(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2022년08월03일
(11) 등록번호 10-2428950
(24) 등록일자 2022년07월29일

(51) 국제특허분류(Int. Cl.)
G06Q 20/38 (2012.01) *G06Q 20/02* (2012.01)
G06Q 20/06 (2012.01) *G06Q 20/14* (2012.01)
H04L 9/08 (2006.01)
(52) CPC특허분류
G06Q 20/3829 (2013.01)
G06Q 20/02 (2013.01)
(21) 출원번호 10-2019-0132499
(22) 출원일자 2019년10월23일
심사청구일자 2019년10월23일
(65) 공개번호 10-2021-0048336
(43) 공개일자 2021년05월03일
(56) 선행기술조사문헌
JP2015220699 A*
(뒷면에 계속)
전체 청구항 수 : 총 19 항

(73) 특허권자
포항공과대학교 산학협력단
경상북도 포항시 남구 청암로 77 (지곡동)
(72) 발명자
박찬익
경상북도 포항시 남구 지곡로 155, 6동 1105호
신동민
부산광역시 북구 만덕1로 8, 102동 2103호
(74) 대리인
특허법인이상

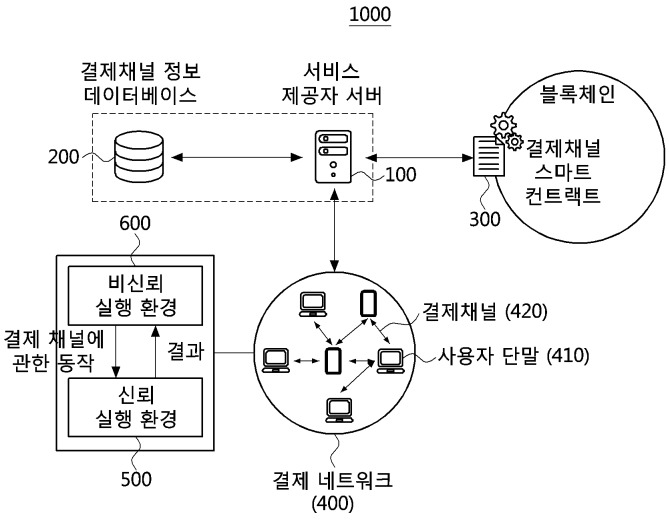
심사관 : 권태헌

(54) 발명의 명칭 **오프체인 결제 방법 및 그 시스템**

(57) 요 약

본 발명은 오프체인(Off-Chain)에서의 제1 단말 및 제2 단말간의 계약을 수행하기 위한 단말 간 동작 방법으로, 신뢰 실행 환경(Trusted Execution Environment, TEE)을 이용하여, 상기 제1 단말 및 상기 제2 단말의 공개 주소(public address)와 개인 키(private key)를 생성하는 단계 및 상기 제1 단말의 공개 주소 및 상기 제2 단말의 공개 주소가 포함된 정보를 이용하여 트랜잭션을 생성하는 단계를 포함한다. 본 발명을 통해 결제 시간을 단축시키고, 처리 성능 및 안정성을 향상시킬 수 있다.

대 표 도 - 도1



(52) CPC특허분류
G06Q 20/065 (2013.01)
G06Q 20/14 (2013.01)
H04L 9/0827 (2013.01)
H04L 2209/56 (2013.01)

(56) 선행기술조사문헌
KR1020190024601 A*
KR1020190048349 A*
'삼성 블록체인 키스토어 SDK의 모든 것', MK뉴스(2019.07.16. 게재)*
'특별한 디앱 개발의 필수품 `제너럴라이즈드` 스테이트 채널', MK뉴스(2019.02.12. 게재)*
*는 심사관에 의하여 인용된 문헌

이 발명을 지원한 국가연구개발사업
과제고유번호 1711125876
과제번호 2020-0-00936-002
부처명 과학기술정보통신부
과제관리(전문)기관명 정보통신기획평가원
연구사업명 블록체인융합기술개발(R&D)
연구과제명 5G 초저지연 서비스를 위한 무선 단말용 블록체인 기술 개발
기 여 율 1/2
과제수행기관명 포항공과대학교 산학협력단
연구기간 2021.01.01 ~ 2021.12.31
이 발명을 지원한 국가연구개발사업
과제고유번호 1711152571
과제번호 2021-0-00484-002
부처명 과학기술정보통신부
과제관리(전문)기관명 정보통신기획평가원
연구사업명 데이터경제를위한블록체인기술개발(R&D)
연구과제명 노드 간 메시지 전달과 합의를 위한 최적 경로 네트워크 프로토콜 기술개발
기 여 율 1/2
과제수행기관명 포항공과대학교 산학협력단
연구기간 2022.01.01 ~ 2022.12.31

명 세 서

청구범위

청구항 1

오프체인(Off-Chain)에서의 복수의 단말 중 제1 단말 및 제2 단말간의 결제를 수행하기 위하여, 스마트 컨트랙트 프로그램을 실행하는 블록체인 네트워크 및 서버를 포함하는 시스템이 단말 간 동작을 제어하는 방법으로서,

신뢰 실행 환경(Trusted Execution Environment, TEE)을 이용하여, 상기 제1 단말 및 상기 제2 단말의 공개 주소(public address)와 개인 키(private key)를 생성하는 단계;

상기 복수의 단말 중, 결제를 수행하려는 상기 제1 단말 및 제2 단말 간의 결제 요청 정보를 수신하여 상기 제1 단말과 상기 제2 단말간의 연결 정보를 이용하여 생성된 결제 네트워크 맵(payment network map)에 기초하여 계산되는 최단 시간 소요 결제 경로를 계산하는 단계;

계산된 상기 최단 시간 소요 결제 경로에 존재하는 단말들에게 상기 최단 시간 소요 결제 경로 생성 후, 상기 최단 시간 소요 결제 경로에 존재하는 단말들의 상태를 갱신이전 상태(PRE-UPDATE) 및 갱신이후 상태(POST-UPDATE)로 전이할 것을 요청하는 상태 전이 명령을 전송하는 단계; 및

상기 제1 단말의 공개 주소 및 상기 제2 단말의 공개 주소가 포함된 정보를 이용하여 트랜젝션을 생성하는 단계;

를 포함하는 단말 간 동작 방법

청구항 2

제1항에 있어서,

상기 개인 키는 상기 신뢰 실행 환경 내에 저장되는 것을 특징으로 하는 단말 간 동작 방법.

청구항 3

제2항에 있어서,

상기 제1 단말 및 상기 제2 단말 간에는 결제 채널(payment channel)이 설정되고,

상기 제1 단말 및 상기 제2 단말은 상기 신뢰 실행 환경에 의해 반환된 명령을 통해 상기 결제 채널과 관련된 동작을 수행하는 것을 특징으로 하는 단말 간 동작 방법.

청구항 4

제3항에 있어서,

상기 결제 채널과 관련된 동작은 상기 신뢰 실행 환경 내에 저장된 개인 키와 연계되는 것을 특징으로 하는 단말 간 동작 방법.

청구항 5

제1항에 있어서,

상기 신뢰 실행 환경은 상기 제1 단말 및 상기 제2 단말 내에 배치되는 것을 특징으로 하는 단말 간 동작 방법.

청구항 6

오프체인(Off-Chain)에서 결제를 수행하기 위한 시스템으로,

복수의 단말 및 상기 복수의 단말을 연결하는 결제 채널을 포함하는 결제 네트워크; 및

상기 복수의 단말 중, 결제를 수행하려는 제1 단말 및 제2 단말 간의 결제 요청 정보를 수신하여 상기 제1 단말과 상기 제2 단말간의 연결 정보를 이용하여 생성된 결제 네트워크 맵(payment network map)에 기초하여 계산되

는 최단 시간 소요 결제 경로를 계산하는 결제 경로 계산 모듈, 상기 계산된 최단 시간 소요 결제 경로에 존재하는 단말들에게 상기 최단 시간 소요 결제 경로 생성 후, 상기 최단 시간 소요 결제 경로에 존재하는 단말들의 상태를 갱신이전 상태(PRE-UPDATE) 및 갱신이후 상태(POST-UPDATE)로 전이할 것을 요청하는 상태 전이 명령을 전송하는 프로토콜 실행 모듈을 포함하는 서비스 제공자 서버;

를 포함하여, 상기 결제 요청 정보는 상기 제1 단말 및 상기 제2 단말의 공개 주소(public address)가 포함된 정보를 이용하여 생성된 트랜잭션 정보를 포함하며, 상기 제1 단말 및 상기 제2 단말의 공개 주소는 신뢰 실행 환경(trusted execution environment, TEE)을 이용하여 생성된 것을 특징으로 하는, 시스템.

청구항 7

제6항에 있어서,

상기 제1 단말 및 상기 제2 단말은 개인 키(private key)를 더 생성하고, 상기 개인 키는 상기 신뢰 실행 환경 내에 저장하는 것을 특징으로 하는, 시스템.

청구항 8

제7항에 있어서,

상기 제1 단말 및 상기 제2 단말 간에는 결제 경로(payment path)가 설정되고,

상기 제1 단말 및 상기 제2 단말은 상기 신뢰 실행 환경에 의해 반환된 명령을 통해 상기 결제 경로와 관련된 동작을 수행하는 것을 특징으로 하는 시스템.

청구항 9

제8항에 있어서,

상기 결제 채널과 관련된 동작은 상기 신뢰 실행 환경 내에 저장된 개인 키와 연계되는 것을 특징으로 하는, 시스템.

청구항 10

제6항에 있어서,

상기 신뢰 실행 환경은 상기 제1 단말 및 상기 제2 단말 내에 배치되는 것을 특징으로 하는, 시스템.

청구항 11

제6항에 있어서,

상기 제1 단말과 상기 제2 단말간의 최단 시간 소요 결제 경로는,

상기 복수 단말의 연결 정보를 이용하여 생성된 결제 네트워크 맵(payment network map)에 기초하여 계산되는 것을 특징으로 하는, 시스템.

청구항 12

제6항에 있어서,

상기 프로토콜 실행 모듈은,

상기 최단 시간 소요 결제 경로 생성 후, 상기 최단 시간 소요 결제 경로에 존재하는 단말들의 상태를 갱신이전 상태(PRE-UPDATE)로 전이할 것을 요청하는 것을 특징으로 하는, 시스템.

청구항 13

제12항에 있어서,

상기 프로토콜 실행 모듈은,

상기 최단 시간 소요 결제 경로에 존재하는 단말들로부터 갱신이전 상태의 채널 정보를 수신한 경우, 상기 최단 시간 소요 결제 경로에 존재하는 채널들의 잔액 정보에 기초하여 상기 최단 시간 소요 결제 경로에 존재하는 채

널들이 상기 결제 요청 정보를 처리할 수 있는 잔액을 보유하고 있는 지 여부를 검증하는 것을 특징으로 하는, 시스템.

청구항 14

제13항에 있어서,

상기 프로토콜 실행 모듈은,

상기 최단 시간 소요 결제 경로에 존재하는 채널들이 상기 결제 요청 정보를 처리할 수 있는 잔액을 보유하고 있는 것으로 검증된 경우, 상기 최단 시간 소요 결제 경로에 존재하는 단말들의 상태를 갱신이후(POST-UPDATE) 상태로 전이할 것을 요청하는 것을 특징으로 하는, 시스템.

청구항 15

제14항에 있어서,

상기 프로토콜 실행 모듈은,

상기 갱신이후 상태로 전이된 상기 최단 시간 소요 결제 경로에 존재하는 단말들로부터 신뢰 실행 환경에 기초한 갱신 정보가 포함된 결제 관련 정보를 수신하고, 결제 실행 메시지를 상기 최단 시간 소요 결제 경로에 존재하는 단말들에게 전송하는 것을 특징으로 하는, 시스템.

청구항 16

제6항에 있어서,

상기 시스템은,

상기 결제 네트워크에 포함된 단말간의 연결 정보가 저장된 결제 채널 정보 데이터베이스(DB)를 더 포함하는 것을 특징으로 하는, 시스템.

청구항 17

제6항에 있어서,

상기 시스템은,

상기 결제 네트워크에 포함된 단말 간의 채널 정보가 포함된 결제 채널 스마트 컨트랙트를 더 포함하는 것을 특징으로 하는, 시스템.

청구항 18

제17항에 있어서,

서비스 제공 서버는,

상기 결제 채널 스마트 컨트랙트와 동기화를 수행하는 계약 정보 동기화 모듈을 더 포함하는 것을 특징으로 하는, 시스템.

청구항 19

제17항에 있어서,

서비스 제공 서버는,

블록체인에 존재하는 스마트 컨트랙트 정보를 수신하는 블록체인 네트워크 통신부를 더 포함하는 것을 특징으로 하는, 시스템.

발명의 설명

기 술 분 야

[0001] 본 발명은 오프체인 결제 방법 및 그 시스템에 관한 것으로, 보다 상세하게는, 블록체인 오프체인 환경에서 블록체인 결제 서비스를 수행하기 위한 결제 방법 및 그 시스템에 관한 것이다.

배 경 기 술

[0002] 블록체인(blockchain)은 서로를 신뢰할 수 없는 분산 시스템 환경에서도 모든 노드들이 동일한 거래(transaction) 장부를 바라볼 수 있도록 도와주는 매커니즘이다. 대표적인 활용 예로 비트코인(Bitcoin)이 있다.

[0003] 또한, 스마트 컨트랙트(smart contract)는 프로그래밍 가능한 컨트랙트로, 단순히 코인과 같은 자산 거래 이외에도 분산 시스템 환경에서 모든 노드들이 동일한 순서로 트랜잭션(transaction)을 수행하여 동일한 프로그램 상태를 바라볼 수 있도록 한다. 대표적인 오픈 프로젝트로 이더리움(ethereum)이 있다.

[0004] 한편, 블록체인 환경에서의 결제 서비스는 블록체인 기반 응용 서비스에서 반드시 필요한 핵심적인 서비스이다. 일반적으로 블록체인 네트워크는 마이너(miner)들이 합의 알고리즘(consensus algorithm)을 수행하여 발생되는 트랜잭션들을 블록 형태로 생성하여 참여 노드들에게 전달한다. 블록체인 네트워크에 참여하는 모든 노드들은 동일한 형태의 블록체인을 유지하며 합의된 블록만을 추가할 수 있다. 이에 따라, 블록체인 네트워크의 안정성이 보장될 수 있도록 한다.

[0005] 비트코인이나 이더리움 블록체인과 같은 공개형 혹은 무허가형(public or permissionless) 블록체인에서는 고유의 토큰을 정의하고 있어, 결제 서비스가 내재되어 있지만, 이러한 공개형 블록체인의 성능 한계로 인해 실제 일상 생활에서 결제 서비스로 활용되기에는 한계점이 있다. 이는 퍼블릭(Public) 블록체인의 경우, 네트워크에 참여하는 노드가 전 세계에 퍼져있고, 그에 따라 발생하는 트랜잭션 또한 점차 늘어나고 있는데, 한 블록안에 포함될 수 있는 트랜잭션의 수가 한정되어 있는 것에 기인한다.

[0006] 구체적으로, 세계적인 디지털 결제 네트워크 기업인 VISA의 초당 처리할 수 있는 거래의 양(transactions per second, TPS)은 약 25,000 인데 반하여, 현재 공개형 블록체인 비트코인과 이더리움의 TPS는 각각 약 7과 15 정도로 알려져 있다. 이와 같이 공개형 블록체인의 성능은 기존의 VISA 성능과 비교할 때 큰 차이가 있다. 그 외에 폐쇄형 혹은 허가형(private or permissioned) 블록체인인 하이퍼레저/패브릭(Hyperledger/Fabric)의 TPS는 약 1,000으로 공개형 블록체인과 비교하면 대폭 향상되었지만, 여전히 VISA의 성능에 비해선 열등하다고 볼 수 있다.

[0007] 현재 이러한 블록체인 확장성(scalability) 문제를 해결하기 위하여 다양한 기술들이 제시되고 있다. 대표적인 기술로는 오프체인(off-chain)기법, 합의 알고리즘(consensus algorithm) 개선, 샤딩(sharding) 및 사이드체인(side-chain) 등이 있다.

[0008] 여기서 오프체인(off-chain) 기법은 빈번한 거래 당사자들끼리의 트랜잭션들을 블록체인 바깥에서 상호 합의하고 실행하게 하며, 최종 결과만을 블록체인에 기록하게 하는 형태의 기법이다. 일 예로, 비트코인 블록체인에서의 라이트닝 네트워크(Lightning Network)와 이더리움 블록체인에서의 레이든 네트워크(Raiden Networks)가 대표적인 오프체인 기법이다. 현재 오프체인 기법 중에서도 오프체인 결제 채널 기술이 일상적인 업무에 적용될 수 있는 블록체인 기반 결제 서비스로 주목받고 있다.

[0009] 기존의 결제 채널 기술로써 많이 활용되고 있는 라이트닝 네트워크(Lightning Network)와 레이든 네트워크(Raiden Network), 그리고 현재까지 연구되어 발표되고 있는 여러 결제 채널 기술들이 가지고 있는 공통적인 한계점은 다음과 같다.

[0010] 첫 번째, 네트워크상 결제 처리를 위한 사용자들의 금액은 결제가 완전히 종료될 때까지 묶여 있게 된다는 점이다. 결제 처리를 위한 사용자들의 금액을 결제 처리 비용이라고 한다. 결제 처리 비용은 네트워크상 결제에 필요한 금액의 총 액수와 총 금액이 묶여 있는 시간에 비례하여 증가한다. 결제 처리 비용은 결제 채널 프로토콜에 있어 필요한 비용이지만, 결제 처리 비용이 클수록 사용자에게 불편함을 주게 된다.

[0011] 두 번째, 직접적으로 결제 채널이 생성 되지 않은 사용자들 사이에서 결제를 진행할 경우, 매우 복잡한 과정을 필요로 한다는 점이다. 결제 과정이 복잡할수록 보안 결함이 생길 확률이 높아지며, 결제를 빠르게 수행하기 어렵다는 문제점이 있다.

[0012] 세 번째, 블록체인상 유효하지 않은 결제 트랜잭션을 지속적으로 감시해야 한다는 점이다. 결제 채널 쌍방간에는 오프체인 상에서 결제가 진행되기 때문에, 매순간 두 사용자 사이에는 서로 간 합의가 된 결제 트랜잭션 결

과들이 축적된다. 이렇게 축적된 결제 트랜잭션 결과들은 개별적으로 보면 상호 합의된 정보를 바탕으로 유효한 결과들이지만, 가장 최신 결제 트랜잭션 결과를 제외한 이전 결제 결과들은 더 이상 유효하지 않은 결과들이라고 볼 수 있다. 이때, 누군가가 유효하지 않게 된 결과 트랜잭션들을 블록체인에 올림으로서, 결제 채널과 연계되어 있는 보증금에 대한 악의적 정리 요청 행동을 할 수 있다. 이를 방지하기 위하여, 일정 시간 이후가 되어야만 유효하게 되는 타임락(timelock) 정보를 결제 채널의 결제 트랜잭션 결과에 연결하여 사용한다.

[0013] 이러한 타임락 기반 방법은 결제 채널의 첫 트랜잭션의 타임락 값에 따라 생성 가능한 결제 트랜잭션 결과의 개수가 의존적이며, 블록체인상에 유효하지 않은 결제 트랜잭션 요청이 올라오는지 여부를 항상 감시해야 하는 온체인(on-chain) 실시간 감시(monitoring) 기능이 반드시 필요한 문제점을 가지고 있다.

발명의 내용

해결하려는 과제

[0014] 상기와 같은 문제점을 해결하기 위한 본 발명의 목적은 고속, 고확장성 및 고안정성을 제공하는 오프체인 결제 방법 및 그 시스템을 제공하는 데 있다.

과제의 해결 수단

[0015] 상기 목적을 달성하기 위한 본 발명의 일 실시예에 따른 오프체인(off-chain)에서의 제1 단말 및 제2 단말간의 결제를 수행하기 위한 단말 간 동작 방법은, 신뢰 실행 환경(trusted execution environment, TEE)을 이용하여, 상기 제1 단말 및 상기 제2 단말의 공개 주소(public address)와 개인 키(private key)를 생성하는 단계 및 상기 제1 단말의 공개 주소 및 상기 제2 단말의 공개 주소가 포함된 정보를 이용하여 트랜젝션을 생성하는 단계를 포함한다.

[0016] 여기서 상기 개인 키는 상기 신뢰 실행 환경 내에 저장되는 것을 특징으로 한다.

[0017] 여기서 상기 제1 단말 및 상기 제2 단말 간에는 결제 경로(payment path)가 설정되고, 상기 제1 단말 및 상기 제2 단말은 상기 신뢰 실행 환경에 의해 반환된 명령을 통해 상기 결제 경로와 관련된 동작을 수행하는 것을 특징으로 한다.

[0018] 여기서 상기 결제 채널과 관련된 동작은 상기 신뢰 실행 환경 내에 저장된 개인 키와 연계되는 것을 특징으로 한다.

[0019] 여기서 상기 신뢰 실행 환경은 상기 제1 단말 및 상기 제2 단말 내에 배치되는 것을 특징으로 한다.

[0020] 또한 본 발명의 일 실 시예에 따른 오프체인(Off-Chain)에서 결제를 수행하기 위한 시스템은 복수의 단말 및 상기 복수의 단말을 연결하는 결제 채널을 포함하는 결제 네트워크 및 상기 복수의 단말 중, 결제를 수행하려는 제1 단말 및 제2 단말 간의 결제 요청 정보를 수신하여, 상기 제1 단말과 상기 제2 단말간의 최적 결제 경로를 계산하는 결제 경로 계산 모듈, 상기 계산된 최적 결제 경로에 존재하는 단말들에게 상태 전이 명령을 전송하는 프로토콜 실행 모듈을 포함하는 서비스 제공자 서버를 포함하여, 상기 결제 요청 정보는, 상기 제1 단말 및 상기 제2 단말의 공개 주소(public address)가 포함된 정보를 이용하여 생성된 트랜잭션 정보를 포함하여, 상기 제1 단말 및 상기 제2 단말의 공개 주소는 신뢰 실행 환경(trusted execution environment, TEE)을 이용하여 생성된 것을 특징으로 한다.

[0021] 여기서 상기 제1 단말 및 상기 제2 단말은 개인 키(private key)를 더 생성하고, 상기 개인 키는 상기 신뢰 실행 환경 내에 저장하는 것을 특징으로 한다.

[0022] 여기서 상기 제1 단말 및 상기 제2 단말 간에는 결제 채널(payment channel)이 설정되고, 상기 제1 단말 및 상기 제2 단말은 상기 신뢰 실행 환경에 의해 반환된 명령을 통해 상기 결제 채널과 관련된 동작을 수행하는 것을 특징으로 한다.

[0023] 여기서 상기 결제 채널과 관련된 동작은 상기 신뢰 실행 환경 내에 저장된 개인 키와 연계되는 것을 특징으로 한다.

[0024] 여기서 상기 신뢰 실행 환경은 상기 제1 단말 및 상기 제2 단말 내에 배치되는 것을 특징으로 한다.

[0025] 여기서 상기 제1 단말과 상기 제2 단말간의 최적 결제 경로는, 상기 복수 단말의 연결 정보를 이용하여 생성된 결제 네트워크 맵(payment network map)에 기초하여 계산되는 것을 특징으로 한다.

[0026] 여기서 상기 프로토콜 실행 모듈은, 상기 최적 결제 경로 생성 후, 상기 최적 결제 경로에 존재하는 단말들의 상태를 갱신이전(PRE-UPDATE) 상태로 전이할 것을 요청하는 것을 특징으로 한다.

[0027] 여기서 상기 프로토콜 실행 모듈은, 상기 최적 결제 경로에 존재하는 단말들로부터 갱신이전 상태의 채널 정보를 수신한 경우, 상기 최적 결제 경로에 존재하는 채널들의 잔액 정보에 기초하여 상기 최적 결제 경로가 상기 결제 요청 정보를 처리하기에 적합한지 여부를 판단하는 것을 특징으로 한다.

[0028] 여기서 상기 프로토콜 실행 모듈은, 상기 최적 결제 경로가 상기 결제 요청 정보를 처리하기에 적합한 것으로 판단된 경우, 상기 최적 결제 경로에 존재하는 단말들의 상태를 갱신이후(POST-UPDATE) 상태로 전이할 것을 요청하는 것을 특징으로 한다.

[0029] 여기서 상기 프로토콜 실행 모듈은, 상기 갱신이후 상태로 전이된 상기 최적 결제 경로에 존재하는 단말들로부터 신뢰 실행 환경에 기초한 갱신 정보가 포함된 결제 관련 정보를 수신하고, 결제 실행 메시지를 상기 최적 결제 경로에 존재하는 단말들에게 전송하는 것을 특징으로 한다.

[0030] 여기서 상기 시스템은, 상기 결제 네트워크에 포함된 단말간의 연결 정보가 저장된 결제 채널 정보 데이터베이스(DB)를 더 포함하는 것을 특징으로 한다.

[0031] 여기서 상기 시스템은, 상기 결제 네트워크에 포함된 단말 간의 채널 정보가 포함된 결제 채널 스마트 컨트랙트를 더 포함하는 것을 특징으로 한다.

[0032] 여기서 상기 서비스 제공 서버는, 상기 결제 채널 스마트 컨트랙트와 동기화를 수행하는 계약 정보 동기화 모듈을 더 포함하는 것을 특징으로 한다.

[0033] 여기서 상기 서비스 제공 서버는, 블록체인에 존재하는 스마트 컨트랙트 정보를 수신하는 블록체인 네트워크 통신부를 더 포함하는 것을 특징으로 한다.

발명의 효과

[0034] 본 발명에 따른 오프체인 결제 방법 및 그 시스템은 오프체인 결제 네트워크 프로토콜의 구성을 단순화하여 결제에 필요한 시간을 단축시킬 수 있고, 이에 따라 담보 비용(collateral cost)을 감소시킬 수 있다.

[0035] 또한 서비스 제공자 서버가 결제 경로에 연관된 사용자들의 상태를 동기화하기 때문에 결제 처리 시간을 대폭 감소시킬 수 있다.

[0036] 또한 서비스 제공자 서버가 오프체인 결제 참여자들로부터 다수의 요청을 수신하여 한번에 처리하므로 결제 성능을 높일 수 있다.

[0037] 또한 결제 시스템은 신뢰 실행 환경(TEE)에 기반하여 결제 동작을 수행하는바, 오프라인 결제 서비스의 안전성 및 신뢰성을 도모할 수 있다.

[0038] 또한 결제 시스템은 신뢰 실행 환경에 기반하여 결제 동작을 수행하는바, 오프체인 결제 당사자들의 악의적인 온체인 활동을 감시할 필요가 없다.

[0039] 다만, 본 발명의 실시 예들에 따른 오프체인 결제 방법 및 그 시스템이 달성할 수 있는 효과는 이상에서 언급한 것들로 제한되지 않으며, 언급하지 않은 또 다른 효과들은 아래의 기재로부터 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 명확하게 이해될 수 있을 것이다.

도면의 간단한 설명

[0040] 본 발명에 관한 이해를 돕기 위해 상세한 설명의 일부로 포함되는, 첨부도면은 본 발명에 대한 실시예를 제공하고, 상세한 설명과 함께 본 발명의 기술적 사상을 설명한다.

도 1은 본 발명의 일 실시예에 따른 오프 체인 결제 시스템(1000)의 구성도이다.

도 2는 본 발명의 일 실시예에 따른 서비스 제공자 서버(100)의 블록도이다.

도 3은 본 발명의 일 실시예에 따른 결제 채널 스마트 컨트랙트(300)의 블록도이다.

도 4는 본 발명의 일 실시예에 따른 결제 네트워크(400)에서의 사용자 단말(410)간 결제 채널(420) 사용에 개념도이다.

도 5a 및 도 5b는 본 발명의 일 실시예에 따른 오프 체인 결제 시스템(1000)의 동작 과정을 나타낸 순서도이다.

도 6은 본 발명의 일 실시예에 따른 사용자 단말(410)의 상태 전이도를 나타낸 개념도이다.

발명을 실시하기 위한 구체적인 내용

[0041] 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.

[0042] 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.

[0043] 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.

[0044] 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.

[0045] 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.

[0046] 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 오프 체인 결제 시스템(1000)의 구성도이다.

[0049] 본 명세서에서, 블록체인(blockchain)은 데이터를 분산 데이터 저장 환경에 저장하여, 누구나 그 데이터를 열람할 수 있으나, 누구도 임의로 수정할 수 없는, 분산 컴퓨팅 기술 기반의 데이터 위변조 방지 기술 내지 분산 데이터 저장 기술을 의미할 수 있다. 블록체인은 복수의 블록이 체인 형태로 연결된 것으로, 여기서 블록은 데이터를 저장하는 단위일 수 있다. 지속적으로 변경되는 데이터가 블록체인의 모든 노드에 의해 기록됨으로써, 전체데이터를 어느 한 노드가 임의로 조작하는 것이 불가능할 수 있다.

[0050] 본 명세서에서, 암호화폐는 전술한 블록체인을 기반으로 한 암호화 방법을 사용하여, 거래 안전이 확보되고 위변조가 방지되는 디지털 자산일 수 있다. 일 실시예로서, 암호화폐에는 비트코인, 이더리움, 리플, 라이트 코인 등이있다.

[0051] 본 명세서에서, 온 체인(on-chain)은 블록체인 네트워크 상을 의미할 수 있다. 어느 연산, 동작이 온 체인에서 수행된다는 표현은, 그 연산, 동작이 블록체인 네트워크상에서 수행된다는 의미로서, 예를 들어 적어도 하나의 노드에 의해 그 연산, 동작이 수행된다는 뜻일 수 있다. 오프 체인(off-chain)은 블록체인 네트워크 밖을 의미할 수 있다. 어느 연산, 동작이 오프 체인에서 수행된다는 표현은, 그 연산, 동작이 블록체인 네트워크와는 구분되는 블록체인 네트워크 밖의 네트워크에서 수행된다는 의미일 수 있다. 예를 들어, 블록체인 노드 간의 블록 생성, 분산 합의 과정 등을 제외한, 사용자 단말, 별도의 서버 및 기타 통신 가능한 장치 등 사이의 통신은 모두 오프체인에서 수행된다고 볼 수 있다.

[0052] 도 1을 참조하면, 본 발명에 따른 오프체인 결제 시스템(1000)은 서비스 제공자 서버(100), 결제 채널 정보 데

이터 베이스(DB)(200), 결제 채널 스마트 컨트랙트(300) 및 결제 네트워크(400)를 포함한다. 결제 네트워크(400)는 복수의 사용자 단말(410) 및 결제 채널(500)를 포함한다. 본 발명에 따른 오프체인 결제 시스템(1000)은 튜링 완전(turing completeness) 스마트 컨트랙트를 지원할 수 있다.

[0053] 서비스 제공자 서버(100)는 멀티홉(multi-hop) 결제 프로토콜과 관련된 명령을 제어 및 실행하고, 결제 채널(500)들에 대한 정보를 가져오기 위한 장치일 수 있다. 서비스 제공자 서버(100)는 데스크탑 혹은 서버일 수 있다. 본 발명은 프로토콜 실행 책임을 담당하는 서비스 제공자 서버(100)를 도입하여, 각 노드의 상태에 대한 동기화가 단순해지도록 할 수 있다. 본 발명에 따른 서비스 제공자 서버(100)의 구체적인 구성에 대해서는 도 2를 참조하여 후술한다.

[0054] 결제 채널 정보 데이터 베이스(DB)(200)는 서비스 제공자 서버(100) 로부터 블록체인 상의 결제 채널 스마트 컨트랙트(300)의 정보와 동기화 정보를 지속적으로 수신할 수 있다. 이를 통해, 현재 결제 네트워크(400)에 참여하고 있는 사용자들 간의 최신 연결 정보를 보유할 수 있다. 일 예로서, 결제 채널 정보 데이터 베이스(DB)(200)는 MySQL 또는 Oracle 데이터 베이스일 수 있다.

[0055] 결제 채널 스마트 컨트랙트(300)는 블록체인 상에서 동작하는 어플리케이션일 수 있고, 오프체인 결제 처리 결과의 정산 및 분쟁 조정에 이용될 수 있다. 트랜잭션은 스마트 컨트랙트의 상태를 변경하기 위한 입력값의 역할을 할 수 있다. 여기서 트랜잭션(transaction)은 오더, 주문의 의미로 사용될 수 있다. 예를 들어, 트랜잭션은 '사용자 A가 사용자 B에게 소정의 암호화폐를 소정의 수량만큼 보낸다'등과 같은 암호화폐 송금, 교환 등의 내용을 하나의 문자열로 나타낸 것일 수 있다.

[0056] 블록체인 상의 블록들의 트랜잭션은 결제 채널 스마트 컨트랙트(300)의 상태를 변경시킬 수 있고, 결제 채널 스마트 컨트랙트(300)는 결제 채널 스마트 컨트랙트(300)의 최신 상태를 보관하고 있을 수 있다. 암호화폐 교환, 예치, 인출을 위한 트랜잭션은 결제 채널 스마트 컨트랙트(300)의 상태를 변경시킬 수 있고, 이에 따라 변경된 상태인 잔고 정보가 결제 채널 스마트 컨트랙트(300)에 저장될 수 있다. 블록체인은, 결제 채널 스마트 컨트랙트(300)를 지원하는 어떠한 블록체인이어도 무방하다. 예를 들어 이더리움과 같은 스마트 컨트랙트 지원 블록체인이 사용될 수 있다. 본 발명에 따른 결제 채널 스마트 컨트랙트(300)의 구체적인 구성에 대해서는 도 3을 참조하여 후술한다.

[0057] 결제 네트워크(400)는 복수의 사용자 단말(410)을 연결하는 결제 채널(420)을 포함한다. 결제 네트워크(800)는 복수의 사용자 단말(410) 및 결제 채널(420)들이 서로 연결되어 하나의 네트워크를 형성하고 있는 것을 의미할 수 있다. 한편, 오프체인 결제 처리에 참여하는 사용자 단말(410)은 모두 신뢰 실행 환경(trusted execution environment: TEE)(500)에 기초한 명령을 통해 동작할 수 있다. 신뢰 실행 환경은 미리 정의한 동작만을 각 노드가 수행할 수 있도록 강제하기 때문에, 오프체인 결제 채널 프로토콜을 실행하는 과정에서 노드의 악의적인 행동을 방지할 수 있다. 신뢰 실행 환경에 기초한 결제 네트워크(400)의 구체적인 동작은 도 4를 참조하여 후술한다.

[0058] 사용자 단말(410)은 하나의 노드라 볼 수 있다. 사용자 단말(410)은 프로토콜에 참여하여 결제 동작을 수행하기 위한 장치로, 일 실시예로서, 데스크탑, 랩탑(laptop) 혹은 모바일 기기일 수 있다. 사용자 단말(410)은 상대방과 직접적으로 연결된 결제 채널(420)에서의 동작을 실행하거나, 결제 경로에 참여한 상태인 경우 서비스 제공자 서버(100)와 프로토콜을 따르기 위한 메시지를 주고받을 수 있다. 이와 같이, 사용자 단말(410)(즉, 노드)은 결제 네트워크(400)의 구성요소 중 하나로서, 해당 블록체인을 유지하기 위한 연산을 수행하는 주체일 수 있다. 블록체인의 유지에는 신규 블록의 생성 작업이 포함될 수 있다. 블록체인의 임의의한 노드는 사용자 단말(410)에 발행한 트랜잭션을 이용하여 블록체인의 블록을 생성할 수 있다. 생성된 블록은 분산합의 과정을 통해 블록체인의 노드들 간에 공유되고 블록체인의 다음 블록으로 연결될 수 있다.

[0059] 사용자 단말(410)은 트랜잭션을 생성할 수 있다. 또한, 사용자 단말(410)은 블록체인의 사용자 단말들 중 어느 하나를 통해, 스마트 컨트랙트에 저장된 잔고 정보 등을 확인할 수 있다. 사용자 클라이언트는 블록체인 클라이언트와 동일한 의미로 사용될 수 있다. 여기서 결제 네트워크(400)는 복수의 사용자 단말(410) 사이에 트랜잭션 또는 블록 등을 공유하는 네트워크를 의미할 수 있다.

[0061] 도 2는 본 발명의 일 실시예에 따른 서비스 제공자 서버(100)의 블록도이다.

[0062] 도 2를 참조하면, 본 발명의 일 실시예에 따른 서비스 제공자 서버(100)는 블록체인상의 결제 채널 스마트 계약(300)의 정보를 지속적으로 서버에 가져오기 위한 계약 정보 동기화 모듈(110), 결제 채널(420)들에 대한 정보를 바탕으로 최적의 결제 경로를 계산하는 결제 경로 계산 모듈(120), 결제 경로상의 여러 사용자 단말(410)들

을 경유하는 멀티홉 결제 진행을 위한 프로토콜 실행 모듈(130) 및 블록체인 네트워크와의 통신을 담당하는 블록체인 네트워크 통신부(140)를 포함한다.

[0063] 계약 정보 동기화 모듈(110)은 결제 채널(420)을 사용 중인 사용자들의 결제 채널(420) 정보들을 저장하고 있는 결제 채널 스마트 컨트랙트(300)와의 동기화를 위한 모듈일 수 있다. 각 사용자 단말(410)들은 신뢰 실행 환경(TEE)이 내부적으로 생성한 공개 주소(public address)로 표현되며, 사용자들의 채널 정보를 가져옴으로써 연결 관계를 파악하고 동기화할 수 있다.

[0064] 결제 경로 계산 모듈(120)은 계약 정보 동기화 모듈(110)이 동기화한 정보를 활용하여 송신자로부터 수신자까지 최적의 결제 경로를 계산하는 모듈일 수 있다. 보다 상세하게는 각 사용자 단말(410)의 연결 정보를 토대로 결제 네트워크 맵(payment network map)을 생성하고, 결제 네트워크 맵에 기초하여 최적의 결제 경로를 결정할 수 있다.

[0065] 프로토콜 실행 모듈(130)은 요청받은 결제를 처리하기 위해, 결제 경로 계산 모듈(120)이 계산한 결제 경로에 포함된 송신자, 중간 사용자들(intermediaries) 그리고 수신자 간에 결제를 위한 프로토콜을 실행할 수 있다. 또한 프로토콜 실행 모듈(130)은 결제 경로에 존재하는 모든 사용자 단말들의 상태를 동기화하여, 사용자 단말 동기적으로 진전(進展)되도록 할 수 있다. 그리고 프로토콜 실행 모듈(130)은 결제 경로 상에 존재하는 사용자 단말들에게 상태 전이 명령을 전송할 수 있다.

[0066] 블록체인 네트워크 통신부(140)는 블록체인에 존재하는 스마트 컨트랙트의 정보를 수신하도록 할 수 있다. 구체적으로 이더리움 상 web3 기반 원격 프로시저 호출(JSON-RPC)을 담당하는 모듈 또는 하이퍼레저/패브릭(Hyperledger/Fabric) SDK 기반 트랜잭션 제출을 담당하는 모듈일 수 있다.

[0068] 도 3은 본 발명의 일 실시예에 따른 결제 채널 스마트 컨트랙트(300)의 블록도이다.

[0069] 도 3을 참조하면, 본 발명에 따른 결제 채널 스마트 컨트랙트(300)는 결제 채널 정보 저장부(310), 프로토콜 방출 정보 저장부(320), 결제 채널 생성부(330), 결제 채널 종료부(340), 프로토콜 방출부(350) 및 결제 채널 정산부(360)를 포함한다.

[0070] 결제 채널 정보 저장부(310)는 사용자 단말(410)들 사이에 연결된 결제 채널(420)들에 대한 정보를 저장할 수 있다. 결제 채널 정보 저장부(310)는 결제 채널의 식별자(identifier)값을 키(key)로 사용하여 결제 채널(420)이 실제로 존재하는지 여부를 파악할 수 있다. 결제 채널(420)이 실제 존재하는 경우, 연결을 구성하는 두 사용자 단말(400)의 주소를 값(value)으로 얻을 수 있다.

[0071] 프로토콜 방출 정보 저장부(320)은 결제 네트워크상에서 거래가 이루어지는 도중 임의의 사용자 단말(410)이 이탈한 경우, 어떠한 상태에서 이탈하였는지에 대한 정보를 포함하고 있다.

[0072] 결제 채널 생성부(330)는 사용자 단말(410)로부터 결제 채널(420)의 생성을 요청하는 메시지가 수신되는 경우 호출되는 모듈일 수 있다. 결제 채널(420)은 임의의 두 사용자가 공식적이거나 비공식적인 형태로 결제 채널(420)을 생성할 것이라는 합의를 본 후, 두 사용자 중 한 사용자가 단말을 통해 두 사용자의 공개 주소를 채널 생성 요청 및 보증금을 함께 전달함으로써 생성될 수 있다.

[0073] 결제 채널 종료부(340)는 임의의 결제 채널에 연결된 사용자 단말(410)로부터 해당 결제 채널의 종료를 요청하는 메시지가 수신되는 경우 호출되는 모듈일 수 있다. 결제 채널 종료부(340)가 결제 채널 종료 요청을 수신하는 경우, 최종적인 잔액(balance) 분배에 대한 정보도 함께 수신할 수 있다. 결제 채널 종료부(340)는 잔액 분배에 대한 정보를 이용하여, 묶여있는 두 사용자의 보증금을 해당 잔액 정보에 따라 결제 채널의 두 사용자의 공개 주소로 각각 알맞게 모두 반환하고, 결제 채널을 종료할 수 있다.

[0074] 프로토콜 방출부(350)는 사용자 단말(410)로부터 결제 네트워크(400)상에서의 이탈을 요청하는 메시지가 수신되는 경우 호출되는 모듈일 수 있다. 프로토콜 방출부(350)가 결제 네트워크상 방출 요청을 수신하는 경우, 관련 결제 채널들의 상태 정보, 최종적인 잔액(balance) 분배 정보 및 결제 금액에 대한 정보를 함께 수신할 수 있다. 프로토콜 방출부(350)는 관련 결제 채널들의 최종 상태 정보, 최종적인 잔액 분배 정보 및 결제 금액에 대한 정보를 이용하여, 해당 결제 채널들을 정산하고 프로토콜 방출 정보 저장부(320)에 방출 정보를 등록할 수 있다.

[0075] 결제 채널 정산부(360)는 결제 네트워크에 관련된 사용자 단말(410)로부터 관련 결제 채널들의 정산을 요청하는 메시지가 수신되는 경우 호출되는 모듈일 수 있다. 결제 채널 정산부(360)가 결제 채널 정산 요청을 수신하는 경우, 관련 결제 채널들의 상태 정보, 최종적인 잔액(balance) 분배 정보 및 결제 금액에 대한 정보를 함께 수

신할 수 있다. 결제 채널 정산부(360)는 최종적인 잔액 분배 정보를 이용하여, 묶여있는 두 사용자의 보증금을 해당 잔액 정보에 따라 결제 채널의 두 사용자의 공개 주소로 각각 알맞게 모두 반환하고, 결제 채널을 종료할 수 있다.

[0077] 도 4는 본 발명의 일 실시예에 따른 결제 네트워크(400)에서의 사용자 단말(410)간 결제 채널(420)의 사용을 도시한 개념도이다.

[0078] 도 4를 참조하면, 본 발명에 따른 일 실시예로서, 두 사용자 단말(410A, 410B)간 결제 채널(420)의 사용 과정이 도시되어 있다.

[0079] 사용자 단말들(410A, 410B)이 결제 채널(420)에 특정한 동작을 행하기 위해서는 비신뢰 실행 환경(600)의 명령이 반드시 신뢰 실행 환경(500)을 경유하여야 한다. 예를 들어, 신뢰 실행 환경(500)에 의해 반환된 명령을 통해 결제 채널(420)과 관련된 동작을 수행할 수 있다.

[0080] 사용자 단말들(410A, 410B) 각각은 신뢰 실행 환경(Trusted Execution Environment, TEE)을 이용하여, 공개 주소(public address)와 개인 키(private key)를 생성할 수 있다. 그리고 신뢰 실행 환경(500)은 제1 사용자 단말(410A)의 공개 주소 및 제2 사용자 단말(410B)의 공개 주소가 포함된 정보를 이용하여 트랜젝션을 생성할 수 있다.

[0081] 신뢰 실행 환경(500)은 공개 주소(public address)를 생성한 후 해당 주소에 대한 개인키(private key)는 내부에 저장할 수 있다. 결제 채널(420)과 관련된 모든 동작은 신뢰 실행 환경 내부에 저장된 개인키와 연계되어 있으므로, 사용자는 결제 채널(420)에 대한 임의의 행동을 취할 수 없다. 결제 채널(420)로 연결된 두 사용자 단말(410A, 410B)이 신뢰 실행 환경 위에서 동작하게 되면, 결제 채널(420)과 관련된 작업 명령은 반드시 미리 정의된 동작을 통한 결과가 반환되기 때문에 사용자 단말들(410A, 410B)이 임의로 행동할 수 없다. 이 경우, 사용자 단말들(410A, 410B)의 올바른 동작이 보장되기 때문에 과거의 합의된 트랜잭션들이 블록체인에 올라올 수 없게 되어 온체인 활동을 감시하지 않아도 된다.

[0082] 또한 신뢰 실행 실행 환경을 활용하는 경우, 각 사용자 단말들(410A, 410B)의 임의적인 행동을 방지하기 때문에, 여러 경우의 수를 생각하지 않아도 되고 따라서 오프체인 결제 채널 프로토콜의 구성을 단순하게 만들 수 있다. 그리고 서비스 제공자 서버(100)가 프로토콜의 실행 상태를 결제와 관련된 사용자 단말들에게 한 번에 전달함으로써, 사용자들의 상태도 함께 갱신되고 동기화될 수 있다. 이로 인해 결제 처리에 필요한 시간을 줄일 수 있고, 결과적으로 담보 비용을 줄일 수 있다. 한편, 상기 신뢰 실행 환경(500)은 제1 사용자 단말(410A) 및 제2 사용자 단말(410B) 내에 배치될 수 있다.

[0083] 신뢰 실행 환경(500)은 TXT(Trusted Execution Technology), ME(Manageability Engine), TrustZone Security System, VTx(Virtualization Technology), microcode enforced thread, 메모리 액세스 분리 등과 같은 공지된 다양한 기술들에 의해 제공될 수 있다.

[0085] 도 5a 및 도 5b는 본 발명의 일 실시예에 따른 오프 체인 결제 시스템(1000)의 동작 과정을 나타낸 순서도이다.

[0086] 도 5a 및 도 5b를 참조하면, 서비스 제공자 서버(100)는 복수의 사용자 단말(410)들에게 메시지를 전달하여 정보를 공유하고, 결제 채널 진행 과정의 중간 단계를 동기화 시킬 수 있다. 여기서 복수의 사용자 단말들(410)은 결제 채널 네트워크(400)를 구성하는 노드로 볼 수 있다.

[0087] 복수의 사용자 단말(410) 중 어느 하나의 사용자 단말(410A)이 다른 특정 사용자 단말(410B)에게 결제 작업을 수행하길 원하는 경우, 결제 작업을 요청하는 사용자 단말은 결제 요청 메시지를 서비스 제공자 서버(100)에게 전송할 수 있다(S501). 상기 결제 요청 메시지는 결제 작업을 수행하려는 사용자 단말들(410A, 410B)의 공개 주소(public address)가 포함된 정보를 이용하여 생성된 트랜잭션 정보를 포함할 수 있다. 여기서 상기 사용자 단말들(410A, 410B)의 공개 주소는 신뢰 실행 환경(trusted execution environment, TEE)을 이용하여 생성된 것일 수 있다.

[0088] 서비스 제공자 서버(100)가 어느 하나의 사용자 단말로부터 결제 요청 메시지(또는 결제 요청 정보)를 수신하면, 서비스 제공자 서버(100)는 결제 네트워크(400)상의 결제 채널(420)들이 구성되어 있는 형태를 파악하기 위해, 결제 채널 정보 데이터 베이스(DB)(200)에 결제 채널(420)들의 구성에 관한 정보들을 요청할 수 있다(S502).

[0089] 서비스 제공자 서버(100)는 결제 채널 정보 데이터 베이스(DB)(200)로부터 결제 채널(420)과 관련된 정보를 수신할 수 있다(S503). 다시 말해, 결제 채널 정보 데이터 베이스(DB)(200)는 서비스 제공자 서버(100)에 결제 채

널(420)과 관련된 정보를 반환할 수 있다(S503).

[0090] 서비스 제공자 서버(100)는 요청한 정보를 전달 받은 후, 해당 결제 채널(420)들에 대한 정보를 바탕으로 결제 작업을 수행하기를 원하는 사용자 단말(410A)과 돈을 받게 될 사용자 단말(410B)사이의 최적의 결제 경로를 계산할수 있다(S504). 이후 결제 네트워크 맵(payment network map)을 구성할 수 있다(S505). 상기 S504 내지 S505 단계는 서비스 제공자 서버(100)의 결제경로 계산 모듈(120)에 의하여 수행될 수 있다.

[0091] 서비스 제공자 서버(100)는 S504, S505 단계를 통해 계산된 결제 네트워크 상에 존재하는 모든 결제 채널(420)들이 결제 요청을 처리할 수 있을 만한 잔액을 보유하고 있는지 여부를 검증하고, 결제 참여 의사를 확인하기 위해, 최적 결제 경로에 포함된 사용자 단말들에게 결제에 참여할 것을 요청할 수 있다(S506).

[0092] 결제에 참여할 것을 요청받은 단말들은 각자의 채널을 갱신이전(PRE-UPDATE) 상태로 전이할 수 있다(S507). 그리고 사용자 단말들은 갱신이전 상태로 전이된 채널 정보를 서비스 제공자 서버(100)로 전달할 수 있다(S508).

[0093] 서비스 제공자 서버(100)는 결제 네트워크에 존재하는 모든 단말들로부터 결제 참여 의사를 수신할 수 있고, 결제 네트워크에 존재하는 모든 단말들로부터 결제 참여 의사가 수신되었는지 여부를 확인할수 있다(S509).

[0094] 서비스 제공자 서버(100)는 결제요청에 대응하는 결제 관련 정보를 생성하여, 결제 네트워크에 존재하는 사용자 단말들에게 신뢰 실행 환경 내에 존재하는 관련 결제 채널들의 정보를 결제 완료 상태로 갱신할 것을 요청할 수 있다(S510).

[0095] 사용자 단말(410)들은 신뢰 실행 환경 내에 존재하는 관련 결제 채널들의 정보를 결제 완료 상태로 갱신한 후, 자신의 채널을 갱신이후(POST-UPDATE) 상태로 전이시킬 수 있다(S511). 그리고 각 사용자 단말은 갱신 완료 사실을 서비스 제공자 서버(100)로 전달할 수 있다(S512).

[0096] 서비스 제공자 서버(100)는 해당 경로에 존재하는 모든 사용자 단말들로부터 신뢰 실행 환경을 통한 갱신 완료 정보를 전달 받았는지 여부를 확인한 후(S513), 결제 완료 메시지를 각 사용자 단말들에게 전달할 수 있다(S514). S506 내지 S514 단계는 서비스 제공자 서버(100)의 프로토콜 실행 모듈(130)에 의하여 수행될 수 있다.

[0098] 도 6은 본 발명의 일 실시예에 따른 사용자 단말(410)의 상태 전이도를 나타낸 개념도이다.

[0099] 도 6 및 도5 를 함께 참조하여 설명한다. 사용자 단말의 채널이 결제 경로에 연관되지 않았다면, 사용자 단말의 상태는 휴식 상태이다(S601). 휴식 상태에서 서비스 제공자 서버(100)로부터 결제 네트워크 구성 요청을 받는 후(S602), 결제 네트워크 구성에 동의한다는 메시지를 다시 서비스 제공자 서버(100)에 전달하면(S603), 사용자 단말은 채널을 갱신이전 상태로 전이시킬 수 있다(S604).

[0100] 한편, 갱신이전 상태의 사용자 단말이 서비스 제공자 서버(100)로부터 신뢰 실행 환경 내에 존재하는 관련 결제 채널들의 정보를 결제 완료 상태로 갱신할 것을 요청 받은 후(S605), 신뢰 실행 환경 내에 존재하는 관련 결제 채널들의 정보를 결제 완료 상태로 갱신하여, 갱신 완료 사실을 다시 서비스 제공자 서버(100)에 전달하면(S606), 사용자 단말의 상태는 갱신이후 상태로 전이될 수 있다(S607).

[0101] 한편, 서명 상태에서 서비스 제공자 서버(100) 로부터 결제 완료 메시지를 수신하면(S608), 사용자 단말의 상태는 휴식 상태(S601)로 전이될 수 있다.

[0103] 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.

[0104] 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.

[0105] 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 의

해(또는 이용하여) 수행될 수 있다. 몇몇의 실시예에서, 가장 중요한 방법 단계들의 하나 이상은 이와 같은 장치에 의해 수행될 수 있다.

[0106] 실시예들에서, 프로그램 가능한 로직 장치(예를 들어, 필드 프로그머블 게이트 어레이)가 여기서 설명된 방법들의 기능의 일부 또는 전부를 수행하기 위해 사용될 수 있다. 실시예들에서, 필드 프로그머블 게이트 어레이는 여기서 설명된 방법들 중 하나를 수행하기 위한 마이크로프로세서와 함께 작동할 수 있다. 일반적으로, 방법들은 어떤 하드웨어 장치에 의해 수행되는 것이 바람직하다.

[0107] 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

[0108] 1000: 오프체인 결제 시스템

100: 서비스 제공자 서버

110: 계약정보 동기화 모듈

120: 결제경로 계산 모듈

130: 프로토콜 실행 모듈

140: 블록체인 네트워크 통신 모듈

200: 결제채널 정보 데이터베이스(DB)

300: 결제채널 스마트 컨트랙트

310: 결제채널 정보 저장부

320: 프로토콜 방출 정보부

330: 결제채널 생성부

340: 결제 채널 종료부

350: 프로토콜 방출부

360: 결제 채널 정산부

400: 결제 네트워크

410, 410A, 410B, 410C, 410D: 사용자 단말

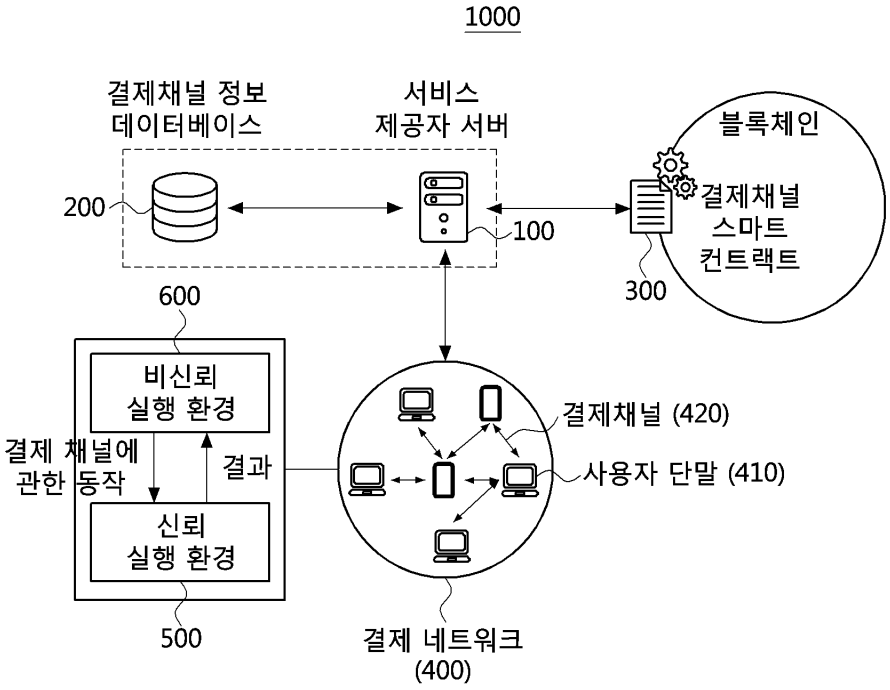
420: 결제채널

500: 신뢰 실행 환경(TEE)

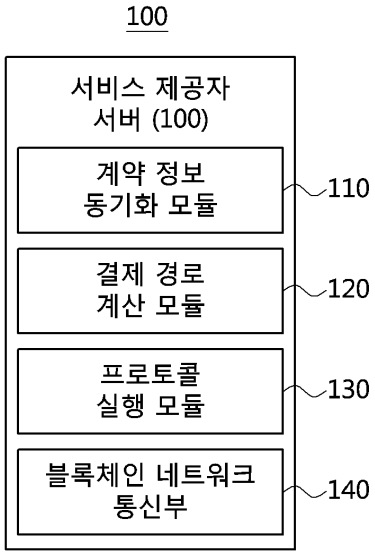
600: 비신뢰 실행 환경

도면

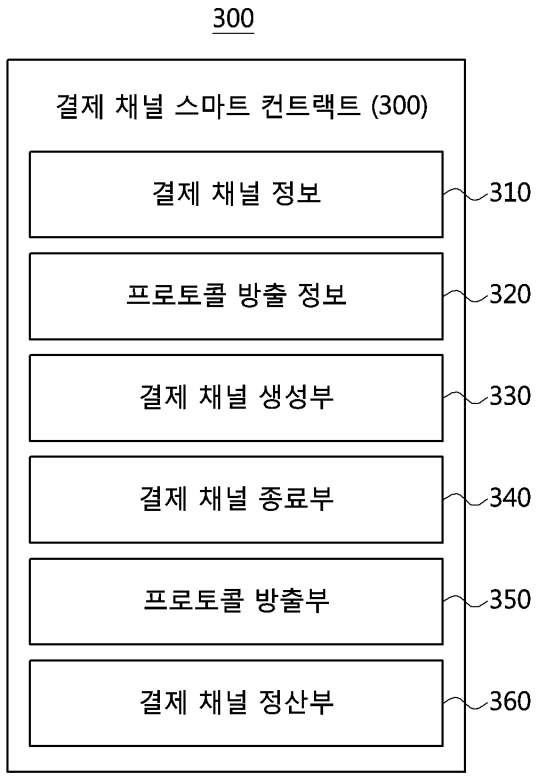
도면1


1000
결제채널 정보
데이터베이스
서비스
제공자 서버
블록체인
결제채널
스마트
컨트랙트
200
100
300
600
비신뢰
실행 환경
결제 채널에
관한 동작
결과
신뢰
실행 환경
500
결제채널 (420)
사용자 단말 (410)
결제 네트워크
(400)

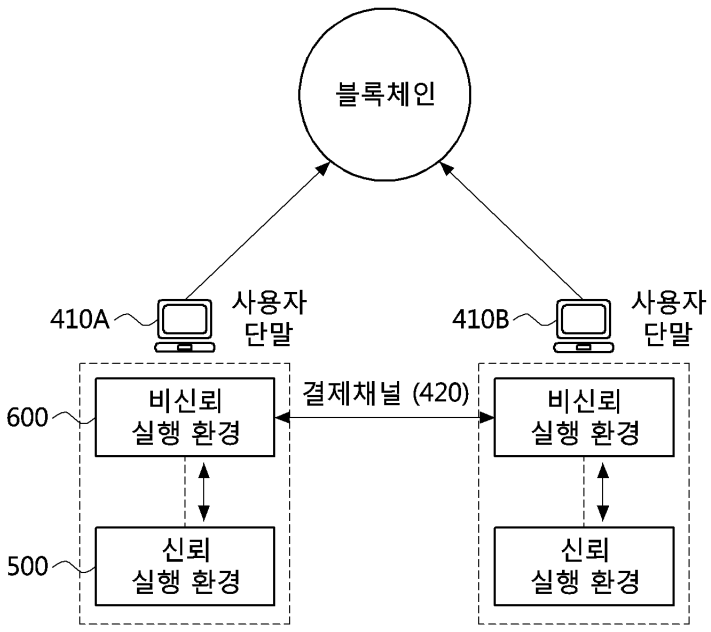
도면2


100
서비스 제공자
서버 (100)
계약 정보
동기화 모듈
110
결제 경로
계산 모듈
120
프로토콜
실행 모듈
130
블록체인 네트워크
통신부
140

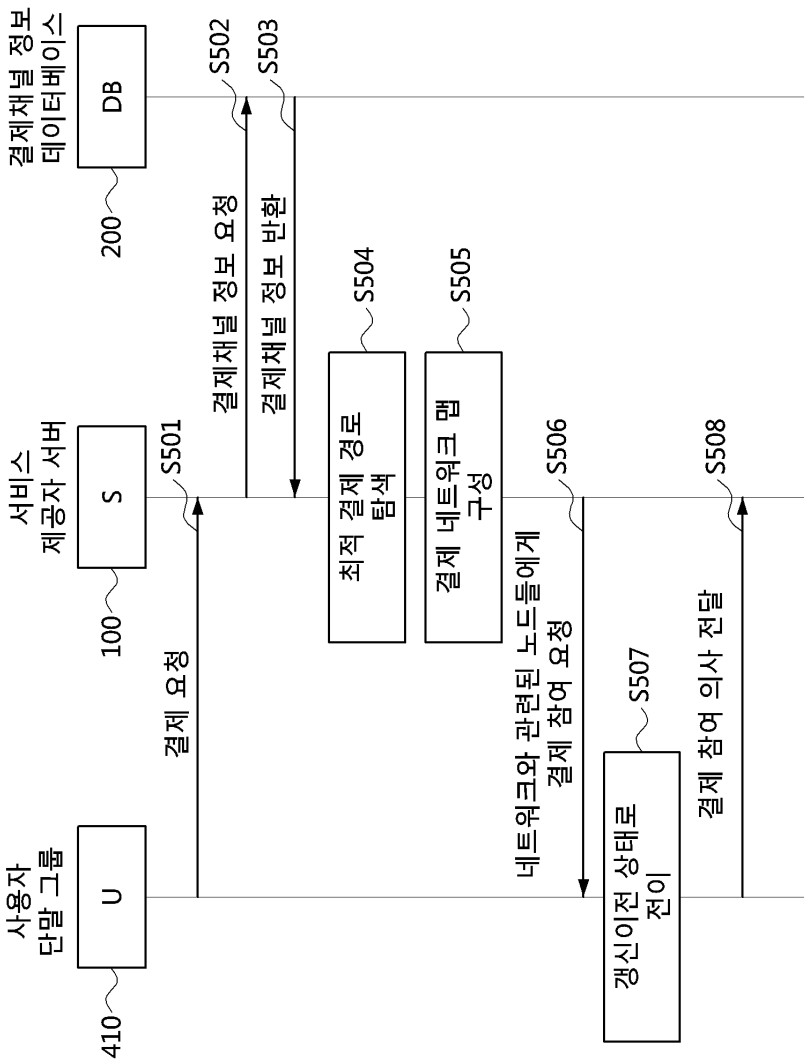
도면3


300
결제 채널 스마트 컨트랙트 (300)
결제 채널 정보
310
프로토콜 방출 정보
320
결제 채널 생성부
330
결제 채널 종료부
340
프로토콜 방출부
350
결제 채널 정산부
360

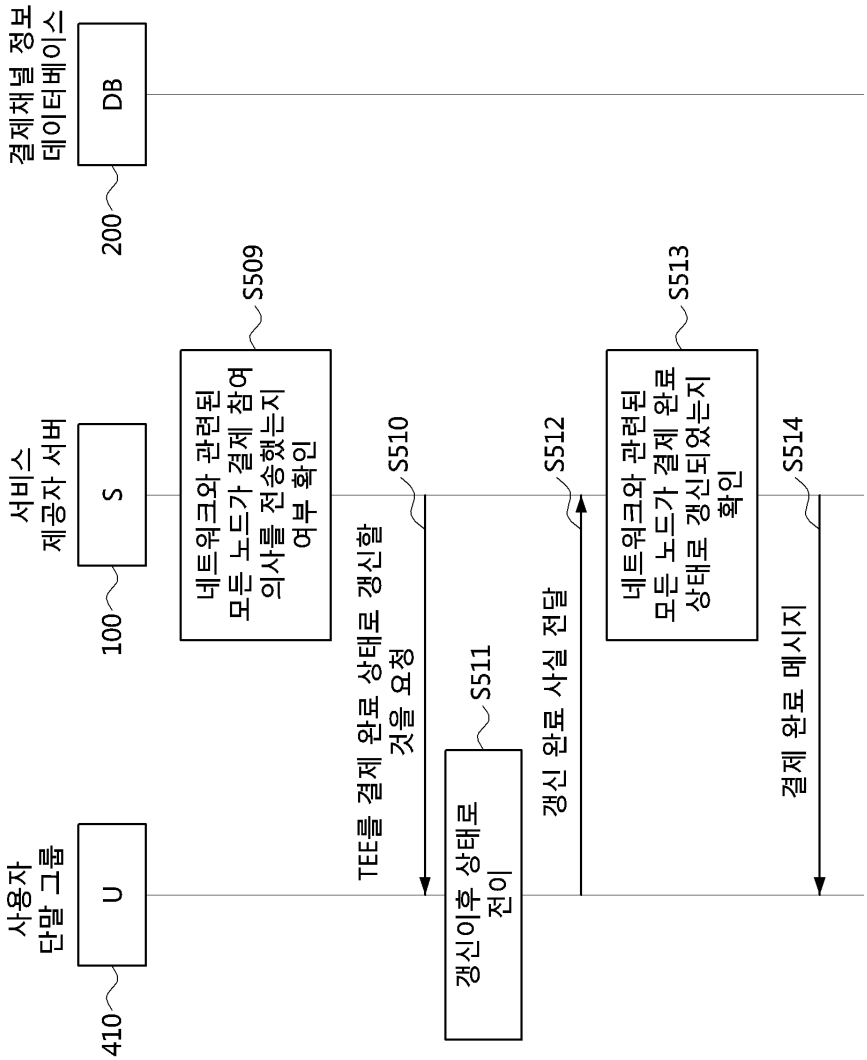
도면4


블록체인
410A
사용자 단말
410B
사용자 단말
600
비신뢰 실행 환경
결제채널 (420)
비신뢰 실행 환경
500
신뢰 실행 환경
신뢰 실행 환경

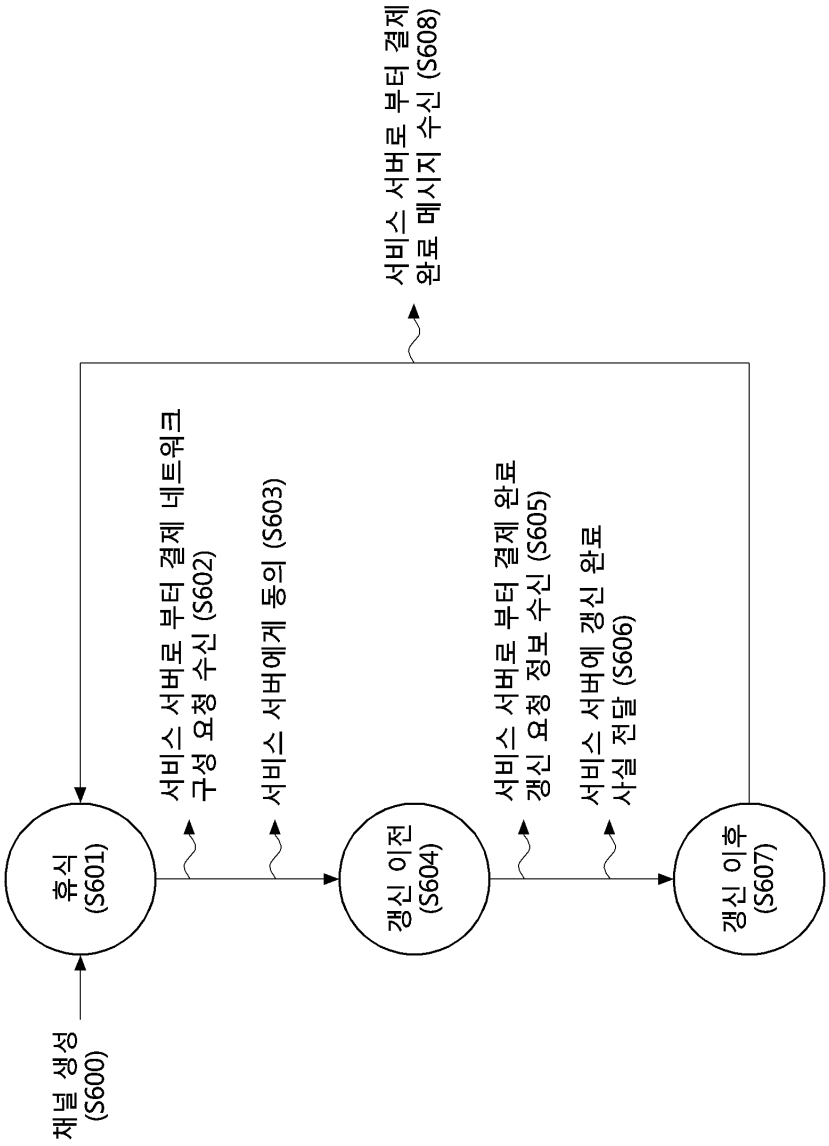
도면5a


결제채널 정보
데이터베이스
DB
200
서비스
제공자 서버
S
100
사용자
단말 그룹
U
410
S501
결제 요청
S502
결제채널 정보 요청
S503
결제채널 정보 반환
S504
최적 결제 경로
탐색
S505
결제 네트워크 맵
구성
S506
네트워크와 관련된 노드들에게
결제 참여 요청
S507
갱신이전 상태로
전이
S508
결제 참여 의사 전달

도면5b


결제채널 정보
데이터베이스
DB
200
서비스
제공자 서버
S
100
사용자
단말 그룹
U
410
S509
네트워크와 관련된
모든 노드가 결제 참여
의사를 전송했는지
여부 확인
S510
TEE를 결제 완료 상태로 갱신할
것을 요청
S511
갱신이후 상태로
전이
S512
갱신 완료 사실 전달
S513
네트워크와 관련된
모든 노드가 결제 완료
상태로 갱신되었는지
확인
S514
결제 완료 메시지

도면6


채널 생성
(S600)
휴식
(S601)
서비스 서버로 부터 결제 네트워크
구성 요청 수신 (S602)
서비스 서버에게 동의 (S603)
갱신 이전
(S604)
서비스 서버로 부터 결제 완료
갱신 요청 정보 수신 (S605)
서비스 서버에 갱신 완료
사실 전달 (S606)
갱신 이후
(S607)
서비스 서버로 부터 결제
완료 메시지 수신 (S608)