(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2022-0118796
(43) 공개일자 2022년08월26일

(51) 국제특허분류(Int. Cl.)
G06F 21/60 (2013.01) *G06F 21/62* (2013.01)
H04L 65/40 (2022.01) *H04L 9/40* (2022.01)
(52) CPC특허분류
G06F 21/604 (2013.01)
G06F 21/602 (2013.01)
(21) 출원번호 10-2021-0022691
(22) 출원일자 2021년02월19일
심사청구일자 2021년02월19일

(71) 출원인
부경대학교 산학협력단
부산광역시 남구 용소로 45, 부경대학교내 (대연동)
(72) 발명자
이경현
부산광역시 남구 신선로 566, 308동 2903호 (용호동, GS하이츠자이)
노시완
부산광역시 북구 은행나무로36번길 45-14 (만덕동)
(74) 대리인
특허법인위더피플

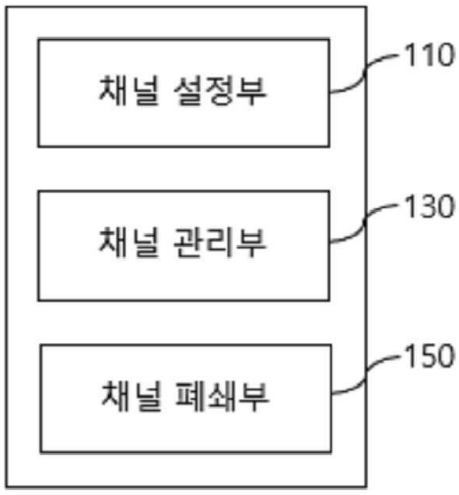
전체 청구항 수 : 총 10 항

(54) 발명의 명칭 **퍼블릭 블록체인에서의 개인 간 데이터 거래 및 공유를 지원하는 액세스 제어 시스템 및 방법**

(57) 요 약

본 발명은 퍼블릭 블록체인에서의 개인 간 데이터 거래 및 공유를 지원하는 액세스 제어 시스템 및 방법을 개시한다. 본 발명의 일 측면에 따른 퍼블릭 블록체인에서의 개인 간 데이터 거래 및 공유를 지원하는 액세스 제어 시스템은, 데이터 소유자와 데이터 요청자가 외부 저장소에 저장된 데이터에 대한 액세스를 제어하기 위한 오프 체인 채널을 생성하는 채널 설정부; 데이터 소유자와 데이터 요청자에 의해 생성된 오프 체인 채널의 상태를 변경하는 트랜잭션을 관리하고, 온 체인에 저장된 채널의 초기 상태를 적절한 액세스 제어 정책으로 변환하는 트랜잭션을 기반으로 데이터 요청자의 액세스 권한 요청을 검증하는 채널 관리부; 및 데이터 소유자와 데이터 요청자 간에 액세스 제어가 더 이상 필요하지 않을 경우, 오프 체인 채널을 폐쇄하는 채널 폐쇄부;를 포함한다.

대 표 도 - 도1



(52) CPC특허분류
G06F 21/6245 (2013.01)
H04L 63/0428 (2013.01)
H04L 63/10 (2013.01)
H04L 67/1097 (2022.05)

이 발명을 지원한 국가연구개발사업
과제고유번호 1711055315
과제번호 2017-0-00156
부처명 과학기술정보통신부
과제관리(전문)기관명 정보통신기획평가원
연구사업명 정보통신방송 연구개발사업
연구과제명 블록체인의 정보보호 프레임워크 및 평가 방법 개발
기 여 율 1/2
과제수행기관명 부경대학교산학협력단
연구기간 2018.01.01 ~ 2018.12.31
이 발명을 지원한 국가연구개발사업
과제고유번호 1711119147
과제번호 2020-0-01596
부처명 과학기술정보통신부
과제관리(전문)기관명 정보통신기획평가원
연구사업명 글로벌핵심인재양성지원
연구과제명 고신뢰 데이터 라이프 사이클링을 위한 ICT 융합 선도기술 연구 및 인재양성
기 여 율 1/2
과제수행기관명 순천향대학교산학협력단
연구기간 2020.06.01 ~ 2021.05.31

명 세 서

청구범위

청구항 1

데이터 소유자와 데이터 요청자가 외부 저장소에 저장된 데이터에 대한 액세스를 제어하기 위한 오프 체인 채널을 생성하는 채널 설정부;

데이터 소유자와 데이터 요청자에 의해 생성된 오프 체인 채널의 상태를 변경하는 트랜잭션을 관리하고, 온 체인에 저장된 채널의 초기 상태를 적절한 액세스 제어 정책으로 변환하는 트랜잭션을 기반으로 데이터 요청자의 액세스 권한 요청을 검증하는 채널 관리부; 및

데이터 소유자와 데이터 요청자 간에 액세스 제어가 더 이상 필요하지 않을 경우, 오프 체인 채널을 폐쇄하는 채널 폐쇄부;를 포함하는 퍼블릭 블록체인에서의 개인 간 데이터 거래 및 공유를 지원하는 액세스 제어 시스템.

청구항 2

제 1 항에 있어서,

상기 오프 체인 채널의 상태는,

스토리지 계층에 저장된 특정 데이터에 대한 액세스 제어 정책인 것을 특징으로 하는 퍼블릭 블록체인에서의 개인 간 데이터 거래 및 공유를 지원하는 액세스 제어 시스템.

청구항 3

제 1 항에 있어서,

상기 데이터 소유자는,

공유하려는 데이터를 클라우드 스토리지에 저장하고, 상태 채널을 설정하여 오프 체인 채널의 상태 전환을 기반으로 데이터에 대한 액세스를 관리하고,

상기 데이터 요청자는,

상기 데이터 소유자가 클라우드 스토리지에 저장한 데이터에 대한 액세스 권한을 획득하고, 스토리지 키퍼에게 상기 권한이 획득된 데이터에 액세스하도록 요청하며,

상기 스토리지 키퍼는,

저장된 데이터를 클라우드 스토리지에 안전하게 보관하고, 적절한 권한이 있는 사용자에게만 요청된 데이터를 제공하는 것을 특징으로 하는 퍼블릭 블록체인에서의 개인 간 데이터 거래 및 공유를 지원하는 액세스 제어 시스템.

청구항 4

제 3 항에 있어서,

상기 데이터 소유자는,

데이터를 저장하기 전에 암호화하는 것을 특징으로 하는 퍼블릭 블록체인에서의 개인 간 데이터 거래 및 공유를 지원하는 액세스 제어 시스템.

청구항 5

제 3 항에 있어서,

상기 스토리지 키퍼는,

상기 데이터 요청자가 증거와 함께 저장된 데이터에 액세스하기 위한 오프 체인 상태를 제출할 때, 온 체인에 기록된 정보를 기반으로 제출된 상태 및 증거의 유효성을 확인하는 것을 특징으로 하는 퍼블릭 블록체인에서의

개인 간 데이터 거래 및 공유를 지원하는 액세스 제어 시스템.

청구항 6

퍼블릭 블록체인에서의 개인 간 데이터 거래 및 공유를 지원하는 액세스 제어 시스템에서의 액세스 제어 방법에 있어서,

데이터 소유자와 데이터 요청자가 외부 저장소에 저장된 데이터에 대한 액세스를 제어하기 위한 오프 체인 채널을 생성하는 채널 설정 단계;

데이터 소유자와 데이터 요청자에 의해 생성된 오프 체인 채널의 상태를 변경하는 트랜잭션을 관리하고, 온 체인에 저장된 채널의 초기 상태를 적절한 액세스 제어 정책으로 변환하는 트랜잭션을 기반으로 데이터 요청자의 액세스 권한 요청을 검증하는 채널 관리 단계; 및

데이터 소유자와 데이터 요청자 간에 액세스 제어가 더 이상 필요하지 않을 경우, 오프 체인 채널을 폐쇄하는 채널 폐쇄 단계;를 포함하는 액세스 제어 방법.

청구항 7

제 6 항에 있어서,

상기 오프 체인 채널의 상태는,

스토리지 계층에 저장된 특정 데이터에 대한 액세스 제어 정책인 것을 특징으로 하는 액세스 제어 방법.

청구항 8

제 6 항에 있어서,

상기 데이터 소유자는,

공유하려는 데이터를 클라우드 스토리지에 저장하고, 상태 채널을 설정하여 오프 체인 채널의 상태 전환을 기반으로 데이터에 대한 액세스를 관리하고,

상기 데이터 요청자는,

상기 데이터 소유자가 클라우드 스토리지에 저장한 데이터에 대한 액세스 권한을 획득하고, 스토리지 키퍼에게 상기 권한이 획득된 데이터에 액세스하도록 요청하며,

상기 스토리지 키퍼는,

저장된 데이터를 클라우드 스토리지에 안전하게 보관하고, 적절한 권한이 있는 사용자에게만 요청된 데이터를 제공하는 것을 특징으로 하는 액세스 제어 방법.

청구항 9

제 8 항에 있어서,

상기 데이터 소유자는,

데이터를 저장하기 전에 암호화하는 것을 특징으로 하는 액세스 제어 방법.

청구항 10

제 8 항에 있어서,

상기 스토리지 키퍼는,

상기 데이터 요청자가 증거와 함께 저장된 데이터에 액세스하기 위한 오프 체인 상태를 제출할 때, 온 체인에 기록된 정보를 기반으로 제출된 상태 및 증거의 유효성을 확인하는 것을 특징으로 하는 액세스 제어 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 퍼블릭 블록체인에서의 개인 간 데이터 거래 및 공유를 지원하는 액세스 제어 시스템 및 방법에 관한 것으로, 더욱 상세하게는 오프 체인 상태 채널을 기반으로 하여 개인 간 데이터 거래 및 공유를 지원하는 퍼블릭 블록체인에서의 개인 간 데이터 거래 및 공유를 지원하는 액세스 제어 시스템 및 방법에 관한 것이다.

배 경 기 술

[0003] 블록 체인은 중앙화된 개체에 대한 종속 문제를 해결하기 위해 중앙 집중화된 개체의 역할을 시스템 참여자의 합의로 대체하여 분산형 시스템을 구현할 수 있는 기술이다. 블록 체인 기술은 다양한 분야에서 적용되는 것으로 고려되고 있다. 그러나, 퍼블릭 블록 체인의 확장성 한계로 인해 많은 연구자들이 시스템의 보안을 낮추면서 확장성을 향상시키는 프라이빗 블록 체인을 고려하게 되었다. 상태 채널은 블록 체인 네트워크의 보안을 보장하면서 퍼블릭 블록 체인 확장성 문제를 해결하기 위한 여러 확장성 솔루션 중에서 선도적인 접근 방식을 나타낸다. 채널의 참가자는 블록 체인 외부의 채널 상태를 업데이트하는 프로세스를 수행한다. 이 프로세스는 블록 체인 네트워크의 합의가 필요하지 않기 때문에 매우 빠르게 진행할 수 있지만, 여전히 온 체인과 같이 비가역성 같은 기능을 보장할 수 있다.

[0004] 따라서, 거래 콘텐츠에 대한 개인 정보 보호화 함께 확장성 문제로 인한 제약을 해결하면서 악의적인 참여자가 채널의 이전 상태를 임의로 사용하는 것을 방지할 수 있는 시스템에 대한 연구가 필요한 실정이다.

선행기술문헌

특허문헌

[0006] (특허문헌 0001) 한국공개특허 제2020-0131307호(2020.11.23 공개)

발명의 내용

해결하려는 과제

[0007] 본 발명은 상기와 같은 문제점을 해결하기 위해 제안된 것으로서, 거래 콘텐츠에 대한 개인 정보 보호와 함께 확장성 문제로 인한 제약을 해결할 수 있는 퍼블릭 블록체인에서의 개인 간 데이터 거래 및 공유를 지원하는 액세스 제어 시스템 및 방법을 제공하는데 그 목적이 있다.

[0008] 본 발명의 다른 목적 및 장점들은 하기의 설명에 의해서 이해될 수 있으며, 본 발명의 일 실시예에 의해 보다 분명하게 알게 될 것이다. 또한, 본 발명의 목적 및 장점들은 특허청구범위에 나타낸 수단 및 그 조합에 의해 실현될 수 있음을 쉽게 알 수 있을 것이다.

과제의 해결 수단

[0010] 상기와 같은 목적을 달성하기 위한 본 발명의 일 측면에 따른 퍼블릭 블록체인에서의 개인 간 데이터 거래 및 공유를 지원하는 액세스 제어 시스템은, 데이터 소유자와 데이터 요청자가 외부 저장소에 저장된 데이터에 대한 액세스를 제어하기 위한 오프 체인 채널을 생성하는 채널 설정부; 데이터 소유자와 데이터 요청자에 의해 생성된 오프 체인 채널의 상태를 변경하는 트랜잭션을 관리하고, 온 체인에 저장된 채널의 초기 상태를 적절한 액세스 제어 정책으로 변환하는 트랜잭션을 기반으로 데이터 요청자의 액세스 권한 요청을 검증하는 채널 관리부; 및 데이터 소유자와 데이터 요청자 간에 액세스 제어가 더 이상 필요하지 않을 경우, 오프 체인 채널을 폐쇄하는 채널 폐쇄부;를 포함한다.

[0011] 상기 오프 체인 채널의 상태는, 스토리지 계층에 저장된 특정 데이터에 대한 액세스 제어 정책인 것을 특징으로 한다.

[0012] 상기 데이터 소유자는, 공유하려는 데이터를 클라우드 스토리지에 저장하고, 상태 채널을 설정하여 오프 체인 채널의 상태 전환을 기반으로 데이터에 대한 액세스를 관리하고, 상기 데이터 요청자는, 상기 데이터 소유자가 클라우드 스토리지에 저장한 데이터에 대한 액세스 권한을 획득하고, 스토리지 키퍼에게 상기 권한이 획득된 데이터에 액세스하도록 요청하며, 상기 스토리지 키퍼는, 저장된 데이터를 클라우드 스토리지에 안전하게 보관하고, 적절한 권한이 있는 사용자에게만 요청된 데이터를 제공하는 것을 특징으로 한다.

[0013] 상기 데이터 소유자는, 데이터를 저장하기 전에 암호화하는 것을 특징으로 한다.

[0014] 상기 스토리지 키퍼는, 상기 데이터 요청자가 증거와 함께 저장된 데이터에 액세스하기 위한 오프 체인 상태를 제출할 때, 온 체인에 기록된 정보를 기반으로 제출된 상태 및 증거의 유효성을 확인하는 것을 특징으로 한다.

[0015] 상기와 같은 목적을 달성하기 위한 본 발명의 다른 측면에 따른 퍼블릭 블록체인에서의 개인 간 데이터 거래 및 공유를 지원하는 액세스 제어 시스템에서의 액세스 제어 방법은, 데이터 소유자와 데이터 요청자가 외부 저장소에 저장된 데이터에 대한 액세스를 제어하기 위한 오프 체인 채널을 생성하는 채널 설정 단계; 데이터 소유자와 데이터 요청자에 의해 생성된 오프 체인 채널의 상태를 변경하는 트랜잭션을 관리하고, 온 체인에 저장된 채널의 초기 상태를 적절한 액세스 제어 정책으로 변환하는 트랜잭션을 기반으로 데이터 요청자의 액세스 권한 요청을 검증하는 채널 관리 단계; 및 데이터 소유자와 데이터 요청자 간에 액세스 제어가 더 이상 필요하지 않을 경우, 오프 체인 채널을 폐쇄하는 채널 폐쇄 단계;를 포함한다.

[0016] 상기 오프 체인 채널의 상태는, 스토리지 계층에 저장된 특정 데이터에 대한 액세스 제어 정책인 것을 특징으로 한다.

[0017] 상기 데이터 소유자는, 공유하려는 데이터를 클라우드 스토리지에 저장하고, 상태 채널을 설정하여 오프 체인 채널의 상태 전환을 기반으로 데이터에 대한 액세스를 관리하고, 상기 데이터 요청자는, 상기 데이터 소유자가 클라우드 스토리지에 저장한 데이터에 대한 액세스 권한을 획득하고, 스토리지 키퍼에게 상기 권한이 획득된 데이터에 액세스하도록 요청하며, 상기 스토리지 키퍼는, 저장된 데이터를 클라우드 스토리지에 안전하게 보관하고, 적절한 권한이 있는 사용자에게만 요청된 데이터를 제공하는 것을 특징으로 한다.

[0018] 상기 데이터 소유자는, 데이터를 저장하기 전에 암호화하는 것을 특징으로 한다.

[0019] 상기 스토리지 키퍼는, 상기 데이터 요청자가 증거와 함께 저장된 데이터에 액세스하기 위한 오프 체인 상태를 제출할 때, 온 체인에 기록된 정보를 기반으로 제출된 상태 및 증거의 유효성을 확인하는 것을 특징으로 한다.

발명의 효과

[0021] 본 발명의 일 측면에 따르면, 거래 콘텐츠에 대한 개인 정보 보호와 함께 확장성 문제로 인한 제약을 해결하면서, 악의적인 참여자가 채널의 이전 상태를 임의로 사용하는 것을 방지할 수 있는 효과가 있다.

[0022] 또한, 상태 채널의 트랜잭션 처리를 오프 체인(블록 체인의 외부)에서 수행함으로써, 블록 체인 3중고(트릴 레마)를 해결하고 오프 체인 채널에서 사용자 간의 트랜잭션을 처리하고 결과만 블록 체인에 기록함으로써, 트랜잭션 처리량을 크게 향상시킬 수 있는 효과가 있다.

[0023] 본 발명에서 얻을 수 있는 효과는 이상에서 언급한 효과로 제한되지 않으며, 언급하지 않은 또 다른 효과들은 아래의 기재로부터 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에게 명확하게 이해될 수 있을 것이다.

도면의 간단한 설명

[0025] 본 명세서에 첨부되는 다음의 도면들은 본 발명의 바람직한 실시예를 예시하는 것이며, 발명을 실시하기 위한 구체적인 내용들과 함께 본 발명의 기술사상을 더욱 이해시키는 역할을 하는 것이므로, 본 발명은 그러한 도면에 기재된 사항에만 한정되어 해석되어서는 아니 된다.

도 1은 본 발명의 일 실시예에 따른 시스템의 개략적인 기능 블록도,

도 2는 본 발명의 일 실시예에 따른 시스템의 개략적인 구조의 일 예,

도 3은 본 발명의 일 실시예에 따른 상태 채널의 일 예,

도 4는 본 발명의 일 실시예에 따른 시스템에서의 액세스 제어 방법의 개략적인 흐름도,

도 5는 본 발명의 일 실시예에 따른 채널 설정 단계 트랜잭션의 일 예,

도 6은 본 발명의 일 실시예에 따른 채널 관리 단계 트랜잭션(액세스 권한 부여)의 일 예,

도 7은 본 발명의 일 실시예에 따른 채널 관리 단계 트랜잭션(권한 수정)의 일 예,

도 8은 본 발명의 일 실시예에 따른 오프 체인 채널의 상태 전환의 일 예 이다.

발명을 실시하기 위한 구체적인 내용

[0026] 상술한 목적, 특징 및 장점은 첨부된 도면과 관련한 다음의 상세한 설명을 통하여 보다 분명해질 것이며, 그에 따라 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자가 본 발명의 기술적 사상을 용이하게 실시할 수 있을 것이다. 또한, 본 발명을 설명함에 있어서 본 발명과 관련된 공지기술에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략하기로 한다. 이하, 첨부된 도면을 참조하여 본 발명에 따른 바람직한 일 실시예를 상세히 설명하기로 한다.

[0027] 명세서 전체에서, 어떤 부분이 어떤 구성요소를 “포함”한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성 요소를 더 포함할 수 있는 것을 의미한다. 또한, 명세서에 기재된 “…부” 등의 용어는 적어도 하나의 기능이나 동작을 처리하는 단위를 의미하며, 이는 하드웨어나 소프트웨어 또는 하드웨어 및 소프트웨어의 결합으로 구현될 수 있다.

[0028] 도 1은 본 발명의 일 실시예에 따른 시스템의 개략적인 기능 블록도, 도 2는 본 발명의 일 실시예에 따른 시스템의 개략적인 구조의 일 예, 도 3은 본 발명의 일 실시예에 따른 상태 채널의 일 예이다.

[0029] 도 1을 참조하면, 본 실시예에 따른 퍼블릭 블록체인에서의 개인 간 데이터 거래 및 공유를 지원하는 액세스 제어 시스템은 채널 설정부(110), 채널 관리부(130) 및 채널 폐쇄부(150)를 포함한다.

[0030] 채널 설정부(110)는 데이터 소유자와 데이터 요청자가 외부 저장소에 저장된 데이터에 대한 액세스를 제어하기 위한 오프 체인 채널을 생성한다. 이때, 오프 체인 채널의 상태는, 스토리지 계층에 저장된 특정 데이터에 대한 액세스 제어 정책일 수 있다.

[0031] 채널 관리부(130)는 데이터 소유자와 데이터 요청자에 의해 생성된 오프 체인 채널의 상태를 변경하는 트랜잭션을 관리하고, 온 체인에 저장된 채널의 초기 상태를 적절한 액세스 제어 정책으로 변환하는 트랜잭션을 기반으로 데이터 요청자의 액세스 권한 요청을 검증한다.

[0032] 채널 폐쇄부(150)는 데이터 소유자와 데이터 요청자 간에 액세스 제어가 더 이상 필요하지 않을 경우, 오프 체인 채널을 폐쇄한다.

[0033] 한편, 상술한 바와 같은 본 발명의 일 실시예에 따른 시스템은 참가자로서 데이터 소유자, 데이터 요청자 및 스토리지 키퍼를 포함한다.

[0034] 데이터 소유자는, 공유하려는 데이터를 클라우드 스토리지에 저장하고, 상태 채널을 설정하여 오프 체인 채널의 상태 전환을 기반으로 데이터에 대한 액세스를 관리하고, 데이터 요청자는, 데이터 소유자가 클라우드 스토리지에 저장한 데이터에 대한 액세스 권한을 획득하고, 스토리지 키퍼에게 상기 권한이 획득된 데이터에 액세스하도록 요청하며, 스토리지 키퍼는, 저장된 데이터를 클라우드 스토리지에 안전하게 보관하고, 적절한 권한이 있는 사용자에게만 요청된 데이터를 제공할 수 있다. 이때, 데이터 소유자, 데이터 요청자 및 스토리지 키퍼는 모듈 형태일 수도 있다. 이때, 데이터 소유자는, 데이터를 저장하기 전에 암호화하는 것이 바람직하다. 또한, 스토리지 키퍼는, 데이터 요청자가 증거와 함께 저장된 데이터에 액세스하기 위한 오프 체인 상태를 제출할 때, 온 체인에 기록된 정보를 기반으로 제출된 상태 및 증거의 유효성을 확인할 수 있다.

[0036] 한편, 본 실시예에 따른 시스템에서 각 참가자의 역할을 요약하면 아래와 같다.

[0037] *데이터 소유자

[0038] 데이터 소유자는 다른 사람과 공유하려는 데이터를 클라우드 스토리지에 저장한다. 권한이 없는 사용자에 의한

데이터 노출을 방지하려면, 데이터를 저장하기 전에 암호화해야한다. 데이터 소유자는 다른 사용자가 이러한 데이터에 액세스할 수 있도록 상태 채널을 설정하고 오프 체인 채널의 상태 전환을 기반으로 데이터에 대한 액세스를 관리한다.

[0039] *데이터 요청자

[0040] 데이터 요청자는 클라우드 스토리지에 저장된 데이터 소유자의 데이터에 액세스하려고 한다. 이를 통해, 데이터 소유자의 데이터에 대한 적절한 액세스 권한을 얻은 후 데이터 요청자는 스토리지 키퍼에게 이러한 데이터에 액세스하도록 요청한다.

[0041] *스토리지 키퍼

[0042] 스토리지 키퍼는 저장된 데이터를 안전하게 보관하고 적절한 권한이 있는 사용자에게만 요청된 데이터를 제공한다. 데이터 요청자가 해당 증거와 함께 저장된 데이터에 액세스하기 위해 오프 체인 상태를 제출할 때, 그들은 온 체인에 기록된 정보를 기반으로 제출된 상태 및 증거의 유효성을 확인한다.

[0043] 도 2를 참조하면, 본 실시예에 따른 퍼블릭 블록체인에서의 개인 간 데이터 거래 및 공유를 지원하는 액세스 제어 시스템은 3개의 레이어로 구성될 수 있다.

[0044] 첫번째 계층은 데이터 소유자와 데이터에 대한 액세스를 요청하는 사용자가 데이터 액세스를 올바르게 관리하기 위해 상태 채널을 만드는 애플리케이션 계층(210)이다. 본 발명의 시스템에서 오프 체인 채널의 상태는 데이터 소유자가 보유한 특정 데이터에 대한 채널 참가자의 액세스 권한을 나타낸다. 이때, 상태 채널은 블록 체인 3중고(트릴 레마)를 해결하고 오프 체인 채널에서 사용자 간의 트랜잭션을 처리하고, 결과만 블록 체인에 기록함으로써 트랜잭션 처리량을 크게 향상시킬 수 있다. 상태 채널의 트랜잭션 처리는 블록 체인 외부(오프 체인이라고 함)에서 수행되므로 퍼블릭 블록 체인의 확률적 최종성에 관계없이 빠른 트랜잭션 처리량을 보장할 수 있다. 또한, 상태 채널에는 두 가지 장점이 있다. 첫째, 트랜잭션 처리가 블록 체인 외부에서 이루어지므로, 블록 체인 네트워크가 리소스를 소비하지 않기 때문에 트랜잭션 처리 수수료가 필요하지 않다. 둘째, 사용자간에 지속적인 거래가 발생하면 도 3과 같이 거래의 첫번째와 최종 상태만 블록 체인에 기록하여 개인 정보 보호를 제공할 수 있다. 상태 채널은 모든 채널 참여자가 동의한 채널의 초기 상태를 블록 체인에 기록하는 시점부터 참여자 중 한 명에 의해 채널의 다양한 상태 중 하나가 블록 체인 네트워크에 전파될 때까지 유효하다. 그러나, 채널에서 생성되는 모든 오프 체인 상태는 채널의 참가자가 언제든지 블록 체인 네트워크로 전파할 수 있는 유효한 상태이다. 따라서, 참가자는 참가자 간에 합의된 최종 상태를 전파하는 대신 상대방의 동의없이 자신의 이익을 위해 블록 체인 네트워크에 이전에 동의한 과거 상태를 최종 상태로 전파할 수 있다.

[0045] 둘째, 블록 체인 계층(220)은 블록 체인의 애플리케이션 계층에서 생성된 오프 체인 채널의 상태를 기록하고 이를 이용하여 스토리지 계층에서 액세스 권한을 검증한다.

[0046] 마지막으로, 스토리지 계층(230)은 사용자가 생성하고 다른 사용자와 공유하려는 데이터를 저장한다. 스토리지 계층에 대한 액세스는 적절한 권한이 있는 사용자에게만 요청된 데이터를 제공하는 스토리지 키퍼에 의해 제어된다.

[0048] 도 4는 본 발명의 일 실시예에 따른 시스템에서의 액세스 제어 방법의 개략적인 흐름도, 도 5는 본 발명의 일 실시예에 따른 채널 설정 단계 트랜잭션의 일 예, 도 6은 본 발명의 일 실시예에 따른 채널 관리 단계 트랜잭션(액세스 권한 부여)의 일 예, 도 7은 본 발명의 일 실시예에 따른 채널 관리 단계 트랜잭션(권한 수정)의 일 예, 도 8은 본 발명의 일 실시예에 따른 오프 체인 채널의 상태 전환의 일 예 이다.

[0049] 도 4를 참조하면, 본 실시예에 따른 액세스 제어 방법은, 채널 생성 단계(S410), 채널 관리 단계(S420) 및 채널 폐쇄 단계(S430)를 포함한다.

[0050] S410 단계는 데이터 소유자와 데이터 요청자가 외부 저장소에 저장된 데이터에 대한 액세스를 제어하기 위한 오프 체인 채널을 생성한다. S410 단계에서, 데이터 소유자와 데이터 요청자는 데이터 소유자가 외부 저장소에 저장된 데이터에 대한 액세스를 제어하기 위해 오프 체인 채널을 생성한다.

[0051] S420 단계는 데이터 소유자와 데이터 요청자에 의해 생성된 오프 체인 채널의 상태를 변경하는 트랜잭션을 관리하고, 온 체인에 저장된 채널의 초기 상태를 적절한 액세스 제어 정책으로 변환하는 트랜잭션을 기반으로 데이터 요청자의 액세스 권한 요청을 검증한다. S420 단계에서, 데이터 소유자는 설정 단계에서 생성된 오프 체인

채널의 상태를 변경하는 트랜잭션을 생성하고 두 참가자는 이를 개별적으로 저장한다. 본 발명의 시스템에서 오프 체인 채널의 상태는 스토리지 계층에 저장된 특정 데이터에 대한 액세스 제어 정책을 나타낸다. 스토리지 키퍼는 온 체인에 저장된 채널의 초기 상태를 적절한 액세스 제어 정책으로 변환하는 트랜잭션을 기반으로 데이터 요청자의 요청을 검증한다. 채널의 상태가 변경될 때마다 데이터 소유자는 데이터 요청자가 요청에서 채널의 이전 상태를 사용하지 못하도록하는 암시적취소를 실행한다.

[0052] S430 단계는 데이터 소유자와 데이터 요청자 간에 액세스 제어가 더 이상 필요하지 않을 경우, 오프 체인 채널을 폐쇄한다. S430 단계에서, 데이터 소유자와 데이터 요청자 간에 액세스 제어가 더 이상 필요하지 않을 때 오프 체인 채널을 닫는 작업을 처리한다. 본 발명의 시스템에서 데이터 액세스 제어를 수행하기 위해 사용자는 다음과 같이 세가지 트랜잭션을 생성한다.

[0053] * 펀딩 트랜잭션(T_{State0}) : 오프 체인 채널을 생성하는 첫번째 거래로 두 사용자(즉, 데이터 소유자 및 데이터 요청자)가 펀딩 거래를 생성하여 자신의 암호 화폐를 채널에 입금한다. 펀딩 거래는 사용자의 예치금이 2 분의 2의 다중 서명 주소(초기 상태)로 이체되고, 일정 시간이 지나면 채널의 예치금이 원래 소유자에게 반환되는 두 가지 유형의 거래로 구성된다(환불 거래).

[0054] * 상태 트랜잭션(T_{Staten}) : 상태 트랜잭션을 생성함으로써 채널의 참가자는 t_{settle} 후, 온 체인에 기록된 환불 트랜잭션이 블록 체인에 포함될 때까지 채널의 상태(즉, 초기 상태 $State_0$에 기록된 예금의 재분배)를 변경할 수 있다. 유효한 상태 트랜잭션에는 채널의 모든 참가자의 디지털 서명과 암호 화폐의 표준 트랜잭션 구조(예 : 비트 코인, 이더리움)와 같은 데이터 소유자 및 요청자의 블록 체인 주소가 포함된다. 그러나, 표준 트랜잭션 구조와 달리 상태 트랜잭션의 서명에는 사용자가 서명의 메시지로 공유하려는 데이터의 해시값이 포함된다. 따라서, 상대방의 동의없이 상태 트랜잭션이 블록 체인 네트워크를 통해 전파되더라도 전파된 트랜잭션은 블록 체인에 포함될 수 없다(잘못된 구조를 가지고 있기 때문). 유효한 상태 트랜잭션을 획득한 후 데이터 요청자는 오프 체인 채널에서 생성된 스토리지 트랜잭션과 함께 디지털 서명을 생성하여 해당 스토리지 키퍼에게 제출한다. 데이터 소유자가 액세스 제어 정책을 수정하려는 경우, 새 채널을 설정하지 않고도 서명에 포함된 해시값을 새 데이터의 해시값으로 변경하는 새 상태 트랜잭션을 만든다.

[0055] * 취소된 상태 트랜잭션(RT_{Staten}) : 상태 트랜잭션과 달리 해지된 상태 트랜잭션의 서명에는 공유 데이터의 해시값이 포함되지 않는다. 결과적으로, 취소된 상태 트랜잭션은 블록 체인 네트워크로 전파되고 블록 체인에 포함될 수 있으며, 이는 데이터 요청자가 액세스 요청에서 채널의 오래된 상태를 사용하는 것을 방지하는데 사용된다.

[0057] <실시예>

[0058] 1. 채널 설정

[0059] 양 당사자는 개별적으로 자금(협상시 사전 정의된 금액)을 예금으로 하나의 2/2 다중 서명 주소로 입금(거래처의 디지털 서명 제외)하는 동일한 구조의 자금 거래를 개별적으로 생성한다. 서명 교환 명령으로 인한 거래의 무단 변경을 방지하기 위해 양 당사자는 개별적으로 환불 거래를 생성할 때까지 서명을 교환하지 않는다. 양 당사자는 도 5와 같이 다음 단계를 실행한다.

[0060] 1) 데이터 요청자는 첫번째 개인키와 공개키 쌍($sk_{데이터\ 요청자,1}$,$pk_{데이터\ 요청자,1}$)에서 파생된 첫번째 주소 $addr_{데이터\ 요청자,1}$을 데이터 소유자에 제공한다.

[0061] 2) 데이터 소유자와 데이터 요청자는 입금을 채널로 보내는 펀딩 거래(이하 FT)와 입금 후 입금을 반환하는 환불 거래를 생성한다.

[0062] 3) 서로의 FT 및 환불 거래를 교환한다.

[0063] 4) 수신된 불완전한 트랜잭션에 서명을 추가한다.

[0064] 5) 마지막으로, 데이터 소유자와 데이터 요청자는 완료된 거래를 블록 체인 네트워크에 전파하여 오프 체인 채널을 구축한다.

[0066] 2. 채널 관리

[0067] 블록 체인에서 FT가 확정되면(즉, FT를 포함하는 블록 깊이가 6 이상임), 데이터 소유자와 데이터 요청자는 새로운 액세스 제어 정책을 나타내기 위해 오프 체인에서 첫번째 상태 트랜잭션을 생성한다. 이 단계에서는, 도 6과 같이 구조가 다른 트랜잭션을 생성한다. 상태 트랜잭션은 오프 체인 채널에 잠긴 데이터 소유자 및 데이터 요청자에 재분배한다. 앞서 설명한 것처럼, 데이터 소유자와 데이터 요청자를 일치시키기 위한 플랫폼이 존재하는 경우 데이터 요청자는 이미 데이터 의 해시값을 알고 있다고 가정한다.

[0068] 1) 데이터 요청자는 임의로 선택된 값 $_1$을 데이터 요청자에 보낸다.

[0069] 2) 데이터 소유자와 데이터 요청자는 도 4와 같이 상태 트랜잭션 T_{state1}을 생성한다(여기서, 서명은 다이제스트 메시지로 데이터 $_{,1}$의 해시값을 포함함).

[0070] 3) 데이터 소유자와 데이터 요청자는 디지털 서명을 상태 트랜잭션에 첨부하고 서로 교환한다.

[0071] 4) 데이터 소유자와 데이터 요청자는 수신된 불완전한 트랜잭션에 디지털 서명을 추가하여 상태 트랜잭션을 완료한다.

[0073] 데이터 요청자는 사용자 인증 및 상태 트랜잭션 T_{state1}에 대한 증명을 제시하여 스토리지 키퍼에게 데이터를 요청한다. 스토리지 키퍼는 데이터 요청자가 제시한 증명과 블록 체인 원장에 표시된 정보를 기반으로 액세스 요청을 검증한다.

[0074] 1) 데이터 요청자는 디지털 서명 $Sig_{sk데이터\ 요청자}()$와 함께 요청 메시지 $m = h_1$, 데이터 소유자, addr, $addr_{데이터\ 요청자}$, FT, $T_{state,\ 1}$, r_1}을 보낸다.

[0075] 2) 스토리지 키퍼는 stateValidate 알고리즘을 사용하여 액세스 요청을 검증한다. stateValidate 알고리즘은 요청이 다음을 충족하는지 확인한다.

[0076] A. 오프 체인 채널의 유효성;

[0077] B. $T_{state,\ 1}$에 포함된 서명을 FT에 포함 된 주소로 확인할 수 있는지 여부;

[0078] C. $T_{state,\ 1}$에 포함된 주소를 사용하여 데이터 요청자가 제시 한 서명을 확인할 수 있는지 여부;

[0079] D. 데이터 요청자가 다이제스트 메시지로 제시 한 r_1에 대한 해시 연산 결과를 사용하여 $T_{state,\ 1}$에 포함 된 서명을 확인할 수 있는지 여부

[0081] 스토리지 키퍼는 상태 트랜잭션에 있는 서명의 메시지 다이제스트에 데이터 요청자가 개체에 대한 액세스 권한을 결정하기 위해 요청한 데이터가 포함되어 있는지 확인할 수 있다. 그러나, 데이터 소유자가 데이터 요청자의 액세스 제어 정책을 수정하기 위해 새 데이터에 대한 서명을 포함하는 새 상태 트랜잭션을 생성하는 경우 데이터 요청자가 과거에 생성된 상태 트랜잭션을 사용하지 않는다고 보장할 수 없다. 따라서, 암묵적인 상태 폐기에 의한 채널 상태의 갱신을 본 발명의 시스템에 적용하여, 데이터 요청자가 과거에 취소된 티켓을 사용하여 접근 권한이 취소된 객체에 접근하면, 도 7과 같이 채널에 예치된 금액을 잃게 된다.

[0082] 1) 데이터 요청자는 무작위로 선택된 값 h_{r2}의 해시값을 새로운 주소 $addr_{데이터\ 요청자,\ 2}$와 함께 데이터 소유자로 보낸다.

[0083] 2) 데이터 소유자와 데이터 요청자는 새로운 상태 트랜잭션 T_{state2}를 생성한다.

[0084] 3) 데이터 요청자는 상태 트랜잭션 T_{state1}과 동일한 구조를 갖는 취소된 상태 트랜잭션 RT_{state1}을 생성한다. 그러나, 서명 메시지 다이제스트에 공유 데이터 $h_{,1}$의 해시값을 포함하지 않는다.

[0085] 4) 데이터 소유자와 데이터 요청자는 디지털 서명을 새로운 상태 트랜잭션에 추가하고 서로 교환한다. 또한, 데이터 요청자만이 RT_{state1}에 대해 동일한 프로세스를 수행하고, RT_{state1}에있는 예금의 소유권을 주장하는 서명을

생성 한 후 데이터 소유자로 보낸다.

[0086] 데이터 소유자 및 데이터 요청자는 수신된 불완전한 트랜잭션에 디지털 서명을 추가하여 수신된 트랜잭션을 완료한다.

[0088] 3. 채널 폐쇄

[0089] 본 발명의 일 실시예에 따른 시스템에서는 아래와 같은 경우 채널 폐쇄를 고려한다.

[0090] A. 데이터 소유자와 데이터 요청자 간에 더 이상의 거래가 없을 경우 클로징 거래를 만들어 이를 블록체인 네트워크에 전파해 채널의 최종 상태를 블록체인에 적용시킨다. 채널의 최종 상태가 블록체인 네트워크로 전파되면 기존에 채널에서 생성된 모든 주거래는 자동으로 무효가 되고 설정 단계에서 잠근 보증금을 돌려준다.

[0091] B. 응답하지 않는 거래 상대방의 경우, 타임락 T_{settle}이 있던 환불거래가 블록체인에 포함되기 때문에 자동으로 채널을 닫아 채널의 예치금을 참가자에게 반환할 수 있다.

[0092] C. 검증 과정에서 이전에 취소 된 상태의 사용이 감지되면, 정직한 스토리지 키퍼는 데이터 요청자에서 데이터 소유자로 받은 취소된 상태 T_{statex}의 사용을 알립니다.

[0093] D. 취소된 상태의 사용이 확인 된 후 데이터 소유자는 취소 된 상태 트랜잭션 RT_{statex}를 블록 체인 네트워크로 전파하고 수정 권한 프로세스에서 데이터 요청자가 받은 서명을 사용하여 RT_{statex}에 있는 데이터 요청자의 예금을 자신의 계정으로 이체합니다.

[0095] 1 단계에서 3 단계로의 채널 상태 전환은 도 6에 나와 있다. 도 6은 액세스 제어 정책이 세번 업데이트되고 채널이 정상적으로 폐쇄되는 시나리오를 보여준다.

[0096] 본 발명의 실시예에 따른 방법들은 애플리케이션으로 구현되거나 다양한 컴퓨터 구성요소를 통하여 수행될 수 있는 프로그램 명령어의 형태로 구현되어 컴퓨터 판독 가능한 기록 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능한 기록 매체는 프로그램 명령어, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 컴퓨터 판독 가능한 기록 매체에 기록되는 프로그램 명령어는, 본 발명을 위한 특별히 설계되고 구성된 것들이거니와 컴퓨터 소프트웨어 분야의 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능한 기록 매체의 예에는, 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체, CD-ROM, DVD와 같은 광기록 매체, 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media) 및 ROM, RAM, 플래시 메모리 등과 같은 프로그램 명령어를 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령어의 예에는, 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드도 포함된다. 상기 하드웨어 장치는 본 발명에 따른 처리를 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[0097] 본 명세서는 많은 특징을 포함하는 반면, 그러한 특징은 본 발명의 범위 또는 특허청구범위를 제한하는 것으로 해석되어서는 아니 된다. 또한, 본 명세서의 개별적인 실시예에서 설명된 특징들은 단일 실시예에서 결합되어 구현될 수 있다. 반대로, 본 명세서의 단일 실시예에서 설명된 다양한 특징들은 개별적으로 다양한 실시예에서 구현되거나, 적절히 결합되어 구현될 수 있다.

[0098] 도면에서 동작들이 특정한 순서로 설명되었으나, 그러한 동작들이 도시된 바와 같은 특정한 순서로 수행되는 것으로 또는 일련의 연속된 순서, 또는 원하는 결과를 얻기 위해 모든 설명된 동작이 수행되는 것으로 이해되어서는 안 된다. 특정 환경에서 멀티태스킹 및 병렬 프로세싱이 유리할 수 있다. 아울러, 상술한 실시예에서 다양한 시스템 구성요소의 구분은 모든 실시예에서 그러한 구분을 요구하지 않는 것으로 이해되어야 한다. 상술한 앱 구성요소 및 시스템은 일반적으로 단일 소프트웨어 제품 또는 멀티플 소프트웨어 제품에 패키지로 구현될 수 있다.

[0099] 이상에서 설명한 본 발명은, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 있어 본 발명의 기술적 사상을 벗어나지 않는 범위 내에서 여러 가지 치환, 변형 및 변경이 가능하므로 전술한 실시예 및 첨부된 도면에 의해 한정되는 것은 아니다.

부호의 설명

[0101] 110 : 채널 설정부

130 : 채널 관리부

150 : 채널 폐쇄부

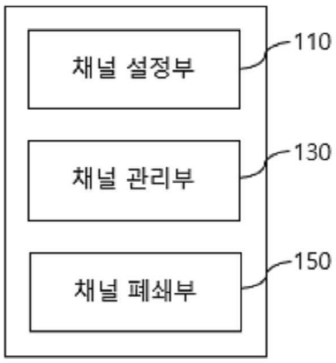
210 : 어플리케이션 계층

220 : 블록 체인 계층

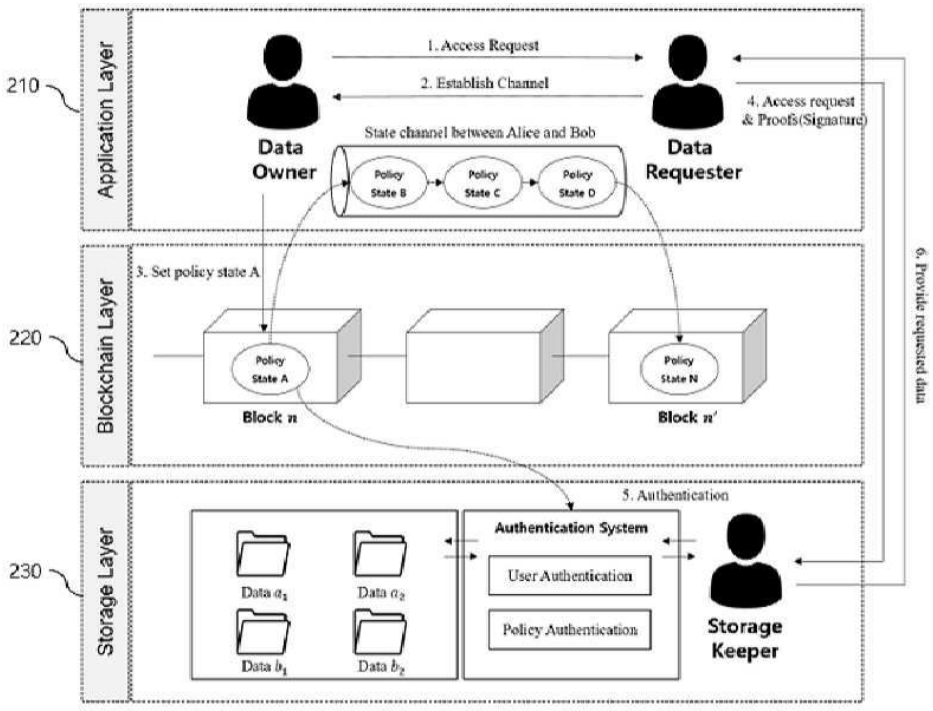
230 : 스토리지 계층

도면

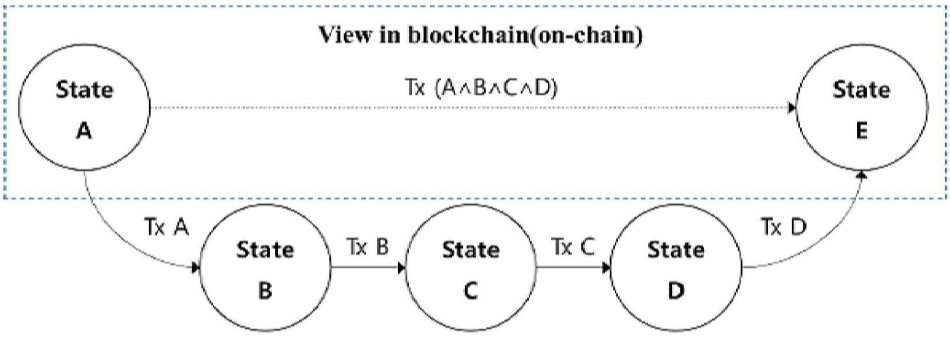
도면1



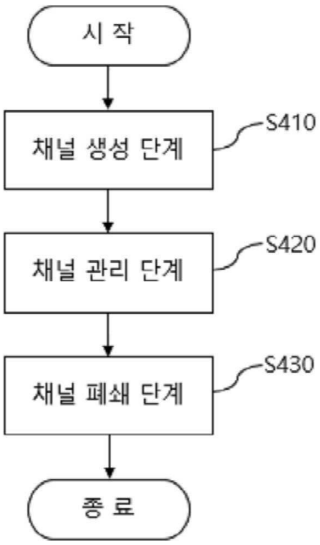
도면2



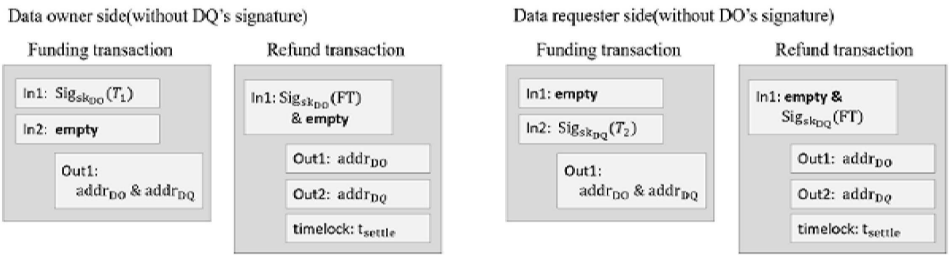
도면3



도면4

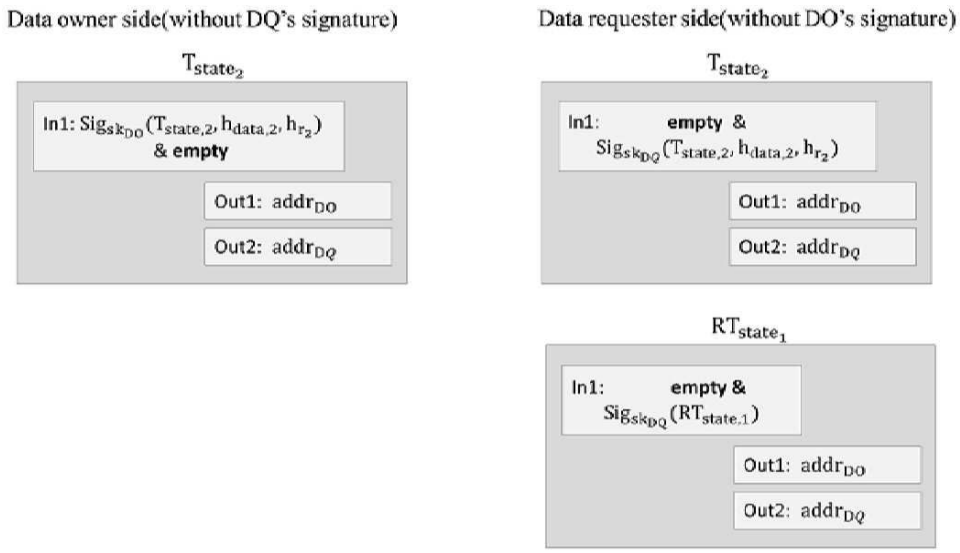


도면5

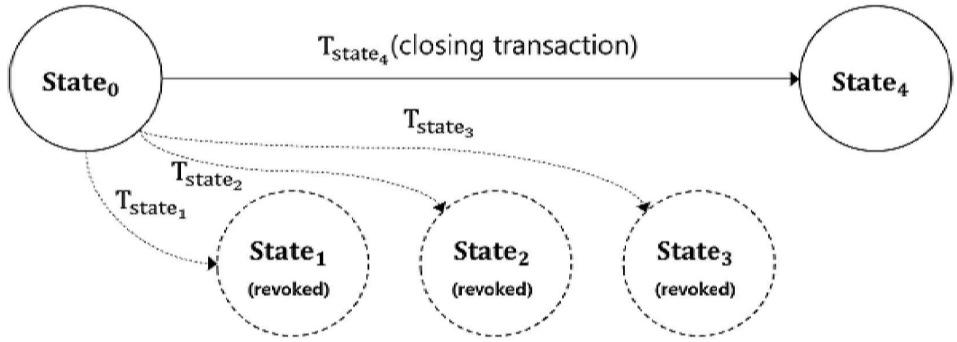


도면6

도면7


Data owner side(without DQ's signature)
T_{state_2}
In1: $Sig_{sk_{DO}}(T_{state,2}, h_{data,2}, h_{r_2})$ & empty
Out1: $addr_{DO}$
Out2: $addr_{DQ}$
Data requester side(without DO's signature)
T_{state_2}
In1: empty & $Sig_{sk_{DQ}}(T_{state,2}, h_{data,2}, h_{r_2})$
Out1: $addr_{DO}$
Out2: $addr_{DQ}$
RT_{state_1}
In1: empty & $Sig_{sk_{DQ}}(RT_{state,1})$
Out1: $addr_{DO}$
Out2: $addr_{DQ}$

도면8


$State_0$
T_{state_4}(closing transaction)
$State_4$
T_{state_3}
T_{state_2}
T_{state_1}
$State_1$ (revoked)
$State_2$ (revoked)
$State_3$ (revoked)