할 수 있다. 결제 채널 네트워크를 이탈하는 사용자 단말(100)이 존재하는 경우, 멀티 홉 결제 관련 모든 사용자 단말 간 진행 중인 결제 채널 상태가 불일치할 수 있다. 이때, 멀티 홉 결제를 진행 중인 결제 채널 네트워크의 모든 사용자 단말(100)은 결제 채널이 멀티 홉 결제가 완료된 상태가 되거나, 혹은 멀티 홉 결제 진행 이전의 상태가 되어야 한다. 이러한 분쟁이 발생하는 경우, 상기 결제 채널 정산 모듈(530)이 모든 결제 채널 정보 및 예치금을 유지 관리함으로써, 멀티 홉 결제 관련된 모든 사용자 단말(100)의 결제 채널을 일관된 상태로 종료할 수 있다.

[0077] 예를 들면, 최초 정산 요청자의 결제 채널 상태가 멀티 홉 결제 준비 상태라면, 이후의 분쟁 조정을 요청한 사용자 단말(100)은 결제 채널 상태(멀티 홉 결제 준비 또는 멀티 홉 결제 커밋 상태 등)에 상관없이 멀티 홉 결제 수행 이전의 상태로 결제 채널이 종료될 수 있다. 반면에, 최초 정산 요청자의 결제 채널 상태가 멀티 홉 결제 커밋 상태라면, 이후, 분쟁 조정을 요청한 사용자 단말(100)은 결제 채널 상태(멀티 홉 결제 준비 혹은 멀티 홉 결제 커밋 상태)에 상관없이 멀티 홉 결제 수행 이후의 상태로 결제 채널이 종료될 수 있다.

[0078] 도 4a는 본 발명의 실시예에 따른 서비스 제공자 서버의 모듈 구성을 보여주는 구성도이고, 도 4b는 본 발명의 실시예에 따른 서비스 제공자 서버의 블록도이다.

[0079] 도 4a를 참조하면, 상기 서비스 제공자 서버(200)는 크로스체인 자산 거래 준비 모듈(210), 크로스체인 자산 거래 커밋 모듈(220), 크로스체인 자산 거래 승인 모듈(230), 크로스체인 자산 거래 환불 승인 모듈(240), 계약 정보 동기화 모듈(250), 자산 거래 경로 계산 모듈(260), 및 멀티 홉 결제 모듈(270)을 포함할 수 있다.

[0080] 상기 크로스체인 자산 거래 준비 모듈(210)은 제1 결제 채널 네트워크(600a) 및 제2 결제 채널 네트워크(600b)들의 모든 사용자 단말(100a~100f)들에게 크로스체인 자산 거래 참여 여부를 요청 및 응답을 처리하는 모듈일 수 있다. 상기 크로스체인 자산 거래 준비 모듈(210)은 크로스체인 자산 거래 준비(PREPARE) 메시지를 생성, 전

송 및 응답 메시지를 검증할 수 있다. 여기서, 상기 메시지 생성은 신뢰 실행 환경(280b) 내부에서 이루어질 수 있다.

[0081] 상기 비신뢰 실행 환경(280a)은 생성한 크로스체인 자산 거래 준비 메시지를 제1 결제 채널 네트워크(600a) 및 제2 결제 채널 네트워크(600b)들의 존재하는 모든 사용자 단말(100a~100f)들에게 전송할 수 있다. 모든 사용자 단말(100a~100f)들의 비신뢰 실행 환경(110)은 크로스체인 자산 거래 준비 메시지를 신뢰 실행 환경(120)으로 주입하여 크로스체인 자산 거래 준비 관련 동작을 수행할 수 있다. 크로스체인 자산 거래 참여 의사에 따라 사용자 단말(100a~100f)들의 신뢰 실행 환경(120)은 준비 완료 메시지를 생성 및 서명하며 비신뢰 실행 환경(110)으로 전송할 수 있다. 이후 사용자 단말(100a~100f)들은 해당 메시지를 상기 서비스 제공자 서버(200)로 전송할 수 있다. 상기 서비스 제공자 서버(200)의 상기 크로스체인 자산 거래 준비 모듈(210)은 수신한 준비 완료 메시지를 검증한다.

[0082] 상기 크로스체인 자산 거래 커밋 모듈(220)은 제1 결제 채널 네트워크(600a) 및 제2 결제 채널 네트워크(600b)들의 모든 사용자 단말(100a~100f)들에게 결제 채널 커밋 요청 및 처리하는 모듈일 수 있다. 상기 크로스체인 자산 거래 커밋 모듈(220)은 크로스체인 자산 거래 커밋(COMMIT) 메시지를 생성 및 전송할 수 있고, 이에 대한 응답 메시지를 검증할 수 있다. 여기서, 메시지 생성은 신뢰 실행 환경(280b) 내부에서 이루어질 수 있다. 상기 비신뢰 실행 환경(280a)은 생성한 크로스체인 자산 거래 커밋 메시지를 제1 결제 채널 네트워크(600a) 및 제2 결제 채널 네트워크(600b)들에 존재하는 모든 사용자 단말(100a~100f)들에게 전송할 수 있다. 이때, 상기 크로스체인 자산 거래 준비 모듈(210)에서 처리한 제1 결제 채널 네트워크(600a)의 사용자 단말(100a~100c) 및 제2 결제 채널 네트워크(600b)의 사용자 단말(100d~100f)들의 준비 완료 메시지도 함께 전송할 수 있다. 모든 사용자 단말(100a~100f)들의 비신뢰 실행 환경(110)은 크로스체인 자산 거래 커밋 메시지 및 다른 사용자 단말의 준비 완료 메시지를 상기 신뢰 실행 환경(120)으로 전송하여 해당 메시지들을 모두 검증한 후 크로스체인 자산 거래 커밋 관련 동작을 진행할 수 있다. 크로스체인 자산 거래 커밋 동작 결과에 따라 사용자 단말(100a~100f)의 상기 신뢰 실행 환경(120)은 커밋 완료 메시지를 생성 및 서명하며 비신뢰 실행 환경(110)으로 전송할 수 있다. 이후 모든 사용자 단말(100a~100f)들은 커밋 완료 메시지를 서비스 제공자 서버(200)의 크로스체인 자산 거래 커밋 모듈(220)로 전송할 수 있다. 상기 크로스체인 자산 거래 커밋 모듈(220)은 수신한 커밋 완료 메시지를 검증할 수 있다.

[0083] 상기 크로스체인 자산 거래 승인 모듈(230)은 제1 결제 채널 네트워크(600a) 및 제2 결제 채널 네트워크(600b)의 모든 사용자 단말(100a~100f)들에게 크로스체인 자산 거래 승인 메시지를 전송하는 모듈일 수 있다. 상기 크로스체인 자산 거래 승인 모듈(230)은 크로스체인 자산 거래 승인 메시지를 생성 및 전송할 수 있고, 이에 대한 응답 메시지를 검증할 수 있다. 여기서, 메시지 생성은 신뢰 실행 환경(280b) 내부에서 이루어질 수 있다. 상기 비신뢰 실행 환경(280a)은 생성한 크로스체인 자산 거래 승인 메시지를 제1 결제 채널 네트워크(600a) 및 제2 결제 채널 네트워크(600b)들에 존재하는 모든 사용자 단말(100a~100f)들에게 전송할 수 있다. 이때, 상기 크로스체인 자산 거래 커밋 모듈(220)에서 처리한 다른 사용자 단말(100a~100c, 100d~100f)들의 커밋 완료 메시지도 함께 전송할 수 있다. 모든 사용자 단말(100a~100f)들의 비신뢰 실행 환경(110)은 크로스체인 자산 거래 승인 메시지 및 커밋 메시지를 신뢰 실행 환경(120)으로 전송하여 해당 메시지들을 검증 후 크로스체인 자산 거래 승인 관련 동작을 진행할 수 있다. 크로스체인 자산 거래 승인 동작 결과에 따라 모든 사용자 단말(100a~100f)들의 신뢰 실행 환경(120)은 승인 완료 메시지를 생성하며 비신뢰 실행 환경(110)으로 전송할 수 있다. 모든 사용자 단말(100a~100f)들은 정상적으로 크로스체인 자산 거래가 완료되었음을 확인하며, 크로스체인 자산 거래는 마무리될 수 있다.

[0084] 상기 크로스체인 자산 거래 환불 승인 모듈(240)은 제1 결제 채널 네트워크(600a) 및 제2 결제 채널 네트워크(600b)의 모든 사용자 단말(100a~100f)들에게 크로스체인 자산 거래 환불 승인 메시지를 전송하는 모듈일 수 있다. 상기 크로스체인 자산 거래 환불 승인 모듈(240)은 크로스체인 자산 거래 환불 승인 메시지를 생성 및 전송할 수 있고, 이에 대한 응답 메시지를 검증할 수 있다. 여기서, 메시지 생성은 신뢰 실행 환경(280b) 내부에서 이루어질 수 있다. 상기 비신뢰 실행 환경(280a)은 생성한 크로스체인 자산 거래 환불 승인 메시지를 제1 결제 채널 네트워크(600a) 및 제2 결제 채널 네트워크(600b)들상에 존재하는 모든 사용자 단말(100a~100f)들에게 전송한다. 모든 사용자 단말(100a~100f)들의 비신뢰 실행 환경(110)은 크로스체인 자산 거래 환불 승인 메시지를 신뢰 실행 환경(120)으로 전송하여 크로스체인 자산 거래 환불 승인 관련 동작을 진행할 수 있다. 크로스체인 자산 거래 환불 승인 동작 결과에 따라 모든 사용자 단말(100a~100f)의 신뢰 실행 환경(120)은 환불 승인 완료 메시지를 생성하며 비신뢰 실행 환경(110)으로 전송할 수 있다. 상기 사용자 단말(100)은 크로스체인 자산 거래와 관련된 결제 채널이 정상적으로 크로스체인 자산 거래 진행 이전 상태로 전이되었음을 확인하며, 크로스체인

자산 거래는 마무리될 수 있다.

[0085] 상기 계약 정보 동기화 모듈(250)은 상기 결제 채널 스마트 컨트랙트(500)가 유지 관리하는 사용자 단말(100a~100f)들의 결제 채널 정보를 동기화하는 모듈일 수 있다.

[0086] 상기 자산 거래 경로 계산 모듈(260)은 결제 채널 정보를 바탕으로 최적의 결제 채널 네트워크를 구성하는 모듈일 수 있다. 여기서, 최적의 결제 채널 네트워크란 송신자 사용자 단말(100)로부터 수신자 사용자 단말(100)까지의 결제 채널 경로가 가장 짧은 경로를 의미할 수 있다.

[0087] 상기 멀티 홉 결제 모듈(270)은 동일 블록체인 상 결제 채널 네트워크를 기반으로 멀티 홉 결제 서비스를 지원하는 모듈일 수 있다. 상기 멀티 홉 결제 서비스는 멀티 홉 결제 준비, 커밋, 승인의 세 단계로 이루어질 수 있다, 멀티 홉 결제 진행 중인 사용자 단말(100)은 아무 시점에나 결제 채널 정산 모듈(530)을 통해 결제 채널 네트워크를 이탈할 수 있다.

[0088] 여기서, 자산 거래는 복수의 블록체인에서 복수의 사용자 사이에 발생하는 자산의 교환을 의미할 수 있고, 멀티 홉 결제는 동일한 블록체인 내에서 하나의 사용자가 다른 사용자에게 자산을 송금하는 것을 의미할 수 있다.

[0089] 도 5a 및 5b는 본 발명의 실시예에 따른 크로스 체인 자산 거래가 진행되는 과정을 보여주는 순서도다.

[0090] 도 5a를 참조하면, 상기 서비스 제공자 서버(200)는 거래소 및 자산 교환 시스템으로부터 크로스체인 자산 거래 요청을 수신할 수 있다. 크로스체인 자산 거래를 지원하기 위하여, 상기 서비스 제공자 서버(200)는 상기 결제 채널 정보 데이터베이스(300)에 결제 채널 정보를 요청할 수 있다.

[0091] 상기 서비스 제공자 서버(200)는 상기 결제 채널 정보 데이터베이스(300)로부터 얻은 결제 채널 정보를 바탕으로 제1 결제 채널 네트워크(600a) 및 제2 결제 채널 네트워크(600b)를 구성할 수 있다. 상기 제1 결제 채널 네트워크(600a) 및 제2 결제 채널 네트워크(600b) 별로 개별적인 크로스체인 자산 거래 준비 메시지를 각각 생성할 수 있다. 즉, 본 실시예에 따르면 상기 서비스 제공자 서버(200)는 두 개의 크로스체인 자산 거래 준비 메시지를 생성할 수 있다. 여기서, 상기 크로스체인 자산 거래 준비 메시지는 상기 크로스체인 자산 거래 준비 모듈(210)을 통해 생성될 수 있다.

[0092] 상기 서비스 제공자 서버(200)는 생성한 각각의 크로스체인 준비 메시지를 대응되는 결제 채널 네트워크(600a~600b)들에 속하는 모든 사용자 단말(100)들에게 전송할 수 있다. 상기 크로스체인 준비 메시지를 수신한 모든 사용자 단말(100)들의 비신뢰 실행 환경(110)은 해당 메시지를 신뢰 실행 환경(120)으로 전달할 수 있다. 상기 사용자 단말(100)들의 신뢰 실행 환경(120)은 크로스체인 자산 거래 준비 메시지를 검증한 후 해당 결제 채널 상태를 준비 완료 상태로 변경할 수 있다. 또한, 상기 신뢰 실행 환경(120)은 준비 완료 메시지를 생성 및 서명한 후 비신뢰 실행 환경(110)에게 전송할 수 있다. 상기 모든 사용자 단말(100)은 신뢰 실행 환경(120)이 전달한 준비 완료 메시지를 상기 서비스 제공자 서버(200)에 전송할 수 있다.

[0093] 상기 서비스 제공자 서버(200)는 크로스체인 자산 거래와 관련된 모든 사용자 단말(100)들로부터 준비 완료 메시지를 수신할 때까지 대기할 수 있다. 또한, 상기 서비스 제공자 서버(200)는 준비 완료 메시지를 수신할 때마다 메시지를 검증하여, 크로스체인 자산 거래에 동의하지 않는 사용자 단말(100)들의 존재 여부를 확인할 수 있다. 상기 크로스체인 자산 거래 준비 모듈(210)은 상기 준비 완료 메시지 검증을 수행할 수 있다.

[0094] 도 5b를 참조하면, 크로스체인 자산 거래와 관련된 모든 사용자 단말(100)로부터 준비 완료 메시지를 수신하면, 상기 서비스 제공자 서버(200)는 신뢰 실행 환경(120)을 통해 크로스체인 자산 거래 커밋 메시지를 생성할 수 있다. 여기서, 크로스체인 자산 거래 커밋 메시지 생성은 크로스체인 자산 거래 커밋 모듈(220)을 통해 생성할 수 있다. 상기 크로스체인 자산 거래 커밋 모듈(220)은 결제 채널 네트워크(600a~600b)별로 상기 크로스체인 자산 거래 커밋 메시지를 생성할 수 있다. 상기 크로스체인 자산 거래 커밋 모듈(220)은 상기 생성된 크로스체인 자산 거래 커밋 메시지들을 결제 채널 네트워크 별(600a~600b) 사용자 단말(100)들에게 전송할 수 있다. 이때, 동일한 결제 채널 네트워크(600a~600b) 사용자 단말로부터 수신한 준비 완료 메시지도 함께 전송할 수 있다.

[0095] 크로스체인 자산 거래와 관련된 모든 사용자 단말(100)들은 수신된 크로스체인 자산 거래 커밋 메시지와 준비 완료 메시지를 비신뢰 실행 환경(110)에서 신뢰 실행 환경(120)으로 전달할 수 있다. 상기 신뢰 실행 환경(120)은 크로스체인 자산 거래 커밋 메시지 및 준비 완료 메시지를 검증한 후 결제 채널 상태 정보를 커밋 완료로 변경할 수 있다. 또한, 상기 신뢰 실행 환경(120)은 커밋 완료 메시지를 생성 및 서명하여 비신뢰 실행 환경(110)으로 전송할 수 있다. 상기 사용자 단말(100)의 비신뢰 실행 환경(110)은 전달받은 메시지를 상기 서비스 제공자 서버(200)에게 전송할 수 있다. 상기 서비스 제공자 서버(200)는 모든 사용자 단말(100)로부터 커밋 완

료 메시지를 수신할 때까지 대기하며, 메시지를 수신할 때마다 크로스체인 자산 거래 커밋 모듈(220)을 통해 해당 메시지를 검증할 수 있다.

[0096] 모든 사용자 단말(100)로부터 커밋 완료 메시지를 수신한다면, 상기 서비스 제공자 서버(200)는 신뢰 실행 환경을 이용하여 승인 메시지를 생성 및 서명할 수 있다. 상기 서비스 제공자 서버(200)는 생성한 승인 메시지를 크로스체인 자산 거래와 관련된 모든 사용자 단말(100)들에게 전송할 수 있다. 이때, 동일한 결제 채널 네트워크(600a~600b) 사용자 단말들로부터 수신한 커밋 완료 메시지도 함께 전송할 수 있다. 승인 및 타 사용자 단말의 커밋 완료 메시지를 수신한 모든 사용자 단말(100)은 신뢰 실행 환경(120)으로 해당 메시지들을 전달할 수 있고, 상기 신뢰 실행 환경(120)은 메시지 검증 후 결제 채널 정보 및 금액을 업데이트할 수 있다.

[0097] 상기의 과정들을 통해서, 크로스체인 자산 거래는 완료될 수 있다.

[0098] 도 6은 본 발명의 실시예에 따른 크로스 체인 자산 거래가 환불되는 과정을 보여주는 순서도다.

[0099] 상기 크로스체인 자산 거래 환불 요청 메시지는 모든 사용자 단말(100a~100f)들이 생성 가능할 수 있다. 다만, 이하의 본 발명의 일 실시예에서는 사용자 단말(100a)이 진행 중인 크로스체인 자산 거래를 취소하고자 하는 경우를 예를 들어 설명한다.

[0100] 상기 사용자 단말(100a)이 진행 중인 크로스체인 자산 거래를 취소하고자 하는 경우, 상기 사용자 단말(100a)의 신뢰 실행 환경(120)이 크로스체인 자산 거래 환불 요청 메시지를 생성할 수 있다. 이때, 상기 환불 요청 메시지는 크로스체인 자산 거래 인스턴스의 번호를 포함할 수 있다. 상기 사용자 단말(100a)은 생성된 환불 요청 메시지를 상기 서비스 제공자 서버(200)에 전송할 수 있다. 상기 서비스 제공자 서버(200)는 수신한 환불 메시지를 상기 신뢰 실행 환경(280b)으로 주입할 수 있고, 상기 신뢰 실행 환경(280b)은 해당 크로스체인 자산 거래 인스턴스의 상태가 COMMITTED와 일치하는지 확인할 수 있다.

[0101] 상기 크로스체인 자산 거래 인스턴스의 상태가 COMMITTED가 아니라면 REFUND AUTHORIZED 상태로 업데이트하며 환불 완료 메시지를 생성할 수 있다. 상기 서비스 제공자 서버(200)는 환불 완료 메시지를 해당 크로스체인 자산 거래와 관련되는 모든 사용자 단말(100a~100f)들에게 전송할 수 있다. 상기 환불 완료 메시지를 수신한 모든 사용자 단말(100a~100f)들의 신뢰 실행 환경(120)은 사용자 환불 완료 메시지를 검증할 수 있고, 결제 채널의 상태를 크로스체인 자산 거래 진행 이전으로 되돌릴 수 있다.

[0102] 여기서, 상기 크로스체인 자산 거래에 참여하는 모든 사용자 단말(100a~100f)들 중 단 하나의 사용자 단말(100a)이라도 환불을 원하는 경우에는 나머지 사용자 단말(100b~100f)들이 거래가 지속되기를 원하더라도, 상기 서비스 제공자 서버(200)는 일방적으로 환불 단계를 진행할 수 있다. 이를 통하여, 환불을 원하는 사용자 단말(100a)이 원하지 않는 거래를 수행함으로써 발생하는 금전적인 손실을 방지할 수 있다. 또한, 사용자 단말(100)이 크로스체인 자산 거래에 참여하였으나 거래가 완료되기 이전에 환불을 요청하여 매번 진행되는 거래를 악의적으로 취소시키더라도, 얻을 수 있는 금전적인 보상이 없을 수 있다. 따라서 본 발명에서는, 사용자 단말(100)은 아무런 실익이 없는, 참여 중인 크로스체인 자산 거래를 악의적으로 취소하지 않음을 가정할 수 있다.

[0103] 도 7은 본 발명의 일 실시예에 따른 크로스체인 자산 거래 이후 결제 채널 종료 과정을 나타내는 순서도다.

[0104] 본 발명의 일 실시예에 따르면 사용자 단말(100a)은 다른 사용자 단말(100b)과의 개설된 결제 채널이 있다. 여기서, 하나의 사용자 단말은 제1 사용자 단말(100a), 다른 하나의 사용자 단말은 제2 사용자 단말(100b)라 한다. 이때, 해당 결제 채널이 크로스체인 자산 거래에 사용 중이 아니라면, 제1 사용자 단말(100a) 또는 제2 사용자 단말(100b) 중 어느 하나의 사용자 단말은 결제 채널 종료를 상기 결제 채널 스마트 컨트랙트(500)로 요청할 수 있다. 본 발명의 일 실시예에서는 제1 사용자 단말(100a)이 상기 결제 채널 종료 요청 메시지를 생성하고 결제 채널 스마트 컨트랙트(500)로 상기 결제 채널 종료 요청 메시지를 전송하는 것으로 설명한다.

[0105] 상기 결제 채널 스마트 컨트랙트(500)는 결제 채널에서 사용된 금액 결과를 계산한 후, 계산 결과를 토대로 해당 결제 채널의 초기 보증금에서 제1 사용자 단말(100a) 및 제2 사용자 단말(100b)에게 분배하며 결제 채널을 종료할 수 있다. 이후, 결제 채널 종료 이벤트를 제1 사용자 단말(100a) 및 제2 사용자 단말(100b)에게 알릴 수 있다. 또한, 결제 채널 종료 이벤트를 상기 서비스 제공자 서버(200)에게 전송하며, 상기 서비스 제공자 서버(200)는 종료된 결제 채널 정보를 상기 결제 채널 정보 데이터베이스(300)로 전달하여 최신 결제 채널 정보를 유지 관리할 수 있다.

[0106] 다시 도 5a 내지 도 7을 참조하면, 복수의 블록체인으로 구성된 상기 크로스체인의 자산거래 과정을 아래와 같이 상세히 설명할 수 있다.

[0107] 크로스체인 자산 거래와 관련하여 사용자 단말(100)의 결제 채널 상태는 총 세 가지 IDLE, PREPARED, COMMITTED를 가질 수 있다. 상기 IDLE 상태는 결제 채널이 사용되지 않는 상태일 수 있다. 상기 PREPARED 상태는 결제 채널을 크로스체인 자산 거래에 사용하기 위해 준비 완료됨을 의미하는 상태일 수 있다.

[0108] 상기 PREPARED 상태는 결제 채널 송신자 가용 금액에서 송금액만큼 차감하며, 차감한 금액만큼 크로스체인 자산 거래 예약금을 증가시킬 수 있다. 상기 COMMITTED 상태는 크로스체인 자산 거래에 관여되는 모든 사용자 단말(100a~100b)들이 결제 채널 사용을 동의(준비)하였으며, 최종적으로 크로스체인 자산 거래가 완료되기를 대기하는 상태일 수 있다. 상기 사용자 단말(100a~100b)들은 크로스체인 자산 거래가 완료되면 상기 COMMITTED 상태에서 IDLE 상태로 변경될 수 있다.

[0109] 크로스체인 자산 거래를 지원하기 위해, 상기 서비스 제공자 서버(200)의 신뢰 실행 환경은 크로스체인 자산 거래 인스턴스를 생성 및 관리할 수 있다. 상기 크로스체인 자산 거래 인스턴스는 총 네 개의 NONE, PREPARED, COMMITTED, REFUND AUTHORIZED 상태를 가질 수 있다.

[0110] 상기 NONE 상태는 크로스체인 자산 거래 인스턴스가 생성 및 초기화된 상태일 수 있다. 상기 PREPARED 상태는 크로스체인 자산 거래에 관여되는 모든 사용자 단말(100a~100b)들이 결제 채널 사용에 동의했음을(준비) 나타내는 상태일 수 있다. 상기 COMMITTED 상태는 크로스체인 자산 거래에 관여되는 모든 사용자 단말(100a~100b)들의 결제 채널의 상태가 커밋 완료임을 나타내는 상태일 수 있다. 상기 REFUND AUTHORIZED는 특정 사용자 단말(100)로부터 진행 중이던 크로스체인 자산 거래 취소 요청을 받은 상태일 수 있다. 따라서, 크로스체인 자산 거래 인스턴스의 상태가 REFUND AUTHORIZED인 경우, 상기 서비스 제공자 서버(200)는 크로스체인 자산 거래와 관련되는 모든 사용자 단말(100a~100b)들의 결제 채널을 크로스체인 자산 거래 이전 상태로 되돌릴 수 있도록 환불 단계를 진행할 수 있다.

[0111] 서비스 제공자 서버(200)는 하나 이상의 블록체인 사용자 단말들의 결제 채널 정보를 유지 관리할 수 있다. 상기 서비스 제공자 서버(200)가 거래소와 같은 외부 자산 교환 서비스 및 시스템으로부터 크로스체인 자산 거래 요청을 수신하면, 다음과 같은 방식으로 거래를 지원할 수 있다. 상기 크로스체인 자산 거래 요청은 블록체인 목록, 블록체인 별 송신자 단말 공개 주소, 블록체인 별 수신자 단말 공개 주소의 집합으로 구성될 수 있다. 여기서, 모든 사용자 단말(100a~100b)들의 결제 채널은 IDLE 상태이며 상기 서비스 제공자 서버(200)의 가용성은 보장됨을 가정할 수 있다.

[0112] 상기 서비스 제공자 서버(200)는 상기 결제 채널 정보 데이터베이스(300)로부터 사용자 단말 간 결제 채널 정보를 요청 및 수신하며, 해당 정보를 기반으로 결제 채널 네트워크를 구성할 수 있다. 이때, 크로스체인 자산 거래에 포함되는 복수 블록체인 목록 별로 결제 채널 네트워크를 구성할 수 있다.

[0113] 예를 들어, 복수의 블록체인으로 제1 블록체인(400a)과 제2 블록체인(400b)이 있을 수 있다. 여기서, 제1 블록체인(400a)에서는 송신자 단말로 제1 사용자 단말A(100a)과 수신자 단말로 제2 사용자 단말A(100c)가 존재할 수 있다. 또한, 제2 블록체인(400b)에서는 송신자 단말로 제2 사용자 단말B(100d)와 수신자 단말로 제1 사용자 단말B(100f)가 존재할 수 있다.

[0114] 여기서, 제1 블록체인(400a) 및 제2 블록체인(400b)에서 두 사용자 단말, 즉, 제1 사용자 단말(100a) 및 제2 사용자 단말(100d)은 각각의 블록체인에 속하는 공개 주소를 가질 수 있다. 예를 들면, 제1 사용자 단말은 제1 블록체인(400a)에서 제1 사용자 단말A(100a)일 수 있고, 제2 블록체인(400b)에서는 제1 사용자 단말B(100f)일 수 있다. 또한, 제2 사용자 단말은 제1 블록체인(400a)에서 제2 사용자 단말A(100c)일 수 있고, 제2 블록체인(400b)에서는 제2 사용자 단말B(100d)일 수 있다.

[0115] 상기 서비스 제공자 서버(200)는 제1 블록체인(400a)의 송신자 단말인 제1 사용자 단말A(100a)가 수신자 단말인 제2 사용자 단말A(100c)에 자산을 전송할 수 있도록 제1 결제 채널 네트워크(600a)를 구성할 수 있고, 제2 블록체인(400b)의 송신자 단말인 제2 사용자 단말B(100d)가 수신자 단말인 제1 사용자 단말B(100f)에게 자산을 전송할 수 있도록 제2 결제 채널 네트워크(600b)를 구성할 수 있다.

[0116] 상기 서비스 제공자 서버(200)가 블록체인 별로 결제 채널 네트워크를 구성한 이후, 서비스 제공자 서버의 신뢰 실행 환경(280b)은 크로스체인 자산 거래 인스턴스를 생성할 수 있다. 상기 크로스체인 자산 거래 인스턴스는 NONE 상태로 초기화될 수 있다. 또한, 상기 크로스체인 자산 거래 인스턴스는 크로스체인 자산 거래 식별자, 크로스체인 자산 거래에 관여되는 모든 사용자 단말(100a~100f)들의 공개 주소, 그리고 송금액을 포함할 수 있다.

[0117] 상기 서비스 제공자 서버(200)는 각 결제 채널 네트워크와 연관된 모든 사용자 단말(100a~100f)들에게 전송되는

준비(PREPARE) 메시지를 신뢰 실행 환경(280b) 내부에서 생성 및 서명할 수 있다. 이때, 상기 준비 메시지는 상기의 생성했던 크로스체인 자산 거래 식별자와 결제 채널 네트워크와 연관된 모든 사용자 단말(100a~100f)들의 공개 주소와 채널 정보, 송금액을 포함할 수 있다. 상기 서비스 제공자 서버(200)는 각각의 결제 채널 네트워크별로 준비 메시지를 생성 및 서명 완료하면, 결제 채널 네트워크와 연관된 사용자 단말들에게 서명한 준비 메시지를 전송할 수 있다.

[0118] 예를 들면, 상기 서비스 제공자 서버의 신뢰 실행 환경(280b)은 크로스체인 자산 거래 식별자, 제1 블록체인(400a)의 송신자 단말인 제1 사용자 단말A(100a)와 수신자 단말인 제2 사용자 단말A(100c)에게 이르는 중간 단말인 사용자 단말(100b)을 포함한 모든 사용자 단말(100a, 100b, 100c)의 공개 주소 및 결제 채널 정보, 송금액을 포함하여 준비 메시지를 생성할 수 있다. 또한, 동일한 방식으로, 상기 서비스 제공자 서버(200)는 크로스체인 자산 거래 식별자, 제2 블록체인(400b)의 송신자 단말인 제2 사용자 단말B(100d)와 수신자 단말인 제1 사용자 단말B(100f)에게 이르는 중간 단말인 사용자 단말(100e)을 포함한 모든 사용자 단말(100d, 100e, 100f)의 공개 주소 및 결제 채널 정보, 송금액을 포함하여 준비 메시지를 생성할 수 있다. 즉, 상기 서비스 제공자 서버의 신뢰 실행 환경(280b)은 거래에 참여하는 블록체인의 수와 같은 두 개의 준비 메시지를 생성할 수 있다.

[0119] 상기 서비스 제공자 서버(200)로부터 준비 메시지를 수신한 모든 사용자 단말(100a~100f)들은 상기 수신된 준비 메시지를 검증할 수 있다. 또한, 크로스체인 자산 거래 인스턴스 식별자가 이전에 사용된 적이 없었는지 확인할 수 있다. 상기 모든 사용자 단말(100a~100f)들은 상기 준비 메시지가 포함하는 모든 사용자 단말(100a~100f)들과 결제 채널 정보, 송금액을 기반으로 크로스체인 자산 거래 준비 여부를 선택할 수 있다. 모든 사용자 단말(100a~100f)들이 크로스체인 자산 거래 진행 준비에 동의하면, 결제 채널 네트워크상 모든 사용자 단말(100a~100f)들의 신뢰 실행 환경(120)은 결제 채널의 송신자 가용 금액에서 송금액만큼 차감하며, 차감한 금액을 크로스체인 자산 거래 예약금으로 저장할 수 있다. 또한, 상기 크로스체인 자산 거래에 사용된 결제 채널은 IDLE에서 PREPARED 상태로 전이될 수 있다. 상기 사용자 단말(100)의 신뢰 실행 환경(120)은 준비 완료(PREPARED) 메시지를 생성 및 서명할 수 있다. 상기 사용자 단말(100)은 상기 준비 완료 메시지를 상기 서비스 제공자 서버(200)에게 전송할 수 있다.

[0120] 상기 서비스 제공자 서버(200)는 사용자 단말(100)로부터 준비 완료 메시지 수신하게 되면, 수신된 준비 완료 메시지를 검증하며, 모든 사용자 단말(100a~100f)들로부터 준비 완료 메시지를 수신할 때까지 대기할 수 있다. 모든 사용자 단말(100a~100f)들로부터 준비 완료 메시지를 수신 완료하면, 상기 서비스 제공자 서버의 신뢰 실행 환경(280b)은 해당 크로스체인 자산 거래 인스턴스의 상태를 NONE에서 PREPARED로 변경할 수 있다.

[0121] 상기 서비스 제공자 서버(200)는 크로스체인 자산 거래와 관련된 모든 사용자 단말(100a~100f)들로부터 준비 완료 메시지를 수신하게 되면, 상기 준비 메시지 생성 단계와 동일한 방식으로 신뢰 실행 환경(280b) 내부에서 커밋(COMMIT) 메시지를 생성 및 서명할 수 있다. 상기 서비스 제공자 서버의 신뢰 실행 환경(280b)이 각각의 결제 채널 네트워크 별로 커밋 메시지를 생성 및 서명 완료하면, 상기 서비스 제공자 서버(200)는 결제 채널 네트워크와 연관된 모든 사용자 단말(100a~100f)들에게 서명한 커밋 메시지를 전송할 수 있다. 여기서, 상기 서비스 제공자 서버(200)는 커밋 메시지 뿐만 아니라 각 결제 채널 네트워크와 관련된 모든 사용자 단말(100a~100f)들의 준비 완료 메시지를 함께 전송할 수 있다.

[0122] 상기 서비스 제공자 서버(200)로부터 커밋 메시지와 결제 채널 네트워크와 관련된 모든 사용자 단말(100a~100f)들의 준비 완료 메시지를 수신한 사용자 단말의 신뢰 실행 환경(120)은 상기 수신한 메시지들을 검증할 수 있다. 상기 사용자 단말의 신뢰 실행 환경(120)은 상기 커밋 메시지가 포함하는 모든 사용자 단말(100a~100f)들과 채널 정보, 송금액을 기반으로 크로스체인 자산 거래 커밋 여부를 선택할 수 있다. 상기 사용자 단말(100)이 크로스체인 자산 거래 커밋에 동의하면, 사용자 단말(100)은 결제 채널 상태를 PREPARED에서 COMMITTED로 변경할 수 있다. 상기 사용자 단말의 신뢰 실행 환경(120)은 커밋 완료(COMMITTED) 메시지를 생성하고 서명할 수 있다. 상기 사용자 단말(100)은 상기 생성된 커밋 완료 메시지를 상기 서비스 제공자 서버(200)에게 전송할 수 있다.

[0123] 상기 서비스 제공자 서버(200)는 상기 사용자 단말(100a~100f)들로부터 커밋 완료 메시지 수신할 때마다 해당 메시지를 검증할 수 있고, 상기 모든 사용자 단말(100a~100f)들로부터 커밋 완료 메시지를 수신할 때까지 대기할 수 있다. 상기 서비스 제공자 서버(200)가 상기 모든 사용자 단말(100a~100f)들로부터 상기 커밋 완료 메시지를 수신 완료하면, 상기 서비스 제공자 서버의 신뢰 실행 환경(280b)은 크로스체인 자산 거래 인스턴스의 상태를 PREPARED에서 COMMITTED로 변경할 수 있다.

[0124] 크로스체인 자산 거래와 관련된 모든 사용자 단말(100a~100f)들로부터 커밋 완료 메시지를 수신한 서비스 제공자 서버(200)는 커밋 메시지 생성 단계와 동일한 방식으로 신뢰 실행 환경(280b) 내부에서 승인(CONFIRM) 메시

지를 생성 및 서명할 수 있다. 상기 서비스 제공자 서버(200)는 각각의 결제 채널 네트워크 별로 승인 메시지를 생성 및 서명 완료하면, 각 결제 채널 네트워크와 연관된 모든 사용자 단말(100a~100f)들에게 서명한 승인 메시지를 전송할 수 있다. 이때, 상기 서비스 제공자 서버(200)는 승인 메시지뿐만 아니라 각 결제 채널 네트워크에 관련된 모든 사용자 단말(100a~100f)들의 커밋 완료 메시지를 함께 전송할 수 있다.

[0125] 상기 서비스 제공자 서버(200)로부터 승인 메시지와 결제 채널 네트워크상 모든 사용자 단말(100a~100f)들의 커밋 완료 메시지를 수신한 사용자 단말의 신뢰 실행 환경(120)은 해당 메시지들을 검증할 수 있다. 이후, 상기 사용자 단말의 신뢰 실행 환경(120)은 승인 메시지가 포함하는 사용자 단말의 공개 주소와 채널 정보, 송금액을 기반으로 크로스체인 자산 거래 승인 여부를 선택할 수 있다. 상기 사용자 단말이 크로스체인 자산 거래 승인에 동의하면, 결제 채널 네트워크에 포함되는 각각의 결제 채널 송신자 및 수신자 단말(100a, 100c, 100d, 100f)의 신뢰 실행 환경(120)은 저장했던 크로스체인 자산 거래 예약금을 차감하며, 추가적으로 수신자 단말의 신뢰 실행 환경(120)은 결제 채널 수신자 금액의 양을 크로스체인 자산 거래 예약 금액만큼 증가시킬 수 있다. 또한, 송신자 및 수신자의 신뢰 실행 환경(120) 모두 결제 채널의 상태를 COMMITTED에서 IDLE로 변경하며, 크로스체인 자산 거래는 종료될 수 있다.

[0126] 본 발명에서는 사용자 단말(100)의 결제 채널이 크로스체인 자산 거래 채널에 사용 중일 때(PREPARED 혹은 COMMITTED 상태), 크로스체인 자산 거래에 관련된 다른 사용자 단말이 오프라인 상태가 되어 더 이상 크로스체인 자산 거래를 진행할 수 없는 경우, 사용자 단말(100)은 상기 서비스 제공자 서버(200)에게 환불 단계 진행을 요청할 수 있다.

[0127] 상기 크로스체인의 자산 거래 환불은 다음과 같은 단계를 포함할 수 있다. 상기 사용자 단말의 신뢰 실행 환경(120)은 환불 메시지를 생성 및 서명하여 상기 서비스 제공자 서버(200)에게 상기 환불 메시지를 전송할 수 있다. 상기 환불 메시지를 수신 및 검증한 상기 서비스 제공자 서버의 신뢰 실행 환경(280b)은 해당 크로스체인 자산 거래 인스턴스의 상태(NONE 혹은 PREPARED)를 REFUND AUTHORIZED로 변경할 수 있다.

[0128] 상기 서비스 제공자 서버의 신뢰 실행 환경(280b)은 환불 승인 메시지를 생성 및 서명 후 크로스체인 자산 거래에 관련된 모든 사용자 단말(100a~100f)들에게 전송할 수 있다.

[0129] 상기 환불 승인 메시지를 수신한 사용자 단말의 신뢰 실행 환경(120)은 사용 중이던 결제 채널의 상태(PREPARED 또는 COMMITTED)를 IDLE로 변경하며 결제 채널 금액을 이전 상태로 되돌릴 수 있다.

[0130] 전술한 바와 같이, 상기 서비스 제공자 서버의 신뢰 실행 환경(280b)이 관리하는 크로스체인 자산 거래 인스턴스는 총 네 개의 NONE, PREPARED, COMMITTED, REFUND AUTHORIZED 상태를 가질 수 있다.

[0131] 상기 COMMITTED 상태는 모든 사용자 단말(100a~100f)들이 크로스체인 자산 거래를 커밋 완료했다는 것을 의미하고, 상기 서비스 제공자 서버의 신뢰 실행 환경(280b)은 이미 승인 메시지를 생성 및 전송했음을 의미할 수 있다. 상기 승인 메시지를 수신한 사용자 단말(100)은 크로스체인 자산 거래를 완료할 수 있으므로, 상기 서비스 제공자 서버의 신뢰 실행 환경(280b)은 크로스체인 자산 거래 인스턴스가 COMMITTED 상태일 때, 사용자 단말(100)로부터 환불 메시지를 수신한다면 환불 단계를 진행하지 않는다.

[0132] 이와 유사하게, 크로스체인 자산 거래 인스턴스가 REFUND AUTHORIZED 상태일 때는, 상기 서비스 제공자 서버(200)가 모든 사용자 단말(100a~100f)들로부터 커밋 완료 메시지를 수신하더라도 COMMITTED 상태로 변경되어서는 안 된다. 상기 환불 승인 메시지를 수신한 사용자 단말(100)은 결제 채널 금액을 이전 상태로 되돌릴 수 있기 때문이다. 즉, 상기 서비스 제공자 서버의 신뢰 실행 환경(280b)은 승인 메시지와 환불 승인 메시지 종류 중 어느 하나의 메시지만 생성하도록 강제한다.

[0133] 본 발명은 상기와 같이, 상기 서비스 제공자 서버(200)가 복수 개의 블록체인 상 자산 거래가 안전하게 이루어질 수 있도록 지원할 수 있다. 또한, 상기 서비스 제공자 서버(200)는 전술한 크로스체인 자산 거래(inter)뿐만 아니라 동일 블록체인 내 오프체인 멀티 홉 결제(inter) 역시 지원 가능할 수 있다.

[0134] 크로스체인 자산 거래에서 서비스 제공자 서버(200)는, 복수의 블록체인 별로 결제 채널 네트워크를 각각 구성할 수 있고, 각 결제 채널 네트워크에 포함되는 모든 사용자 단말(100a~100f)들의 결제 채널 상태를 단계별로 동기화함으로써 안전한 크로스체인 자산 거래를 지원할 수 있다.

[0135] 이와 유사하게 동일 블록체인 내 오프체인 멀티 홉 결제 처리에서 서비스 제공자 서버(200)는, 동일 블록체인 내의 결제 채널 네트워크를 단 하나만 구성하여, 해당 결제 채널 네트워크에 포함되는 모든 사용자 단말(100)들의 결제 채널 상태를 단계별로 동기화함으로써 동일 블록체인 오프체인 멀티 홉 결제 서비스를 안전하게 지원할

수 있다.

[0136] 크로스체인 자산 거래와 동일 블록체인 오프체인 멀티 홉 결제 처리 간 주요한 차이점은, 크로스체인 자산 거래에 참여 중인 사용자 단말(100)은 상기 결제 채널 스마트 컨트랙트(500)에 채널 정산 요청을 할 수 없다는 점이다. 상기 크로스체인 자산 거래에 참여 중인 사용자 단말(100)은 반드시 환불 단계를 거쳐서, 결제 채널이 크로스체인 자산 거래에 사용되지 않은 시점에만 상기 결제 채널 스마트 컨트랙트(500)에 채널 정산 요청이 가능하다. 상기 결제 채널 스마트 컨트랙트(500)는 동일 블록체인 상 사용자 단말(100)의 예치금과 결제 채널 정보만 유지 관리하므로, 다른 블록체인의 사용자 단말을 관리할 수 없기 때문이다.

[0137] 예를 들면, 제1 결제 채널 스마트 컨트랙트(500a)는 제1 블록체인(400a) 상의 사용자 단말(100a~100c)의 예치금과 결제 채널 정보를 유지 관리하고, 제2 결제 채널 스마트 컨트랙트(500b)는 제2 블록체인(400b) 상의 사용자 단말(100d~100f)의 예치금과 결제 채널 정보를 유지 관리할 수 있다. 따라서, 제1 결제 채널 스마트 컨트랙트(500a)는 제2 블록체인(400b)의 사용자 단말(100d~100f)을 관리할 수 없다. 따라서 상기 크로스체인 자산 거래에 참여 중인 사용자 단말(100)은 반드시 환불 단계를 거쳐서, 결제 채널이 크로스체인 자산 거래에 사용되지 않은 시점에만 상기 결제 채널 스마트 컨트랙트(500)에 채널 정산 요청이 가능하다.

[0138] 그러나, 사용자 단말(100)의 결제 채널이 동일 블록체인 멀티 홉 결제 처리에 사용 중이라면 아무 시점에 상관없이 결제 채널 스마트 컨트랙트(500)로 채널 정산 및 분쟁 조정을 요청할 수 있다. 상기 결제 채널 스마트 컨트랙트(500)는 해당 멀티 홉 결제에 관여되는 모든 사용자 단말(100)의 결제 채널 상태를 일관성 있게 종료할 수 있기 때문이다. 여기서, 일관성이 의미하는 것은 모든 사용자 단말의 결제 채널 상태가 멀티 홉 결제가 성공적으로 이루어진 상태이거나, 혹은 멀티 홉 결제가 이루어지지 않은 상태를 의미할 수 있다.

[0139] 본 발명의 실시예에 따른 방법의 동작은 컴퓨터로 읽을 수 있는 기록매체에 컴퓨터가 읽을 수 있는 프로그램 또는 코드로서 구현하는 것이 가능하다. 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 시스템에 의해 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록장치를 포함한다. 또한 컴퓨터가 읽을 수 있는 기록매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어 분산 방식으로 컴퓨터로 읽을 수 있는 프로그램 또는 코드가 저장되고 실행될 수 있다.

[0140] 또한, 컴퓨터가 읽을 수 있는 기록매체는 롬(rom), 램(ram), 플래시 메모리(flash memory) 등과 같이 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치를 포함할 수 있다. 프로그램 명령은 컴파일러(compiler)에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터(interpreter) 등을 사용해서 컴퓨터에 의해 실행될 수 있는 고급 언어 코드를 포함할 수 있다.

[0141] 본 발명의 일부 측면들은 장치의 문맥에서 설명되었으나, 그것은 상응하는 방법에 따른 설명 또한 나타낼 수 있고, 여기서 블록 또는 장치는 방법 단계 또는 방법 단계의 특징에 상응한다. 유사하게, 방법의 문맥에서 설명된 측면들은 또한 상응하는 블록 또는 아이템 또는 상응하는 장치의 특징으로 나타낼 수 있다. 방법 단계들의 몇몇 또는 전부는 예를 들어, 마이크로프로세서, 프로그램 가능한 컴퓨터 또는 전자 회로와 같은 하드웨어 장치에 의해(또는 이용하여) 수행될 수 있다. 몇몇의 실시예에서, 가장 중요한 방법 단계들의 하나 이상은 이와 같은 장치에 의해 수행될 수 있다.

[0142] 실시예들에서, 프로그램 가능한 로직 장치(예를 들어, 필드 프로그래머블 게이트 어레이)가 여기서 설명된 방법들의 기능의 일부 또는 전부를 수행하기 위해 사용될 수 있다. 실시예들에서, 필드 프로그래머블 게이트 어레이는 여기서 설명된 방법들 중 하나를 수행하기 위한 마이크로프로세서와 함께 작동할 수 있다. 일반적으로, 방법들은 어떤 하드웨어 장치에 의해 수행되는 것이 바람직하다.

[0143] 이상 본 발명의 바람직한 실시예를 참조하여 설명하였지만, 해당 기술 분야의 숙련된 당업자는 하기의 특허 청구의 범위에 기재된 본 발명의 사상 및 영역으로부터 벗어나지 않는 범위 내에서 본 발명을 다양하게 수정 및 변경시킬 수 있음을 이해할 수 있을 것이다.

부호의 설명

[0144] 100 사용자 단말

110 비신뢰 실행 환경

120 신뢰 실행 환경

200 서비스 제공자 서버

210 크로스 체인 자산 거래 준비 모듈

220 크로스 체인 자산 거래 커밋 모듈

230 크로스 체인 자산 거래 승인 모듈

240 크로스 체인 자산 거래 환불 승인 모듈

250 계약 정보 동기화 모듈

260 결제 경로 계산 모듈

270 멀티 홉 결제 모듈

280a 비신뢰 실행 환경

280b 신뢰 실행 환경

300 결제 채널 정보 데이터베이스

400 블록체인

500 결제 채널 스마트 컨트랙트

510 결제 채널 생성 모듈 520 결제 채널 종료 모듈

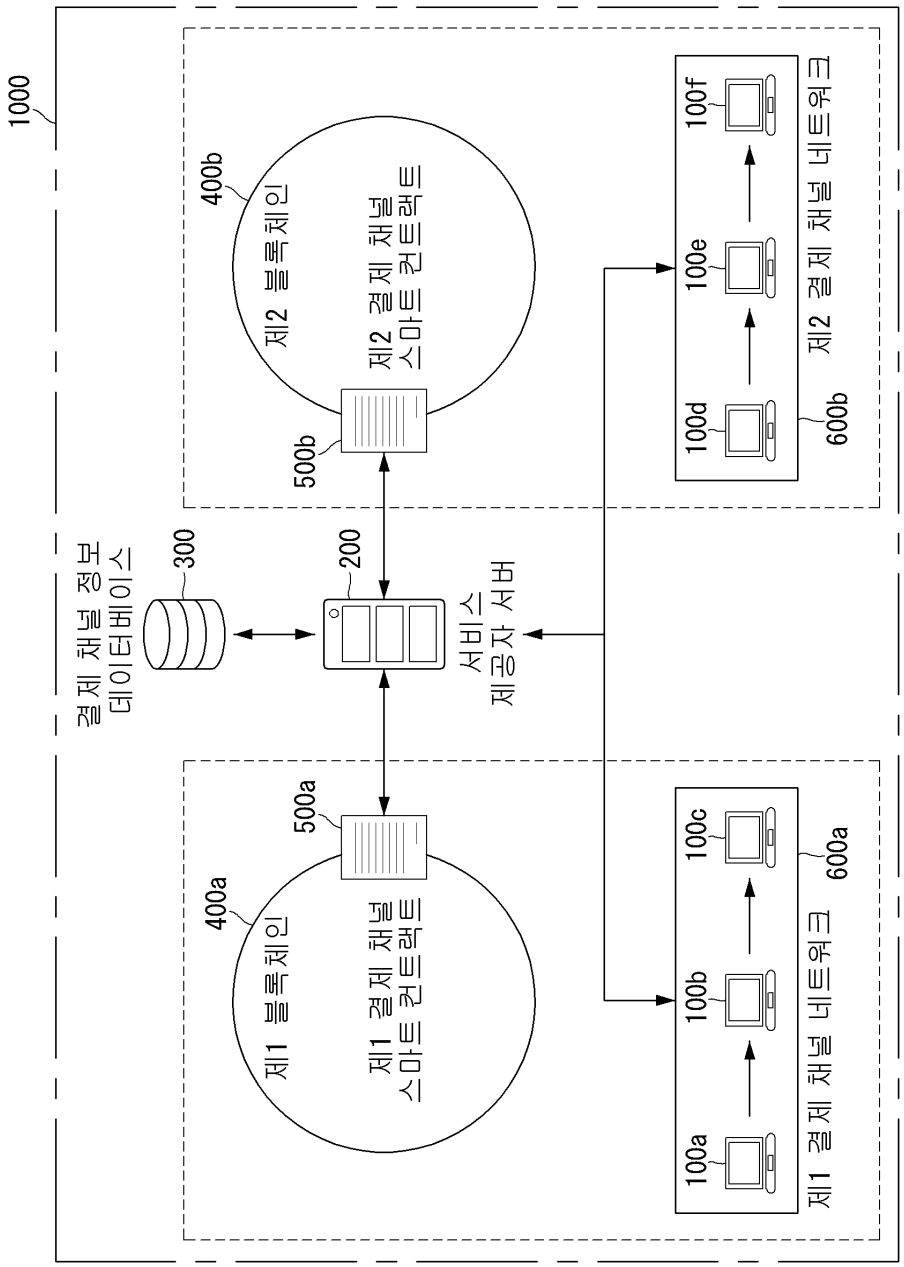
530 결제 채널 정산 모듈 600 결제 채널 네트워크

700 거래소 및 자산 교환 시스템

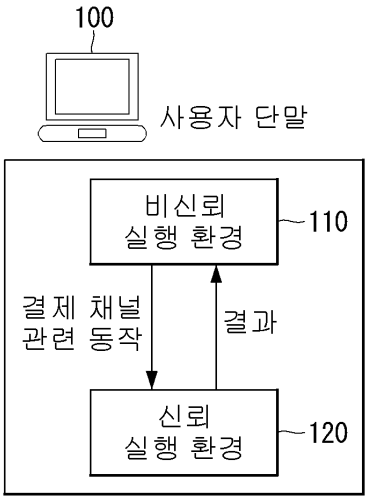
1000 크로스체인 자산관리 시스템

도면

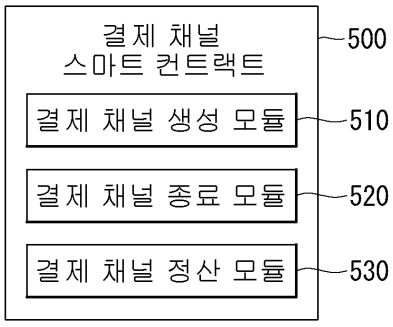
도면1


1000
400b
제2 블록체인
제2 결제 채널
스마트 컨트랙트
500b
100d
100e
100f
600b
제2 결제 채널 네트워크
300
결제 채널 정보
데이터베이스
200
서비스
제공자 서버
500a
400a
제1 블록체인
제1 결제 채널
스마트 컨트랙트
100a
100b
100c
600a
제1 결제 채널 네트워크

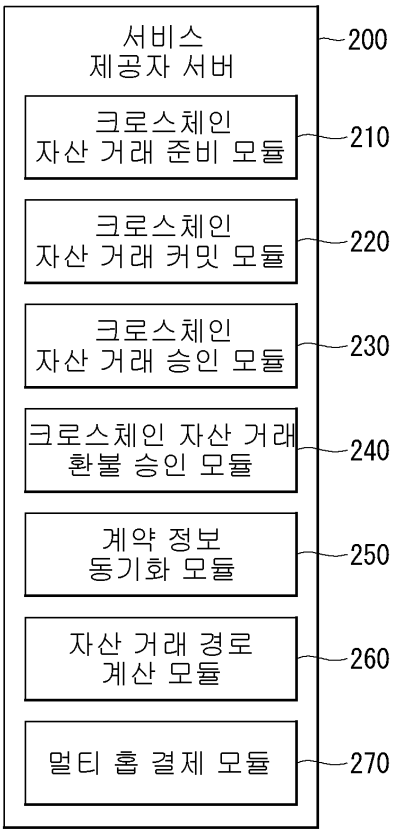
도면2


100
사용자 단말
비신뢰
실행 환경
110
결제 채널
관련 동작
결과
신뢰
실행 환경
120

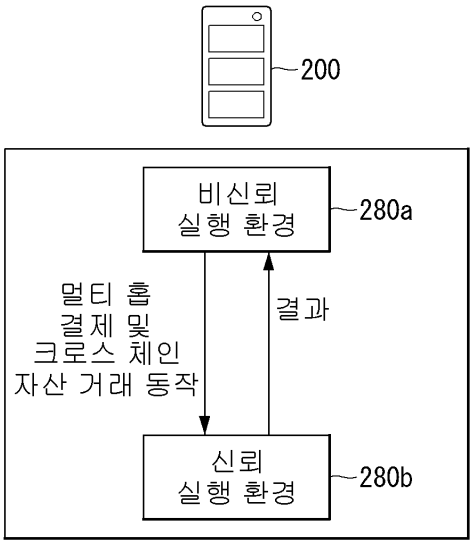
도면3


결제 채널
스마트 컨트랙트
500
결제 채널 생성 모듈
510
결제 채널 종료 모듈
520
결제 채널 정산 모듈
530

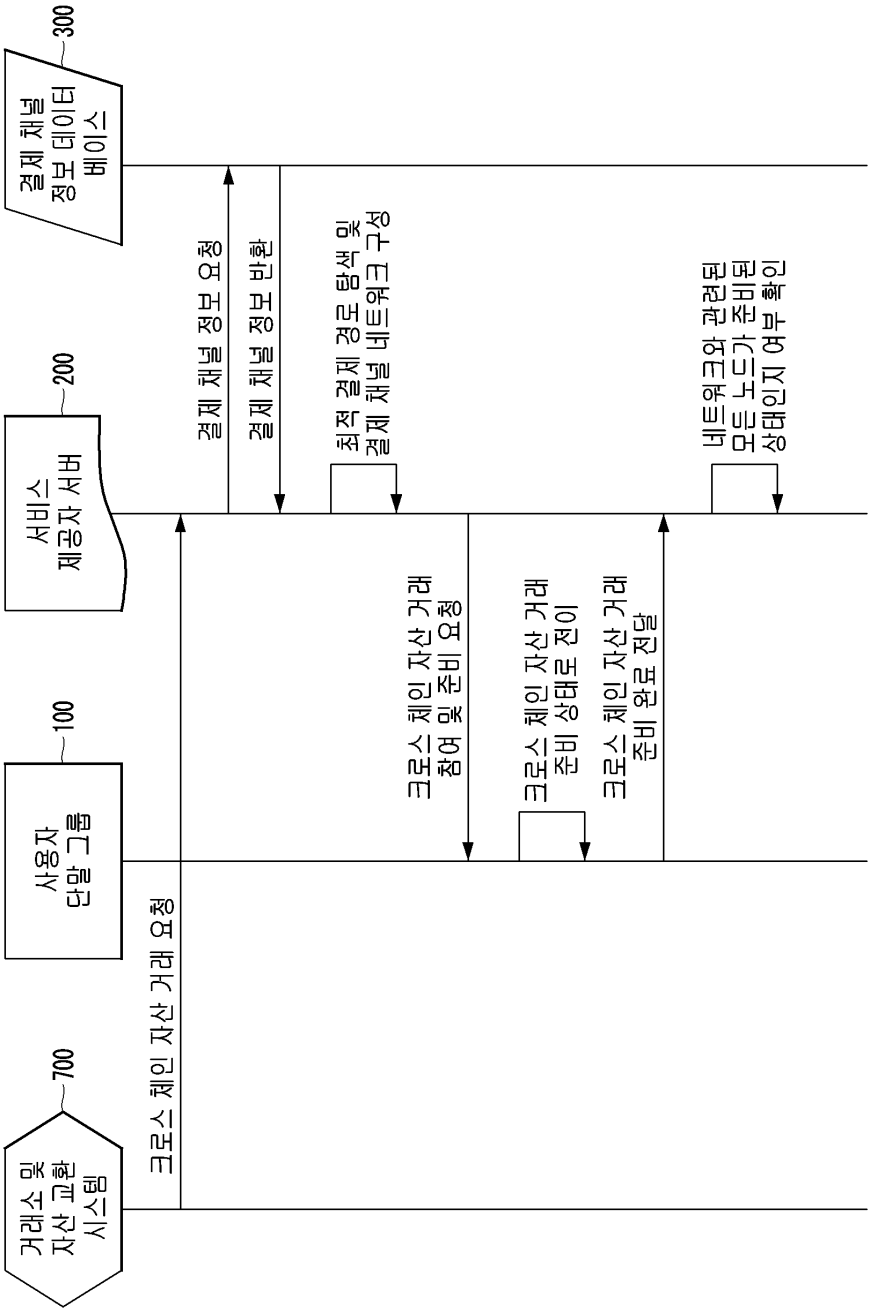
도면4a


서비스
제공자 서버
200
크로스체인
자산 거래 준비 모듈
210
크로스체인
자산 거래 커밋 모듈
220
크로스체인
자산 거래 승인 모듈
230
크로스체인 자산 거래
환불 승인 모듈
240
계약 정보
동기화 모듈
250
자산 거래 경로
계산 모듈
260
멀티 홉 결제 모듈
270

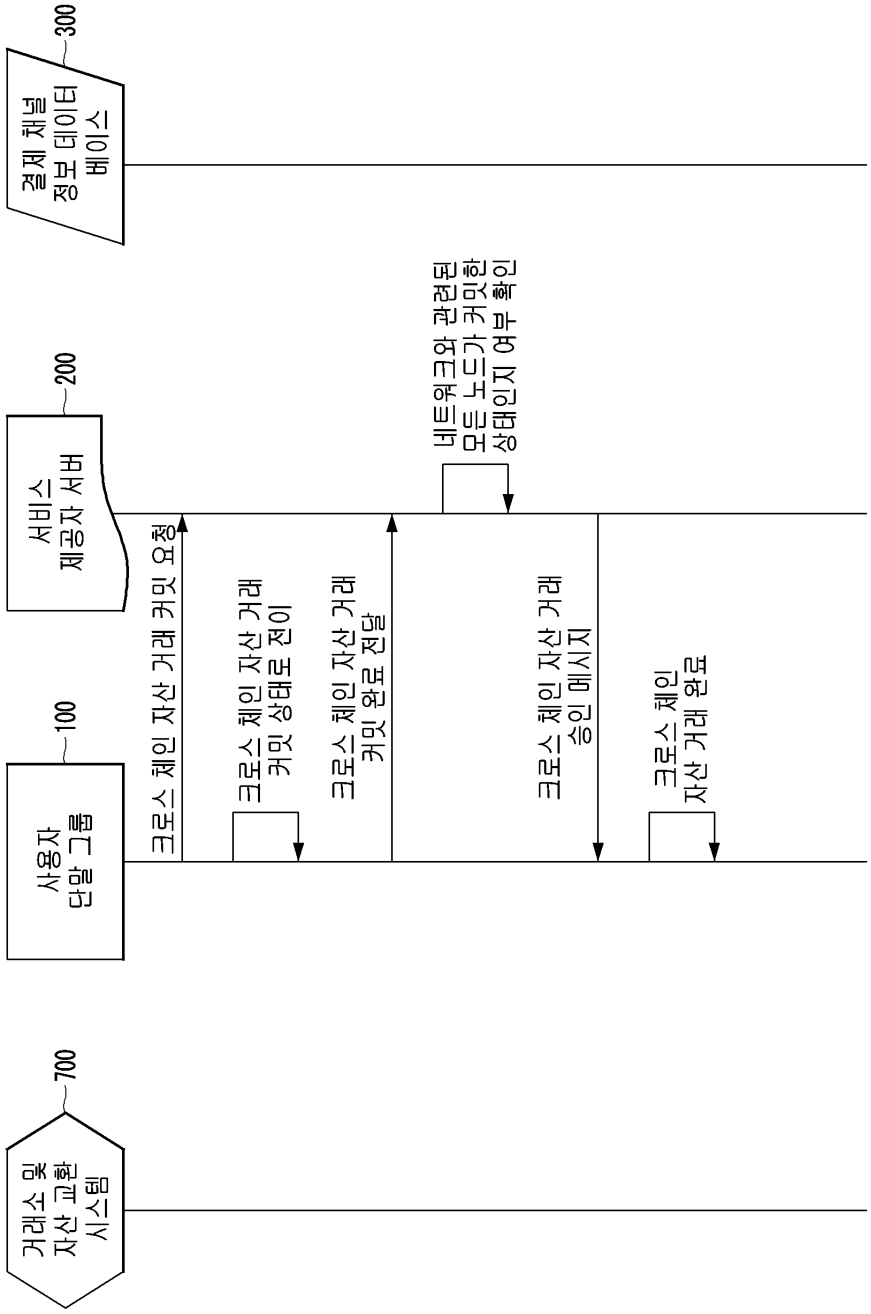
도면4b


200
비신뢰
실행 환경
280a
멀티 홉
결제 및
크로스 체인
자산 거래 동작
결과
신뢰
실행 환경
280b

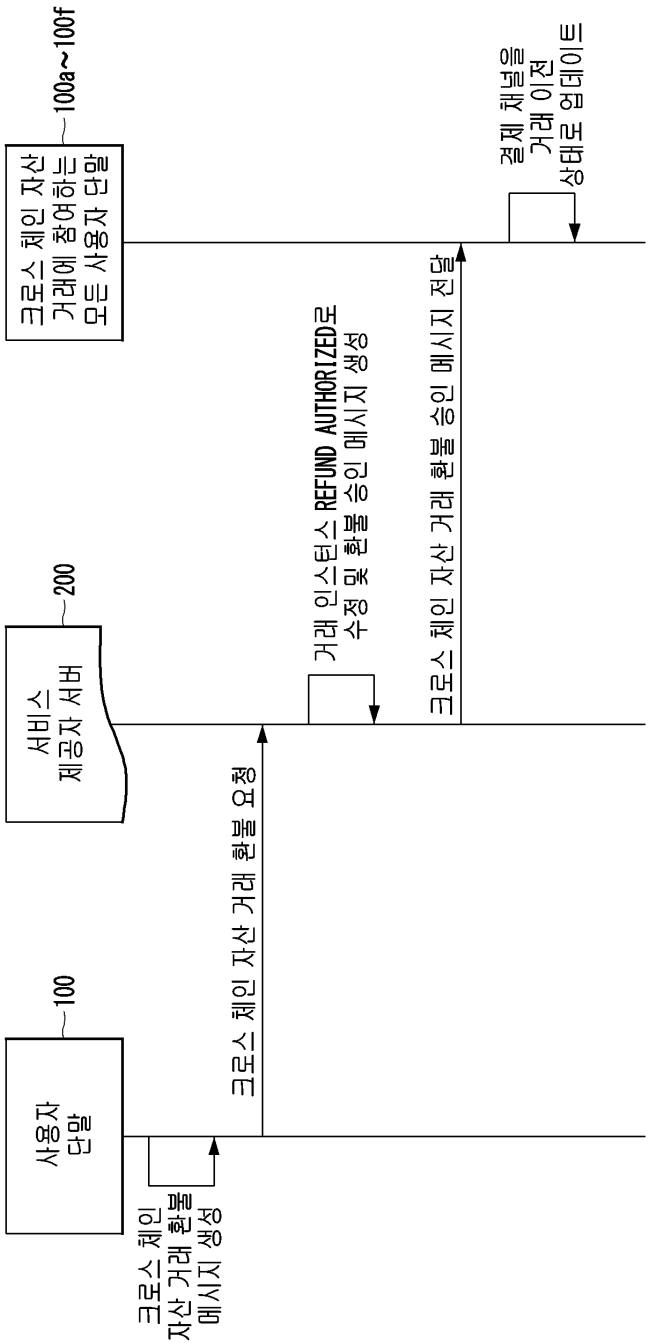
도면5a


300
결제 채널 정보 데이터베이스
200
서비스 제공자 서버
100
사용자 단말 그룹
700
거래소 및 자산 교환 시스템
결제 채널 정보 요청
결제 채널 정보 반환
최적 결제 경로 탐색 및 결제 채널 네트워크 구성
네트워크와 관련된 모든 노드가 준비된 상태인지 여부 확인
크로스 체인 자산 거래 참여 및 준비 요청
크로스 체인 자산 거래 준비 상태로 전이
크로스 체인 자산 거래 준비 완료 전달
크로스 체인 자산 거래 요청

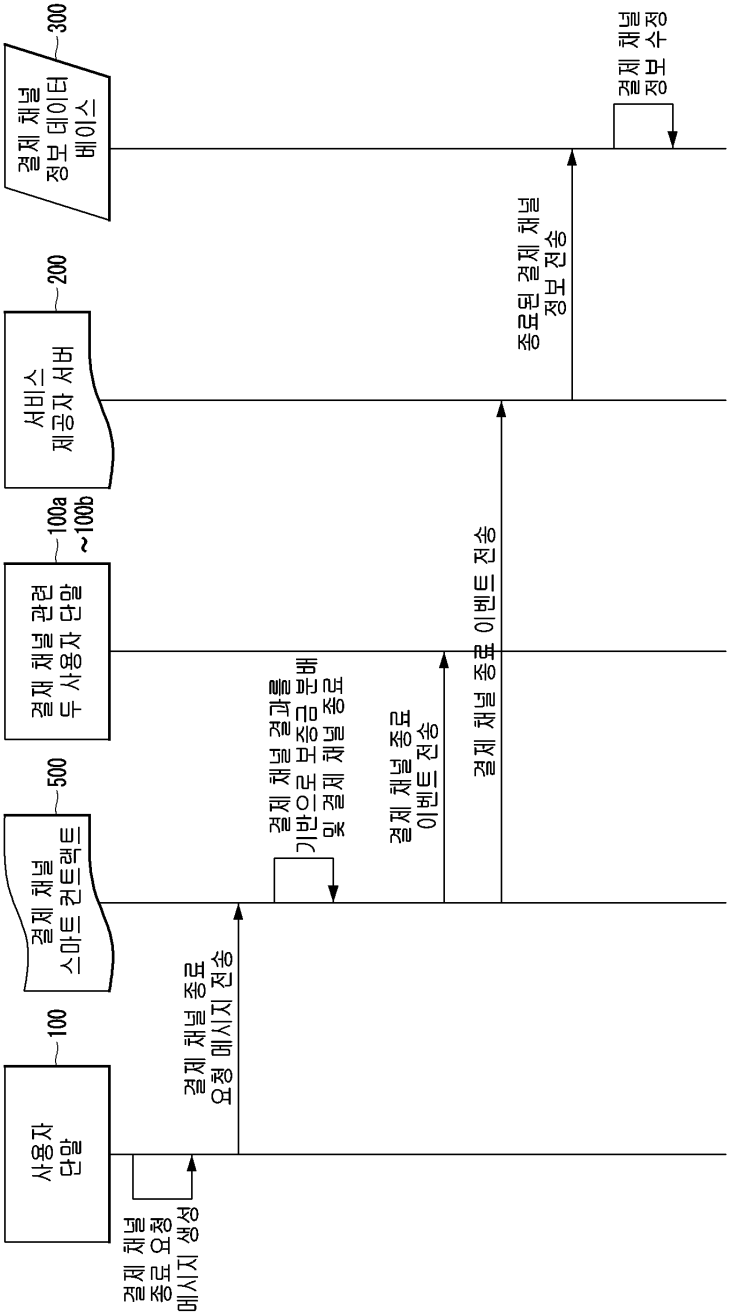
도면5b


300
결제 채널 정보 데이터베이스
200
서비스 제공자 서버
100
사용자 단말 그룹
700
거래소 및 자산 교환 시스템
크로스 체인 자산 거래 커밋 요청
크로스 체인 자산 거래 커밋 상태로 전이
크로스 체인 자산 거래 커밋 완료 전달
네트워크와 관련된 모든 노드가 커밋한 상태인지 여부 확인
크로스 체인 자산 거래 승인 메시지
크로스 체인 자산 거래 완료

도면6


100a~100f
크로스 체인 자산
거래에 참여하는
모든 사용자 단말
결제 채널을
거래 이전
상태로 업데이트
200
서비스
제공자 서버
거래 인스턴스 REFUND AUTHORIZED로
수정 및 환불 승인 메시지 생성
크로스 체인 자산 거래 환불 승인 메시지 전달
100
사용자
단말
크로스 체인 자산 거래 환불 요청
크로스 체인
자산 거래 환불
메시지 생성

도면7


사용자 단말
100
결제 채널 종료 요청 메시지 생성
결제 채널 종료 요청 메시지 전송
결제 채널 스마트 컨트랙트
500
결제 채널 결과를 기반으로 보증금 분배 및 결제 채널 종료
결제 채널 종료 이벤트 전송
결제 채널 종료 이벤트 전송
결제 채널 관련 두 사용자 단말
100a ~100b
서비스 제공자 서버
200
종료된 결제 채널 정보 전송
결제 채널 정보 수정
결제 채널 정보 데이터베이스
300