(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2021년03월16일
(11) 등록번호 10-2227685
(24) 등록일자 2021년03월09일

(51) 국제특허분류(Int. Cl.)
H04L 29/06 (2006.01) *H04L 29/08* (2006.01)
(52) CPC특허분류
H04L 63/20 (2013.01)
H04L 63/0823 (2013.01)
(21) 출원번호 10-2019-7028615
(22) 출원일자(국제) 2019년03월29일
심사청구일자 2019년10월28일
(85) 번역문제출일자 2019년09월27일
(65) 공개번호 10-2020-0116014
(43) 공개일자 2020년10월08일
(86) 국제출원번호 PCT/CN2019/080493
(87) 국제공개번호 WO 2019/120326
국제공개일자 2019년06월27일
(56) 선행기술조사문헌
CN109257336 A*
CN109347941 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
어드밴스드 뉴 테크놀로지스 씨오., 엘티디.
케이만 군도, 그랜드 케이만 케이와이1-9008, 조지 타운, 27 하스피탈 로드, 케이만 코포레이트 센터
(72) 발명자
펑 지위안
중국 저지앙 311121 항저우 유항 디스트릭트 웨스트 웬 이 로드 넘버 969 빌딩 3 알리바바 그룹 리갈 디파트먼트 5층
리 얀펑
중국 저지앙 311121 항저우 유항 디스트릭트 웨스트 웬 이 로드 넘버 969 빌딩 3 알리바바 그룹 리갈 디파트먼트 5층
청 롱
중국 저지앙 311121 항저우 유항 디스트릭트 웨스트 웬 이 로드 넘버 969 빌딩 3 알리바바 그룹 리갈 디파트먼트 5층
(74) 대리인
김태홍, 김진희

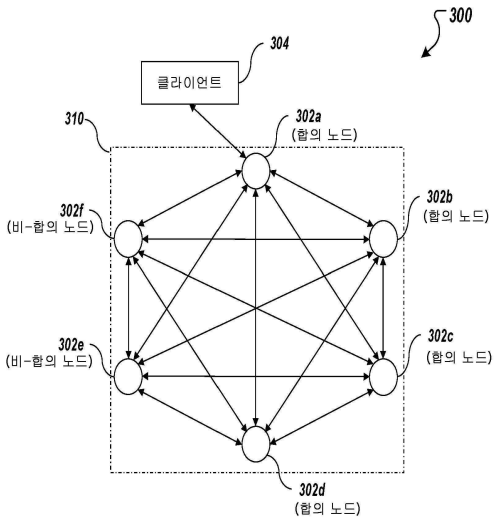
전체 청구항 수 : 총 11 항 심사관 : 홍기완

(54) 발명의 명칭 **블록 체인 네트워크에서 민감 데이터 요소를 관리하는 방법**

(57) 요 약

블록체인 네트워크에 저장된 민감 데이터 요소를 관리하기 위한 컴퓨터 저장 매체 상에 인코딩된 컴퓨터 프로그램을 포함하는 방법, 시스템 및 장치가 여기에 개시된다. 방법들 중 하나는 블록체인 네트워크에 저장된 감시 리스트에 대해 수정을 수행하라는 요청을 클라이언트 디바이스로부터 수신하는 단계를 포함한다. 감시 리스트는 하나 이상의 민감 데이터 요소를 포함한다. 블록체인 네트워크 노드는 요청의 디지털 서명에 기초하여 클라이언트 디바이스가 감시 리스트를 수정하도록 인가되었는지를 결정한다. 클라이언트 디바이스가 감시 리스트를 수정하도록 인가되었다는 결정에 응답하여, 블록체인 네트워크 내의 요청에 대해 합의 절차가 수행된다. 합의가 달성된 후에, 블록체인 네트워크 노드는 감시 리스트에 대한 수정에 기초하여 감시 리스트를 업데이트한다.

대 표 도 - 도3



(52) CPC특허분류
H04L 63/101 (2013.01)
H04L 67/1097 (2013.01)

명 세 서

청구범위

청구항 1

블록체인 네트워크 내에 저장된 민감(sensitive) 데이터 요소를 관리하기 위한 컴퓨터-구현(computer-implemented) 방법에 있어서,

블록체인 네트워크의 네트워크 노드에 의해, 클라이언트 디바이스로부터 상기 블록체인 네트워크 내에 저장된 감시 리스트(watch list)에 대해 수정을 수행하라는 요청을 수신하는 단계 - 상기 감시 리스트는 복수의 민감 데이터 요소를 포함하고, 상기 요청은 상기 클라이언트 디바이스의 개인 키(private key)를 사용하여 생성된 디지털 서명을 포함함 - ;

상기 네트워크 노드에 의해, 상기 디지털 서명에 기초하여 상기 클라이언트 디바이스가 상기 감시 리스트를 수정하도록 인가(authorize)되었는지 여부를 결정하는 단계;

상기 클라이언트 디바이스가 상기 감시 리스트를 수정하도록 인가되었다고 결정하는 것에 응답하여:

상기 네트워크 노드에 의해, 상기 블록체인 네트워크 내의 상기 요청에 대한 합의 절차를 수행하는 단계로서, 상기 합의 절차는,

상기 블록체인 네트워크의 복수의 합의 노드에 요청 검증 메시지를 송신하는 단계 - 각각의 합의 노드는 제 1 엔티티의 서버 상에 있고, 상기 제 1 엔티티 및 상기 복수의 합의 노드는 상기 감시 리스트를 수정하기 위한 인가를 가짐 - , 및

상기 복수의 합의 노드로부터 응답 메시지를 수신하는 단계

를 포함하는 것인, 상기 합의 절차를 수행하는 단계;

상기 응답 메시지에 기초하여, 합의가 달성되었다고 결정하는 단계; 및

상기 네트워크 노드에 의해, 상기 감시 리스트에 대해 수정을 수행하는 단계

를 포함하는, 컴퓨터-구현 방법.

청구항 2

제 1 항에 있어서,

상기 복수의 민감 데이터 요소에 하나 이상의 인가된(authorized) 엔티티에 의해 모니터링, 필터링 또는 둘 모두가 수행되는 것인, 컴퓨터-구현 방법.

청구항 3

제 1 항 또는 제 2 항에 있어서,

상기 감시 리스트에 대해 수정을 수행하라는 요청은, 상기 감시 리스트에 새로운 민감 데이터 요소를 추가하라는 요청, 상기 감시 리스트로부터 민감 데이터 요소를 제거하라는 요청, 및 상기 감시 리스트에서 민감 데이터 요소를 편집하라는 요청 중 하나 이상을 포함하는 것인, 컴퓨터-구현 방법.

청구항 4

제 1 항 또는 제 2 항에 있어서,

상기 복수의 민감 데이터 요소는 암호화되는 것인, 컴퓨터-구현 방법.

청구항 5

제 1 항 또는 제 2 항에 있어서,

상기 네트워크 노드에 의해, 상기 디지털 서명에 기초하여 상기 클라이언트 디바이스가 상기 감시 리스트를 수

정하도록 인가되었는지 여부를 결정하는 단계는, 상기 클라이언트 디바이스가 상기 감시 리스트를 수정하도록 인가되는 인가된 엔티티(authorized entity)의 공개 키(public key) 및 상기 디지털 서명에 기초하여 상기 클라이언트 디바이스가 상기 감시 리스트를 수정하도록 인가되었다고 결정하는 단계를 포함하는 것인, 컴퓨터-구현 방법.

청구항 6

제 5 항에 있어서,

상기 인가된 엔티티는 상기 네트워크 노드 내에 저장되는 화이트리스트(whitelist) 내에 표시되고, 상기 화이트리스트는 상기 감시 리스트를 수정하도록 인가되는 하나 이상의 인가된 엔티티를 포함하는 것인, 컴퓨터-구현 방법.

청구항 7

제 1 항 또는 제 2 항에 있어서,

상기 네트워크 노드에 의해, 상기 블록체인 네트워크 내에 저장되는 상기 감시 리스트 내의 민감 데이터 요소에 대한 조회(inquiry) 요청을 제 2 클라이언트 디바이스로부터 수신하는 단계 - 상기 조회 요청은 상기 제 2 클라이언트 디바이스의 개인 키를 사용하여 생성된 제 2 디지털 서명을 포함함 - ;

상기 네트워크 노드에 의해, 상기 제 2 디지털 서명에 기초하여 상기 제 2 클라이언트 디바이스가 상기 민감 데이터 요소를 획득하도록 인가되었는지 여부를 결정하는 단계; 및

상기 제 2 클라이언트 디바이스가 상기 민감 데이터 요소를 획득하도록 인가되었다고 결정하는 것에 응답하여, 상기 네트워크 노드에 의해, 상기 제 2 클라이언트 디바이스에 응답을 송신하는 단계 - 상기 응답은 암호화되는 상기 민감 데이터 요소를 포함함 -

를 더 포함하는, 컴퓨터-구현 방법.

청구항 8

블록체인 네트워크 내에 저장된 민감 데이터 요소를 관리하기 위한 장치에 있어서, 제 1 항 또는 제 2 항의 방법을 수행하기 위한 복수의 모듈을 포함하는, 민감 데이터 요소 관리 장치.

청구항 9

블록체인 네트워크 내에 저장된 민감 데이터 요소를 관리하기 위한 시스템에 있어서,

하나 이상의 프로세서; 및

상기 하나 이상의 프로세서에 커플링되고, 제 1 항 또는 제 2 항의 방법을 수행하기 위해 상기 하나 이상의 프로세서에 의해 실행 가능한 명령어들이 저장된 하나 이상의 컴퓨터 판독가능 메모리

를 포함하는, 민감 데이터 요소 관리 시스템.

청구항 10

제 1 항에 있어서,

상기 블록체인 네트워크는 비-합의 노드를 포함하고, 상기 비-합의 노드는 제 2 엔티티의 서버 상에 있고, 상기 비-합의 노드 및 상기 제 2 엔티티는 상기 감시 리스트를 수정하기 위한 인가 없이 상기 복수의 합의 노드로부터 상기 감시 리스트를 획득할 수 있는 것인, 컴퓨터-구현 방법.

청구항 11

제 10 항에 있어서,

상기 네트워크 노드에 의해, 상기 비-합의 노드에 상기 수정된 감시 리스트를 송신하는 단계

를 포함하는, 컴퓨터-구현 방법.

발명의 설명

기 술 분 야

[0001] 본 명세서는 블록체인 네트워크에 저장된 민감(sensitive) 데이터 요소를 관리하는 방법에 관한 것이다.

배 경 기 술

[0002] 합의 네트워크 및/또는 블록체인 네트워크로 지칭될 수 있는 분산 원장 시스템(distributed ledger system; DLS)은 참여 엔티티가 데이터를 안전하고 불변적으로 저장할 수 있게 한다. DLS는 일반적으로 임의의 특정 사용자 케이스를 참조하지 않고 블록체인 네트워크로서 지칭된다. 블록체인 네트워크 유형의 예로는 공개형 블록체인 네트워크, 비공개형 블록체인 네트워크 및 컨소시엄 블록체인 네트워크가 있다. 컨소시엄 블록체인 네트워크가 합의 프로세스를 제어하는 선택 그룹 엔티티에 제공되고, 액세스 제어 계층을 포함한다.

[0003] 블록체인 네트워크를 포함하여 컴퓨터 네트워크에서 송신되는 데이터는, 개인에게 추적될 수 있는, 그리고 공개되는 경우 그 사람에게 피해 또는 손실을 가져올 수 있는 개인 정보(예를 들어, 생체 데이터, 의료 정보, 및 사회 보장 번호)와 같은 민감 데이터를 포함할 수 있다. 민감 데이터에는 경쟁사 또는 일반 대중이 발견한 경우 비즈니스 엔티티에 위험을 초래하는 민감한 비즈니스 정보(예를 들어, 영업 비밀, 인수 계획 및 재무 데이터)를 포함할 수도 있다. 민감 데이터는 정부 기관과 관련되고 정보 보안을 보호하기 위해 민감도 레벨(예를 들어, 제한, 기밀, 비밀 및 일급 비밀)에 따라 제한되는 분류된 정보를 포함할 수 있다.

[0004] 컴퓨터 네트워크에서 민감 데이터의 데이터 보안 문제를 해결하기 위한 해결책을 제공하는 것이 바람직 할 것이다.

발명의 내용

[0005] 본 명세서는 블록체인 네트워크에 저장된 민감 데이터 요소를 관리하기 위한 기술을 설명한다. 이러한 기술에는 일반적으로 블록체인 네트워크에서 감시 리스트(watch list)(블록체인 기반 감시 리스트라고도 함)를 구현하는 것이 포함된다. 감시 리스트는 하나 이상의 인가된(authorized) 엔티티(예를 들어, 조직, 규제 기관, 에이전시 또는 정부)에 의해 모니터링 및/또는 필터링될 수 있는 하나 이상의 민감 데이터 요소를 포함한다. 민감 데이터 요소는 민감한, 개인의, 그리고/또는 기밀의 정보를 포함하거나 관련될 수 있다. 일부 실시예에서, 블록체인 기반 감시 리스트는 민감 데이터 요소를 분산 방식으로 블록체인 네트워크에 저장한다. 일부 실시예에서, 블록체인 기반 감시 리스트는 감시 리스트에 저장된 민감 데이터 요소의 관리를 용이하게 할 수 있다. 일부 실시예에서, 블록체인 기반 감시 리스트는 민감 데이터 요소의 변형 억제(tamper-resistant) 보호를 제공하고 감시 리스트에 대한 악의적인 행동 및 사이버 공격을 방지함으로써 향상된 데이터 보안을 제공할 수 있다.

[0006] 본 명세서는 또한, 하나 이상의 프로세서들에 커플링되고 명령어들이 저장된 하나 이상의 비일시적 컴퓨터 판독가능 저장 매체들을 제공하고, 명령어들은 하나 이상의 프로세서들에 의해 실행되는 경우, 하나 이상의 프로세서들로 하여금 본 명세서에 제공된 방법들의 실시예들에 따른 동작들을 수행하게 한다.

[0007] 본 명세서는 본 명세서에 제공된 방법들을 구현하기 위한 시스템을 추가로 제공한다. 시스템은, 하나 이상의 프로세서들, 및 하나 이상의 프로세서들에 커플링되고 명령어들이 저장된 하나 이상의 비일시적 컴퓨터 판독가능 저장 매체들을 포함하고, 명령어들은 하나 이상의 프로세서들에 의해 실행되는 경우, 하나 이상의 프로세서들로 하여금 본 명세서에 제공된 방법들의 실시예들에 따른 동작들을 수행하게 한다.

[0008] 본 명세서에 따른 방법들은 본 명세서에 설명된 양상들 및 특징들의 임의의 조합을 포함할 수 있음이 인식된다. 즉, 본 명세서에 따른 방법들은 본 명세서에 구체적으로 설명된 양상들 및 특징들의 조합들로 제한되는 것이 아니라, 제공된 양상들 및 특징들의 임의의 조합을 또한 포함한다.

[0009] 본 명세서의 하나 이상의 실시예들의 세부사항들은 첨부된 도면들 및 이하의 설명에서 기술된다. 본 명세서의 다른 특징들 및 이점들은 상세한 설명 및 도면들 및 청구항들로부터 명백해질 것이다.

도면의 간단한 설명

[0010] 도 1은 본 명세서의 실시예들을 실행하기 위해 사용될 수 있는 환경의 예를 예시하는 도면이다.

도 2는 본 명세서의 실시예들에 따른 아키텍처의 예를 예시하는 도면이다.

도 3은 본 명세서의 실시예들에 따른 시스템의 예를 예시하는 도면이다.

도 4는 본 명세서의 실시예들에 따라 실행될 수 있는 프로세스의 예를 도시한다.

도 5는 본 명세서의 실시예들에 따라 실행될 수 있는 프로세스의 예를 도시한다.

도 6은 본 명세서의 실시예들에 따른 장치의 모듈들의 예들을 도시한다.

다양한 도면들에서 유사한 참조 부호들 및 지정들은 유사한 요소들을 표시한다.

발명을 실시하기 위한 구체적인 내용

[0011] 본 명세서는 블록체인 네트워크에 저장된 민감 데이터 요소를 관리하기 위한 기술을 설명한다. 이러한 기술에는 일반적으로 블록체인 네트워크에서 감시 리스트(블록체인 기반 감시 리스트라고도 함)를 구현하는 것이 포함된다. 감시 리스트는 하나 이상의 인가된 엔티티(예를 들어, 조직, 규제 기관, 에이전시 또는 정부)에 의해 모니터링 및/또는 필터링될 수 있는 하나 이상의 민감 데이터 요소를 포함한다. 민감 데이터 요소는 민감한, 개인의, 그리고/또는 기밀의 정보를 포함하거나 관련될 수 있다. 일부 실시예에서, 블록체인 기반 감시 리스트는 민감 데이터 요소를 분산 방식으로 블록체인 네트워크에 저장한다. 일부 실시예에서, 블록체인 기반 감시 리스트는 감시 리스트에 저장된 민감 데이터 요소의 관리를 용이하게 할 수 있다. 일부 실시예에서, 블록체인 기반 감시 리스트는 민감 데이터 요소의 변형 억제 보호를 제공하고 감시 리스트에 대한 악의적인 행위 및 사이버 공격을 방지함으로써 향상된 데이터 보안을 제공할 수 있다.

[0012] 본 명세서에 기술된 기술은 하나 이상의 기술적 효과를 생성한다. 일부 실시예에서, 감시 리스트는 블록체인 네트워크에서 구현될 수 있다. 감시 리스트는 하나 이상의 인가된 엔티티에 의해 모니터링 및/또는 필터링되는 하나 이상의 민감 데이터 요소를 포함할 수 있다. 감시 리스트의 민감 데이터 요소는 분산 방식으로 블록체인 네트워크에 저장된다. 분산 블록체인 네트워크의 변형 억제 특성으로 인해, 감시 리스트에 대한 악의적인 행위 및 사이버 공격이 완화될 수 있다. 일부 실시예에서, 블록체인 기반 감시 리스트는 감시 리스트에 저장된 민감 데이터 요소의 관리를 용이하게 할 수 있다. 예를 들어, 클라이언트 디바이스가 블록체인 네트워크에 저장된 감시 리스트에 대해 수정을 수행하기 위한 요청을 제출하면, 요청을 수신한 블록체인 네트워크의 네트워크 노드는 요청에서의 클라이언트 디바이스의 디지털 서명에 기초하여 클라이언트 디바이스를 인증할 수 있다. 일부 실시예들에서, 인증된 클라이언트 디바이스는 수정을 수행하도록 허용될 수 있지만, 인증에 실패한 클라이언트 디바이스는 수정을 수행하는 것이 거부될 것이다. 이는 악의적인 행위자에 의해 블록체인 네트워크에 저장된 민감 데이터가 위태롭게 되는 것을 방지하고, 그에 따라 감시 리스트의 데이터 보안을 향상시킬 수 있다. 일부 실시예에서, 감시 리스트의 민감 데이터 요소는 예를 들어 암호화 알고리즘을 사용하여 암호화된다. 일부 실시예에서, 인가된 자만이 암호화된 데이터 요소를 복호화하고 민감 데이터 요소를 획득할 수 있다. 이것은 악의적인 행위자가 블록체인 네트워크에 침투하여 민감 데이터 요소를 획득하는 것을 방지하고, 그에 따라 감시 리스트의 데이터 보안을 향상시킬 수 있다.

[0013] 본 명세서의 실시예들에 대한 추가적인 콘텍스트를 제공하기 위해, 그리고 앞서 소개된 바와 같이, 합의 네트워크들(예를 들어, 피어-투-피어 노드들로 구성됨)로 또한 지칭될 수 있는 분산 원장 시스템들(DLS들) 및 블록체인 네트워크들은 참여 엔티티들이 트랜잭션을 안전하고 불변으로 수행하고 데이터를 저장할 수 있게 한다. 블록체인이라는 용어는 일반적으로 특정 네트워크들 및/또는 사용 케이스와 연관되고, 본 명세서에서는 일반적으로 임의의 특정 사용 케이스를 참조하지 않고 DLS를 지칭하기 위해 블록체인이 사용된다.

[0014] 블록체인은, 트랜잭션들이 불변인 방식으로 트랜잭션들을 저장하는 데이터 구조이다. 따라서, 블록체인 상에 레코딩된 트랜잭션들은 신뢰가능하고 믿을 수 있다. 블록체인은 하나 이상의 블록들을 포함한다. 체인 내의 각각의 블록은 이전 블록의 암호화 해시(hash)를 포함하여 체인 내에 존재하기 직전의 이전 블록에 링크된다. 각각의 블록은 또한 타임스탬프, 자기 자신의 암호화 해시, 및 하나 이상의 트랜잭션을 포함한다. 블록체인 네트워크의 노드들에 의해 이미 검증된 트랜잭션들은 해시되고 머클 트리(Merkle tree)로 인코딩된다. 머클 트리는, 트리의 리프(leaf) 노드들의 데이터가 해시되고, 트리의 각각의 브랜치(branch)의 모든 해시들이 브랜치의 루트에서 연쇄되는 데이터 구조이다. 이러한 프로세스는 전체 트리의 루트까지 트리를 계속하여 트리의 모든 데이터를 나타내는 해시를 저장한다. 트리에 저장된 트랜잭션인 것으로 알려진 해시는, 이것이 트리의 구조와 일치하는지 여부를 결정함으로써 신속하게 검증될 수 있다.

[0015] 블록체인은 트랜잭션들을 저장하기 위한 분산 또는 적어도 부분적으로 분산의 데이터 구조이지만, 블록체인 네트워크는 트랜잭션들에 브로드캐스트, 검증 및 확인 등을 행함으로써 하나 이상의 블록체인들을 관리, 업데이트

및 유지하는 노드들을 컴퓨팅하는 네트워크이다. 앞서 소개된 바와 같이, 블록체인 네트워크는 공개형 블록체인 네트워크, 비공개형 블록체인 네트워크 또는 컨소시엄 블록체인 네트워크로서 제공될 수 있다. 본 명세서의 실시예들은 컨소시엄 블록체인 네트워크를 참조하여 본 명세서에서 더 상세히 설명된다. 그러나, 본 명세서의 실시예들은 임의의 적절한 유형의 블록체인 네트워크에서 실현될 수 있는 것으로 고려된다.

[0016] 일반적으로, 컨소시엄 블록체인 네트워크는 참여 엔티티들 사이에서 비공개형이다. 컨소시엄 블록체인 네트워크에서, 합의 프로세스는 합의 노드로서 지칭될 수 있는, 인가된(authorized) 노드 세트에 의해 제어되고, 하나 이상의 노드들은 각각의 엔티티(예를 들어, 금융 기관, 보험 회사)에 의해 동작된다. 예를 들어, 열(10)개의 엔티티들(예를 들어, 금융 기관들, 보험 회사들)의 컨소시엄이 컨소시엄 블록체인 네트워크를 동작시킬 수 있고, 이들 각각은 컨소시엄 블록체인 네트워크의 적어도 하나의 노드를 동작시킨다.

[0017] 일부 예들에서, 컨소시엄 블록체인 네트워크 내에서는, 모든 노드들에 걸쳐 복제된 블록체인으로서 글로벌 블록체인이 제공된다. 즉, 모든 합의 노드들은 글로벌 블록체인에 대해 완전한 합의 상태에 있다. 합의(예를 들어, 블록체인에 블록을 추가하는 것에 대한 동의)를 달성하기 위해, 합의 프로토콜이 컨소시엄 블록체인 네트워크 내에서 구현된다. 예를 들어, 컨소시엄 블록체인 네트워크는 아래에서 더 상세히 설명되는 PBFT(practical Byzantine fault tolerance) 합의를 구현할 수 있다.

[0018] 도 1은 본 명세서의 실시예들을 실행하기 위해 사용될 수 있는 환경(100)의 예를 예시하는 도면이다. 일부 예들에서, 환경(100)은 엔티티들이 컨소시엄 블록체인 네트워크(102)에 참여할 수 있게 한다. 환경(100)은 컴퓨팅 디바이스들(106, 108) 및 네트워크(110)를 포함한다. 일부 예들에서, 네트워크(110)는 로컬 영역 네트워크(local area network; LAN), 광역 네트워크(wide area network; WAN), 인터넷 또는 이들의 조합을 포함하고, 웹 사이트들, 사용자 디바이스들(예를 들어, 컴퓨팅 디바이스들) 및 백엔드 시스템들을 접속한다. 일부 예들에서, 네트워크(110)는 유선 및/또는 무선 통신 링크를 통해 액세스될 수 있다. 일부 예들에서, 네트워크(110)는 컨소시엄 블록체인 네트워크(102)와의 및 컨소시엄 블록체인 네트워크(102) 내의 통신을 가능하게 한다. 일반적으로 네트워크(110)는 하나 이상의 통신 네트워크들을 나타낸다. 일부 경우들에서, 컴퓨팅 디바이스들(106, 108)은 클라우드 컴퓨팅 시스템(도시되지 않음)의 노드들일 수 있거나, 또는 각각의 컴퓨팅 디바이스(106, 108)는 네트워크에 의해 상호접속된 다수의 컴퓨터들을 포함하고 분산 프로세싱 시스템으로 기능하는 별개의 클라우드 컴퓨팅 시스템일 수 있다.

[0019] 도시된 예에서, 컴퓨팅 시스템들(106, 108) 각각은 컨소시엄 블록체인 네트워크(102)의 노드로서 참여를 가능하게 하는 임의의 적절한 컴퓨팅 시스템을 포함할 수 있다. 컴퓨팅 디바이스들의 예들은 제한 없이 서버, 데스크탑 컴퓨터, 랩탑 컴퓨터, 태블릿 컴퓨팅 디바이스 및 스마트폰을 포함한다. 일부 예들에서, 컴퓨팅 시스템들(106, 108)은 컨소시엄 블록체인 네트워크(102)와 상호작용하기 위한 하나 이상의 컴퓨터-구현 서비스들을 호스팅한다. 예를 들어, 컴퓨팅 시스템(106)은, 제 1 엔티티(예를 들어, 사용자 A)가 하나 이상의 다른 엔티티들(예를 들어, 다른 사용자들)과 자신의 트랜잭션들을 관리하기 위해 사용하는 트랜잭션 관리 시스템과 같은, 제 1 엔티티의 컴퓨터-구현 서비스들을 호스팅할 수 있다. 컴퓨팅 시스템(108)은, 제 2 엔티티(예를 들어, 사용자 B)가 하나 이상의 다른 엔티티들(예를 들어, 다른 사용자들)과 자신의 트랜잭션들을 관리하기 위해 사용하는 트랜잭션 관리 시스템과 같은, 제 2 엔티티의 컴퓨터-구현 서비스들을 호스팅할 수 있다. 도 1의 예에서, 컨소시엄 블록체인 네트워크(102)는 노드들의 피어-투-피어 네트워크로서 나타내고, 컴퓨팅 시스템들(106, 108)은 각각, 컨소시엄 블록체인 네트워크(102)에 참여한 제 1 엔티티 및 제 2 엔티티의 노드들을 제공한다.

[0020] 도 2는 본 명세서의 실시예들에 따른 아키텍처(200)의 예를 도시한다. 예시적인 개념적 아키텍처(200)는 참여자 A, 참여자 B, 및 참여자 C에 각각 대응하는 참여자 시스템들(202, 204, 206)을 포함한다. 각각의 참여자(예를 들어, 사용자, 기업)는 다수의 노드들(214)을 포함하는 피어-투-피어 네트워크로서 제공된 블록체인 네트워크(212)에 참여하고, 노드들 중 적어도 일부는 정보를 블록체인(216)에 불변으로 레코딩한다. 단일 블록체인(216)이 블록체인 네트워크(212) 내에 개략적으로 도시되지만, 블록체인(216)의 다수의 카피들이 제공되고, 본 명세서에 더 상세히 설명되는 바와 같이 블록체인 네트워크(212)에 걸쳐 유지된다.

[0021] 도시된 예에서, 각각의 참여자 시스템(202, 204, 206)는 각각 참여자 A, 참여자 B 및 참여자 C에 의해 또는 그 대신에 제공되고, 블록체인 네트워크 내에서 각각의 노드(214)로서 기능한다. 본 명세서에서 사용되는 바와 같이, 노드는 일반적으로 블록체인 네트워크(212)에 접속된 개별적인 시스템(예를 들어, 컴퓨터, 서버)을 지칭하며, 각각의 참여자가 블록체인 네트워크에 참여할 수 있게 한다. 도 2의 예에서, 참여자는 각각의 노드(214)에 대응한다. 그러나, 참여자는 블록체인 네트워크(212) 내의 다수의 노드들(214)을 동작시킬 수 있고 그리고/또는 다수의 참여자들이 노드(214)를 공유할 수 있음이 고려된다. 일부 예들에서, 참여자 시스템들(202, 204,

206)은 프로토콜(예를 들어, 하이퍼텍스트 전송 프로토콜 보안(hypertext transfer protocol secure; HTTPS))을 사용하여 그리고/또는 원격 절차 호출(remote procedure call; RPC)들을 사용하여 블록체인 네트워크(212)과 또는 블록체인 네트워크(212)를 통해 통신한다.

[0022] 노드들(214)은 블록체인 네트워크(212) 내에서 다양한 참여도를 가질 수 있다. 예를 들어, 일부 노드들(214)은 합의 프로세스에 참여할 수 있는 한편(예를 들어, 블록체인(216)에 블록들을 추가하는 마인더(minder) 노드들), 다른 노드들(214)은 합의 프로세스에 참여하지 않는다. 다른 예로서, 일부 노드들(214)은 블록체인(216)의 완전한 카피를 저장하는 한편, 다른 노드들(214)은 블록체인(216)의 부분들의 카피들만을 저장한다. 예를 들어, 데이터 액세스 특권들은, 각각의 참여자가 자신의 각각의 시스템 내에 저장하는 블록체인 데이터를 제한할 수 있다. 도 2의 예에서, 참여자 시스템들(202, 204)은 블록체인(216)의 각각의 완전한 카피들(216', 216")을 저장한다.

[0023] 블록체인(예를 들어, 도 2의 블록체인(216))은 블록들의 체인으로 이루어지고, 각각의 블록은 데이터를 저장한다. 데이터의 예들은 둘 이상의 참여자들 사이의 트랜잭션을 나타내는 트랜잭션 데이터를 포함한다. 트랜잭션들은 비제한적인 예시의 방식으로 본 명세서에서 사용되지만, 임의의 적절한 데이터가 블록체인에 저장될 수 있음이 고려된다(예를 들어, 문서들, 이미지들, 비디오들, 오디오). 트랜잭션의 예들은 제한 없이 어떠한 값(예를 들어, 자산들, 제품들, 서비스들, 화폐)의 교환들을 포함할 수 있다. 트랜잭션 데이터는 블록체인 내에 불변으로 저장된다. 즉, 트랜잭션 데이터는 변경될 수 없다.

[0024] 블록에 저장하기 전에, 트랜잭션 데이터는 해시된다. 해시는 트랜잭션 데이터(스트링 데이터로서 제공됨)를 고정 길이 해시 값(또한 스트링 데이터로서 제공됨)으로 변환하는 프로세스이다. 트랜잭션 데이터를 획득하기 위해, 해시 값을 언-해시하는 것은 가능하지 않다. 해시하는 것은, 트랜잭션 데이터에서 심지어 약간의 변화로도 완전히 상이한 해시 값을 도출하는 것을 보장한다. 추가로, 그리고 앞서 언급된 바와 같이, 해시 값은 고정 길이이다. 즉, 트랜잭션 데이터의 크기와 무관하게, 해시 값의 길이가 고정된다. 해시하는 것은 해시 값을 생성하기 위해 해시 함수를 통해 트랜잭션 데이터를 프로세싱하는 것을 포함한다. 해시 함수의 예는 제한 없이, 보안 해시 알고리즘(SHA)-256을 포함하고, 이는 256-비트 해시 값들을 출력한다.

[0025] 다수의 트랜잭션들의 트랜잭션 데이터는 해시되고 블록에 저장된다. 예를 들어, 2개의 트랜잭션들의 해시 값들이 제공되고, 다른 해시를 제공하기 위해 스스로 해시된다. 이러한 프로세스는, 블록에 저장될 모든 트랜잭션들에 대해, 단일 해시 값이 제공될 때까지 반복된다. 이러한 해시 값은 머클 루트 해시로 지칭되고, 블록의 헤더에 저장된다. 트랜잭션들 중 임의의 것에서의 변화는 그 해시 값에서의 변화, 및 궁극적으로 머클 루트 해시에서의 변화를 도출할 것이다.

[0026] 블록들은 합의 프로토콜을 통해 블록체인에 추가된다. 블록체인 네트워크 내의 다수의 노드들은 합의 프로토콜에 참여하고, 블록을 블록체인에 추가되는 블록을 갖기 위한 작업을 수행한다. 이러한 노드들은 합의 노드들로 지칭된다. 앞서 소개된 PBFT는 합의 프로토콜의 비제한적인 예로서 사용된다. 합의 노드들은 합의 프로토콜을 실행하여, 블록체인에 트랜잭션들을 추가하고, 블록체인 네트워크의 전체 상태를 업데이트한다.

[0027] 더 상세하게는, 합의 노드는 블록 헤더를 생성하고, 블록 내의 트랜잭션들 전부를 해시하고, 블록 내의 모든 트랜잭션들에 대해 단일 해시 값이 제공될 때까지 추가적인 해시 값들을 생성하기 위해 해시 값을 쌍으로 조합한다(머클 루트 해시). 이러한 해시는 블록 헤더에 추가된다. 합의 노드는 또한 블록체인에서 가장 최근의 블록(즉, 블록체인에 추가된 마지막 블록)의 해시 값을 결정한다. 합의 노드는 또한 넌스(nonce) 값 및 타임스탬프를 블록 헤더에 추가한다.

[0028] 일반적으로, PBFT는 비잔틴(Byzantine) 오류들(예를 들어, 오작동 노드들, 악성 노드들)을 견디는 실용적인 비잔틴 상태 머신 복제를 제공한다. 이는, 오류들이 발생할 것으로 가정(예를 들어, 독립적 노드 실패들 및/또는 합의 노드들에 의해 전송된 조작된 메시지들의 존재를 가정)함으로써 PBFT에서 달성된다. PBFT에서, 합의 노드들은, 프라이머리 합의 노드 및 백업 합의 노드들을 포함하는 시퀀스에서 제공된다. 프라이머리 합의 노드는 주기적으로 변경되고, 트랜잭션들은, 블록체인 네트워크의 월드 상태에 관한 동의에 도달한 블록체인 네트워크 내의 모든 합의 노드들에 의해 블록체인에 추가된다. 이러한 프로세스에서, 메시지들은 합의 노드들 사이에서 송신되고, 각각의 합의 노드들은, 메시지가 특정 피어 노드로부터 수신된 것을 입증하고, 메시지가 송신 동안 수정되지 않은 것을 검증한다.

[0029] PBFT에서, 합의 프로토콜은 동일한 상태에서 시작하는 모든 합의 노드들에 의해 다수의 상태들에서 제공된다. 시작하기 위해, 클라이언트는 서비스 동작을 호출(예를 들어, 블록체인 네트워크 내에서 트랜잭션을 실행)하기

위해 프라이머리 합의 노드에 요청을 전송한다. 요청을 수신하는 것에 응답하여, 프라이머리 합의 노드는 요청을 백업 합의 노드들에 멀티캐스트한다. 백업 합의 노드들은 요청을 실행하고, 각각 답신을 클라이언트에 전송한다. 클라이언트는 임계 수의 답신들이 수신될 때까지 대기한다. 일부 예들에서, 클라이언트는 f+1개의 답신들이 수신되기를 대기하고, 여기서 f는 블록체인 네트워크 내에서 견디어 질 수 있는 오류 합의 노드들의 최대 수이다. 최종 결과는, 충분한 수의 합의 노드들이 블록체인에 추가될 레코드의 주문에 동의하고, 레코드가 수락되거나 거부되는 것이다.

[0030] 일부 블록체인 네트워크들에서, 트랜잭션들의 프라이버시를 유지하기 위해 암호화가 구현된다. 예를 들어, 블록체인 네트워크의 다른 노드들이 트랜잭션의 세부사항들을 인식할 수 없도록 2개의 노드들이 트랜잭션을 비밀로 유지하기를 원하면, 그 노드들은 트랜잭션 데이터를 암호화할 수 있다. 암호화의 예는 제한 없이 대칭적 암호화 및 비대칭적 암호화를 포함한다. 대칭적 암호화는 암호화(평문으로부터 암호문을 생성함) 및 복호화(암호문으로부터 평문을 생성함) 둘 모두에 대해 단일 키를 사용하는 암호화 프로세스를 지칭한다. 대칭적 암호화에서는, 다수의 노드들에 동일한 키가 이용가능하여, 각각의 노드는 트랜잭션 데이터를 암호화/복호화할 수 있다.

[0031] 비대칭적 암호화는, 개인 키(private key) 및 공개 키(public key)를 각각 포함하는 키 쌍들을 사용하고, 개인 키는 오직 각각의 노드에만 알려지고, 공개 키는 블록체인 네트워크의 임의의 또는 모든 다른 노드들에 알려진다. 노드는 데이터를 암호화하기 위해 다른 노드의 공개 키를 사용할 수 있고, 암호화된 데이터는 다른 노드의 개인 키를 사용하여 복호화될 수 있다. 예를 들어, 도 2를 다시 참조하면, 참여자 A는 참여자 B의 공개 키를 사용하여 데이터를 암호화하고 암호화된 데이터를 참여자 B에게 전송할 수 있다. 참여자 B는 자신의 개인 키를 사용하여 암호화된 데이터(암호문)를 복호화하고 원래의 데이터(평문)을 추출할 수 있다. 노드의 공개 키로 암호화된 메시지들은 오직 노드의 개인 키를 사용하여 복호화될 수 있다.

[0032] 비대칭적 암호화는 디지털 서명들을 제공하기 위해 사용되며, 이는 트랜잭션 내의 참여자들이 트랜잭션 내의 다른 참여자들 뿐만 아니라 트랜잭션의 유효성을 확인할 수 있게 한다. 예를 들어, 노드는 메시지를 디지털 방식으로 서명할 수 있고, 다른 노드는 메시지가 참여자 A의 디지털 서명에 기초하여 노드에 의해 전송된 것을 확인할 수 있다. 디지털 서명들은 또한 메시지들이 전달 동안 위조되지 않은 것을 보장하기 위해 사용될 수 있다. 예를 들어, 도 2를 다시 참조하면, 참여자 A는 참여자 B에게 메시지를 전송할 것이다. 참여자 A는 메시지의 해시를 생성하고, 그 다음, 자신의 개인 키를 사용하여, 해시를 암호화하여 암호화된 해시로서 디지털 서명을 제공한다. 참여자 A는 디지털 서명을 메시지에 첨부하고, 디지털 서명을 갖는 메시지를 참여자 B에게 전송한다. 참여자 B는 참여자 A의 공개 키를 사용하여 디지털 서명을 복호화하고 해시를 추출한다. 참여자 B는 메시지를 해시하고 해시들을 비교한다. 해시들이 동일하면, 참여자 B는 메시지가 실제로 참여자 A로부터의 것이었고 위조되지 않았음을 확인할 수 있다.

[0033] 도 3은 블록체인 네트워크에 저장된 민감 데이터 요소를 관리하는 시스템(300)의 예를 나타내는 도면이다. 도시된 바와 같이, 시스템(300)은 다수의 블록체인 네트워크 노드(302a-f)를 포함하는 블록체인 네트워크(310) 및 하나 이상의 클라이언트 디바이스(304)를 포함한다. 블록체인 네트워크(310)는 단지 예시를 위해 6개의 블록체인 네트워크 노드(302)를 포함하는 것으로 도시되어 있음에 유의한다. 블록체인 네트워크(310)는 임의의 적절한 수의 블록체인 네트워크 노드(302)를 포함할 수 있다. 클라이언트 디바이스(304)는 본 명세서에 설명된 방법을 수행하도록 프로그래밍된 임의의 적절한 컴퓨터, 모듈, 서버 또는 컴퓨팅 요소일 수 있다.

[0034] 일부 실시예에서, 블록체인 네트워크(310)는 인가된 엔티티(예를 들어, 조직, 규제 기관, 에이전시, 또는 정부)에 의해 모니터링 및/또는 필터링되는 민감 데이터 요소를 포함하는 감시 리스트를 저장하도록 구성된다. 일부 실시예에서, 민감 데이터 요소는 프라이버시 보호, 데이터 보안 및/또는 검열 또는 감시 목적을 위해 모니터링 또는 필터링될 수 있다. 일부 예들에서, 민감 데이터는 개인에게 추적될 수 있는, 그리고 공개되는 경우 개인에게 피해 또는 손실을 가져올 수 있는 개인 식별가능 정보(예를 들어, 생체 데이터, 의료 정보, 및 사회보장 번호)와 같은 개인 정보를 포함할 수 있다. 일부 실시예들에서, 민감 데이터는 경쟁자 또는 일반 대중에 의해 발견되는 경우 비지니스 엔티티에 위험을 초래하는 민감한 비즈니스 정보(예를 들어, 영업 비밀, 인수 계획 및 재무 데이터)를 포함할 수 있다. 일부 실시예들에서, 민감 데이터는 정부 기관과 관련되고 정보 보안을 보호하기 위해 민감도 레벨(예를 들어, 제한, 기밀, 비밀 및 일급 비밀)에 따라 제한되는 분류된 정보를 포함할 수 있다. 일부 실시예들에서, 민감 데이터는 무엇보다도 텍스트, 오디오, 비디오 또는 이미지의 포맷을 가질 수 있다. 일부 실시예들에서, 민감 데이터는 잠재적인 보안 위협을 초래하는 악성 프로그램을 포함할 수 있다.

[0035] 일부 실시예들에서, 블록체인 네트워크(310)의 네트워크 노드(302)(예를 들어, 노드(302a))는 클라이언트 디바이스(304)로부터 요청을 수신한다. 요청은 감시 리스트에 대한 수정을 위한 요청(예를 들어, 리스트에 데이터

요소를 추가하기 위한 요청, 리스트로부터 데이터 요소를 삭제하기 위한 요청, 또는 리스트에서 데이터 요소를 편집하기 위한 요청)을 포함할 수 있다. 네트워크 노드(302a)는 블록체인 네트워크 노드(302)의 서브세트(예를 들어, 합의 노드(302a-d))가 제안된 수정에 대해 합의를 도달할 수 있는 경우 감시 리스트에 대해 요청된 수정이 수행될 수 있도록 블록체인 네트워크(310) 내에서 합의 절차를 개시할 수 있다.

[0036] 일부 실시예에서, 블록체인 네트워크(310)는 합의 절차에 참여하지 않는 블록체인 네트워크 노드(302)(예를 들어, 비-합의 노드(302e-f))의 서브세트를 포함한다. 일부 실시예에서, 블록체인 네트워크(310)의 합의 노드(302a-d)는 감시 리스트에 대해 수정을 수행하라는 클라이언트 디바이스(304)로부터의 요청을 처리하도록 허용될 수 있는 반면, 블록체인 네트워크(310)의 비-합의 노드(302e-f)는 감시 리스트에 대해 수정을 수행하라는 클라이언트 디바이스(304)로부터의 요청을 처리하도록 허용되지 않는다. 예를 들어, 합의 노드(302)는 감시 리스트에 대한 액세스를 제어하고 감시 리스트를 주기적으로 업데이트하는 인가된 엔티티(예를 들어, 정부)의 서버에 구현될 수 있지만, 비-합의 노드(302)는 감시 리스트 수정에 대한 허가 또는 인가없이 합의 노드(302)로부터 감시 리스트를 획득할 수 있는 인가된 엔티티(예를 들어, 출판 플랫폼)의 자회사의 서버에 구현될 수 있다.

[0037] 도 4는 본 명세서의 실시예들에 따른 신호 흐름(400)의 예를 도시한다. 신호 흐름(400)은 블록체인 네트워크에 저장된 민감 데이터 요소를 관리하기 위한 프로세스를 나타낸다. 편의상, 프로세스는 하나 이상의 컴퓨터 시스템에 의해 수행되고, 하나 이상의 위치에 위치되고, 본 명세서에 따라 적절히 프로그래밍되는 것으로 설명될 것이다. 예를 들어, 적절하게 프로그램된 분산 시스템(예를 들어, 도 3의 시스템(300))은 프로세스를 수행할 수 있다.

[0038] 프로세스(400)는 클라이언트 디바이스(예를 들어, 클라이언트(304a))가 블록체인 네트워크에 저장된 감시 리스트에 대해 수정을 수행하라는 요청을 블록체인 네트워크(310)으로 전송하는 단계(402)에서 시작한다. 예를 들어, 클라이언트(304a)는 블록체인 네트워크(310)의 합의 노드(302a)에 요청을 전송한다. 감시 리스트는 하나 이상의 인가된 엔티티에 의해 모니터링, 필터링 또는 둘 모두가 수행되는 다수의 민감 데이터 요소(예를 들어, 키워드)를 포함한다. 일부 실시예에서, 감시 리스트에 대한 수정은 리스트에 데이터 요소를 추가하는 것, 리스트로부터 데이터 요소를 삭제하는 것, 또는 리스트에서 데이터 요소를 편집하는 것 중 하나 이상을 포함한다. 일부 실시예들에서, 감시 리스트 내의 민감 데이터 요소들의 일부 또는 전부는 이들이 일반 대중에게 보여 지거나 알려지지 않도록 암호화될 수 있다.

[0039] 일부 실시예들에서, 요청은 클라이언트 디바이스(304a)의 신원 정보(예를 들어, 식별자) 및 클라이언트 디바이스(304a)의 개인 키를 사용하여 생성된 디지털 서명을 포함한다. 디지털 서명은 클라이언트 디바이스(304a)의 신원을 검증 또는 인증하는데 사용될 수 있다.

[0040] 404에서, 블록체인 네트워크 노드(302a)는 클라이언트 디바이스(304a)가 블록체인 네트워크(310)에 저장된 감시 리스트를 수정하도록 인가되었는지를 결정한다. 일부 실시예에서, 블록체인 네트워크 노드(302a)는 감시 리스트를 수정하도록 인가된 클라이언트 디바이스의 식별자를 포함하는 화이트리스트(whitelist)를 저장한다.

[0041] 일부 실시예들에서, 블록체인 네트워크 노드(302a)는 요청에서의 클라이언트 디바이스(304a)의 식별자가 화이트리스트에서의 클라이언트 디바이스의 식별자와 매칭하는지를 결정할 수 있다. 추가적으로 또는 대안적으로, 블록체인 네트워크 노드(302a)는 화이트리스트에서의 클라이언트 디바이스의 공개 키(예를 들어, 식별자가 요청에서의 클라이언트(304a)의 식별자와 매칭하는 화이트리스트에서의 클라이언트의 공개 키)를 사용하여 요청에서의 디지털 서명이 복호화될 수 있는지를 결정할 수 있다. 일부 실시예에서, 화이트리스트에서의 클라이언트 디바이스의 공개 키는 블록체인 네트워크에 저장된다. 블록체인 네트워크 노드(302a)는 화이트리스트에서의 클라이언트 디바이스의 공개 키를 블록체인 네트워크로부터 리트리브(retrieve)하거나 다른 리소스로부터 획득할 수 있다.

[0042] 화이트리스트에서의 클라이언트 디바이스의 공개 키를 사용하여 생성된 서명을 사용하여 요청에서의 디지털 서명이 복호화되면, 블록체인 네트워크 노드(302a)는 요청에서 클라이언트 디바이스(304a)에 의해 생성된 해시를 추출할 수 있다. 블록체인 네트워크 노드(302a)는 수신된 요청을 해시하고 생성된 해시를 디지털 서명으로부터 추출된 해시와 비교할 수 있다. 해시가 매칭하는 경우, 블록체인 네트워크 노드(302a)는 클라이언트 디바이스(304a)가 감시 리스트를 수정하도록 인가되었다고 결정하고 프로세스는 다음 단계로 진행한다. 해시가 매칭하지 않거나 또는 화이트리스트에서의 임의의 클라이언트 디바이스의 공개 키를 사용하여 요청에서의 디지털 서명이 복호화될 수 없는 경우, 블록체인 네트워크 노드(302a)는 클라이언트 디바이스(304a)가 감시 리스트를 수정하도록 인가되지 않았다고 결정하고, 프로세스를 종료할 수 있다. 예를 들어, 블록체인 네트워크 노드(302a)는 클라이언트 디바이스(304a)가 감시 리스트를 수정하도록 인가되지 않았고 요청이 거부되었음을 나타내는 에러

메시지를 클라이언트 디바이스(304a)로 전송할 수 있다.

[0043] 406에서, 블록체인 네트워크 노드(302a)는 클라이언트 디바이스(304a)로부터 제안된 수정에 대해 블록체인 네트워크(310) 내에서 합의 절차를 개시한다. 블록체인 네트워크 노드(302a)는 블록체인 네트워크(310)에서 다른 합의 노드(302b-d)를 식별할 수 있다. 일부 실시예에서, 합의 절차는 블록체인 네트워크(310)의 합의 노드(302a-d) 사이에서 수행된다. 본 명세서에 설명된 합의 절차의 예로는 그중에도 작업 증명(proof of work), 지분 증명(proof of stake) 또는 실현가능한 비잔티움 장애 허용을 포함한다. 예를 들어, 합의 절차는, 합의 노드(302a)가 다른 합의 노드(예를 들어, 노드(302b-d))로 요청을 검증하기 위한 초기 메시지를 멀티캐스트하는 단계; 합의 노드(302b-d)가 스마트 계약을 사용하여 요청을 검증한 후 응답 메시지를 노드(302a)로 전송하는 단계; 및 합의 노드(302a)가 동일한 결과를 갖는 상이한 노드들로부터의 다수의 응답 메시지를 기다리는 단계를 수반할 수 있다. 동일한 결과를 갖는 상이한 노드로부터의 응답 메시지의 수가 미리 결정된 문턱값을 초과하는 경우, 합의 노드(302a)는 합의가 달성되었다고 결정하고 요청에서 제안된 수정을 수행할 수 있다. 예를 들어, 수정이 새로운 민감 데이터 요소를 감시 리스트에 추가하는 것을 포함하는 경우, 합의 노드(302a)는 새로운 민감 데이터 요소를 감시 리스트에 저장할 수 있다.

[0044] 408에서, 블록체인 네트워크 노드(302a)는 블록체인 네트워크(310)의 다른 네트워크 노드에 통지를 전송한다. 일부 실시예에서, 통지는 클라이언트 디바이스(304a)로부터의 요청에서의 수정 및 합의 절차를 실행하도록 다른 네트워크 노드를 지시하는 요청을 포함한다. 일부 실시예에서, 블록체인 네트워크 노드(302a)는 합의 노드(302a-d)만이 합의 절차에 참여하도록 통지되도록 합의 노드(302b-d)에 통지를 전송한다.

[0045] 410에서, 블록체인 네트워크 노드(302b-d)는 합의 절차를 실행한다. 일부 실시예들에서, 각각의 노드들(302b-d)은 다른 합의 노드들로 요청을 검증하기 위한 초기 메시지를 멀티캐스트하고, 동일한 결과를 갖는 상이한 노드들로부터의 다수의 응답 메시지를 기다린다. 동일한 결과를 갖는 상이한 노드로부터의 응답 메시지의 수가 미리 결정된 문턱값을 초과하는 경우, 블록체인 네트워크 노드(302b-d)는 합의가 달성되었다고 결정하고 요청에서 제안된 수정을 수행할 수 있다. 예를 들어, 수정이 새로운 민감 데이터 요소를 감시 리스트에 추가하는 것을 포함하는 경우, 블록체인 네트워크 노드(302b-d)는 새로운 합의 데이터 요소를 감시 리스트에 저장하여 각각의 합의 노드(302a-d)가 새로운 민감 데이터 요소를 포함하는 업데이트된 감시 리스트를 가질 수 있다.

[0046] 412에서, 블록체인 네트워크 노드(302b-d)는 각 네트워크 노드에서 합의 절차가 실행되었고 합의가 달성되었음을 나타내는 통지를 네트워크 노드(302a)에 전송한다.

[0047] 414에서, 블록체인 네트워크 노드(302a)는 다른 합의 노드로부터의 통지에 기초하여 블록체인 네트워크(310)의 합의 노드에 의해 합의 절차가 실행되었다고 결정한다. 일부 실시예들에서, 블록체인 네트워크 노드(302a)는 클라이언트 디바이스(304a)로부터의 요청에 기초하여 블록체인 트랜잭션을 생성하고 블록체인 트랜잭션에 기초하여 머클 트리 루트 해시 값을 계산한다. 머클 트리 루트 해시 값은 향후 합의 절차에서 악의적인 네트워크 노드를 식별하기 위해 합의 노드(302a-d)에 의해 사용될 수 있다.

[0048] 416에서, 클라이언트 디바이스(예를 들어, 클라이언트 디바이스(304b))는 블록체인 네트워크(310)에 저장된 감시 리스트의 민감 데이터 요소에 대한 조회 요청을 블록체인 네트워크 노드(302a)로 전송한다. 일부 실시예에서, 조회 요청은 클라이언트 디바이스(304b)의 개인 키를 사용하여 생성된 디지털 서명을 포함한다.

[0049] 418에서, 블록체인 네트워크 노드(302a)는 클라이언트 디바이스(304b)가 감시 리스트에서 민감 데이터 요소를 획득하도록 인가되었는지를 결정한다. 일부 실시예들에서, 블록체인 네트워크 노드(302a)는, 예를 들어, 요청에서의 디지털 서명, 및 404와 관련하여 또는 다른 방식으로 설명된 기술에 따라 블록체인 네트워크 노드(302a)에 저장된 화이트리스트에 리스트된 인가된 엔티티의 공개키에 기초하여, 클라이언트 디바이스(304b)가 감시 리스트의 민감 데이터 요소를 획득하도록 인가되었는지를 결정할 수 있다. 블록체인 네트워크 노드(302a)가 클라이언트 디바이스(304b)가 감시 리스트의 민감 데이터 요소를 획득하도록 인가되지 않았다고 결정하는 경우, 블록체인 네트워크 노드(302a)는 요청을 거부할 수 있다.

[0050] 420에서, 블록체인 네트워크 노드(302a)는 클라이언트 디바이스(304b)가 민감 데이터 요소를 획득하도록 인가되었다는 결정에 응답하여 민감 데이터 요소를 클라이언트 디바이스(304b)에 전송한다. 일부 실시예들에서, 민감 데이터 요소는 암호화되고 클라이언트 디바이스(304b)는 암호화된 민감 데이터 요소를 수신할 수 있다. 일부 실시예들에서, 민감 데이터 요소는 비밀 키(secret key)를 사용하여 암호화될 수 있다. 클라이언트 디바이스(304b)가 비밀 키를 보유하면, 클라이언트 디바이스(304b)는 암호화된 민감 데이터 요소를 복호화함으로써 민감 데이터 요소를 획득할 수 있다.

[0051] 도 5는 블록체인 네트워크에 저장된 민감 데이터 요소를 관리하기 위한 프로세스(500)의 예의 흐름도이다. 편의상, 프로세스(500)는 하나 이상의 위치에 위치되고 본 명세서에 따라 적절히 프로그래밍된 하나 이상의 컴퓨터의 시스템에 의해 수행되는 것으로 설명될 것이다. 예를 들어, 적절하게 프로그래밍된 분산 시스템, 예를 들어 도 3의 분산 시스템(300)은 프로세스(500)를 수행할 수 있다.

[0052] 502에서, 블록체인 네트워크 노드(예를 들어, 블록체인 네트워크 노드(302))는 클라이언트 디바이스(예를 들어, 클라이언트 디바이스(304))로부터 블록체인 네트워크(예를 들어, 블록체인 네트워크 노드(302))에 저장된 감시 리스트에 대해 수정을 수행하라는 요청을 수신한다. 일부 실시예에서, 블록체인 네트워크 노드는 블록체인 네트워크의 합의 노드일 수 있다. 일부 실시예들에서, 감시 리스트는 예를 들어 네트워크 노드(예를 들어, 블록체인 네트워크 또는 인터넷과 같은 또다른 네트워크)에 의해 모니터링 및/또는 필터링되는 다수의 민감 데이터 요소(예를 들어, 키워드의 형태)를 포함한다. 일부 실시예에서, 요청은 클라이언트 디바이스의 개인 키를 사용하여 생성된 디지털 서명을 포함한다. 일부 실시예들에서, 요청에서의 수정은 리스트에 데이터 요소를 추가하기 위한 요청, 리스트로부터 데이터 요소를 삭제하기 위한 요청, 또는 리스트에서 데이터 요소를 편집하기 위한 요청 중 하나 이상을 포함한다. 일부 실시예에서, 감시 리스트의 민감 데이터 요소는 암호화될 수 있다.

[0053] 504에서, 블록체인 네트워크 노드는 클라이언트 디바이스가 감시 리스트를 수정하도록 인가되었는지를 결정한다. 일부 실시예들에서, 블록체인 네트워크 노드는 클라이언트 디바이스가 클라이언트 디바이스로부터의 요청의 디지털 서명에 기초하여 감시 리스트를 수정하도록 인가되었지를 결정한다. 일부 실시예에서, 블록체인 네트워크 노드는 감시 리스트를 수정하도록 인가된 하나 이상의 클라이언트 디바이스의 식별자 및/또는 공개 키를 포함하는 화이트리스트를 저장한다. 일부 실시예에서, 네트워크 노드에 의해, 디지털 서명에 기초하여 클라이언트 디바이스가 감시 리스트를 수정하도록 인가되었는지를 결정하는 단계는, 예를 들어, 404와 관련하여 또는 또다른 방식으로 설명된 기술에 따라, 감시 리스트를 수정하도록 인가되는 인가된 엔티티의 공개 키 및 요청의 디지털 서명에 기초하여 클라이언트 디바이스가 감시 리스트를 수정하도록 인가되었다고 결정하는 단계를 포함한다.

[0054] 클라이언트 디바이스가 감시 리스트를 수정하도록 인가된 것으로 결정되면, 프로세스는 단계(506)로 진행한다. 클라이언트 디바이스가 감시 리스트를 수정하도록 인가되지 않은 것으로 결정되면, 프로세스는 단계(516)으로 진행하며, 여기서 요청은 거부된다.

[0055] 506에서, 블록체인 네트워크 노드는 클라이언트 디바이스가 감시 리스트를 수정하도록 인가된 것으로 결정되었다고 결정한 후에, 블록체인 네트워크 내의 요청에 대한 합의 절차를 수행한다. 본 명세서에 기술된 합의 절차의 예는 무엇보다도 작업 증명, 지분 증명 또는 실현가능한 비잔티움 장애 허용을 포함한다. 일부 실시예에서, 블록체인 네트워크 노드는 블록체인 네트워크에서 다른 합의 노드를 식별할 수 있다. 일부 실시예들에서, 합의 절차는 블록체인 네트워크의 합의 노드들 사이에서 수행된다. 예를 들어, 합의 절차는, 블록체인 네트워크 노드가 다른 합의 노드로 요청을 검증하기 위한 초기 메시지를 멀티캐스트하는 단계; 다른 합의 노드가 스마트 계약을 사용하여 요청을 검증한 후에, 블록체인 네트워크 노드로 응답 메시지를 전송하는 단계; 블록체인 네트워크 노드가 동일한 결과를 갖는 상이한 노드들로부터 다수의 응답 메시지를 기다리는 단계를 수반할 수 있다. 동일한 결과를 갖는 다른 합의 노드로부터의 응답 메시지의 수가 미리 결정된 문턱값을 초과하는 경우, 블록체인 네트워크 노드는 합의가 달성되었다고 결정할 수 있다.

[0056] 508에서, 블록체인 네트워크 노드는 합의 절차를 완료하고 합의가 달성되었다고 결정한 후에, 요청에서의 수정을 수행한다. 일부 예들에서, 수정이 새로운 민감 데이터 요소를 감시 리스트에 추가하는 것을 포함하는 경우, 블록체인 네트워크 노드는 새로운 민감 데이터 요소를 감시 리스트에 저장할 수 있다. 일부 실시예에서, 블록체인 네트워크 노드는 감시 리스트에 새로운 민감 데이터 요소를 저장하기 전에 새로운 민감 데이터 요소를 암호화할 수 있다.

[0057] 510에서, 블록체인 네트워크 노드는 예를 들어 제 2 클라이언트 디바이스로부터, 블록체인 네트워크에 저장된 감시 리스트의 민감 데이터 요소에 대한 조회 요청을 수신한다. 일부 실시예에서, 조회 요청은 제 2 클라이언트 디바이스의 개인 키를 사용하여 생성된 제 2 디지털 서명을 포함한다.

[0058] 512에서, 블록체인 네트워크 노드는 제 2 클라이언트 디바이스가 제 2 디지털 서명에 기초하여 민감 데이터 요소를 검토, 액세스, 또는 그렇지 않으면 획득하도록 인가되었는지를 결정한다. 일부 실시예에서, 블록체인 네트워크 노드는 감시 리스트의 민감 데이터 요소를 검토, 액세스 또는 그렇지 않으면 획득(총괄적으로 감시 리스트 조회로 지칭됨)하도록 인가된 하나 이상의 클라이언트 디바이스의 식별자 및/또는 공개 키를 포함하는 화이트리스트를 저장한다. 일부 실시예에서, 화이트리스트는 감시 리스트를 수정하도록 인가된 하나 이상의 클라이

언트 디바이스의 식별자 및/또는 공개 키를 포함하는 화이트리스트와 동일하거나 상이할 수 있다. 일부 실시예에서, 클라이언트 디바이스는 감시 리스트의 허용된 동작에 대하여 추가의 또는 상이한 레벨의 인가(authority)를 할당받을 수 있으며, 단일 또는 다중 화이트리스트에 표시될 수 있다.

[0059] 일부 실시예에서, 네트워크 노드에 의해, 클라이언트 디바이스가 디지털 서명에 기초하여 감시 리스트를 조회하도록 인가되었는지를 결정하는 단계는, 예를 들어, 404와 관련하여 또는 또다른 방식으로 설명된 기술에 따라, 감시 리스트를 조회하도록 인가되는 인가된 엔티티의 공개 키 및 디지털 서명에 기초하여 클라이언트 디바이스가 감시 리스트를 조회하도록 인가되었다고 결정하는 단계를 포함한다.

[0060] 클라이언트 디바이스가 감시 리스트를 조회하도록 인가된 것으로 결정되면, 프로세스는 단계(514)로 진행한다. 클라이언트 디바이스가 감시 리스트를 조회하도록 인가되지 않은 것으로 결정되면, 프로세스는 단계(518)로 진행하고, 여기서 요청은 거부된다.

[0061] 514에서, 제 2 클라이언트 디바이스가 민감 데이터 요소를 획득하도록 인가되었다는 결정에 응답하여, 블록체인 네트워크 노드는 제 2 클라이언트 디바이스로 응답을 전송한다. 응답은 요청된 민감 데이터 요소를 포함한다. 일부 실시예들에서, 감시 리스트의 민감 데이터 요소는 암호화되고, 응답은 암호화된 민감 데이터 요소를 포함한다.

[0062] 도 6은 본 명세서의 실시예들에 따른 장치(600)의 모듈들의 예의 도면이다. 장치(600)는 블록체인 네트워크에 저장된 민감 데이터 요소를 관리하도록 구성된 블록체인 네트워크의 노드의 실시예의 예일 수 있다. 장치(600)는 상술된 실시예들에 대응할 수 있고, 장치(600)는, 블록체인 네트워크에 저장된 감시 리스트에 대해 수정을 수행하라는 요청을 클라이언트 디바이스로부터 수신하는 수신 모듈(602) - 감시 리스트는 다수의 민감 데이터 요소를 포함하고, 요청은 클라이언트 디바이스의 개인 키를 사용하여 생성된 디지털 서명을 포함함 - ; 디지털 서명에 기초하여 클라이언트 디바이스가 감시 리스트를 수정하도록 인가되었는지를 결정하는 결정 모듈(604); 클라이언트 디바이스가 감시 리스트를 수정하도록 인가되었다는 결정에 응답하여 블록체인 네트워크 내의 요청에 대한 합의 절차를 수행하는 수행 모듈(606); 합의 절차가 완료된 후에 합의가 달성되었다는 결정에 응답하여 감시 리스트에 대해 수정을 수행하는 수행 모듈(608); 및 감시 리스트에 대해 수정을 수행하라는 클라이언트 디바이스로부터의 요청을 거부하는 거부 모듈(610)을 포함한다.

[0063] 선택적 실시예에서, 다수의 민감 데이터 요소에는 하나 이상의 인가된 엔티티에 의해 모니터링, 필터링 또는 둘 모두가 수행된다.

[0064] 선택적인 실시예에서, 감시 리스트에 대해 수정을 수행하라는 요청은 감시 리스트에 새로운 민감 데이터 요소를 추가하라는 요청, 감시 리스트로부터 민감 데이터 요소를 제거하라는 요청, 또는 감시 리스트에서 민감 데이터 요소를 편집하라는 요청 중 하나 이상을 포함한다.

[0065] 선택적 실시예에서, 다수의 민감 데이터 요소는 암호화된다.

[0066] 선택적인 실시예에서, 장치(600)는, 감시 리스트를 수정하도록 인가되는 인가된 엔티티의 공개 키 및 디지털 서명에 기초하여 클라이언트 디바이스가 감시 리스트를 수정하도록 인가되었다고 결정하는 결정 서브모듈을 더 포함한다.

[0067] 선택적 실시예에서, 인가된 엔티티는 네트워크 노드에 저장된 화이트리스트에 표시되고, 화이트리스트는 감시 리스트를 수정하도록 인가된 하나 이상의 인가된 엔티티를 포함한다.

[0068] 선택적인 실시예에서, 장치(600)는, 블록체인 네트워크에 저장된 감시 리스트의 민감 데이터 요소에 대한 조회 요청을 제 2 클라이언트 디바이스로부터 수신하는 수신 모듈 - 조회 요청은 제 2 클라이언트 디바이스의 개인 키를 사용하여 생성된 제 2 디지털 서명을 포함함 - ; 상기 제 2 디지털 서명에 기초하여 제 2 클라이언트 디바이스가 상기 민감 데이터 요소를 획득하도록 인가되었는지를 결정하는 결정 모듈; 및 암호화된 민감 데이터 요소를 포함하는 응답을 상기 제 2 클라이언트 디바이스로 송신하는 송신 모듈을 더 포함한다.

[0069] 이전의 실시예들에서 예시된 시스템, 장치, 모듈 또는 유닛은 컴퓨터 칩 또는 엔티티를 사용함으로써 구현될 수 있거나 또는 특정 기능을 갖는 제품을 사용함으로써 구현될 수 있다. 통상적인 실시예 디바이스는 컴퓨터이고, 컴퓨터는 개인용 컴퓨터, 랩탑 컴퓨터, 셀룰러 폰, 카메라 폰, 스마트 폰, 개인 휴대 정보 단말, 미디어 플레이어, 네비게이션 디바이스, 이메일 수신 및 전송 디바이스, 게임 콘솔, 태블릿 컴퓨터, 웨어러블 디바이스, 또는 이러한 디바이스들의 임의의 조합일 수 있다.

[0070] 장치에서 각각의 모듈의 기능들 및 역할들의 실시예 프로세스에 대해, 이전 방법에서의 대응하는 단계들의 실시

예 프로세스가 참조될 수 있다. 세부사항들은 단순화를 위해 여기에서 생략된다.

[0071] 장치 실시예가 기본적으로 방법 실시예에 대응하기 때문에, 관련 부분들에 대해, 방법 실시예에서의 관련 설명들이 참조될 수 있다. 이전에 설명된 장치 실시예는 단지 예이다. 별개의 부분들로 설명된 모듈들은 물리적으로 별개일 수 있거나 아닐 수 있고, 모듈들로 디스플레이된 부분들은 물리적 모듈들일 수 있거나 아닐 수 있고, 하나의 위치에 위치될 수 있거나, 또는 다수의 네트워크 모듈들 상에 분산될 수 있다. 모듈들 중 일부 또는 전부는 본 명세서의 솔루션들의 목적들을 달성하기 위한 실제 요구들에 기초하여 선택될 수 있다. 당업자는 창작적 노력 없이 본 출원의 실시예들을 이해하고 구현할 수 있다.

[0072] 도 6을 다시 참조하면, 블록체인 데이터 요소 관리 장치의 내부 기능 모듈 및 구조를 예시하는 것으로 해석될 수 있다. 블록체인 데이터 요소 관리 장치는 블록체인 네트워크에 저장된 민감 데이터 요소를 관리하도록 구성된 블록체인 네트워크 노드의 예일 수 있다. 본질적으로 실행 바디는 전자 디바이스일 수 있고, 전자 디바이스는, 하나 이상의 프로세서, 및 하나 이상의 프로세서의 실행 가능한 명령어를 저장하도록 구성된 메모리를 포함한다.

[0073] 본 명세서에 기술된 기술은 하나 이상의 기술적 효과를 생성한다. 일부 실시예에서, 클라이언트 디바이스가 블록체인 네트워크에 저장된 감시 리스트에 수정을 수행하라는 요청을 제출할 때, 요청을 수신하는 블록체인 네트워크의 네트워크 노드는 요청의 클라이언트 디바이스의 디지털 서명에 기초하여 클라이언트 디바이스를 인증할 필요가 있다. 일부 실시예에서, 인증된 클라이언트 디바이스는 수정을 수행하도록 허용될 수 있지만, 인증에 실패한 클라이언트 디바이스는 수정을 수행하는 것이 거부될 것이다. 이는 악의적인 행위자에 의해 블록체인 네트워크에 저장된 민감 데이터가 위태롭게 되는 것을 방지함으로써 블록체인 네트워크의 데이터 보안을 향상시킬 수 있다. 또한, 일부 실시예에서, 감시 리스트의 민감 데이터 요소는 암호화된다(예를 들어, 비밀 키를 사용하여 암호화). 비밀 키를 보유한 클라이언트 디바이스만이 암호화된 데이터 요소를 복호화하고 민감 데이터 요소를 획득할 수 있다. 이는 악의적인 행위자가 블록체인 네트워크에 침투하여 민감 데이터 요소를 획득하는 것을 방지함으로써, 블록체인 네트워크의 데이터 보안을 향상시킨다. 게다가, 감시 리스트의 민감 데이터 요소는 분산 방식으로 블록체인 네트워크에 저장된다. 분산 블록체인 네트워크의 변형 억제(tamper-resistant) 특성으로 인해, 감시 리스트에 대한 악의적인 행위 및 사이버 공격이 완화될 수 있다.

[0074] 본 발명의 설명된 실시예는 하나 이상의 특징을 단독으로 또는 조합하여 포함할 수 있다. 예를 들어, 제 1 실시예에서, 블록체인 네트워크에 저장된 민감 데이터 요소를 관리하는 방법은, 블록체인 네트워크의 네트워크 노드에 의해 클라이언트 디바이스로부터 블록체인 네트워크에 저장된 감시 리스트에 대해 수정을 수행하라는 요청을 수신하는 단계 - 감시 리스트는 복수의 민감 데이터 요소를 포함하고, 요청은 클라이언트 디바이스의 개인 키를 사용하여 생성된 디지털 서명임 - ; 네트워크 노드에 의해, 디지털 서명에 기초하여 클라이언트 디바이스가 감시 리스트를 수정하도록 인가되었는지를 결정하는 단계; 클라이언트 디바이스가 감시 리스트를 수정하도록 인가되었다는 결정에 응답하여, 네트워크 노드에 의해 블록체인 네트워크 내의 요청에 대한 합의 절차를 수행하고, 합의 절차를 완료한 후에 합의가 달성되었다는 결정에 응답하여, 네트워크 노드에 의해 감시 리스트에 대해 수정을 수행하는 단계; 및 클라이언트 디바이스가 감시 리스트를 수정하도록 인가되지 않았다는 결정에 응답하여, 네트워크 노드에 의해, 클라이언트 디바이스로부터의 감시 리스트에 대해 수정을 수행하라는 요청을 거부하는 단계를 포함한다. 상기 및 다른 설명된 실시예는 각각 선택적으로 다음 특징 중 하나 이상을 포함할 수 있다:

[0075] 하기 특징들 중 임의의 특징과 커플링될 수 있는 제 1 특징은, 복수의 민감 데이터 요소에 하나 이상의 인가된 엔티티에 의해 모니터링, 필터링 또는 둘 모두가 수행된다는 것을 명시한다.

[0076] 상기 또는 하기 특징들 중 임의의 것과 커플링될 수 있는 제 2 특징은, 감시 리스트에 대해 수정을 수행하라는 요청은, 감시 리스트에 새로운 민감 데이터 요소를 추가하라는 요청, 감시 리스트로부터 민감 데이터 요소를 제거하라는 요청, 및 감시 리스트에서 민감 데이터 요소를 편집하라는 요청 중 하나 이상을 포함한다는 것을 명시한다.

[0077] 상기 또는 하기 특징들 중 임의의 것과 커플링될 수 있는 제 3 특징은, 복수의 민감 데이터 요소가 암호화된다는 것을 명시한다.

[0078] 상기 또는 하기 특징들 중 임의의 것과 커플링될 수 있는 제 4 특징은, 네트워크 노드에 의해 디지털 서명에 기초하여 클라이언트 디바이스가 감시 리스트를 수정하도록 인가되었는지를 결정하는 단계는, 클라이언트 디바이스가 감시 리스트를 수정하도록 인가되는 인증된 엔터티의 공개 키 및 디지털 서명에 기초하여 클라이언트 디바

이스가 감시 리스트를 수정하도록 인가되었다고 결정하는 단계를 포함한다는 것을 명시한다.

[0079] 상기 또는 하기 특징들 중 임의의 것과 커플링될 수 있는 제 5 특징은, 인가된 엔티티는 네트워크 노드에 저장된 화이트리스트에 표시되고, 화이트리스트는 감시 리스트를 수정하도록 인가되는 하나 이상의 인가된 엔티티를 포함한다는 것을 명시한다.

[0080] 상기 또는 하기 특징들 중 임의의 것과 커플링될 수 있는 제 6 특징은, 상기 방법이, 네트워크 노드에 의해 블록체인 네트워크에 저장된 감시 리스트의 민감 데이터 요소에 대한 조회 요청을 제 2 클라이언트 디바이스로부터 수신하는 단계 - 조회 요청은 제 2 클라이언트 디바이스의 개인 키를 사용하여 생성된 제 2 디지털 서명을 포함함 - ; 네트워크 노드에 의해 제 2 디지털 서명에 기초하여 제 2 클라이언트 디바이스가 민감 데이터 요소를 획득하도록 인가되었는지를 결정하는 단계; 및 제 2 클라이언트 디바이스가 민감 데이터 요소를 획득하도록 인가되었다는 결정에 응답하여, 네트워크 노드에 의해 제 2 클라이언트 디바이스로 응답을 송신하는 단계 - 응답은 암호화된 민감 데이터 요소를 포함함 - 를 더 포함한다는 것을 명시한다.

[0081] 본 명세서에 설명된 요지, 액션들 및 동작들의 실시예들은 디지털 전자 회로로, 유형적으로 구현된 컴퓨터 소프트웨어 또는 펌웨어로, 또는 본 명세서에서 개시된 구조들 및 이들의 구조적 등가물들을 포함하는 컴퓨터 하드웨어로, 또는 이들의 하나 이상의 조합들로 구현될 수 있다. 본 명세서에 설명된 요지의 실시예들은 하나 이상의 컴퓨터 프로그램들, 예를 들어, 데이터 프로세싱 장치에 의한 실행을 위해 또는 데이터 프로세싱 장치의 동작을 제어하기 위해, 컴퓨터 프로그램 캐리어 상에 인코딩된 컴퓨터 프로그램 명령어들의 하나 이상의 모듈들로서 구현될 수 있다. 예를 들어, 컴퓨터 프로그램 캐리어는, 인코딩된 또는 저장된 명령어들을 갖는 하나 이상의 컴퓨터 판독가능 저장 매체를 포함할 수 있다. 캐리어는 자기, 광자기, 또는 광학 디스크, 솔리드 스테이트 드라이브, 랜덤 액세스 메모리(RAM), 판독 전용 메모리(ROM) 또는 다른 유형들의 매체들과 같은 유형의 비일시적 컴퓨터 판독가능 매체일 수 있다. 대안적으로 또는 추가적으로, 캐리어는 인공적으로 생성된 전파되는 신호, 예를 들어, 데이터 프로세싱 장치에 의한 실행을 위해 적절한 수신기 장치로의 송신을 위해 정보를 인코딩하도록 생성된 머신-생성된 전기적, 광학적 또는 전자기적 신호일 수 있다. 컴퓨터 저장 매체는 머신 판독가능 저장 디바이스, 머신 판독가능 저장 기판, 랜덤 또는 직렬 액세스 메모리 디바이스, 또는 이들 중 하나 이상의 조합일 수 있거나 또는 이들의 일부일 수 있다. 컴퓨터 저장 매체는 전파되는 신호가 아니다.

[0082] 프로그램, 소프트웨어, 소프트웨어 애플리케이션, 앱, 모듈, 소프트웨어 모듈, 엔진, 스크립트 또는 코드로 또한 지칭되거나 설명될 수 있는 컴퓨터 프로그램은 컴파일된 또는 해석된 언어들, 또는 선언적 또는 절차적 언어들을 포함하는 임의의 형태의 프로그래밍 언어로 기록될 수 있고, 독립형 프로그램으로서 또는 모듈, 컴포넌트, 엔진, 서브루틴 또는 컴퓨팅 환경에서 실행하기에 적합한 다른 유닛을 포함하는 임의의 형태로 배치될 수 있고, 이러한 환경은 하나 이상의 위치들에서 데이터 통신 네트워크에 의해 상호접속되는 하나 이상의 컴퓨터들을 포함할 수 있다.

[0083] 컴퓨터 프로그램은 파일 시스템 내의 파일에 대응할 수 있지만 반드시 그럴 필요는 없다. 컴퓨터 프로그램은 다른 프로그램들 또는 데이터, 예를 들어, 마크업 언어 문서에 저장된 하나 이상의 스크립트들, 문제의 프로그램에 전용되는 단일 파일, 또는 다수의 조정된 파일들, 예를 들어, 하나 이상의 모듈들, 서브-프로그램 또는 코드의 일부들을 저장하는 파일들에 저장될 수 있다.

[0084] 컴퓨터 프로그램의 실행을 위한 프로세서들은 예시의 방식으로, 범용 및 특수 목적 마이크로프로세서들 둘 모두, 및 임의의 종류의 디지털 컴퓨터의 임의의 하나 이상의 프로세서들을 포함한다. 일반적으로, 프로세서는 실행을 위한 컴퓨터 프로그램의 명령어들 뿐만 아니라 프로세서에 커플링된 비일시적 컴퓨터 판독가능 매체로부터의 데이터를 수신할 것이다.

[0085] 용어 "데이터 프로세싱 장치"는 예를 들어, 프로그래밍가능 프로세서, 컴퓨터, 또는 다수의 프로세서들 또는 컴퓨터들을 포함하는, 데이터를 프로세싱하기 위한 모든 종류의 장치들, 디바이스들 및 머신들을 포함한다. 데이터 프로세싱 장치는 특수 목적 로직 회로, 예를 들어, FPGA(field programmable gate array), ASIC(application-specific integrated circuit) 또는 GPU(graphics processing unit)를 포함할 수 있다. 장치는 또한 하드웨어에 추가로, 컴퓨터 프로그램들에 대한 실행 환경을 생성하는 코드, 예를 들어, 프로세서 펌웨어, 프로토콜 스택, 데이터베이스 관리 시스템, 운영 시스템 또는 이들의 하나 이상의 조합을 구성하는 코드를 포함할 수 있다.

[0086] 본 명세서에서 설명된 프로세스들 및 로직 흐름들은 입력 데이터에 대해 동작하고 출력을 생성함으로써 동작들을 수행하기 위해 하나 이상의 컴퓨터 프로그램들을 실행하는 하나 이상의 컴퓨터들 또는 프로세서들에 의해 수

행될 수 있다. 프로세스들 및 로직 흐름들은 또한 특수 목적 로직 회로, 예를 들어, FPGA, ASIC 또는 GPU에 의해, 또는 특수 목적 로직 회로와 하나 이상의 프로그래밍된 컴퓨터들의 조합에 의해 수행될 수 있다.

[0087] 컴퓨터 프로그램의 실행에 적합한 컴퓨터들은 범용 또는 특수 목적 마이크로프로세서들 또는 둘 모두, 또는 임의의 다른 종류의 중앙 프로세싱 유닛에 기초할 수 있다. 일반적으로, 중앙 프로세싱 유닛은 판독 전용 메모리 또는 랜덤 액세스 메모리 또는 둘 모두로부터 명령어들 및 데이터를 수신할 것이다. 컴퓨터의 요소들은 명령어들을 실행하기 위한 중앙 프로세싱 유닛 및 명령어들 및 데이터를 저장하기 위한 하나 이상의 메모리 디바이스들을 포함할 수 있다. 중앙 프로세싱 유닛 및 메모리는 특수 목적 로직 회로에 의해 보완되거나 그에 통합될 수 있다.

[0088] 일반적으로, 컴퓨터는 또한 데이터를 하나 이상의 저장 디바이스들을 포함하거나, 또는 이들로부터 데이터를 수신하거나 이들에 데이터를 전송하기 위해 동작가능하게 커플링될 것이다. 저장 디바이스들은, 예를 들어, 자기, 광자기 또는 광학 디스크들, 솔리드 스테이트 드라이브들 또는 임의의 다른 유형의 비일시적 컴퓨터 판독가능 매체들일 수 있다. 그러나, 컴퓨터는 이러한 디바이스들을 가질 필요가 없다. 따라서, 컴퓨터는 로컬 및/또는 원격인 하나 이상의 메모리들과 같은 하나 이상의 저장 디바이스들에 커플링될 수 있다. 예를 들어, 컴퓨터는 컴퓨터의 통합 컴포넌트들인 하나 이상의 로컬 메모리들을 포함할 수 있거나, 또는 컴퓨터는 클라우드 네트워크에 있는 하나 이상의 원격 메모리들에 커플링될 수 있다. 또한, 컴퓨터는 다른 디바이스, 예를 들어, 몇몇 예를 들자면, 모바일 전화, 개인 휴대 정보 단말(PDA), 모바일 오디오 또는 비디오 플레이어, 게임 콘솔, GPS(Global Positioning System) 수신기, 휴대용 저장 디바이스, 예를 들어, 범용 직렬 버스(USB) 플래시 드라이브에 내장될 수 있다.

[0089] 컴포넌트들은 직접적으로 또는 하나 이상의 중간적 컴포넌트들을 통해 서로 전기적으로 또는 광학적으로 접속되는 것과 같이 통신가능하게 됨으로써 서로 "커플링"될 수 있다. 컴포넌트들은 또한, 컴포넌트들 중 하나가 다른 것에 통합되면 서로 "커플링"될 수 있다. 예를 들어, 프로세서에 통합되는 저장 컴포넌트(예를 들어, L2 캐시 컴포넌트)는 프로세서에 "커플링"된다.

[0090] 사용자와의 상호작용을 제공하기 위해, 본 명세서에서 설명된 요지의 실시예들은, 사용자에게 정보를 디스플레이하기 위한 디스플레이 디바이스, 예를 들어, LCD(liquid crystal display) 모니터, 및 사용자가 컴퓨터에 입력을 제공할 수 있게 하는 입력 디바이스, 예를 들어, 키보드 및 포인팅 디바이스, 예를 들어, 마우스, 트랙볼 또는 터치패드를 갖는 컴퓨터 상에 구현되거나 그와 통신하도록 구성될 수 있다. 다른 종류들의 디바이스들이 또한 사용자와의 상호작용을 제공하기 위해 사용될 수 있는데: 예를 들어, 사용자에게 제공된 피드백은 임의의 형태의 센서 피드백, 예를 들어, 시각적 피드백, 청각적 피드백 또는 촉각적 피드백일 수 있고; 사용자로부터의 입력은 음향, 스피치 또는 촉각적 입력을 포함하는 임의의 형태로 수신될 수 있다. 또한, 컴퓨터는 예를 들어, 웹 브라우저로부터 수신된 요청들에 응답하여 사용자의 디바이스 상의 웹 브라우저에 웹 페이지들을 전송함으로써, 또는 사용자 디바이스, 예를 들어, 스마트폰 또는 전자 태블릿 상에서 실행되는 앱과 상호작용함으로써, 사용자에 의해 사용되는 디바이스에 문서들을 전송하고 그로부터 문서들을 수신함으로써 사용자와 상호작용할 수 있다. 또한, 컴퓨터는 개인용 디바이스, 예를 들어, 메시징 애플리케이션을 실행하고 리턴으로 사용자로부터 응답 메시지들을 수신하는 스마트폰에 텍스트 메시지들 또는 다른 형태들의 메시지를 전송함으로써 사용자와 상호작용할 수 있다.

[0091] 본 명세서는 시스템들, 장치 및 컴퓨터 프로그램 컴포넌트들과 관련하여 용어 "구성되는"을 사용한다. 하나 이상의 컴퓨터들의 시스템이 특정 동작들 또는 액션들을 수행하도록 구성되는 것은, 시스템이 시스템으로 하여금 동작들 또는 액션들을 수행하게 하도록 동작하는 소프트웨어, 펌웨어, 하드웨어 또는 이들의 조합이 설치되어 있음을 의미한다. 하나 이상의 컴퓨터 프로그램들이 특정 동작들 또는 액션들을 수행하도록 구성되는 것은, 하나 이상의 프로그램들이 데이터 프로세싱 장치에 의해 실행되는 경우 장치로 하여금 동작들 또는 액션들을 수행하게 하는 명령어들을 포함함을 의미한다. 특수 목적 로직 회로가 특정 동작들 또는 액션들을 수행하도록 구성되는 것은, 회로가 동작들 또는 액션들을 수행하는 전자 로직을 가짐을 의미한다.

[0092] 본 명세서서는 많은 특정 실시예 세부사항들을 포함하지만, 이들은, 청구항들 자체에 의해 정의되는, 청구되고 있는 범주에 대한 제한들로서 해석되는 것이 아니라, 오히려 특정 실시예들에 특정될 수 있는 특징들의 설명들로서 해석되어야 한다. 별개의 실시예들의 콘텍스트에서 본 명세서에서 설명된 특정 특징들은 또한 조합하여 단일 실시예로 실현될 수 있다. 반대로, 단일 실시예들의 맥락에서 설명된 다양한 특징들은 또한 다수의 실시예들에서 별개로 또는 임의의 적절한 하위 조합으로 실현될 수 있다. 또한, 특징들은 특정 조합들로 작용하는 것으로 앞서 설명되고 심지어 초기에 이와 같이 청구될 수 있지만, 청구된 조합으로부터의 하나 이상의 특징들

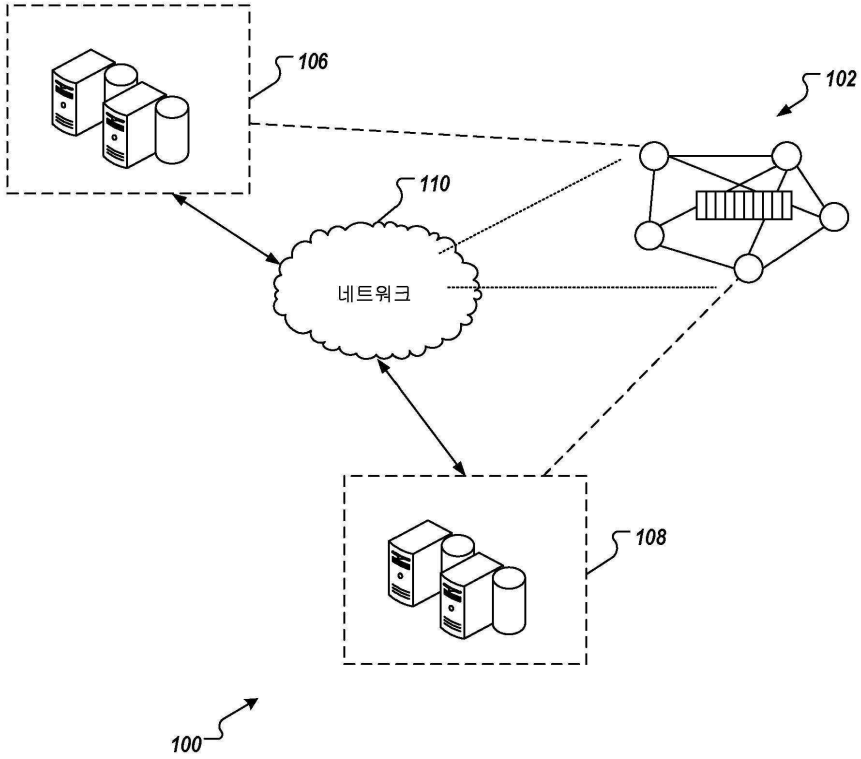
은 일부 경우들에서 조합으로부터 제거될 수 있고, 청구항은 하위 조합 또는 하위 조합의 변형으로 유도될 수 있다.

[0093] 유사하게, 동작들이 도면들에서 도시되고 청구항들에서 특정 순서로 인용되어 있지만, 이는 바람직한 결과들을 달성하기 위해 이러한 동작들이 도시된 특정 순서로 또는 순차적인 순서로 수행되거나 모든 예시된 동작들이 수행되도록 요구하는 것으로 이해되어서는 안된다. 특정 상황들에서, 멀티태스킹 및 병렬적 프로세싱이 유리할 수 있다. 또한, 앞서 설명된 실시예들에서 다양한 시스템 모듈들 및 컴포넌트들의 분리는 모든 실시예들에서 이러한 분리를 요구하는 것으로 이해되지 않아야 하며, 설명된 프로그램 컴포넌트들 및 시스템들은 일반적으로 단일 소프트웨어 제품에서 함께 통합되거나 다수의 소프트웨어 제품들로 패키징될 수 있음을 이해해야 한다.

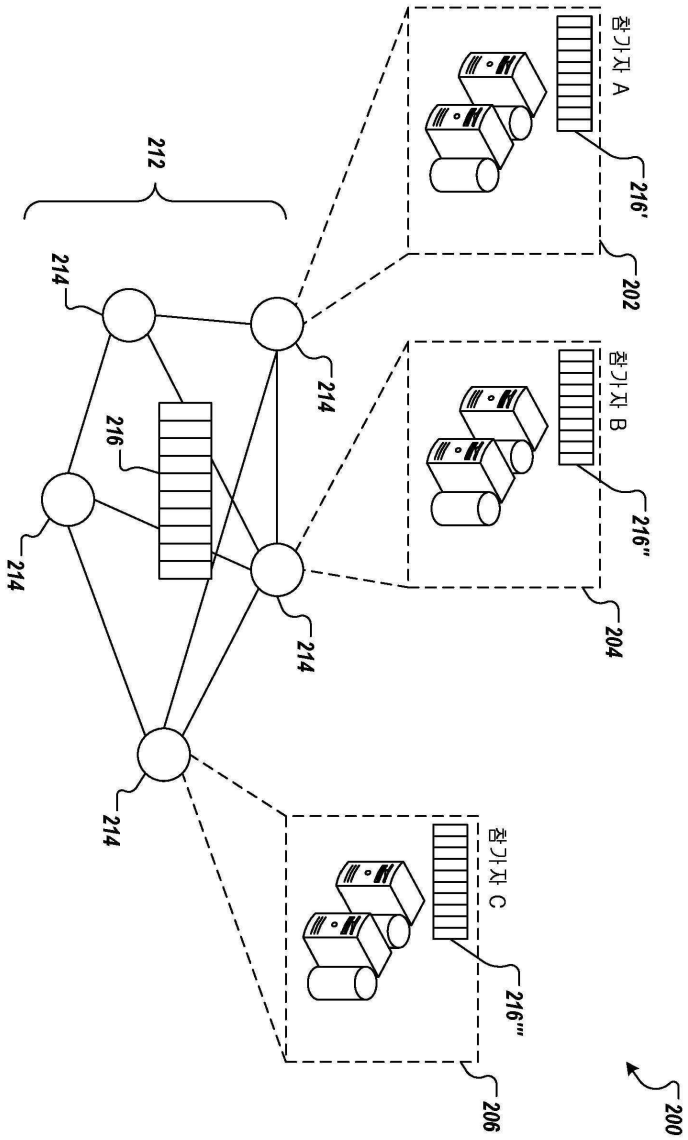
[0094] 요지의 특정 실시예들이 설명되었다. 다른 실시예들은 다음의 청구항들의 범위 내에 존재한다. 예를 들어, 청구항들에서 인용되는 액션들은 상이한 순서로 수행되고 여전히 바람직한 결과들을 달성할 수 있다. 일례로서, 첨부된 도면들에 도시된 프로세스들은, 바람직한 결과들을 달성하기 위해, 반드시 도시된 특정 순서 또는 순차적인 순서를 요구하지는 않는다. 일부 경우들에서, 멀티태스킹 및 병렬적 프로세싱이 유리할 수 있다.

도면

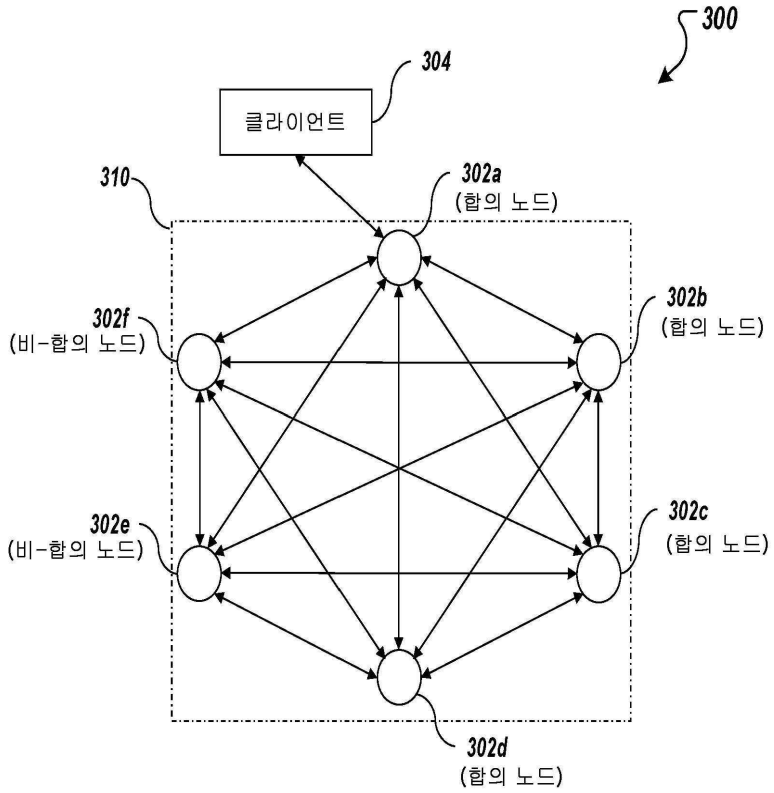
도면1



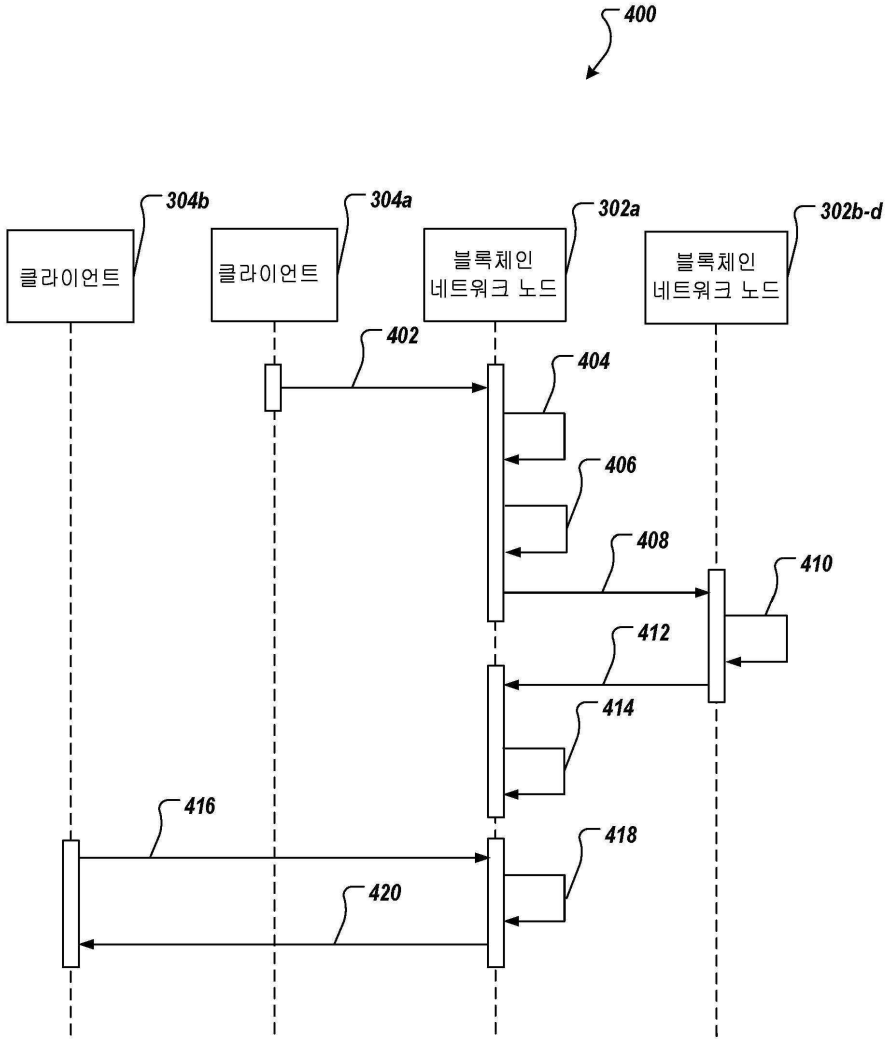
도면2


참가자 A
216'
202
212
214
214
216
참가자 B
216''
204
214
214
참가자 C
216'''
206
200

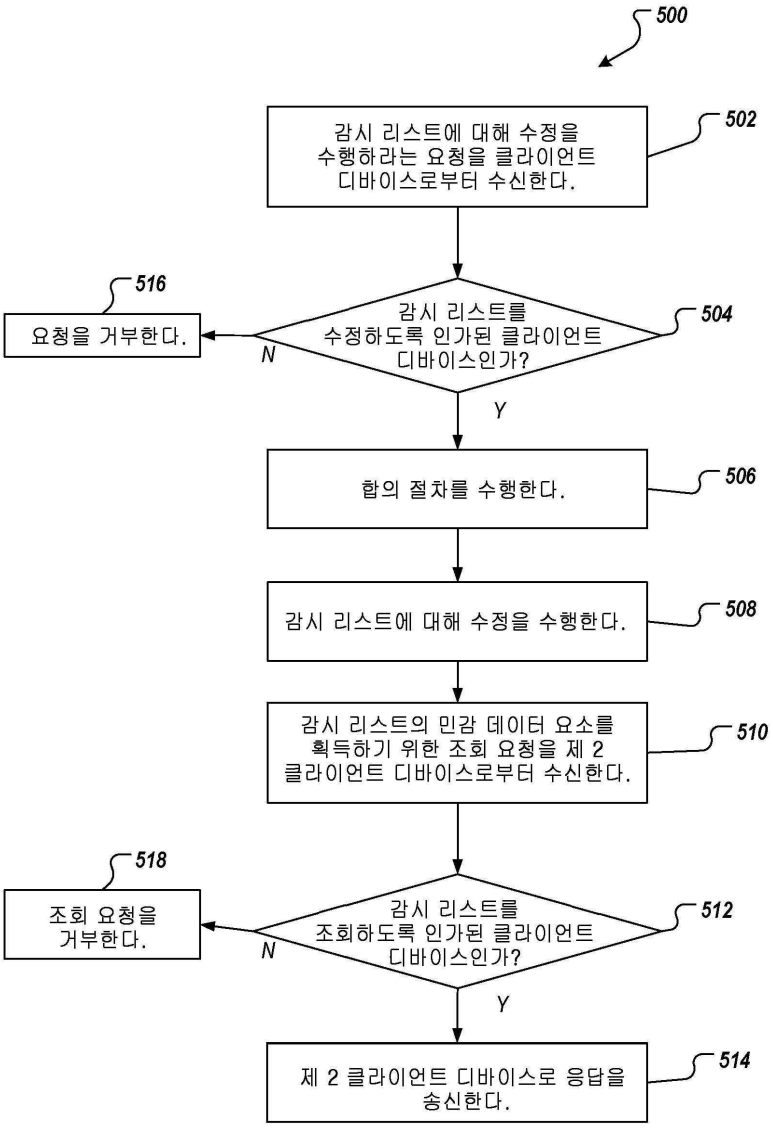
도면3


300
304
클라이언트
310
302a
(합의 노드)
302b
(합의 노드)
302c
(합의 노드)
302d
(합의 노드)
302e
(비-합의 노드)
302f
(비-합의 노드)

도면4


400
304b
304a
302a
302b-d
클라이언트
클라이언트
블록체인
네트워크 노드
블록체인
네트워크 노드
402
404
406
408
410
412
414
416
418
420

도면5


500
감시 리스트에 대해 수정을 수행하라는 요청을 클라이언트 디바이스로부터 수신한다.
502
감시 리스트를 수정하도록 인가된 클라이언트 디바이스인가?
504
N
516
요청을 거부한다.
Y
합의 절차를 수행한다.
506
감시 리스트에 대해 수정을 수행한다.
508
감시 리스트의 민감 데이터 요소를 획득하기 위한 조회 요청을 제 2 클라이언트 디바이스로부터 수신한다.
510
감시 리스트를 조회하도록 인가된 클라이언트 디바이스인가?
512
N
518
조회 요청을 거부한다.
Y
제 2 클라이언트 디바이스로 응답을 송신한다.
514

도면6