(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2023년07월18일
(11) 등록번호 10-2557341
(24) 등록일자 2023년07월14일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *H04L 9/08* (2006.01)
(52) CPC특허분류
H04L 9/3247 (2013.01)
H04L 9/0825 (2013.01)
(21) 출원번호 10-2023-7014239(분할)
(22) 출원일자(국제) 2017년07월27일
심사청구일자 2023년04월26일
(85) 번역문제출일자 2023년04월26일
(65) 공개번호 10-2023-0062672
(43) 공개일자 2023년05월09일
(62) 원출원 특허 10-2019-7005619
원출원일자(국제) 2017년07월27일
심사청구일자 2020년07월27일
(86) 국제출원번호 PCT/US2017/044186
(87) 국제공개번호 WO 2018/022891
국제공개일자 2018년02월01일
(30) 우선권주장
62/368,408 2016년07월29일 미국(US)
(56) 선행기술조사문헌
US20030172297 A1*
US20140032913 A1*
US20160192194 A1*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
매직 립, 인코포레이티드
미국 플로리다 플랜타티온 웨스트 선라이즈 블러바드 7500 (우: 33322)
(72) 발명자
캘러, 아드리안
미국 90027 캘리포니아 로스 앤젤레스 노스 웨스턴 애비뉴 1940
(74) 대리인
특허법인 남앤남

전체 청구항 수 : 총 5 항 심사관 : 양종필

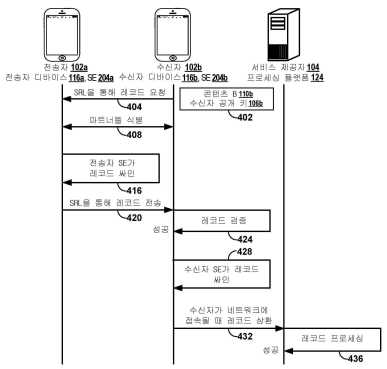
(54) 발명의 명칭 **암호화방식으로 싸인된 레코드들의 안전한 교환**

(57) 요 약

암호화방식으로 싸인된 레코드(signed record)들을 안전하게 교환하기 위한 시스템들 및 방법들이 개시된다. 일 양상에서, 콘텐츠 요청을 수신한 후에, 전송자 디바이스는 요청을 하는 수신자 디바이스(예컨대, 에이전트 디바이스)에 레코드를 전송할 수 있다. 레코드는, 디바이스들이 중앙집중형 프로세싱 플랫폼과 통신하지 않을 수도

(뒷면에 계속)

대 표 도 - 도4



있지만 비중앙집중형(예컨대, 피어-투-피어) 방식으로 단거리 링크를 통해 전송될 수 있다. 레코드는 전송자 디바이스의 개인 키를 사용하여 생성된 전송자 서명을 포함할 수 있다. 수신자 디바이스는 전송자 디바이스의 공개 키를 사용하여 전송자 서명의 진본성을 검증할 수 있다. 암호화 방식-기반 수신자 서명을 부가한 후에, 수신자 디바이스는 레코드를 플랫폼에 상환할 수 있다. 레코드의 성공적 검증 시에, 플랫폼은 레코드의 콘텐츠에 의해 명령된 대로 수행할 수 있다(예컨대, 사용자 계정을 수정 또는 업데이트함).

(52) CPC특허분류
H04L 2209/80 (2013.01)

명 세 서

청구범위

청구항 1

에이전트들에 의해 암호화방식으로 싸인된 레코드들을 안전하게 교환하기 위한 방법으로서,

하드웨어 프로세서의 제어 하에:

본인 디바이스로부터 본인-수정된 개별 레코드를 수신하는 단계 - 상기 본인-수정된 개별 레코드는 상기 본인-수정된 개별 레코드의 서명 및 에이전트-수정된 개별 레코드를 포함하고,

상기 에이전트-수정된 개별 레코드는 오리지널 개별 레코드, 에이전트 디바이스의 에이전트 공개 키, 및 상기 에이전트-수정된 개별 레코드의 서명을 포함하고,

상기 오리지널 개별 레코드는 레코드 콘텐츠, 레코드 전송자 디바이스의 전송자 공개 키, 상기 본인 디바이스의 본인 공개 키, 및 상기 오리지널 개별 레코드의 서명을 포함하고,

상기 본인-수정된 개별 레코드의 서명은 상기 본인 디바이스의 본인 개인 키를 사용하여 생성되고,

상기 본인 공개 키 및 상기 본인 개인 키는 본인 공개-키 암호 쌍을 형성하고,

상기 에이전트-수정된 개별 레코드는 상기 본인 디바이스로부터 상기 오리지널 개별 레코드를 수신한 후에 상기 에이전트 디바이스에 의해 생성되고,

상기 에이전트-수정된 개별 레코드의 서명은 상기 에이전트 디바이스의 에이전트 개인 키를 사용하여 생성되고,

상기 에이전트 공개 키 및 상기 에이전트 개인 키는 에이전트 공개-키 암호 쌍을 형성하고,

상기 오리지널 개별 레코드는, 상기 에이전트 디바이스로부터 콘텐츠 요청을 수신하고 그리고 상기 에이전트 디바이스를 식별한 후에 상기 레코드 전송자 디바이스에 의해 생성되고,

상기 오리지널 개별 레코드의 서명은 상기 레코드 전송자 디바이스의 전송자 개인 키를 사용하여 생성되며, 그리고

상기 전송자 공개 키 및 상기 전송자 개인 키는 전송자 공개-키 암호 쌍을 형성함 -;

상기 본인-수정된 개별 레코드를 검증하는 단계; 및

상기 본인-수정된 개별 레코드에 의해 명령된 대로 상기 본인 디바이스에 대해 수행하는 단계

를 포함하는, 에이전트들에 의해 암호화방식으로 싸인된 레코드들을 안전하게 교환하기 위한 방법.

청구항 2

에이전트들에 의해 암호화방식으로 싸인된 레코드들을 안전하게 교환하기 위한 방법으로서,

하드웨어 프로세서의 제어 하에:

에이전트 디바이스로부터 콘텐츠 요청을 수신하는 단계;

상기 에이전트 디바이스를 식별하는 단계;

오리지널 개별 레코드를 생성하는 단계 - 상기 오리지널 개별 레코드는 레코드 콘텐츠, 레코드 전송자 디바이스의 전송자 공개 키, 본인 디바이스의 본인 공개 키, 및 상기 오리지널 개별 레코드의 서명을 포함하고, 상기 오리지널 개별 레코드의 서명은 상기 레코드 전송자 디바이스의 전송자 개인 키를 사용하여 생성되고, 상기 전송자 공개 키 및 상기 전송자 개인 키는 전송자 공개-키 암호 쌍을 형성함 -;

상기 에이전트 디바이스에 상기 오리지널 개별 레코드를 전송하는 단계;

상기 에이전트 디바이스의 표시를 수신하는 단계: 상기 오리지널 개별 레코드를 수신하는 단계;

상기 전송자 공개 키를 사용하여 상기 오리지널 개별 레코드를 검증하는 단계;

에이전트-수정된 개별 레코드를 생성하는 단계 - 상기 에이전트-수정된 개별 레코드는 상기 오리지널 개별 레코드, 상기 에이전트 디바이스의 에이전트 공개 키, 및 상기 에이전트-수정된 개별 레코드의 서명을 포함하고, 상기 에이전트-수정된 개별 레코드의 서명은 상기 에이전트 디바이스의 에이전트 개인 키를 사용하여 생성되며, 그리고 상기 에이전트 공개 키 및 상기 에이전트 개인 키는 에이전트 공개-키 암호 쌍을 형성함 -;

상기 본인 디바이스에 상기 에이전트-수정된 개별 레코드를 전송하는 단계; 및 본인 디바이스의 표시를 수신하는 단계:

상기 에이전트-수정된 개별 레코드를 수신하는 단계; 본인-수정된 개별 레코드를 생성하는 단계 -본인-수정된 개별 레코드는 상기 본인-수정된 개별 레코드의 서명 및 상기 에이전트-수정된 개별 레코드를 포함하고, 상기 본인-수정된 개별 레코드의 서명은 상기 본인 디바이스의 본인 개인 키를 사용하여 생성되며, 그리고 상기 본인 공개 키 및 상기 본인 개인 키는 본인 공개-키 암호 쌍을 형성함-;

상기 본인-수정된 개별 레코드를 프로세싱 플랫폼에 상환하는 단계;

상기 본인-수정된 개별 레코드에 의해 명령된 대로 상기 프로세싱 플랫폼에 의한 퍼포먼스를 수신하는 단계; 및

상기 에이전트 디바이스에 상기 퍼포먼스의 수신을 통지하는 단계

를 포함하는, 에이전트들에 의해 암호화방식으로 싸인된 레코드들을 안전하게 교환하기 위한 방법.

청구항 3

에이전트들에 의해 암호화방식으로 싸인된 레코드들을 안전하게 교환하기 위한 방법으로서,

하드웨어 프로세서의 제어 하에:

레코드 전송자 디바이스에 콘텐츠 요청을 전송하는 단계;

상기 레코드 전송자 디바이스로부터 오리지널 개별 레코드를 수신하는 단계 - 상기 오리지널 개별 레코드는, 상기 레코드 전송자 디바이스로부터 상기 콘텐츠 요청을 수신하고 에이전트 디바이스를 식별한 후에 상기 레코드 전송자 디바이스에 의해 생성되고,

상기 오리지널 개별 레코드는 레코드 콘텐츠, 레코드 전송자 디바이스의 전송자 공개 키, 본인 디바이스의 본인 공개 키, 및 상기 오리지널 개별 레코드의 서명을 포함하고,

상기 오리지널 개별 레코드의 서명은 상기 레코드 전송자 디바이스의 전송자 개인 키를 사용하여 생성되며, 그리고

상기 전송자 공개 키 및 상기 전송자 개인 키는 전송자 공개-키 암호 쌍을 형성함 -;

상기 전송자 공개 키를 사용하여 상기 오리지널 개별 레코드를 검증하는 단계;

에이전트-수정된 개별 레코드를 생성하는 단계 - 상기 에이전트-수정된 개별 레코드는 상기 오리지널 개별 레코드, 상기 에이전트 디바이스의 에이전트 공개 키, 및 상기 에이전트-수정된 개별 레코드의 서명을 포함하고,

상기 에이전트-수정된 개별 레코드의 서명은 상기 에이전트 디바이스의 에이전트 개인 키를 사용하여 생성되며, 그리고

상기 에이전트 공개 키 및 상기 에이전트 개인 키는 에이전트 공개-키 암호 쌍을 형성함 -;

상기 본인 디바이스에 상기 에이전트-수정된 개별 레코드를 전송하는 단계; 및 상기 본인 디바이스의 표시를 수신하는 단계:

상기 에이전트-수정된 개별 레코드를 수신하는 단계; 및

본인-수정된 개별 레코드를 생성하는 단계 - 상기 본인-수정된 개별 레코드는 상기 본인-수정

된 개별 레코드의 서명 및 상기 에이전트-수정된 개별 레코드를 포함하고,

상기 본인-수정된 개별 레코드의 서명은 상기 본인 디바이스의 본인 개인 키를 사용하여 생성되며, 그리고

상기 본인 공개 키 및 상기 본인 개인 키는 본인 공개-키 암호 쌍을 형성함 -;

상기 본인-수정된 개별 레코드를 프로세싱 플랫폼에 상환하는 단계; 및

상기 본인-수정된 개별 레코드에 의해 명령된 대로 상기 프로세싱 플랫폼에 의한 퍼포먼스를 수신하는 단계

를 포함하는, 에이전트들에 의해 암호화방식으로 싸인된 레코드들을 안전하게 교환하기 위한 방법.

청구항 4

컴퓨터 프로그램을 저장한 비-일시적 컴퓨터 스토리지로서,

상기 컴퓨터 프로그램은 제1 항 내지 제3 항 중 어느 한 항의 방법을 적어도 수행하기 위한 컴퓨터 시스템에 명령하기 위한 실행가능한 명령들을 포함하는,

컴퓨터 프로그램을 저장한 비-일시적 컴퓨터 스토리지.

청구항 5

웨어러블 디스플레이 시스템으로서,

디스플레이;

실행가능한 명령들을 저장하는 비-일시적 컴퓨터-판독가능 저장 매체; 및

제1 항 내지 제3 항 중 어느 한 항의 방법을 수행하기 위해 상기 실행가능한 명령들에 의해 프로그래밍되는 하나 또는 그 초과의 하드웨어 프로세서들

을 포함하는,

웨어러블 디스플레이 시스템.

발명의 설명

기 술 분 야

[0001] [0001] 본 출원은 "SECURE EXCHANGE OF CRYPTOGRAPHICALLY SIGNED RECORDS"라는 명칭으로 2016년 7월 29일에 출원된 미국 가출원번호 제62/368408호의 우선권을 주장하며, 그에 의해 이 가출원의 내용은 그 전체가 인용에 의해 본원에 포함된다.

[0002] [0002] 본 개시내용은 일반적으로 암호화 방식(cryptography)을 위한 시스템들 및 방법들에 관한 것으로, 더욱 구체적으로는 컴퓨터 네트워크들을 통해, 암호화방식으로 싸인된 레코드(cryptographically signed record)들을 안전하게 교환하는 것에 관한 것이다.

배 경 기 술

[0003] [0003] 종래의 시스템들, 이를테면 디지털 송신들은 컴퓨터 네트워크를 통해 콘텐츠들 및 레코드들을 교환하는 데 유용하다. 이러한 디지털 송신들은 레코드들의 전통적인 물리적 교환들에 대한 필요성을 대체할 수 있다. 이러한 종래의 시스템들을 활용하는 당사자들은 교환시에 인터넷과 같은 네트워크에 연결될 필요가 있다. 이들 종래의 시스템들은 교환들을 위한 당사자들이 교환들을 인증하기 위한 중앙 데이터 센터들에 계속해서 액세스할 것을 요구한다.

발명의 내용

[0004] [0004] 암호화방식으로 싸인된 레코드들을 안전하게 교환하기 위한 시스템들 및 방법들이 개시된다. 시스템들

및 방법들은 공개 키(public key) 및 개인 키(private key) 암호화 기법들을 활용할 수 있다. 일 양상에서, 콘텐츠 요청을 수신한 후에, 전송자 디바이스는 요청을 하는 제1 수신자 디바이스에 레코드를 전송할 수 있다. 레코드는 비중앙집중형(decentralized)(예컨대, 피어-투-피어) 방식으로 단거리 링크(short range link)를 통해 전송될 수 있는 반면에, 디바이스들은 중앙집중형(centralized) 프로세싱 플랫폼과 통신하지 못할 수 있다. 레코드는 전송자 디바이스의 개인 키를 사용하여 생성된 전송자 서명(sender signature)을 포함할 수 있다. 제1 수신자 디바이스는 전송자 디바이스의 공개 키를 사용하여 전송자 서명의 진본성(authenticity)을 검증할 수 있다. "프로세싱만을 위한 배서(for processing only endorsement)" 및 수신자 서명을 부가한 후에, 제1 수신자 디바이스는 프로세싱 플랫폼에 레코드를 상환(redeem)할 수 있다. 전송자 서명 및 수신자 서명의 성공적 검증시에, 프로세싱 플랫폼은 레코드의 콘텐츠에 의해 명령된 대로 수행할 수 있다.

[0005] [0005] 다른 양상에서, 제1 수신자 디바이스는 제1 수신자 서명을 레코드에 부가한 후에 제2 수신자 디바이스에 레코드를 전송할 수 있다. 제2 수신자 디바이스는 제1 수신자 디바이스 및 전송자 디바이스의 공개 키들을 사용하여 서명의 진본성을 검증할 수 있다. "프로세싱만을 위한 배서" 및 제2 수신자 서명을 부가한 후에, 제2 수신자 디바이스는 프로세싱 플랫폼에 레코드를 상환할 수 있다.

[0006] [0006] 다른 양상에서, 콘텐츠 요청을 수신한 후에, 전송자 디바이스는 본인(principal) 대신에 요청을 하는 에이전트 디바이스에 레코드를 전송할 수 있다. 에이전트 디바이스는 전송자 디바이스의 공개 키를 사용하여 레코드의 전송자 서명의 진본성을 검증할 수 있다. 에이전트 디바이스는 본인이 프로세싱 플랫폼에 레코드를 상환하기 전에 "배서에 의해 핸들링됨(handled by endorsement)"을 레코드에 부가할 수 있다.

[0007] [0007] 일 양상에서, 전송자 디바이스는 레코드를 수신자 디바이스에 전송할 수 있다. 수신자 디바이스는 악의적인 거동(malicious behavior), 이를테면 단일 수신자에 대한 전송자 클로닝(cloning), 마우징(mousing), 고스팅(ghosting), 다수의 수신자들에 대한 전송자 클로닝, 또는 포킹(forking)을 검출함으로써 수신된 레코드의 유효성을 검증(validate)할 수 있다. 악의적인 거동을 검출한 후에, 수신자 디바이스는 배서된 레코드를 프로세싱 플랫폼에 전송하기 전에 악의적인 배서를 레코드에 부가할 수 있다. 프로세싱 플랫폼은 퍼지 규칙(fuzzy ruling) 또는 부울(Boolean) 분석을 수행한 후에 블랙리스트에 전송자 디바이스를 부가할 수 있다. 다른 양상에서, 프로세싱 플랫폼은 악의적인 거동, 이를테면 수신자 클로닝 또는 고스팅을 검출함으로써 디바이스로부터 수신된 레코드의 유효성을 검증할 수 있다.

[0008] [0008] 암호화방식으로 싸인된 레코드들을 안전하게 교환하기 위한 시스템들 및 방법들의 실시예들이 개시된다. 일 양상에서, 콘텐츠 요청을 수신한 후에, 전송자 디바이스는 요청을 하는 수신자 디바이스에 레코드를 전송할 수 있다. 레코드는 비중앙집중형(예컨대, 피어-투-피어) 방식으로 단거리 링크를 통해 전송될 수 있는 반면에, 디바이스들은 중앙집중형 프로세싱 플랫폼과 통신하지 못할 수 있다. 레코드는 전송자 디바이스의 개인 키를 사용하여 생성된 전송자 서명을 포함할 수 있다. 수신자 디바이스는 전송자 디바이스의 공개 키를 사용하여 전송자 서명의 진본성을 검증할 수 있다. "프로세싱만을 위한 배서" 및 수신자 서명을 부가한 후에, 수신자 디바이스는 프로세싱 플랫폼에 레코드를 상환할 수 있다. 전송자 서명 및 수신자 서명의 성공적 검증시에, 프로세싱 플랫폼은 레코드의 콘텐츠에 의해 명령된 대로 수행할 수 있다.

[0009] [0009] 암호화방식으로 싸인된 레코드들을 안전하게 교환하기 위한 시스템들 및 방법들의 실시예들이 개시된다. 일 양상에서, 콘텐츠 요청을 수신한 후에, 전송자 디바이스는 본인 대신에 요청을 하는 에이전트 디바이스에 레코드를 전송할 수 있다. 레코드는 비중앙집중형 (예컨대, 피어-투-피어) 방식으로 단거리 링크를 통해 전송될 수 있는 반면에, 디바이스들은 중앙집중형 프로세싱 플랫폼과 통신하지 못할 수 있다. 레코드는 전송자 디바이스의 개인 키를 사용하여 생성된 전송자 서명을 포함할 수 있다. 에이전트 디바이스는 전송자 디바이스의 공개 키를 사용하여 전송자 서명의 진본성을 검증할 수 있다. 에이전트 디바이스는 본인이 프로세싱 플랫폼에 레코드를 상환하기 전에 "배서에 의해 핸들링됨"을 레코드에 부가할 수 있다. 전송자 서명 및 수신자 서명의 성공적 검증시에, 프로세싱 플랫폼은 레코드의 콘텐츠에 의해 명령된 대로 수행할 수 있다.

[0010] [0010] 다수의 수신자들을 수반하는, 암호화방식으로 싸인된 레코드들의 체인들을 안전하게 교환하기 위한 시스템들 및 방법들의 실시예들이 개시된다. 일 양상에서, 전송자 디바이스는 제1 수신자 디바이스에 레코드를 전송할 수 있다. 레코드는 전송자 디바이스의 개인 키를 사용하여 생성된 전송자 서명을 포함할 수 있다. 제1 수신자 디바이스는 전송자 디바이스의 공개 키를 사용하여 서명의 진본성을 검증할 수 있다. 제1 수신자 디바이스는 제1 수신자 서명을 레코드에 부가한 후에 제2 수신자 디바이스에 레코드를 전송할 수 있다. 제2 수신자 디바이스는 전송자 디바이스 및 제1 수신자 디바이스의 공개 키들을 사용하여 서명들의 진본성을 검증할 수 있다. "프로세싱만을 위한 배서" 및 제2 수신자 서명을 부가한 후에, 제2 수신자 디바이스는 프로세싱 플랫폼에

레코드를 상환할 수 있다. 서명들의 성공적 검증시에, 프로세싱 플랫폼은 레코드의 콘텐츠에 의해 명령된 대로 수행할 수 있다.

[0011] [0011] 암호화방식으로 싸인된 레코드들의 유효성을 검증하기 위한 시스템들 및 방법들의 실시예들이 개시된다. 일 양상에서, 전송자 디바이스는 레코드를 수신자 디바이스에 전송할 수 있다. 수신자 디바이스는 악의적인 거동, 이를테면 단일 수신자에 대한 전송자 클로닝, 마우징, 고스팅, 다수의 수신자들에 대한 전송자 클로닝, 또는 포킹을 검출함으로써 수신된 레코드의 유효성을 검증할 수 있다. 악의적인 거동을 검출한 후에, 수신자 디바이스는 배서된 레코드를 프로세싱 플랫폼에 전송하기 전에 악의적인 배서를 레코드에 부가할 수 있다. 프로세싱 플랫폼은 퍼지 규칙 또는 부울 분석을 수행한 후에 블랙리스트에 전송자 디바이스를 부가할 수 있다. 다른 양상에서, 프로세싱 플랫폼은 악의적인 거동, 이를테면 수신자 클로닝 또는 고스팅을 검출함으로써 디바이스로부터 수신된 레코드의 유효성을 검증할 수 있다.

[0012] [0012] 본 명세서에 설명된 청구대상의 하나 이상의 구현들의 세부사항들은 이하의 상세한 설명 및 첨부 도면들에 기재되어 있다. 다른 특징들, 양상들 및 장점들은 상세한 설명, 도면들 및 청구항들로부터 자명해질 것이다. 이러한 요약도 이하의 상세한 설명도 본 발명의 청구대상의 범위를 한정하거나 제한하는 것으로 의도하지 않는다.

도면의 간단한 설명

[0013] [0013] 도 1a 및 도 1b는 무선 네트워크를 통해, 암호화방식으로 싸인된 콘텐츠들 및 레코드들을 안전하게 교환하기 위한 일 실시예를 개략적으로 예시한다.

[0014] [0014] 도 2는 공개 및 개인 암호 키들을 저장하도록 구성된 예시적인 사용자 디바이스의 블록 다이어그램이다.

[0015] [0015] 도 3은 사용자 디바이스들의 공개 암호 키들을 저장하도록 구성된 예시적인 프로세싱 플랫폼의 블록 다이어그램이다.

[0016] [0016] 도 4는 하나의 레코드 수신자에 대해 생성된 개별 레코드를 안전하게 교환 및 상환하기 위한 일 실시예를 예시하는 상호작용 다이어그램이다.

[0017] [0017] 도 5는 하나의 레코드 수신자에 대해 생성된 개별 레코드의 일 예를 개략적으로 예시한다.

[0018] [0018] 도 6은 2개의 레코드 수신자들에 대해 생성된 개별 레코드들을 안전하게 교환 및 상환하는 일 실시예를 예시하는 상호작용 다이어그램이다.

[0019] [0019] 도 7은 2개의 레코드 수신자들에 대해 생성된 예시적인 개별 레코드들을 개략적으로 예시한다.

[0020] [0020] 도 8은 복수의 레코드 수신자들에 대해 생성된 예시적인 개별 레코드들을 개략적으로 예시한다.

[0021] [0021] 도 9는 에이전트 및 수신자를 수반하는, 개별 레코드들을 안전하게 교환 및 상환하는 일 실시예를 예시하는 상호작용 다이어그램이다.

[0022] [0022] 도 10은 에이전트 및 레코드 수신자를 수반하는 예시적인 개별 레코드들을 개략적으로 예시한다.

[0023] [0023] 도 11은 질의 배서(query endorsement)를 수반하는 개별 레코드들을 안전하게 교환 및 상환하는 일 실시예를 예시하는 상호작용 다이어그램이다.

[0024] [0024] 도 12는 질의 배서를 수반하는 예시적인 개별 레코드들을 개략적으로 예시한다.

[0025] [0025] 도 13은 프로세싱 플랫폼으로부터 공통 레코드들을 분배하는 일 실시예를 예시하는 상호작용 다이어그램이다.

[0026] [0026] 도 14는 분배를 위한 예시적인 공통 레코드들을 개략적으로 예시한다.

[0027] [0027] 도 15는 레코드 수신자 디바이스에 의한 공통 레코드들의 전파의 예를 예시하는 상호작용 다이어그램이다.

[0028] [0028] 도 16은 레코드 전송자 디바이스에 의한 공통 레코드들의 전파의 예를 예시하는 상호작용 다이어그램이다.

[0029] [0029] 도 17은 다수의 수신자들에 대한 전송자 클로닝에 의한 악의적인 거동의 예를 예시하는 상호작용 다이

어그램이다.

[0030] 도 18은 단일 수신자에 대한 전송자 클로닝에 의한 악의적인 거동의 예를 예시하는 상호작용 다이어그램이다.

[0031] 도 19는 포킹에 의한 악의적인 거동의 예를 예시하는 상호작용 다이어그램이다.

[0032] 도 20은 수신자 클로닝에 의한 악의적인 거동의 예를 예시하는 상호작용 다이어그램이다.

[0033] 도 21은 마우징에 의한 악의적인 거동의 예를 예시하는 상호작용 다이어그램이다.

[0034] 도 22는 고스팅에 의한 악의적인 거동의 예를 예시하는 상호작용 다이어그램이다.

[0035] 도 23은 예시적인 사용자 디바이스의 블록 다이어그램이다.

[0036] 도 24는 예시적인 프로세싱 플랫폼의 블록 다이어그램이다.

[0037] 도 25는 표준 거래의 예를 개략적으로 예시한다.

[0038] 도 26은 다수의 판매자들에 대한 구매자 클로닝의 예를 개략적으로 예시한다.

[0039] 도 27은 단일 판매자에 대한 구매자 클로닝의 예를 개략적으로 예시한다.

[0040] 도 28은 수표 포킹(cheque forking)의 예를 개략적으로 예시한다.

[0041] 도 29는 판매자 클로닝의 예를 개략적으로 예시한다.

[0042] 도 30은 마우징의 예를 개략적으로 예시한다.

[0043] 도 31은 고스팅의 예를 개략적으로 예시한다.

[0044] 도 32는 PoS(point of sale) 거래의 예를 개략적으로 예시한다.

[0045] 도 33a-33b는 암호화방식으로 싸인된 디지털 수표들을 안전하게 교환하는 일 실시예를 개략적으로 예시한다. 도 33c는 암호화방식으로 싸인된 디지털 수표들을 안전하게 교환하는 다른 실시예를 개략적으로 예시한다.

[0046] 도 34a는 암호화방식으로 싸인된 디지털 수표들을 안전하게 교환 및 상환하는 일 실시예를 예시하는 상호작용 다이어그램이다. 도 34b는 암호화방식으로 싸인된 디지털 수표들을 안전하게 교환 및 상환하기 위한 다른 실시예를 예시하는 상호작용 다이어그램이다.

[0047] 도 35는 웨어러블 디스플레이 시스템의 예를 개략적으로 예시한다.

[0048] 도면들 전체에 걸쳐, 참조된 엘리먼트들 간의 관련성(correspondence)을 표시하기 위하여 참조 부호들이 재사용될 수 있다. 도면들은 본원에서 설명된 예시적인 실시예들을 예시하기 위하여 제공되며 개시내용의 범위를 제한하는 것으로 의도되지 않는다.

발명을 실시하기 위한 구체적인 내용

[0014] 개요

[0015] [0049] 본원에서 개시된 시스템들 및 방법들은 디지털 송신들 및 물리적 교환들과 관련된 다양한 난제들을 처리한다. 예컨대, 콘텐츠들 및 레코드들은 하이브리드 시스템을 사용하여 네트워크를 통해 안전하게 전달 및 교환될 수 있다. 하이브리드 시스템은 콘텐츠들 또는 레코드들의 의미있는 또는 만족스러운 중앙집중형 및 피어-투-피어 교환들을 제공한다. 다른 장점들은 사용의 용이성, 교환의 스피드, 검증 능력, 보안, 익명성, 비가역성, 및 부인방지를 포함한다. 본원에서 개시된 시스템들 및 방법들은 물리적 교환들을 발생시킬 수 있는 유사한 문제들에 직면할 수 있다. 가상 및 물리적 환경들의 차이점들 때문에, 거래 증서들이 카피될 수 있는 사소한 문제와 같은, 디지털 거래들과 관련된 다양한 난제들이 처리된다. 디지털 플랫폼들 상에서 이용가능한 디지털 툴들 및 기법들에 기반한, 예컨대 디지털 암호화방식, 문서들의 배서를 위한 전통적인 수기 서명들의 훨씬 더 강력한 암호화 아날로그를 사용하는 특징들이 개시된다.

[0016] 암호화방식으로 싸인된 레코드들을 안전하게 교환하는 예

[0017] [0050] 도 1a는 암호화방식으로 싸인된 콘텐츠들 및 레코드들, 예컨대 암호화방식으로 싸인된 개별 레코드

(100)를 안전하게 교환하는 일 실시예를 개략적으로 예시한다. 레코드 전송자 디바이스를 사용하는 레코드 전송자(102a)는 개별 레코드(100)를 생성하여 레코드 수신자(102b)에 전송할 수 있다. 레코드 전송자(102a)는 레코드 수신자(102b)에 콘텐츠들 또는 레코드들을 전달하기를 원하는 사람일 수 있다. 레코드 수신자(102b)는 레코드 전송자(102a)로부터 콘텐츠들 또는 레코드들을 수신하기를 원하는 사람일 수 있다.

[0018] [0051] 이후, 레코드 수신자 디바이스를 사용하는 레코드 수신자(102b)는 수정된 개별 레코드(100m1)를 생성하기 위하여 개별 레코드(100)를 수정할 수 있으며, 여기서 m은 개별 레코드(100)가 수정되었음을 표시하며, 그리고 m1은 개별 레코드(100)의 제1 수정을 표시한다. 레코드 수신자(102b)는 수정된 개별 레코드(100m1)를 서비스 제공자(104)에 상환할 수 있다. 보안 전자 프로세싱 플랫폼을 동작시키는 서비스 제공자(104)가 개별 레코드(100m1)를 성공적으로 프로세싱한 후에, 서비스 제공자(104)는, 예컨대, 수정된 개별 레코드(100m1)에 의해 명령된 대로 문서를 레코드 수신자(102b)에 제공할 수 있다. 레코드 전송자(102a) 및 레코드 수신자(102b)는 분산형 또는 비중앙집중형(예컨대, 피어-투-피어) 방식으로 개별 레코드(100)를 교환할 수 있다.

[0019] [0052] 예시를 위해, 하기의 예들은 전송자(102a)와 수신자(102b) 간의 전자 레코드들의 교환을 설명할 것이다. 전송자(102a) 및 수신자(102b)가 전자 레코드들의 교환을 수행하기 위하여 물리적 전자 디바이스들을 사용한다는 것이 이해되어야 한다. 예컨대, 전송자 및 수신자 전자 디바이스들은 셀룰러 전화, 휴대용 컴퓨팅 디바이스(예컨대, 랩톱, 태블릿, e-리더), 데스크톱 컴퓨팅 디바이스, 증강 현실 디바이스(예컨대, 머리-장착 증강, 가상, 또는 혼합 현실 디스플레이) 등을 포함할 수 있다. 서비스 제공자(104)가 교환된 전자 레코드들을 프로세싱하기 위하여 물리적 전자 디바이스를 사용할 수 있다는 것이 이해되어야 한다. 예컨대, 서비스 제공자 전자 디바이스는 하나 이상의 중앙집중형, 또는 분산형 서버 컴퓨터들을 포함할 수 있다.

[0020] [0053] 예컨대, 자신의 사용자 디바이스를 사용하는 레코드 전송자(102a)는 개별 레코드(100)를 레코드 수신자(102b)에 직접 전송할 수 있거나, 또는 단거리 링크, 예컨대 블루투스 링크를 사용하여 피어-투-피어 방식으로 시스템의 다른 사용자를 통해 직접 전송할 수 있다. 개별 레코드(100)를 전송할 때, 레코드 전송자(102a) 및 레코드 수신자(102b)의 사용자 디바이스들은 온라인 또는 오프라인일 수 있다. 예컨대, 레코드 전송자(102a) 및 레코드 수신자(102b)의 사용자 디바이스들 둘 모두는 온라인일 수 있으며, 인터넷과 같은 네트워크에 연결될 수 있다. 다른 예로서, 레코드 전송자(102a) 및 레코드 수신자(102b)의 사용자 디바이스들 중 하나 또는 둘 모두는 오프라인일 수 있고 네트워크에 연결되지 않을 수 있다. 레코드 수신자(102b)는, 레코드 수신자(102b)의 사용자 디바이스가 서비스 제공자(104)와 통신할 때, 수정된 개별 레코드(100m1)를 서비스 제공자(104)에 상환할 수 있다.

[0021] [0054] 개별 레코드(100)는 레코드 전송자(102a)로부터 레코드 수신자(102b)로 송신될 수 있는 복수의 블록들을 포함하는 디지털 객체일 수 있다. 일부 실시예들에서, 개별 레코드(100)는 블록(105a)을 포함할 수 있다. 블록(105a)은 다수의 구성 부분들을 포함할 수 있다.

[0022] [0055] 교환을 위한 보안을 제공하기 위하여, 암호 기법들이 전자 레코드에서 사용될 수 있다. 예컨대, 거래에 대한 각각의 당사자(전송자(102a) 및 수신자(102b)) 또는 거래에 대한 각각의 디바이스(전송자 디바이스 및 수신자 디바이스)가 공개 키(광범위하게 배포될 수 있음) 및 개인 키(보안이 유지되며 당사자에게만 알려짐) 둘 모두와 연관될 수 있는 공개 키 암호 기법들이 사용될 수 있다. 임의의 전송자는 수신자의 공개 키를 사용하여 수신자에 대한 메시지를 암호화할 수 있으나, 암호화된 메시지는 단지, 수신자의 개인 키를 사용하여 수신자에 의해서만 암호 해독될 수 있다. 메시지의 수신자는, 오직 전송자만이 전송자의 개인 키를 사용하여 응답 메시지를 암호해독할 수 있도록, 전송자의 공개 키를 사용하여 응답 메시지를 암호화함으로써 전송자에게 다시 안전하게 응답할 수 있다. 아래에서 추가로 설명되는 바와 같이, 전송자 및 수신자의 전자 디바이스들은, 개개의 당사자의 개인 키를 안전하게 저장하고 배포된 공개 키들을 사용하여 암호화 및 암호해독을 수행할 수 있는 하드웨어 또는 소프트웨어를 포함할 수 있다. 공개 키 암호 방식은 암호화를 위한 키(예컨대, 수신자의 공개 키)가 암호해독을 위한 키(예컨대, 수신자의 개인 키)와 상이한 비대칭 암호화 방식의 예이다. 다른 실시예들에서는, 다른 비대칭 암호 기법들이 사용될 수 있다.

[0023] [0056] 예컨대, 블록(105a)은 블록(105a)의 "from 필드"의 레코드 전송자 디바이스의 공개 키(106a), "to 필드"의 레코드 수신자 디바이스의 공개 키(106b), 레코드 ID(identifier)(108), 콘텐츠(110) 및 레코드 전송자 서명(112a)을 포함할 수 있다. 레코드 전송자 디바이스의 공개 키(106a)는 개별 레코드(100)의 발신자, 즉 레코드 전송자(102a)를 식별할 수 있다. 레코드 수신자 디바이스의 공개 키(106b)는 개별 레코드(100)의 수신자, 즉 레코드 수신자(102b)를 식별할 수 있다.

[0024] [0057] 레코드 ID(108)는 증가, 예컨대 단조적으로 증가할 수 있어서, 레코드 전송자 디바이스에 의해 생성된

2개의 개별 레코드들(100)은 동일한 레코드 ID(108)를 갖지 못한다. 콘텐츠(110)는 예컨대, 레코드 수신자(102b)가 수정된 개별 레코드(100m1)를 서비스 제공자(104)에 상환할 때 수신할 수 있는 문서를 식별할 수 있다. 서비스 제공자(104)는 저절로 또는 간접적으로 제3 자를 통해 콘텐츠(100)에 의해 명령된 대로 수행할 수 있다.

[0025] [0058] 사용자들은 개별 레코드들의 보안 암호 서명들을 생성함으로써 개별 레코드들(100)을 싸인할 수 있다. 레코드 전송자(102a)는 레코드 전송자 서명(112a)을 생성함으로써 개별 레코드(100)를 싸인하기 위하여 자신의 사용자 디바이스를 사용할 수 있다. 개별 레코드(100)를 싸인하기 위하여, 레코드 전송자 디바이스는 레코드 전송자(102a)의 인증을 요구할 수 있다. 인증의 비-제한적인 예들은 암호구 인증(passphrase authentication), 생체인식 인증, 이를테면 지문 인증 또는 홍채 인증, 또는 생물학적 데이터 인증을 포함한다. 레코드 전송자 서명(112a)은 암호화 방식을 사용하여 생성된 디지털 서명일 수 있다. 예컨대, 레코드 전송자 디바이스는 개별 레코드(100)의 SHA(secure hash algorithm)-2와 같이 해시를 암호화하기 위한 RSA(Rivest-Shamir-Adleman) 암호화와 같은 공개-키 암호화 방식을 사용할 수 있다. 예컨대, 224, 245, 384, 또는 512 비트의 레코드 다이제스트들을 사용하는 SHA-2 해시 함수들 중 임의의 함수가 사용될 수 있다(예컨대, SHA-256). 레코드 전송자 서명(112a)은 레코드 전송자 디바이스 공개-키 암호 쌍의 개인 키를 사용하여 생성될 수 있다. 레코드 전송자 디바이스는 개인 키를 안전하게 저장할 수 있다. 레코드 전송자 서명(112a)은 전송자(102a), 예컨대 레코드 전송자 디바이스의 공개 키(106a)를 소유하는 레코드 수신자(102b)에 의해 진정으로 싸인된 다른 것들에 의해 검증될 수 있다. 레코드 수신자(102b)는 개별 레코드(100)로부터 레코드 전송자 디바이스의 공개 키(106a)를 획득할 수 있다. 일단 생성되면, 레코드 전송자 서명(112a)은 블록(105a)을 싸인한다. 레코드 전송자 디바이스의 공개 키(106a), 레코드 수신자 디바이스의 공개 키(106b), 레코드 ID(108), 콘텐츠(110) 및 레코드 전송자 서명(112a)은 개별 레코드(100)의 블록(105a)을 완료할 수 있다.

[0026] [0059] 일단 레코드 수신자(102b)의 소유이면, 레코드 수신자(102b)는, 수정된 개별 레코드(100m1)를 생성하기 위하여 배서 블록(105b)의 배서를 개별 레코드(100)에 부가할 수 있다. 예컨대, 배서는, 수정된 개별 레코드(100m1)가 단지 블록(105a)의 개별 레코드의 수신자, 즉 레코드 수신자(102b)에 의해서만 상환될 수 있는 것을 특정하는 "프로세싱만을 위한 배서"(114)일 수 있다. 일단 배서, 예컨대 "프로세싱만을 위한 배서"(114)가 부가되면, 레코드 수신자(102b)는 수정된 개별 레코드(100)를 생성하기 위하여 배서 블록(105b)에 대한 레코드 수신자 서명(112b)을 생성하는 프로세스를 반복할 수 있다. 레코드 수신자 서명(112b)은 수정된 개별 레코드(100m1)의 하나 이상의 부분들에 기반할 수 있다. 예컨대, 레코드 수신자 서명(112b)은 배서 블록(105b)에 기반할 수 있다. 다른 예로서, 레코드 수신자 서명(112b)은 블록(105a), 배서 블록(105b) 또는 이들의 임의의 조합에 기반할 수 있다. 수정된 개별 레코드(100m1)는 서비스 제공자(104)에 또는 다른 당사자의 전자 디바이스에 전자적으로 통신될 수 있다.

[0027] [0060] 그에 따라서, 개별 레코드는 블록들의 체인을 포함하고, 각각의 블록은 자신의 발신자를 식별한다. 각각의 블록에서, 체인의 전체 이전 부분은 당시에 블록들을 핸들링하는 사용자에 의해 싸인될 수 있다. 사용자는 체인의 전체 이전 부분을 싸인하기 위해 자신의 사용자 디바이스와 연관된 개인 키를 사용할 수 있다. 예컨대, 수정된 개별 레코드(100m1)는 2개의 블록들(105a 및 105b)을 포함하는 체인일 수 있다. 개별 레코드(100)의 블록(105a)은, 레코드 전송자 디바이스의 공개 키(106a)와 함께 레코드 전송자(102a)를 식별할 수 있는 레코드 전송자 디바이스의 공개 키(106a)를 포함할 수 있다. 레코드 전송자 서명(112a)은 레코드 전송자 디바이스 공개-키 암호 쌍의 개인 키를 사용하여 레코드 전송자 디바이스에 의해 싸인될 수 있다. 배서 블록(105b)은, 레코드 수신자 디바이스의 공개 키(106b)와 함께, 레코드 수신자 디바이스를 식별할 수 있는 레코드 수신자 서명(112b)을 포함할 수 있다. 레코드 수신자 서명(112b)은 레코드 수신자 디바이스 공개-키 암호 쌍의 개인 키를 사용하여 레코드 수신자 디바이스에 의해 싸인될 수 있다. 레코드 수신자 서명(112b)은 배서 블록(105b)에 기반할 수 있거나, 또는 배서 블록(105b), 배서 블록(105b) 이전의 하나 이상의 블록들, 예컨대, 블록(105a) 또는 이들의 임의의 조합에 기반할 수 있다.

[0028] [0061] 개별 레코드, 예컨대, 수정된 개별 레코드(100m1)는 "FPOE(for processing only endorsement)"(114)를 포함하는 자신의 마지막 블록과 함께 서비스 제공자(104)에게 전자적으로 통신되고 그에 상환될 수 있다. 상환 시에, 서비스 제공자(104)는, 블록들(105a 및 105b)의 체인 내의 하나 이상의 서명들의 진본성을 검증함으로써, 수정된 개별 레코드(100m1)를 프로세싱할 수 있다. 예컨대, 서비스 제공자(104)는 레코드 전송자 서명(112a) 및 레코드 수신자 서명(112b)을 포함하는, 수정된 개별 레코드(100m1) 내의 모든 서명들의 진본성을 검증할 수 있다. 서명의 진본성은 특정 개인 키를 사용하여 생성되고 있는 서명을 참조할 수 있다. 예컨대, 레코드 전송자 서명(112a) 진본이기 위해, 레코드 전송자 서명(112a)은 레코드 전송자 디바이스의 공개 키를 사용하여 검증

되고, 레코드 전송자 디바이스의 개인 키를 사용하여 생성된 것으로 결정될 수 있다. 따라서, 레코드 전송자 디바이스에 의해 디지털방식으로 싸인된 개별 레코드(100)는, 레코드 전송자(102a)가 자신의 개인 키가 개인으로 유지되었다고 주장하는 한 레코드 전송자(102a)에 의해 복제될 수 없다.

[0029] [0062] 레코드 수신자(102b)가, 예컨대, 특정 ID를 갖는 문서에 대한 액세스를 부여받아야 한다는 명령을 콘텐츠(110)가 포함하고, 체인의 모든 서명들이 진본인 것으로 검증되면, 문서는 수정된 개별 레코드(100m1)의 체인의 마지막 포인트에서 레코드 수신자(102b) 또는 레코드 수신자(102b)의 사용자 디바이스에 부여될 수 있다. 예컨대, 수정된 오리지널 레코드(100m1)의 레코드 전송자 서명(112a) 및 레코드 수신자 서명(112b)이 진본인 것으로 검증되면, 서비스 제공자(104)는 예컨대 콘텐츠(110)에 의해 명령된 바와 같은 문서를 레코드 수신자(102b)에게 제공할 수 있다. 레코드 수신자(102b)가 서비스 제공자(104)에게 연결되게 되고 수정된 개별 레코드(100m1)를 상환하는 시간은, 상환 이벤트를 구성한다.

[0030] [0063] 레코드(100)의 콘텐츠(110)는 예컨대, 메시지, 데이터, 문서 또는 다른 정보를 엔티티에 제공하라는 명령들, 컴퓨터 프로그램을 실행하라는 명령들, 계약상의 의무들 또는 권리들(예컨대, 스마트 계약), 보수(consideration)(예컨대, 통화, 암호화폐, 유가 증권, 실제 또는 무형의 자산들 등)을 송금하라는 명령들 등을 포함할 수 있다. 특정 실시예들의 장점은, 베어러 문서들이 아닌 개별 레코드들을 활용함으로써, 당사자들 둘 모두가 중앙 보관소에 나타나지 않고도 많은 금액의 보수가 교환될 수 있다는 점이다.

[0031] [0064] 하나의 비-제한적인 예에서, 전송자(102a)는 수신자(102b)인 판매자로부터의 자산의 구매자이다. 콘텐츠(110)는 서비스 제공자(104)가 상당한 금액의 암호화폐를 전송자(102a)의 계정으로부터 수신자(102b)의 계정으로 송금하라는 명령들을 포함한다. 전송자의 디바이스는 전송자 디바이스의 개인 키를 사용하여 레코드(100)를 디지털방식으로 싸인하고 레코드(100)를 수신자의 디바이스에 전자적으로 통신한다. 수신자 디바이스는 배서(114)(예컨대, 이런 맥락에서, 배서는 "예금만을 위한 배서"일 수 있음)로 레코드를 배서하고 수정된 레코드(100m1)를 생성하기 위해 수신자 디바이스의 개인 키를 사용하여 레코드를 디지털방식으로 싸인한다. 수신자 디바이스는 수정된 레코드(100m1)를 서비스 제공자(104)에게 통신하고, 서비스 제공자(104)는 수정된 레코드(100m1)를 상환한다. 서비스 제공자(104)는 수정된 레코드(100m1)가 전송자(102a) 및 수신자(102b) 둘 모두에 의해 진정으로 싸인된 것을 (이들 개개의 공개 키들을 사용하여) 검증할 수 있고, (콘텐츠(110) 내의) 상당한 금액의 암호화폐를 전송자의 계정으로부터 수신자의 계정으로 송금할 수 있다.

[0032] [0065] 그에 따라서, 이런 비-제한적인 예에서, 레코드는 디지털 수표 시스템에서 수표로서 기능하고, 자산에 대해 판매자(수신자(102b))에게 지불하기 위해 구매자(전송자(102a))에 의해 사용될 수 있다. 일부 이러한 경우들에서, 자산은 전자 자산(예컨대, 구매자를 위해 원하는 기능을 제공하는 컴퓨터 코드)이다. 판매자(수신자(102b))는 콘텐츠로서 전자 자산을 갖는 (레코드(100)와 유사한) 레코드를 생성하고 디지털방식으로 싸인할 수 있고 레코드를 구매자(전송자(102a))에게 전자적으로 통신할 수 있다. 따라서, 구매자 및 판매자는 보수(예컨대, 상당한 금액의 암호화폐)에 대한 리턴으로 판매자로부터 구매자에게 자산을 송금하기 위해 암호화방식으로 보안 레코드들을 상호 교환할 수 있다. 서비스 제공자(104)는 (예컨대, 구매자의 암호화폐 계정을 데빗팅(debit)하고 판매자의 암호화폐 계정을 크레딧팅(credit)하기 위해) 이런 교환의 적어도 일부에 대해 어음 교환소(clearinghouse)로서의 역할을 할 수 있다.

[0033] 암호화방식으로 싸인된 개별 레코드들을 교환하기 위한 예시적인 시스템

[0034] *예시적인 사용자 디바이스들*

[0035] [0066] 본 개시내용의 콘텐츠들 및 레코드들을 안전하게 교환하기 위한 방법들 및 시스템들은 하나 이상의 사용자 디바이스들 및 하나 이상의 프로세싱 플랫폼들에 의해 구현될 수 있다. 도 1b에 도시된 비-제한적인 예시적 시스템에서, 사용자들은 개별 레코드들(100)을 생성, 전송, 수신, 수정 또는 상환하도록 사용자 디바이스들을 동작시킬 수 있다. 예컨대, 레코드 전송자(102a)는 레코드 전송자 디바이스(116a)를 동작시킬 수 있고, 레코드 수신자(102b)는 레코드 수신자 디바이스(116b)를 동작시킬 수 있다.

[0036] [0067] 사용자 디바이스들, 예컨대, 레코드 전송자 디바이스(116a) 및 레코드 수신자 디바이스(116b)는 동일할 수 있거나 상이할 수 있다. 사용자 디바이스들은 셀룰러 전화들, 태블릿 컴퓨터들, e-리더들, 스마트 시계들, 머리 장착 증강, 가상 또는 혼합 현실 디스플레이 시스템들, 웨어러블 디스플레이 시스템들 또는 컴퓨터들을 포함할 수 있다. 사용자 디바이스들(116a, 116b)은 도 35를 참조하여 아래에서 설명되는 웨어러블 디스플레이 시스템(3500)의 실시예들을 포함할 수 있다. 사용자 디바이스(116a 또는 116b)는 통신 링크(120a, 120b), 예컨대 셀룰러 통신 링크를 사용하여 네트워크(118) 상의 다른 디바이스들과 통신할 수 있다. 네트워크(118)는

예컨대, IEEE(Institute of Electrical and Electronics Engineers) 802.11 표준들을 구현하는 유선 또는 무선 통신 링크들에 의해 액세스가능한 LAN(local area network), WAN(wide area network) 또는 인터넷일 수 있다.

[0037] [0068] 개별 레코드(100)를 전송할 때, 레코드 전송자 디바이스(116a) 및 레코드 수신자 디바이스(116b) 중 하나 또는 둘 모두는 오프라인이고 네트워크(118)에 연결되지 않을 수 있다. 레코드 전송자 디바이스(116a)를 사용하는 레코드 전송자(102a)는 SRL(short range link)(122)을 사용하여 레코드 수신자(102b)에 개별 레코드(100)를 전송할 수 있다. SRL(short range link)(122)은, 사용자 디바이스(116a 또는 116b)가 서로 통신할 수 있게 하는 피어-투-피어 라디오 또는 다른 링크들일 수 있다. SRL(short range link)(122)은 IrDA(Infrared Data Association)/IrPHY(Infrared Physical Layer Specification), Bluetooth®, NFC(Near Field Communication), 애드 혹 802.11 또는 임의의 다른 유선 또는 무선 통신 방법들 또는 시스템들에 기반할 수 있다.

[0038] [0069] 서비스 제공자(104)에 의해 동작되는 프로세싱 플랫폼(124)은 통신 링크(126)를 사용하여 네트워크(118) 상의 다른 디바이스들, 예컨대 사용자 디바이스들(116a 및 116b)과 통신할 수 있다. 통신 링크(120a, 120b, 또는 126)는 유선 또는 무선 통신들, 셀룰러 통신, Bluetooth®, LAN(local area network), WLAN(wide local area network), RF(radio frequency), IR(infrared) 또는 임의의 다른 통신 방법들 또는 시스템들일 수 있다. 사용자들(102a 또는 102b)은 프로세싱 플랫폼(124)에 개별 레코드들을 상환할 수 있다. 예컨대, 레코드 수신자 디바이스(116b)를 사용하는 레코드 수신자(102b)는 수정된 개별 레코드(100m1)를 프로세싱 플랫폼(124)에 상환할 수 있다.

[0039] [0070] 도 2는 공개 및 개인 암호 키들을 저장하도록 구성된 예시적인 사용자 디바이스(116)의 블록도이다. 사용자 디바이스(116)는 개별 레코드 컨테이너(202), SE(secure element)(204) 및 공통 레코드들(206)을 포함할 수 있다. 개별 레코드 컨테이너(202)는 미상환 개별 레코드들(208)을 포함하도록 구성된 디지털 데이터 구조일 수 있다. 예컨대, 레코드 수신자 디바이스(116b)의 개별 레코드 컨테이너(202b)는, 수정된 개별 레코드(100m1)가 프로세싱 플랫폼(124)에 전자적으로 통신되고 그에 상환되기 전에, 수정된 개별 레코드(100m1)를 포함할 수 있다.

[0040] [0071] SE(secure element)(204)는 사용자 디바이스의 개인 키(210) 및 서비스 제공자 공개 키(212)를 안전하게 저장할 수 있다. SE(secure element)(204)는 개별 레코드들(100) 및 수정된 개별 레코드들(100m1)을 싸인하기 위해 사용자 디바이스의 개인 키(212)를 사용할 수 있다. 예컨대, 레코드 전송자 디바이스(116a)의 SE(secure element)(204a)는 개별 레코드(100)의 레코드 전송자 서명(112a)을 생성할 수 있다. 다른 예로서, 레코드 수신자 디바이스(116b)의 SE(secure element)(204b)는 수정된 개별 레코드(100m1)의 레코드 수신자 서명(112b)을 생성할 수 있다. 일부 실시예들에서, 레코드 전송자 디바이스(116a)의 SE(secure element)(204a)는 레코드 전송자 디바이스의 공개 키(106a), 레코드 수신자 디바이스의 공개 키(106b), 레코드 ID(108) 및 콘텐츠(110) 중 하나 이상을 개별 레코드(100)에 부가할 수 있다.

[0041] [0072] SE(secure element)(204)는 서비스 제공자(104)로부터 수신된 정보의 진본성을 검증하기 위해 서비스 제공자 공개 키(212)를 사용할 수 있다. 예컨대, 프로세싱 플랫폼(124)을 사용하는 서비스 제공자(104)는 디바이스들(214)의 업데이트된 공개 키들을 사용자 디바이스(116a 또는 116b)에 전송할 수 있다. 프로세싱 플랫폼(124)은 서비스 제공자 공개-키 암호 쌍의 개인 키로 디바이스들(214)의 공개 키들을 싸인할 수 있다. 일부 실시예들에서, 서비스 제공자 개인 키는 서비스 제공자의 배타적 소유이다. SE(secure element)(204)는 디바이스들(214)의 업데이트된 공개 키의 진본성을 검증할 수 있다. 디바이스들(214)의 업데이트된 공개 키들의 진본성을 검증하는 것은 서비스 제공자 공개 키(212)를 사용하여, 디바이스들(214)의 공개 키들의 서명이 서비스 제공자 공개 키로 생성되었는지 여부를 결정하는 것을 포함할 수 있다. 일부 실시예들에서, 독립적으로 동작하는 둘 이상의 프로세싱 플랫폼들(124)이 존재할 수 있다. 그리고 사용자 디바이스(116)는 둘 이상의 프로세싱 플랫폼들(124)에 대한 하나 이상의 서비스 제공자 공개 키들(212)을 포함할 수 있다.

[0042] [0073] 공통 레코드들(206)은 서비스 제공자 프로세싱 플랫폼(124)의 사용자들에 대한 유효한 사용자 아이덴티티들 및 부가적인 정보를 포함할 수 있다. 공통 레코드들(206)은 프로세싱 플랫폼(124)의 사용자들 사이에 공개적으로 배포되고 공유된다. 예컨대, 공통 레코드들(206)은, 다른 사용자들이 디지털 서명들을 암호화방식으로 검증하도록 시스템에 의해 배포된 사용자 디바이스들(214)의 공개 키들을 포함할 수 있다. 레코드 전송자 디바이스(116a)의 공통 레코드들(206a) 내의 사용자 디바이스들(214a)의 공개 키들 및 레코드 수신자 디바이스(116b)의 공통 레코드들(206b) 내의 사용자 디바이스들(214b)의 공개 키들은 동일할 수 있거나 상이할 수 있다. 도 1b를 참조하면, 레코드 전송자(116a)가 새로운 사용자 디바이스(116a2)를 사용하기 위해, 프로세싱 플랫폼

(104)은 사용자 디바이스(116')의 공개 키의 시스템에 다른 사용자 디바이스들(116)을 통지해야 할 수 있다. 프로세싱 플랫폼(124)은 사용자 디바이스(116')의 공개 키를 포함하는 디바이스들(214)의 업데이트된 공개 키들을 포함하는 업데이트된 공통 레코드(206)를, 다른 사용자 디바이스들(116)이 네트워크(118)에 연결될 때 다른 사용자 디바이스들(116)에 전송할 수 있다. 사용자 디바이스(116a)가 네트워크(118)에 연결되고 사용자 디바이스(116b)가 연결되지 않으면, 사용자 디바이스(116a)는 디바이스들(214a)의 업데이트된 공개 키들을 수신할 수 있다. 따라서, 사용자 디바이스(116b)의 공통 레코드들(206b) 내의 디바이스들(214b)의 공개 키들은 사용자 디바이스(116a)의 공통 레코드들(206a) 내의 디바이스들(214a)의 업데이트된 공개 키들의 서브세트일 수 있다.

[0043] [0074] 일부 실시예들에서, 일부 공개 키들은 더 이상 사용되지 않을 수 있고 프로세싱 플랫폼(124)에 의해 디바이스들(214)의 공개 키들로부터 제거될 수 있다. 예컨대, 레코드 전송자(102a)가 더 이상 레코드 전송자 디바이스(116a)를 사용하고 있지 않으면, 프로세싱 플랫폼(124)은 레코드 전송자 디바이스의 공개 키(106a)를 프로세싱 플랫폼의 레코드로부터 제거할 수 있다. 프로세싱 플랫폼(124)은 레코드 전송자 디바이스의 공개 키(106a)를 배제하는 디바이스들(214)의 업데이트된 공개 키들을 다른 사용자 디바이스들(116)에 전송할 수 있다. 암호 보안을 유지하기 위해, 레코드 전송자 디바이스(116a)가 더 이상 사용되고 있지 않으면, 디바이스 개인 키(210)가 영구적으로 삭제되거나 디바이스가 파괴되어야 한다.

[0044] [0075] 사용자 디바이스들은 사용자 디바이스들(214)의 공개 키들을 사용하여, 수신된 개별 레코드들의 진본성을 검증할 수 있다. 예컨대, 레코드 수신자 디바이스(116b)의 공통 레코드들(206b) 내의 사용자 디바이스들(214b)의 공개 키들은 레코드 전송자 디바이스의 공개 키(106a)를 포함할 수 있다. 그리고 레코드 수신자 디바이스(116b)는 레코드 전송자 디바이스의 공개 키(106a)를 사용하여, 개별 레코드(112a)의 레코드 서명(112a)이 레코드 전송자 디바이스(116a)의 개인 키를 사용하여 생성되었는지 여부를 결정함으로써 개별 레코드(100)의 진본성을 검증할 수 있다.

[0045] *예시적인 프로세싱 플랫폼*

[0046] [0076] 도 3은 사용자 디바이스의 공개 암호 키들을 저장하도록 구성된 예시적인 프로세싱 플랫폼(124)의 블록도이다. 프로세싱 플랫폼(124)은 시스템에 대한 인프라구조일 수 있는 서버 또는 서버들의 콜렉션을 포함할 수 있다. 프로세싱 플랫폼(124)은 네트워크(118)에 직접 연결될 수 있고, 간접적으로 및 가능하게는 오직 간헐적으로 네트워크(118)를 통해 사용자 디바이스들(116)에 연결될 수 있다. 프로세싱 플랫폼(124)은 사용자들, 사용자 디바이스들(116), 및 레코드들에서 식별된 콘텐츠들에 대한 액세스를 계속해서 추적하기 위해 중앙 레코드들(302)을 포함하고 유지할 수 있다. 프로세싱 플랫폼(124)은 레코드들(100)의 콘텐츠들(110)에 포함된 명령들을 프로세싱할 수 있다. 예컨대, 위에서 설명된 바와 같이, 레코드(100)의 콘텐츠(110)가 사용자들의 계정들 사이에서 암호화폐를 송금하라는 명령을 포함하면, 플랫폼(124)은 레코드의 상환 시에 송금을 수행할 수 있다.

[0047] [0077] 프로세싱 플랫폼(124)은 공통 레코드들(206)을 유지할 수 있거나 또는 중앙 레코드들(302)로부터 공통 레코드들(206)을 생성할 수 있다. 중앙 레코드들(302)은 디바이스들(214)의 공개 키들을 포함할 수 있다. 사용자 디바이스(116)의 공통 레코드들(206) 내의 디바이스들(214)의 공개 키들은 중앙 레코드들(302) 내의 사용자 디바이스들(214)의 공개 키들의 서브세트일 수 있다. 예컨대, 사용자 디바이스들(214)의 공개 키들은 업데이트되었을 수 있고, 사용자 디바이스(116)는 사용자 디바이스들(214)의 업데이트된 공개 키들을 수신하지 않았을 수 있다.

[0048] [0078] 중앙 레코드들(302)은 사용자들(102a 또는 102b) 또는 사용자 디바이스들(116a 또는 116b)의 식별 정보 및 보조적인 정보를 포함할 수 있다. 중앙 레코드들(302)은 사용자 디바이스들과 사용자들의 연관성을 식별할 수 있는 사용자 정보(304)를 포함할 수 있다. 예컨대, 중앙 레코드들(302)은 2개의 레코드 전송자 디바이스들(116a 및 116a')과 레코드 전송자(102a)의 연관성을 포함할 수 있다. 일부 실시예들에서, 다수의 디바이스들을 갖는 하나의 사용자는 다수의 사용자들로 고려될 수 있다. 일부 실시예들에서, 다수의 디바이스들을 갖는 하나의 사용자는 하나의 사용자로 고려될 수 있다. 공통 레코드들(206)은 사용자 정보(304)를 포함하지 않을 수 있다.

[0049] [0079] 중앙 레코드들(302)은 사용자들의 정보를 추적하기 위해 사용자 레코드 상황(user record status)(306)을 포함할 수 있다. 예컨대, 개별 레코드(100)의 콘텐츠(110)는 콘텐츠(110)에 저장된 자신의 문서 ID를 갖는 문서에 대한 액세스를 레코드 수신자(102b)에게 제공하도록 프로세싱 플랫폼(124)에 명령할 수 있다. 그러나, 사용자 레코드 상황(306)은, 오직 레코드 전송자(102a) 자신만이 문서에 대한 액세스를 갖고; 레코드 전송자(102a)는 문서에 대한 액세스를 다른 사용자들에게 그랜트할 수 없음을 표시할 수 있다. 다른 예로서, 사용자 레코드 상황(306)은 레코드 전송자(102a)가 문서의 액세스를 다른 사용자들에게 부여할 수 있음을 표시할 수

있다. 또 다른 예로서, 사용자 레코드 상황(306)은 레코드 전송자(102a)가 문서의 액세스를 오직 사용자들에게만 여러번, 이를테면 한번 부여할 수 있음을 표시할 수 있고; 사용자 레코드 상황(306)은 개별 레코드(100)가 임의의 사용자, 예컨대 레코드 수신자(102b)에 의해 상환 및 액세스되었는지 여부를 계속해서 추적할 수 있다.

[0050] [0080] 비-제한적인 예로서, 사용자 레코드 상황(306)은 예컨대, 암호화폐에서 레코드 전송자의 계정 잔액(account balance)을 계속해서 추적할 수 있다. 레코드 전송자의 계정은 지불인 계정일 수 있다. 레코드 수신자(102b)에게 레코드 전송자의 계정 잔액보다 적거나 그와 동일한 금액을 지불하도록 개별 레코드(100)의 콘텐츠(110)가 프로세싱 플랫폼(124)에 명령하면, 프로세싱 플랫폼(124)은 특정 금액만큼 레코드 전송자의 계정을 데빗팅하고 동일한 금액만큼 레코드 수신자의 계정을 크레딧팅할 수 있다. 레코드 수신자의 계정은 수취인 계정일 수 있다. 레코드 수신자(102b)에게 레코드 전송자의 계정 잔액보다 많은 금액을 지불하도록 개별 레코드(100)의 콘텐츠(110)가 프로세싱 플랫폼(124)에 명령하면, 프로세싱 플랫폼(124)은 특정 금액만큼 레코드 수신자의 계정을 크레딧팅하는 것을 거부할 수 있다. 그러나, 레코드 전송자의 계정은 당좌대월(overdraft) 청구에 의해 데빗팅될 수 있다. 공통 레코드들(206)은 사용자 레코드 상황(306)을 포함하지 않을 수 있다.

[0051] [0081] 본원에서 개시된 암호화방식으로 싸인된 개별 레코드들의 교환은 다수의 이익들을 포함할 수 있다. 이익들은 예컨대, 사용의 용이성 또는 교환의 스피드를 포함할 수 있다. 도 1에 예시된 바와 같이, 레코드 전송자 디바이스(116a)는, 어느 당사자도 네트워크(118)를 통해 서비스 제공자(104)와 통신함이 없이 SRL(short range link)(122)을 통해 개별 레코드(100)를 레코드 수신자 디바이스(116b)에 전송할 수 있다. 부가적인 또는 대안적인 이익들은, 예컨대, 디지털 서명들의 검증 또는 인증의 능력을 포함할 수 있다. 도 2에 예시된 바와 같이, 사용자 디바이스들의 공개 키들(214)은 공통 레코드들(206)에서 배포된다. 따라서, 레코드 수신자 디바이스(116b)는 개별 레코드(100)에서 레코드 전송자 서명(112a)의 진본성을 그리고 레코드 전송자 디바이스(116a)가 개별 레코드(100)를 전송한 것을 검증할 수 있다. 다른 이익은 예컨대 암호 보안일 수 있다. 도 1a에 예시된 바와 같이, 레코드 전송자 디바이스(116a)는 레코드 전송자 서명(112a)으로 개별 레코드(100)를 싸인할 수 있고, 레코드 수신자 디바이스(116b)는 수정된 개별 레코드(100m1)를 레코드 수신자 서명(112b)으로 싸인할 수 있다. 레코드 수신자 디바이스(116b)가 아닌 악의적인 사용자 디바이스들은 레코드 수신자 서명(112b)을 위조할 수 없는데, 이는 이들이 레코드 수신자 개인 키를 모르기 때문이다. 악의적인 사용자 디바이스는 수정된 개별 레코드(100m1)를 프로세싱 플랫폼(124)에 상환할 수 없는데, 이는, 개별 레코드(100)가 그의 수신측이 레코드 수신자 디바이스(116b)이고 악의적 사용자 디바이스가 아닌 것으로 나타내기 때문이다. 부가적인 또는 대안적인 이익들은, 예컨대, 익명성(실제 법적 이름들이 사용될 필요가 없고, 단지 공개 키들과 연관된 사용자 식별 정보만이 요구됨) 또는 부인방지(디지털 서명들은 공개 키들을 사용하여 인증될 수 있고, 서명자는 자신의 개인 키가 비공개(private)로 유지됨을 또한 주장하는 동안 서명을 부인할 수 없음)를 포함할 수 있다. 추가의 이익은 예컨대 비가역성일 수 있다. 레코드 전송자 디바이스(116a)가 개별 레코드(100)를 레코드 수신자 디바이스(116b)에 전송하면, 프로세싱 플랫폼(124)은 프로세싱 플랫폼(124)이 개별 레코드(100)의 콘텐츠(110)에 의해 명령된 대로 수행하지 않도록 레코드 전송자 디바이스(116a)에 의한 요청을 부인할 수 있다. 다른 이익은 예컨대, 개별 레코드들(100)이 상이한 콘텐츠들(110)을 포함할 수 있다는 것일 수 있다. 또한, 레코드 전송자(102a)는, 레코드 수신자(102b)에게 정보를 직접 전송함이 없이, 방대한 양의 정보, 예컨대 개별 레코드들(100)의 콘텐츠(110)에 저장된 ID들을 갖는 문서들에 대한 액세스를 레코드 수신자(102b)에게 부여할 수 있다.

[0052] 예시적인 하나의 수신자

[0053] [0082] 일부 실시예들에서, 레코드 수신자는 레코드 전송자로부터 개별 레코드를 수신할 수 있다. 도 4는 하나의 레코드 수신자에 대해 생성된 개별 레코드를 안전하게 교환하고 상환하는 일 실시예를 예시하는 상호작용 다이어그램이다. 레코드 수신자 디바이스(116b)를 사용하는 레코드 수신자(102b)는 콘텐츠 요청(402)을 레코드 전송자 디바이스(116a)에 전송함으로써 레코드 전송자(102a)로부터 개별 레코드(100)를 요청할 수 있다. 레코드 수신자(102b)는 상호작용(404)에서 SRL(short range link)(122)을 사용하여 레코드 전송자(102a)에게 콘텐츠 요청(402)을 전송할 수 있다. 콘텐츠 요청(402)은 콘텐츠, 예컨대, 레코드 수신자 디바이스의 콘텐츠 B(110b) 및 공개 키(106b)를 포함할 수 있다. 콘텐츠 B(110b)는 예컨대, 콘텐츠 B(110b)에 저장된 자신의 문서 ID를 갖는 문서에 대한 요청을 포함할 수 있다. 일부 실시예들에서, 레코드 수신자 디바이스의 공개 키(106b)는 레코드 수신자 디바이스(116b)를 고유하게 식별할 수 있다. 일부 실시예들에서, 레코드 수신자 디바이스의 공개 키(106b)는 레코드 수신자(102b)를 고유하게 식별할 수 있다. 공개 키(106b)는 일부 실시예들에서 SE(secure element)(204b)에 저장될 수 있는 공통 레코드들에 있을 수 있다.

[0054] *예시적인 파트너 식별*

[0055] [0083] 도 4를 참조로, 상호작용(408)에서, 자신의 거래 파트너 식별자를 사용하는 레코드 전송자 디바이스(116a)는 파트너 식별에 의해 레코드 수신자 디바이스(116b)의 아이덴티티를 확인할 수 있다. 콘텐츠 요청(402)은 레코드 전송자 디바이스(116a)에 전자적으로 송신되었을 수 있기 때문에, 레코드 전송자 디바이스(116a)는 콘텐츠 요청(402)을 전송한 사용자 디바이스의 아이덴티티에 대해 확신하지 않을 수 있다. 파트너 식별은 유리할 수 있다. 예컨대, 파트너 식별로, 레코드 전송자 디바이스(116a)는 콘텐츠 요청들(402)을 레코드 수신자 디바이스(116b)로부터 그리고 악의적 사용자들로부터 구별할 수 있다. 다른 예로서, 파트너 식별로, 악의적 사용자는 그에 의도되지 않은 개별 레코드를 수신할 수 없다. 또 다른 예로서, 파트너 식별로, 악의적 사용자는 그에 의도되지 않은 개별 레코드를 수신한 후에도, 개별 레코드를 상환할 수 없다.

[0056] *예시적인 개별 레코드 생성*

[0057] [0084] 도 5는 하나의 레코드 수신자에 대해 생성된 하나의 예시적인 개별 레코드를 개략적으로 예시한다. 도 4-도 5에 예시된 바와 같이, 레코드 전송자 디바이스(116a)의 SE(secure element)(204a)가 레코드 전송자의 인증 정보(512a)를 검증한 후, SE(secure element)(204a)는 상호작용(416)에서 개별 레코드(100)를 싸인할 수 있다. 상호작용(416)에서 개별 레코드(100)를 싸인하기 전에, SE(secure element)(204a)는 레코드 전송자(102a)의 인증 및 디지털방식으로 싸인될 블록, 예컨대 개별 레코드(100)의 블록(105a) 프로비전 둘 모두를 요구할 수 있다. 인증의 비-제한적인 예들은 암호구 인증, 생체인식 인증, 이를테면 지문 인증 또는 홍채 인증, 생물학적 데이터 인증 또는 이들의 임의의 조합을 포함할 수 있다. 생체인식 인증은 예컨대 지문들 또는 눈 이미지들에 기반하여 생체인식 템플릿을 활용할 수 있다. SE(secure element)(204a)는 생체인식 템플릿을 인식하기 위한 생체인식 퍼지 금고를 구현할 수 있다.

[0058] [0085] 개별 레코드(100)는 하나 이상의 블록들을 포함하는 디지털 객체일 수 있다. 개별 레코드(100)는 블록(105a)을 포함할 수 있고, 블록(105a)은 "from 필드" 내의 레코드 전송자 디바이스의 공개 키(106a), "to 필드" 내의 레코드 수신자 디바이스의 공개 키(106b), 레코드 ID(108), 콘텐츠 A(110a) 및 블록(105a)의 레코드 전송자 서명(112a)을 포함할 수 있다. 레코드 전송자 디바이스의 공개 키(106a)는 개별 레코드(100)의 발신자인 레코드 전송자 디바이스(116a)를 식별할 수 있다. 레코드 수신자 디바이스의 공개 키(106b)는 개별 레코드(100)의 오리지널 수신측인 레코드 수신자 디바이스(116b)를 식별할 수 있다. 콘텐츠 A(110a)의 콘텐츠는 변할 수 있다. 콘텐츠 A(110a)와 콘텐츠 B(110b)는 동일하거나 유사하거나 관련되거나 상이할 수 있다. 콘텐츠 A(110a)는 콘텐츠 B(110b)와 동일할 수 있으며, 예컨대 특정 문서일 수 있다. 콘텐츠 A(110a)는 콘텐츠 B(110b)와 유사하거나 관련될 수 있다. 예컨대, 콘텐츠 B(110b)는 문서에 대한 액세스를 요청할 수 있고, 콘텐츠 A(110a)는 문서에 대한 액세스를 그랜트할 수 있다. 다른 예로서, 콘텐츠 B(110b)는 2개의 문서들에 대한 액세스를 요청할 수 있고, 콘텐츠 A(110a)는 2개의 문서들에 대한 액세스만을 그랜트할 수 있다. 위에서 설명된 바와 같이, 암호화폐의 맥락에서, 콘텐츠 A(110a)와 콘텐츠 B(110b)는 동일한 양의 암호화폐일 수 있다. 콘텐츠 A(110a)와 콘텐츠 B(110b)는 유사하거나 관련될 수 있다. 예컨대, 콘텐츠 B(110b)는 세전(pre-tax) 금액일 수 있고 콘텐츠 A(110a)는 세후(after-tax) 금액일 수 있다. 다른 예로서, 콘텐츠 B(110b)는 팁전 금액일 수 있고, 콘텐츠 A(110a)는 팁후 금액일 수 있다.

[0059] [0086] 도 4를 참조하면, 상호작용(420)에서, 레코드 전송자(102a)는 예컨대, SRL(short range link)을 사용하여 피어-투-피어 방식으로 레코드 수신자(102b)에 개별 레코드(100)를 전송할 수 있다. 일단 레코드 수신자(102b)의 소유이면, 레코드 수신자(102b)는 상호작용(424)에서 개별 레코드(100)를 검증할 수 있다. 개별 레코드(100)를 검증하는 것은 레코드 전송자 서명(112a)을 인증하는 것을 포함할 수 있다. 레코드 전송자 서명(112a)을 인증하는 것은 레코드 전송자 디바이스의 공개 키(106a)를 사용하여, 레코드 전송자 서명(112a)이 레코드 전송자 디바이스의 개인 키(210)를 사용하여 생성되었는지 여부를 결정하는 것을 포함할 수 있다. 레코드 전송자 디바이스의 공개 키(106a)는 다수의 방식들로 획득될 수 있다. 예컨대, 레코드 전송자 디바이스의 공개 키(106a)는 개별 레코드(100)로부터 획득될 수 있다. 다른 예로서, 레코드 전송자 디바이스의 공개 키(106a)는 레코드 수신자 디바이스(116b)의 공통 레코드들(206)로부터 획득될 수 있다.

[0060] *예시적인 개별 레코드 상환*

[0061] [0087] 도 4를 참조하면, 개별 레코드(100)를 성공적으로 검증한 후에, 레코드 수신자 디바이스(116b)는 자신의 보안 엘리먼트(204b)를 사용하여, 상호작용(428)에서, 수정된 개별 레코드(100m1)를 생성하고 싸인할 수 있다. 상호작용(428)에서 수정된 개별 레코드(100m1)에 싸인하기 전에, SE(secure element)(204b)는 레코드 수신자의 인증 정보(512b) 및 디지털방식으로 싸인될 블록, 예컨대 수정된 개별 레코드(100m1)의 블록(105b)의 프로비전 둘 모두를 요구할 수 있다. 수정된 개별 레코드(100m1)는 개별 레코드(100)의 블록(105a) 및 배서 블록

(105b)을 포함할 수 있다. 예컨대, 배서는, 레코드 수신자의 공개 키(106b)와 함께, 수정된 개별 레코드(100m1)가 레코드 수신자(102b)에 의해서만 상환될 수 있음을 특정하는 "프로세싱만을 위한 배서"(FPOE)(114)일 수 있다. 위에서 설명된 바와 같이, 암호화폐의 맥락에서, FPOE 배서의 예는, 프로세싱 플랫폼(124)이 레코드 수신자(102b)의 계정에 상당한 금액의 암호화폐를 예치할 것이지만 다른 당사자에 대한 추가 배서를 인식하지 않을 "예금만을 위한 배서"(FDOE)를 포함한다.

[0062] [0088] 수정된 개별 레코드(100m1)에 싸인한 후에, 레코드 수신자(102b)가 예컨대, 네트워크(118)를 통해 프로세싱 플랫폼(124)과 통신할 때, 레코드 수신자(102b)는 상호작용(432)에서 프로세싱 플랫폼(124)에 수정된 개별 레코드(100m1)를 상환할 수 있다. 상환시에, 프로세싱 플랫폼(124)을 동작시키는 서비스 제공자(104)는 수정된 개별 레코드(100m1) 내의 블록들(105a, 105b) 체인 내의 하나 이상의 서명들의, 예컨대 레코드 전송자 서명(112a) 및 레코드 수신자 서명(112b)의 진본성을 검증함으로써, 수정된 개별 레코드(100m1)를 상호작용(436)에서 프로세싱할 수 있다. 성공적 검증 후에, 프로세싱 플랫폼(124)은 수정된 개별 레코드(100m1)의 콘텐츠 A(110a)에 의해 명령된 대로 수행할 수 있다.

[0063] [0089] 전송자 디바이스(116a)는 프로세싱 플랫폼(124)이 수정된 개별 레코드(100m1)의 콘텐츠 A(110a)에 의해 명령된 대로 수행했다는 또는 수행하지 않았다는 표시를 수신할 수 있다. 예컨대, 프로세싱 플랫폼(124)은 프로세싱 플랫폼(124)이 수정된 개별 레코드(100m1)의 콘텐츠 A(110a)에 의해 명령된 대로 수행되었다는 것을 명시하는 이메일을 전송자 디바이스(116a)에 전송할 수 있다. 다른 예로서, 콘텐츠 A(110a)가 저장소에 저장된 문서를 레코드 수신자 디바이스(116b)에 제공하도록 프로세싱 플랫폼(124)에 지시하고 저장소가 일시적으로 또는 영구적으로 이용할 수 없기 때문에, 프로세싱 플랫폼(124)은 프로세싱 플랫폼(124)이 수정된 개별 레코드(100m1)의 콘텐츠 A(110a)에 의해 명령된 대로 수행되지 않았다는 것을 명시하는 전자 메시지를 전송자 디바이스(116a)에 전송할 수 있다. 또 다른 예로서, 프로세싱 플랫폼(124)은 주기적으로, 이를테면 매시간, 매일, 매주, 매달 또는 매년 전송자 디바이스(116a)에 자신의 사용자 레코드 상황(306)을 제공할 수 있다. 프로세싱 플랫폼(124)은 하나 이상의 조건들이 만족될 때, 이를테면 레코드 전송자 디바이스(116)가 더 이상 문서에 대한 다른 사용자 디바이스 액세스를 제공할 수 없을 때, 전송자 디바이스(116a)에 자신의 사용자 레코드 상황(306)을 제공할 수 있다.

[0064] *예시적인 파트너 식별*

[0065] [0090] 파트너 식별은 다양한 방법들에 기반할 수 있다. 파트너 식별을 위한 방법들의 비-제한적인 예들은 콘텐츠 인가(content authorization), 노킹, 물리적 표시, 빔 형성, 이전 어레인지먼트, 피상적인 유효성 검증(cursory validation), 또는 이들의 임의의 조합을 포함한다.

[0066] *예시적인 콘텐츠 인가*

[0067] [0091] 일부 실시예들에서, 파트너 식별은 콘텐츠 인가를 포함할 수 있다. 콘텐츠 인가를 활용하여, 레코드 전송자(102a)는 콘텐츠 요청(402) 내의 공개 키(106b)에 기반하여 개별 레코드를 교환하려는 의도를 레코드 수신자 디바이스(116b)에 발행할 수 있다. 개별 레코드를 교환하려는 의도의 콘텐츠는 변할 수 있다. 예컨대, 개별 레코드를 교환하려는 의도의 콘텐츠는 비어 있을 수 있거나 하나 이상의 제로(0) 값들을 포함할 수 있다. 레코드 수신자 디바이스(116b)가 개별 레코드를 교환하려는 의도를 수신한 후에, 레코드 수신자(102b)는 비-전자 수단에 의해, 자신이 개별 레코드를 교환하려는 의도의 수신측임을 확인할 수 있다. 예컨대, 레코드 수신자(102b)는 자신이 개별 레코드 교환하려는 의도를 수신했음을 레코드 전송자(102a)에게 구두로 알릴 수 있다. 다른 예로서, 레코드 수신자(102b)는 자신이 개별 레코드를 전자적으로 교환하려는 의도를 수신했음을 레코드 전송자(102a)에게 알릴 수 있다. 확인 후에, 레코드 수신자(102b)로부터의 콘텐츠 요청(402)은 유효성이 검증될 수 있고, 레코드 전송자(102a)는 적절한 콘텐츠를 갖는 개별 레코드(100)를 레코드 수신자 디바이스(116b)에 전송할 수 있다.

[0068] *예시적인 노킹*

[0069] [0092] 일부 실시예들에서, 파트너 식별은 노킹을 포함할 수 있다. 레코드 전송자 디바이스(116a) 및 레코드 수신자 디바이스(116b)는 각각 모션 센서들을 포함할 수 있다. 노킹을 활용하여, 레코드 전송자 디바이스(116a) 및 레코드 수신자 디바이스(116b)는 물리적으로 접촉할 수 있다. 이러한 접촉은 레코드 전송자 디바이스(116a) 및 레코드 수신자 디바이스(116b)의 모션 센서들에 의해 측정될 수 있다. 접촉의 그리고 콘텐츠 요청(402)을 전송 및 수신하는 상대적인 타이밍은 변할 수 있다. 예컨대, 레코드 수신자 디바이스(116b)는 접촉 당시에(예컨대, "노크" 당시에) 콘텐츠 요청(402)을 전송할 수 있다. 다른 예로서, 레코드 수신자 디바이스

(116b)는 접촉 직후에(예컨대, 10초, 20초, 30초, 1분, 10분 등의 임계 시간 내에) 콘텐츠 요청(402)을 전송할 수 있다. 임계 시간 내에 콘텐츠 요청이 전송되지 않는다면, 파트너 식별은 디바이스들이 다시 노킹될 것을 요구할 수 있다.

[0070] [0093] 레코드 전송자 디바이스(116a)는 콘텐츠 요청(402)의 수신 및 접촉의 시간 동시성에 기반하여 콘텐츠 요청(402)을 수락할 수 있다. 일부 실시예들에서, 레코드 수신자 디바이스(116b)는 레코드 전송자 디바이스(116a)에 접촉의 서명을 전송할 수 있다. 접촉의 서명은 레코드 수신자 디바이스 공개-키 암호 쌍의 개인 키를 사용하여 생성될 수 있다. 접촉의 서명은 레코드 수신자 디바이스(116b)의 모션 센서에 의해 측정된 접촉 및 측정된 접촉의 타이밍에 기반할 수 있다. 접촉의 서명은 콘텐츠 요청(402)의 부분일 수 있거나 레코드 수신자 디바이스(116b)로부터 레코드 전송자 디바이스(116a)로의 별개의 통신일 수 있다. 접촉은 레코드 전송자 디바이스(116a)에서 동등하고 상반되는 리액션을 야기할 수 있기 때문에, 레코드 전송자 디바이스(116a)는 접촉의 서명을 검증할 수 있다.

[0071] *예시적인 물리적 표시*

[0072] [0094] 일부 실시예들에서, 파트너 식별은 물리적 표시를 포함할 수 있다. 레코드 전송자 디바이스(116a) 및 레코드 수신자 디바이스(116b)는 이미징 센서들(예컨대, 디지털 카메라들)을 포함할 수 있다. 레코드 전송자 디바이스(116a) 및 레코드 수신자 디바이스(116b)는 이들의 이미징 센서들을 사용하여 서로 "보도록" 배향될 수 있다. 레코드 수신자 디바이스(116b)는 자신이 캡처한 레코드 전송자 디바이스(116a)의 이미지를 레코드 전송자 디바이스(116a)에 전송할 수 있다. 이미지는 콘텐츠 요청(402)의 부분일 수 있거나 레코드 수신자 디바이스(116b)로부터 레코드 전송자 디바이스(116a)로의 별개의 통신일 수 있다. 레코드 전송자 디바이스(116a)의 이미지 및 레코드 수신자 디바이스(116b)의 이미지는 서로 반대일 수 있기 때문에, 레코드 전송자 디바이스(116a)는 이미지들의 질적 또는 양적 비교들에 의해 레코드 수신자 디바이스(116b)의 아이덴티티를 확인할 수 있다. 예컨대, 레코드 전송자 디바이스(116a)가 레코드 수신자 디바이스(116b)를 위로 그리고 왼쪽으로 "본다"면, 레코드 수신자 디바이스(116b)는 레코드 수신자 디바이스(116b)에 의해 캡처된 레코드 전송자 디바이스(116a)의 이미지에서 아래로 그리고 오른쪽으로 나타나야 한다.

[0073] [0095] 일부 실시예들에서, 물리적 표시는 레코드 전송자 디바이스(116a) 및 레코드 수신자 디바이스(116b)의 환경들의 동시 관측들에 기반할 수 있다. 레코드 전송자 디바이스(116a) 및 레코드 수신자 디바이스(116b)는 마이크로폰들을 포함할 수 있다. 물리적 표시는 레코드 전송자 디바이스(116a) 및 레코드 수신자 디바이스(116b)의 마이크로폰들에 의한 환경들의 동시 오디오 레코딩에 기반할 수 있다. 레코드 전송자 디바이스(116a)와 레코드 수신자 디바이스(116b) 둘 모두는 마이크로폰들을 사용하여 자신의 환경들을 동시에 "청취"할 수 있다. 레코드 수신자 디바이스(116b)는 자신이 캡처한 자신의 환경들의 오디오 레코딩 및 레코딩 시간을 레코드 전송자 디바이스(116a)에 전송할 수 있다. 오디오 레코딩은 콘텐츠 요청(402)의 부분일 수 있거나 레코드 수신자 디바이스(116b)로부터 레코드 전송자 디바이스(116a)로의 별개의 통신일 수 있다. 레코드 수신자 디바이스(116b)에 의해 전송된 사운드 레코딩은 레코드 전송자 디바이스(116a)가 동시에 "청취"한 것과 동일하거나 유사할 수 있기 때문에, 레코드 전송자 디바이스(116a)는 사운드 레코딩과 자신이 "청취"한 것의 질적 또는 양적 비교들에 의해 레코드 수신자 디바이스(116b)의 아이덴티티를 확인할 수 있다. 다른 예로서, 물리적 표시는 레코드 전송자 디바이스(116a) 및 레코드 수신자 디바이스(116b)에 의한 서로의 동시 오디오 관측들에 기반할 수 있다. 또 다른 예로서, 물리적 표시는 레코드 전송자 디바이스(116a) 및 레코드 수신자 디바이스(116b)에 의한 환경들의 동시 시각적 관측들에 기반할 수 있다.

[0074] *예시적인 빔 형성*

[0075] [0096] 일부 실시예들에서, 파트너 식별은 빔 형성을 포함할 수 있다. 사용자 디바이스(116)는 지향성인(예컨대, 빔-형성 또는 지향성 안테나를 사용하는) SRL(short range link) 인터페이스를 포함할 수 있다. 레코드 전송자 디바이스(116a) 및 레코드 수신자 디바이스(116b)는 서로에게 포인팅된 그들의 SRL(short range link) 인터페이스를 포함할 수 있다. 빔 형성을 활용하여, 레코드 전송자 디바이스(116a)는 레코드 수신자 디바이스(116b)로부터 콘텐츠 요청(402)을 수신할 수 있고, 그리고 예컨대, 악의적인 사용자들로부터 다른 방향들로부터 전송된 다른 콘텐츠 요청은 수신할 수 없다. 빔 형성을 활용하여, 다른 사용자들이 아닌 레코드 전송자 디바이스(116a)만이 레코드 수신자 디바이스(116b)로부터 콘텐츠 요청(402)을 수신할 수 있다.

[0076] *예시적인 이전 어레인지먼트*

[0077] [0097] 일부 실시예들에서, 파트너 식별은 이전 어레인지먼트를 포함할 수 있다. 예컨대, 레코드 전송자 디바

이스(116a)는 레코드 수신자 디바이스(116b)로부터 콘텐츠 요청(402)을 수신하기 이전에 레코드 수신자 디바이스의 공개 키(106b)에 대한 사전 지식을 가질 수 있다. 다른 예로서, 레코드 전송자 디바이스(116a)는 공개 키(106b)를 갖는 레코드 수신자 디바이스가 콘텐츠 요청, 예컨대 콘텐츠 요청(402)을 자신에게 송신할 것이라는 사전 지식을 가질 수 있다. 예컨대, 전송자(102a)는 레코드가 전송될 것이라고 이전에 수신자(102b)에게 말했을 수 있다. 수신자(102b)는 수신자 디바이스(116b) 상의 UI(user interface)를 활용하여, (예컨대, 임계 시간 기간 내에) 레코드가 전송자 디바이스(116a)로부터 오는 것으로 예상된다는 표시를 제공할 수 있다.

[0078] *예시적인 피상적인 유효성 검증*

[0079] [0098] 일부 실시예들에서, 파트너 식별은 피상적인 유효성 검증을 포함할 수 있다. 예컨대, 공통 레코드들(206)은 콘텐츠 요청(402)의 피상적인 유효성 검증을 위해 사용될 수 있는 식별 스트링들, 예컨대 BigBoxStore를 포함할 수 있다. 수신자(102b)가 상인인 예로서, 레코드 수신자(102b)는 공통 레코드들(206) 내의 상인으로서 식별될 수 있다. 식별은 아이덴티티가 프로세싱 플랫폼(124)에 의해 유효성이 검증된 공통 레코드들(206) 내의 표시, 예컨대 비트와 연관될 수 있다. 그러한 유효성이 검증된 아이덴티티는 사용자들 자체에 의해 할당된 또는 제공된 아이덴티티들과 구별될 수 있다.

[0080] 예시적인 콘텐츠들 및 교환들

[0081] [0099] 개별 레코드들(100)의 콘텐츠들(110)은 변할 수 있다. 예컨대, 콘텐츠들(110)은 콘텐츠들(110)에 저장된 자신의 문서 ID들을 갖는 문서들을 레코드 수신자들(102b)에게 제공하기 위한 명령들을 포함할 수 있다. 다른 예로서, 콘텐츠들(110)은 특정 수의 화폐 단위들, 예컨대 미국 달러를 레코드 수신자들(102b)에게 지불하기 위한 명령들을 포함할 수 있다. 지불들은 예컨대, 국가 통화, 명목 화폐, 원자재 또는 원자재 통화, 암호화폐, 금융 상품 또는 증권(예컨대, 주식들 또는 채권들), 또는 이들의 임의의 조합의 형태일 수 있다.

[0082] [0100] 개별 레코드들(100)의 콘텐츠들(110)은 소프트웨어 코드를 포함할 수 있다. 프로세싱 플랫폼(124)은 특정 조건들이 만족될 때 소프트웨어 코드를 실행할 수 있다. 이러한 조건들은 시간 기반일 수 있는데, 이를테면, 레코드 수신자(102b)가 소프트웨어 코드를 포함하는 개별 레코드(100)를 상환하는 시간 기반일 수 있다. 콘텐츠들(110)은 자체-실행 소프트웨어 코드를 포함할 수 있다. 자체-실행 코드는 특정 조건들이 만족될 때 자동으로 실행될 수 있다. 일부 실시예들에서, 사용자들은 예컨대, 특정 조건들, 이를테면 사기가 검출될 때, 소프트웨어 코드들의 실행을 방지하거나 지연시킬 수 있다. 일부 실시예들에서, 사용자들은 소프트웨어 코드들의 실행을 방지하거나 지연하지 못할 수 있다.

[0083] [0101] 개별 레코드들(100)의 콘텐츠들(110)은 전송자와 수신자 간의 계약상 의무들 또는 권리들(예컨대, 스마트 계약들)을 포함할 수 있다. 예컨대, 레코드 수신자(102b)는 서비스, 이를테면 레코드 전송자의 컴퓨터 인프라구조의 백업을 수행하기 위한 계약상 의무 하에 있을 수 있으며, 서비스에 대한 지불을 받을 계약상의 권리를 가질 수 있고; 그리고 레코드 전송자(102a)는 서비스에 대해 레코드 수신자(102b)에게 지불할 계약상 의무 하에 있을 수 있고, 레코드 수신자의 퍼포먼스(performance)를 수신하기 위한 계약상 권리를 가질 수 있다. 개별 사용자들, 파트너십들, 회사들 또는 기업들 간에 스마트 계약들이 있을 수 있다. 스마트 계약은 소프트웨어 코드의 반복 실행을 수반할 수 있다. 소프트웨어 코드는 특정 조건들이 만족될 때 실행될 수 있는 소프트웨어 코드를 포함할 수 있다. 예로서, 소프트웨어 코드는 수신자의 컴퓨터 인프라구조의 백업 또는 보안 스캔을 위한 소프트웨어 코드를 포함할 수 있다. 소프트웨어 코드는 조건(예컨대, 암호화폐의 매달 지불을 전송자에게 송금하는 것)의 발생시 실행될 수 있다. 일부 실시예들에서, 스마트 계약들은 특정 조건들이 만족될 때 지불들을 반복하는 것을 수반할 수 있다. 예컨대, 스마트 계약은 주기적으로, 이를테면 매주 레코드 전송자의 컴퓨터 인프라구조를 백업하도록 레코드 수신자(102b)에게 요구할 수 있다. 주기적 퍼포먼스의 조건이 만족되면, 레코드 전송자(102a)는 레코드 수신자(102b)에게 주기적으로 지불하도록 스마트 계약 하에 계약상 의무를 갖는다.

[0084] [0102] 콘텐츠들(110)은 에스크로우를 수반할 수 있다. 예컨대, 레코드 전송자(102a) 및 레코드 수신자(102b)는 코드들, 이를테면 소프트웨어 코드들을 교환하기를 원할 것이다. 저장소, 예컨대 프로세싱 플랫폼(124)에 제1 소프트웨어 코드들을 제공한 후에, 레코드 전송자(102a)는 제1 조건들이 만족된다면 제1 소프트웨어 코드들을 레코드 수신자(102b)에게 제공하도록 저장소에 명령하는 제1 개별 레코드(100)를 레코드 수신자(102b)에게 제공할 수 있다. 유사하게, 오리지널 레코드 수신자(102b)는, 제2 조건들이 만족된다면 오리지널 레코드 전송자(102a)에게 제2 소프트웨어 코드들을 제공하도록 저장소에 명령하는 제2 개별 레코드(100m1)를 오리지널 레코드 전송자(102a)에게 제공할 수 있다. 제1 조건들 및 제2 조건들은 시간 기반일 수 있다. 제1 조건들 및 제2 조건들은 동일하거나 상이할 수 있다.

[0085] [0103] 일부 실시예들에서, 레코드 전송자(102a)는 교환의 부분으로서 개별 레코드(100)를 레코드 수신자(102b)에게 제공할 수 있다. 예컨대, 개별 레코드의 콘텐츠(110)는 제1 금액을 레코드 전송자의 계정에서 데빗팅하도록 그리고 제2 금액을 레코드 수신자의 계정에서 크레딧팅하도록 프로세싱 플랫폼(124)에 명령할 수 있다. 예컨대, 제품 또는 일부 코드들을 레코드 전송자(102a)에게 제공하는 레코드 수신자(102b)에 의해 계정 데빗팅 및 크레딧팅이 동반될 수 있다.

[0086] 예시적인 두 수신자들

[0087] *예시적인 제1 콘텐츠 요청*

[0088] [0104] 일부 실시예들에서, 레코드 전송자로부터 개별 레코드를 수신한 후에, 레코드 수신자는 수신된 개별 레코드를 후속적 레코드 수신자에게 전송할 수 있다. 도 6은 2개의 레코드 수신자들을 위해 생성된 개별 레코드들을 안전하게 교환하고 상환하는 일 실시예를 예시하는 상호작용 다이어그램이다. 도 4-도 5에 예시된 바와 같이, 제1 레코드 수신자 디바이스(116b)를 사용하는 제1 레코드 수신자(102b)는 상호작용(404)에서 제1 콘텐츠 요청(402)을 제1 레코드 전송자 디바이스(116a)에 전송함으로써 제1 레코드 전송자(102a)로부터의 개별 레코드를 요청할 수 있다. 제1 콘텐츠 요청(402)은 제1 레코드 수신자 디바이스의 제1 공개 키(106b) 및 콘텐츠 B(110b)를 포함할 수 있다.

[0089] [0105] 상호작용(408)에서, 제1 레코드 전송자 디바이스(116a)는 파트너 식별에 의해 제1 레코드 수신자 디바이스(116b)의 아이덴티티를 확인할 수 있다. 제1 레코드 전송자 디바이스(116a)의 SE(secure element)(204a)가 제1 레코드 전송자의 인증 정보(512a)를 검증한 후에, SE(secure element)(204a)는 상호작용(416)에서 개별 레코드(100)에 싸인할 수 있다.

[0090] [0106] 도 7은 2개의 레코드 수신자들을 위해 생성된 예시적인 개별 레코드들을 개략적으로 예시한다. 도 6-도 7에 예시된 바와 같이, 개별 레코드(100)는 블록(105a)을 포함하는 디지털 객체일 수 있다. 블록(105a)은 "from 필드" 내의 제1 레코드 전송자 디바이스의 제1 공개 키(106a), "to 필드" 내의 제1 레코드 수신자 디바이스의 제1 공개 키(106b), 레코드 ID(108), 콘텐츠 A(110a) 및 블록(105a)의 제1 레코드 전송자 서명(112a)을 포함할 수 있다.

[0091] [0107] 상호작용(420)에서, 제1 레코드 전송자(102a)는 예컨대, SRL(short range link)(122)을 사용하여 피어-투-피어 방식으로 제1 레코드 수신자(102b)에 개별 레코드(100)를 전송할 수 있다. 일단 제1 레코드 수신자(102b)의 소유이면, 제1 레코드 수신자(102b)는 상호작용(424)에서 개별 레코드(100)를 검증할 수 있다.

[0092] *예시적인 제2 콘텐츠 요청*

[0093] [0108] 도 6을 참조하면, 레코드 수신자 디바이스를 사용하는 제2 레코드 수신자는 상호작용(604)에서 SRL(short range link)(122)을 사용하여 레코드 전송자 디바이스에 콘텐츠 요청을 전송함으로써 레코드 전송자로부터 개별 레코드를 요청할 수 있다. 예컨대, 제2 레코드 수신자 디바이스(116c)를 사용하는 제2 레코드 수신자(102c)는 제1 레코드 수신자 디바이스(116b)에 제2 콘텐츠 요청(602)을 전송함으로써 제1 레코드 수신자(102b)로부터 개별 레코드를 요청할 수 있다. 제1 레코드 수신자(102b)는 제2 레코드 전송자일 수 있고, 제1 레코드 수신자 디바이스(116b)는 제2 레코드 전송자 디바이스로서 지칭될 수 있다. 제2 콘텐츠 요청(602)은 콘텐츠, 예컨대 콘텐츠 C(110c) 및 제2 레코드 수신자 디바이스의 공개 키(106c)를 포함할 수 있다.

[0094] [0109] 상호작용(608)에서, 제2 레코드 전송자 디바이스(116b)는 파트너 식별에 의해 제2 레코드 수신자 디바이스(116c)의 아이덴티티를 확인할 수 있다. 제2 레코드 전송자/제1 레코드 수신자 디바이스(116b)의 SE(secure element)(204b)가 제2 레코드 전송자의 인증 정보(512b)를 검증한 후에, 제2 레코드 전송자 디바이스(116b)는 제1 수정 레코드(100m1)에 싸인한 후에, 이를 다양한 이유들 및 목적들로 제2 레코드 수신자 디바이스(116c)에 전송하는 것으로 판단할 수 있다. 예컨대, 제2 레코드 수신자(102c)는 제2 레코드 전송자(102b)의 양수인일 수 있다. 프로세싱 플랫폼(124)이 콘텐츠 A(110a)에 의해 명령된 대로 제1 레코드 수신자/제2 레코드 전송자(102b)에 대해 수행하는 대신에, 프로세싱 플랫폼(124)은 제2 레코드 수신자(102c)에 대해 수행할 수 있다. 콘텐츠 A(110a), 콘텐츠 B(110b) 및 콘텐츠 C(110c)는 동일하거나 유사하거나 관련되거나 상이할 수 있다.

[0095] [0110] SE(secure element)(204b)는 상호작용(612)에서 제1 수정된 개별 레코드(100m1)에 싸인할 수 있다. 제1 수정된 개별 레코드(100m1)에 싸인하는 것은 블록, 예컨대 블록(105b)을 개별 레코드(100)에 부가하여 제1 수정된 개별 레코드(100m1)를 생성하는 것을 포함할 수 있다. 제1 수정된 개별 레코드(100m1)의 블록(105b)은 제2 레코드 수신자 디바이스의 제2 공개 키(106c) 및 블록(105b)의 제2 레코드 전송자 서명/제1 레코드 수신자

서명(112b)을 포함할 수 있다.

[0096] [0111] 상호작용(616)에서, 제2 레코드 전송자(102b)는 예컨대, SRL(short range link)(122)을 사용하여 피어-투-피어 방식으로 제2 레코드 수신자(102c)에 제1 수정된 개별 레코드(100m1)를 전송할 수 있다. 일단 제2 레코드 수신자(102c)의 소유이면, 제2 레코드 수신자(102c)는 상호작용(620)에서 제1 수정된 개별 레코드(100m1)를 검증할 수 있다. 제1 수정된 개별 레코드(100m1)를 검증하는 것은 예컨대, 제1 수정된 개별 레코드(100m1) 내의 제1 레코드 전송자 디바이스의 공개 키(106a) 및 제2 레코드 전송자 디바이스의 공개 키(106b)를 사용하여 제1 레코드 전송자 서명(112a) 및 제2 레코드 전송자 서명(112b)을 인증하는 것을 포함할 수 있다.

[0097] *예시적인 개별 레코드 상환*

[0098] [0112] 도 6을 참조하면, 제1 수정된 개별 레코드(100m1)를 성공적으로 검증한 후에, 제2 레코드 수신자 디바이스(116c)는 자신의 SE(secure element)(204c)를 사용하여 상호작용(624)에서 제2 수정된 개별 레코드(100m2)를 생성하고 싸인할 수 있으며, 여기서 m은 개별 레코드(100)가 수정되었음을 표시하고, m2는 개별 레코드(100)가 적어도 2번 수정되었음을 표시한다. 제2 수정된 개별 레코드(100m2)에 싸인하기 전에, SE(secure element)(204c)는 제2 레코드 수신자의 인증 정보(512c) 및 디지털방식으로 싸인될 블록, 예컨대 제2 수정된 개별 레코드(100m2)의 블록(105c)의 프로비전 둘 모두를 요구할 수 있다. 제2 수정된 개별 레코드(100m2)는 개별 레코드(100)의 블록(105a), 제1 수정된 개별 레코드의 블록(105b) 및 배서 블록(105c)을 포함할 수 있다. 예컨대, 배서는 레코드 수신자 디바이스의 공개 키(106c)와 함께, 제2 수정된 개별 레코드(100m2)가 제2 레코드 수신자(102c)에 의해서만 상환될 수 있음을 특정하는 "프로세싱만을 위한 배서"(FPOE)(114)일 수 있다.

[0099] [0113] 제2 수정된 개별 레코드(100m2)에 싸인한 후, 제2 레코드 수신자(102c)는 상호작용(628)에서 프로세싱 플랫폼(124)에 제2 수정된 개별 레코드(100m2)를 상환할 수 있다. 상환 시, 프로세싱 플랫폼(124)을 동작시키는 서비스 제공자(104)는 제2 수정된 개별 레코드(100m2) 내의 블록들(105a, 105b 및 105c)의 체인 내의 하나 이상의 서명들의 진본성을 검증함으로써 상호작용(632)에서 제2 수정된 개별 레코드(100m2)를 프로세싱할 수 있다. 검증된 싸인들은 제1 레코드 전송자 서명(112a), 제2 레코드 전송자 서명/제1 레코드 수신자 서명(112b) 및 제2 레코드 수신자 서명(112c)을 포함할 수 있다. 성공적인 검증 후, 프로세싱 플랫폼(124)은 제2 수정된 개별 레코드(100m1)의 콘텐츠 A(110a)에 의해 명령된 대로 수행할 수 있다.

[0100] 예시적인 N개의 수신자들

[0101] [0114] 일부 실시예에서, 레코드 전송자로부터 개별 레코드를 수신한 후, 레코드 수신자는 수신된 개별 레코드를 후속적 레코드 수신자에 전송할 수 있다. 차례로, 후속적 레코드 수신자는 자신이 수신한 개별 레코드를 다른 레코드 수신자에 전송할 수 있다. 마지막 레코드 수신자는 자신이 수신한 개별 레코드를 처리 플랫폼에 상환할 수 있다. 레코드들의 체인의 전송자들/수신자들의 수(N)는 2, 3, 4, 5, 6, 10, 20, 100 또는 그 초과일 수 있다.

[0102] *예시적인 제1 콘텐츠 요청*

[0103] [0115] 도 8은 복수의 레코드 수신자들을 위해 생성된 예시적인 개별 레코드들을 개략적으로 예시한다. 도 4 내지 도 7에 예시된 바와 같이, 제1 레코드 수신자 디바이스(116b)를 사용하는 제1 레코드 수신자(102b)는, SRL(short range link)(122)를 사용하여 제1 레코드 전송자 디바이스(116a)에 제1 콘텐츠 요청을 전송함으로써 제1 레코드 전송자(102a)로부터의 개별 레코드를 요청할 수 있다. 제1 콘텐츠 요청은 제1 레코드 수신자 디바이스의 제1 공개 키(106b) 및 콘텐츠 B를 포함할 수 있다.

[0104] [0116] 제1 레코드 전송자 디바이스(116a)는 파트너 식별에 의해 제1 레코드 수신자 디바이스(116b)의 아이덴티티를 확인할 수 있다. 제1 레코드 전송자 디바이스(116a)의 SE(secure element)(204a)가 제1 레코드 전송자의 인증 정보(512a)를 검증한 후, SE(secure element)(204a)는 상호작용(416)에서 개별 레코드(100)를 싸인할 수 있다.

[0105] [0117] 개별 레코드(100)는 블록(105a)을 포함하는 디지털 객체일 수 있다. 블록(105a)은 "from 필드"내의 제1 레코드 전송자 디바이스의 제1 공개 키(106a), "to 필드"내의 제1 레코드 수신자 디바이스의 제1 공개 키(106b), 레코드 ID(108), 콘텐츠 A(110a), 및 블록(105a)의 제1 레코드 전송자 서명(112a)을 포함한다.

[0106] [0118] 제1 레코드 전송자(102a)는 예컨대, SRL(short range link)(122)을 사용하는 피어 투 피어(peer-to-peer) 방식으로 개별 레코드(100)를 제1 레코드 수신자(102b)에 전송할 수 있다. 일단 제1 레코드 수신자(102b)의 소유이면, 제1 레코드 수신자(102b)는 개별 레코드(100)를 검증할 수 있다.

[0107] *예시적인 제2 콘텐츠 요청*

[0108] [0119] 도 8을 참조하면, 레코드 수신자 디바이스를 사용하는 제2 레코드 수신자는 SRL(short range link)(122)을 사용하여 레코드 전송자 디바이스에 콘텐츠 요청을 전송함으로써 레코드 전송자로부터의 개별 레코드를 요청할 수 있다. 예컨대, 제2 레코드 수신자 디바이스(116c)를 사용하는 제2 레코드 수신자(102c)는 SRL(short range link)(122)을 사용하여 제2 레코드 전송자 디바이스(116b)에 제2 콘텐츠 요청을 전송함으로써 제2 레코드 전송자(102b)로부터의 개별 레코드를 요청할 수 있다. 제1 레코드 수신자(102b)는 제2 레코드 전송자일 수 있고, 제1 레코드 수신자 디바이스(116b)는 제2 레코드 전송자 디바이스로 지칭될 수 있다. 제2 콘텐츠 요청은 제2 레코드 수신자 디바이스의 공개 키(106c) 및 콘텐츠 C를 포함할 수 있다.

[0109] [0120] 제2 레코드 전송자 디바이스/제1 레코드 수신자 디바이스(116b)는 파트너 식별에 의해 제2 레코드 수신자 디바이스(116c)의 아이덴티티를 확인할 수 있다. 제2 레코드 전송자 디바이스/제1 레코드 수신자 디바이스(116b)의 SE(secure element)(204b)가 제2 레코드 전송자의 인증 정보(512b)를 검증한 후, 제2 레코드 전송자 디바이스(116b)는 제1 수정된 레코드(100m1)를 싸인한 후 이를 제2 레코드 수신자 디바이스(116c)에 전송하기로 결정할 수 있다.

[0110] [0121] 제2 레코드 전송자 디바이스(116b)의 SE(secure element)(204b)는 상호작용(612)에서 제1 수정된 개별 레코드(100m1)를 싸인할 수 있다. 제1 수정된 개별 레코드(100m1)를 싸인하는 것은, 블록, 예컨대 블록(105b)을 개별 레코드(100)에 추가하여 제1 수정된 개별 레코드(100m1)를 생성하는 것을 포함할 수 있다. 제1 수정된 개별 레코드(100m1)의 블록(105b)은 제2 레코드 수신자 디바이스의 제2 공개 키(106c) 및 블록(105b)의 제2 레코드 전송자 서명/제1 레코드 수신자 서명(112b)을 포함할 수 있다.

[0111] [0122] 제2 레코드 전송자(102b)는 예컨대, SRL(short range link)(122)을 사용하는 피어-투-피어 방식으로 제1 수정된 개별 레코드(100m1)를 제2 레코드 수신자(102c)에 전송할 수 있다. 일단 제2 레코드 수신자(102c)의 소유이면, 제2 레코드 수신자(102c)는 제1 수정된 개별 레코드(100m1)를 검증할 수 있다. 제1 수정된 개별 레코드(100m1)를 검증하는 것은, 예컨대, 제1 수정된 개별 레코드(100m1)내의 제1 레코드 전송자 디바이스의 공개 키(106a) 및 제2 레코드 전송자 디바이스의 공개 키(106b)를 사용하여 제1 레코드 전송자 서명(112a) 및 제2 레코드 전송자 서명(112b)을 인증하는 것을 포함할 수 있다.

[0112] *예시적인 제3 콘텐츠 요청*

[0113] [0123] 도 8을 참조하면, 제3 레코드 수신자 디바이스를 사용하는 제3 레코드 수신자는 SRL(short range link)(122)을 사용하여 레코드 전송자 디바이스에 콘텐츠 요청을 전송함으로써 레코드 전송자로부터의 개별 레코드를 요청할 수 있다. 예컨대, 제3 레코드 수신자 디바이스를 사용하는 제3 레코드 수신자는 SRL(short range link)(122)을 사용하여 제3 레코드 전송자 디바이스(116c)에 제3 콘텐츠 요청을 전송함으로써 제3 레코드 전송자로부터의 개별 레코드를 요청할 수 있다. 제2 레코드 수신자(102b)는 제3 레코드 전송자일 수 있고, 제2 레코드 수신자 디바이스(116b)는 제3 레코드 전송자 디바이스로 지칭될 수 있다. 제3 콘텐츠 요청은 제3 레코드 수신자 디바이스의 공개 키 및 콘텐츠를 포함할 수 있다.

[0114] [0124] 제3 레코드 전송자 디바이스(116c)는 파트너 식별에 의해 제3 레코드 수신자 디바이스의 아이덴티티를 확인할 수 있다. 제3 레코드 전송자 디바이스/제3 레코드 수신자 디바이스(116c)의 SE(secure element)(204c)가 제3 레코드 전송자의 인증 정보(512c)를 검증한 후, 제3 레코드 전송자 디바이스는 제2 수정된 레코드(100m2)를 싸인한 후 이를 제3 레코드 수신자 디바이스에 전송할 수 있다.

[0115] [0125] SE(secure element)(204c)는 상호작용(624)에서 제2 수정된 개별 레코드(100m2)를 싸인할 수 있다. 제2 수정된 개별 레코드(100m2)를 싸인하는 것은, 블록, 예컨대 블록(105c)을 제1 수정된 개별 레코드(100m1)에 추가하여 제2 수정된 개별 레코드(100m2)를 생성하는 것을 포함할 수 있다. 제2 수정된 개별 레코드(100m2)의 블록(105c)은 제2 레코드 수신자 디바이스의 제3 공개 키(106c) 및 블록(105c)의 제3 레코드 전송자 서명/제2 레코드 수신자 서명(112c)을 포함할 수 있다.

[0116] [0126] 제3 레코드 전송자(102c)는 예컨대, SRL(short range link)(122)을 사용하는 피어-투-피어 방식으로 제2 수정된 개별 레코드(100m2)를 제3 레코드 수신자에 전송할 수 있다. 일단 제3 레코드 수신자의 소유이면, 제3 레코드 수신자는 제2 수정된 개별 레코드(100m2)를 검증할 수 있다. 제2 수정된 개별 레코드(100m2)를 검증하는 것은, 예컨대, 제2 수정된 개별 레코드(100m2) 내의 제1 레코드 전송자 디바이스, 제2 레코드 전송자 디바이스 및 제3 레코드 전송자 디바이스의 공개 키들(106a, 106b 및 106c)을 사용하여, 제1 레코드 전송자 서명(112a), 제2 레코드 전송자 서명/제1 레코드 수신자 서명(112b) 및 제3 레코드 전송자 서명/제2 레코드 수신자

서명(112c)을 인증하는 것을 포함할 수 있다.

[0117] *예시적인 제n 콘텐츠 요청*

[0118] [0127] 도 8을 참조하면, 제n 레코드 수신자 디바이스를 사용하는 제n 레코드 수신자는 SRL(short range link)(122)을 사용하여 제n 레코드 전송자 디바이스에 제n 콘텐츠 요청을 전송함으로써 제n 레코드 전송자로부터의 개별 레코드를 요청할 수 있다. 제n 레코드 전송자는 제(n-1) 레코드 수신자일 수 있고, 제(n-1) 레코드 수신자 디바이스는 제n 레코드 전송자 디바이스로 지칭될 수 있다. 제n 콘텐츠 요청은 제n 레코드 수신자 디바이스의 공개 키 및 콘텐츠를 포함할 수 있다.

[0119] [0128] 제n 레코드 전송자 디바이스는 파트너 식별에 의해 제n 레코드 수신자 디바이스의 아이덴티티를 확인할 수 있다. 제n 레코드 전송자 디바이스/제(n-1) 레코드 수신자 디바이스의 SE(secure element)가 제n 레코드 전송자의 인증 정보를 검증한 후, 제n 레코드 전송자 디바이스는 제(n-1) 수정된 레코드(100m(n-1))를 싸인한 후, 이를 제n 레코드 수신자 디바이스에 전송할 수 있고, 여기서 m은 개별 레코드(100)가 수정되었음을 표시하고, m(n-1)은 개별 레코드(100)가 적어도 (n-1)번 수정되었음을 표시한다.

[0120] [0129] 제n 레코드 전송자 디바이스의 SE(secure element)는 제(n-1) 수정된 개별 레코드(100m(n-1))를 싸인할 수 있다. 제(n-1) 수정된 개별 레코드(100m(n-1))를 싸인하는 것은 제(n-2) 수정된 개별 레코드에 블록(105(n-1))을 부가하여 제(n-1) 수정된 개별 레코드(100m(n-1))를 생성하는 것을 포함할 수 있다. 제(n-1) 수정된 개별 레코드(100m(n-1))의 블록(105(n-1))의 제n 레코드 수신자 디바이스의 제n 공개 키(106n)와 블록(105(n-1))의 제n 레코드 전송자 서명/레코드 수신자 서명(112(n-1))을 포함할 수 있다.

[0121] [0130] 제n 레코드 전송자는, 예컨대, SRL(short range link)(122)을 사용하는 피어-투-피어 방식으로 제n 레코드 수신자에 제(n-1) 수정된 개별 레코드(100m(n-1))를 전송할 수 있다. 일단 제n 레코드 수신자의 소유이면, 제n 레코드 수신자는 제(n-1) 수정된 개별 레코드(100m(n-1))를 검증할 수 있다. 제(n-1) 수정된 개별 레코드(100m(n-1))를 검증하는 것은, 예컨대, 제(n-1) 수정된 개별 레코드(100m(n-1)) 내의 제1 레코드 전송자 디바이스(112a), 제2 레코드 전송자 디바이스(112b), 제3 레코드 전송자 디바이스(112c), ..., 및 제n 레코드 전송자 디바이스의 공개 키들을 사용하여, 제1 레코드 전송자 서명(112a), 제2 레코드 전송자 서명(112b),..., 제(n-1) 레코드 전송자 서명(112(n-1))을 인증하는 것을 포함할 수 있다.

[0122] *예시적인 개별 레코드 상환*

[0123] [0131] 도 8을 참조하면, 제(n-1) 수정된 개별 레코드(100m(n-1))를 성공적으로 검증한 후, 제n 레코드 수신자 디바이스는, 자신의 보안 엘리먼트를 사용하여, 제n 수정된 개별 레코드(100mn)를 생성 및 싸인할 수 있고, 여기서 m은 개별 레코드(100)가 수정되었음을 표시하고, mn은 개별 레코드(100)가 적어도 N번 수정되었음을 표시한다. 제n 수정된 개별 레코드(100MM)를 싸인하기 전에, SE(secure element)는 제n 레코드 수신자의 인증 정보 및 디지털방식으로 싸인될 블록, 예컨대 제n 수정된 개별 레코드(100mn)의 블록(105n)의 프로비전 둘 모두를 요구할 수 있다. 제n 수정된 개별 레코드(100mn)는 배서 블록(105n)을 포함할 수 있다. 예컨대, 배서는, 제n 수정된 개별 레코드(100mn)의 공개 키들과 함께 제n 수정된 개별 레코드(100mn)가 제n 레코드 수신자에 의해서만 상환될 수 있다고 특정하는 "FPOE(for processing only endorsement)"(114)일 수 있다.

[0124] [0132] 제n 수정된 개별 레코드(100mn)를 싸인한 후, 제n 레코드 수신자는 프로세싱 플랫폼에 제n 수정된 개별 레코드(100mn)를 상환할 수 있다. 상환 시, 프로세싱 플랫폼을 동작시키는 서비스 제공자는, 제n 수정된 개별 레코드(100mn) 내의 블록들의 체인(105a, 105b, 105c, ..., 105(n-1) 및 105n)의 서명들의 진본성을 검증함으로써 제n 수정된 개별 레코드(100mn)를 프로세싱할 수 있다. 성공적인 검증 후, 프로세싱 플랫폼(124)은 제n 수정된 개별 레코드(100mn)의 콘텐츠 A(110a)에 의해 명령된 대로 수행할 수 있다.

[0125] 에이전트와 레코드 수신자 간의 예시적인 상호작용들

[0126] *레코드 전송자로부터 에이전트로의 예*

[0127] [0133] 일부 실시예에서, 에이전트는 레코드 수신자 대신에 행동할 수 있다. 상인 또는 본인의 예시적인 상황에서, 상인 또는 본인은 레코드 수신자일 수 있고, 에이전트는 계산대 또는 지불 부스의 종업원일 수 있다. 다른 예시적인 상황에서, 에이전트는, 커스터머들이 상인으로부터 자신의 구매를 프로세싱할 수 있게 하는 셀프-체크아웃 머신 또는 키오스크일 수 있다. 종업원은 일반적으로 커스터머의 전자 디바이스(116a)로부터 전송된 지불을 수신하기 위해 현금 등록기와 같은 POS(point-of-sale) 디바이스를 사용하여 커스터머 체크아웃시 상인을 대신하여 지불들을 수락한다.

[0128] [0134] 도 9는 에이전트 및 수신자를 수반하는 개별 레코드를 안전하게 교환하고 상환하는 일 실시예를 예시하는 상호작용 다이어그램이다. 에이전트 디바이스(116d)를 사용하는 레코드 수신자(102b)의 에이전트(102d)는, 상호작용(404)에서 SRL(short range link)(122)을 사용하여 콘텐츠 요청(402)을 레코드 전송자 디바이스(116a)에 전송함으로써 레코드 전송자(102a)로부터 개별 레코드를 요청할 수 있다. 콘텐츠 요청(402)은 레코드 수신자의 공개 키(106b) 및 콘텐츠 B(110b)를 포함할 수 있다.

[0129] [0135] 레코드 수신자(102b), 예컨대, 상인은 하나 이상의 에이전트들(102d), 예컨대 10개의 에이전트들(예컨대, 체커들)을 가질 수 있거나 이들과 연관될 수 있다. 에이전트들(102d)과 에이전트 디바이스들(116d) 간의 관계들은 변할 수 있다. 예컨대, 일부 에이전트들(102d)은 하나의 에이전트 디바이스(116d)를 공유할 수 있고, 에이전트 디바이스들(116d)은 인가된 에이전트들(102d)에 의한 다수의 로그인들을 지원할 수 있다. 다른 예로서, 일부 에이전트들(102d)은 에이전트 디바이스들(116d)을 공유하지 않는다. 또 다른 예로서, 일부 에이전트들(102d) 각각은 하나보다 많은 에이전트 디바이스(116d)를 가질 수 있다. 일부 에이전트들(102d)은 자신의 에이전트 디바이스들(116d)을 가질 수 있다.

[0130] [0136] 레코드 수신자(102b)는 하나 이상의 공개 키들(106b)을 가질 수 있거나 또는 이들과 연관될 수 있다. 예컨대, 레코드 수신자(102b)는 하나의 공개 키(106b)를 가질 수 있다. 다른 예로서, 레코드 수신자(102b)는 위치, 예컨대 물리적 위치 또는 가상 위치마다 하나의 공개 키(106b)를 가질 수 있다. 물리적 위치는 상점 위치 또는 교환의 위치일 수 있다. 또 다른 예로서, 레코드 수신자(102b)는 외부 디바이스 마다 하나의 공개 키(106b)를 가질 수 있다.

[0131] [0137] 에이전트들(102d)은 본 개시 내용의 시스템들 및 방법들의 일부가 아닌 외부 디바이스들과 유리하게 상호작용할 수 있다. 외부 디바이스들의 비-제한적인 예들은, 셀룰러 전화들, 태블릿 컴퓨터들, e-리더들, 스마트 시계들, 머리 장착 증강, 가상 또는 혼합 현실 디스플레이 시스템들, 웨어러블 디스플레이 시스템들, 컴퓨터들, 서버 컴퓨터들, PoS(point of sale) 시스템들 또는 현금 등록기들을 포함한다. 외부 디바이스들은 위치들, 예컨대 물리적 위치 이를테면 상점 위치에 고정될 수 있다. 외부 디바이스들은, 인프라구조, 예컨대, 기존 인프라구조의 일부일 수 있다.

[0132] [0138] 공개 키들(106b)의 관리는 변할 수 있다. 예컨대, 레코드 수신자(102b)는 레코드 수신자 디바이스(116b) 또는 자신이 동작시키는 하나 이상의 다른 컴퓨터들을 사용하여 공개 키들(106b) 자체를 관리할 수 있다. 다른 예로서, 서비스 제공자(104)는 "Saas(software as a service)"와 유사한 서비스로서 레코드 수신자의 공개 키들(106b)을 관리할 수 있다.

[0133] [0139] 유리하게, 블록(105a)이 에이전트 디바이스(116d)의 공개 키(106d)가 아니라 레코드 수신자 디바이스(116b)의 공개 키(106b)를 포함하기 때문에, 에이전트(102d)는 개별 레코드(100) 또는 제1 수정된 개별 레코드(100m1)를 프로세싱 플랫폼(124)에 상환할 수 없다.

[0134] [0140] 상호작용(408)에서, 레코드 전송자 디바이스(116a)는 파트너 식별에 의해 에이전트 디바이스(116d)의 아이덴티티 또는 레코드 수신자 디바이스(116b)의 아이덴티티를 확인할 수 있다. 레코드 전송자 디바이스(116a)의 SE(secure element)(204a)가 레코드 전송자의 인증 정보(512a)를 검증한 후, SE(secure element)(204a)는 상호작용(416)에서 개별 레코드(100)를 싸인할 수 있다.

[0135] [0141] 도 10은 에이전트 및 레코드 수신자를 수반하는 예시적인 개별 레코드들을 개략적으로 예시한다. 도 9 및 10에 예시된 바와 같이, 개별 레코드(100)는 블록(105a)을 포함하는 디지털 객체일 수 있다. 블록(105a)은 "from 필드"의 레코드 전송자 디바이스의 공개 키(106a), "to 필드"의 레코드 수신자 디바이스의 공개 키(106b), 레코드 ID(108), 콘텐츠 A(110a), 및 블록(105a)의 레코드 전송자 서명(112a)을 포함한다.

[0136] [0142] 상호작용(420)에서, 레코드 전송자(102a)는, 예컨대, SRL(short range link)(122)을 사용하는 피어-투-피어 방식으로 개별 레코드(100)를 에이전트(102d)에 전송할 수 있다. 일단 에이전트(102d)의 소유이면, 에이전트(102d)는 상호작용(424)에서 개별 레코드(100)를 검증할 수 있다. 일부 실시예들에서, 에이전트 디바이스(116d)는 레코드 수신자(102b)의 사설 네트워크를 통해, 네트워크, 예컨대 네트워크(118)에 연결될 수 있다. 네트워크(118)에 대한 이러한 연결성을 이용하여, 에이전트 디바이스(116d)는 개별 레코드(100)를 프로세싱 플랫폼(124)으로 검증할 수 있다. 일부 실시예들에서, 레코드 전송자 디바이스(116a)가 아닌, 에이전트 디바이스(116d)가 네트워크에 액세스할 수 있다.

[0137] *에이전트로부터 레코드 수신자까지의 예*

[0138] [0143] 도 9를 참조하면, 일부 실시들예에서, 에이전트 디바이스(116d)의 SE(secure element)(204d)는, 상호작용(908)에서 제1 수정된 개별 레코드(100m1)를 레코드 수신자(102b)에 보내기 전에, 상호작용(904)에서 제1 수정된 개별 레코드(100m1)를 생성하고 싸인할 수 있다. 제1 수정된 개별 레코드(100m1)를 싸인하는 것은, 블록(105b)을 제1 개별 레코드(100)에 부가하여 제1 수정된 개별 레코드(100m1)를 생성하는 것을 포함할 수 있다. 제1 수정된 개별 레코드(100m1)의 블록(105b)은 에이전트 디바이스의 공개 키(106d), 배서, 및 블록(105b)의 에이전트 서명(112d)을 포함할 수 있다. 배서는 예컨대 "HBE(handled by endorsement)"(114a)일 수 있다. 레코드 전송자 디바이스의 공개 키(106a) 및 레코드 수신자 디바이스의 공개 키(106b)와 함께, "HBE(handled by endorsement)", 에이전트 디바이스의 공개 키(106d) 및 에이전트 서명(112d)은, 에이전트 디바이스(116d)가 레코드 수신자(102b)를 대신하여 레코드 전송자 디바이스(116a)로부터 개별 레코드(100)를 수신했을 수 있음을 나타낼 수 있다.

[0139] [0144] 상호작용(908)에서, 에이전트(102d)는 통신 링크를 통해 직접 또는 간접적으로 제1 수정된 개별 레코드(100m1)를 레코드 수신자(102b)에 전송할 수 있다. 예컨대, 에이전트(102d)는 예컨대, SRL(short range link)(122)을 사용하는 피어-투-피어 방식으로 제1 수정된 개별 레코드(100m1)를 레코드 수신자(102b)에 전송할 수 있다. 다른 예로서, 에이전트(102d)는 네트워크, 예컨대, 네트워크(118)를 통해 제1 수정된 개별 레코드(100m1)를 레코드 수신자(102b)에 전송할 수 있다. 레코드 수신자 디바이스(116b)의 구성은 변할 수 있다. 예컨대, 레코드 수신자 디바이스(116b)는, 도 2에 예시된 사용자 디바이스(116), 도 3에 예시된 프로세싱 플랫폼(124) 또는 이들의 임의의 조합과 유사하거나 동일할 수 있다.

[0140] [0145] 일부 실시예들에서, 일단 레코드 수신자(102b)의 소유이면, 레코드 수신자(102b)는 제1 수정된 개별 레코드(100m1)를 검증할 수 있다. 제1 수정된 개별 레코드(100m1)를 검증하는 것은, 에이전트 디바이스와 연관된 공개 키(106d)가 인가된 에이전트(102d)와 연관되는지의 여부를 결정하는 것을 포함할 수 있다. 레코드 수신자(102b)는 비인가된 사람에 의해 수신되거나 인가된 에이전트에 의해 배서되지 않는 채로 수신된 개별 레코드들을 거절할 수 있다. 제1 수정된 개별 레코드(100m1)를 검증하는 것은, 예컨대, 제1 수정된 개별 레코드(100m1)에서 레코드 전송자 디바이스의 공개 키(106a) 및 에이전트 디바이스의 공개 키(106d)를 사용하여, 레코드 전송자 서명(112a) 및 에이전트 서명(112d)을 인증하는 것을 포함할 수 있다.

[0141] *예시적인 개별 레코드 상환*

[0142] [0146] 도 9를 참조로, 레코드 수신자 디바이스(116b)는 예컨대, 자신의 SE(secure element)(204b)를 사용하여 제2 수정된 개별 레코드(100m2)를 생성하고 싸인할 수 있다. 일부 실시예들에서, 상호작용(912)에서 제2 수정된 개별 레코드(100m2)를 싸인하기 전에, 레코드 수신자 디바이스(116b)의 SE(secure element)(204b)는, 레코드 수신자 또는 레코드 수신자(102b)를 위해 일하는 인가된 인원의 인증 정보 및 디지털방식으로 싸인될 블록, 예컨대 제2 수정된 개별 레코드(100m2)의 블록(105c)의 프로비전 둘 모두를 요구할 수 있다.

[0143] [0147] 제2 수정된 개별 레코드(100m2)의 콘텐츠는 변할 수 있다. 예컨대, 제2 수정된 개별 레코드(100m2)는, 제1 수정된 개별 레코드(100m1)의 블록(105b)을 포함할 수 있다. 다른 예로서, 제2 수정된 개별 레코드(100m2)는, 제1 수정된 개별 레코드(100m1)의 블록(105b)을 포함하지 않을 수 있다. 제2 수정된 개별 레코드(100m2)는 배서 블록(105c)을 포함할 수 있다. 예컨대, 배서는, 레코드 수신자의 공개 키(106b)와 함께, 제2 수정된 개별 레코드(100m2)만이 레코드 수신자(102b)에 의해 상환될 수 있다고 특정하는 "FPOE(for processing only endorsement)"(114b)일 수 있다 .

[0144] [0148] 제2 수정된 개별 레코드(100m2)를 싸인한 후, 레코드 수신자(102b)는 상호작용(916)에서 프로세싱 플랫폼(124)에 제2 수정된 개별 레코드(100m2)를 상환할 수 있다. 상환 시, 프로세싱 플랫폼(124)을 동작시키는 서비스 제공자(104)는 제2 수정된 개별 레코드(100m2) 내의 블록들(105a, 105b 및 105c)의 체인 내의 하나 이상의 서명들의 진본성을 검증함으로써 상호작용(920)에서 제2 수정된 개별 레코드(100m2)를 프로세싱할 수 있다. 예컨대, 프로세싱 플랫폼(124)은 레코드 전송자 서명(112a), 에이전트 서명(112d) 및 레코드 수신자 서명(112b)을 검증할 수 있다. 성공적인 검증 후, 프로세싱 플랫폼(124)은 제2 수정된 개별 레코드(100m2)의 콘텐츠 A(110a)에 의해 명령된 대로 수행할 수 있다.

[0145] [0149] 일부 실시예들에서, 프로세싱 플랫폼(124)은 제2 수정된 개별 레코드(100m2)가 성공적으로 프로세싱되었다는 것을 상호작용(924)에서 레코드 수신자 디바이스(116b)에 통보할 수 있다. 차례로, 레코드 수신자 디바이스(116b)는, 수정된 개별 레코드(100m1)가 예컨대 "HBE(handled by endorsement)"를 사용하여 성공적으로 프로세싱되었다는 것을 상호작용(928)에서 에이전트 디바이스(116d)에 통지할 수 있다.

[0146] [0150] 에이전트 디바이스(116d)는 미상환 개별 레코드들(208) 중 하나로서 에이전트 디바이스(116d)의 개별 레코드 컨테이너(202)에 저장된 수정된 개별 레코드(100m1)를 제거할 수 있다. 에이전트 디바이스(116d)는 개별 레코드(100)의 콘텐츠 A(110a)를, 예컨대 "record cleared"와 같은 메시지와 함께 외부 디바이스에 입력할 수 있다.

[0147] 구매자들/지불인들 및 판매자들/수취인들의 예시적인 콘텍스트

[0148] [0151] 일부 실시예들에서, 콘텐츠 요청(402)은 금액 B(110b)를 포함하는 지불 요청(402)일 수 있다. 개별 레코드들(100)은 디지털 수표들(100)을 포함할 수 있다. 개별 레코드(100)의 콘텐츠 A(110a)는 금액 A(110a)를 포함할 수 있다. 금액 B 및 금액 A는 동일하거나, 유사하거나, 상이할 수 있다. 금액은 명목 화폐, 암호화폐(예컨대, 비트코인), 금융 유가증권(예컨대, 주식 또는 채권), 또는 임의의 타입의 부동산, 무형의 자산, 또는 가상 자산일 수 있다. 레코드 ID(108)는 수표 ID(108)를 포함할 수 있다. 개별 레코드들(100)을 생성하는 것은 디지털 수표들(100)을 생성하는 것을 포함할 수 있고, 수정된 개별 레코드들(100m1)을 생성하는 것은 수정된 디지털 체크들(100m1)을 생성하는 것을 포함할 수 있다. "FPOE(for processing only endorsement)"는 "FDOE(for deposit only endorsement)"일 수 있다.

[0149] [0152] 레코드 전송자(102a)는 구매자 또는 지불인(102a)일 수 있고, 레코드 수신자(102b)는 판매자 또는 수취인(102b)일 수 있다. 레코드 전송자 디바이스(116a) 및 레코드 수신자 디바이스(116b)는 구매자 디바이스 또는 지불인 디바이스(116a) 및 판매자 디바이스 또는 수취인 디바이스(116b)일 수 있다. 개별 레코드(100)를 수반하는 교환은 레코드 전송자(102a)가, 예컨대, 레코드 수신자(102b)로부터 컴퓨터를 구매하는 것, 및 레코드 전송자(102a)가 컴퓨터의 구매 가격인 금액 A(110a)을 갖는 디지털 수표(100)로 그 구매를 지불하는 것일 수 있다. 도 9에 예시된 에이전트(102d)는 체커 또는 캐셔(102d)일 수 있다. 도 9에 예시된 레코드 수신자(102b)는 상인(102b)일 수 있다. 외부 디바이스는 PoS(point of sale) 시스템 또는 현금 등록기일 수 있다.

[0150] [0153] 공통 레코드 컨테이너(240) 내의 공통 레코드들(206)은 공통 회개장부 컨테이너(240) 내의 공통 회계장부(206)일 수 있다. 개별 레코드 컨테이너(202)에 저장된 미상환 개별 레코드들(208)은 월렛(202)에 저장된 미상환 수표들(208)일 수 있다.

[0151] [0154] 프로세싱 플랫폼(124)은 지불들을 프로세싱할 수 있다. 수정된 개별 레코드(100m1)의 콘텐츠(110)에 의해 명령된 대로 레코드 수신자(102b)에 대해 프로세싱 플랫폼(124)이 수행하는 것은 수정된 디지털 수표(100m1)에 의해 명령된 대로 금액 A(110a)을 수취인 디바이스에 제공하는 것을 포함할 수 있다. 중앙 레코드 컨테이너(332)는 중앙 회계장부(central ledger)일 수 있고, 중앙 레코드들(302)은 공통 회계장부를 포함할 수 있다. 사용자 레코드 상황(306)은 사용자 현재 잔액(306)을 포함할 수 있다.

[0152] 비용들/요금들의 예들

[0153] [0155] 사용자들(102a 또는 102b) 및 서비스 제공자(104) 이외의 제3 자들은 특정 활동들에 대한 요금들을 제3자에게 청구할 수 있다. 예컨대, 개별 레코드들(100)의 콘텐츠들(110)에 저장된 자신들의 문서 ID들을 갖는, 예컨대, 문서들을 유지하는 제3 자는 이러한 문서들에 액세스하기 위한 액세스 요금들을 프로세싱 플랫폼(124)에 청구할 수 있다. 결과적으로, 프로세싱 플랫폼(124)은 액세스 요금들을 사용자들(102a 또는 102b)에 청구할 수 있다.

[0154] [0156] 프로세싱 플랫폼(124)은 특정 거래들에 대한 거래 요금들을 청구할 수 있다. 예컨대, 프로세싱 플랫폼(124)은 개별 레코드들(100)을 프로세싱하기 위한 또는 사용자 계정들을 유지하기 위한 거래 요금들을 청구할 수 있다. 다른 예로서, 프로세싱 플랫폼(124)은 개별 레코드들(100)의 콘텐츠들(110)에 의해 명령된 대로 문서들에 액세스하기 위한 거래 요금들을 청구할 수 있다. 또 다른 예로서, 프로세싱 플랫폼(124)은, 개별 레코드들(100)의 콘텐츠들(110)에 저장된 자신들의 문서 ID들을 갖는 문서들에 대한 액세스를 레코드 수신자들에게 제공하기 위한 거래 요금들을 청구할 수 있다. 프로세싱 플랫폼(124)은 동일하거나 유사한 거래들, 이를테면, 동일하거나 유사한 문서들에 액세스하는 것에 대한 상이한 요금들을 상이한 사용자들에게 청구할 수 있다. 또 다른 예로서, 프로세싱 플랫폼(124)은 원하지 않는 거동들, 예컨대, 다른 사용자들이 액세스하지 않아야 할 때 문서들에 대한 액세스를 그들에게 그랜트하는 것에 대해 사용자들에게 청구할 수 있다. 거래 요금들이 거래 사이즈 또는 거래들의 수에 기반할 수 있거나, 또는 고정될 수 있거나, 또는 이들의 임의의 조합이 가능할 수 있다.

[0155] [0157] 프로세싱 플랫폼(124)은, 예컨대, 키 쌍들에 대한 유지보수 요금들을 에이전트들(102d)을 사용하여 레코드 수신자(102b)에게 청구할 수 있다. 유지보수 요금들은, 예컨대, 프로세싱 플랫폼(124)이 레코드 수신자(102b)에게 키 쌍들을 제공할 때, 한번 청구될 수 있거나, 주기적으로 청구될 수 있다. 청구 요금은 고정되거

나, 협상되거나, 할인되거나, 특혜가 있거나, 배타적이거나, 이들의 임의의 조합일 수 있다.

[0156] 예시적인 질의 배서

[0157] [0158] 일부 실시예들에서, 레코드 전송자는 네트워크에 연결될 수 없을지라도, 레코드 수신자는 네트워크에 연결될 수 있다. 예컨대, 레코드 전송자(102a) 및 레코드 수신자(102b)는 레코드 전송자의 영업 장소에서 개별 레코드(100)를 교환할 수 있다. 레코드 수신자(102b)에 의해 동작되는 레코드 수신자 디바이스(116b)는, 예컨대, 레코드 수신자(106b)에 의해 동작되는 사설 네트워크를 통해, 네트워크(118)에 연결될 수 있다. 그리고, 레코드 전송자(102a)에 의해 동작되는 레코드 전송자 디바이스(116a)는, 예컨대, 열악한 셀룰러 연결성 때문에 네트워크(118)에 연결되지 않을 수 있다. 개별 레코드(100)를 수반하는 교환을 수락하기 전에, 레코드 수신자(102b)는, 개별 레코드(100)가 프로세싱 플랫폼(124)에 전자적으로 통신되고 프로세싱 플랫폼(124)에 상환될 때, 프로세싱 플랫폼(124)이 개별 레코드(100)의 콘텐츠 A(110a)에 명령된 대로 수행할 것인지 여부에 관하여 프로세싱 플랫폼(124)에 전자적으로 질의할 수 있다. 예컨대, 콘텐츠 A(110a)는, 콘텐츠 A(110a)에 저장된 자신의 문서 ID를 갖는 문서에 대한 액세스를 레코드 수신자 디바이스(102b)에 제공할 수 있다. 수신자(102b)는, 레코드 전송자(102a)가 문서에 대한 액세스를 레코드 수신자(102b)에게 제공할 수 있다는 것을, 예컨대, 프로세싱 플랫폼(124)과의 "QE(query endorsement)"를 사용하여 검증할 수 있다.

[0158] [0159] 도 11은 질의 배서를 수반하는 개별 레코드들을 안전하게 교환 및 상환하는 일 실시예를 예시하는 상호작용 다이어그램이다. 도 4-도 5에 예시된 바와 같이, 레코드 수신자 디바이스(116b)를 사용하는 레코드 수신자(102b)는, 상호작용(404)에서 SRL(short range link)(122)을 사용하여 콘텐츠 요청(402)을 레코드 전송자 디바이스(116A)에 전송함으로써, 레코드 전송자(102A)로부터의 개별 레코드(100)를 요청할 수 있다. 콘텐츠 요청(402)은 레코드 수신자 디바이스의 공개 키(106b) 및 콘텐츠 B(110b)를 포함할 수 있다.

[0159] [0160] 상호작용(408)에서, 레코드 전송자 디바이스(116A)는 파트너 식별에 의해 레코드 수신자 디바이스(116b)의 아이덴티티를 확인할 수 있다. 레코드 전송자 디바이스(116A)의 SE(secure element)(204A)가 레코드 전송자의 인증 정보(512A)를 검증한 후에, 보안 엘리먼트(204A)는 상호작용(416)에서 개별 레코드(100)를 싸인할 수 있다. 상호작용(416)에서 개별 레코드(100)를 싸인하기 전에, 보안 엘리먼트(204A)는 레코드 전송자(102A)의 인증 및 디지털방식으로 싸인될 블록, 예컨대, 개별 레코드(100)의 블록(105A)의 프로비전 둘 모두를 요구할 수 있다.

[0160] [0161] 도 12는 질의 배서를 수반하는 예시적인 개별 레코드들을 개략적으로 예시한다. 도 11-도 12에 예시된 바와 같이, 개별 레코드(100)는 하나 이상의 블록들을 포함하는 디지털 객체일 수 있다. 개별 레코드(100)는 블록(105a)을 포함할 수 있다. 블록(105a)은 "from 필드" 내의 레코드 전송자 디바이스의 공개 키(106a), 레코드 수신자 디바이스의 공개 키(106b), "to 필드" 내의 레코드 ID(108), 콘텐츠 A(110a), 및 블록(105a)의 레코드 전송자 서명(112a)을 포함할 수 있다.

[0161] [0162] 도 11에 예시된 바와 같이, 상호작용(420)에서, 레코드 전송자(102a)는, 예컨대, SRL(short range link)(122)을 사용하는 피어-투-피어 방식으로 개별 레코드(100)를 레코드 수신자(102b)에 전송할 수 있다. 일단 레코드 수신자(102b)의 소유이면, 레코드 수신자(102b)는 상호작용(424)에서 개별 레코드(100)를 검증할 수 있다. 개별 레코드(100)를 검증하는 것은, 예컨대, 개별 레코드(100) 내의 레코드 전송자 디바이스의 공개 키(106a)를 사용하여 레코드 전송자 서명(112a)을 인증하는 것을 포함할 수 있다.

[0162] *예시적인 질의*

[0163] [0163] 도 11을 참조로, 개별 레코드(100)를 성공적으로 검증한 후에, 레코드 수신자 디바이스(116b)는, 자신의 보안 엘리먼트(204b)를 사용하여, 제1 수정된 개별 레코드(100m1)를 생성 및 싸인할 수 있다. 상호작용(1104)에서 제1 수정된 개별 레코드(100m1)를 싸인하기 전에, SE(secure element)(204b)는 레코드 수신자의 인증 정보(512b) 및 디지털방식으로 싸인될 블록, 예컨대, 수정된 개별 레코드(100m1)의 블록(105b)의 프로비전 둘 모두를 요구할 수 있다. 제1 수정된 개별 레코드(100m1)는 개별 레코드(100)의 블록(105a) 및 블록(105b)을 포함할 수 있다. 블록(105b)은 블록(105b)의 레코드 수신자 서명(112b) 및 배서를 포함할 수 있다. 예컨대, 배서는 "QE(query endorsement)(114a)"일 수 있다. "질의 배서(114a)"는, 제1 수정된 개별 레코드가 질의를 위한 것이지 상환을 위한 것이 아님을 표시할 수 있다. "질의 배서(114a)"는, 하나 이상의 조건들이 만족되면, 프로세싱 플랫폼(124)이 제1 수정된 개별 레코드(100m1)의 콘텐츠 A(110a)에 의해 명령된 대로 수행할 것인지 여부를 수신자 디바이스(102b)가 알기를 바란다는 것을 표시할 수 있거나 질의를 포함할 수 있다. 조건들의 비-제한적인 예들은, "FPOE(for processing only endorsement)"를 갖는 개별 레코드(100)에 기반하는 제2 수정된

개별 레코드(100m2)가 레코드 수신자(102b)에 전자적으로 통신되고 레코드 수신자(102b)에 의해 프로세싱 플랫폼(124)에 상환되는 것, 레코드 전송자(102a) 또는 레코드 수신자(102b)가 작업을 수행하는 것, 또는 특정 시간, 또는 또 다른 사용자 또는 비-사용자로부터 인가를 수신하는 것과 같은 이벤트의 발생을 포함한다. 일부 실시예들에서, 프로세싱 플랫폼(124)은 소싱 정보 및 요금 분할 정보를 레코드 수신자(102b)에 제공할 수 있다.

[0164] [0164] 제1 수정된 개별 레코드(100m1)를 싸인한 후에, 레코드 수신자(102b)는 상호작용(1108)에서 수정된 개별 레코드(100m1)를 프로세싱 플랫폼(124)에 전송할 수 있다. 상호작용(1112)에서 제1 수정된 개별 레코드(100m1) 내의 질의 배서(114a)를 프로세싱한 후에, 프로세싱 플랫폼(124)은 상호작용(1116)에서 질의 결과를 레코드 수신자(102b)에 제공할 수 있다. 예컨대, 질의 결과는, 프로세싱 플랫폼(124)이 제1 수정된 개별 레코드(100m1)의 콘텐츠 A(110a) 및 퍼포먼스의 타이밍에 의해 명령된 대로 수행하거나 수행하지 않을 것이라는 것을 표시할 수 있다. 다른 예로서, 질의 결과는, 하나 이상의 조건들이 만족되었다면, 프로세싱 플랫폼(124)이 콘텐츠 A(110a)에 의해 명령된 대로 수행할 것임일 수 있다. 또 다른 예로서, 질의 결과는 소스 정보 또는 비용을 포함할 수 있다.

[0165] *예시적인 개별 레코드 상환*

[0166] [0165] 도 11을 참조로, 질의 결과가 정해지면, 레코드 수신자(102b)는 레코드 전송자(102a)와의 개별 레코드(100)를 수반하는 교환을 수락할지 여부를 판단할 수 있다. 레코드 수신자(102b)가 교환을 수락하고, 프로세싱 플랫폼(124)에 개별 레코드(100)를 상환하기로 판단하면, 레코드 수신자 디바이스(116b)는, 자신의 보안 엘리먼트(204b)를 사용하여, 제2 수정된 개별 레코드(100m2)를 생성 및 싸인할 수 있다. 상호작용(428)에서 수정된 개별 레코드(100m1)를 싸인하기 전에, SE(secure element)(204b)는 레코드 수신자의 인증 정보(512b) 및 디지털방식으로 싸인될 블록, 예컨대, 제2 수정된 개별 레코드(100m2)의 블록(105c)의 프로비전 둘 모두를 요구할 수 있다. 수정된 개별 레코드(100m1)는 개별 레코드(100)의 블록(105a) 및 배서 블록(105c)을 포함할 수 있다. 블록(105c)은 블록(105c)의 레코드 수신자 서명(112b') 및 배서를 포함할 수 있다. 예컨대, 배서는, 수정된 개별 레코드(100m1)가 단지 레코드 수신자(102b)에 의해 상환될 수 있다는 것을 특정하는 "FPOE(for processing only endorsement)(114b)"일 수 있다. 일부 실시예들에서, 제2 수정된 개별 레코드(100m2)는 제1 수정된 개별 레코드(100m1)의 블록(105b)을 포함할 수 있다.

[0167] [0166] 제2 수정된 개별 레코드(100m2)를 싸인한 후에, 레코드 수신자(102b)는 상호작용(432)에서 프로세싱 플랫폼(124)에 제2 수정된 개별 레코드(100m2)를 상환할 수 있다. 상환 시에, 프로세싱 플랫폼(124)을 동작시키는 서비스 제공자(104)는, 수정된 개별 레코드(100m1) 내의 블록들(105a 및 105c)의 체인 내의 하나 이상의 서명들의 진본성을 검증함으로써 제2 수정된 개별 레코드(100m2)를 상호작용(436)에서 프로세싱할 수 있다. 인증된 서명들은 레코드 전송자 서명(112a) 및 제2 레코드 수신자 서명(112b)을 포함할 수 있다. 성공적 검증 후에, 프로세싱 플랫폼(124)은 제2 수정된 개별 레코드(100m2)의 콘텐츠 A(110a)에 의해 명령된 대로 수행할 수 있다.

[0168] [0167] 완벽한 것으로 고려되는 개별 레코드(100)를 수반하는 교환의 타이밍은 상이한 구현들에서 상이할 수 있다. 예컨대, 개별 레코드(100)를 수반하는 교환은, 상호작용(1116)에서 질의 결과를 수신한 후에, 레코드 수신자(102b)가 레코드 전송자(102a)와의 개별 레코드(100)를 수반하는 교환을 수락할 때, 완벽한 것으로 고려될 수 있다. 질의 결과는, 프로세싱 플랫폼(124)이 제1 수정된 개별 레코드(100m1)의 콘텐츠 A(110a) 및 퍼포먼스의 타이밍에 의해 명령된 대로 수행할 것이라는 것을 표시할 수 있다. 다른 예로서, 개별 레코드(100)를 수반하는 교환은, 프로세싱 플랫폼(124)을 동작시키는 서비스 제공자(104)가 제2 수정된 개별 레코드(100m2)를 상호작용(436)에서 성공적으로 프로세싱할 때, 완벽한 것으로 고려될 수 있다. 프로세싱 플랫폼(124)은 수정된 개별 레코드(100m1) 내의 블록들(105a 및 105c)의 체인 내의 하나 이상의 서명들의 진본성을 검증할 수 있다. 또 다른 예로서, 개별 레코드(100)를 수반하는 교환은, 중앙 플랫폼(124)이 제2 수정된 개별 레코드(100m2)의 콘텐츠 A(110a)에 의해 명령된 대로 수행할 때, 완벽한 것으로 고려될 수 있다.

[0169] 공통 레코드들의 예시적인 분배

[0170] *업데이트들의 예시적인 빈도*

[0171] [0168] 프로세싱 플랫폼(124)은, 업데이트된 공통 레코드들(206)을 하나 이상의 사용자 디바이스들에 전송함으로써 때때로 또는 규칙적 인터벌로 공통 레코드들(206)을 업데이트할 수 있다. 일부 실시예들에서, 규칙적 인터벌들은 시간-기반, 예컨대, 매시간, 매일, 매주 또는 매달일 수 있다.

[0172] [0169] 일부 실시예들에서, 규칙적 인터벌들은 변경된 상황에서 사용자들 또는 사용자 디바이스들의 수 또는

퍼센티지에 기반할 수 있다. 변경된 상황의 비-제한적인 예들은 디바이스가 사용자 디바이스(116)가 되는 것, 디바이스(116)가 더 이상 사용자 디바이스가 아닌 것, 사용자(102a 또는 102b) 또는 사용자 디바이스(116)가 디메리트 리스트(demerit list)(디메리트들이 아래에서 설명될 것임)로부터 부가 또는 제거되는 것, 디메리트 리스트 상의 사용자(102a 또는 102b) 또는 사용자 디바이스(116a 또는 116b)의 디메리트 상황이 변한 것, 이를테면, 디메리트 포인트들의 증가 또는 감소, 또는 사용자(102a 또는 102b) 또는 사용자 디바이스(116)가 블랙리스트로부터 부가 또는 제거되는 것을 포함한다. 예컨대, 변경된 상황에서 사용자들 또는 사용자 디바이스들(116)의 수는 100일 수 있다. 다른 예로서, 변경된 상황에서 사용자들 또는 사용자 디바이스들(116)의 퍼센티지는 모든 사용자들 또는 사용자 디바이스들(116) 중 1%일 수 있다.

[0173] [0170] 일부 실시예들에서, 규칙적 인터벌들은 프로세싱 플랫폼(124)의 에러 관리자에 의해 검출되거나 사용자 디바이스들(116)의 에러 관리자들에 의해 결정된 에러 이벤트들의 수, 예컨대, 100개의 에러 이벤트들에 기반할 수 있다. 에러 이벤트는, 예컨대, 프로세싱 플랫폼이 "MC(malicious code)" 배서(아래에서 추가로 설명됨)를 갖는 개별 레코드를 수신하는 것일 수 있다.

[0174] *프로세싱 플랫폼으로부터 수신된 예시적인 공통 레코드들*

[0175] [0171] 도 13은 프로세싱 플랫폼(124)으로부터의 공통 레코드들(206)을 분배하는 일 실시예를 예시하는 상호작용 다이어그램이다. 상호작용(1304)에서, 프로세싱 플랫폼(124)은, 예컨대, 공통 레코드 생성기를 사용하여, 공통 레코드 메시지(1308)를 생성할 수 있다. 도 14는 분배를 위한 예시적인 공통 레코드들을 개략적으로 예시한다. 도 13-도 14에 예시된 바와 같이, 공통 레코드 메시지(1308)는, 디바이스들(214)의 업데이트된 공개 키들을 포함할 수 있는 업데이트된 공통 레코드들(206)을 포함할 수 있다. 공통 레코드 메시지(1308)는 디메리트 리스트(1402) 및 블랙리스트(1404)를 포함할 수 있다. 프로세싱 플랫폼(124)은, 서비스 제공자 서명(1312)을 공통 레코드 메시지(1308)에 부가함으로써 공통 레코드 메시지(1308)를 싸인할 수 있다. 서비스 제공자 서명(1312)은 서비스 제공자 소유의 서비스 제공자 개인 키(348)를 사용하여 공통 레코드 생성기(340)에 의해 생성될 수 있다.

[0176] [0172] 프로세싱 플랫폼(124)의 공통 레코드 분배기는 공통 레코드 메시지(1308)를 사용자 디바이스들에 분배할 수 있다. 프로세싱 플랫폼(124)은 공통 레코드 메시지(1308)를 사용자 디바이스들로 순차적으로 분배할 수 있다. 예컨대, 프로세싱 플랫폼(124)은, 상호작용(1316a)에서, 처음에 공통 레코드 메시지(1308)를 레코드 수신자 디바이스(102b)에 분배하고, 이후에 상호작용(1316b)에서 레코드 전송자 디바이스(102a)에 분배할 수 있다. 그러한 순차적 분배는 유리하게 트래픽 혼잡 및 대역폭 병목현상을 피할 수 있다. 레코드 전송자 디바이스(102a) 및 레코드 수신자 디바이스(102b)의 공통 레코드 수신자들은 프로세싱 플랫폼(124)으로부터 공통 레코드 메시지(1308)를 수신할 수 있다.

[0177] [0173] 프로세싱 플랫폼(124)은 동시에 또는 가까운 시간에 공통 레코드 메시지(1308)를 하나 이상의 사용자 디바이스들(116)에 분배할 수 있다. 예컨대, 공통 레코드 분배기는 공통 레코드 메시지(1308)를 100개의 사용자 디바이스들(116)로 동시에 분배할 수 있다. 다른 예로서, 공통 레코드 분배기(344)는 공통 레코드 메시지(1308)를 사용자 디바이스들(116) 중 10%에 동시에 분배할 수 있다. 또 다른 예로서, 공통 레코드 분배기(344)는 공통 레코드 메시지(1308)를 사용자 디바이스들(116)에 100개의 배치들(batches)로 분배할 수 있다.

[0178] [0174] 상호작용(1320)에서, 레코드 수신자 디바이스(102b)의 SE(secure element)(130b)는 공통 레코드 메시지(1308)의 진본성을 검증할 수 있다. 공통 레코드 메시지(1308)의 진본성을 검증하는 것은 서비스 제공자 서명(1308)을 검증하는 것을 포함할 수 있다. 서비스 제공자 서명(1308)을 검증하는 것은, 보안 엘리먼트(204b)에 저장된 서비스 제공자 공개 키(212)를 사용하여, 서비스 제공자 서명(1308)이 서비스 제공자 개인 키(348)를 사용하여 생성되었는지 여부를 결정하는 것을 포함할 수 있다. 유사하게, 상호작용(1328)에서, 레코드 전송자 디바이스(102a)의 보안 엘리먼트(204a)는 공통 레코드 메시지(1308)의 진본성을 검증할 수 있다.

[0179] *레코드 수신자로부터 수신된 예시적인 공통 레코드들*

[0180] [0175] 사용자 디바이스들, 예컨대, 레코드 수신자 디바이스는, 프로세싱 플랫폼(124)으로부터 공통 레코드 메시지(1308)를 수신한 후에, 레코드 전송자 디바이스를 포함하여, 다른 사용자 디바이스들에 공통 레코드 메시지(1308)를 전파할 수 있다. 예컨대, 공통 레코드 메시지(1308)를 수신한 사용자 디바이스들은, 공통 레코드 메시지(1308)를 수신한 후 일정 시간 기간 동안 또는 프로세싱 플랫폼(124)으로부터 새로운 공통 레코드 메시지를 수신할 때까지 연속해서, 수신된 공통 레코드 메시지(1308)를 다른 사용자 디바이스들에 브로드캐스팅할 수 있다.

[0181] [0176] 도 15는 레코드 수신자 디바이스에 의한 공통 레코드들의 전파의 예를 예시하는 상호작용 다이어그램이다. 상호작용(1304)에서 공통 레코드 메시지(1308)를 생성 및 싸인한 후에, 프로세싱 플랫폼(124)은 상호작용(1316)에서 사용자 디바이스들, 예컨대, 레코드 수신자 디바이스(102b)에 공통 레코드 메시지(1308)를 분배할 수 있다. 상호작용(1320)에서, 레코드 수신자 디바이스(102b)의 SE(secure element)(204b)는 공통 레코드 메시지(1308)의 진본성을 검증할 수 있다.

[0182] [0177] 개별 레코드, 예컨대, 도 4-도 12에 예시된 개별 레코드(100)를 교환하기 이전에, 레코드 전송자 디바이스(102a)는 프로세싱 플랫폼(124) 또는 임의의 다른 사용자 디바이스(116)로부터 공통 레코드 메시지(1308)를 수신하지 않았을 수 있다. 상호작용(1504)에서, 레코드 수신자 디바이스(102b)는, 공통 레코드 메시지(1308)를 레코드 전송자 디바이스(102a)에 전송하도록 제안하고 전송함으로써, 공통 레코드 메시지(1308)를 전파할 수 있다. 레코드 수신자 디바이스(102b)로부터 레코드 전송자 디바이스(102a)에서 수신된 공통 레코드 메시지(1308)는 레코드 수신자 디바이스의 서명을 포함할 수 있다. 상호작용(1508)에서, 레코드 전송자 디바이스(102a)의 SE(secure element)(204a)는 공통 레코드 메시지(1308)의 진본성을 검증할 수 있다.

[0183] *레코드 전송자로부터 수신된 예시적인 공통 레코드들*

[0184] [0178] 사용자 디바이스들, 예컨대, 레코드 전송자 디바이스는, 프로세싱 플랫폼(124)으로부터 공통 레코드들(206)을 수신한 후에, 레코드 수신자 디바이스를 포함하여, 다른 사용자 디바이스들에 공통 레코드들(206)을 전파할 수 있다. 도 16은 레코드 전송자 디바이스에 의한 공통 레코드들의 전파의 예를 예시하는 상호작용 다이어그램이다. 상호작용(1304)에서 공통 레코드 메시지(1308)를 생성 및 싸인한 후에, 프로세싱 플랫폼(124)은 상호작용(1316)에서 사용자 디바이스들, 예컨대, 레코드 전송자 디바이스(102b)에 공통 레코드 메시지(1308)를 분배할 수 있다. 상호작용(1328)에서, 레코드 전송자 디바이스(102a)의 SE(secure element)(204a)는 공통 레코드 메시지(1308)의 진본성을 검증할 수 있다.

[0185] [0179] 개별 레코드, 예컨대, 도 4-도 12에 예시된 개별 레코드(100)를 교환하기 이전에, 레코드 수신자 디바이스(102b)는 프로세싱 플랫폼(124) 또는 임의의 다른 사용자 디바이스(116)로부터 공통 레코드 메시지(1308)를 수신하지 않았을 수 있다. 예컨대, 레코드 전송자 디바이스(116a)는 새로운 사용자 디바이스일 수 있고, 레코드 수신자 디바이스(116b)는 레코드 전송자 디바이스의 공개 키(106a)를 소유하지 않을 수 있다. 레코드 전송자 디바이스의 공개 키(106)를 포함하는 공통 레코드 메시지(1308)를 수신하지 않고서, 레코드 수신자(102b)는, 레코드 전송자 디바이스(116a)가 유효한 사용자 디바이스라는 것을 검증하지 못할 수 있다.

[0186] [0180] 상호작용(1504)에서, 레코드 전송자 디바이스(102a)는, 공통 레코드 메시지(1308)를 레코드 수신자 디바이스(102b)에 전송하도록 제안하고 전송함으로써, 공통 레코드 메시지(1308)를 전파할 수 있다. 상호작용(1508)에서, 레코드 수신자 디바이스(102b)의 SE(secure element)(204b)는 공통 레코드 메시지(1308)의 진본성을 검증할 수 있다. 그러한 전파는 유리하게, 레코드 전송자 디바이스(102a)로부터 공통 레코드 메시지(1308)를 수신하기 이전에, 레코드 수신자 디바이스(102b)가 레코드 전송자 디바이스의 공개 키(102a)를 소유하지 않을 수 있을지라도, 개별 레코드의 교환을 할 수 있게 한다.

[0187] 예시적인 에러 관리

[0188] [0181] 프로세싱 플랫폼(124)이 사용자 디바이스들로부터 수신하는 개별 레코드들은 의도된 또는 의도되지 않은 에러들을 포함할 수 있다. 사용자들은, 무효 개별 레코드들, 예컨대, 무효 서명들을 갖는 개별 레코드들을 생성함으로써 악의적으로 거동할 수 있다. 부도덕한 사용자들은, 예컨대, 다른 사용자들로 하여금 무효 개별 레코드들을 생성하게 함으로써, 다른 사용자들로 하여금 악의적인 사용자들처럼 보이게 할 수 있다.

[0189] *다수의 수신자들에 대한 예시적인 전송자 클로닝*

[0190] [0182] 일부 실시예들에서, 악의적인 레코드 전송자는 개별 레코드를 2명의 상이한 레코드 수신자들에 전송할 수 있다. 도 17은 다수의 수신자들에 대한 전송자 클로닝으로 지칭될 수 있는 이러한 악의적인 거동을 예시하는 상호작용 다이어그램이다. 제1 레코드 수신자 디바이스(116b)를 사용하는 제1 레코드 수신자(102b)는, 상호작용(404)에서 SRL(short range link)(122)을 사용하여 제1 콘텐츠 요청(402)을 제1 레코드 전송자 디바이스(116a)에 전송함으로써, 레코드 전송자(102a)로부터의 개별 레코드를 요청할 수 있다. 제1 콘텐츠 요청(402)은 제1 레코드 수신자 디바이스의 제1 공개 키(106b) 및 콘텐츠 B(110b)를 포함할 수 있다. 제2 레코드 수신자 디바이스(116c)를 사용하는 제2 레코드 수신자(102c)는, 상호작용(1704)에서 단거리 링크(122)를 사용하여 제2 콘텐츠 요청(1702)을 레코드 전송자 디바이스(116a)에 전송함으로써, 레코드 전송자(102a)로부터의 개별 레코드를 요청할 수 있다. 제2 콘텐츠 요청(402)은 제2 레코드 수신자 디바이스의 제2 공개 키(106c) 및 콘텐츠 C(110

c)를 포함할 수 있다. 레코드 전송자(102a)는, 제2 콘텐츠 요청(1702)을 수신하기 이전에, 이에 후속하여, 또는 동시에 제1 콘텐츠 요청(402)을 수신할 수 있다.

[0191] [0183] 레코드 전송자 디바이스(116a)의 SE(secure element)(204a)는, 상호작용(420)에서 개별 레코드(100)의 제1 카피를 제1 레코드 수신자 디바이스(116b)에 전송하기 이전에 상호작용(416)에서 개별 레코드(100)를 생성 및 싸인할 수 있다. 상호작용(424)에서 개별 레코드(100)의 성공적 검증 후에, 제1 레코드 수신자 디바이스(116b)는 상호작용(432)에서 개별 레코드(100)를 프로세싱 플랫폼(124)에 상환할 수 있다. 상환 시에, 프로세싱 플랫폼(124)을 동작시키는 서비스 제공자(104)는, 상환된 개별 레코드(100) 내의 하나 이상의 서명들의 진본성을 검증함으로써 상호작용(436)에서 개별 레코드(100)를 프로세싱할 수 있다. 성공적 검증 후에, 프로세싱 플랫폼(124)은 개별 레코드(100)의 콘텐츠 A(110a)에 의해 명령된 대로 수행될 수 있다.

[0192] [0184] 상호작용(416)에서 개별 레코드(100)를 생성 및 싸인한 후에, 레코드 전송자 디바이스(116a)는 또한, 상호작용(1720)에서 개별 레코드(100)의 제2 카피를 제2 레코드 수신자 디바이스(116b)에 전송할 수 있다. 레코드 전송자(102a)는, 개별 레코드(100)의 다른 카피를 제2 레코드 수신자(102c)에 전송하기 이전에, 그에 후속하여, 또는 그와 동시에 개별 레코드(100)의 카피를 제1 레코드 수신자(102b)에 전송할 수 있다.

[0193] [0185] 콘텐츠 B(100b) 및 콘텐츠 C(100c)는, 제1 콘텐츠 요청(402) 및 제2 콘텐츠 요청(1702)을 각각 충족하는 것으로 콘텐츠 A(100a)가 제1 레코드 수신자(102b) 및 제2 레코드 수신자(102c)에 나타날 수 있도록 동일하거나 또는 유사할 수 있다. 그러나, 상호작용(1724)에서 제2 레코드 수신자(116c)에 의한 개별 레코드(100)의 검증은, 개별 레코드(100)가 제1 레코드 수신자 디바이스의 공개 키(106b)를 포함하고 제2 레코드 수신자 디바이스의 공개 키(106c)를 포함하지 않을 수 있기 때문에 실패할 수 있다. 이것은, 개별 레코드(100)가 제2 레코드 수신자(102c)가 아니라 제1 레코드 수신자(102b)에 대해 의도된다는 것을 표시할 수 있다. 실패한 검증 때문에, 제2 레코드 수신자(106c)는 레코드 전송자(102a)와의 제2 콘텐츠 요청(1702)을 수반하는 교환을 거절할 수 있다. 일부 실시예들에서, 실패한 검증 후에, 제2 레코드 전송자 디바이스(116c)는, 상호작용(1728)에서 프로세싱 플랫폼(124)에 "MRE(malicious record endorsement)"를 전송하기 이전에 그것을 개별 레코드(100)에 부가할 수 있다.

[0194] *단일 수신자에 대한 예시적인 전송자 클로닝*

[0195] [0186] 일부 실시예들에서, 악의적인 레코드 전송자는 동일한 개별 레코드의 2개의 카피들을 하나의 레코드 수신자에 전송할 수 있다. 도 18은, 단일 수신자에 대한 전송자 클로닝으로 지칭될 수 있는 이러한 악의적인 거동을 예시하는 상호작용 다이어그램이다. 레코드 수신자 디바이스(116b)를 사용하는 레코드 수신자(102b)는, 상호작용(404)에서 SRL(short range link)(122)을 사용하여 제1 콘텐츠 요청(402)을 레코드 전송자 디바이스(116a)에 전송함으로써, 레코드 전송자(102a)로부터의 개별 레코드를 요청할 수 있다. 제1 콘텐츠 요청(402)은 레코드 수신자 디바이스의 콘텐츠 B(110b) 및 공개 키(106b)를 포함할 수 있다. 유사하게, 레코드 수신자(102b)는, 상호작용(1804)에서 단거리 링크(122)를 사용하여 제2 콘텐츠 요청(1802)을 레코드 전송자 디바이스(116a)에 전송함으로써, 레코드 전송자(102a)로부터의 다른 개별 레코드를 요청할 수 있다. 제2 콘텐츠 요청(1802)은 레코드 수신자 디바이스의 콘텐츠 B'(110b') 및 공개 키(106b)를 포함할 수 있다. 레코드 수신자(102b)는 제1 콘텐츠 요청(402) 및 제2 콘텐츠 요청(1802)을 동시에 또는 상이한 시간들에 전송할 수 있다.

[0196] [0187] 레코드 전송자 디바이스(116a)의 SE(secure element)(204a)는, 상호작용(420)에서 개별 레코드(100)의 제1 카피를 레코드 수신자 디바이스(116b)에 전송하기 이전에 상호작용(416)에서 개별 레코드(100)를 생성 및 싸인할 수 있다. 개별 레코드(100)의 레코드 ID는, 예컨대 N일 수 있다. 상호작용(424)에서 개별 레코드(100)의 성공적 검증 후에, 레코드 수신자 디바이스(116b)는 상호작용(432)에서 개별 레코드(100)를 프로세싱 플랫폼(124)에 상환할 수 있다. 상환 시에, 프로세싱 플랫폼(124)을 동작시키는 서비스 제공자(104)는, 상환된 개별 레코드(100)내의 하나 이상의 서명들의 진본성을 검증함으로써 상호작용(436)에서 개별 레코드(100)를 프로세싱할 수 있다. 성공적 검증 후에, 프로세싱 플랫폼(124)은 개별 레코드(100)의 콘텐츠 A(110a)에 의해 명령된 대로 수행할 수 있다.

[0197] [0188] 상호작용(1820)에서, 레코드 전송자 디바이스(116a)는 개별 레코드(100)의 제2 카피를 레코드 수신자 디바이스(116b)에 전송할 수 있다. 콘텐츠 B(100b) 및 콘텐츠 B'(100b')는, 제1 콘텐츠 요청(402) 및 제2 콘텐츠 요청(1802)을 충족하는 것으로 콘텐츠 A(100a)가 레코드 수신자(102b)에 나타날 수 있도록 동일하거나 또는 유사할 수 있다.

[0198] [0189] 그러나, 상호작용(1820)에서 레코드 수신자(116b)에 의한 개별 레코드(100)의 제2 카피의 검증은 실패

할 수 있다. 각각의 사용자 디바이스 -각각의 사용자 디바이스로부터 레코드 수신자 디바이스(116b)가 하나 이상의 개별 레코드들을 수신했음-에 대해, 레코드 수신자 디바이스(116b)의 레코드 히스토리 추적기는 사용자 디바이스로부터 수신된 마지막 개별 레코드의 레코드 ID를 계속해서 추적할 수 있다. 예컨대, 레코드 히스토리 추적기는, 그것이 레코드 전송자 디바이스(116a)로부터 수신했던 마지막 개별 레코드(100)의 레코드 ID(108) N을 계속해서 추적할 수 있다. 따라서, 레코드 전송자 디바이스(116a)는 동일한 레코드 ID(108) N을 포함하는 개별 레코드(100)의 제2 카피를 레코드 수신자 디바이스(116b)에 전송하지 않아야 한다.

[0199] [0190] 일부 실시예들에서, 각각의 사용자 디바이스 -각각의 사용자 디바이스로부터 레코드 수신자 디바이스(116b)가 하나 이상의 개별 레코드들을 수신했음-에 대해, 레코드 히스토리 추적기는 수신된 가장 큰 레코드 ID(108)를 갖는 개별 레코드(100)를 계속해서 추적할 수 있다. 유리하게, 각각의 사용자 디바이스 - 각각의 사용자 디바이스로부터 레코드 수신자 디바이스(116b)가 하나 이상의 개별 레코드들을 수신했음 - 에 대해, 하나의 레코드 전송자에 의해 생성된 개별 레코드들의 레코드 ID들(108)이 단조적으로 증가하고 있을 수 있기 때문에, 레코드 수신자 디바이스(116b)는 사용자 디바이스로부터 수신된 마지막 개별 레코드(100)의 레코드 ID(108)만을 계속해서 추적할 수 있다. 일부 실시예들에서, 레코드 히스토리 추적기는 수신된 모든 개별 레코드들의 레코드 ID들(108)을 계속해서 추적할 수 있다.

[0200] [0191] 실패한 검증 때문에, 레코드 수신자(106b)는 레코드 전송자(102a)와의 제2 콘텐츠 요청(1802)을 수반하는 교환을 거절할 수 있다. 일부 실시예들에서, 실패한 검증 후에, 레코드 전송자 디바이스(116b)는, 상호작용(1828)에서 프로세싱 플랫폼(124)에 "악의적인 레코드 배서"를 전송하기 이전에 이를 개별 레코드(100)의 제2 카피에 부가할 수 있다.

[0201] *예시적인 포킹*

[0202] [0192] 일부 실시예들에서, 악의적인 레코드 수신자는 개별 레코드를 배서하기 전에 개별 레코드를 카피하고, 개별 레코드의 저장된 카피를 제2 레코드 수신자에게 전송하려고 시도할 수 있다. 도 19는, 포킹으로 지칭될 수 있는 이러한 악의적인 거동을 예시하는 상호작용 다이어그램이다. 제1 레코드 수신자 디바이스(116b)를 사용하는 제1 레코드 수신자(102b)는, 상호작용(404)에서 SRL(short range link)(122)을 사용하여 제1 콘텐츠 요청(402)을 제1 레코드 전송자 디바이스(116a)에 전송함으로써, 제1 레코드 전송자(102a)로부터의 개별 레코드를 요청할 수 있다. 제1 콘텐츠 요청(402)은 제1 레코드 수신자 디바이스의 콘텐츠 B(110b) 및 공개 키(106b)를 포함할 수 있다.

[0203] [0193] 제1 레코드 전송자 디바이스(116a)의 SE(secure element)(204a)는, 상호작용(420)에서 개별 레코드(100)를 제1 레코드 수신자 디바이스(116b)에 전송하기 이전에 상호작용(416)에서 개별 레코드(100)를 생성 및 싸인할 수 있다. 상호작용(424)에서 개별 레코드(100)의 성공적 검증 후에, 제1 레코드 수신자 디바이스(116b)는 상호작용(428)에서 제1 레코드 수신자 서명(112b)을 이용하여 수정된 개별 레코드(100m1)를 생성할 수 있다. 상호작용(432)에서의 프로세싱 플랫폼(124)에 수정된 개별 레코드(100m1)의 상환 시에, 프로세싱 플랫폼(124)을 동작시키는 서비스 제공자(104)는 수정된 개별 레코드(100m1) 내의 하나 이상의 서명들의 진본성을 검증함으로써 상호작용(436)에서 수정된 개별 레코드(100m1)를 프로세싱할 수 있다. 성공적 검증 후에, 프로세싱 플랫폼(124)은 수정된 개별 레코드(100m1)의 콘텐츠 A(110a)에 의해 명령된 대로 수행될 수 있다.

[0204] [0194] 제2 레코드 수신자 디바이스(116c)를 사용하는 제2 레코드 수신자(102c)는, 제2 콘텐츠 요청(1902)을 제1 레코드 수신자 디바이스(116b)에 전송함으로써, 제1 레코드 수신자(102b)로부터의 개별 레코드를 요청할 수 있다. 제1 레코드 수신자(102b)는 제2 레코드 전송자(102b)일 수 있고, 제1 레코드 전송자 디바이스(116b)는 제2 레코드 전송자 디바이스(116b)로 지칭될 수 있다. 제2 콘텐츠 요청(1902)은 제2 레코드 수신자 디바이스의 콘텐츠 C(110c) 및 공개 키(106c)를 포함할 수 있다.

[0205] [0195] 제2 레코드 전송자 디바이스(116b)는 상호작용(1916)에서 개별 레코드(100)의 카피를 제2 레코드 수신자 디바이스(116c)에 전송할 수 있다. 그러나, 상호작용(1920)에서 제2 레코드 수신자(116c)에 의한 개별 레코드(100)의 검증은, 개별 레코드(100)가 제2 레코드 전송자 디바이스의 공개 키(106b)를 포함하고 제2 레코드 수신자 디바이스의 공개 키(106c)를 포함하지 않을 수 있기 때문에 실패할 수 있다. 이것은, 개별 레코드(100)가 제2 레코드 수신자(102c)가 아니라 제1 레코드 수신자(102b)에 대해 의도된다는 것을 의미할 수 있다. 실패한 검증 때문에, 제2 레코드 수신자(106c)는 제2 레코드 전송자(102b)와의 제2 콘텐츠 요청(1902)을 수반하는 교환을 거절할 수 있다. 일부 실시예들에서, 실패한 검증 후에, 제2 레코드 전송자 디바이스(116c)는, 상호작용(1924)에서 프로세싱 플랫폼(124)에 "악의적인 레코드 배서"를 전송하기 이전에 그것을 개별 레코드(100)에 부가할 수 있다.

[0206] *예시적인 수신자 클로닝*

[0207] [0196] 일부 실시예들에서, 악의적인 레코드 수신자는 개별 레코드를 2번 상환하려고 시도할 수 있다. 일부 실시예들에서, 악의적인 레코드 수신자는, 단일 수신자에 대한 레코드 전송자 클로닝의 레코드 전송자를 고발하려고 시도할 시에 개별 레코드를 2번 상환할 수 있다. 도 20은, 수신자 클로닝으로 지칭될 수 있는 이러한 악의적인 거동을 예시하는 상호작용 다이어그램이다. 레코드 수신자 디바이스(116b)를 사용하는 레코드 수신자(102b)는, 상호작용(404)에서 SRL(short range link)(122)을 사용하여 콘텐츠 요청(402)을 레코드 전송자 디바이스(116a)에 전송함으로써, 레코드 전송자(102a)로부터의 개별 레코드를 요청할 수 있다. 콘텐츠 요청(402)은 레코드 수신자 디바이스의 콘텐츠 B(110b) 및 공개 키(106b)를 포함할 수 있다.

[0208] [0197] 레코드 전송자 디바이스(116a)의 SE(secure element)(204a)는, 상호작용(420)에서 개별 레코드(100)를 레코드 수신자 디바이스(116b)에 전송하기 이전에 상호작용(416)에서 레코드 ID(108) N을 갖는 개별 레코드(100)를 생성 및 싸인할 수 있다. 424에서의 개별 레코드(100)의 성공적 검증 후에, 레코드 수신자 디바이스(116b)는, 상호작용(432)에서 수정된 개별 레코드(100m1)의 제1 카피를 프로세싱 플랫폼(124)에 상환하기 이전에 상호작용(428)에서 레코드 수신자 서명(112b)을 이용하여 수정된 개별 레코드(100m1)를 생성할 수 있다. 상환 시에, 프로세싱 플랫폼(124)을 동작시키는 서비스 제공자(104)는, 수정된 개별 레코드(100m1) 내의 하나 이상의 서명들의 진본성을 검증함으로써 상호작용(436)에서 수정된 개별 레코드(100m1)를 프로세싱할 수 있다. 성공적 검증 후에, 프로세싱 플랫폼(124)은 개별 레코드(100)의 콘텐츠 A(110a)에 의해 명령된 대로 수행할 수 있다.

[0209] [0198] 레코드 전송자 디바이스(116b)는 상호작용(2032)에서 수정된 개별 레코드(100m1)의 제2 카피를 프로세싱 플랫폼(124)에 상환하려고 시도할 수 있다. 그러나, 수정된 개별 레코드(100m1)의 제2 카피의 프로세싱은 상호작용(2036)에서 실패할 수 있다. 프로세싱 플랫폼(124)은 상호작용(436)에서 수정된 개별 레코드(100m1)의 제1 카피를 이전에 성공적으로 프로세싱했다. 각각의 레코드 전송자 디바이스에 대해, 중앙 레코드들(302)의 사용자 레코드 상황(306)은, 프로세싱 플랫폼(302)이 프로세싱했던 개별 레코드들의 레코드 ID들을 포함할 수 있다. 예컨대, 레코드 전송자 디바이스(116a)에 대해, 중앙 레코드들(302)의 사용자 레코드 상황(306)은 수정된 개별 레코드(100m1)의 레코드 ID(108) N을 포함할 수 있다. 레코드 전송자 디바이스(116b)가 동일한 레코드 ID(108) N을 갖는 수정된 개별 레코드(100m1)의 제2 카피를 상환하려고 시도할 때, 프로세싱 플랫폼(124)은, 수정된 개별 레코드(100m1)의 레코드 ID(108) N과 사용자 레코드 상황(306)을 비교함으로써 이러한 악의적인 상환을 검출할 수 있다.

[0210] *예시적인 마우징*

[0211] [0199] 일부 실시예들에서, 악의적인 레코드 전송자는 자신의 레코드 전송자 디바이스의 SE(secure element)를 우회함으로써 부적합한 서명들을 이용하여 개별 레코드들을 생성할 수 있다. 도 21은, 마우징으로 지칭될 수 있는 이러한 악의적인 거동을 예시하는 상호작용 다이어그램이다. 레코드 수신자 디바이스(116b)를 사용하는 레코드 수신자(102b)는, 상호작용(404)에서 SRL(short range link)(122)을 사용하여 콘텐츠 요청(402)을 레코드 전송자 디바이스(116a)에 전송함으로써, 레코드 전송자(102a)로부터의 개별 레코드를 요청할 수 있다. 콘텐츠 요청(402)은 레코드 수신자 디바이스의 콘텐츠 B(110b) 및 공개 키(106b)를 포함할 수 있다.

[0212] [0200] 자신의 SE(secure element)(204a)를 해킹 또는 우회함으로써, 레코드 전송자 디바이스(116a)는, 상호작용(420)에서 개별 레코드(100)를 레코드 수신자 디바이스(116b)에 전송하기 이전에 상호작용(416)에서 부적합한 서명(112a')을 이용하여 개별 레코드(100)를 생성할 수 있다. 부적합한 서명(112')은 랜덤 서명일 수 있거나 또는 레코드 전송자 디바이스(106b)와 연관되지 않은 개인 키를 사용하여 생성될 수 있다.

[0213] [0201] 상호작용(424)에서 레코드 수신자(116b)에 의한 개별 레코드(100)의 검증은 실패할 수 있다. 레코드 수신자 디바이스(116b)는, 부적합한 서명(112')이 레코드 전송자 디바이스의 개인 키(210a)를 사용하여 생성되었다고 결정할 수 없다. 레코드 수신자 디바이스(116b)는, 레코드 전송자 디바이스의 공개 키(106a)를 사용하여 부적합한 서명(112')을 암호해독할 수 없다. 실패한 검증 때문에, 레코드 수신자(106b)는 레코드 전송자(102a)와의 콘텐츠 요청(402)을 수반하는 교환을 거절할 수 있다. 일부 실시예들에서, 실패한 검증 후에, 레코드 전송자 디바이스(116b)는, 상호작용(2124)에서 프로세싱 플랫폼(124)에 "악의적인 레코드 배서"를 전송하기 이전에 그것을 개별 레코드(100)에 부가할 수 있다.

[0214] *예시적인 고스팅*

[0215] [0202] 일부 실시예들에서, 악의적인 레코드 전송자는 부적합한 서명들을 이용하여 개별 레코드들을 생성할 수

있다. 도 22는, 고스팅으로 지칭될 수 있는 이러한 악의적인 거동을 예시하는 상호작용 다이어그램이다. 레코드 수신자 디바이스(116b)를 사용하는 레코드 수신자(102b)는, 상호작용(404)에서 SRL(short range link)(122)을 사용하여 콘텐츠 요청(402)을 레코드 전송자 디바이스(116a)에 전송함으로써, 레코드 전송자(102a)로부터 개별 레코드를 요청할 수 있다. 콘텐츠 요청(402)은 레코드 수신자 디바이스의 콘텐츠 B(110b) 및 공개 키(106b)를 포함할 수 있다.

[0216] [0203] 자신의 SE(secure element)(204a)를 해킹 또는 우회함으로써, 레코드 전송자 디바이스(116a)는, 상호작용(420)에서 개별 레코드(100)를 레코드 수신자 디바이스(116b)에 전송하기 이전에 상호작용(416')에서 부적합한 공개 키(106a') 및 부적합한 서명(112')을 이용하여 개별 레코드(100)를 생성할 수 있다. 레코드 전송자 디바이스의 부적합한 공개 키(106') 및 공개 키(106a)는 상이할 수 있다. 부적합한 서명(112')은 부적합한 개인 키(210')를 사용하여 생성될 수 있다.

[0217] [0204] 424a에서의 레코드 수신자(116b)에 의한 개별 레코드(100)의 검증은, 레코드 수신자 디바이스가 디바이스들의 최신 공개 키들(214b)을 가지면 실패할 수 있다. 레코드 수신자 디바이스(116b)가 부적합한 서명(112')을 암호해독할 수 있더라도, 레코드 수신자 디바이스(116b)는, 부적합한 공개 키(106')가 사용자 디바이스에 속하지 않을 수 있다는 것을 인식할 수 있다. 부적합한 공개 키(106')는 공통 레코드들(206)의 디바이스들(214b)의 공개 키들에 존재하지 않을 수 있다. 실패한 검증 때문에, 레코드 수신자(106b)는 레코드 전송자(102a)와의 콘텐츠 요청(402)을 수반하는 교환을 거절할 수 있다. 일부 실시예들에서, 실패한 검증 후에, 레코드 전송자 디바이스(116b)는, 상호작용(2224)에서 프로세싱 플랫폼(124)에 "MRE(malicious record endorsement)"를 전송하기 이전에 그것을 개별 레코드(100)에 부가할 수 있다.

[0218] [0205] 일부 실시예들에서, 상호작용(424b)에서의 레코드 수신자(116b)에 의한 개별 레코드(100)의 검증은, 레코드 수신자 디바이스가 디바이스들의 최신 공개 키들(214b)을 갖지 않기 때문에 성공적일 수 있다. 부적합한 서명(112')이 부적합한 개인 키(210')를 사용하여 생성되었기 때문에, 레코드 수신자 디바이스(116b)는 개별 레코드(100a) 내의 부적합한 공개 키(106')를 사용하여 부적합한 서명(112')을 성공적으로 암호해독할 수 있다. 상호작용(424b)에서의 개별 레코드(100)의 성공적 검증 후에, 제1 레코드 수신자 디바이스(116b)는, 상호작용(432)에서 수정된 개별 레코드(100m1)를 프로세싱 플랫폼(124)에 상환하기 이전에 상호작용(428)에서 레코드 수신자 서명(112b)을 이용하여 수정된 개별 레코드(100m1)를 생성할 수 있다. 그러나, 부적합한 공개 키(106a')가 중앙 레코드들(302)의 디바이스들의 공개 키들(214)에 존재하지 않기 때문에, 수정된 개별 레코드(100m1)의 프로세싱은 상호작용(436)에서 실패할 수 있다. 일부 실시예들에서, 상호작용(424b)에서의 레코드 수신자(116b)에 의한 개별 레코드(100)의 검증이 성공적일 수 있더라도, 부적합한 공개 키(106a)가 공통 레코드들(206)의 디바이스들의 공개 키들(214)에 존재하지 않기 때문에, 레코드 수신자(102b)는 레코드 전송자(102a)와의 콘텐츠 요청(402)을 수반하는 교환을 거절할 수 있다. 일부 실시예들에서, 암호화 알고리즘의 전유 변형을 이용하여, 그에 따라 고스팅을 불가능하게 만들 수 있다.

[0219] *예시적인 디메리트 및 블랙리스트*

[0220] [0206] 사용자들에 의한 특정 액션들은 본원에서 개시된 방법들 및 시스템들에서 바람직하지 않다. 일부 실시예들에서, 원하지 않는 액션들은 사용자 디바이스들을 변경 또는 해킹하는 것을 요구하지 않을 수 있다. 예컨대, 원하지 않는 액션은, 레코드 전송자(116a)가 부적합한 콘텐츠(110)를 이용하여 개별 레코드(100)를 생성하는 것의 결과일 수 있다. 예컨대, 사용자 레코드 상황(306)은, 레코드 전송자(102a) 그 자체만이 콘텐츠(110)에 저장된 그 문서 ID를 갖는 문서에 대한 액세스를 갖는다는 것을 표시할 수 있으며; 레코드 전송자(102a)는 문서에 대한 다른 사용자들의 액세스를 그랜트하지 않을 수 있다. 개별 레코드(100)의 콘텐츠(110)가 문서에 대한 레코드 수신자(102b)의 액세스를 그랜트하려고 시도하면, 콘텐츠(110)는 부적합할 수 있다. 부적합한 콘텐츠(110)를 이용하여 개별 레코드(100)를 생성함으로써, 레코드 전송자(102a)는 원하지 않게 행동할 수 있다.

[0221] [0207] 프로세싱 플랫폼(124)은, 사용자들에 의한 원하지 않는 액션들의 수를 계속해서 추적하도록 구성된 디메리트 리스트를 포함할 수 있다. 디메리트 리스트는, 프로세싱된 원하지 않는 액션들의 수 또는 프로세싱된 부적합한 콘텐츠들(110)을 갖는 개별 레코드들(100)의 수, 원하지 않는 액션들 또는 부적합한 콘텐츠들(110)의 타입들, 원하지 않는 액션들이 발생했던 때 및 얼마나 최근에 발생했는지, 부적합한 콘텐츠들(110)을 갖는 개별 레코드들(100)이 프로세싱되었던 때 및 얼마나 최근에 프로세싱되었는지, 또는 이들의 임의의 조합을 계속해서 추적할 수 있고 그들에 기반할 수 있다. 일부 실시예들에서, 디메리트 리스트는 사용자들 및 사용자 디바이스들(116)에 대한 디메리트 포인트들을 결정할 수 있다. 디메리트 포인트들은, 디메리트 리스트가 계속해서 추적할 수 있는 정보에 기반할 수 있다. 디메리트 포인트들은 모든 사용자들 또는 일부 사용자들, 예컨대 새로운

사용자들에 대해 정규화될 수 있다.

[0222] [0208] 일부 실시예들에서, 원하지 않는 액션들은 사용자 디바이스들을 변경 또는 해킹하는 것을 요구할 수 있다. 사용자 디바이스들을 변경하는 것을 요구하는 원하지 않는 액션들의 비-제한적인 예들은, 다수의 수신자들에 대한 전송자 클로닝, 단일 수신자에 대한 전송자 클로닝, 포킹, 수신자 클로닝, 마우징, 고스팅, 또는 이들의 임의의 조합을 포함할 수 있다. 원하지 않는 액션들은 다수의 검출 방식들 및 방법들을 이용하여 검출될 수 있다. 이들 원하지 않는 액션들은 도 17-도 22에 예시된 바와 같이 검출될 수 있다. 다른 예로서, 프로세싱 플랫폼(124)은 사용자 디바이스들(116) 상의 소프트웨어 및 하드웨어에 대한 싸인된 증명서 및 체크섬들에 기반하여 디바이스 변경들을 검출할 수 있다.

[0223] [0209] 프로세싱 플랫폼(124)은, 디바이스 변경들을 요구하는 원하지 않는 액션들의 변경되었던 사용자 디바이스들의 참여들을 검출함으로써, 그 변경되었던 사용자 디바이스들을 계속해서 추적할 수 있는 블랙리스트를 포함할 수 있다. 일부 실시예들에서, 사용자의 사용자 디바이스가 블랙리스트 상에 존재하면, 사용자의 모든 사용자 디바이스들이 블랙리스트(1404) 상에 존재할 수 있다. 사용자 디바이스가 블랙리스트 상에 존재하면, 그 사용자 디바이스는 본원에서 개시된 방법들 및 시스템들로부터 일시적으로 또는 영구적으로 금지될 수 있다. 일부 실시예들에서, 특정 수의 디메리트 포인트들을 갖는 사용자들 및 사용자 디바이스들(116)이 블랙리스트 상에 배치될 수 있다.

[0224] *예시적인 악의적인 레코드 배서*

[0225] [0210] 일부 원하지 않는 액션들에 대해, 레코드 수신자 디바이스들(116b)은 레코드 전송자 디바이스들(116a) 자체의 변경들 또는 해킹을 검출할 수 있다. 예컨대, 도 17에 예시된 다수의 수신자들에 대한 전송자 클로닝에 대해, 제2 레코드 수신자 디바이스(116c)는, 개별 레코드(100)가 제1 레코드 수신자 디바이스(116b)에 대해 의도된다는 것을 저절로 검출할 수 있다. 일부 실시예들에서, 실패한 검증 시에, 제2 레코드 전송자 디바이스(116c)는, 상호작용(1724)에서 프로세싱 플랫폼(124)에 "MRE(malicious record endorsement)"를 전송하기 이전에 그것을 개별 레코드(100)에 부가할 수 있다. 제2 레코드 전송자 디바이스(116c)는 레코드 수신자 서명(112c)과 함께 "악의적인 레코드 배서"를 갖는 개별 레코드(100)를 전송할 수 있으며, 이는 프로세싱 플랫폼(124)에 대한 싸인된 "악의적인 레코드 배서"로 지칭될 수 있다. 레코드 전송자 디바이스(116c)는, 그것이 네트워크(118)에 연결될 때 "악의적인 레코드 배서"를 갖는 개별 레코드(100)를 전송할 수 있다.

[0226] *예시적인 퍼지 규칙*

[0227] [0211] 프로세싱 플랫폼(124)이 싸인된 "악의적인 레코드 배서"를 갖는 개별 레코드(100)를 수신할 때, 프로세싱 플랫폼(124)은 악의적인 사용자가 존재한다고 결정할 수 있다. 그러나, 프로세싱 플랫폼(124)은 특정 원하지 않는 액션들, 이를테면 단일 수신자에 대한 전송자 클로닝 및 수신자 클로닝을 구별하지 못할 수 있다. 그리고, 프로세싱 플랫폼(124)은 특정 사용자 또는 사용자 디바이스(116)에게 책임 또는 잘못을 물을 수 없다.

[0228] [0212] 특정 원하지 않는 액션들에 대해, 프로세싱 플랫폼(124)은 특정 사용자에게 책임 또는 잘못을 물을 수 있다. 예컨대, 레코드 전송자(102a) 및 제1 레코드 수신자(102b)를 수반하는 개별 레코드(100)의 2개의 동일한 카피들이 프로세싱 플랫폼(124)에서 상환되면, 레코드 전송자(102a) 또는 제1 레코드 수신자(102b) 중 어느 하나는 악의적인 사용자이다. 레코드 전송자(102a) 또는 제1 레코드 수신자(102b) 중 어느 하나가 악의적인 사용자이라는 것에 기반하여, 프로세싱 플랫폼(124)은 다수의 규칙들을 생성할 수 있다. 비-제한적인 예시적 규칙은:

[0229] M(전송자) + M(제1 수신자) = 참 (규칙 1)

[0230] 이고, 여기서, M()은, 아규먼트가 악의적인지를 결정하는 부울 오퍼레이터를 나타내고, "+"는 논리적 OR 연산을 나타낸다.

[0231] [0213] 이러한 정보는 향후 사용을 위해 저장될 수 있다. 예컨대, 레코드 전송자(102a) 및 제2 레코드 수신자(102b')를 수반하는 다른 개별 레코드의 2개의 동일한 카피들이 프로세싱 플랫폼(124)에서 상환되면, 프로세싱 플랫폼(124)은 다수의 규칙들을 생성할 수 있다. 비-제한적인 예시적 규칙은:

[0232] (M(전송자) + M(제1 수신자)) * (M(전송자) + M(제2 수신자)) = 참 (규칙 2)

[0233] 이고, 여기서, "*"는 논리적 AND 연산을 나타낸다.

[0234] 규칙 2는 다음과 같이 다시 쓰여질 수 있다:

[0235] M(전송자) + (M(제1 수신자)) * (M(제2 수신자)) = 참 (규칙 3)

[0236] [0214] 규칙들을 해석하는 데 있어, 프로세싱 플랫폼(124)은 예컨대 2명의 사용자들이 악의적이지 않다고 가정할 수 있다. 2명의 사용자들이 악의적이지 않다면, 프로세싱 플랫폼(124)은, 규칙 3으로부터, 레코드 전송자(102a)가 악의적이라고 결론을 내릴 수 있다. 다른 예로서, 프로세싱 플랫폼(124)은, 악의적인 사용자들이 드물 수 있다(0보다 크고 1보다 작은 확률 "p"로 발생함)는 사전 믿음을 주장할 수 있다. 그런다음, 둘 모두의 제1 레코드 수신자(102b)와 제2 레코드 수신자(102b') 둘 모두가 악의적일 확률은 규칙 3에서 p * p일 수 있다. 규칙 3의 좌변은 p + p * p로서 표현될 수 있다.

[0237] [0215] 유사하게, 그러한 해석들 및 가정들은 프로세싱 플랫폼(124)에 의해 모든 사용자들의 모든 관측들을 포함하도록 확장될 수 있으며, 곱들의 합 형태로 표현될 수 있다. 따라서, 곱에서 최소 엘리먼트들을 갖는 항이 참(true)일 가능성이 가장 높을 수 있다. 예컨대, 규칙 3에서, M(전송자)란 항이 최소 엘리먼트를 가질 수 있고, 참일 가능성이 가장 높을 수 있다. 이들 사용자들 및 사용자 디바이스들은, 임시로, 즉시, 악의적인 것으로서 라벨링되고 블랙리스트에 올려질 수 있거나, 또는 추가로 조사될 수 있다.

[0238] 예시적인 사용자 디바이스

[0239] *예시적인 프로세서, 메모리, 스토리지, 네트워크 인터페이스, 및 단거리 링크 인터페이스*

[0240] [0216] 도 23은 예시적인 사용자 디바이스(116)를 개략적으로 예시한다. 사용자 디바이스들(116)은 레코드 전송자 디바이스들, 레코드 수신자 디바이스들, 및 에이전트 디바이스들일 수 있다. 사용자 디바이스(116)는, 메모리(2308), 예컨대 RAM(random access memory)에 저장된 명령들을 실행하도록 구성된 프로세서(2304)를 포함할 수 있다. 메모리(2308)는, 사용자 디바이스(116)가 파워 온될 때 명령들 및 데이터를 저장하도록 구성될 수 있다. 메모리(2308)는 판독 전용 메모리와 기록가능 메모리 둘 모두를 포함할 수 있다. 사용자 디바이스(116)는, 사용자 디바이스(116)가 파워 온 또는 파워 오프될 때 명령들 및 데이터를 저장하도록 구성된 스토리지(2312)를 포함할 수 있다. 메모리(2308)와 스토리지(2312) 중 하나 또는 둘 모두는, 콘텐츠들 및 레코드들을 안전하게 교환하기 위한 명령들을 저장할 수 있다.

[0241] [0217] 사용자 디바이스(116)는 네트워크 인터페이스(2316) 및 SRL(short range link) 인터페이스(2320)를 포함할 수 있다. 네트워크 인터페이스(2316)는 동기식으로 또는 비동기식으로 네트워크(118) 상의 다른 디바이스들, 예컨대 프로세싱 플랫폼(124)과 통신하도록 구성될 수 있다. 네트워크 인터페이스(2316)의 비-제한적인 예들은 유선 통신, 무선 통신, 셀룰러 통신, 그리고 Bluetooth®, RF(radio frequency), 또는 IR(infrared)을 사용하는 통신들을 포함한다. SRL(short range link) 인터페이스(2320)는 SRL(short range link)(122)을 통해 다른 사용자 디바이스들(116)과 통신하도록 구성될 수 있다. 단거리 링크 인터페이스(2320)는, 사용자 디바이스들(116a 또는 116b)이 서로 통신할 수 있게 하는 피어-투-피어 라디오 또는 다른 인터페이스들일 수 있다. 단거리 링크 인터페이스(2320)는, IrDA(Infrared Data Association)/IrPHY(Infrared Physical Layer Specification), Bluetooth®, NFC(Near Field Communication), ad hoc IEEE(Institute of Electrical and Electronics Engineers) 802.11, 또는 임의의 다른 무선 통신 방법들 및 시스템들에 기반할 수 있다.

[0242] *예시적인 센서들*

[0243] [0218] 사용자 디바이스(116)는 사용자 디바이스의 주위를 감지하기 위한 하나 이상의 센서들(2324)을 포함할 수 있다. 일부 실시예들에서, 센서들(2324)은 모션 센서들, 배향 센서들, 위치 센서들, 또는 이들의 임의의 조합을 포함할 수 있다. 모션 센서는, 사용자 디바이스(116)를 동작시키는 사용자, 예컨대 사용자 디바이스(116)를 흔드는 사용자의 움직임들을 감지, 검출, 및 결정하도록 구성될 수 있다. 일부 실시예들에서, 모션 센서는 사용자 디바이스(116)에 의한 프로세싱을 위해 사용자의 모션들을 전기 신호들로 변환할 수 있다. 예컨대, 모션 센서는 사용자에 의해 사용자 디바이스(116) 상에 전해지는 움직임들을 감지, 검출, 및 결정하도록 구성된 단일 축 가속도계를 포함할 수 있다. 다른 예로서, 모션 센서는, 다수의 방향들로 지향성 움직임들 및 진동들의 검출을 가능하게 하기 위해 그리고 검출 감도를 증가시키기 위해, 다수의 가속도계들, 예컨대 단일 축 가속도계들과 3D 가속도계들을 포함할 수 있다.

[0244] [0219] 배향 센서는 사용자 디바이스(116)의 배향을 결정하도록 구성될 수 있다. 예컨대, 전송자 디바이스(116a)의 배향 센서는 고정 평면, 예컨대 레코드 전송자(102a)와 레코드 수신자(102b)가 개별 레코드(100)를 안전하게 교환하고 있는 비즈니스 장소의 플로어에 대한 레코드 전송자의 머리를 결정할 수 있다. 일부 실시예들에서, 배향 센서는 사용자 디바이스(116)에 의한 프로세싱을 위해 배향 정보를 전기 신호들로 변환할 수 있다. 위치 센서는 사용자 디바이스(116)의 위치에 기반하여 사용자의 위치를 결정하도록 구성될 수 있다. 위치 센서

들의 비-제한적인 예들은 GPS(global positioning system) 또는 aGPS(assisted GPS) 트랜시버들을 포함한다.

[0245] [0220] 센서들(2324)은 이미징 센서들(예컨대, 디지털 카메라들), 마이크로폰들, 또는 생체인식 센서들을 포함할 수 있다. 이미징 센서는 사용자가 보는 것을 캡처하도록 구성될 수 있다. 예컨대, 레코드 전송자 디바이스(116a)의 이미징 센서는 레코드 전송자(102a)가 보는 것의 하나 이상의 이미지들을 캡처할 수 있다. 다른 예로서, 레코드 전송자(102a)와 레코드 수신자(102b)가 개별 레코드(100)를 안전하게 교환하고 있을 때, 레코드 전송자 디바이스(116a)를 인증하기 위하여, 레코드 전송자 디바이스(116a)의 이미징 센서는 레코드 수신자 디바이스(116b)의 이미지를 캡처할 수 있다. 일부 실시예들에서, 이미징 센서는 사용자 디바이스(116)에 의한 프로세싱을 위해 광자들을 전기 신호들 및 이미지들로 변환할 수 있다.

[0246] [0221] 마이크로폰은, 사용자를 둘러싸는 환경으로부터 그리고 사용자로부터 음파들을 검출하도록 구성될 수 있다. 사용자 디바이스(116)는, 사용자가 청취하고 말하는 것을 검출 및 "청취"할 수 있다. 일부 실시예들에서, 마이크로폰은 사용자 디바이스(116)에 의한 프로세싱을 위해 음파들을 전기 신호들로 변환할 수 있다. 생체인식 센서는 사용자의 생체인식 정보를 캡처하도록 구성될 수 있다. 생체인식 정보의 비-제한적인 예들은 홍채 스캔, 피부 색조, 피부 질감, 또는 지문들을 포함한다.

[0247] *예시적인 개별 레코드 프로세서, 컨테이너, 통신기, 및 추적기*

[0248] [0222] 사용자 디바이스(116)는 개별 레코드 프로세서(2326), 개별 레코드 컨테이너(202), 개별 레코드 통신기(2328), 및 레코드 히스토리 추적기(2332)를 포함할 수 있다. 개별 레코드 프로세서(2326)는 개별 레코드들을 생성 및 수정하도록 구성될 수 있다. 개별 레코드 컨테이너(202)는 미상환 개별 레코드들(208)을 저장하도록 구성될 수 있다. 개별 레코드 통신기(2328)는 개별 레코드들 및 수정된 개별 레코드들을 전송, 수신, 또는 상환하도록 구성될 수 있다. 레코드 히스토리 추적기(2332)는, 사용자 디바이스(116)가 생성, 수신, 수정, 또는 상환한 개별 레코드들을 추적하도록 구성될 수 있다.

[0249] [0223] 예컨대, 레코드 전송자 디바이스(116a)의 개별 레코드 프로세서(2326)는 개별 레코드(100)를 생성할 수 있다. 레코드 전송자 디바이스(116a)의 개별 레코드 통신기(2328)는 개별 레코드(100)를 레코드 수신자 디바이스(116b)에 전송할 수 있다. 레코드 수신자 디바이스(116b)는 자신의 개별 레코드 통신기(2328)를 사용하여 개별 레코드(100)를 수신할 수 있다. 레코드 수신자 디바이스(116b)의 개별 레코드 프로세서(2326)는 수정된 개별 레코드(100m1)를 생성하기 위해 개별 레코드(100)를 수정할 수 있다. 레코드 수신자 디바이스(116b)는, 미상환 개별 레코드들(208) 중 하나로서, 수정된 개별 레코드(100m1)를 개별 레코드 컨테이너(202)에 저장할 수 있다. 레코드 수신자(116b)는, 프로세싱 플랫폼(124)에 자신의 개별 레코드 통신기(2328)를 사용하여, 수정된 개별 레코드(100m1)를 상환할 수 있다.

[0250] [0224] 레코드 히스토리 추적기(2332)는, 사용자 디바이스(116)가 가장 최근에 생성한 개별 레코드(100)의 레코드 ID를 추적하기 위해 가장 높은 레코드 ID(2336)를 포함할 수 있다. 사용자 디바이스(116)가 가장 높은 레코드 ID(2336)보다 더 큰 레코드 ID를 갖는 새로운 개별 레코드를 생성한 후에, 사용자 디바이스(116)는 가장 높은 레코드 ID(2336)를 업데이트할 수 있다. 다른 예로서, 레코드 히스토리 추적기(2332)는, 사용자 디바이스(116)가 생성, 수신, 수정, 또는 상환한 개별 레코드들(100) 전부를 계속해서 추적할 수 있다. 레코드 전송자 디바이스(116a)는 개별 레코드(100)의 카피를 포함할 수 있고, 레코드 수신자 디바이스(116b)는 수정된 개별 레코드(100m1)의 카피를 포함할 수 있다.

[0251] *예시적인 SE(secure element)*

[0252] [0225] 사용자 디바이스(116)는 SE(secure element)(204)를 포함할 수 있다. 보안 엘리먼트(204)는 사용자 디바이스의 개인 키(210) 및 하나 이상의 서비스 제공자 공개 키들(212)을 안전하게 저장하도록 구성될 수 있다. 일부 실시예들에서, 보안 엘리먼트(204)는 서비스 제공자(124)의 공개 키를 포함할 수 있다. 일부 실시예들에서, 보안 엘리먼트(204)는 하나의 서비스 제공자들(124)의 둘 이상의 서비스 제공자 공개 키들(212)을 포함할 수 있다. 일부 실시예들에서, 보안 엘리먼트(204)는 둘 이상의 서비스 제공자들의 둘 이상의 서비스 제공자 공개 키들(212)을 포함할 수 있다. 보안 엘리먼트(204)는 사용자 디바이스의 개인 키(210)를 사용하여 개별 레코드들(100)에 싸인할 수 있다. 레코드 전송자 디바이스(116a)의 보안 엘리먼트(204a)는 개별 레코드(100)에 수신자 공개 키(106b) 및 레코드 ID(108)를 부가할 수 있다. 레코드 ID(108)는 예컨대 레코드 히스토리 추적기(2332)에 의해 추적되는 가장 높은 레코드 ID(2336)에 기반할 수 있다. 일부 실시예들에서, 보안 엘리먼트(204)는 레코드 히스토리 추적기(2332)와 가장 높은 레코드 ID(2336) 중 하나 이상을 포함할 수 있다.

[0253] [0226] SE(secure element)(204)는 서비스 제공자 공개 키(212)를 사용하여, 서비스 제공자(104)로부터 수신

된 정보의 진본성을 검증할 수 있다. 예컨대, 서비스 제공자(104)로부터 수신된 정보는, 서비스 제공자 공개-키 암호 쌍의 개인 키를 사용하여 생성된 서비스 제공자 서명을 포함할 수 있다. 서비스 제공자(104)로부터 수신된 정보의 진본성을 검증하는 것은, 서비스 제공자 개인 키를 사용하여 서비스 제공자 서명이 생성되었는지 여부를 서비스 제공자 공개 키(212)를 사용하여 결정하는 것을 포함할 수 있다. 일부 실시예들에서, 서비스 제공자 공개 키(212)는 보안 엘리먼트(204)에 하드코딩될 수 있다. 일부 실시예들에서, 서비스 제공자 공개 키(212)는 프로세싱 플랫폼(124)에 의해 업데이트될 수 있다.

[0254] [0227] SE(secure element)(204)는 하드웨어 구현, 보안 가상화, 보안 실행 환경, 또는 이들의 임의의 조합을 포함하는 상이한 구현들을 가질 수 있다. 예컨대, 보안 엘리먼트(204)는 사용자 디바이스(116)와 연관된 개인 키(210)를 안전하게 저장할 수 있는 집적 회로 또는 다른 하드웨어 컴포넌트를 포함할 수 있다. 다른 예로서, 보안 엘리먼트(204)는 가상화된 인프라구조에 의해 구현될 수 있다. 가상화된 인프라구조는 사용자 디바이스(116)의 프로세서, 예컨대 프로세서(2304)에서의 하나 이상의 하드웨어 피처들에 의해 지지될 수 있다. 또 다른 예로서, 보안 엘리먼트(204)는 보안 실행 환경으로서 구현될 수 있다. 보안 실행 환경은 인프라구조, 이를테면 자바 카드 애플릿들이 실행될 수 있는 GP(Global Platform)의 가상 구현일 수 있다. 글로벌 플랫폼 시스템은, 예컨대, TEE(trusted execution environment)를 제공하는 사용자 디바이스(116)의 ARM(Advanced RISC(Reduced Instruction Set Computing) Machine) 프로세서의 트러스트 존 피처들에 의해 호스팅될 수 있다.

[0255] *예시적인 공통 레코드 수신자 및 컨테이너*

[0256] [0228] 사용자 디바이스(116)는, 공통 레코드 컨테이너(2340)에의 스토리지를 위해 공통 레코드들(206)을 수신하도록 구성될 수 있는 공통 레코드 수신자(2338)를 포함할 수 있다. 공통 레코드들(206)은 디바이스들(214)의 공개 키들을 포함할 수 있다. 일부 실시예들에서, 공통 레코드들(206)은 사용자 레코드 상황(306)을 포함할 수 있다. 일부 실시예들에서, 공통 레코드들(206)은 디메리트 리스트(1402) 및 블랙리스트(1404)를 포함할 수 있다. 사용자 또는 사용자 디바이스가 태스크를 수행하지 않아야 할 때 태스크를 수행하도록 프로세싱 플랫폼(124)에 명령하는 개별 레코드를 사용자 또는 사용자 디바이스가 생성했다면, 사용자 또는 사용자 디바이스는 디메리트 리스트(1402) 상에 있을 수 있다. 사용자 또는 사용자 디바이스가, 예컨대, 사용자 디바이스에 할당되지 않은 개인 키를 사용하여 개별 레코드에 싸인함으로써 이 개별 레코드를 상환하려고 시도했다면, 사용자 또는 사용자 디바이스는 블랙리스트(1404) 상에 있을 수 있다.

[0257] *예시적인 거래 파트너 식별자*

[0258] [0229] 사용자 디바이스(116)는 레코드 전송자 디바이스들 및 레코드 수신자 디바이스들을 식별하도록 구성된 거래 파트너 식별자(2348)를 포함할 수 있다. 예컨대, 도 1b에 예시된 바와 같이, 레코드 전송자 디바이스(116a)가 개별 레코드(100)를 생성하여 레코드 수신자 디바이스(116b)에 전송하는 경우, 레코드 전송자 디바이스(116a)는 레코드 수신자 디바이스(116b)의 공개 키(106b)를 식별할 필요가 있을 수 있다. 레코드 수신자 디바이스(116b)는 예컨대 단거리 링크 인터페이스(2320)를 사용하여 레코드 전송자 디바이스(116a)에 공개 키를 전송할 수 있다. 레코드 전송자 디바이스(116a)의 거래 파트너 식별자(2348)는, 예컨대, 레코드 수신자 디바이스(116b)로부터 수신된 공개 키가 정말 레코드 수신자 디바이스의 공개 키(106b)라는 것을 확인할 수 있다.

[0259] *예시적인 에러 관리자*

[0260] [0230] 사용자 디바이스(116)는 수신된 부적절한 개별 레코드들을 프로세싱하기 위한 에러 관리자(2356)를 포함할 수 있다. 예컨대, 레코드 수신자 디바이스(116b)는, 레코드 전송자 디바이스(116a)로부터 수신된 개별 레코드(100)의 레코드 전송자 서명(112a)의 진본성을 검증하지 못할 수 있다. 일부 실시예들에서, 부적절한 개별 레코드들을 수신하는 것에 대한 응답으로, 에러 관리자(2356)는, 부적절한 개별 레코드들에 "악의적인 레코드 배서"를 부가한 후에, 프로세싱 플랫폼(124)에 개별 레코드들을 전송할 수 있다.

[0261] *예시적인 소싱*

[0262] [0231] 사용자 디바이스(116)는 소스 정보(2364)를 유지하도록 구성된 소스 컨테이너(2360)를 포함할 수 있다. 소스 정보(2364)는 식별 스트링들, 예컨대 보관소의 이름과 연관될 수 있다. 소스 정보(2364)는, 예컨대, 자신의 ID가 개별 레코드(100)의 콘텐츠(110)에 저장된 문서를 획득하기 위한 다수의 소스들을 식별할 수 있다. 소스들은 프로세싱 플랫폼(264)의 부분일 수 있거나 또는 부분이 아닐 수 있다.

[0263] [0232] 사용자 디바이스들(116)은 소스 정보를 저장하기 위한 소스 필드들을 갖는 개별 레코드들(100)을 생성할 수 있다. 일부 실시예들에서, 개별 레코드들(100)이 빈 소스 필드들을 갖거나 또는 소스 필드들을 갖지 않으면, 개별 레코드들(100)은 디폴트 소스들을 갖는 것으로 가정될 수 있다. 예컨대, 개별 레코드(100)가, 레코

드 수신자(102b)에 문서를 제공하도록 프로세싱 플랫폼(124)에 명령하면, 개별 레코드(100)는 소스 필드, 이를테면 문서를 획득하기 위한 특정 보관소를 포함할 수 있다. 개별 레코드(100)가 소스 필드를 포함하지 않거나 또는 빈 소스 필드를 포함하면, 프로세싱 플랫폼(124)은 디폴트 보관소로부터 문서를 획득할 수 있다.

[0264] [0233] 일부 실시예들에서, 개별 레코드들(100)은, 레코드 전송자들(102a) 또는 레코드 수신자들(102b)이 소싱과 연관된 소싱 수수료들을 지불하거나 또는 분할할 것인지 여부에 관한 수수료 공유 필드들을 포함할 수 있다. 예컨대, 보관소는 개별 레코드(100)에 의해 명령된 문서에 액세스하기 위한 프로세싱 플랫폼(100)에 청구할 수 있으며, 수수료 공유 필드는, 레코드 전송자(102a) 또는 레코드 전송자(102b)가 보관소에 의한 청구 요금을 담당할 것인지 여부, 또는 그들이 청구 요금을 분할할 수 있는지 그리고 어떻게 분할할 수 있는지를 표시할 수 있다. 일부 실시예들에서, 사용자 디바이스들(116)은 소정의 소스 필드들, 수수료 공유 필드들, 또는 이들의 임의의 조합을 갖는 개별 레코드들(100)을 거절할 수 있다.

[0265] [0234] 사용자 디바이스(116)는 사용자들로부터 소스 정보(2364)를 수신하기 위한 소스 사용자 인터페이스(2368)를 포함할 수 있다. 예컨대, 사용자들은 사용자 디바이스들(116) 상의 애플리케이션 또는 웹 인터페이스를 사용하여 소스 정보(2364)를 입력할 수 있다. 다른 예로서, 소스 사용자 인터페이스(2368)는 소스 정보(264)를 포함하는 문서들로부터 소스 정보(2364)를 추출하기 위한 시각적 인터페이스를 제공할 수 있다. 시각적 인터페이스는 센서들(2324), 예컨대 이미징 센서, 및 컴퓨터 비전 알고리즘들을 사용할 수 있다.

[0266] 예시적인 프로세싱 플랫폼

[0267] *예시적인 프로세서, 메모리, 스토리지, 및 네트워크 인터페이스*

[0268] [0235] 프로세싱 플랫폼(124)은 하나 이상의 서버 컴퓨터들을 포함할 수 있다. 서버 컴퓨터들은 중앙집중형 또는 분산형일 수 있다. 도 24는 예시적인 프로세싱 플랫폼(124)을 개략적으로 예시한다. 프로세싱 플랫폼(124)은, 메모리(2408), 예컨대 RAM(random access memory)에 저장된 명령들을 실행하도록 구성된 프로세서(2404)를 포함할 수 있다. 메모리(2408)는, 프로세싱 플랫폼(124)이 파워 온될 때 명령들 및 데이터를 저장하도록 구성될 수 있다. 메모리(2408)는 판독 전용 메모리와 기록가능 메모리 둘 모두를 포함할 수 있다. 프로세싱 플랫폼(124)은, 프로세싱 플랫폼(124)이 파워 온 또는 파워 오프될 때 명령들 및 데이터를 저장하도록 구성된 스토리지(2412)를 포함할 수 있다. 메모리(2408)와 스토리지(2412) 중 하나 또는 둘 모두는, 레코드 수신자 디바이스(116b)가 프로세싱 플랫폼(104)에 상환한 개별 레코드들, 예컨대 수정된 개별 레코드(100m1)를 프로세싱하기 위한 명령들을 저장할 수 있다. 프로세싱 플랫폼(124)은, 연속적으로 또는 간헐적으로, 동기식으로 또는 비동기식으로, 네트워크(118) 상의 다른 디바이스들, 예컨대 사용자 디바이스들(116)과 통신하도록 구성된 네트워크 인터페이스(2416)를 포함할 수 있다. 프로세싱 플랫폼(124)의 네트워크 인터페이스(2416)와 사용자 디바이스(116)의 네트워크 인터페이스(306)는 동일하거나 또는 상이할 수 있다.

[0269] *예시적인 개별 레코드 수신자 및 프로세서*

[0270] [0236] 프로세싱 플랫폼(124)은, 사용자 디바이스들(116)로부터 개별 레코드들(100)을 수신하도록 구성된 개별 레코드 수신자(2420)를 포함할 수 있다. 프로세싱 플랫폼(124)의 개별 레코드 프로세서(2424)는 사용자 디바이스들(116)로부터 개별 레코드 수신자(2420)에 의해 수신된 개별 레코드들(100)을 프로세싱하도록 구성될 수 있다. 예컨대, 프로세싱 플랫폼(124)의 개별 레코드 프로세서(2424)는 레코드 수신자(102b)로부터 개별 레코드 수신자(2420)에 의해 수신된 수정된 개별 레코드(100m1)를 프로세싱할 수 있다.

[0271] [0237] 개별 레코드(100)를 프로세싱하는 것은, 개별 레코드(100)의 발신자로부터 "FPOE(for processing only endorsement)"의 서명자까지 개별 레코드(100) 내의 서명들 중 일부 또는 전부를 인증하는 것을 포함할 수 있다. 예컨대, 수정된 개별 레코드(100m1)를 프로세싱하는 것은, 레코드 전송자 서명(112a)과 레코드 수신자 서명(112b) 중 하나 또는 둘 모두를 인증하는 것을 포함할 수 있다.

[0272] [0238] 개별 레코드들(100) 내의 서명들을 인증하는 것은, 중앙 레코드들(302)을 포함하는 중앙 레코드 컨테이너(2432)에 저장된, 사용자 디바이스들의 공개 키들(214)에 기반할 수 있다. 예컨대, 개별 레코드 프로세서(2424)는 수정된 개별 레코드(100m1) 내의 레코드 전송자 서명(112a)과 레코드 수신자 서명(112b)을 인증할 수 있다. 레코드 전송자 서명(112a)과 레코드 수신자 서명(112b)을 인증하는 것은, 레코드 전송자 서명(112a)과 레코드 수신자 서명(112b)이, 각각, 레코드 전송자 디바이스의 개인 키(212a)와 레코드 수신자 디바이스(116b)의 개인 키(212b)를 사용하여 생성되었는지 여부를 결정하는 것을 포함할 수 있다. 레코드 전송자 서명(112a)과 레코드 수신자 서명(112b)이, 레코드 전송자 디바이스의 개인 키(212a)와 레코드 수신자 디바이스의 개인 키(212b)를 사용하여 생성되었는지 여부를 결정하는 것은, 레코드 전송자 디바이스의 공개 키(106a)와 레코드 수

신자 디바이스의 공개 키(106b)를 사용하여 서명들의 진본성을 결정하는 것을 포함할 수 있다.

[0273] [0239] 개별 레코드들을 프로세싱하는 것은, 프로세싱된 개별 레코드들(100)의 콘텐츠들(110)에 의해 명령된 대로 행동하는 것을 포함할 수 있다. 예컨대, 수정된 개별 레코드(100m1)의 콘텐츠(110)가, 레코드 수신자 디바이스(116b)가 특정 문서 ID를 갖는 문서에 대한 액세스를 제공받아야 한다는 명령을 포함하면, 수정된 개별 레코드(100m1)를 프로세싱하는 것은, 그러한 액세스를 레코드 수신자 디바이스(116b)에 제공하는 것을 포함할 수 있다.

[0274] *예시적인 중앙 레코드 프로세서 및 컨테이너*

[0275] [0240] 개별 레코드 프로세서(2424)가 수신된 개별 레코드들을 프로세싱하는 것을 완료한 후에, 프로세싱 플랫폼(124)의 중앙 레코드 프로세서(2428)는 중앙 레코드 컨테이너(2432)에 포함된 중앙 레코드들(302)을 업데이트하도록 구성될 수 있다. 중앙 레코드 프로세서(2428)는 중앙 레코드 컨테이너(2432)에 포함된 중앙 레코드들(302)을 예컨대 백업 스토리지에 백업할 수 있다. 일부 실시예들에서, 중앙 레코드 컨테이너(2432)에 포함된 중앙 레코드들(302)은 권위있다(authoritative). 예컨대, 중앙 레코드들(302)의 사용자 레코드 상황(306)은 사용자들 또는 사용자 디바이스들의 가장 최신의 그리고 가장 정확한 정보를 포함할 수 있다. 일부 실시예들에서, 임의의 정해진 시간에, 상환되지 않은, 그리고 중앙 레코드들(302)에 의해 반영되지 않을 수 있는 개별 레코드들이 존재할 수 있다.

[0276] [0241] 중앙 레코드들(302)은 사용자 디바이스들의 공개 키들(214), 사용자 정보(304), 사용자 레코드 상황(306), 디메리트 리스트(1402), 블랙리스트(1404), 및 소스 정보(2436)를 포함할 수 있다. 예컨대, 개별 레코드 프로세서(2424)가 수정된 개별 레코드(100m1)의 콘텐츠(110)에 의해 명령된 대로 문서에 대한 액세스를 레코드 수신자 디바이스(116b)에 제공한 후에, 중앙 레코드 프로세서(2428)는 액세스의 그러한 그랜트를 반영하도록 사용자 레코드 상황(306)을 업데이트할 수 있다.

[0277] [0242] 소스 정보(2436)는, 개별 레코드들(100)의 콘텐츠들(110)이 어떻게 프로세싱될 수 있는지에 관한 정보를 포함할 수 있다. 예컨대, 수정된 개별 레코드(100m1)는 특정 문서 ID를 갖는 문서에 대한 액세스를 레코드 수신자 디바이스(116b)에 제공하도록 프로세싱 플랫폼(124)에 명령할 수 있으며, 문서는 2개의 데이터베이스들에 저장될 수 있다. 소스 정보(2436)는, 어느 데이터베이스들로부터든지 문서가 획득될 수 있다는 것, 또는 가능하다면 2개의 데이터베이스들 중 하나로부터 문서가 획득되어야 한다는 것을 표시할 수 있다.

[0278] *예시적인 공통 레코드 생성기 및 분배기*

[0279] [0243] 프로세싱 플랫폼(124)의 공통 레코드 생성기(2440)는 공통 레코드 분배기(2444)에 의한 사용자 디바이스들(116)로의 분배를 위해 중앙 레코드들(302)로부터 공통 레코드들(206)을 생성할 수 있다. 공통 레코드들(206)의 콘텐츠들은 변할 수 있다. 예컨대, 공통 레코드들(206)은 중앙 레코드들(302)과 동일할 수 있다. 다른 예로서, 공통 레코드들(206)은 중앙 레코드들(302)의 서브세트일 수 있다. 공통 레코드들(206)은 디바이스들의 공개 키들(214), 사용자 정보(304), 사용자 레코드 상황(306), 디메리트 리스트(1402), 블랙리스트(1404), 및 소스 정보(2436) 중 하나 이상을 포함할 수 있다. 공통 레코드 분배기(2444)는 서비스 제공자 개인 키(2448)를 사용하여 생성된, 공통 레코드들(206)의 서명과 함께 공통 레코드들(206)을 분배할 수 있다. 서비스 제공자 공개 키(212)와 서비스 제공자 개인 키(2448) 중 하나 또는 둘 모두는 프로세싱 플랫폼(124)의 SE(secure element)에 저장될 수 있다. 서비스 제공자 개인 키(2448)는 프로세싱 플랫폼(124)의 배타적 또는 비-배타적 소유로 있을 수 있다.

[0280] *예시적인 에러 관리자*

[0281] [0244] 프로세서 플랫폼(124)은, 부적절한 개별 레코드들을 프로세싱하도록 구성된 에러 관리자(2452)를 포함할 수 있다. 예컨대, 레코드 수신자 디바이스(116b)는, 배서 블록(105b)에서 "악의적인 레코드 배서"를 갖는 수정된 개별 레코드(100m1)를 전송할 수 있다. 에러 관리자(2452)는, 프로세싱 플랫폼(124)에 의해 수신된 부적절한 개별 레코드들에 기반하여 레코드 전송자 디바이스(116a)가 디메리트 리스트(1402) 상에 또는 블랙리스트(1404) 상에 배치되어야 하는지 여부를 결정하도록 구성될 수 있다.

[0282] *예시적인 소싱*

[0283] [0245] 프로세싱 플랫폼(124)은, 중앙 레코드들(302)에 저장된 소스 정보(2436)를 관리하기 위한 소스 관리자(2456)를 포함할 수 있다. 소스 관리자(2456)는, 소스들과의 상호작용들을 가능하게 하고 상호작용할 소스들을 결정하도록 구성될 수 있다. 소스 정보(2436)는, 상환된 개별 레코드들(100)의 콘텐츠들(110)에 의해 명령된

대로 수행하기 위한, 상이한 소스들에 대한 선호도들 및 디폴트 소스들을 포함하여 다수의 소스들을 식별할 수 있다. 소스 정보(2436)는, 소스들에 액세스하는 것과 연관된 비용들, 예컨대, 소스들에 액세스하기 위해 소스들이 청구하는 비용들을 포함할 수 있다. 소스 정보(2436)는 사용자들로부터 수신된 정보를 포함할 수 있다.

[0284] 펀드들을 암호화방식으로 보안 송금하기 위한 예시적인 시스템

[0285] [0246] 펀드들의 오프라인 디지털 송금을 위한 시스템들 및 방법들이 본원에서 개시된다. 예컨대, 디지털 수표들과 같은 거래 증서들이 하이브리드 시스템을 사용하여 안전하게 송금 및 교환될 수 있다. 하이브리드 시스템은, 모든 거래 당사자들이 거래를 인증할 수 있는 중앙 데이터 서버들에 연결되어 있지는 않을 때, 의미있거나 만족스러운 중앙집중형 및 피어-투-피어의 디지털 수표들의 교환들 또는 값의 송신을 제공할 수 있다. 디지털 수표들은 가변적인 값을 가질 수 있고, 지참인 문서(이를테면, 현금)가 아니므로, 디지털 수표들은, 한 사람 또는 엔티티로부터 다른 사람 또는 엔티티로, 두 당사자들 모두가 은행과 같은 중앙 보관소에 나타나는 것을 요구하지 않고도 다량의 값이 송금될 수 있게 한다. 디지털 수표들이 카피될 수 있다는 사소한 문제와 같은 디지털 송신들에 관련된 난제들이 처리된다. 예컨대, 디지털 수표들의 배서를 위해 전통적인 수기된 서명의 훨씬 더 강력한 암호 아날로그인 디지털 암호화 방식을 사용하는, 디지털 플랫폼들 상에서 이용가능한 디지털 툴들 및 기법들에 기반한 피처들이 개시된다.

[0286] [0247] 하이브리드 시스템은, 시스템의 하나의 사용자로부터 다른 사용자로 펀드들을 송금하기 위한 하나 이상의 컴포넌트들을 포함할 수 있다. 하이브리드 시스템은, 중앙집중형 컴포넌트뿐만 아니라 피어-투-피어 컴포넌트 둘 모두를 가질 수 있다. 하이브리드 시스템을 이용하여, 사용자들은, 거래들 당시에 시스템의 중앙 컴포넌트들에 액세스하지 않고도 서로 금융 거래들을 할 수 있다. 시스템은, 인터넷, IEEE(Institute of Electrical and Electronics Engineers) 802.11 표준 802.11과 같은 프로토콜들을 구현하는 유선 또는 무선 통신들에 의해 액세스될 수 있는 전 세계적인 네트워크, 또는 장거리 네트워크, 이를테면 셀룰러 전화 네트워크들과 같은 네트워크를 활용할 수 있다.

[0287] [0248] 시스템의 하나 이상의 컴포넌트들은, 디지털 수표, 구매자 또는 판매자와 같은 사용자들, MC(mobile computers)들, 월렛, SRL(short range link), 프로세싱 플랫폼, 중앙 회계장부, 공통 회계장부, 또는 회사를 포함할 수 있다. 디지털 수표는, 시스템의 하나의 컴포넌트로부터 다른 컴포넌트로 송신될 수 있는 데이터의 블록인 디지털 객체일 수 있다. 구매자는, 다른 사람, 예컨대 판매자에게 펀드들을 송금하기를 원하는 지불인일 수 있다. 판매자는, 다른 사람, 예컨대 구매자로부터 펀드들을 받기를 원하는 수취인일 수 있다. 모바일 컴퓨터들은, 구매자 및 판매자의 소유의 컴퓨팅 디바이스들일 수 있다. 구매자 및 판매자의 소유의 모바일 컴퓨터들은 동일하거나 상이할 수 있다. 모바일 컴퓨터들은, 예컨대 셀룰러 전화들일 수 있다. 월렛은, 모바일 컴퓨터 상에 상주하는, 아직 프로세싱 플랫폼으로 송신되지 않은 그 모바일 컴퓨터에 의해 수신된 모든 디지털 수표들을 포함하는 디지털 데이터 구조일 수 있다. 단거리 링크는 피어-투-피어 라디오, 또는 모바일 컴퓨터들이 서로 통신할 수 있게 하는 다른 링크들일 수 있다. 링크는, IrDA(Infrared Data Association)/IrPHY(Infrared Physical Layer Specification), 블루투스®, NFC(Near Field Communication), 애드 혹 IEEE(Institute of Electrical and Electronics Engineers) 802.11, 또는 임의의 다른 무선 통신 방법들 및 시스템에 기반할 수 있다.

[0288] [0249] 프로세싱 플랫폼은, 시스템에 대한 인프라구조일 수 있는 머신 또는 머신들의 집합을 포함하는 서버일 수 있다. 프로세싱 플랫폼은 네트워크에 연결될 수 있고, 간접적으로 (그렇지만 가능하게는 간헐적으로만) 모바일 컴퓨터들에 연결될 수 있다. 프로세싱 플랫폼은 중앙 회계장부뿐만 아니라 공통 회계장부를 유지할 수 있다. 중앙 회계장부는, 통화 단위들로 측정된 잔액들을 유지하는 데이터베이스일 수 있다. 통화 단위들은 기존의 국가 통화들(예컨대, US 달러)일 수 있다. 통화 단위들은 시스템을 위해 생성된 신규한 명목 화폐일 수 있다. 이러한 잔액 정보는 시스템의 모든 각각의 사용자에 대해 저장될 수 있다. 중앙 회계장부는, 각각의 사용자에 관한 다른 보조적인 정보 또는 식별 정보를 유지할 수 있다. 중앙 회계장부와 연관된 공통 회계장부는 시스템 전반에 걸쳐 배포될 수 있다. 공통 회계장부는 유효한 사용자 ID(identifier)들의 리스트를 포함할 수 있다. 공통 회계장부는 또한 사용자들에 관한 부가적인 정보를 포함할 수 있다. 공통 회계장부는, 일부 실시예들에서 공통 회계장부가 계정 잔액들을 포함하지 않는다는 점에서 중앙 회계장부와 다르다. 공통 회계장부는, 중앙 회계장부의 다른 정보를 생략할 수 있다. 회사는, 프로세싱 플랫폼을 동작시키는 엔티티 또는 서비스 제공자일 수 있다.

[0289] 예시적인 기본 거래들

[0290] [0250] 도 25는 표준 거래의 예를 개략적으로 예시한다. 구매자는, 판매자에게 주어질 수 있는 명령을 중앙

회계장부에 발행할 수 있다. 그러한 명령은 디지털 수표일 수 있다. 그런 다음, 판매자는, 돈을 송금하기 위해, 중앙 회계장부를 유지하는 프로세싱 플랫폼에 그 디지털 수표를 상환할 수 있다. 구매자와 판매자 사이의 거래가 오프라인으로 이루어질 수 있으므로, 어느 당사자도 네트워크에 연결되지 않고 데이터 송신이 SRL(short range link)을 통해 대신 이루어질 수 있다. 그런 다음, 판매자는, 판매자의 모바일 컴퓨터가 네트워크를 통해 프로세싱 플랫폼에 연결되는 임의의 나중의 시간에, 중앙 회계장부를 유지하는 프로세싱 플랫폼에 디지털 수표를 상환할 수 있다.

[0291] [0251] 구매자 및 판매자 둘 모두는 MC(mobile computer)를 가질 수 있다. 모바일 컴퓨터에는 SE(secure element)가 구비될 수 있다. 보안 엘리먼트는, 하드웨어 구현, 보안 가상화, 보안 실행 환경들 또는 이들의 임의의 조합을 포함하는 상이한 구현들을 가질 수 있다. 예컨대, 보안 엘리먼트는, RSA(Rivest-Shamir-Adleman) 암호화와 같은 공개 키 암호 알고리즘들의 개인 키를 안전하게 저장할 수 있는 칩 또는 다른 하드웨어 컴포넌트일 수 있다. 다른 예로서, SE는, MC의 다른 프로세서에 있는 하드웨어 피처들에 의해 지원될 수 있는 가상화된 인프라구조일 수 있다. 또 다른 예로서, SE는, 자바 카드 애플릿들이 그 상에서 실행되는 GP(Global Platform)와 같은 인프라구조의 가상 구현일 수 있다. 전체 GP 시스템은, 모바일 디바이스의 ARM(Advanced Reduced Instruction Set Computing(RISC) Machine) 프로세서의 TrustZone 피처들, 예컨대 ARM 글로벌 플랫폼 TEE(trusted execution environment)를 통해 호스팅될 수 있다.

[0292] [0252] 보안 엘리먼트는 디지털 수표들의 데이터 블록들을 싸인할 수 있다. 보안 엘리먼트는, SE가 또한 가질 수 있는 다른 (가능하게는 관련되지 않은) 기능들을 가질 수 있다. 데이터 블록들을 싸인할 시, 보안 엘리먼트는 또한 블록의 2개의 부가적인 필드들을 완료할 수 있다. 제1 부가적인 필드는, SE에 저장될 수 있는 사용자와 연관된 공개 키일 수 있다. 제2 부가적인 필드는, 동일한 수가 결코 2번 나타나지 않도록 SE의 내부에서 균일하게 증가하는 수인 수표 ID(identifier)일 수 있다.

[0293] [0253] SE의 액션은, 디지털방식으로 싸인될 디지털 수표의 블록의 프로비전뿐만 아니라 암호구 또는 생체인식 템플릿 둘 모두에 의해 트리거링될 수 있다. 암호구 또는 생체인식 템플릿은 SE가 서명을 발행하기 위해 요구될 수 있다. 생체인식 템플릿은, 지문, 홍채, 또는 임의의 다른 소스로부터 도출될 수 있다. SE는, 생체인식 템플릿을 인식하도록 구성된 생체인식 퍼지 금고를 구현할 수 있다. 서명은 블록을 완료 및 싸인할 수 있다. 서명은 디지털 서명일 수 있고, 블록의 SHA(secure hash algorithm)-2와 같은 해시를 암호화하기 위해 RSA와 같은 알고리즘의 사용으로 생성될 수 있다. 서명은 SE에 저장된 개인 키로 생성될 수 있지만, 사용자의 연관된 공개 키의 임의의 소유자에 의해 검증될 수 있다.

[0294] [0254] 구매자는 싸인된 디지털 수표를 판매자에게 직접 송신할 수 있거나, SRL을 통해서 또는 임의의 다른 수단에 의해서, 임의의 다른 당사자를 통해 간접적으로 송신할 수 있다. 일단 판매자의 소유이면, 판매자는 배서 블록을 디지털 수표에 부가하는 것을 선택할 수 있다. 이러한 배서는, 디지털 수표가 예치만 될 수 있다는 것을 특정하는 "FDOE(for deposit only endorsement)"일 수 있다. 이러한 배서는 디지털 수표를 제3 자에게 추가로 다시 보낼 수 있다. 일단 배서가 부가되면, 판매자는, 오리지널 블록, 구매자의 서명, 및 배서 블록을 포함하는 전체 디지털 수표에 대한 서명을 생성하는 프로세스를 반복할 수 있다. 그에 따라서, 임의의 디지털 수표는, 각각이 자신의 발신자를 식별하는 블록들의 체인일 수 있다. 각각의 블록에서, 체인의 전체 이전 부분은, 그때 블록들을 핸들링하는 당사자에 의해 그의 모바일 컴퓨터의 개인 키를 사용하여 싸인될 수 있다.

[0295] [0255] 마지막 블록이 FDOE인 임의의 디지털 수표는 프로세싱 플랫폼에 상환될 수 있다. 상환 시, 프로세싱 플랫폼은, 체인의 각각의 서명의 진본성을 디지털 수표의 발신자, 예컨대 오리지널 구매자에게 다시 검증할 수 있다. 서명들 전부가 진본이라면, 펀드는 발신자의 계정으로부터 송금되어 디지털 수표의 체인의 마지막 포인트에서 사용자의 계정에 배치될 것이다. 판매자가 프로세싱 플랫폼에 연결되어 그의 월렛에서 디지털 수표를 상환하는 시간은 상환 이벤트일 수 있다.

[0296] 예시적인 중앙 회계장부

[0297] [0256] 회사는 프로세싱 플랫폼을 유지하는 것을 담당할 수 있고, 프로세싱 플랫폼은 중앙 회계장부를 유지하도록 구성될 수 있다. 중앙 회계장부는, 사용자들의 데이터베이스일 수 있거나 그를 포함할 수 있다. 중앙 회계장부는, 사용자들의 공개 키들 및 사용자들의 현재 잔액들을 포함하여 사용자들에 관해 알려진 정보를 포함할 수 있다. 일부 실시예들에서, 중앙 회계장부는, 시스템에 알려진 사용자들에 관한 모든 정보를 포함할 수 있다. 공개 키들은, 모바일 컴퓨터들의 SE들에 있는 개인 키들과 연관될 수 있다. 중앙 회계장부의 레코드는 개인이 아니라 디바이스의 레코드일 수 있다. 사용자가 소유한 모바일 컴퓨터들은, 그러한 정보가 이용가능하다면, 사용자에 의해 함께 그룹화될 수 있다. 특정 사용자와 연관된 디바이스들 간의 잔액들은 일부 실시예들

에서 풀링(pool)될 수 있다.

[0298] [0257] 중앙 회계장부의 백업 카피들이 존재할 수 있다 하더라도, 중앙 회계장부는 고유할 수 있으므로, 중앙 회계장부가 포함하는 잔액들은 시스템의 권위 있는 잔액들이다. 임의의 정해진 시간에, 중앙 회계장부가 알지 못 할 수 있는, 시스템에서 미처리된(outstanding) 디지털 수표들이 존재할 수 있다. 중앙 회계장부를 유지하는 프로세싱 플랫폼은, 임의의 디지털 수표를 그 디지털 수표의 발생지점(point of origin)에서부터 FDOE의 서명자까지 인증하기 위해, 중앙 회계장부의 정보를 사용할 수 있다.

[0299] 예시적인 공통 회계장부

[0300] [0258] 시스템의 개별 모바일 컴퓨터들은 공통 회계장부로 칭해지는 데이터 구조를 유지할 수 있다. 공통 회계장부는, 재정 잔액 정보를 포함하지 않는 중앙 회계장부의 파생물일 수 있다. 공통 회계장부는, 시스템의 유효한 공개 키들, 즉, 사용자 아이덴티티들 전부의 리스트를 포함할 수 있다. 공통 회계장부는 또한, 개별 사용자들에 관한 정보, 이를테면, 사용자들의 디메리트들 또는 블랙리스트 상황(아래에 추가로 설명됨)을 포함할 수 있다.

[0301] [0259] 공통 회계장부는, 프로세싱 플랫폼에 의해 종종 업데이트될 수 있다. 배포될 때, 공통 회계장부는, 프로세싱 플랫폼에만 알려진 개인 키를 사용하여 암호화방식으로 싸인될 수 있다. 모든 각각의 수신측에는, 공통 회계장부 상의 서명을 검증하는 데 요구되는 대응하는 공개 키가 미리 프로비저닝될 수 있다.

[0302] 예시적인 거래 파트너 식별

[0303] [0260] 시스템의 디지털 수표가 구매자로부터 판매자로 전자적으로 송신될 수 있기 때문에, 구매자는 판매자의 아이덴티티에 확신이 없을 수 있다. 예컨대, 판매자로서의 역할을 하는 상인이 수취인으로서의 역할을 하는 구매자로부터 지불을 원할 때, 상인은 SRL을 통해 "PR(payment request)"을 발행할 수 있다. 지불 요청은, 상인의 ID(identifier), 예컨대 상인의 공개 키, 및 요청된 값을 포함할 수 있다. 악의적인 행위자는, 구매자가 지불 요청을 발행한 상인이 아니라 자신에게 디지털 수표를 잘못 전송할 수 있기를 바라면서, 상인과 거의 동시에 지불 요청을 생성했을 수 있다. 그에 따라서, 구매자는, 판매자를 식별할 수 있을 필요가 있을 수 있다. 구매자는 파트너 식별에 의해 판매자를 식별할 수 있다. 파트너 식별을 위한 방법들의 비-제한적인 예들은, 지불 인가, 노킹, 물리적 표시, 빔 형성, 이전 어레인지먼트, 피상적인 유효성 검증, 또는 이들의 임의의 조합을 포함한다.

[0304] *예시적인 지불 인가*

[0305] [0261] 일부 실시예들에서, 파트너 식별은 PA(payment authorization)를 포함할 수 있다. 예컨대, 구매자는 IP(intent to pay)를 발행할 수 있다. IP(intent to pay)는, 지불 요청에서 제공되는, 구매자에게 전송된 제로 값 거래, 예컨대, 판매자의 모바일 컴퓨터의 공개 키일 수 있다. IP(intent to pay)가 판매자의 MC에 도착한다면, 판매자는, 비-전자 방법들에 의해 그가 IP(intent to pay)의 수신측임을 표시할 수 있다. 예컨대, 판매자는, 그가 IP(intent to pay)를 수신했음을 구매자에게 구두로 알릴 수 있다. 판매자가, 그가 IP(intent to pay)의 수신측임을 구매자에게 표시할 때, 판매자의 요청된 지불은 유효성이 검증될 수 있고 구매자는 판매자에게 지불을 전송할 수 있다.

[0306] *예시적인 노킹*

[0307] [0262] 일부 실시예들에서, 파트너 식별은 노킹을 포함할 수 있다. 예컨대, 구매자의 MC(mobile computer)들 및 판매자의 모바일 컴퓨터는 물리적으로 접촉, 예컨대 노킹할 수 있다. 모바일 컴퓨터들은 모션 센서들을 포함할 수 있다. 그리고 구매자의 모바일 컴퓨터 및 판매자의 모바일 컴퓨터의 모션 센서들은 물리적 접촉을 측정할 수 있다. 구매자의 모바일 컴퓨터 및 판매자의 모바일 컴퓨터에 의해 측정되는 물리적 접촉의 동시성은 진본성의 증거일 수 있다. 판매자의 모바일 컴퓨터는, 노크가 발생할 때 지불 인가를 전송할 수 있다. 구매자의 모바일 컴퓨터는, 구매자의 모바일 컴퓨터 자신이 측정한 물리적 접촉의 시간 동시성 및 지불 인가의 수신에 기반하여 지불 인가를 수락할 수 있다. 일부 실시예들에서, 부가적인 보안을 제공하기 위해, 판매자는, 자신이 측정한 접촉의 서명을 구매자에게 전송할 수 있다. 접촉이 구매자의 모바일 컴퓨터에서 동등하고 상반되는 리액션을 야기할 수 있기 때문에, 구매자의 모바일 컴퓨터는 판매자의 모바일 컴퓨터에 의해 측정된 접촉의 유효성을 검증할 수 있다.

[0308] *예시적인 물리적 표시*

[0309] [0263] 일부 실시예들에서, 파트너 식별은 물리적 표시를 포함할 수 있다. 예컨대, MC(mobile computer)들이

(예컨대, 카메라들과 같은 이미징 센서들을 통해) 환경을 지각할 수 있다면, 2개의 모바일 컴퓨터들은 서로를 지각하도록 배향될 수 있다. 다른 MC의 관측된 포즈는, 파트너 식별을 위해 노킹이 사용될 때, 노크의 서명과 유사한 역할을 한다. 예컨대, A의 모바일 컴퓨터의 카메라가 B의 MC를 위로 그리고 좌측으로 본다면, B의 모바일 컴퓨터의 카메라는 A의 MC를 아래로 그리고 우측으로 보아야 한다. 지각된 배향들은 질적으로 또는 양적으로 비교될 수 있다.

[0310] *예시적인 빔 형성*

[0311] [0264] 일부 실시예들에서, 파트너 식별은 빔 형성을 포함할 수 있다. 예컨대, 모바일 컴퓨터들의 SRL(short range link)은 (예컨대, 빔-형성 또는 지향성 안테나를 사용하여) 지향성일 수 있다. 빔 형성을 이용하여, 구매자의 모바일 컴퓨터 및 판매자의 모바일 컴퓨터는, 지불 요청을 전송 또는 수신할 때 서로를 가리킬 수 있다. 그에 따라, 판매자의 모바일 컴퓨터로부터의 PR(payment request)이 구매자의 MC(mobile computer)에 전송될 수 있다. 다른 PR이 다른 방향으로부터 전송된다면, 구매자의 MC가 판매자의 MC를 향해 배향되기 때문에, 구매자의 모바일 컴퓨터에 의해 응답이 수신되지 못할 수 있다.

[0312] *예시적인 이전 어레인지먼트*

[0313] [0265] 일부 실시예들에서, 파트너 식별은 이전 어레인지먼트를 포함할 수 있다. 예컨대, 구매자는 특정 판매자의 ID(identifier)를 알 수 있고, 그에 따라, 유효성 검증이 불필요할 수 있다.

[0314] *예시적인 피상적인 유효성 검증*

[0315] [0266] 일부 실시예들에서, 파트너 식별은 피상적인 유효성 검증을 포함할 수 있다. 공통 회계장부는, 지불 요청의 피상적인 유효성 검증에 사용될 수 있는 식별 스트링, 예컨대 BigBoxStore를 포함할 수 있다. 예컨대, 상인은, 공통 회계장부의 프로세싱 플랫폼을 동작시키는 회사에 의해 BigBoxStore로서 식별될 수 있다. 그러한 식별은, BigBoxStore의 아이덴티티가 회사에 의해 유효성이 검증되었음을 표시하는 공통 회계장부의 표시, 예컨대 비트와 연관될 수 있다. 유효성이 검증된 아이덴티티는 사용자들 스스로에 의해 할당되거나 제공되는 아이덴티티들과 구별될 수 있다.

[0316] 에러 관리

[0317] [0267] 본원에서 개시된 시스템은, 디지털 수표의 배서들의 임의의 체인을, 그들이 진본일 때 인증할 수 있을 수 있다. 그러나, 디지털 수표들은 에러들을 포함할 수 있다. 시스템 내에서 동작하는 부도덕한 사용자들은 무효 디지털 수표들을 생성함으로써 시스템을 공격할 수 있거나, 또는 부도덕한 엔티티들은, 시스템의 다른 사용자들을, 이러한 다른 사용자들이 악의적인 행위자들로 보이게 함으로써 공격할 수 있다. 일부 실시예들에서, 일부 공격들은 초기에 다른 공격들과 구별불가능할 수 있다.

[0318] *다수의 판매자들에 대한 예시적인 구매자 클로닝*

[0319] [0268] 악의적인 구매자는, 디지털 수표를 싸인한 후 그를 카피하여, 2 명의 상이한 판매자들에게, 자신은 한 번만 지불하면서 판매자들 둘 모두로부터 상품들을 받을 수 있게 하려는 목표로, 디지털 수표의 동일한 카피들을 전송할 수 있다. 도 26은, 다수의 판매자들에 대한 구매자 클로닝으로서 지칭될 수 있는 이러한 악의적인 거동의 예를 개략적으로 예시한다. 예컨대, 악의적인 구매자는, 디지털 수표가 제1 판매자에 대해 의도된 때, 디지털 수표의 동일한 카피들을 제1 판매자 및 제2 판매자에게 전송할 수 있다. 디지털 수표의 카피를 수신할 시에, 제2 판매자는 자신이 수신한 디지털 수표가 그에 배서가 되어 있지 않다는 것을 즉시 결정할 수 있다. 그에 따라서, 제2 판매자는 디지털 수표를 거절할 수 있다.

[0320] *단일 판매자에 대한 예시적인 구매자 클로닝*

[0321] [0269] 악의적인 구매자는, 디지털 수표를 싸인한 후 그를 카피하여, 동일한 판매자에 대해, 자신은 한 번만 지불하면서 그 판매자로부터 상품들을 2번 받을 수 있게 하려는 목표로, 나중에 그 디지털 수표를 재사용하려 시도할 수 있다. 도 27은, 단일 판매자에 대한 구매자 클로닝으로서 지칭될 수 있는 이러한 악의적인 거동을 개략적으로 예시한다. 판매자의 MC(mobile computer)는 그러한 악의적인 거동을 검출할 수 있다. 예컨대, 판매자의 모바일 컴퓨터는, 자신이 디지털 수표들을 수신한 임의의 특정 사용자로부터의 마지막 디지털 수표로부터의 수표 ID의 레코드를 유지할 수 있다. 일부 실시예들에서, 수표 ID들이 엄격하게 증가하는 순서로 발행될 수 있기 때문에, 판매자의 모바일 컴퓨터는, 자신이 임의의 특정 사용자로부터 수신한 마지막 디지털 수표의 ID를 계속해서 추적할 수 있다. 일부 실시예들에서, 판매자의 모바일 컴퓨터는, 자신이 수신한 모든 디지털 수표들의 ID들을 계속해서 추적할 수 있다. 특정 사용자로부터 수신된 임의의 새로운 디지털 수표는, 레코드 상의

가장 높은 수표 ID보다 큰 수표 ID를 가져야 한다.

[0322] [0270] 중앙 회계장부가 카피된 디지털 수표를 항상 검출할 수 있기 때문에, 프로세싱 플랫폼은 결코 카피된 디지털 수표를 지불하지 않을 것이다. 따라서, 거래들의 이러한 레코드를 유지하는 것은 판매자의 책임이다. 판매자의 MC는, 거래들 및 자신이 수신한 디지털 수표들을 자동으로 로깅(log)할 수 있는 소프트웨어 프로그램 또는 하드웨어 프로그램을 실행하고, 모든 새로운 거래들을 이러한 로그에 대하여 비교할 수 있다.

[0323] *예시적인 포킹*

[0324] [0271] 악의적인 판매자는 구매자로부터 디지털 수표를 수신할 수 있다. 디지털 수표를 수신한 후에, 판매자는, 디지털 수표에 배서하기 전에 그를 카피하여, 제2 판매자에게, 제2 판매자로부터의 상품들을 그 상품들에 대해 지불하지 않으면서 구매하려는 목적으로, 수신된 디지털 수표를 사용하여 지불하려 시도할 수 있다. 도 28은, 수표 포킹으로서 지칭될 수 있는 이러한 악의적인 거동을 개략적으로 예시한다. 제2 판매자는, 악의적인 판매자로부터 수신된 디지털 수표를, 수신된 디지털 수표가 자신을 의도된 수신측으로서 표시하지 않는다는 것을 검증할 수 있기 때문에 거절할 수 있다.

[0325] *예시적인 판매자 클로닝*

[0326] [0272] 악의적인 판매자는, 수신된 디지털 수표가 거래에 대해 2번 지불될 수 있게 하려는 목표로, 수신된 디지털 수표를 복사하여 그 수표를 2번 예치할 수 있다. 도 29는, 판매자 클로닝으로서 지칭될 수 있는 이러한 악의적인 거동을 개략적으로 예시한다. 악의적인 판매자는, 구매자가 구매자 클로닝으로 고발되게 하려는 의도로 판매자 클로닝을 시도할 수 있다.

[0327] [0273] 중앙 회계장부가 구매자로부터 동일한 수표 ID 번호를 포함할 수 있기 때문에, 프로세싱 플랫폼은, 악의적인 판매자가 수신된 디지털 수표를 재차 예치할 때 이러한 악의적인 거동을 식별할 수 있다. 이러한 공격을 검출하기 위해, 중앙 회계장부는, 모바일 컴퓨터의 특정 발신 ID로부터 상환된 모든 수표 ID 번호들의 레코드를 보유할 수 있다. 일부 실시예들에서, 공통 회계장부는 이러한 레코드를 포함할 수 있고 시스템의 사용자들 또는 모바일 디바이스들에 배포될 수 있다. 그에 따라서, 사용자들 또는 사용자 디바이스들은 순서를 벗어나(out of order) 수신되는 디지털 수표들을 수신할 수 있다.

[0328] *예시적인 마우징*

[0329] [0274] 악의적인 구매자는 그것의 모바일 컴퓨터의 보안 엘리먼트를 바이패스하고 그리고 디지털 수표의 거짓 서명을 생성할 수 있다. 거짓 서명은 악의적인 구매자의 모바일 컴퓨터의 개인 키를 사용하지 않고 생성된 서명일 수 있다. 도 30은 마우징으로서 지칭될 수 있는 이런 악의적인 거동을 개략적으로 예시한다. 악의적인 구매자의 목표는, 디지털 수표가 상환불가능할 수 있는 경우에는 그것이 악의적인 구매자로부터 발신된 것임을 판매자가 검증할 수 없다는 이유에 있을 수 있다. 디지털 수표의 서명은 구매자의 ID, 예컨대 디지털 수표의 부분인 악의적인 구매자의 공개 키로 암호해독될 수 없기 때문에, 판매자는 이런 악의적인 거동을 즉시 검출가능할 수 있다. 그에 따라서, 판매자는 디지털 수표를 즉시 거절할 수 있다.

[0330] *예시적인 고스팅*

[0331] [0275] 악의적인 구매자는 고유의 ID와는 상이한 ID를 사용하여 디지털 수표를 생성할 수 있고, 그 디지털 수표는 그런다음 상이한 ID와 연관된 개인 키를 사용하여 싸인된다. 도 31은 고스팅으로서 지칭될 수 있는 이런 악의적인 거동을 개략적으로 예시한다. 판매자는, 디지털 수표가 회계장부에 도달하는 때를 프로세싱 플랫폼이 검출가능할 수 있는 동안에 만약 판매자가 시스템의 모든 사용자들의 최신 리스트를 갖는다면 고스팅을 검출할 수 있다. 판매자는 공통 회계장부의 카피를 가질 수 있고, 그리고 그의 공통 회계장부가 디지털 수표에 대한 구매자 ID를 포함하지 않는 경우에는 디지털 수표를 거절할 수 있거나 또는 위험부담을 안고 디지털 수표를 수락할 수 있다. 일부 실시예들에서, 시스템은 암호화 알고리즘의 전유 변형을 이용하여서, 고스팅을 불가능하게 만들 수 있다.

[0332] 예시적인 메리트, 디메리트, 및 블랙리스트

[0333] [0276] 사용자들에 의한 특정 활동들은 원해지지 않을 수 있다. 시스템은 원하지 않는 활동들에 수반되어진 사용자들에게 다양한 방식들로 응답할 수 있다. 제1 타입의 원하지 않는 활동들은 모바일 컴퓨터들 또는 MC(mobile computer)들 상에서 실행되는 컴퓨터 프로그램들의 어떤 명확한 수정도 요구하지 않는다. 제1 타입의 원하지 않는 활동들, 당좌대월들은 디지털 수표들을 "바운싱하는 것", 예컨대 발행자의 잔액이 지원할 수 있는 것 보다 디지털 수표들의 더 많은 값을 발행하는 것을 포함할 수 있다. 사용자들이 당좌대월들에 수반될

때, 시스템은 그것들에 디메리트들을 제공할 수 있다. 디메리트 시스템은, 예컨대, 바운싱된 디지털 수표들의 수에 기반한 디메리트들, 바운싱된 디지털 수표들의 값에 기반한 디메리트들, 바운싱된 디지털 수표들의 최신성에 기반한 디메리트들, 또는 이들의 임의의 조합 중 하나 이상을 계속해서 추적할 수 있다. 디메리트 시스템은 디메리트들 중 일부 또는 모두를 정규화할 수 있고 그리고 상환된 디지털 수표들의 총 번호 또는 상환된 모든 디지털 수표들의 값들에 의해 계속해서 추적한다.

[0334] [0277] 제2 종류의 원하지 않는 활동들, 해킹은 모바일 컴퓨터들, 모바일 컴퓨터들의 SE(secure element)들, 또는 모바일 컴퓨터들 상에서 실행되는 컴퓨터 프로그램들을 탬퍼링하는 것을 요구할 수 있다. 제2 종류의 원하지 않는 활동들은 이전 섹션에서 언급된 공격들, 예컨대 포킹, 클로닝, 또는 마우징을 포함할 수 있는데, 이것들은 모바일 컴퓨터들, 모바일 컴퓨터들의 보안 엘리먼트들, 모바일 컴퓨터들 상에서 실행되는 컴퓨터 프로그램들의 명확한 해킹 또는 수정(즉, 모바일 컴퓨터들, 보안 엘리먼트들 또는 컴퓨터 프로그램들의 거동들의 비인가된 수정)을 요구한다. 시스템은 모바일 컴퓨터들 상에서 실행되는 컴퓨터 프로그램들에 대한 체크섬들 및 싸인된 증명서들을 사용하여 일부 해킹들을 검출할 수 있다. 사용자들이 해킹에 수반될 때, 시스템은 이들을 블랙리스트에 올릴 수 있다. 블랙리스트는 일시적으로 또는 향후 모든 거래들이 금지되는 사용자 ID들의 리스트일 수 있다. 사용자 ID들이 모바일 컴퓨터들에 독특하게 결부될 수 있기 때문에, 사용자 ID를 블랙리스트에 올리는 것은 모바일 컴퓨터를 블랙리스트에 올리는 것과 동일할 수 있다. 해킹된 디바이스로부터 발신되는 공격에 참여한 것으로 보이는 어떤 사용자도 블랙리스트에 오를 수 있다.

[0335] *예시적인 싸인된 내역서들*

[0336] [0278] 판매자들은 특정 타입들의 해킹을 즉시 검출할 수 있다. 예컨대, 다수의 판매자들에 대한 구매자 클로닝의 경우, 제2 판매자는 자신이 악의적인 "해킹된" 수표를 수신하였음을 즉시 검출할 수 있다. 만약 그러한 해킹 이벤트가 프로세싱 플랫폼에 리포트된다면 유리할 수 있다. 예컨대, 판매자의 모바일 컴퓨터는 수신된 디지털 수표를 MC("malicious cheque") 배서로 배서할 수 있다. MC 배서들은 제2 판매자로부터의 임의의 다른 디지털 수표들처럼 싸인될 수 있고, 배서된 수표는 그 판매자 소유의 다른 디지털 수표들이 프로세싱 플랫폼에 상환될 때 프로세싱 플랫폼에 송신될 수 있다.

[0337] [0279] 싸인된 MC 배서의 프로세싱 플랫폼에 의한 수신은 악의적인 행위자가 시스템에 존재함을 의미할 수 있다. 그러나, 악의적인 행위자의 아이덴티티는 불명료할 수 있다. 예컨대, 판매자에 의해서 제공되는 MC는 그것이 실제로 거래되는 악의적인 구매자로부터의 구매자 클로닝을 표시할 수 있지만, 그것은 또한 구매자 클로닝의 구매자를 고발할 목표로 구매자의 체크를 스스로 클로닝하는 악의적인 판매자에 의해 수신된 적법한 디지털 수표일 수 있다. 여하튼, 악의적인 행위자가 시스템에 존재한다.

[0338] *예시적인 퍼지 규칙*

[0339] [0280] 일부 부류의 해킹들의 경우에, 거래시 특정 당사자에게 분명히 책임을 묻는 것은 어렵거나 불가능할 수 있다. 그러나, 디지털 수표들은 거래시 당사자들에게만 이용가능한 서명들을 사용하여 싸인되기 때문에, 임의의 수의 당사자들 중 한 명의 당사자에게 죄를 묻는 것이 가능할 수 있다. 예컨대, 만약 2개의 동일한 디지털 수표들이 프로세싱 플랫폼에서 상환된다면, 발신자(구매자) 또는 예금자(판매자)는 악의적인 행위자일 수 있다. 그러한 관찰시, 비-제한적인 규칙이 생성될 수 있다:

[0340] M (구매자) + M (전송자) = 참, (규칙 4)

[0341] 여기서, M()은 아규먼트가 악의적인지를 결정하는 부울 오퍼레이터를 나타내고, "+"는 논리적 OR 연산을 나타낸다.

[0342] [0281] 이런 정보는 향후 사용을 위해 저장될 수 있다. 예컨대, 만약 중앙 회계장부가 상이한 판매자 및 동일한 구매자로부터 다른 쌍의 동일한 디지털 수표들을 나중에 수신한다면, 다른 비-제한적인 규칙이 생성될 수 있다:

[0343] (M (구매자) + M (제1 판매자)) * (M (구매자) + M (제2 판매자)) = 참, (규칙 5)

[0344] 여기서, "*"는 논리적 AND 연산을 나타낸다. 규칙 5는 다음과 같이 다시 쓰여질 수 있다:

[0345] M (구매자) + (M (제1 판매자) * M (제2 판매자)) = 참. (규칙 6)

[0346] [0282] 예컨대, 규칙들을 해석하는 데 있어, 프로세싱 플랫폼은 두 행위자들 중 아무도 악의적이지 않음을 가정할 수 있다. 그에 따라서, 프로세싱 플랫폼은 구매자가 악의적이라고 규칙 6으로부터 결론을 내릴 수 있다.

다른 예로서, 프로세싱 플랫폼은, 악의적인 행위자들이 드물어서 0보다 크고 1보다 작은 확률 "p"로 발생한다는 사전 믿음을 주장할 수 있다. 그런다음, 판매자들 둘 모두가 악의적일 확률은 규칙 6에서 p*p일 수 있다. 규칙 6의 왼쪽 사이즈는 p+p*p로서 표현될 수 있다.

[0347] [0283] 유사하게, 그러한 해석들 및 가정들은 시스템에 의해서 모든 사용자들의 모든 관측들을 포함하도록 확장될 수 있고, 그리고 곱들의 합 형태로 표현될 수 있다. 따라서, 곱에서 최소 엘리먼트들을 갖는 조건은 참일 가능성이 가장 높을 수 있다. 이들 행위자들은 악의적인 것 및 블랙리스트에 오른 것으로서 즉시, 임시로, 또는 향후 조사되어 라벨링될 수 있다.

[0348] 예시적인 PoS(Point of Sale)

[0349] [0284] 시스템은 PoS(point of sale) 시스템과 상호작용할 수 있다. 도 32는 PoS(point of sale) 거래의 예를 개략적으로 예시한다. PoS(point of sale) 시스템은 현금 등록기 또는 등가물일 수 있다. PoS(point of sale) 시스템은 고정 위치에 있을 수 있다. PoS(point of sale) 시스템은 인프라구조, 예컨대 BigBoxStore와 같은 상인의 현금 등록기들을 갖는 기존 인프라구조의 부분일 수 있다.

[0350] [0285] 상인은 하나 이상의 사용자 ID(identifier)들과 연관될 수 있다. 상인은 단일 계정, 현금 등록기마다 하나의 계정, 또는 저장 위치마다 하나의 계정을 가질 수 있다. 상인의 계정들은 다른 사용자들과 같이 모바일 컴퓨터들과 연관될 수 있거나, 또는 시스템에 의해서 상인에게 발행된 키 쌍들과 연관될 수 있다. 상인 키 쌍들은 상인이 소유한 컴퓨터들에 의해서 관리될 수 있거나, 또는 SaaS("software as a service")와 유사한 서비스로서 회사에 의해 호스팅될 수 있다.

[0351] [0286] 상인을 위해 작동하는 체커, 캐셔, 또는 PoS 오퍼레이터는 그에게 특별히 발행된 MC(mobile computer)에 액세스할 수 있거나, 또는 모바일 컴퓨터는 상인을 위해 작동하는 인가된 체커들, 캐셔들, 또는 PoS 오퍼레이터들에 의해서 다수의 로그인들을 지원할 수 있다.

[0352] [0287] 구매자가 상품 또는 서비스들을 상인에게서 구매기를 원할 때, 구매자는 상인의 사용자 ID에 발행되지만 SRL(short range link)을 통해 체커에 송신되는 디지털 수표를 생성할 수 있다. 일단 체커의 소유이면, 체커는 예컨대 상인의 네트워크에 액세스함으로써 디지털 수표가 유효함을 검증할 수 있다. 상인의 네트워크는 구매자가 아닌 체커가 액세스할 수 있는 보안 IEEE(Institute of Electrical and Electronics Engineers) 802.11 네트워크 또는 유사한 네트워크들일 수 있다. 체커는 예컨대 상인의 보안 네트워크를 통해 상인의 월렛에 디지털 수표를 송신할 수 있다.

[0353] [0288] PoS(point of sale) 시스템을 수반하는 거래시에, 구매자로부터의 오리지널 디지털 수표가 상인을 위해 발행될 수 있지만 체커에게 제공될 수 있다. 그런다음, 체커는 상인에게 디지털 수표를 송신하기 전에 HBE("handled by endorsement")를 부가할 수 있다. 그런다음, 상인은 FDOE("for deposit only endorsement")를 부가하고 그리고 프로세싱 플랫폼에 디지털 수표를 상환할 수 있다.

[0354] [0289] 디지털 수표를 상인에게 전송하기 전에, 체커는 그 소유의 사용자 ID를 포함하면서 그의 모바일 컴퓨터의 보안 엘리먼트에 의해 싸인된 HBE("handled by" endorsement)를 부가할 수 있다. 상인은 그의 체커들 중 하나로부터의 HBE가 마킹된 디지털 수표들만을 핸들링하기로 선정할 수 있다.

[0355] [0290] 디지털 수표가 상인에 의해서 상환될 때, 프로세싱 플랫폼이 디지털 수표를 클리어하였다는 것을 표시하는 메시지가 예컨대 HBE를 사용하여 체커에게 전송될 수 있다. 이 때, 체커는 디지털 수표의 값을 "입찰 체크" 또는 적합한 목적지로서 캐시 레지스터에 입력함으로써 판매를 종료할 수 있다.

[0356] [0291] 상인의 PoS 시스템은 거의 변경을 요구하지 않거나 어떤 변경도 요구하지 않을 수 있다. 상인은 모바일 컴퓨터들을 그의 체커들에게 발행할 수 있다. 일부 체커들은 그들 소유의 MC들을 소유할 수 있고, 그리고 상인은 체커들의 개인적으로 소유된 MC들로부터 발행되는 HBE를 갖는 디지털 수표들을 수락하기로 선정할 수 있다.

[0357] 중앙 회계장부에 관한 펀드들의 예시적인 입출

[0358] [0292] 펀드들은 다른 공통 통화 증서들로부터 중앙 회계장부에 들어가고 나갈 수 있다. 사용자 또는 사용자 디바이스가 중앙 회계장부에 돈을 부가하길 원할 때, 프로세싱 플랫폼은 그 돈을 사용자 또는 사용자 디바이스의 계정에 입금 방법(transfer-in method)을 통해서 송금할 수 있다. 입금 방법은 신용 카드들로부터의 인출, ACH(automated clearing house) 송금, 물리적 체크의 메일링, 또는 물리적 현금 증서들의 핸들링일 수 있다. 프로세싱 플랫폼은 돈을 수신한 후에 사용자 또는 사용자 디바이스의 계정에 입금할 수 있다. 거래 수수료들이

존재하는 그런 증서들의 경우에, 프로세싱 플랫폼은 이들 수수료들을 변제할 수 있거나 변제하지 않을 수 있다.

[0359] [0293] 사용자 또는 사용자 디바이스가 중앙 회계장부로부터 돈을 옮기길 원할 때, 프로세싱 플랫폼은 그 돈을 사용자 또는 사용자 디바이스의 계정으로부터 출금 방법(transfer-out method)을 통해서 송금할 수 있다. 출금 방법은 ACH 송금, 물리적 체크의 메일링, 또는 임의의 유사한 수단일 수 있다. 프로세싱 플랫폼은 출금 방법을 사용하여 돈을 전송하기 이전에 사용자 또는 사용자 디바이스의 계정을 데빗팅할 수 있다. 프로세싱 플랫폼은 돈이 옮겨진 것에 대한 수수료를 청구할 수 있다. 이런 수수료는 상이한 커스터머들에 대해서 또는 상이한 타입들의 커스터머들에 대해서 상이할 수 있다.

[0360] [0294] 상인들 또는 사용자들은 키 쌍들에 대해서 청구받을 수 있다. 예컨대, 상인들 또는 사용자들은 주기적으로(예컨대, 매 달), 또는 단지 한번만(예컨대, 셋업 동안에) 청구받을 수 있다. 키 쌍들은 고정 가격 또는 협상 가격으로 팔릴 수 있고, 그 협상 가격은 다수의 활성 키 쌍들을 갖는 상인들에 대한 수량 할인들을 포함할 수 있다. 프로세싱 플랫폼은 일부 사용자들 또는 상인들을 위한 선호적 또는 배타적 가격책정을 가질 수 있다.

[0361] 예시적인 수수료들

[0362] [0295] 위에서 설명된 바와 같이, 시스템 내로의, 시스템 밖으로의, 또는 시스템 내에서의 임의의 송금에 대해 수수료들이 청구될 수 있다. 이들 송금 수수료들은 거래 사이즈에 비례하거나, 고정되거나, 또는 그 둘의 조합일 수 있다. 불충분한 계정 잔액들을 갖는 사용자 디바이스들에 의해 발행된 디지털 수표들에 대해서 수수료들이 또한 평가될 수 있다. 프로세싱 플랫폼은 생성된 부채를 커버하기로 선택할 수 있고, 그리고 그런 경우에는 최종 부채와 연관된 이자 또는 수수료들을 청구할 수 있다.

[0363] 예시적인 소싱된 거래들

[0364] [0296] 본원에서 개시된 시스템에서의 거래들은 중앙 회계장부를 통해 구매자의 계정의 이용가능한 잔액로부터 "소싱"될 수 있다. 구매자가 알려진 소스로부터 공통 회계장부로 자신의 펀드들을 자동으로 인출할 디지털 수표를 발행하는 것이 유리할 수 있지만, 그 일부는 아닐 수 있다. 예컨대, 구매자는 $100로 상인에게서 물품을 구매하길 원할 수 있고, 그리고 구매자의 은행의 구매자의 체킹 계정과 같은 특정 소스로부터 또는 특정 신용 카드로부터 $100을 인출하도록 중앙 회계장부에 요구할 수 있다. 시스템은 은행 계정 정보 또는 신용 카드 정보와 같은 SI(source information)를 중앙 회계장부에 입력하기 위한 인터페이스들을 포함할 수 있다. 구매자들의 모바일 컴퓨터들은 SAIS(source accounts with identification strings)를 저장할 수 있다. 디지털 수표는 SAIS를 저장하기 위한 데이터 필드를 포함할 수 있다.

[0365] [0297] 소스 정보를 시스템에 입력하기 위한 인터페이스들은 상이한 구현들에서는 상이할 수 있다. 예컨대, 인터페이스들은 MC 상의 "앱" 또는 웹페이지를 포함할 수 있다. 그런 인터페이스는 물리적 체크, 은행 내역서, 물리적 신용 카드, 신용 카드 내역서, 또는 이들의 임의의 조합으로부터 소스 정보를 추출하기 위한 시각적 인터페이스(예컨대, 디지털 카메라 및 소프트웨어 구현 컴퓨터 비전 알고리즘들을 사용하는)를 포함할 수 있다.

[0366] [0298] 시스템은 공백의 SAIS 필드를 갖는 디지털 수표들을 수락하지 않을 수 있다. 만약 시스템이 공백의 SAIS 필드를 갖는 디지털 수표들을 수락한다면, 공백의 SAIS 필드는 프로세싱 플랫폼이 사용자들의 계정들 또는 다른 디폴트 소스들에 있는 펀드들을 인출해야 함을 암시하는 것으로 해석될 수 있다.

[0367] [0299] 디지털 수표들은 수수료 공유 정책을 표시하는 수수료 공유 필드들을 포함할 수 있다. 수수료 공유 필드들은 비트들, 비트 필드들, 또는 구매자가 소싱과 연관된 수수료들을 지불할 것 또는 판매자들 또는 구매자들이 소싱과 연관된 수수료들을 어떻게 분할할지와 같은 수수료 공유 정책을 표시하는 다른 넘버들일 수 있다. 예컨대, 디지털 수표는, 구매자가 소스 계정과 연관된 소싱 수수료들(예컨대, 신용 카드 수수료)을 지불할(또는 지불하지 않을) 것임을 표시하는 비트, 및 구매자가 송금 수수료(예컨대, 구매자의 계정으로부터 판매자의 계정으로의 펀드들의 송금에 대해 프로세싱 플랫폼에 의해서 청구되는 수수료)를 지불할(또는 지불하지 않을) 것임을 표시하는 제2 비트를 포함할 수 있다.

[0368] [0300] 시스템은 이들 수수료들이 구매자들 또는 판매자들에게 보이거나 보이지 않게 만들 수 있다. 일부 실시예들에서, 판매자들은 그들의 연관된 수수료들 및 구매자의 수수료 공유 정책에 기반하여 선택적으로 디지털 수표들을 거부하는 것이 가능할 수 있다.

[0369] 예시적인 펀드 검증

[0370] [0301] 판매자는 인터넷과 같은 네트워크를 통해 프로세싱 플랫폼에 연결될 수 있지만, 구매자는 그렇지 않을 수 있다. 예컨대, 비록 구매자가 예컨대 열악한 셀룰러 전화 연결성 때문에 프로세싱 플랫폼에 연결될 수 없을

지라도, 상인은 그의 사설 네트워크 연결을 통해 인터넷으로의 유선 또는 무선 연결성을 가질 수 있다. 판매자가 인터넷에 액세스할 때, 판매자는 거래를 수락하기 전에 구매자의 계정의 펀드들의 가용성을 검증할 수 있다.

[0371] [0302] 예컨대, 판매자는 디지털 수표가 단지 질의로서만 사용되어야 함을 표시하는 QE("query endorsement")와 같은 배서를 갖고 구매자에 의해 발행된 디지털 수표의 배서된 버전을 제출하도록 허용될 수 있다. 그런 QE(query endorsement)는 판매자에 의해서 싸인될 수 있다. QE를 갖는 디지털 수표를 수신할 때, 프로세싱 플랫폼은 거래를 완료하기 위한 구매자의 능력 및 구매자에 관한 정보를 판매자에게 리턴할 수 있다. 예컨대, 프로세싱 플랫폼은 즉각적인 펀드 가용성과 같은 정보(현재 중앙 회계장부 잔액, 또는 현재 중앙 회계장부 잔액이 디지털 수표의 값을 충족하거나 초과하는지 여부), 디지털 수표가 SAIS 필드에 의해 소싱되는 경우의 소스 정보(예컨대, 현재 펀드들에 대한 당좌대월이 예상되는 경우의 디폴트 소스 정보를 포함함), 또는 이들의 임의의 조합을 리턴할 수 있다. 소스 정보는 수수료들에 관한 정보를 포함할 수 있다. 수수료 공유 필드들은, 수수료 정보가 QE 디지털 수표에 대한 응답으로 공유될 지를 결정하는 데 사용될 수 있다(예컨대, 수수료 정보는 구매자가 수수료들을 커버하고 있음을 표시하는 디지털 수표를 홀딩하고 있는 판매자와 공유되지 않을 수 있음).

[0372] 금융 기관을 수반하는 암호화방식으로 싸인된 디지털 수표들의 예시적인 보안 교환

[0373] [0303] 본 개시내용의 콘텐츠들 및 레코드들(예컨대, 암호화방식으로 싸인된 디지털 수표들)을 안전하게 교환하는 시스템들 및 방법들이 하나 이상의 사용자 디바이스들, 하나 이상의 프로세싱 플랫폼들, 및 하나 이상의 금융 기관 서버들에 의해서 구현될 수 있다. 도 33은 하나의 금융 기관을 수반하는 암호화방식으로 싸인된 디지털 수표들을 안전하게 교환하는 다른 실시예를 개략적으로 예시한다. 도 33에 도시된 비-제한적인 예시적 실시예에서, 사용자들은 암호화방식으로 싸인된 디지털 수표들과 같은 개별 레코드들(100)을 생성, 전송, 수신, 수정, 또는 상환하도록 사용자 디바이스들을 동작시킬 수 있다. 예컨대, 디지털 수표의 전송자(102a)는 수표 전송자 디바이스(116a 또는 116a')를 동작시킬 수 있다. 디지털 수표의 수신자(102b)는 수표 수신자 디바이스(116b)를 동작시킬 수 있다.

[0374] [0304] 사용자 디바이스들, 예컨대 수표 전송자 디바이스(116a) 및 수표 수신자 디바이스(116b)는 동일할 수 있거나 또는 상이할 수 있다. 사용자 디바이스들은 셀룰러 전화들, 태블릿 컴퓨터들, e-리더들, 스마트 시계들, 머리 장착 증강, 가상 또는 혼합 현실 디스플레이 시스템들, 웨어러블 디스플레이 시스템들, 또는 컴퓨터들을 포함할 수 있다. 사용자 디바이스(116a 또는 116b)는 통신 링크(120a, 120b), 예컨대 셀룰러 통신 링크를 사용하여 네트워크(118) 상의 다른 디바이스들과 통신할 수 있다. 네트워크(118)는 LAN(local area network), WAN(wide area network), 또는 예컨대 IEEE(Institute of Electrical and Electronics Engineers) 802.11 표준들을 구현하는 유선 또는 무선 통신 링크들에 의해 액세스가능한 인터넷일 수 있다.

[0375] [0305] 디지털 수표(100)를 전송할 때, 수표 전송자 디바이스(116a) 및 수표 수신자 디바이스(116b) 중 하나 또는 둘 모두는 오프라인일 수 있고, 네트워크(118)에 연결되지 않을 수 있다. 수표 전송자 디바이스(116a)를 사용는 수표 전송자(102a)는, 암호화방식으로 싸인된 디지털 수표(100)를 수표 수신자(102b)에 SRL(short range link)(122)을 사용하여 전송할 수 있다. SRL(short range link)(122)은 피어-투어-피어 라디오 또는 다른 링크들일 수 있고, 그 링크들을 통해서 사용자 디바이스(116a 또는 116b)가 서로 통신할 수 있다. SRL(short range link)(122)은 IrDA(Infrared Data Association)/IrPHY(Infrared Physical Layer Specification), 블루투스®, NFC(Near Field Communication), 애드 혹 802.11, 또는 임의의 다른 유선 또는 무선 통신 방법들 또는 시스템들에 기반할 수 있다.

[0376] [0306] 서비스 제공자(104)에 의해서 동작되는 프로세싱 플랫폼(124)은 통신 링크(126)를 사용하여 네트워크(118) 상의 다른 디바이스들, 예컨대 사용자 디바이스들(116a, 116b)과 통신할 수 있다. 서비스 제공자(104)에 의해서 동작되는 금융 기관 서버(3304) 또는 프로세싱 플랫폼(104)과 연계된 금융 기관은 네트워크(118) 상의 다른 디바이스들, 예컨대 프로세싱 플랫폼(124)과 통신할 수 있다. 통신 링크(120a, 120b, 126, 또는 3304)는 유선 또는 무선 통신들, 셀룰러 통신, 블루투스®, LAN(local area network), WLAN(wide local area network), RF(radio frequency), IR(infrared), 또는 임의의 다른 통신 방법들 또는 시스템들일 수 있다.

[0377] [0307] 사용자들(102a 또는 102b)은 암호화방식으로 싸인된 디지털 수표들을 프로세싱 플랫폼(124)에 상환할 수 있다. 예컨대, 수표 전송자 디바이스(116a)를 동작시키는 전송자(102a),는 수표 수신자 디바이스(116b)를 동작시키는 수신자(102b)인 판매자로부터의 서비스 또는 제품의 구매자일 수 있다. 도 33b를 참조로, 디지털 수표(100)의 콘텐츠(110)는 전송자(102a)의 계정으로부터 수신자(102b)의 계정으로 송금하기 위한 상당한 금액의 암호화폐(또는 실제 통화) 또는 프로세싱 플랫폼(124)이 전송자(102a)의 계정으로부터 수신자(102b)의 계정으로(또는 수표 전송자 디바이스(116a)의 계정으로부터 수표 수신자 디바이스(116b)의 계정으로) 상당한 금액의

암호화폐를 송금하게 하기 위한 명령들을 포함할 수 있다. 수표 전송자 디바이스(116a)는 전송자 디바이스 개인 키를 사용하여 디지털 수표(100)를 디지털적으로 싸인할 수 있고, 디지털 수표(100)를 수신자 디바이스(116b)에 전자적으로 통신한다. 수신자 디바이스(116b)는 배서(114)로 수표를 배서하고(예컨대, 이런 맥락에서, 배서는 "예금만을 위한 배서"일 수 있음), 그리고 수정된 디지털 수표(100m1)를 생성하기 위해서 수신자 디바이스 개인 키를 사용하여 디지털 수표를 디지털적으로 싸인한다. 수신자 디바이스(116b)는 수정된 디지털 수표(100m1)를 서비스 제공자(104)에게 통신하고, 서비스 제공자(104)는 수정된 디지털 수표(100m1)를 상환한다.

[0378] [0308] 프로세싱 플랫폼(124)은, 수정된 디지털 수표(100m1)가 전송자 디바이스(116a) 및 수신자 디바이스(116b) 둘 모두에 의해서 (그들의 개개의 공개 키들을 사용하여) 진정으로 싸인되었음을 검증할 수 있다. 결과적으로, 프로세싱 플랫폼(124)은 전송자(102a)의 계정으로부터 수신자(102b)의 계정으로(또는 수표 전송자 디바이스(116a)의 계정으로부터 수표 수신자 디바이스(116b)의 계정으로) 상당한 금액의 암호화폐를 송금하도록 금융 기관 서버(3304)에 명령할 수 있다. 금융 기관 서버(3304)는 전송자(102a)의 계정 및 수신자(102b)의 계정을 유지할 수 있다. 일부 구현들에서, 프로세싱 플랫폼(124)은 또한 전송자(102a)의 계정의 잔액 및 수신자(102b)의 계정의 잔액을 계속 추적할 수 있다. 그에 따라서, 이런 비-제한적인 예에서, 레코드는 디지털 수표 시스템에서 수표로서 기능하고, 그리고 자산에 대해 판매자(수신자(102b))에게 지불하기 위해서 구매자(전송자(102a))에 의해 사용될 수 있다. 서비스 제공자(104)는 이런 교환의 적어도 일부를 위해 (예컨대, 구매자의 암호화폐 또는 실제 통화 계정을 데빗팅하고 판매자의 암호화폐 계정에 입금하기 위한) 어음 교환소로서의 역할을 할 수 있다.

[0379] [0309] 도 33c는 암호화방식으로 싸인된 디지털 수표들을 안전하게 교환하는 다른 실시예를 개략적으로 예시한다. 수정된 디지털 수표(100m1)를 수신한 후에, 프로세싱 플랫폼(124)은, 수정된 디지털 수표(100m1)가 전송자 디바이스(116a) 및 수신자 디바이스(116b) 둘 모두에 의해서 (그들의 개개의 공개 키들을 사용하여) 진정으로 싸인되었음을 검증할 수 있다. 결과적으로, 프로세싱 플랫폼(124)은 금융 기관의 전송자(102a)의 계정으로부터 다른 금융 기관의 수신자(102b)의 계정으로(또는 금융 기관의 수표 전송자 디바이스(116a)의 계정으로부터 다른 금융 기관의 수표 수신자 디바이스(116b)의 계정으로) 상당한 금액의 암호화폐를 송금하도록 금융 기관의 서버(3304a)에 명령할 수 있다. 금융 기관 서버(3304a)는 전송자(102a)의 계정을 유지할 수 있다. 금융 기관 서버(3304b)는 수신자(102b)의 계정을 유지할 수 있다. 상당한 금액의 암호화폐의 송금을 수신한 후에, 다른 금융 기관의 서버(3304b)는 다른 금융 기관의 수신자(102b)의 계정(또는 수표 수신자 디바이스(116b)의 계정)의 잔액을 업데이트할 수 있다. 일부 구현들에서, 프로세싱 플랫폼(124)은 또한 전송자(102a)의 계정의 잔액 및 수신자(102b)의 계정의 잔액을 계속 추적할 수 있다.

[0380] [0310] 일부 실시예들에서, 본원에서 설명된 용어들 중 일부는 15 U.S.C.§1693에서 정의(소비자 보호에 대한 정의들)된 바와 같은 의미들을 가질 수 있다. 예컨대, 금융 기관은 주립 또는 국립 은행, 주립 또는 연방 저축 대부조합, 상호 저축 은행, 주립 또는 연방 신용 조합, 또는 소비자에게 속하는 계정을 간접적으로 또는 직접적으로 홀딩하는 임의의 다른 사람일 수 있다. 다른 예로서, 계정은 요구불 예금, 저축 예금, 또는 (신용 잔액 이외의) 다른 자산 계정일 수 있다.

[0381] *예시적인 디지털 수표*

[0382] [0311] 일부 실시예들에서, 수표 수신자는 수표 전송자로부터 암호화방식으로 싸인된 디지털 수표를 수신할 수 있다. 도 4는 하나의 레코드 수신자에 대해 생성된 개별 레코드를 안전하게 교환하고 상환하는 일 실시예를 예시하는 상호작용 다이어그램이다. 수표 수신자 디바이스(116b)를 사용하는 수표 수신자(102b)(예컨대, 수취인)은 수표 전송자 디바이스(116a)에 지불 요청(402)을 전송함으로써 수표 전송자(102a)(예컨대, 지불인)로부터 디지털 수표(100)를 요청할 수 있다. 수표 수신자(102b)는 상호작용(404)에서 SRL(short range link)(122)를 사용하여 수표 전송자(102a)에게 지불 요청(402)을 전송할 수 있다. 지불 요청(402)은 콘텐츠, 예컨대, 수표 수신자 디바이스의 지불 금액(110b) 및 공개 키(106b)를 포함할 수 있다. 지불 금액(110b)은 수표 수신자(102b)가 수표 전송자(102a)로부터 수신할 것으로 예상되는 금액일 수 있다. 일부 실시예들에서, 수표 수신자 디바이스의 공개 키(106b)는 수표 수신자 디바이스(116b)를 독특하게 식별할 수 있다. 일부 실시예들에서, 수표 수신자 디바이스의 공개 키(106b)는 수표 수신자(102b)를 독특하게 식별할 수 있다. 공개 키(106b)는 일부 실시예들에서 SE(secure element)(204b)에 저장될 수 있는 공통 레코드들에 있을 수 있다.

[0383] *예시적인 파트너 식별*

[0384] [0312] 도 34a를 참조로, 상호작용(408)에서, 자신의 거래 파트너 식별자를 사용하는 수표 전송자 디바이스

(116a)는 파트너 식별에 의해 수표 수신자 디바이스(116b)의 아이덴티티를 확인할 수 있다. 지불 요청(402)이 수표 수신자 디바이스(116a)에 전자적으로 송신되었을 수 있기 때문에, 수표 수신자 디바이스(116a)는 지불 요청(402)을 전송하는 사용자 디바이스의 아이덴티티에 대해 확신이 없을 수 있다. 파트너 식별이 유리할 수 있다. 예컨대, 파트너 식별을 통해, 수표 전송자 디바이스(116a)는 수표 수신자 디바이스(116b)로부터의 그리고 악의적인 사용자들로부터의 지불 요청들(402)을 구별할 수 있다. 다른 예로서, 파트너 식별을 통해, 악의적인 사용자가 그것에 대해 의도되지 않은 디지털 수표를 수신할 수 없다. 또 다른 예로서, 파트너 식별을 통해, 악의적인 사용자는 그것에 대해 의도되지 않은 디지털 수표를 수신한 후에라도, 디지털 수표를 상환할 수 없다.

[0385] *예시적인 디지털 수표 생성*

[0386] [0313] 수표 전송자 디바이스(116a)의 SE(secure element)(204a)가 레코드 전송자의 인증 정보를 검증한 후에, SE(secure element)(204a)는 상호작용(416)에서 디지털 수표(100)에 싸인할 수 있다. 상호작용(416)에서 개별 레코드(100)에 싸인하기 전에, 레코드 전송자(102a)의 인증 및 SE(secure element)(204a)는 디지털방식으로 싸인될 블록, 예컨대, 디지털 수표(100)의 블록(105a)의 프로비전 둘 모두를 요구할 수 있다. 인증의 비-제한적인 예들은 암호구 인증, 생체인식 인증, 이를테면, 지문 인증 또는 홍채 인증, 생물학적 데이터 인증, 또는 이들의 임의의 조합을 포함할 수 있다. 생체인식 인증은 예컨대, 지문들 또는 눈 이미지들에 기반한 생체인식 템플릿을 활용할 수 있다. SE(secure element)(204a)는 생체인식 템플릿을 인식하기 위해 생체인식 퍼지 금고를 구현할 수 있다.

[0387] [0314] 도 33b를 참조로, 디지털 수표(100)는 하나 이상의 블록들을 포함하는 디지털 객체일 수 있다. 디지털 수표(100)는 블록(105a)을 포함할 수 있고, 블록(105a)은 블록(105a)의 "from 필드"의 수표 전송자 디바이스(116a)의 공개 키(106a), "to 필드"의 수표 수신자 디바이스의 공개 키(106b), 수표 ID(108), 지불 금액(110a), 및 수표 전송자 서명(112a)을 포함할 수 있다. 수표 전송자 디바이스(116a)의 공개 키(106a)는 디지털 수표(100)의 발신자인 수표 전송자 디바이스(116a)를 식별할 수 있다. 수표 수신자 디바이스의 공개 키(106b)는 디지털 수표(100)의 오리지널 수신측인 수표 수신자 디바이스(116b)를 식별할 수 있다. 지불 금액(110a)은 변할 수 있다. 디지털 수표(100a)의 지불 금액(110a) 및 도 34a에서 요청된 지불 금액(110b)은 동일하거나, 유사하거나, 관련되거나 상이할 수 있다. 암호화폐의 맥락에서, 전송된 지불 금액(110a) 및 요청된 지불 금액(110b)은 동일한 금액의 암호화폐일 수 있다. 전송된 지불 금액(110a) 및 요청된 지불 금액(110b)은 유사하거나 관련될 수 있다. 예컨대, 요청된 지불 금액(110b)은 세전 금액일 수 있고, 전송된 지불 금액(110a)은 세후 금액일 수 있다. 다른 예로서, 요청된 지불 금액(110b)은 팁전 금액일 수 있고, 전송된 지불 금액(110a)은 팁후 금액일 수 있다.

[0388] [0315] 도 34a를 참조로, 상호작용(420)에서, 수표 전송자(102a)는 예컨대, SRL(short range link)를 사용하여 피어-투-피어 방식으로 수표 수신자(102b)에 디지털 수표(100)를 전송할 수 있다. 일단, 수표 수신자(102b)의 소유이면, 수표 수신자(102b)는 상호작용(424)에서 디지털 수표(100)를 검증할 수 있다. 디지털 수표(100)를 검증하는 것은 수표 전송자 서명(112a)을 인증하는 것을 포함할 수 있다. 수표 전송자 서명(112a)을 인증하는 것은 수표 전송자 디바이스의 공개 키(106a)를 사용하여, 수표 전송자 서명(112a)이 수표 전송자 디바이스의 개인 키(210)를 사용하여 생성되었는지 여부를 결정하는 것을 포함할 수 있다. 수표 전송자 디바이스의 공개 키(106a)는 다수의 방식들로 획득될 수 있다. 예컨대, 수표 전송자 디바이스의 공개 키(106a)는 디지털 수표(100)로부터 획득될 수 있다. 다른 예로서, 수표 전송자 디바이스의 공개 키(106a)는 수표 수신자 디바이스(116b)의 공통 레코드들(206)로부터 획득될 수 있다.

[0389] *예시적인 개별 레코드 상환 - 하나의 금융 기관*

[0390] [0316] 도 33b 및 도 34a를 참조로, 디지털 수표(100)를 성공적으로 검증한 후에, 수표 수신자 디바이스(116b)는, 상호작용(428)에서, 자신의 보안 엘리먼트(204b)를 사용하여, 수정된 디지털 수표(100m1)를 생성하고 싸인할 수 있다. 상호작용(428)에서 수정된 디지털 수표(100m1)에 싸인하기 전에, SE(secure element)(204b)는 수표 수신자의 인증 정보(512b) 및 디지털방식으로 싸인될 블록, 예컨대, 수정된 디지털 수표(100m1)의 블록(105b)의 프로비전 둘 다를 요구할 수 있다. 수정된 디지털 수표(100m1)는 디지털 수표(100)의 블록(105a) 및 배서 블록(105b)을 포함할 수 있다. 예컨대, 배서는 수표 수신자의 공개 키(106b)와 함께, 수정된 디지털 수표(100m1)가 수표 수신자(102b)에 의해서만 상환될 수 있음을 특정하는 FPOE("for deposit only endorsement")(114)일 수 있다. 암호화폐의 맥락에서, FDOE("for deposit only endorsement")의 디지털 수표를 수신한 후에, 프로세싱 플랫폼(124)은 수표 수신자(102b)의 계정에 일정량의 암호화폐를 예치하거나 예치되도록 명령할 수 있지만, 다른 당사자에 대한 추가의 배서를 인식하지 않을 것이다.

[0391] [0317] 수정된 디지털 수표(100m1)에 싸인한 후, 수표 수신자(102b)가 예컨대, 네트워크(118)를 통해 프로세싱 플랫폼(124)과 통신할 때, 수표 수신자(102b)는 상호작용(432)에서, 수정된 디지털 수표(100m1)를 프로세싱 플랫폼(124)에 상환할 수 있다. 상환 시에, 프로세싱 플랫폼(124)을 동작시키는 서비스 제공자(104)는 상호작용(436)에서, 수정된 디지털 수표(100m1)의 블록들(105a 및 105b)의 체인 내의 하나 이상의 서명들, 예컨대, 수표 전송자 서명(112a) 및 수표 수신자 서명(112b)의 진본성을 검증함으로써 수정된 개별 레코드(100m1)를 프로세싱할 수 있다. 성공적 검증 후에, 프로세싱 플랫폼(124)은 수정된 디지털 수표(100m1)의 지불 금액(110a)에 기반하여 수행할 수 있다.

[0392] [0318] 프로세싱 플랫폼(124)은 예컨대, 전송자(102a)의 계정으로부터 수신자(102b)의 계정으로(또는 수표 전송자 디바이스(116a)의 계정으로부터 수표 수신자 디바이스(116b)의 계정으로) 암호화폐 또는 실제 통화의 지불 금액(110a)을 송금하도록 금융 기관 서버(3304)에 명령할 수 있다. 서버(3304a)를 동작시키는 금융 기관은 전송자(102a)의 계정 및 수신자(102b)의 계정을 유지할 수 있다. 상호작용(3404)에서, 프로세싱 플랫폼(124)은, 지불 금액(110a) 만큼 전송자 계정에서 데빗팅하고 수신자 계정에 크레딧팅하도록 금융 기관 또는 금융 기관에 의해 동작되는 서버(3304a)에 명령할 수 있다. 프로세싱 플랫폼(124) 및 전송자 계정에서 충분한 펀드를 인증한 후에, 금융 기관은 상호작용(3408)에서, 지불 금액(110a)만큼 전송자 계정에서 데빗팅하고, 수신자 계정에 크레딧팅할 수 있다. 상호작용(3424)에서, 금융 기관 서버(3304a)로부터, 계정들이 데빗팅 및 크레딧팅되었다는 표시를 수신한 후, 프로세싱 플랫폼(124)은 상호작용(3428)에서, 수정된 디지털 수표(100m1)의 전송된 지불 금액(110a)에 기반하여 프로세싱 플랫폼(124)이 수행했다는 표시를 수신자 디바이스(116b)에 전송할 수 있다. 일부 구현들에서, 프로세싱 플랫폼(124)은 전송자(102a)의 계정의 잔액 및 수신자(102b)의 계정의 잔액을 계속해서 추적하고 상호작용(3424) 후에 계정들의 잔액들을 업데이트할 수 있다.

[0393] *예시적인 개별 레코드 상환 - 다수의 금융 기관들*

[0394] [0319] 도 34b는 2개의 금융 기관을 수반하는 암호화방식으로 싸인된 디지털 수표를 안전하게 교환하고 상환하는 다른 실시예를 예시하는 상호작용 다이어그램이다. 도 34b의 지불 요청(402) 및 상호작용들(404, 408, 416, 420, 424, 428, 432 및 436)은 도 34a를 참조하여 설명된 바와 같다. 상호작용(436)에서, 성공적 검증 후에, 프로세싱 플랫폼(124)은 수정된 디지털 수표(100m1)의 지불 금액(110a)에 기반하여 수행할 수 있다.

[0395] [0320] 프로세싱 플랫폼(124)은 전송자(102a)의 계정으로부터 수신자(102b)의 계정으로(또는 수표 전송자 디바이스(116a)의 계정으로부터 수표 수신자 디바이스(116b)의 계정으로) 전송된 지불 금액(110a)을 송금하도록 금융 기관 서버(3304)에 명령할 수 있다. 서버(3304a)를 동작시키는 금융 기관은 전송자(102a)의 계정을 유지할 수 있다. 서버(3304a)를 동작시키는 금융 기관은 수신자(102b)의 계정을 유지할 수 있다. 상호작용(3404)에서, 프로세싱 플랫폼(124)은, 요청된 지불 금액(110a) 만큼 전송자 계좌에서 데빗팅하고 수신자 계좌에 크레딧팅하도록 금융 기관 또는 금융 기관에 의해 동작되는 서버(3304a)에 명령할 수 있다. 프로세싱 플랫폼(124) 및 전송자 계좌에서 충분한 펀드를 인증한 후에, 금융 기관은 상호작용(3408)에서, 전송자 계좌에서 데빗팅할 수 있다. 결과적으로, 금융 기관 서버(3304a)는 상호작용(3412)에서, 전송된 지불 금액(110a) 만큼 수신자 계정에 크레딧팅하도록 다른 금융 기관 또는 다른 금융 기관에 의해 동작되는 서버(3304b)에 요청할 수 있다. 상호작용(3412)에서 전송된 지불 금액(110a) 만큼 수신자 계정에 성공적으로 크레딧팅한 후, 서버(3304b)는, 수신자 계정이 성공적으로 크레딧팅되었다는 표시를 금융 기관의 서버(3304a)에 전송할 수 있다.

[0396] [0321] 상호작용(3424)에서, 금융 플랫폼 서버(3304a)로부터, 계정들이 데빗팅 및 크레딧팅되었다는 표시를 수신한 후, 프로세싱 플랫폼(124)은 상호작용(3428)에서, 수정된 디지털 수표(100m1)의 전송된 지불 금액(110a)에 기반하여 프로세싱 플랫폼(124)이 수행했다는 표시를 수신자 디바이스(116b)에 전송할 수 있다. 일부 구현들에서, 프로세싱 플랫폼(124)은 전송자(102a)의 계정의 잔액 및 수신자(102b)의 계정의 잔액을 계속해서 추적하고 상호작용(3424) 후에 계정들의 잔액들을 업데이트할 수 있다.

[0397] *예시적인 지불 타입들*

[0398] [0322] 전송자(102a)로부터 수신자(102b)로의 지불은 체크 거래, 데빗 거래, 크래딧 카드 거래, ACH(automated clearing house) 거래, 유선 송금 또는 이들의 조합과 유사할 수 있다. 체크-타입 거래는 예컨대, UCC(uniform commercial code) 하의 "아이템"을 요구할 수 있다. 체크 거래는 금융 기관(예컨대, 서버(3304a)를 동작시키는 금융 기관) 및 금융 기관의 계정을 소유하는 커스터머(예컨대, 전송자(102a)) 간의 계약으로 고려될 수 있다. 지불은, (1) 금융 기관의 카운터(예컨대, 가상 카운터)를 통해 프로세싱된다면, 즉시, 또는 (2) 수정된 체크(100m1)가 금융 기관에 수신되는 날 자정에 완료될 수 있다. 금융 기관은, 계정 소유자가 부주의한 경우를 제

외한 사기 활동 또는 비인가된 지불에 대한 책임이 있을 수 있다.

[0399] [0323] 데빗-타입 거래는 데빗 거래가 거래를 완료하는 "신호"를 수반할 수 있으므로, 아이템의 UCC 정의에 대한 예외로 고려될 수 있다. 지불은, 계정에서 판매자로 데빗팅하도록 금융 기관에 대한 즉각적인 인가와 더불어, 판매 시에(예컨대, 판매자, 수취인 또는 수표 수신자가 디지털 수표를 수신할 때) 완료될 수 있다. 일부 실시예들에서, 비인가된 지불들은 수표 전송자 "공제금액" 책임의 대상이다. 예컨대, 비인가된 지불이 짧은 시간 기간(예컨대, 2일) 내에 수표 전송자로 알려진 사람에 의해 리포트된다면, 공제금액은 $50일 수 있다. 비인가된 지불이 중간 시간 기간(예컨대, 60일) 내에 수표 전송자로 알려진 사람에 의해 리포트된다면, 공제금액은 $500일 수 있다. 비인가된 지불이 중간 시간 기간 내에 리포트되지 않는다면, 수표 전송자로 알려진 사람은 비인가된 지불에 대한 책임이 있다. 수표 전송자로 알려진 사람의 금융 기관은, 계정 소유자가 부주의한 경우를 제외한 잔여 비인가된 잔액에 대한 책임이 있을 수 있다.

[0400] [0324] 신용 카드-타입 거래에 있어, 수표 전송자가 금융 기관(예컨대, 신용 카드 회사)에 납부할 때 지불이 완료된다. 청구요금들에 관한 분쟁들은, 내역서가 납부된다면 허용되지 않을 수 있다(분쟁을 일으키는 2개의 빌링 사이클들). 금융 기관은 내역서가 아직 납부되지 않은 한 항상 책임이 있다.

[0401] [0325] ACH-타입 거래는 신용 ACH 지불들 및 데빗 ACH 지불들을 포함할 수 있다. 신용 ACH 지불들에 있어, 금융 기관은 임의의 이유로, 지불을 취소할 수 있다. 데빗 ACH 지불들에 있어, 계정 소유자(예컨대, 수표 전송자)는 지불을 중단하기 위한 1 영업일을 가지며, 중단이 없으면, 지불이 진행되고, 커스터머는 비인가된 지불을 통지하기 위한 15일을 갖는다. 지불은 판매 시에, 또는 데빗 ACH의 경우 하루만에 또는 신용 ACH의 경우 이틀만에 완료되는 것으로 고려될 수 있다.

[0402] [0326] 유선 송금들은 금융 기관들 간의 송금들일 수 있다. 전자 펀드 이체 법(Electronic Funds Transfer Act)은 자연인들을 수반하는 유선 송금들을 허용한다. 유선 송금은 2 스테이지의 지불 명령들을 포함하는데: 첫째, 지불인 또는 수표 전송자는 제1 금융 기관, 이를테면, 서버(3304a)(또는 프로세싱 플랫폼(124))를 동작시키는 금융 기관에 송금 정보를 제공하여 제2 금융 기관(예컨대, 서버(3304b)를 동작시키는 다른 금융 기관)에 돈을 송금한다. 둘째, 제1 금융 기관은 제2 금융 기관에 송금에 대한 명령들을 제공할 수 있다. 단계 2가 완료되면, 펀드들이 실제로 제1 금융 기관으로부터 제2 금융 기관으로 송금되었든 안 되었든 간에, 지불이 완료된 것으로 고려될 수 있다. 따라서, 수표 전송자 또는 지불인은 수표 수신자 수취인에 대해 매우 신속하게 책임이 있지만, 제2 금융 기관은 이들이 송금에서 실수를 범한다면 책임이 있을 수 있다.

[0403] [0327] 일부 구현들에서, 본원에서 개시된 시스템들 및 방법들은 복잡한 교섭에 사용될 수 있다. 예컨대, 판매자 또는 벤더는, 판매자가 펀드들을 더 빨리 취득할 수 있기 때문에, 데빗-타입 거래에 대해 한 가격으로 판매할 수 있다. 그러나 구매자가 악의적일 수 있고, 판매자는 공제금액 임계치로 인해 $ 50 미만의 상품들의 지불에 대해 데빗 요청들을 자동으로 차단할 수 있다. 다른 예로서, 판매자는 그들이 금융 기관들 간의 검증이 발생할 것임을 알고 있기 때문에 유선 송금 지불을 요청할 수 있다. 그러나 구매자는, 수수료 공유가 수반되지 않는 한 구매자가 2 단계들의 송금 수수료들을 납부하기를 원하지 않을 수 있기 때문에 이러한 요청을 거절할 수 있다.

[0404] 예시적인 웨어러블 디스플레이 시스템들

[0405] [0328] 사용자 디바이스(116)는 웨어러블 디스플레이 디바이스들일 수 있거나 이에 포함될 수 있으며, 이는 보다 몰입형 VR(virtual reality), AR(augmented reality), 또는 MR(mixed reality) 경험을 유리하게 제공할 수 있고, 여기서, 디지털방식으로 재생된 이미지들 또는 이미지들의 부분들은, 그것들이 실제인 것으로 보이거나, 실제로서 지각될 수 있는 방식으로 착용자에게 제시된다.

[0406] [0329] 이론에 의해 제한됨이 없이, 인간 눈이 통상적으로 깊이 지각을 제공하기 위하여 유한 수의 깊이 평면들을 해석할 수 있다고 여겨진다. 결과적으로, 지각된 깊이의 매우 믿을 만한 시뮬레이션은, 눈에, 이들 제한된 수의 깊이 평면들 각각에 대응하는 이미지의 상이한 프리젠테이션들을 제공함으로써 달성될 수 있다. 예컨대, 도파관들의 스택을 포함하는 디스플레이들은 사용자, 또는 뷰어의 눈들의 전면에 포지셔닝되게 착용되도록 구성될 수 있다. 도파관들의 스택은, 이미지 주입 디바이스(예컨대, 이산 디스플레이들, 또는 하나 이상의 광섬유들을 통해 이미지 정보를 파이핑(pipe)하는 멀티플렉싱된 디스플레이의 출력 단부들)로부터의 광을 특정 도파관과 연관된 깊이 평면에 대응하는 특정 각도들(및 발산 양들)로 뷰어의 눈으로 지향시키기 위해 복수의 도파관들을 사용함으로써 눈/뇌에 3차원 지각을 제공하는 데 활용될 수 있다.

[0407] [0330] 일부 실시예들에서, 도파관들의 2개의 스택들(뷰어의 각각의 눈마다 하나씩)은 각각의 눈에 상이한 이

미지들을 제공하기 위해 활용될 수 있다. 일 예로서, 증강 현실 장면은 AR 기술의 착용자가 배경에 있는 사람들, 나무들, 빌딩들, 및 콘크리트 플랫폼을 피처링(featuring)하는 실세계 공원형 세팅을 보는 그러한 장면일 수 있다. 이들 아이템들에 더하여, AR 기술의 착용자는 또한, 그가 실세계 플랫폼 상에 서 있는 로봇 동상, 및 호박벌의 의인화인 것으로 보여지는 날고 있는 만화-형 아바타 캐릭터를 "보는 것"을 지각할 수 있더라도, 로봇 동상 및 호박벌은 실세계에 존재하지 않는다. 도파관들의 스택(들)은 입력 이미지에 대응하는 광 필드를 생성하는 데 사용될 수 있고, 일부 구현들에서, 웨어러블 디스플레이는 웨어러블 광 필드 디스플레이를 포함한다. 광 필드 이미지들을 제공하기 위한 웨어러블 디스플레이 디바이스 및 도파관 스택들의 예들은 미국 특허 공보 제2015/0016777호에서 설명되며, 그리하여, 이 특허 공보는 그것이 포함하는 전부에 대해 그 전체가 인용에 의해 본원에 포함된다.

[0408] [0331] 도 35는 착용자(3504)에 AR, MR 또는 VR 경험을 제시하는 데 사용될 수 있는 웨어러블 디스플레이 시스템(3500)의 예를 예시한다. 웨어러블 디스플레이 시스템(3500)은 본원에서 설명된 애플리케이션들 또는 실시예들 중 임의의 것을 수행하도록 프로그래밍될 수 있다. 디스플레이 시스템(3500)은 디스플레이(3508), 및 그 디스플레이(3508)의 기능을 지원하기 위한 다양한 기계적 및 전자적 모듈들 및 시스템들을 포함한다. 디스플레이(3508)는 디스플레이 시스템 착용자 또는 뷰어(3504)에 의해 착용가능하고 그리고 착용자(3504)의 눈들의 전면에 디스플레이(3508)를 포지셔닝하도록 구성된 프레임(3512)에 커플링될 수 있다. 디스플레이(3508)는 광 필드 디스플레이일 수 있다. 일부 실시예들에서, 스피커(35616)는 프레임(3512)에 커플링되고 사용자의 외이도에 인접하게 포지셔닝되고, 일부 실시예들에서, 도시되지 않은 다른 스피커가 사용자의 다른 외이도에 인접하게 포지셔닝되어 스테레오/성형가능(shapeable) 사운드 제어를 제공한다. 디스플레이(3508)는 이를테면, 유선 리드 또는 무선 연결성에 의해, 다양한 구성들로 장착될 수 있는, 이를테면, 프레임(3512)에 고정되게 부착되거나, 사용자에 의해 착용된 헬멧 또는 모자에 고정되게 부착되거나, 헤드폰들에 내장되거나, 그렇지 않으면 사용자(3504)에게 제거가능하게 부착되는 (예컨대, 백팩(backpack)-스타일 구성으로, 벨트-커플링 스타일 구성으로) 로컬 데이터 프로세싱 모듈(3524)에 동작가능하게 커플링(3520)된다.

[0409] [0332] 로컬 프로세싱 및 데이터 모듈(3524)은 하드웨어 프로세서는 물론, 비일시적인 디지털 메모리 이를테면, 비-휘발성 메모리(예컨대, 플래시 메모리)를 포함할 수 있고, 이 둘 모두는 데이터의 프로세싱, 캐싱(caching) 및 저장을 보조하기 위해 활용될 수 있다. 데이터는 a) 센서들(예컨대 프레임(3512)에 동작가능하게 커플링되거나 그렇지 않으면 착용자(3504)에게 부착될 수 있음), 이를테면, 이미지 캡처 디바이스들(이를테면, 카메라들), 마이크로폰들, 관성 측정 유닛들, 가속도계들, 컴퍼스(compass)들, GPS 유닛들, 라디오 디바이스들, 및/또는 자이로(gyro)들로부터 캡처되고; 및/또는 b) 원격 프로세싱 모듈(3528) 및/또는 원격 데이터 저장소(repository)(3532)를 사용하여 취득 및/또는 프로세싱되는 (가능하게는, 이러한 프로세싱 또는 리트리벌(retrieval) 후 디스플레이(3508)에 전달하기 위한) 데이터를 포함한다. 로컬 프로세싱 및 데이터 모듈(3524)은 통신 링크들(3536, 3540)에 의해, 이를테면, 유선 또는 무선 통신 링크들을 통해 원격 프로세싱 모듈(3528) 및 원격 데이터 저장소(3532)에 동작가능하게 커플링될 수 있어서, 이들 원격 모듈들(3528, 3532)은 서로 동작가능하게 커플링되고 자원들로서 로컬 프로세싱 및 데이터 모듈(3524)에 대해 이용가능하게 된다.

[0410] [0333] 일부 실시예들에서, 원격 프로세싱 모듈(3528)은 데이터 및/또는 이미지 정보, 이를테면, 이미지 캡처 디바이스에 의해 캡처된 비디오 정보를 분석 및 프로세싱하도록 구성된 하나 이상의 프로세서들을 포함할 수 있다. 비디오 데이터는 로컬 프로세싱 및 데이터 모듈(3524) 및/또는 원격 데이터 저장소(3532)에 로컬로 저장될 수 있다. 일부 실시예들에서, 원격 데이터 저장소(3532)는 "클라우드" 자원 구성에서 인터넷 또는 다른 네트워킹 구성을 통하여 이용가능할 수 있는 디지털 데이터 저장 설비를 포함할 수 있다. 일부 실시예들에서, 모든 데이터는 저장되고 모든 컴퓨테이션들은 로컬 프로세싱 및 데이터 모듈(3524)에서 수행되어, 원격 모듈로부터 완전히 자율적인 사용을 허용한다.

[0411] [0334] 일부 구현들에서, 로컬 프로세싱 및 데이터 모듈(3524) 및/또는 원격 프로세싱 모듈(3528)은 본원에서 개시된 시스템들 및 방법들의 실시예들을 수행하도록 프로그래밍된다. 이미지 캡처 디바이스는 특정 애플리케이션에 대한 비디오(예컨대, 눈 추적 애플리케이션의 경우 착용자의 눈의 비디오 또는 제스처 식별 애플리케이션의 경우 착용자의 손 또는 손가락의 비디오)를 캡처할 수 있다. 비디오는 프로세싱 모듈들(3524, 3528) 중 하나 또는 둘 모두에 의해 분석될 수 있다. 일부 경우들에서, 분석 중 적어도 일부를 (예컨대, "클라우드"의) 원격 프로세싱 모듈로 오프로딩(off-loading)하는 것은 컴퓨테이션들의 효율 또는 스피드를 개선할 수 있다. 본원에서 개시된 시스템들 및 방법들의 파라미터들은 데이터 모듈들(3524 및/또는 3532)에 저장될 수 있다.

[0412] [0335] 분석의 결과들은 부가적인 동작들 또는 프로세싱을 위해 프로세싱 모듈들(3524, 3528) 중 하나 또는 둘 모두에 의해 사용될 수 있다. 예컨대, 생체인식 식별, 눈-추적, 인식, 또는 제스처들, 객체, 포즈의 분류 등은

웨어러블 디스플레이 시스템(3500)에 의해 사용될 수 있다. 예컨대, 웨어러블 디스플레이 시스템(3500)은 착용자(3504)의 손의 캡처된 비디오를 분석하고 착용자의 손에 의한 제스처를 인식할 수 있고 (예컨대, 실제 또는 가상의 객체를 픽 업하거나, 또는 찬성 또는 반대 (예컨대, "엄지 손가락 올리기", 또는 "엄지 손가락 내리기"를 시그널링하는 등을 함), 웨어러블 디스플레이 시스템(3500)은 착용자의 제스처(예컨대, 가상 객체의 이동, 착용자의 찬성/반대에 기반한 부가적인 동작의 수행)에 대한 응답으로 적절한 액션을 수행할 수 있다. 다른 예로서, 착용자의 눈(들)의 비디오가 웨어러블 디스플레이 시스템(3500)에 의해 분석되어 디스플레이(3508)를 통한 착용자(3504)의 시선의 방향을 결정할 수 있다. 또 다른 예로서, 프로세싱 모듈들(3524, 3528)은 (예컨대, 착용자(3504) 근처의 "고양이들" 또는 "자동차들"을 식별하기 위해) 객체들 중 특정 클래스의 객체들을 식별(또는 카운트)하기 위해 착용자의 주변의 비디오를 분석할 수 있다. 웨어러블 디스플레이 시스템(3500)의 프로세싱 모듈들(3524, 3528)은 본원에서 설명된 방법들 또는 비디오 또는 이미지 프로세싱 애플리케이션들 중 임의의 것, 또는 본원에서 설명된 암호화된 방식으로 싸인된 레코드들의 안전한 교환을 위한 방법들 또는 애플리케이션들 중 임의의 것을 수행하도록 프로그래밍될 수 있다. 예컨대, 웨어러블 디스플레이 시스템(3500)의 실시예들은 사용자 디스플레이(116a)(예컨대, 전송자(102a)) 또는 사용자 디스플레이(116b)(예컨대, 수신자(102b))로서 구성되고 본원에서 설명된 바와 같이 암호화방식으로 안전한 방식으로 레코드들(100)을 생성, 전송, 수신, 수정 또는 상환하는 데 사용될 수 있다.

[0413] 부가적인 양상들

[0414] *암호화방식으로 싸인된 레코드들의 안전한 교환*

[0415] [0336] 제1 양상에서, 암호화방식으로 싸인된 레코드들을 안전하게 교환하기 위한 방법이 개시된다. 방법은 하드웨어 프로세서의 제어 하에 수행되며, 그리고 레코드 수신자 디바이스로부터 수신자 개별 레코드를 수신하는 단계 - 수신자 개별 레코드는 수신자 개별 레코드의 수신자 서명 및 전송자 개별 레코드를 포함하고, 전송자 개별 레코드는, 레코드 수신자 디바이스로부터 레코드 콘텐츠 요청을 수신하고 레코드 수신자 디바이스를 식별한 후에, 레코드 전송자 디바이스에 의해 생성되고, 전송자 개별 레코드는 레코드 콘텐츠, 레코드 전송자 디바이스의 전송자 공개 키, 레코드 수신자 디바이스의 수신자 공개 키, 및 전송자 개별 레코드의 전송자 서명을 포함하고, 전송자 서명은 레코드 전송자 디바이스의 전송자 개인 키를 사용하여 생성되고, 전송자 공개 키 및 전송자 개인 키는 전송자 공개-키 암호 쌍을 형성하고, 수신자 개별 레코드는, 레코드 전송자 디바이스로부터 전송자 개별 레코드를 수신하고, 반드시 그런 것은 아니지만 프로세싱 플랫폼과 통신하면서 전송자 공개 키를 사용하여 전송자 개별 레코드를 검증한 후에, 레코드 수신자 디바이스에 의해 생성되고, 수신자 서명은 레코드 수신자 디바이스의 수신자 개인 키를 사용하여 생성되며, 수신자 공개 키 및 수신자 개인 키는 수신자 공개-키 암호 쌍을 형성함 - 수신자 개별 레코드를 검증하는 단계; 및 수신자 개별 레코드에 의해 명령된 대로 레코드 수신자 디바이스에 대해 수행하는 단계를 포함한다.

[0416] [0337] 제2 양상에서, 양상 1의 방법에 있어서, 콘텐츠 요청은 수신자 공개 키 및 요청된 콘텐츠를 포함하고, 레코드 콘텐츠는 요청된 콘텐츠와 관련된다.

[0417] [0338] 제3 양상에서, 양상 1 또는 양상 2의 방법에 있어서, 레코드 수신자 디바이스를 식별하는 것은 파트너 식별을 수행하는 것을 포함하고, 파트너 식별은 콘텐츠 인가, 노킹, 물리적 표시, 빔 형성, 이전 어레인지먼트, 피상적인 유효성 검증, 또는 이들의 임의의 조합을 포함한다.

[0418] [0339] 제4 양상에서, 양상 1 내지 양상 3 중 어느 한 양상의 방법에 있어서, 전송자 개별 레코드는 레코드 식별자를 더 포함한다.

[0419] [0340] 제5 양상에서, 양상 4의 방법에 있어서, 레코드 식별자는 단조적으로 증가하는 수이다.

[0420] [0341] 제6 양상에서, 양상 1 내지 양상 5 중 어느 한 양상의 방법에 있어서, 레코드 수신자 디바이스로부터 전송자 개별 레코드를 수신하는 것은, 중간 디바이스를 통해 또는 직접적으로 단거리 링크를 통해 레코드 전송자 디바이스로부터 전송자 개별 레코드를 수신하는 것을 포함한다.

[0421] [0342] 제7 양상에서, 양상 6의 방법에 있어서, 단거리 링크는 피어-투-피어 통신 링크이다.

[0422] [0343] 제8 양상에서, 양상 1 내지 양상 7 중 어느 한 양상의 방법에 있어서, 수신자 개별 레코드는 상환 전용 배서, 질의 배서, 악의적인 레코드 배서, 또는 이들의 임의의 조합을 더 포함한다.

[0423] [0344] 제9 양상에서, 양상 1 내지 양상 8 중 어느 한 양상의 방법에 있어서, 전송자 개별 레코드는 레코드 전송자 디바이스에 의해 레코드 전송자의 인증 정보를 수신한 후에 생성되며, 그리고 수신자 개별 레코드는 레코

드 수신자 디바이스에 의해 레코드 수신자의 인증 정보를 수신한 후에 생성된다.

[0424] [0345] 제10 양상에서, 양상 1 내지 양상 9 중 어느 한 양상의 방법에 있어서, 전송자 개별 레코드를 검증하는 것은, 전송자 공개 키를 사용하여, 전송자 서명이 전송자 개인 키를 사용하여 생성됨을 결정하는 것; 및 전송자 공개 키를 사용하여, 전송자 서명이 전송자 개인 키를 사용하여 생성됨을 결정하는 것을 포함한다.

[0425] [0346] 제11 양상에서, 양상 1 내지 양상 10 중 어느 한 양상의 방법은, 레코드 전송자 디바이스 및 레코드 수신자 디바이스에 공통 레코드들을 제공하는 단계를 더 포함하고, 공통 레코드들은 전송자 공개 키 및 수신자 공개 키를 포함한다.

[0426] [0347] 제12 양상에서, 양상 1 내지 양상 10 중 어느 한 양상의 방법은, 레코드 전송자 디바이스에 공통 레코드들을 제공하는 단계 - 공통 레코드들은 전송자 공개 키 및 수신자 공개 키를 포함함 -; 및 레코드 전송자 디바이스로 하여금 레코드 수신자 디바이스에 공통 레코드들을 전송하게 하는 단계를 더 포함한다.

[0427] [0348] 제13 양상에서, 양상 1 내지 양상 10 중 어느 한 양상의 방법은, 레코드 수신자 디바이스에 공통 레코드들을 제공하는 단계 - 공통 레코드들은 전송자 공개 키 및 수신자 공개 키를 포함함 -; 및 레코드 수신자 디바이스로 하여금 레코드 전송자 디바이스에 공통 레코드들을 전송하게 하는 단계를 더 포함한다.

[0428] [0349] 제14 양상에서, 양상 11 내지 양상 13 중 어느 한 양상의 방법에 있어서, 공통 레코드들은 공통 레코드들의 제3 서명을 더 포함하고, 공통 레코드들은 공통 레코드들의 제3 서명을 더 포함하며, 그리고 제3 서명은 프로세싱 플랫폼의 제3 개인 키를 사용하여 생성된다.

[0429] [0350] 제15 양상에서, 양상 11 내지 양상 14 중 어느 한 양상의 방법은, 중앙 레코드들로부터 공통 레코드들을 생성하는 단계를 더 포함하고, 중앙 레코드들은 전송자 공개 키, 수신자 공개 키, 레코드 전송자 디바이스의 사용자 레코드 상황, 및 레코드 수신자 디바이스의 사용자 레코드 상황을 포함한다.

[0430] [0351] 제16 양상에서, 양상 15의 방법은, 프로세싱 플랫폼이 수신자 개별 레코드에 의해 명령된 대로 레코드 수신자 디바이스를 수행하는 것을 레코드 전송자의 사용자 레코드 상황이 금지한다는 것을 결정하는 단계; 및 디메리트 리스트에 지불인 디바이스를 부가하는 단계를 더 포함한다.

[0431] [0352] 제17 양상에서, 암호화방식으로 싸인된 레코드들을 안전하게 교환하기 위한 방법이 개시된다. 방법은 하드웨어 프로세서의 제어 하에 수행되며, 그리고 레코드 수신자 디바이스로부터 콘텐츠 요청을 수신하는 단계; 레코드 수신자 디바이스를 식별하는 단계; 전송자 개별 레코드를 생성하는 단계 - 전송자 개별 레코드는 레코드 콘텐츠, 레코드 전송자 디바이스의 전송자 공개 키, 레코드 수신자 디바이스의 수신자 공개 키, 및 전송자 개별 레코드의 전송자 서명을 포함하고, 전송자 서명은 레코드 전송자 디바이스의 전송자 개인 키를 사용하여 생성되고, 전송자 공개 키 및 전송자 개인 키는 전송자 공개-키 암호 쌍을 형성함 -; 레코드 수신자 디바이스에 전송자 개별 레코드를 전송하는 단계; 및 레코드 수신자 디바이스의 표시를 수신하는 단계: 전송자 개별 레코드를 수신하는 단계; 반드시 그런 것은 아니지만 프로세싱 플랫폼과 통신하면서 전송자 공개 키를 사용하여 전송자 개별 레코드를 검증하는 단계; 수신자 개별 레코드를 생성하는 단계 - 수신자 개별 레코드는 수신자 개별 레코드의 수신자 서명 및 전송자 개별 레코드를 포함하고, 수신자 서명은 레코드 수신자 디바이스의 수신자 개인 키를 사용하여 생성되고, 수신자 공개 키 및 수신자 개인 키는 수신자 공개-키 암호 쌍을 형성함 -; 수신자 개별 레코드를 프로세싱 플랫폼에 상환하는 단계; 및 수신자 개별 레코드에 의해 명령된 대로 프로세싱 플랫폼에 의한 퍼포먼스를 수신하는 단계를 포함한다.

[0432] [0353] 제18 양상에서, 양상 17의 방법에 있어서, 콘텐츠 요청은 수신자 공개 키 및 요청된 콘텐츠를 포함하고, 레코드 콘텐츠는 요청된 콘텐츠와 관련된다.

[0433] [0354] 제19 양상에서, 양상 17 또는 양상 18의 방법에 있어서, 레코드 수신자 디바이스를 식별하는 단계는 파트너 식별을 수행하는 단계를 포함하고, 파트너 식별은 콘텐츠 인가, 노킹, 물리적 표시, 빔 형성, 이전 어레인지먼트, 피상적인 유효성 검증, 또는 이들의 임의의 조합을 포함한다.

[0434] [0355] 제20 양상에서, 양상 17 내지 양상 19 중 어느 한 양상의 방법에 있어서, 전송자 개별 레코드는 레코드 식별자를 더 포함한다.

[0435] [0356] 제21 양상에서, 양상 20의 방법에 있어서, 레코드 식별자는 단조적으로 증가하는 수이다.

[0437] *[0357] 제22 양상에서, 양상 17 내지 양상 21 중 어느 한 양상의 방법에 있어서, 레코드 수신자 디바이스에 전송자 개별 레코드를 전송하는 단계는, 중간 디바이스를 통해 또는 직접적으로 단거리 링크를 통해 레코드 수신

자 디바이스에 전송자 개별 레코드를 전송하는 단계를 포함한다.

[0438] [0358] 제23 양상에서, 양상 22의 방법에 있어서, 단거리 링크는 피어-투-피어 통신 링크이다.

[0439] [0359] 제24 양상에서, 양상 17 내지 양상 23 중 어느 한 양상의 방법에 있어서, 수신자 개별 레코드는 상환 전용 배서, 질의 배서, 악의적인 레코드 배서, 또는 이들의 임의의 조합을 더 포함한다.

[0440] [0360] 제25 양상에서, 양상 24의 방법에 있어서, 수신자 개별 레코드는 질의 집행(query enforcement)을 더 포함하고, 수신자 개별 레코드에 의해 명령된 대로 레코드 수신자 디바이스를 수행하는 것은 레코드 수신자 디바이스에 질의 결과를 전송하는 것을 포함하며, 그리고 질의 결과는, 프로세싱 플랫폼이 수신자 개별 레코드에 의해 명령된 대로 수행할 것임을 표시한다.

[0441] [0361] 제26 양상에서, 양상 17 내지 양상 25 중 어느 한 양상의 방법에 있어서, 전송자 개별 레코드를 생성하는 단계는 레코드 전송자 디바이스에 의해 레코드 전송자의 인증 정보를 수신하는 단계를 포함하며, 그리고 수신자 개별 레코드를 생성하는 단계는 레코드 수신자 디바이스에 의해 레코드 수신자의 인증 정보를 수신하는 단계를 포함한다.

[0442] [0362] 제27 양상에서, 양상 17 내지 양상 26 중 어느 한 양상의 방법에 있어서, 전송자 개별 레코드를 검증하는 단계는, 전송자 공개 키를 사용하여, 전송자 서명이 전송자 개인 키를 사용하여 생성됨을 결정하는 단계를 포함한다.

[0443] [0363] 제28 양상에서, 양상 17 내지 양상 27 중 어느 한 양상의 방법에 있어서, 전송자 서명은 전송자 개인 키를 사용하여 레코드 전송자 디바이스의 보안 엘리먼트에 의해 생성되며, 전송자 개인 키는 레코드 전송자 디바이스의 보안 엘리먼트에 저장된다.

[0444] [0364] 제29 양상에서, 양상 17 내지 양상 28 중 어느 한 양상의 방법에 있어서, 수신자 서명은 수신자 개인 키를 사용하여 레코드 수신자 디바이스의 보안 엘리먼트에 의해 생성되고, 수신자 개인 키는 레코드 수신자 디바이스의 보안 엘리먼트에 저장된다.

[0445] [0365] 제30 양상에서, 양상 17 내지 양상 29 중 어느 한 양상의 방법은, 프로세싱 플랫폼으로부터 공통 레코드들을 수신하는 단계를 더 포함하고, 공통 레코드들은 전송자 공개 키 및 수신자 공개 키를 포함한다.

[0446] [0366] 제31 양상에서, 양상 17 내지 양상 29 중 어느 한 양상의 방법은, 레코드 수신자 디바이스로부터 공통 레코드들을 수신하는 단계를 더 포함하고, 공통 레코드들은 전송자 공개 키 및 수신자 공개 키를 포함한다.

[0447] [0367] 제32 양상에서, 양상 30 또는 양상 31의 방법에 있어서, 공통 레코드들은 공통 레코드들의 제3 서명을 더 포함하고, 제3 서명은 프로세싱 플랫폼의 제3 개인 키를 사용하여 생성되고, 방법은: 반드시 그런 것은 아니지만 프로세싱 플랫폼과 통신하면서 프로세싱 플랫폼의 제3 공개 키를 사용하여 공통 레코드들을 검증하는 단계를 더 포함하고, 제3 공개 키 및 제3 개인 키는 제3 공개-키 암호 쌍을 형성하며, 그리고 공통 레코드들을 검증하는 단계는, 제3 공개 키를 사용하여, 제3 서명이 제3 개인 키를 사용하여 생성됨을 결정하는 단계를 포함한다.

[0448] [0368] 제33 양상에서, 암호화방식으로 싸인된 레코드들을 안전하게 교환하기 위한 방법이 개시된다. 방법은 하드웨어 프로세서의 제어 하에 수행되며, 그리고 레코드 전송자 디바이스에 콘텐츠 요청을 송신하는 단계; 레코드 전송자 디바이스로부터 전송자 개별 레코드를 수신하는 단계 – 전송자 개별 레코드는, 레코드 수신자 디바이스로부터 콘텐츠 요청을 수신하고 레코드 수신자 디바이스를 식별한 후에, 레코드 전송자 디바이스에 의해 생성되고, 전송자 개별 레코드는 레코드 콘텐츠, 레코드 전송자 디바이스의 전송자 공개 키, 레코드 수신자 디바이스의 수신자 공개 키, 및 전송자 개별 레코드의 전송자 서명을 포함하고, 전송자 서명은 레코드 전송자 디바이스의 전송자 개인 키를 사용하여 생성되고, 전송자 공개 키 및 전송자 개인 키는 전송자 공개-키 암호 쌍을 형성함 –; 반드시 그런 것은 아니지만 프로세싱 플랫폼과 통신하면서 전송자 공개 키를 사용하여 전송자 개별 레코드를 검증하는 단계; 수신자 개별 레코드를 생성하는 단계 – 수신자 개별 레코드는 수신자 개별 레코드의 수신자 서명 및 전송자 개별 레코드를 포함하고, 수신자 서명은 레코드 수신자 디바이스의 수신자 개인 키를 사용하여 생성되고, 수신자 공개 키 및 수신자 개인 키는 수신자 공개-키 암호 쌍을 형성함 –; 수신자 개별 레코드를 프로세싱 플랫폼에 상환하는 단계; 및 수신자 개별 레코드에 의해 명령된 대로 프로세싱 플랫폼에 의한 퍼포먼스를 수신하는 단계를 포함한다.

[0449] [0369] 제34 양상에서, 양상 33의 방법에 있어서, 콘텐츠 요청은 수신자 공개 키 및 요청된 콘텐츠를

포함하고, 레코드 콘텐츠는 요청된 콘텐츠와 관련된다.

[0450] [0370] 제35 양상에서, 양상 33 또는 양상 34의 방법에 있어서, 수취인 디바이스를 식별하는 것은 파트너 식별을 수행하는 것을 포함하고, 파트너 식별은 지불 인가, 노킹, 물리적 표시, 빔 형성, 이전 어레인지먼트, 피상적인 유효성 검증, 또는 이들의 임의의 조합을 포함한다.

[0451] [0371] 제36 양상에서, 양상 33 내지 양상 35 중 어느 한 양상의 방법에 있어서, 전송자 개별 레코드는 레코드 식별자를 더 포함한다.

[0452] [0372] 제37 양상에서, 양상 36의 방법에 있어서, 레코드 식별자는 단조적으로 증가하는 수이다.

[0453] [0373] 제38 양상에서, 양상 33 내지 양상 37 중 어느 한 양상의 방법에 있어서, 레코드 전송자 디바이스로부터 전송자 개별 레코드를 수신하는 단계는, 중간 디바이스를 통해 또는 직접적으로 단거리 링크를 통해 레코드 전송자 디바이스로부터 전송자 개별 레코드를 수신하는 단계를 포함한다.

[0454] [0374] 제39 양상에서, 양상 38의 방법에 있어서, 단거리 링크는 피어-투-피어 통신 링크이다.

[0455] [0375] 제40 양상에서, 양상 33 내지 양상 39 중 어느 한 양상의 방법에 있어서, 수신자 개별 레코드는 상환 전용 배서, 질의 배서, 악의적인 레코드 배서, 또는 이들의 임의의 조합을 더 포함한다.

[0456] [0376] 제41 양상에서, 양상 33 내지 양상 40 중 어느 한 양상의 방법에 있어서, 전송자 개별 레코드는 레코드 전송자 디바이스에 의해 레코드 전송자의 인증 정보를 수신한 후에 생성되고, 그리고 수신자 개별 레코드를 생성하는 단계는 레코드 수신자 디바이스에 의해 레코드 수신자의 인증 정보를 수신하는 단계를 포함한다.

[0457] [0377] 제42 양상에서, 양상 33 내지 양상 41 중 어느 한 양상의 방법에 있어서, 전송자 개별 레코드를 검증하는 단계는, 전송자 공개 키를 사용하여, 전송자 서명이 전송자 개인 키를 사용하여 생성됨을 결정하는 단계를 포함한다.

[0458] [0378] 제43 양상에서, 양상 33 내지 양상 42 중 어느 한 양상의 방법에 있어서, 전송자 서명은 전송자 개인 키를 사용하여 레코드 전송자 디바이스의 보안 엘리먼트를 사용하여 생성되며, 전송자 개인 키는 레코드 전송자 디바이스의 보안 엘리먼트에 저장된다.

[0459] [0379] 제44 양상에서, 양상 33 내지 양상 43 중 어느 한 양상의 방법에 있어서, 수신자 서명은 수신자 개인 키를 사용하여 레코드 수신자 디바이스의 보안 엘리먼트를 사용하여 생성되고, 수신자 개인 키는 레코드 수신자 디바이스의 보안 엘리먼트에 저장된다.

[0460] [0380] 제45 양상에서, 양상 33 내지 양상 44 중 어느 한 양상의 방법은 프로세싱 플랫폼으로부터 공통 레코드들을 수신하는 단계를 더 포함하고, 공통 레코드들은 전송자 공개 키 및 수신자 공개 키를 포함한다.

[0461] [0381] 제46 양상에서, 양상 45의 방법은 레코드 전송자 디바이스에 공통 레코드들을 전송하는 단계를 더 포함한다.

[0462] [0382] 제47 양상에서, 양상 33 내지 양상 44 중 어느 한 양상의 방법은 레코드 전송자 디바이스로부터 공통 레코드들을 수신하는 단계를 더 포함하고, 공통 레코드들은 전송자 공개 키 및 수신자 공개 키를 포함한다.

[0463] [0383] 제48 양상에서, 양상 45 내지 양상 47 중 어느 한 양상의 방법에 있어서, 공통 레코드들은 공통 레코드들의 제3 서명을 더 포함하고, 제3 서명은 프로세싱 플랫폼의 제3 개인 키를 사용하여 생성되며, 방법은: 반드시 그런 것은 아니지만 프로세싱 플랫폼과 통신하면서 프로세싱 플랫폼의 제3 공개 키를 사용하여 공통 레코드들을 검증하는 단계를 더 포함하고, 제3 공개 키 및 제3 개인 키는 제3 공개-키 암호 쌍을 형성하며, 그리고 공통 레코드들을 검증하는 단계는, 제3 공개 키를 사용하여, 제3 서명이 제3 개인 키를 사용하여 생성됨을 결정하는 단계를 포함한다.

[0464] [0384] 제49 양상에서, 컴퓨터 시스템이 개시된다. 컴퓨터 시스템은: 하드웨어 프로세서; 및 명령들이 저장된 비-일시적 메모리를 포함하며, 명령들은, 프로세서에 의해 실행될 때, 프로세서로 하여금 양상 1 내지 양상 48 중 어느 한 양상의 방법을 수행하게 한다.

[0465] [0385] 제50 양상에서, 양상 49의 컴퓨터 시스템에 있어서, 컴퓨터 시스템은 모바일 디바이스이다.

[0466] [0386] 제51 양상에서, 양상 50의 컴퓨터 시스템에 있어서, 모바일 디바이스는 웨어러블 디스플레이 시스템이다.

[0467] *에이전트들에 의해 암호화방식으로 싸인된 레코드들의 안전한 교환*

[0468] [0387] 제52 양상에서, 에이전트들에 의해 암호화방식으로 싸인된 레코드들을 안전하게 교환하기 위한 방법이 개시된다. 방법은 하드웨어 프로세서의 제어 하에 수행되며, 그리고 본인 디바이스로부터 본인-수정된 개별 레코드를 수신하는 단계 – 본인-수정된 개별 레코드는 본인-수정된 개별 레코드의 서명 및 에이전트-수정된 개별 레코드를 포함하고, 에이전트-수정된 개별 레코드는 오리지널 개별 레코드, 에이전트 디바이스의 에이전트 공개 키, 및 에이전트-수정된 개별 레코드의 서명을 포함하고, 오리지널 개별 레코드는 레코드 콘텐츠, 레코드 전송자 디바이스의 전송자 공개 키, 본인 디바이스의 본인 공개 키, 및 오리지널 개별 레코드의 서명을 포함하고, 본인-수정된 개별 레코드의 서명은 본인 디바이스의 본인 개인 키를 사용하여 생성되고, 본인 공개 키 및 본인 개인 키는 본인 공개-키 암호 쌍을 형성하고, 에이전트-수정된 개별 레코드는 본인 디바이스로부터 오리지널 개별 레코드를 수신한 후에 에이전트 디바이스에 의해 생성되고, 에이전트-수정된 개별 레코드의 서명은 에이전트 디바이스의 에이전트 개인 키를 사용하여 생성되고, 에이전트 공개 키 및 에이전트 개인 키는 에이전트 공개-키 암호 쌍을 형성하고, 오리지널 개별 레코드는, 에이전트 디바이스로부터 콘텐츠 요청을 수신하고, 에이전트 디바이스를 식별한 후에 레코드 전송자 디바이스에 의해 생성되고, 오리지널 개별 레코드의 서명은 레코드 전송자 디바이스의 전송자 개인 키를 사용하여 생성되며, 그리고 전송자 공개 키 및 전송자 개인 키는 전송자 공개-키 암호 쌍을 형성함 –; 본인-수정된 개별 레코드를 검증하는 단계; 및 본인-수정된 개별 레코드에 의해 명령된 대로 본인 디바이스에 대해 수행하는 단계를 포함한다.

[0469] [0388] 제53 양상에서, 양상 52의 방법에 있어서, 콘텐츠 요청은 본인 공개 키 및 요청된 콘텐츠를 포함하고, 레코드 콘텐츠는 요청된 콘텐츠와 관련된다.

[0470] [0389] 제54 양상에서, 양상 52 또는 양상 53의 방법에 있어서, 에이전트 디바이스를 식별하는 것은 파트너 식별을 수행하는 것을 포함하고, 파트너 식별은 지불 인가, 노킹, 물리적 표시, 빔 형성, 이전 어레인지먼트, 피상적인 유효성 검증, 또는 이들의 임의의 조합을 포함한다.

[0471] [0390] 제55 양상에서, 양상 54의 방법에 있어서, 오리지널 개별 레코드는 레코드 식별자를 더 포함한다.

[0472] [0391] 제56 양상에서, 양상 55의 방법에 있어서, 레코드 식별자는 단조적으로 증가하는 수이다.

[0473] [0392] 제57 양상에서, 양상 52 내지 양상 56 중 어느 한 양상의 방법에 있어서, 레코드 전송자 디바이스로부터 오리지널 개별 레코드를 수신하는 것은, 중간 디바이스를 통해 또는 직접적으로 단거리 링크를 통해 레코드 전송자 디바이스로부터 오리지널 개별 레코드를 수신하는 것을 포함한다.

[0474] [0393] 제58 양상에서, 양상 57의 방법에 있어서, 단거리 링크는 피어-투-피어 통신 링크이다.

[0475] [0394] 제59 양상에서, 양상 52 내지 양상 58 중 어느 한 양상의 방법에 있어서, 에이전트-수정된 개별 레코드는, 배서에 의해 핸들링됨, 질의 배서, 악의적인 레코드 배서, 또는 이들의 임의의 조합을 더 포함하고, 본인-수정된 개별 레코드는 상환 전용 배서, 질의 배서, 악의적인 레코드 배서, 또는 이들의 임의의 조합을 더 포함한다.

[0476] [0395] 제60 양상에서, 양상 52 내지 양상 59 중 어느 한 양상의 방법에 있어서, 오리지널 개별 레코드는, 레코드 전송자 디바이스에 의해 레코드 전송자의 인증 정보를 수신한 후에 레코드 전송자 디바이스에 의해 생성되고, 에이전트-수정된 개별 레코드는, 에이전트 디바이스에 의해 에이전트의 인증 정보를 수신한 후에 에이전트 디바이스에 의해 생성된다.

[0477] [0396] 제61 양상에서, 양상 52 내지 양상 60 중 어느 한 양상의 방법에 있어서, 오리지널 개별 레코드를 검증하는 것은, 전송자 공개 키를 사용하여, 오리지널 개별 레코드의 서명이 전송자 개인 키를 사용하여 생성됨을 결정하는 것; 에이전트 공개 키를 사용하여, 에이전트-수정된 개별 레코드의 서명이 에이전트 개인 키를 사용하여 생성됨을 결정하는 것; 및 본인 공개 키를 사용하여, 본인 디바이스의 서명이 본인 개인 키를 사용하여 생성됨을 결정하는 것을 포함한다.

[0478] [0397] 제62 양상에서, 양상 52 내지 양상 61 중 어느 한 양상의 방법은 레코드 전송자 디바이스, 에이전트 디바이스, 및 본인 디바이스에 공통 레코드들을 제공하는 단계를 더 포함하고, 공통 레코드들은 전송자 공개 키 및 본인 공개 키를 포함한다.

[0479] [0398] 제63 양상에서, 양상 52 내지 양상 61 중 어느 한 양상의 방법은, 레코드 전송자 디바이스에 공통 레코드들을 제공하는 단계 – 공통 레코드들은 전송자 공개 키 및 본인 공개 키를 포함함 –; 및 레코드 전송자 디

바이스로 하여금 에이전트에 공통 레코드들을 제공하게 하는 단계를 더 포함한다.

[0480] [0399] 제64 양상에서, 양상 52 내지 양상 61 중 어느 한 양상의 방법은, 에이전트에 공통 레코드들을 제공하는 단계 - 공통 레코드들은 전송자 공개 키 및 본인 공개 키를 포함함 -; 및 에이전트로 하여금 레코드 전송자 디바이스에 공통 레코드들을 제공하게 하는 단계를 더 포함한다.

[0481] [0400] 제65 양상에서, 양상 52 내지 양상 61 중 어느 한 양상의 방법은, 본인 디바이스에 공통 레코드들을 제공하는 단계 - 공통 레코드들은 전송자 공개 키 및 본인 공개 키를 포함함 -; 및 본인 디바이스로 하여금 에이전트에 공통 레코드들을 제공하게 하는 단계를 더 포함한다.

[0482] [0401] 제66 양상에서, 양상 65의 방법은 에이전트로 하여금 레코드 전송자 디바이스에 공통 레코드들을 제공하게 하는 단계를 더 포함한다.

[0483] [0402] 제67 양상에서, 양상 62 내지 양상 66 중 어느 한 양상의 방법에 있어서, 공통 레코드들은 공통 레코드 서명을 더 포함하고, 공통 레코드 서명은 프로세싱 플랫폼의 프로세싱 플랫폼 개인 키를 사용하여 생성되고, 방법은: 반드시 그런 것은 아니지만 프로세싱 플랫폼과 통신하면서 프로세싱 플랫폼의 프로세싱 플랫폼 공개 키를 사용하여 공통 레코드들을 검증하는 단계를 더 포함하고, 프로세싱 플랫폼 공개 키 및 프로세싱 플랫폼 개인 키는 프로세싱 플랫폼 공개-키 암호 쌍을 형성하며, 그리고 공통 레코드들을 검증하는 단계는, 프로세싱 플랫폼 공개 키를 사용하여, 공통 레코드 서명이 프로세싱 플랫폼 개인 키를 사용하여 생성됨을 결정하는 단계를 포함한다.

[0484] [0403] 제68 양상에서, 양상 62 내지 양상 67 중 어느 한 양상의 방법은 중앙 레코드들로부터 공통 레코드들을 생성하는 단계를 더 포함하고, 중앙 레코드들은 전송자 공개 키, 본인 공개 키, 에이전트 공개 키, 레코드 전송자 디바이스의 사용자 레코드 상황, 및 본인 디바이스의 사용자 레코드 상황을 포함한다.

[0485] [0404] 제69 양상에서, 양상 52 내지 양상 68 중 어느 한 양상의 방법은 에이전트 공개-키 암호 쌍 또는 본인 암호 쌍에 대해 상인에게 주기적으로 또는 한번 청구하는 단계를 더 포함한다.

[0486] [0405] 제70 양상에서, 에이전트들에 의해 암호화방식으로 싸인된 레코드들을 안전하게 교환하기 위한 방법이 개시된다. 방법은 하드웨어 프로세서의 제어 하에 수행되며, 그리고 에이전트 디바이스로부터 콘텐츠 요청을 수신하는 단계; 에이전트 디바이스를 식별하는 단계; 오리지널 개별 레코드를 생성하는 단계 - 오리지널 개별 레코드는 레코드 콘텐츠, 레코드 전송자 디바이스의 전송자 공개 키, 본인 디바이스의 본인 공개 키, 및 오리지널 개별 레코드의 서명을 포함하고, 오리지널 개별 레코드의 서명은 레코드 전송자 디바이스의 전송자 개인 키를 사용하여 생성되고, 전송자 공개 키 및 전송자 개인 키는 전송자 공개-키 암호 쌍을 형성함 -; 에이전트 디바이스에 오리지널 개별 레코드를 전송하는 단계; 에이전트 디바이스의 표시를 수신하는 단계: 오리지널 개별 레코드를 수신하는 단계; 반드시 그런 것은 아니지만 프로세싱 플랫폼과 통신하면서 전송자 공개 키를 사용하여 오리지널 개별 레코드를 검증하는 단계; 에이전트-수정된 개별 레코드를 생성하는 단계 - 에이전트-수정된 개별 레코드는 오리지널 개별 레코드, 에이전트 디바이스의 에이전트 공개 키, 및 에이전트-수정된 개별 레코드의 서명을 포함하고, 에이전트-수정된 개별 레코드의 서명은 에이전트 디바이스의 에이전트 개인 키를 사용하여 생성되며, 그리고 에이전트 공개 키 및 에이전트 개인 키는 에이전트 공개-키 암호 쌍을 형성함 -; 본인 디바이스에 에이전트-수정된 개별 레코드를 전송하는 단계; 및 본인 디바이스의 표시를 수신하는 단계: 에이전트-수정된 개별 레코드를 수신하는 단계; 본인-수정된 개별 레코드를 생성하는 단계 -본인-수정된 개별 레코드는 본인-수정된 개별 레코드의 서명 및 에이전트-수정된 개별 레코드를 포함하고, 본인-수정된 개별 레코드의 서명은 본인 디바이스의 본인 키를 사용하여 생성되며, 그리고 본인 공개 키 및 본인 개인 키는 본인 공개-키 암호 쌍을 형성함-; 본인-수정된 개별 레코드를 프로세싱 플랫폼에 상환하는 단계; 본인-수정된 개별 레코드에 의해 명령된 대로 프로세싱 플랫폼에 의한 퍼포먼스를 수신하는 단계; 및 에이전트 디바이스에 퍼포먼스 수신을 통지하는 단계를 포함한다.

[0487] [0406] 제71 양상에서, 양상 70의 방법에 있어서, 콘텐츠 요청은 본인 공개 키 및 요청된 콘텐츠를 포함하고, 레코드 콘텐츠는 요청된 콘텐츠와 관련된다.

[0488] [0407] 제72 양상에서, 양상 70 또는 양상 71의 방법에 있어서, 에이전트 디바이스를 식별하는 단계는 파트너 식별을 수행하는 단계를 포함하고, 파트너 식별은 지불 인가, 노킹, 물리적 표시, 빔 형성, 이전 어레인지먼트, 피상적인 유효성 검증, 또는 이들의 임의의 조합을 포함한다.

[0489] [0408] 제73 양상에서, 양상 70 내지 양상 72 중 어느 한 양상의 방법에 있어서, 오리지널 개별 레코드는 레코

드 식별자를 더 포함한다.

[0490] [0409] 제74 양상에서, 양상 73의 방법에 있어서, 레코드 식별자는 단조적으로 증가하는 수이다.

[0491] [0410] 제75 양상에서, 양상 70 내지 양상 74 중 어느 한 양상의 방법에 있어서, 에이전트 디바이스에 오리지널 개별 레코드를 전송하는 단계는, 중간 디바이스를 통해 또는 직접적으로 단거리 링크를 통해 에이전트 디바이스에 오리지널 개별 레코드를 전송하는 단계를 포함한다.

[0492] [0411] 제76 양상에서, 양상 75의 방법에 있어서, 단거리 링크는 피어-투-피어 통신 링크이다.

[0494] *[0412] 제77 양상에서, 양상 70 내지 양상 76 중 어느 한 양상의 방법에 있어서, 에이전트-수정된 개별 레코드는, 배서에 의해 핸들링됨, 질의 배서, 악의적인 레코드 배서, 또는 이들의 임의의 조합을 더 포함하고, 본인-수정된 개별 레코드는 상환 전용 배서, 질의 배서, 악의적인 레코드 배서, 또는 이들의 임의의 조합을 더 포함한다.

[0495] [0413] 제78 양상에서, 양상 70 내지 양상 77 중 어느 한 양상의 방법에 있어서, 오리지널 개별 레코드를 생성하는 단계는 레코드 전송자 디바이스에 의해 레코드 전송자의 인증 정보를 수신하는 단계를 포함하고, 에이전트-수정된 개별 레코드를 생성하는 단계는 에이전트 디바이스에 의해 에이전트의 인증 정보를 수신하는 단계를 포함한다.

[0496] [0414] 제79 양상에서, 양상 70 내지 양상 78 중 어느 한 양상의 방법에 있어서, 오리지널 개별 레코드를 검증하는 단계는, 전송자 공개 키를 사용하여, 오리지널 개별 레코드의 서명이 전송자 개인 키를 사용하여 생성됨을 결정하는 단계를 포함한다.

[0497] [0415] 제80 양상에서, 양상 70 내지 양상 79 중 어느 한 양상의 방법에 있어서, 오리지널 개별 레코드의 서명은 전송자 개인 키를 사용하여 레코드 전송자 디바이스의 보안 엘리먼트에 의해 생성되고, 전송자 개인 키는 레코드 전송자 디바이스의 보안 엘리먼트에 저장된다.

[0498] [0416] 제81 양상에서, 양상 70 내지 양상 80 중 어느 한 양상의 방법에 있어서, 에이전트-수정된 개별 레코드의 서명은 에이전트 개인 키를 사용하여 에이전트 디바이스의 보안 엘리먼트에 의해 생성되고, 에이전트 개인 키는 에이전트 디바이스의 보안 엘리먼트에 저장된다.

[0499] [0417] 제82 양상에서, 양상 70 내지 양상 81 중 어느 한 양상의 방법은 프로세싱 플랫폼으로부터 공통 레코드들을 수신하는 단계를 더 포함하고, 공통 레코드들은 전송자 공개 키 및 본인 공개 키를 포함한다.

[0500] [0418] 제83 양상에서, 양상 70 내지 양상 81 중 어느 한 양상의 방법은 에이전트 디바이스로부터 공통 레코드들을 수신하는 단계를 더 포함하고, 공통 레코드들은 전송자 공개 키 및 본인 공개 키를 포함한다.

[0501] [0419] 제84 양상에서, 양상 82 또는 양상 83의 방법에 있어서, 공통 레코드들은 공통 레코드 서명을 더 포함하고, 공통 레코드 서명은 프로세싱 플랫폼의 프로세싱 플랫폼 개인 키를 사용하여 생성되고, 방법은: 반드시 그런 것은 아니지만 프로세싱 플랫폼과 통신하면서 프로세싱 플랫폼의 프로세싱 플랫폼 공개 키를 사용하여 공통 레코드들을 검증하는 단계를 더 포함하고, 프로세싱 플랫폼 공개 키 및 프로세싱 플랫폼 개인 키는 프로세싱 플랫폼 공개-키 암호 쌍을 형성하며, 그리고 공통 레코드들을 검증하는 단계는, 프로세싱 플랫폼 공개 키를 사용하여, 공통 레코드 서명이 프로세싱 플랫폼 개인 키를 사용하여 생성됨을 결정하는 단계를 포함한다.

[0502] [0420] 제85 양상에서, 에이전트들에 의해 암호화방식으로 싸인된 레코드들을 안전하게 교환하기 위한 방법이 개시된다. 방법은 하드웨어 프로세서의 제어 하에 수행되며, 그리고 레코드 전송자 디바이스에 콘텐츠 요청을 전송하는 단계; 레코드 전송자 디바이스로부터 오리지널 개별 레코드를 수신하는 단계 – 오리지널 개별 레코드는, 레코드 전송자 디바이스로부터 콘텐츠 요청을 수신하고, 에이전트 디바이스를 식별한 후에 레코드 전송자 디바이스에 의해 생성되고, 오리지널 개별 레코드는 레코드 콘텐츠, 레코드 전송자 디바이스의 전송자 공개 키, 본인 디바이스의 본인 공개 키, 및 오리지널 개별 레코드의 서명을 포함하고, 오리지널 개별 레코드의 서명은 레코드 전송자 디바이스의 전송자 개인 키를 사용하여 생성되며, 그리고 전송자 공개 키 및 전송자 개인 키는 전송자 공개-키 암호 쌍을 형성함–; 반드시 그런 것은 아니지만 프로세싱 플랫폼과 통신하면서 전송자 공개 키를 사용하여 오리지널 개별 레코드를 검증하는 단계; 에이전트-수정된 개별 레코드를 생성하는 단계 –에이전트-수정된 개별 레코드는 오리지널 개별 레코드, 에이전트 디바이스의 에이전트 공개 키, 및 에이전트-수정된 개별 레코드의 서명을 포함하고, 에이전트-수정된 개별 레코드의 서명은 에이전트 디바이스의 에이전트 개인 키를 사용하여 생성되며, 그리고 에이전트 공개 키 및 에이전트 개인 키는 에이전트 공개-키 암호 쌍을 형성함 –; 본인 디바이스에 에이전트-수정된 개별 레코드를 전송하는 단계; 및 본인 디바이스의 표시를 수신하는 단계: 에

이전트-수정된 개별 레코드를 수신하는 단계; 본인-수정된 개별 레코드를 생성하는 단계 -본인-수정된 개별 레코드는 본인-수정된 개별 레코드의 서명 및 에이전트-수정된 개별 레코드를 포함하고, 본인-수정된 개별 레코드의 서명은 본인 디바이스의 본인 개인키를 사용하여 생성되며, 그리고 본인 공개 키 및 본인 개인 키는 본인 공개-키 암호 쌍을 형성함 -; 본인-수정된 개별 레코드를 프로세싱 플랫폼에 상환하는 단계; 및 본인-수정된 개별 레코드에 의해 명령된 대로 프로세싱 플랫폼에 의한 퍼포먼스를 수신하는 단계를 포함한다.

[0503] [0421] 제86 양상에서, 양상 85의 방법에 있어서, 콘텐츠 요청은 본인 공개 키 및 요청된 콘텐츠를 포함하고, 레코드 콘텐츠는 요청된 콘텐츠와 관련된다.

[0504] [0422] 제87 양상에서, 양상 85 또는 양상 86의 방법에 있어서, 에이전트 디바이스를 식별하는 것은 파트너 식별을 수행하는 것을 포함하고, 파트너 식별은 지불 인가, 노킹, 물리적 표시, 빔 형성, 이전 어레인지먼트, 피상적인 유효성 검증, 또는 이들의 임의의 조합을 포함한다.

[0505] [0423] 제88 양상에서, 양상 85 내지 양상 87 중 어느 한 양상의 방법에 있어서, 오리지널 개별 레코드는 레코드 식별자를 더 포함한다.

[0506] [0424] 제89 양상에서, 양상 88의 방법에 있어서, 레코드 식별자는 단조적으로 증가하는 수이다.

[0507] [0425] 제90 양상에서, 양상 85 내지 양상 89 중 어느 한 양상의 방법에 있어서, 레코드 전송자 디바이스로부터 오리지널 개별 레코드를 수신하는 단계는, 중간 디바이스를 통해 또는 직접적으로 단거리 링크를 통해 레코드 전송자 디바이스로부터 오리지널 개별 레코드를 수신하는 단계를 포함한다.

[0508] [0426] 제91 양상에서, 양상 90의 방법에 있어서, 단거리 링크는 피어-투-피어 통신 링크이다.

[0509] [0427] 제92 양상에서, 양상 85 내지 양상 91 중 어느 한 양상의 방법에 있어서, 에이전트-수정된 개별 레코드는, 배서에 의해 핸들링됨, 질의 배서, 악의적인 레코드 배서, 또는 이들의 임의의 조합을 더 포함하고, 본인-수정된 개별 레코드는 상환 전용 배서, 질의 배서, 악의적인 레코드 배서, 또는 이들의 임의의 조합을 더 포함한다.

[0510] [0428] 제93 양상에서, 양상 85 내지 양상 92 중 어느 한 양상의 방법에 있어서, 오리지널 개별 레코드를 생성하는 것은 레코드 전송자 디바이스에 의해 레코드 전송자의 인증 정보를 수신하는 것을 포함하고, 에이전트-수정된 개별 레코드를 생성하는 단계는 에이전트 디바이스에 의해 에이전트의 인증 정보를 수신하는 단계를 포함한다.

[0511] [0429] 제94 양상에서, 양상 85 내지 양상 93 중 어느 한 양상의 방법에 있어서, 오리지널 개별 레코드를 검증하는 단계는, 전송자 공개 키를 사용하여, 오리지널 개별 레코드의 서명이 전송자 개인 키를 사용하여 생성됨을 결정하는 단계를 포함한다.

[0512] [0430] 제95 양상에서, 양상 85 내지 양상 94 중 어느 한 양상의 방법에 있어서, 오리지널 개별 레코드의 서명은 전송자 개인 키를 사용하여 레코드 전송자 디바이스의 보안 엘리먼트에 의해 생성되고, 전송자 개인 키는 레코드 전송자 디바이스의 보안 엘리먼트에 저장된다.

[0513] [0431] 제96 양상에서, 양상 85 내지 양상 95 중 어느 한 양상의 방법에 있어서, 에이전트-수정된 개별 레코드의 서명은 에이전트 개인 키를 사용하여 에이전트 디바이스의 보안 엘리먼트에 의해 생성되며, 에이전트 개인 키는 에이전트 디바이스의 보안 엘리먼트에 저장된다.

[0514] [0432] 제97 양상에서, 양상 85 내지 양상 96 중 어느 한 양상의 방법은, 프로세싱 플랫폼으로부터 공통 레코드들을 수신하는 단계를 더 포함하며, 공통 레코드들은 전송자 공개 키 및 본인 공개 키를 포함한다.

[0515] [0433] 제98 양상에서, 양상 97의 방법은, 공통 레코드들을 레코드 전송자 디바이스에 전송하는 단계를 더 포함한다.

[0516] [0434] 제99 양상에서, 양상 85 내지 양상 96 중 어느 한 양상의 방법은, 본인 디바이스로부터 공통 레코드들을 수신하는 단계를 더 포함하며, 공통 레코드들은 전송자 공개 키 및 본인 공개 키를 포함한다.

[0517] [0435] 제100 양상에서, 양상 97 내지 양상 99 중 어느 한 양상의 방법에 있어서, 공통 레코드들은 공통 레코드 서명을 더 포함하며, 공통 레코드 서명은 프로세싱 플랫폼의 프로세싱 플랫폼 개인 키를 사용하여 생성되며, 방법은, 반드시 그런 것은 아니지만 프로세싱 플랫폼과 통신하면서 프로세싱 플랫폼의 프로세싱 플랫폼 공개 키를 사용하여 공통 레코드들을 검증하는 단계를 더 포함하며, 프로세싱 플랫폼 공개 키 및 프로세싱 플랫폼 개인

키는 프로세싱 플랫폼 공개-키 암호 쌍을 형성하며, 공통 레코드들을 검증하는 단계는, 공통 레코드 서명이 프로세싱 플랫폼 개인 키를 사용하여 생성됨을 결정하기 위해, 프로세싱 플랫폼 공개 키를 사용하는 단계를 포함한다.

[0518] [0436] 제101 양상에서, 컴퓨터 시스템이 개시된다. 컴퓨터 시스템은: 프로세서; 및 프로세서에 의해 실행될 때, 프로세서로 하여금 양상 52 내지 양상 100 중 어느 한 양상의 방법을 수행하게 하는 명령들이 저장된 비-일시적 메모리를 포함한다.

[0519] [0437] 제102 양상에서, 양상 101의 컴퓨터 시스템에 있어서, 컴퓨터 시스템은 모바일 디바이스이다.

[0520] [0438] 제103 양상에서, 양상 102의 컴퓨터 시스템에 있어서, 모바일 디바이스는 웨어러블 디스플레이 시스템이다.

[0521] *암호화방식으로 싸인된 레코드들의 체인들의 안전한 교환*

[0522] [0439] 제104 양상에서, 암호화방식으로 싸인된 레코드들의 체인들을 안전하게 교환하기 위한 방법이 개시된다. 방법은 하드웨어 프로세서의 제어 하에 수행되며, 그리고 후속적 수신자 개별 레코드를 후속적 레코드 수신자 디바이스로부터 수신하는 단계 – 후속적 수신자 개별 레코드는 후속적 수신자 개별 레코드의 후속적 수신자 서명 및 오리지널 수신자 개별 레코드를 포함하며, 오리지널 수신자 개별 레코드는 전송자 개별 레코드, 후속적 레코드 수신자 디바이스의 후속적 수신자 공개 키, 및 오리지널 수신자 개별 레코드의 오리지널 수신자 서명을 포함하며, 전송자 개별 레코드는 레코드 콘텐츠, 레코드 전송자 디바이스의 전송자 공개 키, 오리지널 레코드 수신자 디바이스의 오리지널 수신자 공개 키, 및 전송자 개별 레코드의 전송자 서명을 포함하며, 전송자 개별 레코드는 오리지널 레코드 수신자 디바이스로부터 오리지널 콘텐츠 요청을 수신하고 오리지널 레코드 수신자 디바이스를 식별한 후에 레코드 전송자 디바이스에 의해 생성되며, 전송자 서명은 레코드 전송자 디바이스의 전송자 개인 키를 사용하여 생성되며, 전송자 공개 키 및 전송자 개인 키는 전송자 공개-키 암호 쌍을 형성하며, 오리지널 수신자 개별 레코드는 후속적 레코드 수신자 디바이스로부터 후속적 콘텐츠 요청을 수신하고 후속적 레코드 수신자 디바이스를 식별한 후에 오리지널 레코드 수신자 디바이스에 의해 생성되며, 오리지널 수신자 서명은 오리지널 레코드 수신자 디바이스의 오리지널 수신자 개인 키를 사용하여 생성되며, 오리지널 수신자 공개 키 및 오리지널 수신자 개인 키는 오리지널 수신자 공개-키 암호 쌍을 형성하며, 후속적 수신자 서명은 후속적 레코드 수신자 디바이스의 후속적 수신자 개인 키를 사용하여 생성되며, 후속적 수신자 공개 키 및 후속적 수신자 개인 키는 후속적 수신자 공개-키 암호 쌍을 형성함 –; 후속적 수신자 개별 레코드를 검증하는 단계; 및 후속적 레코드 수신자에 대해 후속적 수신자 개별 레코드에 의해 명령된 대로 수행하는 단계를 포함한다.

[0523] [0440] 제105 양상에서, 양상 104의 방법에 있어서, 오리지널 콘텐츠 요청은 오리지널 수신자 공개 키 및 오리지널 콘텐츠를 포함하며, 레코드 콘텐츠는 오리지널 콘텐츠와 관련되며, 후속적 콘텐츠 요청은 후속적 수신자 공개 키 및 후속적 콘텐츠를 포함하며, 오리지널 콘텐츠는 후속적 콘텐츠와 관련된다.

[0524] [0441] 제106 양상에서, 양상 104 또는 양상 105의 방법에 있어서, 오리지널 콘텐츠 요청자를 식별하는 단계 또는 후속적 콘텐츠 요청자를 식별하는 단계는 파트너 식별을 수행하는 단계를 포함하며, 파트너 식별은 콘텐츠인가, 노킹, 물리적 표시, 빔 형성, 이전 어레인지먼트, 피상적인 유효성 검증, 또는 이들의 임의의 조합을 포함한다.

[0525] [0442] 제107 양상에서, 양상 104 내지 양상 106 중 어느 한 양상의 방법에 있어서, 전송자 개별 레코드는 레코드 식별자를 더 포함한다.

[0526] [0443] 제108 양상에서, 양상 107의 방법에 있어서, 레코드 식별자는 단조적으로 증가하는 수이다.

[0527] [0444] 제109 양상에서, 양상 104 내지 양상 108 중 어느 한 양상의 방법에 있어서, 전송자 개별 레코드는 중간 디바이스를 통해 또는 직접적으로 제1 단거리 링크를 통해 레코드 전송자 디바이스에 의해 오리지널 레코드 수신자 디바이스에 전송되며, 오리지널 수신자 개별 레코드를 후속적 레코드 수신자 디바이스에 전송하는 단계는 중간 디바이스를 통해 또는 직접적으로 제2 단거리 링크를 통해 오리지널 수신자 개별 레코드를 후속적 레코드 수신자 디바이스에 전송하는 단계를 포함한다.

[0528] [0445] 제110 양상에서, 양상 109의 방법에 있어서, 제1 단거리 링크는 피어-투-피어 통신 링크이거나 또는 제2 단거리 링크는 피어-투-피어 통신 링크이다.

[0529] [0446] 제111 양상에서, 양상 104 내지 양상 110 중 어느 한 양상의 방법에 있어서, 후속적 수신자 개별 레코

드는 상환 전용 배서, 질의 배서, 악의적인 레코드 배서, 또는 이들의 임의의 조합을 더 포함한다.

[0530] [0447] 제112 양상에서, 양상 104 내지 양상 111 중 어느 한 양상의 방법에 있어서, 전송자 개별 레코드는 레코드 전송자의 인증 정보를 수신한 후에 레코드 전송자 디바이스에 의해 생성되며, 오리지널 수신자 개별 레코드는 오리지널 레코드 수신자 디바이스의 인증 정보를 수신한 후에 오리지널 레코드 수신자 디바이스에 의해 생성되며, 후속적 수신자 개별 레코드는 후속적 레코드 수신자 디바이스에 의해 후속적 레코드 수신자 디바이스의 인증 정보를 수신한 후에 생성된다.

[0531] [0448] 제113 양상에서, 양상 104 내지 양상 112 중 어느 한 양상의 방법에 있어서, 후속적 수신자 개별 레코드를 검증하는 단계는: 전송자 서명이 전송자 개인 키를 사용하여 생성됨을 결정하기 위해 전송자 공개 키를 사용하는 단계; 오리지널 수신자 서명이 오리지널 수신자 개인 키를 사용하여 생성됨을 결정하기 위해 오리지널 수신자 공개 키를 사용하는 단계; 및 후속적 수신자 서명이 후속적 수신자 개인 키를 사용하여 생성됨을 결정하기 위해 후속적 수신자 공개 키를 사용하는 단계를 포함한다.

[0532] [0449] 제114 양상에서, 양상 104 내지 양상 113 중 어느 한 양상의 방법에 있어서, 전송자 서명은 전송자 개인 키를 사용하여 레코드 전송자 디바이스의 보안 엘리먼트에 의해 생성되며, 전송자 개인 키는 레코드 전송자 디바이스의 보안 엘리먼트에 저장되며, 오리지널 수신자 서명은 오리지널 수신자 개인 키를 사용하여 오리지널 레코드 수신자 디바이스의 보안 엘리먼트에 의해 생성되며, 오리지널 수신자 개인 키는 오리지널 레코드 수신자 디바이스의 보안 엘리먼트에 저장되며, 후속적 수신자 서명은 후속적 수신자 개인 키를 사용하여 후속적 레코드 수신자 디바이스의 보안 엘리먼트에 의해 생성되며, 후속적 수신자 개인 키는 후속적 레코드 수신자 디바이스의 보안 엘리먼트에 저장된다.

[0533] [0450] 제115 양상에서, 암호화방식으로 싸인된 레코드들의 체인들을 안전하게 교환하기 위한 방법이 개시된다. 방법은 하드웨어 프로세서의 제어 하에 수행되며, 그리고 오리지널 레코드 수신자 디바이스로부터 오리지널 콘텐츠 요청을 수신하는 단계; 오리지널 레코드 수신자 디바이스를 식별하는 단계; 전송자 개별 레코드를 생성하는 단계 – 전송자 개별 레코드는 레코드 콘텐츠, 레코드 전송자 디바이스의 전송자 공개 키, 오리지널 레코드 수신자 디바이스의 오리지널 수신자 공개 키, 및 전송자 개별 레코드의 전송자 서명을 포함하며, 전송자 서명은 레코드 전송자 디바이스의 전송자 개인 키를 사용하여 생성되며, 전송자 공개 키 및 전송자 개인 키는 전송자 공개-키 암호 쌍을 형성함 –; 전송자 개별 레코드를 오리지널 콘텐츠 요청자에게 전송하는 단계; 및 오리지널 콘텐츠 요청자의 표시를 수신하는 단계: 전송자 개별 레코드를 수신하는 단계; 반드시 그런 것은 아니지만 프로세싱 플랫폼과 통신하면서 전송자 공개 키를 사용하여 전송자 개별 레코드를 검증하는 단계; 후속적 레코드 수신자 디바이스로부터 후속적 콘텐츠 요청을 수신하는 단계; 후속적 레코드 수신자 디바이스를 식별하는 단계; 오리지널 수신자 개별 레코드를 생성하는 단계 – 오리지널 수신자 개별 레코드는 전송자 개별 레코드, 후속적 레코드 수신자 디바이스의 후속적 수신자 공개 키, 및 오리지널 수신자 개별 레코드의 오리지널 수신자 서명을 포함하며, 오리지널 수신자 서명은 오리지널 레코드 수신자 디바이스의 오리지널 수신자 개인 키를 사용하여 생성되며, 오리지널 수신자 공개 키 및 오리지널 수신자 개인 키는 오리지널 수신자 공개-키 암호 쌍을 형성함 –; 오리지널 수신자 개별 레코드를 후속적 레코드 수신자 디바이스에 전송하는 단계; 및 후속적 레코드 수신자의 표시를 수신하는 단계: 오리지널 수신자 개별 레코드를 수신하는 단계; 반드시 그런 것은 아니지만 프로세싱 플랫폼과 통신하면서 전송자 공개 키 및 오리지널 수신자 공개 키를 사용하여 오리지널 수신자 개별 레코드를 검증하는 단계; 후속적 수신자 개별 레코드를 생성하는 단계 – 후속적 수신자 개별 레코드는 후속적 수신자 개별 레코드의 후속적 수신자 서명 및 오리지널 수신자 개별 레코드를 포함하며, 후속적 수신자 서명은 후속적 레코드 수신자 디바이스의 후속적 수신자 개인 키를 사용하여 생성되며, 후속적 수신자 공개 키 및 후속적 수신자 개인 키는 후속적 수신자 공개-키 암호 쌍을 형성함 –; 오리지널 수신자 개별 레코드를 프로세싱 플랫폼에 상환하는 단계; 및 후속적 수신자 개별 레코드에 의해 명령된 대로 프로세싱 플랫폼에 의한 퍼포먼스를 수신하는 단계를 포함한다.

[0534] [0451] 제116 양상에서, 양상 115의 방법에 있어서, 오리지널 콘텐츠 요청은 오리지널 수신자 공개 키 및 오리지널 콘텐츠를 포함하며, 레코드 콘텐츠는 오리지널 콘텐츠와 관련되며, 후속적 콘텐츠 요청은 후속적 수신자 공개 키 및 후속적 콘텐츠를 포함하며, 오리지널 콘텐츠는 후속적 콘텐츠와 관련된다.

[0535] [0452] 제117 양상에서, 양상 115 또는 양상 116의 방법에 있어서, 오리지널 콘텐츠 요청자를 식별하는 단계 또는 후속적 콘텐츠 요청자를 식별하는 단계는 파트너 식별을 수행하는 단계를 포함하며, 파트너 식별은 콘텐츠인가, 노킹, 물리적 표시, 빔 형성, 이전 어레인지먼트, 피상적인 유효성 검증, 또는 이들의 임의의 조합을 포함한다.

[0536] [0453] 제118 양상에서, 양상 115 내지 양상 117 중 어느 한 양상의 방법에 있어서, 전송자 개별 레코드는 레코드 식별자를 더 포함한다.

[0537] [0454] 제119 양상에서, 양상 118의 방법에 있어서, 레코드 식별자는 단조적으로 증가하는 수이다.

[0538] [0455] 제120 양상에서, 양상 115 내지 양상 119 중 어느 한 양상의 방법에 있어서, 전송자 개별 레코드를 오리지널 레코드 수신자 디바이스에 전송하는 단계는 중간 디바이스를 통해 또는 직접적으로 제1 단거리 링크를 통해 전송자 개별 레코드를 오리지널 레코드 수신자 디바이스에 전송하는 단계를 포함하고, 오리지널 수신자 개별 레코드를 후속적 레코드 수신자 디바이스에 전송하는 단계는 중간 디바이스를 통해 또는 직접적으로 제2 단거리 링크를 통해 오리지널 수신자 개별 레코드를 후속적 레코드 수신자 디바이스에 전송하는 단계를 포함한다.

[0539] [0456] 제121 양상에서, 양상 120의 방법에 있어서, 제1 단거리 링크는 피어-투-피어 통신 링크이거나 또는 제2 단거리 링크는 피어-투-피어 통신 링크이다.

[0540] [0457] 제122 양상에서, 양상 115 내지 양상 121 중 어느 한 양상의 방법에 있어서, 후속적 수신자 개별 레코드는 상환 전용 배서, 질의 배서, 악의적인 레코드 배서, 또는 이들의 임의의 조합을 더 포함한다.

[0541] [0458] 제123 양상에서, 양상 115 내지 양상 122 중 어느 한 양상의 방법에 있어서, 전송자 개별 레코드를 생성하는 단계는 레코드 전송자 디바이스에 의해 레코드 전송자의 인증 정보를 수신하는 단계를 포함하며, 오리지널 수신자 개별 레코드를 생성하는 단계는 오리지널 레코드 수신자 디바이스에 의해 오리지널 레코드 수신자의 인증 정보를 수신하는 단계를 포함하며, 후속적 수신자 개별 레코드를 생성하는 단계는 후속적 레코드 수신자 디바이스에 의해 후속적 레코드 수신자의 인증 정보를 수신하는 단계를 포함한다.

[0542] [0459] 제124 양상에서, 양상 115 내지 양상 123 중 어느 한 양상의 방법에 있어서, 전송자 개별 레코드를 검증하는 단계는 전송자 서명이 전송자 개인 키를 사용하여 생성됨을 결정하기 위해 전송자 공개 키를 사용하는 단계를 포함하며, 오리지널 수신자 개별 레코드를 검증하는 단계는 오리지널 수신자 서명이 오리지널 수신자 개인 키를 사용하여 생성됨을 결정하기 위해 오리지널 수신자 공개 키를 사용하는 단계를 포함한다.

[0543] [0460] 제125 양상에서, 양상 115 내지 양상 124 중 어느 한 양상의 방법에 있어서, 전송자 서명은 전송자 개인 키를 사용하여 레코드 전송자 디바이스의 보안 엘리먼트에 의해 생성되며, 전송자 개인 키는 레코드 전송자 디바이스의 보안 엘리먼트에 저장되며, 오리지널 수신자 서명은 오리지널 수신자 개인 키를 사용하여 오리지널 레코드 수신자 디바이스의 보안 엘리먼트에 의해 생성되며, 오리지널 수신자 개인 키는 오리지널 레코드 수신자 디바이스의 보안 엘리먼트에 저장되며, 후속적 수신자 서명은 후속적 수신자 개인 키를 사용하여 후속적 레코드 수신자 디바이스의 보안 엘리먼트에 의해 생성되며, 후속적 수신자 개인 키는 후속적 레코드 수신자 디바이스의 보안 엘리먼트에 저장된다.

[0544] [0461] 제126 양상에서, 암호화방식으로 싸인된 레코드들의 체인들을 안전하게 교환하기 위한 방법이 개시된다. 방법은 하드웨어 프로세서의 제어 하에 수행되며, 그리고 오리지널 콘텐츠 요청을 레코드 전송자 디바이스에 전송하는 단계; 레코드 전송자 디바이스로부터 전송자 개별 레코드를 수신하는 단계 – 전송자 개별 레코드는 레코드 콘텐츠, 레코드 전송자 디바이스의 전송자 공개 키, 오리지널 레코드 수신자 디바이스의 오리지널 수신자 공개 키, 및 전송자 개별 레코드의 전송자 서명을 포함하며, 전송자 서명은 레코드 전송자 디바이스의 전송자 개인 키를 사용하여 생성되며, 전송자 공개 키 및 전송자 개인 키는 전송자 공개-키 암호 쌍을 형성함 –; 반드시 그런 것은 아니지만 프로세싱 플랫폼과 통신하면서 전송자 공개 키를 사용하여 전송자 개별 레코드를 검증하는 단계; 후속적 레코드 수신자 디바이스로부터 후속적 콘텐츠 요청을 수신하는 단계; 후속적 레코드 수신자 디바이스를 식별하는 단계; 오리지널 수신자 개별 레코드를 생성하는 단계 – 오리지널 수신자 개별 레코드는 전송자 개별 레코드, 후속적 레코드 수신자 디바이스의 후속적 수신자 공개 키, 및 오리지널 수신자 개별 레코드의 오리지널 수신자 서명을 포함하며, 오리지널 수신자 서명은 오리지널 레코드 수신자 디바이스의 오리지널 수신자 개인 키를 사용하여 생성되며, 오리지널 수신자 공개 키 및 오리지널 수신자 개인 키는 오리지널 수신자 공개-키 암호 쌍을 형성함 –; 오리지널 수신자 개별 레코드를 후속적 레코드 수신자 디바이스에 전송하는 단계; 및 후속적 레코드 수신자의 표시를 수신하는 단계: 오리지널 수신자 개별 레코드를 수신하는 단계; 반드시 그런 것은 아니지만 프로세싱 플랫폼과 통신하면서 전송자 공개 키 및 오리지널 수신자 공개 키를 사용하여 오리지널 수신자 개별 레코드를 검증하는 단계; 후속적 수신자 개별 레코드를 생성하는 단계 – 후속적 수신자 개별 레코드는 후속적 수신자 개별 레코드의 후속적 수신자 서명 및 오리지널 수신자 개별 레코드를 포함하며, 후속적 수신자 서명은 후속적 레코드 수신자 디바이스의 후속적 수신자 개인 키를 사용하여 생성되며, 후속적 수신자 공개 키 및 후속적 수신자 개인 키는 후속적 수신자 공개-키 암호 쌍을 형성함 –; 오

리지널 수신자 개별 레코드를 프로세싱 플랫폼에 상환하는 단계; 및 후속적 수신자 개별 레코드에 의해 명령된 대로 프로세싱 플랫폼에 의한 퍼포먼스를 수신하는 단계를 포함한다.

[0545] [0462] 제127 양상에서, 양상 126의 방법에 있어서, 오리지널 콘텐츠 요청은 오리지널 수신자 공개 키 및 오리지널 콘텐츠를 포함하며, 레코드 콘텐츠는 오리지널 콘텐츠와 관련되며, 후속적 콘텐츠 요청은 후속적 수신자 공개 키 및 후속적 콘텐츠를 포함하며, 오리지널 콘텐츠는 후속적 콘텐츠와 관련된다.

[0546] [0463] 제128 양상에서, 양상 126 또는 양상 127의 방법에 있어서, 오리지널 콘텐츠 요청자를 식별하는 단계 또는 후속적 콘텐츠 요청자를 식별하는 단계는 파트너 식별을 수행하는 단계를 포함하며, 파트너 식별은 콘텐츠인가, 노킹, 물리적 표시, 빔 형성, 이전 어레인지먼트, 피상적인 유효성 검증, 또는 이들의 임의의 조합을 포함한다.

[0547] [0464] 제129 양상에서, 양상 126 내지 양상 128 중 어느 한 양상의 방법에 있어서, 전송자 개별 레코드는 레코드 식별자를 더 포함한다.

[0548] [0465] 제130 양상에서, 양상 129의 방법에 있어서, 레코드 식별자는 단조적으로 증가하는 수이다.

[0549] [0466] 제131 양상에서, 양상 126 내지 양상 130 중 어느 한 양상의 방법에 있어서, 전송자 개별 레코드를 오리지널 레코드 수신자 디바이스에 전송하는 단계는 중간 디바이스를 통해 또는 직접적으로 제1 단거리 링크를 통해 전송자 개별 레코드를 오리지널 레코드 수신자 디바이스에 전송하는 단계를 포함하며, 오리지널 수신자 개별 레코드를 후속적 레코드 수신자 디바이스에 전송하는 단계는 중간 디바이스를 통해 또는 직접적으로 제2 단거리 링크를 통해 오리지널 수신자 개별 레코드를 후속적 레코드 수신자 디바이스에 전송하는 단계를 포함한다.

[0550] [0467] 제132 양상에서, 양상 131의 방법에 있어서, 제1 단거리 링크는 피어-투-피어 통신 링크이거나 또는 제2 단거리 링크는 피어-투-피어 통신 링크이다.

[0551] [0468] 제133 양상에서, 양상 126 내지 양상 132 중 어느 한 양상의 방법에 있어서, 후속적 수신자 개별 레코드는 상환 전용 배서, 질의 배서, 악의적인 레코드 배서, 또는 이들의 임의의 조합을 더 포함한다.

[0552] [0469] 제134 양상에서, 양상 126 내지 양상 133 중 어느 한 양상의 방법에 있어서, 전송자 개별 레코드를 생성하는 단계는 레코드 전송자 디바이스에 의해 레코드 전송자의 인증 정보를 수신하는 단계를 포함하며, 오리지널 수신자 개별 레코드를 생성하는 단계는 오리지널 레코드 수신자 디바이스에 의해 오리지널 레코드 수신자의 인증 정보를 수신하는 단계를 포함하며, 후속적 수신자 개별 레코드를 생성하는 단계는 후속적 레코드 수신자 디바이스에 의해 후속적 레코드 수신자의 인증 정보를 수신하는 단계를 포함한다.

[0553] [0470] 제135 양상에서, 양상 126 내지 양상 134 중 어느 한 양상의 방법에 있어서, 전송자 개별 레코드를 검증하는 단계는 전송자 서명이 전송자 개인 키를 사용하여 생성됨을 결정하기 위해 전송자 공개 키를 사용하는 단계를 포함하며, 오리지널 수신자 개별 레코드를 검증하는 단계는 오리지널 수신자 서명이 오리지널 수신자 개인 키를 사용하여 생성됨을 결정하기 위해 오리지널 수신자 공개 키를 사용하는 단계를 포함한다.

[0554] [0471] 제136 양상에서, 양상 126 내지 양상 135 중 어느 한 양상의 방법에 있어서, 전송자 서명은 전송자 개인 키를 사용하여 레코드 전송자 디바이스의 보안 엘리먼트에 의해 생성되며, 전송자 개인 키는 레코드 전송자 디바이스의 보안 엘리먼트에 저장되며, 오리지널 수신자 서명은 오리지널 수신자 개인 키를 사용하여 오리지널 레코드 수신자 디바이스의 보안 엘리먼트에 의해 생성되며, 오리지널 수신자 개인 키는 오리지널 레코드 수신자 디바이스의 보안 엘리먼트에 저장되며, 후속적 수신자 서명은 후속적 수신자 개인 키를 사용하여 후속적 레코드 수신자 디바이스의 보안 엘리먼트에 의해 생성되며, 후속적 수신자 개인 키는 후속적 레코드 수신자 디바이스의 보안 엘리먼트에 저장된다.

[0555] [0472] 제137 양상에서, 암호화방식으로 싸인된 레코드들의 체인들을 안전하게 교환하기 위한 방법이 개시된다. 방법은 하드웨어 프로세서의 제어 하에 수행되며, 그리고 후속적 콘텐츠 요청을 오리지널 레코드 수신자 디바이스에 전송하는 단계, 오리지널 레코드 수신자 디바이스로부터 오리지널 수신자 개별 레코드를 수신하는 단계 – 오리지널 수신자 개별 레코드는 전송자 개별 레코드, 후속적 레코드 수신자 디바이스의 후속적 수신자 공개 키, 및 오리지널 수신자 개별 레코드의 오리지널 수신자 서명을 포함하며, 전송자 개별 레코드는 레코드 콘텐츠, 레코드 전송자 디바이스의 전송자 공개 키, 오리지널 레코드 수신자 디바이스의 오리지널 수신자 공개 키, 및 전송자 개별 레코드의 전송자 서명을 포함하며, 전송자 개별 레코드는 오리지널 레코드 수신자 디바이스로부터 오리지널 콘텐츠 요청을 수신하고 오리지널 레코드 수신자 디바이스를 식별한 후에 레코드 전송자 디바이스에 의해 생성되며, 전송자 서명은 레코드 전송자 디바이스의 전송자 개인 키를 사용하여 생성되며, 전

송자 공개 키 및 전송자 개인 키는 전송자 공개-키 암호 쌍을 형성하며, 오리지널 수신자 개별 레코드는 후속적 레코드 수신자 디바이스로부터 후속적 콘텐츠 요청을 수신하고 후속적 레코드 수신자 디바이스를 식별한 후에 오리지널 레코드 수신자 디바이스에 의해 생성되며, 오리지널 수신자 서명은 오리지널 레코드 수신자 디바이스의 오리지널 수신자 개인 키를 사용하여 생성되며, 오리지널 수신자 공개 키 및 오리지널 수신자 개인 키는 오리지널 수신자 공개-키 암호 쌍을 형성함 -; 반드시 그런 것은 아니지만 프로세싱 플랫폼과 통신하면서 오리지널 수신자 개별 레코드를 검증하는 단계; 후속적 수신자 개별 레코드를 생성하는 단계 - 후속적 수신자 개별 레코드는 후속적 수신자 개별 레코드의 후속적 수신자 서명 및 오리지널 수신자 개별 레코드를 포함하며, 후속적 수신자 서명은 후속적 레코드 수신자 디바이스의 후속적 수신자 개인 키를 사용하여 생성되며, 후속적 수신자 공개 키 및 후속적 수신자 개인 키는 후속적 수신자 공개-키 암호 쌍을 형성함 -; 후속적 수신자 개별 레코드를 프로세싱 플랫폼에 상환하는 단계; 및 후속적 수신자 개별 레코드에 의해 명령된 대로 프로세싱 플랫폼에 의한 퍼포먼스를 수신하는 단계를 포함한다.

[0556] [0473] 제138 양상에서, 양상 137의 방법에 있어서, 오리지널 콘텐츠 요청은 오리지널 수신자 공개 키 및 오리지널 콘텐츠를 포함하며, 레코드 콘텐츠는 오리지널 콘텐츠와 관련되며, 후속적 콘텐츠 요청은 후속적 수신자 공개 키 및 후속적 콘텐츠를 포함하며, 오리지널 콘텐츠는 후속적 콘텐츠와 관련된다.

[0557] [0474] 제139 양상에서, 양상 137 또는 양상 138의 방법에 있어서, 오리지널 콘텐츠 요청자를 식별하는 단계 또는 후속적 콘텐츠 요청자를 식별하는 단계는 파트너 식별을 수행하는 단계를 포함하며, 파트너 식별은 콘텐츠인가, 노킹, 물리적 표시, 빔 형성, 이전 어레인지먼트, 피상적인 유효성 검증, 또는 이들의 임의의 조합을 포함한다.

[0558] [0475] 제140 양상에서, 양상 137 내지 양상 139 중 어느 한 양상의 방법에 있어서, 전송자 개별 레코드는 레코드 식별자를 더 포함한다.

[0559] [0476] 제141 양상에서, 양상 140의 방법에 있어서, 레코드 식별자는 단조적으로 증가하는 수이다.

[0560] [0477] 제142 양상에서, 양상 137 내지 양상 141 중 어느 한 양상의 방법에 있어서, 오리지널 레코드 수신자 디바이스로부터 오리지널 수신자 개별 레코드를 수신하는 단계는 중간 디바이스를 통해 또는 직접적으로 단거리 링크를 통해 오리지널 레코드 수신자 디바이스로부터 오리지널 수신자 개별 레코드를 수신하는 단계를 포함한다.

[0561] [0478] 제143 양상에서, 양상 142의 방법에 있어서, 단거리 링크는 피어-투-피어 통신 링크이다.

[0562] [0479] 제144 양상에서, 양상 137 내지 양상 143 중 어느 한 양상의 방법에 있어서, 후속적 수신자 개별 레코드는 상환 전용 배서, 질의 배서, 악의적인 레코드 배서, 또는 이들의 임의의 조합을 더 포함한다.

[0563] [0480] 제145 양상에서, 양상 137 내지 양상 144 중 어느 한 양상의 방법에 있어서, 전송자 개별 레코드는 레코드 전송자의 인증 정보를 수신한 후에 레코드 전송자 디바이스에 의해 생성되며, 오리지널 수신자 개별 레코드는 오리지널 레코드 수신자 디바이스의 인증 정보를 수신한 후에 오리지널 레코드 수신자 디바이스에 의해 생성되며, 후속적 수신자 개별 레코드를 생성하는 단계는 후속적 레코드 수신자 디바이스에 의해 후속적 레코드 수신자의 인증 정보를 수신하는 단계를 포함한다.

[0564] [0481] 제146 양상에서, 양상 137 내지 양상 145 중 어느 한 양상의 방법에 있어서, 오리지널 수신자 개별 레코드를 검증하는 단계는: 전송자 서명이 전송자 개인 키를 사용하여 생성됨을 결정하기 위해 전송자 공개 키를 사용하는 단계; 및 오리지널 수신자 서명이 오리지널 수신자 개인 키를 사용하여 생성됨을 결정하기 위해 오리지널 수신자 공개 키를 사용하는 단계를 포함한다.

[0565] [0482] 제147 양상에서, 양상 137 내지 양상 146 중 어느 한 양상의 방법에 있어서, 전송자 서명은 전송자 개인 키를 사용하여 레코드 전송자 디바이스의 보안 엘리먼트에 의해 생성되며, 전송자 개인 키는 레코드 전송자 디바이스의 보안 엘리먼트에 저장되며, 오리지널 수신자 서명은 오리지널 수신자 개인 키를 사용하여 오리지널 레코드 수신자 디바이스의 보안 엘리먼트에 의해 생성되며, 오리지널 수신자 개인 키는 오리지널 레코드 수신자 디바이스의 보안 엘리먼트에 저장되며, 후속적 수신자 서명은 후속적 수신자 개인 키를 사용하여 후속적 레코드 수신자 디바이스의 보안 엘리먼트에 의해 생성되며, 후속적 수신자 개인 키는 후속적 레코드 수신자 디바이스의 보안 엘리먼트에 저장된다.

[0566] *암호화방식으로 싸인된 디지털 수표들의 안전한 교환*

[0567] [0483] 제148 양상에서, 암호화방식으로 싸인된 디지털 수표들을 안전하게 교환하기 위한 방법이 개시된다.

방법은 하드웨어 프로세서의 제어 하에 수행되며, 그리고 수취인 디바이스로부터 배서된 디지털 수표를 수신하는 단계 - 배서된 디지털 수표는 오리지널 디지털 수표 및 배서된 디지털 수표의 수취인 서명을 포함하며, 오리지널 디지털 수표는 수취인으로부터 지불 요청을 수신하고 그리고 수취인 디바이스를 식별한 후에 지불인에 의해 생성되며, 오리지널 디지털 수표는 지불 금액, 지불인 공개 키, 수취인 공개 키, 및 오리지널 디지털 수표의 지불인 서명을 포함하며, 지불인 서명은 지불인 디바이스의 지불인 개인 키를 사용하여 생성되며, 지불인 공개 키 및 수취인 공개 키는 수취인 공개-키 암호 쌍을 형성하며, 배서된 디지털 수표는 지불인 디바이스로부터 오리지널 디지털 수표를 수신하고 그리고 반드시 그런 것은 아니지만 프로세싱 플랫폼과 통신하면서 지불인 공개 키를 사용하여 오리지널 디지털 수표를 검증한 후에 수취인 디바이스에 의해 생성되며, 수취인 서명은 수취인 디바이스에 의해 수취인 개인 키를 사용하여 생성되며, 수취인 공개 키 및 수취인 공개 키는 수취인 공개 키 암호 쌍을 형성함 -; 배서된 디지털 수표를 검증하는 단계; 및 지불 금액의 지불을 수취인에게 제공하는 단계를 포함한다.

[0568] [0484] 제149 양상에서, 양상 148의 방법에 있어서, 지불 요청은 수취인 공개 키 및 요청된 금액을 포함하며, 지불 금액은 요청된 금액과 관련된다.

[0569] [0485] 제150 양상에서, 양상 148 또는 양상 149의 방법에 있어서, 수취인 디바이스를 식별하는 단계는 파트너 식별을 수행하는 단계를 포함하며, 파트너 식별은 콘텐츠 인가, 노킹, 물리적 표시, 빔 형성, 이전 어레인지먼트, 피상적인 유효성 검증, 또는 이들의 임의의 조합을 포함한다.

[0570] [0486] 제151 양상에서, 양상 148 내지 양상 150 중 어느 한 양상의 방법에 있어서, 오리지널 디지털 수표는 수표 식별자를 더 포함한다.

[0571] [0487] 제152 양상에서, 양상 151의 방법에 있어서, 수표 식별자는 단조적으로 증가하는 수이다.

[0572] [0488] 제153 양상에서, 양상 148 내지 양상 152 중 어느 한 양상의 방법에 있어서, 지불인 디바이스로부터 오리지널 디지털 수표를 수신하는 단계는 중간 디바이스를 통해 또는 직접적으로 단거리 링크를 통해 지불인 디바이스로부터 오리지널 디지털 수표를 수신하는 단계를 포함한다.

[0573] [0489] 제154 양상에서, 양상 153의 방법에 있어서, 단거리 링크는 피어-투-피어 통신 링크이다.

[0574] [0490] 제155 양상에서, 양상 148 내지 양상 154 중 어느 한 양상의 방법에 있어서, 배서된 디지털 수표는 상환 전용 배서, 질의 배서, 악의적인 수표 배서, 또는 이들의 임의의 조합을 더 포함한다.

[0575] [0491] 제156 양상에서, 양상 148 내지 양상 155 중 어느 한 양상의 방법에 있어서, 오리지널 디지털 수표는 지불인의 인증 정보를 수신한 후에 지불인 디바이스에 의해 생성되며, 배서된 디지털 수표는 수취인의 인증 정보를 수신한 후에 수취인 디바이스에 의해 생성된다.

[0576] [0492] 제157 양상에서, 양상 148 내지 양상 156 중 어느 한 양상의 방법에 있어서, 오리지널 디지털 수표를 검증하는 단계는: 지불인 서명이 지불인 개인 키를 사용하여 생성됨을 결정하기 위해 지불인 공개 키를 사용하는 단계; 및 수취인 서명이 수취인 개인 키를 사용하여 생성됨을 결정하기 위해 수취인 공개 키를 사용하는 단계를 포함한다.

[0577] [0493] 제158 양상에서, 양상 148 내지 양상 157 중 어느 한 양상의 방법은 공통 회계장부를 지불인 디바이스 및 수취인 디바이스에 제공하는 단계를 더 포함하며, 공통 회계장부는 지불인 공개 키 및 수취인 공개 키를 포함한다.

[0578] [0494] 제159 양상에서, 양상 148 내지 양상 157 중 어느 한 양상의 방법은 공통 회계장부를 지불인 디바이스에 제공하는 단계 - 공통 회계장부는 지불인 공개 키 및 수취인 공개 키를 포함함-; 및 지불인 디바이스로 하여금 공통 회계장부를 수취인 디바이스에 제공하게 하는 단계를 더 포함한다.

[0579] [0495] 제160 양상에서, 양상 148 내지 양상 157 중 어느 한 양상의 방법은, 공통 회계장부를 수취인 디바이스에 제공하는 단계 - 공통 회계장부는 지불인 공개 키 및 수취인 공개 키를 포함함-; 및 수취인 디바이스로 하여금 공통 회계장부를 지불인 디바이스에 제공하게 하는 단계를 더 포함한다.

[0580] [0496] 제161 양상에서, 양상 158 내지 양상 160 중 어느 한 양상의 방법에 있어서, 공통 회계장부는 공통 회계장부 서명을 더 포함하며, 공통 회계장부 서명은 프로세싱 플랫폼의 프로세싱 플랫폼 개인 키를 사용하여 생성되며, 방법은, 반드시 그런 것은 아니지만 프로세싱 플랫폼과 통신하면서 프로세싱 플랫폼의 프로세싱 플랫폼 공개 키를 사용하여 공통 회계장부를 검증하는 단계를 더 포함하며, 프로세싱 플랫폼 공개 키 및 프로세싱 플랫

폼 개인 키는 프로세싱 플랫폼의 공개-키 암호 쌍을 형성하며, 공통 회계장부를 검증하는 단계는, 공통 회계장부 서명이 프로세싱 플랫폼 개인 키를 사용하여 생성됨을 결정하기 위해 프로세싱 플랫폼 공개 키를 사용하는 단계를 포함한다.

[0581] [0497] 제162 양상에서, 양상 158 내지 양상 161 중 어느 한 양상의 방법은, 공통 회계장부로부터 중앙 회계장부를 생성하는 단계를 더 포함하며, 중앙 회계장부는 지불인 디바이스의 지불인 계정 및 수취인 디바이스의 수취인 계정을 포함하며, 지불인 계정은 지불인 공개 키 및 지불인 계정의 계정 잔액을 포함하며, 수취인 계정은 수취인 공개 키 및 수취인 계정의 계정 잔액을 포함한다.

[0582] [0498] 제163 양상에서, 양상 162의 방법에 있어서, 수취인 디바이스에 지불 금액의 지불을 제공하는 단계는: 지불인 계정이 지불 금액을 지불하기에 충분한 잔액을 가짐을 결정하는 단계; 지불 금액만큼 지불인 계정을 데빗팅하는 단계; 및 지불 금액만큼 수취인 계정을 크레딧팅하는 단계를 포함한다.

[0583] [0499] 제164 양상에서, 양상 163의 방법은, 수취인 디바이스로부터 수취인 계정에서(out of) 돈을 송금하기 위한 요청을 수신하는 단계 - 수취인 계정에서 돈을 송금하기 위한 요청은 출금액 및 출금 방법을 포함하며, 출금 방법은 ACH(automated clearing house) 송금, 유선 송금, 또는 물리적 체크를 전송하는 것을 포함함 -; 출금액만큼 수취인 계정을 데빗팅하는 단계; 및 출금 방법을 사용하여 출금액을 전송하는 단계를 더 포함한다.

[0584] [0500] 제165 양상에서, 양상 164의 방법은, 송금 수수료만큼 수취인 계정을 데빗팅하는 단계를 더 포함하며, 수수료는 출금액에 비례하거나 또는 고정된다.

[0585] [0501] 제166 양상에서, 양상 162 내지 양상 165 중 어느 한 양상의 방법에 있어서, 수취인 디바이스에 지불 금액의 지불을 제공하는 단계는: 지불인 계정이 지불 금액을 지불하기에 불충분한 잔액을 가짐을 결정하는 단계; 불충분한 잔액에 대한 수수료만큼 지불인 계정을 데빗팅하는 단계; 및 지불인 디바이스를 디메리트 리스트에 부가하는 단계를 포함한다.

[0586] [0502] 제167 양상에서, 양상 162 내지 양상 166 중 어느 한 양상의 방법에 있어서, 오리지널 디지털 수표는 소스 계정을 더 포함하며, 수취인 디바이스에 지불 금액의 지불을 제공하는 단계는: 소스 계정으로부터 지불 금액을 수신하는 단계; 및 지불 금액만큼 수취인 계정을 크레딧팅하는 단계를 포함한다.

[0587] [0503] 제168 양상에서, 양상 148 내지 양상 167 중 어느 한 양상의 방법에 있어서, 오리지널 디지털 수표는 수수료 공유 정책을 포함한다.

[0588] [0504] 제169 양상에서, 암호화방식으로 싸인된 디지털 수표들을 안전하게 교환하기 위한 방법은, 하드웨어 프로세서의 제어 하에: 수취인 디바이스로부터 지불 요청을 수신하는 단계; 수취인 디바이스를 식별하는 단계; 오리지널 디지털 수표를 생성하는 단계 - 오리지널 디지털 수표는 지불 금액, 지불인 디바이스의 지불인 공개 키, 수취인 디바이스의 수취인 공개 키, 및 오리지널 디지털 수표의 지불인 서명을 포함하고, 지불인 서명은 지불인 디바이스의 지불인 개인 키를 사용하여 생성되며, 지불인 공개 키 및 지불인 개인 키는 지불인 공개-키 암호 쌍을 형성함 -; 수취인 디바이스에 오리지널 디지털 수표를 전송하는 단계; 및 수취인 디바이스의 표시를 수신하는 단계: 오리지널 디지털 수표를 수신하는 단계; 반드시 그런 것은 아니지만 프로세싱 플랫폼과 통신하면서 지불인 공개 키를 사용하여 오리지널 디지털 수표를 검증하는 단계; 배서된 디지털 수표를 생성하는 단계 -배서된 디지털 수표는 배서된 디지털 수표의 수취인 서명 및 오리지널 디지털 수표를 포함하고, 수취인 서명은 수취인 개인 키를 사용하여 생성되며, 수취인 공개 키 및 수취인 개인 키는 수취인 공개-키 암호 쌍을 형성함-; 배서된 디지털 수표를 프로세싱 플랫폼에 상환하는 단계; 및 프로세싱 플랫폼으로부터 지불 금액의 지불을 수신하는 단계를 포함한다.

[0589] [0505] 제170 양상에서, 양상 169의 방법에 있어서, 지불 요청은 수취인 공개 키 및 요청된 금액을 포함하며, 지불 금액은 요청된 금액과 관련된다.

[0590] [0506] 제171 양상에서, 양상 169 내지 양상 170 중 어느 한 양상의 방법에 있어서, 수취인 디바이스를 식별하는 단계는 파트너 식별을 수행하는 단계를 포함하며, 파트너 식별은 지불 인가, 노킹, 물리적 표시, 빔 형성, 이전 어레인지먼트, 피상적인 유효성 검증, 또는 이들의 임의의 조합을 포함한다.

[0591] [0507] 제172 양상에서, 양상 169 내지 양상 171 중 어느 한 양상의 방법에 있어서, 오리지널 디지털 수표는 수표 식별자를 더 포함한다.

[0592] [0508] 제173 양상에서, 양상 172의 방법에 있어서, 수표 식별자는 단조적으로 증가하는 수이다.

[0593] [0509] 제174 양상에서, 양상 169 내지 양상 173 중 어느 한 양상의 방법에 있어서, 수취인 디바이스에 오리지널 디지털 수표를 전송하는 단계는 중간 디바이스를 통해 또는 직접적으로 단거리 링크를 통해 수취인 디바이스에 오리지널 디지털 수표를 전송하는 단계를 포함한다.

[0594] [0510] 제175 양상에서, 양상 174의 방법에 있어서, 단거리 링크는 피어-투-피어 통신 링크이다.

[0595] [0511] 제176 양상에서, 양상 169 내지 양상 175 중 어느 한 양상의 방법에 있어서, 배서된 디지털 수표는 상환 전용 배서, 질의 배서, 악의적인 수표 배서, 또는 이들의 임의의 조합을 더 포함한다.

[0596] [0512] 제177 양상에서, 양상 169 내지 양상 176 중 어느 한 양상의 방법에 있어서, 오리지널 디지털 수표를 생성하는 단계는 지불인 디바이스에 의해 지불인의 인증 정보를 수신하는 단계를 포함하고, 배서된 디지털 수표를 생성하는 단계는 수취인 디바이스에 의해 수취인의 인증 정보를 수신하는 단계를 포함한다.

[0597] [0513] 제178 양상에서, 양상 169 내지 양상 177 중 어느 한 양상의 방법에 있어서, 오리지널 디지털 수표를 검증하는 단계는 지불인 서명이 지불인 개인 키를 사용하여 생성됨을 결정하기 위해 지불인 공개 키를 사용하는 단계를 포함한다.

[0598] [0514] 제179 양상에서, 양상 169 내지 양상 178 중 어느 한 양상의 방법에 있어서, 지불인 서명은 지불인 개인 키를 사용하여 지불인 디바이스의 보안 엘리먼트에 의해 생성되고, 지불인 개인 키는 지불인 디바이스의 보안 엘리먼트에 저장된다.

[0599] [0515] 제180 양상에서, 양상 169 내지 양상 179 중 어느 한 양상의 방법에 있어서, 수취인 서명은 수취인 개인 키를 사용하여 수취인 디바이스의 보안 엘리먼트에 의해 생성되고, 수취인 개인 키는 수취인 디바이스의 보안 엘리먼트에 저장된다.

[0600] [0516] 제181 양상에서, 양상 169 내지 양상 180 중 어느 한 양상의 방법은 프로세싱 플랫폼으로부터 공통 회계장부를 수신하는 단계를 더 포함하며, 공통 회계장부는 지불인 공개 키 및 수취인 공개 키를 포함한다.

[0601] [0517] 제182 양상에서, 양상 169 내지 양상 180 중 어느 한 양상의 방법은 수취인 디바이스로부터 공통 회계장부를 수신하는 단계를 더 포함하며, 공통 회계장부는 지불인 공개 키 및 수취인 공개 키를 포함한다.

[0602] [0518] 제183 양상에서, 양상 181 내지 양상 182 중 어느 한 양상의 방법에 있어서, 공통 회계장부는 공통 회계장부 서명을 더 포함하며, 공통 회계장부 서명은 프로세싱 플랫폼의 프로세싱 플랫폼 개인 키를 사용하여 생성되며, 방법은, 반드시 그런 것은 아니지만 프로세싱 플랫폼과 통신하면서 프로세싱 플랫폼의 프로세싱 플랫폼 공개 키를 사용하여 공통 회계장부를 검증하는 단계를 더 포함하며, 프로세싱 플랫폼 공개 키 및 프로세싱 플랫폼 개인 키는 프로세싱 플랫폼의 공개-키 암호 쌍을 형성하며, 공통 회계장부를 검증하는 단계는, 공통 회계장부 서명이 프로세싱 플랫폼 개인 키를 사용하여 생성됨을 결정하기 위해 프로세싱 플랫폼 공개 키를 사용하는 단계를 포함한다.

[0603] [0519] 제184 양상에서, 암호화방식으로 싸인된 디지털 수표들을 안전하게 교환하기 위한 방법이 개시된다. 방법은 하드웨어 프로세서의 제어 하에 수행되며, 그리고 지불인 디바이스에 지불 요청을 전송하는 단계; 지불인 디바이스로부터 오리지널 디지털 수표를 수신하는 단계 – 오리지널 디지털 수표는 수취인 디바이스로부터 지불 요청을 수신하고 수취인 디바이스를 식별한 후에 지불인 디바이스에 의해 생성되고, 오리지널 디지털 수표는 지불 금액, 지불인 디바이스의 지불인 공개 키, 수취인 디바이스의 수취인 공개 키, 및 오리지널 디지털 수표의 지불인 서명을 포함하고, 지불인 서명은 지불인 디바이스의 지불인 개인 키를 사용하여 생성되며, 지불인 공개 키 및 수취인 공개 키는 지불인 공개-키 암호 쌍을 형성함–; 반드시 그런 것은 아니지만 프로세싱 플랫폼과 통신하면서 지불인 공개 키를 사용하여 오리지널 디지털 수표를 검증하는 단계; 배서된 디지털 수표를 생성하는 단계 – 배서된 디지털 수표는 배서된 디지털 수표의 수취인 서명 및 오리지널 디지털 수표를 포함하고, 수취인 서명은 수취인 디바이스의 수취인 개인 키를 사용하여 생성되며, 수취인 공개 키 및 수취인 공개 키는 수취인 공개 키 암호 쌍을 형성함 –; 배서된 디지털 수표를 프로세싱 플랫폼에 상환하는 단계; 및 프로세싱 플랫폼으로부터 지불 금액의 지불을 수신하는 단계를 포함한다.

[0604] [0520] 제185 양상에서, 양상 184의 방법에 있어서, 지불 요청은 수취인 공개 키 및 요청된 금액을 포함하며, 지불 금액은 요청된 금액과 관련된다.

[0605] [0521] 제186 양상에서, 양상 184 또는 양상 185의 방법에 있어서, 수취인 디바이스를 식별하는 단계는 파트너 식별을 수행하는 단계를 포함하며, 파트너 식별은 지불 인가, 노킹, 물리적 표시, 빔 형성, 이전 어레인지먼트,

피상적인 유효성 검증, 또는 이들의 임의의 조합을 포함한다.

[0606] [0522] 제187 양상에서, 양상 184 내지 양상 186 중 어느 한 양상의 방법에 있어서, 오리지널 디지털 수표는 수표 식별자를 더 포함한다.

[0607] [0523] 제188 양상에서, 양상 187의 방법에 있어서, 수표 식별자는 단조적으로 증가하는 수이다.

[0608] [0524] 제189 양상에서, 양상 184 내지 양상 188 중 어느 한 양상의 방법에 있어서, 지불인 디바이스로부터 오리지널 디지털 수표를 수신하는 단계는 중간 디바이스를 통해 또는 직접적으로 단거리 링크를 통해 지불인 디바이스로부터 오리지널 디지털 수표를 수신하는 단계를 포함한다.

[0609] [0525] 제190 양상에서, 양상 189의 방법에 있어서, 단거리 링크는 피어-투-피어 통신 링크이다.

[0610] [0526] 제191 양상에서, 양상 184 내지 양상 190 중 어느 한 양상의 방법에 있어서, 배서된 디지털 수표는 상환 전용 배서, 질의 배서, 악의적인 수표 배서, 또는 이들의 임의의 조합을 더 포함한다.

[0611] [0527] 제192 양상에서, 양상 184 내지 양상 191 중 어느 한 양상의 방법에 있어서, 오리지널 디지털 수표를 생성하는 단계는 지불인 디바이스에 의해 지불인 인증 정보를 수신하는 단계를 포함하고, 배서된 디지털 수표를 생성하는 단계는 수취인 디바이스에 의해 수취인 인증 정보를 수신하는 단계를 포함한다.

[0612] [0528] 제193 양상에서, 양상 184 내지 양상 192 중 어느 한 양상의 방법에 있어서, 오리지널 디지털 수표를 검증하는 단계는 지불인 서명이 지불인 개인 키를 사용하여 생성됨을 결정하기 위해 지불인 공개 키를 사용하는 단계를 포함한다.

[0613] [0529] 제194 양상에서, 양상 184 내지 양상 193 중 어느 한 양상의 방법에 있어서, 지불인 서명은 지불인 개인 키를 사용하여 지불인 디바이스의 보안 엘리먼트에 의해 생성되고, 지불인 개인 키는 지불인 디바이스의 보안 엘리먼트에 저장된다.

[0614] [0530] 제195 양상에서, 양상 184 내지 양상 194 중 어느 한 양상의 방법에 있어서, 수취인 서명은 수취인 개인 키를 사용하여 수취인 디바이스의 보안 엘리먼트에 의해 생성되고, 수취인 개인 키는 수취인 디바이스의 보안 엘리먼트에 저장된다.

[0615] [0531] 제196 양상에서, 양상 184 내지 양상 195 중 어느 한 양상의 방법은 프로세싱 플랫폼으로부터 공통 회계장부를 수신하는 단계를 더 포함하며, 공통 회계장부는 지불인 공개 키 및 수취인 공개 키를 포함한다.

[0616] [0532] 제197 양상에서, 양상 196의 방법은 지불인 디바이스에 공통 레코드들을 전송하는 단계를 더 포함한다.

[0617] [0533] 제198 양상에서, 양상 184 내지 양상 195 중 어느 한 양상의 방법은 지불인 디바이스로부터 공통 회계장부를 수신하는 단계를 더 포함하며, 공통 회계장부는 지불인 공개 키 및 수취인 공개 키를 포함한다.

[0618] [0534] 제199 양상에서, 양상 196 내지 양상 198 중 어느 한 양상의 방법에 있어서, 공통 회계장부는 공통 회계장부 서명을 더 포함하며, 공통 회계장부 서명은 프로세싱 플랫폼의 프로세싱 플랫폼 개인 키를 사용하여 생성되며, 방법은, 반드시 그런 것은 아니지만 프로세싱 플랫폼과 통신하면서 프로세싱 플랫폼의 프로세싱 플랫폼 공개 키를 사용하여 공통 회계장부를 검증하는 단계를 더 포함하며, 프로세싱 플랫폼 공개 키 및 프로세싱 플랫폼 개인 키는 프로세싱 플랫폼의 공개-키 암호 쌍을 형성하며, 공통 회계장부를 검증하는 단계는, 공통 회계장부 서명이 프로세싱 플랫폼 개인 키를 사용하여 생성됨을 결정하기 위해 프로세싱 플랫폼 공개 키를 사용하는 단계를 포함한다.

[0619] [0535] 제200 양상에서, 컴퓨터 시스템이 개시된다. 컴퓨터 시스템은: 하드웨어 프로세서; 및 프로세서에 의해 실행될 때, 프로세서로 하여금 양상 148 내지 양상 199 중 어느 한 양상의 방법을 수행하게 하는 명령들이 저장된 비-일시적 메모리를 포함한다.

[0620] [0536] 제201 양상에서, 양상 200의 컴퓨터 시스템에 있어서, 컴퓨터 시스템은 모바일 디바이스이다.

[0621] [0537] 제202 양상에서, 양상 201의 컴퓨터 시스템에 있어서, 모바일 디바이스는 웨어러블 디스플레이 시스템이다.

[0622] *암호화방식으로 싸인된 레코드들의 유효성 검증*

[0623] [0538] 제203 양상에서, 암호화방식으로 싸인된 레코드들의 유효성을 검증하기 위한 방법이 개시된다. 방법은 하드웨어 프로세서의 제어 하에 수행되며, 그리고 레코드 전송자 디바이스로부터 전송자 개별 레코드를 수신하

는 단계 – 전송자 개별 레코드는 레코드 식별자, 레코드 콘텐츠, 전송자 공개 키, 레코드 수신자 디바이스의 수신자 공개 키, 및 전송자 개별 레코드의 전송자 서명을 포함하며, 전송자 개별 레코드는 레코드 수신자 디바이스로부터 콘텐츠 요청을 수신하고 레코드 수신자 디바이스를 식별한 후에 레코드 전송자 디바이스에 의해 생성됨 –; 반드시 그런 것은 아니지만 프로세싱 플랫폼과 통신하면서 전송자 개별 레코드가 무효임을 결정하는 단계; 수신자 개별 레코드를 생성하는 단계 – 수신자 개별 레코드는 전송자 개별 레코드, 악의적인 레코드 배서, 및 수신자 개별 레코드의 수신자 서명을 포함하고, 수신자 서명은 레코드 수신자 디바이스의 수신자 개인 키를 사용하여 생성되며, 수신자 공개 키 및 수신자 개인 키는 수신자 공개-키 암호 쌍을 형성함 –; 및 프로세싱 플랫폼에 수신자 개별 레코드를 전송하는 단계를 포함한다.

[0624] [0539] 제204 양상에서, 양상 203의 방법에 있어서, 전송자 개별 레코드가 무효임을 결정하는 단계는 단일 수신자에 대한 전송자 클로닝을 검출하는 단계, 마우징을 검출하는 단계, 또는 고스팅을 검출하는 단계를 포함한다.

[0625] [0540] 제205 양상에서, 양상 204의 방법에 있어서, 전송자 개별 레코드의 레코드 식별자는 단조적으로 증가하는 수이고, 레코드 수신자 디바이스는 이전에 수신된 개별 레코드들의 전송자 공개 키들로서 레코드 전송자 디바이스의 전송자 공개 키를 갖는 이전에 수신된 개별 레코드들의 가장 높은 레코드 식별자를 유지하며, 전송자 클로닝을 검출하는 단계는 전송자 개별 레코드의 레코드 식별자가 가장 높은 레코드 식별자보다 더 크지 않음을 결정하는 단계를 포함한다.

[0626] [0541] 제206 양상에서, 양상 205의 방법에 있어서, 전송자 개별 레코드의 레코드 식별자는 레코드 전송자 디바이스에 의해 생성된 개별 레코드들에 대해 상이하고, 레코드 수신자 디바이스는 레코드 전송자 디바이스로부터 이전에 수신된 개별 레코드들의 레코드 식별자들을 유지하며, 전송자 클로닝을 검출하는 단계는 레코드 전송자 디바이스로부터 이전에 수신된 모든 개별 레코드들의 레코드 식별자들에 전송자 개별 레코드의 레코드 식별자가 있지 않음을 결정하는 단계를 포함한다.

[0627] [0542] 제207 양상에서, 양상 205 또는 양상 206의 방법에 있어서, 전송자 공개 키는 레코드 전송자 디바이스의 전송자 공개 키이고, 전송자 서명은 레코드 전송자 디바이스의 전송자 개인 키를 사용하여 생성되며, 전송자 공개 키 및 전송자 개인 키는 전송자 공개-키 암호 쌍을 형성한다.

[0628] [0543] 제208 양상에서, 양상 204 내지 양상 207 중 어느 한 양상의 방법에 있어서, 전송자 공개 키는 레코드 전송자 디바이스의 전송자 공개 키이고, 마우징을 검출하는 단계는 전송자 서명이 레코드 전송자 디바이스의 전송자 개인 키를 사용하여 생성되지 않음을 결정하는 단계를 포함하고, 전송자 공개 키 및 전송자 개인 키는 전송자 공개-키 암호 쌍을 형성하며, 전송자 서명이 레코드 전송자 디바이스의 전송자 개인 키를 사용하여 생성되지 않음을 결정하는 단계는 전송자 서명이 전송자 개인 키를 사용하여 생성되지 않음을 결정하기 위해 전송자 공개 키를 사용하는 단계를 포함한다.

[0629] [0544] 제209 양상에서, 양상 204 내지 양상 208 중 어느 한 양상의 방법에 있어서, 고스팅을 검출하는 단계는 전송자 공개 키가 사용자 디바이스의 유효 공개 키가 아님을 결정하는 단계를 포함하고, 전송자 공개 키가 유효 공개 키가 아님을 결정하는 단계는 프로세싱 플랫폼으로부터 공통 레코드들을 수신하는 단계 – 공통 레코드들은 사용자 디바이스들의 유효 공개 키들을 포함함 –; 및 공통 레코드들이 레코드 전송자 디바이스의 전송자 공개 키를 포함함을 결정하는 단계를 포함한다.

[0630] [0545] 제210 양상에서, 양상 209의 방법에 있어서, 전송자 서명은 전송자 개인 키를 사용하여 생성되며, 전송자 공개 키 및 전송자 개인 키는 전송자 공개-키 암호 쌍을 형성한다.

[0631] [0546] 제211 양상에서, 양상 203 내지 양상 210 중 어느 한 양상의 방법은 프로세싱 플랫폼으로 하여금 악의적인 사용자 디바이스들의 블랙리스트에 레코드 전송자 디바이스를 부가하게 하는 단계를 더 포함한다.

[0632] [0547] 제212 양상에서, 암호화방식으로 싸인된 레코드들의 유효성을 검증하기 위한 방법이 개시된다. 방법은 하드웨어 프로세서의 제어 하에 수행되며, 그리고 레코드 전송자 디바이스로부터 전송자 개별 레코드를 수신하는 단계 – 전송자 개별 레코드는 레코드 콘텐츠, 전송자 공개 키, 수신자 공개 키, 및 전송자 개별 레코드의 전송자 서명을 포함하고, 전송자 서명은 전송자 개인 키를 사용하여 생성되고, 전송자 공개 및 및 전송자 개인 키는 전송자 공개-키 암호 쌍을 형성하며, 개별 레코드는 레코드 수신자 디바이스로부터 콘텐츠 요청을 수신하고 레코드 수신자 디바이스를 식별한 후에 레코드 전송자 디바이스에 의해 전송됨 –; 반드시 그런 것은 아니지만 프로세싱 플랫폼과 통신하면서 전송자 개별 레코드가 무효임을 결정하는 단계; 수신자 개별 레코드를 생성하는 단계 – 수신자 개별 레코드는 전송자 개별 레코드, 악의적인 레코드 배서, 및 수신자 개별 레코드의 수신자

서명을 포함하고, 수신자 서명은 레코드 수신자 디바이스의 수신자 개인 키를 사용하여 생성되며, 수신자 공개 키 및 수신자 개인 키는 수신자 공개-키 암호 쌍을 형성함 -; 및 프로세싱 플랫폼에 수신자 개별 레코드를 전송하는 단계를 포함한다.

[0633] [0548] 제213 양상에서, 양상 212의 방법에 있어서, 전송자 개별 레코드가 무효임을 결정하는 단계는 다수의 수신자들에 대한 전송자 클로닝을 검출하는 단계 또는 포킹을 검출하는 단계를 포함한다.

[0634] [0549] 제214 양상에서, 양상 213의 방법에 있어서, 다수의 수신자들에 대한 전송자 클로닝을 검출하는 단계는: 전송자 공개 키가 레코드 전송자 디바이스의 전송자 공개 키임을 결정하는 단계; 및 수신자 공개 키가 레코드 수신자 디바이스의 공개 키가 아님을 결정하는 단계를 포함한다.

[0635] [0550] 제215 양상에서, 양상 213의 방법에 있어서, 포킹을 검출하는 단계는: 전송자 공개 키가 레코드 전송자 디바이스의 공개 키가 아님을 결정하는 단계; 레코드 수신자 디바이스의 공개 키가 전송자 개별 레코드에 있지 않음을 결정하는 단계; 및 수신자 공개 키가 레코드 수신자 디바이스의 공개 키가 아님을 결정하는 단계를 포함한다.

[0636] [0551] 제216 양상에서, 양상 214 또는 양상 215의 방법에 있어서, 전송자 서명은 전송자 개인 키를 사용하여 생성되며, 전송자 공개 키 및 전송자 개인 키는 전송자 공개-키 암호 쌍을 형성한다.

[0637] [0552] 제217 양상에서, 양상 212 내지 양상 216 중 어느 한 양상의 방법은 프로세싱 플랫폼으로 하여금 악의적인 사용자 디바이스들의 블랙리스트에 레코드 전송자 디바이스를 부가하게 하는 단계를 더 포함한다.

[0638] [0553] 제218 양상에서, 암호화방식으로 싸인된 레코드들의 유효성을 검증하기 위한 방법이 개시된다. 방법은 하드웨어 프로세서의 제어 하에 수행되며, 그리고 레코드 수신자 디바이스로부터 수신자 개별 레코드를 수신하는 단계 - 수신자 개별 레코드는 전송자 개별 레코드, 프로세싱만을 위한 배서, 및 수신자 개별 레코드의 수신자 서명을 포함하고, 전송자 개별 레코드는 레코드 콘텐츠, 전송자 공개 키, 레코드 수신자 디바이스의 수신자 공개 키, 및 전송자 개별 레코드의 전송자 서명을 포함하고, 전송자 서명은 전송자 개인 키를 사용하여 생성되고, 전송자 공개 키 및 전송자 개인 키는 전송자 공개-키 암호 쌍을 형성하고, 수신자 개별 레코드는 레코드 전송자 디바이스로부터 전송자 개별 레코드를 수신하고, 반드시 그런 것은 아니지만 프로세싱 플랫폼과 통신하면서, 전송자 공개 키를 사용하여 전송자 개별 레코드를 검증한 후에 레코드 수신자 디바이스에 의해 생성되고, 수신자 서명은 레코드 수신자 디바이스의 수신자 개인 키를 사용하여 생성되며, 수신자 공개 키 및 수신자 개인 키는 수신자 공개-키 암호 쌍을 형성함 -; 수신자 개별 레코드가 무효인 것으로 결정하는 단계; 및 레코드 콘텐츠에 의해 명령된 대로 레코드 수신자 디바이스에 대해 수행하는 것을 거절하는 단계를 포함한다.

[0639] [0554] 제219 양상에서, 양상 218의 방법에 있어서, 수신자 개별 레코드가 무효인 것으로 결정하는 단계는 수신자 클로닝을 검출하는 단계 또는 고스팅을 검출하는 단계를 포함한다.

[0640] [0555] 제220 양상에서, 양상 219의 방법에 있어서, 전송자 개별 레코드는 레코드 식별자를 포함하고, 전송자 공개 키는 레코드 전송자 디바이스의 전송자 공개 키이고, 전송자 개인 키는 레코드 전송자 디바이스의 전송자 개인 키이며, 수신자 클로닝을 검출하는 단계는 수신자 개별 레코드를 수신하기 이전에, 레코드 식별자 및 전송자 공개 키를 포함하는 개별 레코드가 수신되었음을 결정하는 단계를 포함한다.

[0641] [0556] 제221 양상에서, 양상 220의 방법에 있어서, 수신자 개별 레코드를 수신하기 이전에, 레코드 식별자 및 전송자 공개 키를 포함하는 개별 레코드가 수신되었음을 결정하는 단계는: 이전에 수신된 개별 레코드들의 전송자 공개 키들로서 레코드 전송자 디바이스의 전송자 공개 키를 갖는 이전에 수신된 개별 레코드들의 레코드 식별자들을 유지하는 단계; 및 이전에 수신된 개별 레코드들의 전송자 공개 키들로서 레코드 전송자 디바이스의 전송자 공개 키를 갖는 이전에 수신된 개별 레코드들의 레코드 식별자들에 전송자 개별 레코드의 레코드 식별자가 있지 않음을 결정하는 단계를 포함한다.

[0642] [0557] 제222 양상에서, 양상 219 내지 양상 221 중 어느 한 양상의 방법에 있어서, 고스팅을 검출하는 단계는: 전송자 공개 키가 무효 공개 키임을 결정하는 단계를 포함한다.

[0643] [0558] 제223 양상에서, 양상 222의 방법에 있어서, 전송자 공개 키가 무효 공개 키임을 결정하는 단계는: 유효 전송자 공개 키들을 유지하는 단계; 및 유효 전송자 공개 키들이 전송자 개별 레코드의 전송자 공개 키를 포함함을 결정하는 단계를 포함한다.

[0644] [0559] 제224 양상에서, 양상 218 내지 양상 223 중 어느 한 양상의 방법은: 수신자 클로닝이 검출된다면, 악의적인 사용자들의 블랙리스트에 레코드 전송자 디바이스를 부가하는 단계; 및 고스팅이 검출된다면, 악의적인

사용자들의 블랙리스트에 레코드 수신자 디바이스를 부가하는 단계를 더 포함한다.

[0645] [0560] 제225 양상에서, 암호화방식으로 싸인된 레코드들의 유효성을 검증하는 방법이 개시된다. 방법은 하드웨어 프로세서의 제어 하에 수행되며, 그리고 레코드 수신자 디바이스로부터 수신자 개별 레코드를 수신하는 단계 – 수신자 개별 레코드는 전송자 개별 레코드, 배서, 및 수신자 개별 레코드의 수신자 서명을 포함하고, 배서는 악의적인 레코드 배서 또는 프로세싱만을 위한 배서이고, 전송자 개별 레코드는 레코드 콘텐츠, 레코드 전송자 디바이스의 전송자 공개 키, 레코드 수신자 디바이스의 수신자 공개 키, 및 전송자 개별 레코드의 전송자 서명을 포함하고, 전송자 서명은 레코드 전송자 디바이스의 전송자 개인 키를 사용하여 생성되고, 전송자 공개 키 및 전송자 개인 키는 전송자 공개-키 암호 쌍을 형성함 –; 수신자 개별 레코드가 무효임을 결정하는 단계; 및 수신자 개별 레코드가 무효인 원인을 결정하는 단계를 포함한다.

[0646] [0561] 제226 양상에서, 양상 225의 방법에 있어서, 수신자 개별 레코드가 무효인 원인을 결정하는 단계는 부울 분석을 사용하여 수신자 개별 레코드가 무효인 원인을 결정하는 단계를 포함한다.

[0647] [0562] 제227 양상에서, 양상 225의 방법에 있어서, 수신자 개별 레코드가 무효인 원인을 결정하는 단계는 퍼지 규칙을 사용하여 수신자 개별 레코드가 무효인 원인을 결정하는 단계를 포함하며, 그 단계는: 레코드 전송자 디바이스가 임의의 개별 레코드가 무효인 제1 원인이 될 제1 확률을 유지하는 단계; 레코드 수신자 디바이스가 임의의 개별 레코드가 무효인 제2 원인이 될 제2 확률을 유지하는 단계; 제1 확률과 제3 확률을 곱함으로써, 레코드 전송자 디바이스가 임의의 개별 레코드가 무효인 제1 원인이 될 제1 확률을 업데이트하는 단계 – 제3 확률은 레코드 전송자 디바이스 또는 레코드 수신자 디바이스가 수신자 개별 레코드가 무효인 원인이 될 확률임 –; 제2 확률과 제3 확률을 곱함으로써, 레코드 수신자 디바이스가 임의의 개별 레코드가 무효인 제2 원인이 될 제2 확률을 업데이트하는 단계; 및 제1 확률이 제2 확률보다 더 크다면, 레코드 전송자 디바이스인 것으로, 또는 제2 확률이 제1 확률보다 더 크다면, 레코드 수신자 디바이스인 것으로, 수신자 개별 레코드가 무효인 원인을 결정하는 단계를 포함한다.

[0648] [0563] 제228 양상에서, 양상 227의 방법은 악의적인 사용자 디바이스들의 블랙리스트에, 수신자 개별 레코드가 무효인 원인을 부가하는 단계를 더 포함한다.

[0650] *[0564] 제229 양상에서, 컴퓨터 시스템이 개시된다. 컴퓨터 시스템은: 하드웨어 프로세서; 및 프로세서에 의해 실행될 때, 프로세서로 하여금 양상 203 내지 양상 228 중 어느 한 양상의 방법을 수행하게 하는 명령들이 저장된 비-일시적 메모리를 포함한다.

[0651] [0565] 제230 양상에서, 양상 229의 컴퓨터 시스템에 있어서, 컴퓨터 시스템은 모바일 디바이스이다.

[0652] [0566] 제231 양상에서, 양상 230의 컴퓨터 시스템에 있어서, 모바일 디바이스는 웨어러블 디스플레이 시스템이다.

[0653] *암호화방식으로 싸인된 디지털 수표들의 안전한 교환 – 금융 기관(들)*

[0654] [0567] 제232 양상에서, 암호화방식으로 싸인된 디지털 수표들을 안전하게 교환하기 위한 방법이 개시된다. 방법은 하드웨어 프로세서의 제어 하에 수행되며, 그리고 수취인 디바이스로부터 배서된 디지털 수표를 수신하는 단계 – 배서된 디지털 수표는 오리지널 디지털 수표 및 배서된 디지털 수표의 수취인 서명을 포함하며, 오리지널 디지털 수표는 수취인으로부터 지불 요청을 수신하고 그리고 수취인 디바이스를 식별한 후에 지불인에 의해 생성되며, 오리지널 디지털 수표는 지불 금액, 지불인 공개 키, 수취인 공개 키, 및 오리지널 디지털 수표의 지불인 서명을 포함하며, 지불인 서명은 지불인 디바이스의 지불인 개인 키를 사용하여 생성되며, 지불인 공개 키 및 수취인 공개 키는 수취인 공개-키 암호 쌍을 형성하며, 배서된 디지털 수표는 지불인 디바이스로부터 오리지널 디지털 수표를 수신하고 그리고 반드시 그런 것은 아니지만 프로세싱 플랫폼과 통신하면서 지불인 공개 키를 사용하여 오리지널 디지털 수표를 검증한 후에 수취인 디바이스에 의해 생성되며, 수취인 서명은 수취인 디바이스에 의해 수취인 개인 키를 사용하여 생성되며, 수취인 공개 키 및 수취인 공개 키는 수취인 공개 키 암호 쌍을 형성함 –; 배서된 디지털 수표를 검증하는 단계; 및 지불 금액의 지불로 하여금 수취인에게 제공되게 하는 단계를 포함한다.

[0655] [0568] 제233 양상에서, 양상 232의 방법에 있어서, 지불 요청은 수취인 공개 키 및 요청된 금액을 포함하며, 지불 금액은 요청된 금액과 관련된다.

[0656] [0569] 제234 양상에서, 양상 232 또는 양상 233의 방법에 있어서, 수취인 디바이스를 식별하는 단계는 파트너 식별을 수행하는 단계를 포함하며, 파트너 식별은 콘텐츠 인가, 노킹, 물리적 표시, 빔 형성, 이전 어레인지먼

트, 피상적인 유효성 검증, 또는 이들의 임의의 조합을 포함한다.

[0657] [0570] 제235 양상에서, 양상 232 내지 양상 234 중 어느 한 양상의 방법에 있어서, 오리지널 디지털 수표는 수표 식별자를 더 포함한다.

[0658] [0571] 제236 양상에서, 양상 235의 방법에 있어서, 수표 식별자는 단조적으로 증가하는 수이다.

[0659] [0572] 제237 양상에서, 양상 232 내지 양상 236 중 어느 한 양상의 방법에 있어서, 지불인 디바이스로부터 오리지널 디지털 수표를 수신하는 단계는 중간 디바이스를 통해 또는 직접적으로 단거리 링크를 통해 지불인 디바이스로부터 오리지널 디지털 수표를 수신하는 단계를 포함한다.

[0660] [0573] 제238 양상에서, 양상 237의 방법에 있어서, 단거리 링크는 피어-투-피어 통신 링크이다.

[0661] [0574] 제239 양상에서, 양상 232 내지 양상 238 중 어느 한 양상의 방법에 있어서, 배서된 디지털 수표는 예금만을 위한 배서, 질의 배서, 악의적인 수표 배서, 또는 이들의 임의의 조합을 더 포함한다.

[0662] [0575] 제240 양상에서, 양상 232 내지 양상 239 중 어느 한 양상의 방법에 있어서, 오리지널 디지털 수표는 지불인의 인증 정보를 수신한 후에 지불인 디바이스에 의해 생성되며, 배서된 디지털 수표는 수취인의 인증 정보를 수신한 후에 수취인 디바이스에 의해 생성된다.

[0663] [0576] 제241 양상에서, 양상 232 내지 양상 240 중 어느 한 양상의 방법에 있어서, 오리지널 디지털 수표를 검증하는 단계는: 지불인 서명이 지불인 개인 키를 사용하여 생성됨을 결정하기 위해 지불인 공개 키를 사용하는 단계; 및 수취인 서명이 수취인 개인 키를 사용하여 생성됨을 결정하기 위해 수취인 공개 키를 사용하는 단계를 포함한다.

[0664] [0577] 제242 양상에서, 양상 232 내지 양상 241 중 어느 한 양상의 방법은 공통 회계장부를 지불인 디바이스 및 수취인 디바이스에 제공하는 단계를 더 포함하며, 공통 회계장부는 지불인 공개 키 및 수취인 공개 키를 포함한다.

[0665] [0578] 제243 양상에서, 양상 232 내지 양상 241 중 어느 한 양상의 방법은 공통 회계장부를 지불인 디바이스에 제공하는 단계 - 공통 회계장부는 지불인 공개 키 및 수취인 공개 키를 포함함-; 및 지불인 디바이스로 하여금 공통 회계장부를 수취인 디바이스에 제공하게 하는 단계를 더 포함한다.

[0666] [0579] 제244 양상에서, 양상 232 내지 양상 241 중 어느 한 양상의 방법은, 공통 회계장부를 수취인 디바이스에 제공하는 단계 - 공통 회계장부는 지불인 공개 키 및 수취인 공개 키를 포함함-; 및 수취인 디바이스로 하여금 공통 회계장부를 지불인 디바이스에 제공하게 하는 단계를 더 포함한다.

[0667] [0580] 제245 양상에서, 양상 242 내지 양상 244 중 어느 한 양상의 방법에 있어서, 공통 회계장부는 공통 회계장부 서명을 더 포함하며, 공통 회계장부 서명은 프로세싱 플랫폼의 프로세싱 플랫폼 개인 키를 사용하여 생성되며, 방법은, 반드시 그런 것은 아니지만 프로세싱 플랫폼과 통신하면서 프로세싱 플랫폼의 프로세싱 플랫폼 공개 키를 사용하여 공통 회계장부를 검증하는 단계를 더 포함하며, 프로세싱 플랫폼 공개 키 및 프로세싱 플랫폼 개인 키는 프로세싱 플랫폼의 공개-키 암호 쌍을 형성하며, 공통 회계장부를 검증하는 단계는, 공통 회계장부 서명이 프로세싱 플랫폼 개인 키를 사용하여 생성됨을 결정하기 위해 프로세싱 플랫폼 공개 키를 사용하는 단계를 포함한다.

[0668] [0581] 제246 양상에서, 양상 242 내지 양상 245 중 어느 한 양상의 방법은, 공통 회계장부로부터 중앙 회계장부를 생성하는 단계를 더 포함하며, 중앙 회계장부는 지불인 디바이스의 지불인 계정 및 수취인 디바이스의 수취인 계정을 포함하며, 지불인 계정은 지불인 공개 키 및 지불인 계정의 계정 잔액을 포함하며, 수취인 계정은 수취인 공개 키 및 수취인 계정의 계정 잔액을 포함한다.

[0669] [0582] 제247 양상에서, 양상 246의 방법에 있어서, 지불 금액의 지불로 하여금 수취인에게 제공되게 하는 단계는: 지불인 계정이 지불 금액을 지불하기에 충분한 잔액을 가짐이 결정되게 하는 단계; 지불인 계정으로 하여금 지불 금액만큼 데빗팅되게 하는 단계; 및 수취인 계정으로 하여금 지불 금액만큼 크레딧팅되게 하는 단계를 포함한다.

[0670] [0583] 제248 양상에서, 양상 247의 방법에 있어서, 지불인 계정으로 하여금 지불 금액만큼 데빗팅되게 하는 단계는 지불 금액만큼 지불인 계정을 데빗팅하도록 제1 금융 기관에 명령하는 단계를 포함하며, 수취인 계정으로 하여금 지불 금액만큼 크레딧팅되게 하는 단계는 지불 금액만큼 지불인 계정을 데빗팅하도록 제1 금융 기관에 명령하는 단계를 포함한다.

[0671] [0584] 제249 양상에서, 양상 247의 방법에 있어서, 지불인 계정으로 하여금 지불 금액만큼 데빗팅되게 하는 단계는 지불 금액만큼 지불인 계정을 데빗팅하도록 제1 금융 기관에 명령하는 단계를 포함하며, 수취인 계정으로 하여금 지불 금액만큼 크레딧팅되게 하는 단계는 지불 금액만큼 지불인 계정을 데빗팅하도록 제2 금융 기관에 명령하는 단계를 포함한다.

[0672] [0585] 제250 양상에서, 양상 247 내지 양상 249 중 어느 한 양상의 방법은, 수취인 디바이스로부터 수취인 계정에서 돈을 출금하기 위한 요청을 수신하는 단계 - 수취인 계정에서 돈을 출금하기 위한 요청은 출금액 및 출금 방법을 포함하며, 출금 방법은 ACH(automated clearing house) 송금, 유선 송금, 또는 물리적 체크를 전송하는 것을 포함함 -; 수취인 계정으로 하여금 출금액만큼 데빗팅되게 하는 단계; 및 출금 방법을 사용하여 출금액으로 하여금 전송되게 하는 단계를 더 포함한다.

[0673] [0586] 제251 양상에서, 양상 250의 방법은, 수취인 계정으로 하여금 송금 수수료만큼 데빗팅되게 하는 단계를 더 포함하며, 수수료는 출금액에 비례하거나 또는 고정된다.

[0674] [0587] 제252 양상에서, 양상 251의 방법은, 수취인 디바이스로부터 수취인 계정에서 돈을 입금하기 위한 요청을 수신하는 단계 - 수취인 계정에서 돈을 입금하기 위한 요청은 입금액 및 입금 방법을 포함하며, 입금 방법은 ACH(automated clearing house) 송금, 유선 송금, 또는 물리적 체크를 전송하는 것을 포함함 -; 수취인 계정으로 하여금 입금액만큼 데빗팅되게 하는 단계; 및 입금 방법을 사용하여 입금액으로 하여금 전송되게 하는 단계를 더 포함한다.

[0675] [0588] 제253 양상에서, 양상 252의 방법은, 수취인 계정으로 하여금 송금 수수료만큼 데빗팅되게 하는 단계를 더 포함하며, 수수료는 입금액에 비례하거나 또는 고정된다.

[0676] [0589] 제254 양상에서, 양상 246 내지 양상 253 중 어느 한 양상의 방법에 있어서, 지불 금액의 지불로 하여금 수취인에게 제공되게 하는 단계는: 지불인 계정이 지불 금액을 지불하기에 불충분한 잔액을 가짐이 결정되게 하는 단계; 지불인 계정으로 하여금 불충분한 잔액에 대한 수수료만큼 데빗팅되게 하는 단계; 및 지불인 디바이스를 디메리트 리스트에 부가하는 단계를 포함한다.

[0677] [0590] 제255 양상에서, 양상 246 내지 양상 254 중 어느 한 양상의 방법에 있어서, 오리지널 디지털 수표는 소스 계정을 더 포함하며, 지불 금액의 지불로 하여금 수취인에게 제공되게 하는 단계는: 지불 금액으로 하여금 소스 계정으로부터 수신되게 하는 단계; 및 수취인 계정으로 하여금 지불 금액만큼 크레딧팅되게 하는 단계를 더 포함한다.

[0678] [0591] 제256 양상에서, 양상 232 내지 양상 255 중 어느 한 양상의 방법에 있어서, 오리지널 디지털 수표는 수수료 공유 정책을 포함한다.

[0679] [0592] 제257 양상에서, 양상 232 내지 양상 256 중 어느 한 양상의 방법에 있어서, 오리지널 디지털 수표는 거래 타입을 포함한다.

[0680] [0593] 제258 양상에서, 양상 257의 방법에 있어서, 거래 타입은 체크-타입 거래, 데빗-타입 거래, 신용 카드-타입 거래, ACH-타입 거래, 또는 이들의 조합을 포함한다.

[0681] *시스템들 및 디바이스들*

[0682] [0594] 제259 양상에서, 시스템이 개시된다. 시스템은, 실행가능한 명령들을 저장하는 비일시적 컴퓨터-판독가능한 메모리; 및 제1 양상 내지 제259 양상 중 어느 한 양상의 방법을 수행하도록, 실행가능한 명령들에 의해 프로그래밍된 하나 이상의 하드웨어 프로세서들을 포함한다.

[0683] [0595] 제260 양상에서, 웨어러블 디스플레이 시스템이 개시된다. 웨어러블 디스플레이 시스템은, 디스플레이; 실행가능한 명령들을 저장하는 비일시적 컴퓨터-판독가능한 저장 매체; 및 제1 양상 내지 제259 양상 중 어느 한 양상의 방법을 수행하도록, 실행가능한 명령들에 의해 프로그래밍된 하나 이상의 하드웨어 프로세서들을 포함한다.

[0684] 결론

[0685] [0596] 본원에서 설명되고 그리고/또는 첨부된 도면들에 도시된 프로세스들, 방법들 및 알고리즘들 각각은, 하나 이상의 물리적 컴퓨팅 시스템들, 하드웨어 컴퓨터 프로세서들, 주문형 회로, 및/또는 특수 및 특정 컴퓨터 명령들을 실행하도록 구성된 전자 하드웨어에 의해 실행되는 코드 모듈들로 구현되며, 전체적으로 또는 부분적으로 이 코드 모듈들에 의해 자동화될 수 있다. 예컨대, 컴퓨팅 시스템들은 특정 컴퓨터 명령들로 프로그래밍

된 범용 컴퓨터들(예컨대, 서버들) 또는 특수 목적 컴퓨터들, 특수 목적 회로 등을 포함할 수 있다. 코드 모듈은 실행가능한 프로그램으로 컴파일링되고 링크되거나, 동적 링크 라이브러리에 설치되거나, 또는 해석형 프로그래밍 언어로 작성될 수 있다. 일부 구현들에서, 특정 동작들 및 방법들은 정해진 기능에 특정한 회로에 의해 수행될 수 있다.

[0686] [0597] 더욱이, 본 개시내용의 기능성의 특정 구현들은 충분히 수학적으로, 계산적으로 또는 기술적으로 복잡하여, (적절히 전문화된 실행가능한 명령들을 활용하는) 주문형 하드웨어 또는 하나 이상의 물리적 컴퓨팅 디바이스들이 예컨대, 실질적으로 실시간으로 결과들을 제공하기 위하여 또는 수반되는 계산들의 양 또는 복잡성으로 인해 그 기능성을 수행할 필요가 있을 수 있다. 예컨대, 비디오는 많은 프레임들—각각의 프레임은 수백만 개의 픽셀들을 가짐—을 포함할 수 있으며, 상업적으로 적정한 시간량에서 원하는 이미지 프로세싱 태스크 또는 애플리케이션을 제공하기 위해, 특수하게 프로그래밍된 컴퓨터 하드웨어가 비디오 데이터를 프로세싱할 필요가 있다. 더욱이, 서비스 제공자(104)의 프로세싱 플랫폼(124)은 수천 또는 수백만 개의 사용자 디바이스들(116a, 116b)과 전자 통신할 수 있으며, 사용자 디바이스들(116a, 116b)이 프로세싱 플랫폼(124)과 전자 통신할 때 또는 다수의 경우들에서 실질적으로 실시간으로 수십만, 수백만 또는 수억만 개의 암호화방식으로 싸인된 레코드들의 교환을 다루도록 구성될 수 있다.

[0687] [0598] 코드 모듈들 또는 임의의 타입의 데이터는 임의의 타입의 비일시적 컴퓨터-판독가능한 매체, 이를테면 하드 드라이브들, 고체 상태 메모리, RAM(random access memory), ROM(read only memory), 광학 디스크, 휘발성 또는 비휘발성 스토리지, 이들의 조합들 등을 포함하는 물리적 컴퓨터 스토리지 상에 저장될 수 있다. 방법들 및 모듈들(또는 데이터)은 또한, 생성된 데이터 신호들로서(예컨대, 반송파 또는 다른 아날로그 또는 디지털 전파 신호의 일부로서) 무선 기반 및 유선/케이블 기반 매체들을 포함하는 다양한 컴퓨터-판독가능한 송신 매체들 상에서 송신될 수 있고, 그리고 (예컨대, 단일 또는 멀티플렉싱된 아날로그 신호의 일부로서, 또는 다수의 이산 디지털 패킷들 또는 프레임들로서) 다양한 형태들을 취할 수 있다. 개시된 프로세스들 또는 프로세스 단계들의 결과들은 임의의 타입의 비일시적, 유형의 컴퓨터 스토리지에 영구적으로 또는 다른 방식으로 저장될 수 있거나, 또는 컴퓨터-판독가능한 송신 매체를 통해 통신될 수 있다.

[0688] [0599] 본원에 설명되고 그리고/또는 첨부된 도면들에 도시된 흐름도들에서의 임의의 프로세스들, 블록들, 상태들, 단계들, 또는 기능성들은, 프로세스의 단계들 또는 (예컨대, 논리적 또는 산술적) 특정 기능들을 구현하기 위한 하나 이상의 실행가능한 명령들을 포함하는 코드 모듈들, 세그먼트들 또는 코드의 부분들을 잠재적으로 나타내는 것으로 이해되어야 한다. 다양한 프로세스들, 블록들, 상태들, 단계들 또는 기능성들은 본원에 제공된 예시적인 예들에서 조합되거나, 재배열되거나, 이들에 부가되거나, 이들로부터 삭제되거나, 수정되거나 다르게 변경될 수 있다. 일부 실시예들에서, 부가적인 또는 상이한 컴퓨팅 시스템들 또는 코드 모듈들은 본원에 설명된 기능성들 중 일부 또는 모두를 수행할 수 있다. 본원에 설명된 방법들 및 프로세스들은 또한 임의의 특정 시퀀스로 제한되지 않고, 이에 관련된 블록들, 단계들 또는 상태들은 적절한 다른 시퀀스들로, 예컨대 직렬로, 병렬로, 또는 일부 다른 방식으로 수행될 수 있다. 태스크들 또는 이벤트들은 개시된 예시적인 실시예들에 부가되거나 이들로부터 제거될 수 있다. 게다가, 본원에 설명된 구현들에서 다양한 시스템 컴포넌트들의 분리는 예시 목적들을 위한 것이며 모든 구현들에서 그러한 분리를 요구하는 것으로 이해되지 않아야 한다. 설명된 프로그램 컴포넌트들, 방법들 및 시스템들이 일반적으로, 단일 컴퓨터 제품으로 함께 통합되거나 다수의 컴퓨터 제품들로 패키징될 수 있다는 것이 이해되어야 한다. 많은 구현 변형들이 가능하다.

[0689] [0600] 프로세스들, 방법들 및 시스템들은 네트워크(또는 분산형) 컴퓨팅 환경에서 구현될 수 있다. 네트워크 환경들은 전사적 컴퓨터 네트워크들, 인트라넷들, LAN(local area network)들, WAN(wide area network)들, PAN(personal area network)들, 클라우드 컴퓨팅 네트워크들, 크라우드-소스드(crowd-sourced) 컴퓨팅 네트워크들, 인터넷, 클라우드-기반 네트워크(cloud-based network)들 및 월드 와이드 웹(World Wide Web)을 포함한다. 네트워크는 유선 또는 무선 네트워크, 위성 또는 밸룬-기반(balloon-based) 네트워크, 또는 임의의 다른 타입의 통신 네트워크일 수 있다.

[0690] [0601] 본 개시내용의 시스템들 및 방법들 각각은 몇몇 혁신적인 양상들을 가지며, 이 양상들 중 어떤 단일의 양상도 본원에 개시된 바람직한 속성들을 전적으로 담당하거나 이를 위해 요구되지 않는다. 위에서 설명된 다양한 특징들 및 프로세스들은 서로 독립적으로 사용될 수 있거나, 또는 다양한 방식들로 조합될 수 있다. 모든 가능한 조합들 및 서브조합들은 본 개시내용의 범위 내에 속하도록 의도된다. 본 개시내용에 설명된 구현들에 대한 다양한 수정들은 당업자들에게 자명할 수 있고, 그리고 본원에 정의된 일반적인 원리들은 본 개시내용의 사상 또는 범위를 벗어나지 않고 다른 구현들에 적용될 수 있다. 따라서, 청구항들은 본원에 도시된 구현들로 제한되는 것으로 의도되는 것이 아니라, 본원에 개시된 본 개시내용, 원리들 및 신규한 특징들과 일치하는 가장

넓은 범위에 부합될 것이다.

[0691] [0602] 별개의 구현들의 맥락에서 본 명세서에 설명된 특정 특징들은 또한 단일 구현으로 결합하여 구현될 수 있다. 반대로, 단일 구현의 맥락에서 설명된 다양한 특징들은 또한 별도로 다수의 구현들로 또는 임의의 적절한 서브조합으로 구현될 수 있다. 게다가, 비록 특징들이 특정 결합들로 동작하는 것으로서 위에서 설명될 수 있고 심지어 그와 같이 처음에 청구될 수 있지만, 청구된 조합으로부터의 하나 이상의 특징들은 일부 경우들에서 조합으로부터 제거될 수 있고, 그리고 청구된 조합은 서브조합 또는 서브조합의 변형에 관련될 수 있다. 단일 특징 또는 특징들의 그룹이 각각의 그리고 모든 각각의 실시예에 필요하거나 필수적인 것은 아니다.

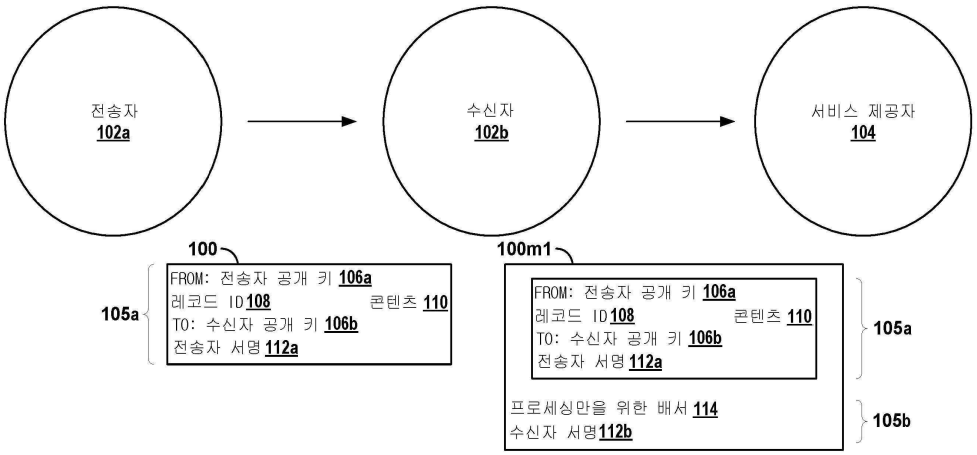
[0692] [0603] 특정하게 다르게 언급되지 않거나, 사용된 맥락 내에서 다르게 이해되지 않으면, 본원에 사용된 조건어, 이를테면 특히, "할 수 있다(can, could, might, may)", "예컨대" 등은 일반적으로, 특정 실시예들이 특정 특징들, 엘리먼트들 및/또는 단계들을 포함하지만, 다른 실시예들은 이들을 포함하지 않는 것을 전달하기 위해 의도된다. 따라서, 그런 조건어는 일반적으로, 특징들, 엘리먼트들 및/또는 단계들이 하나 이상의 실시예들을 위해 어떤 식으로든 요구된다는 것을 또는 하나 이상의 실시예들이, 저자(author) 입력 또는 프롬프팅으로 또는 이들 없이, 이들 특징들, 엘리먼트들 및/또는 단계들이 임의의 특정 실시예에 포함되는지 또는 임의의 특정 실시예에서 수행될지를 판정하기 위한 로직을 반드시 포함하는 것을 의미하도록 의도되지 않는다. "포함하는(comprising)", "포함하는(including)", "가지는(having)" 등의 용어들은 동의어이고 오픈-엔디드(open-ended) 방식으로 포괄적으로 사용되고, 그리고 부가적인 엘리먼트들, 특징들, 작용들, 동작들 등을 배제하지 않는다. 또한, "또는"이란 용어는 그의 포괄적인 의미(및 그의 배타적 의미가 아님)로 사용되어, 예컨대 리스트의 엘리먼트들을 연결하기 위해 사용될 때, "또는"이란 용어는 리스트 내 엘리먼트들 중 하나, 일부 또는 모두를 의미한다. 게다가, 본 출원 및 첨부된 청구항들에 사용된 단수 표현들은 다르게 특정되지 않으면 "하나 이상" 또는 "적어도 하나"를 의미하는 것으로 이해될 것이다.

[0693] [0604] 본원에 사용된 바와 같이, 아이템들의 리스트 중 "적어도 하나"를 지칭하는 어구는 단일 부재들을 포함하여, 이들 아이템들의 임의의 조합을 지칭한다. 예로서, "A, B 또는 C 중 적어도 하나"는, A, B, C, A 및 B, A 및 C, B 및 C, 그리고 A, B 및 C를 커버하도록 의도된다. 특정하게 다르게 언급되지 않으면, "X, Y 및 Z 중 적어도 하나"라는 어구와 같은 접속어는, 아이템, 용어 등이 X, Y 또는 Z 중 적어도 하나 일 수 있다는 것을 전달하기 위해 일반적으로 사용되는 맥락으로 달리 이해된다. 따라서, 그런 접속어는 일반적으로, 특정 실시예들이 X 중 적어도 하나, Y 중 적어도 하나 및 Z 중 적어도 하나가 각각 존재할 것을 요구하는 것을 의미하도록 의도되지 않는다.

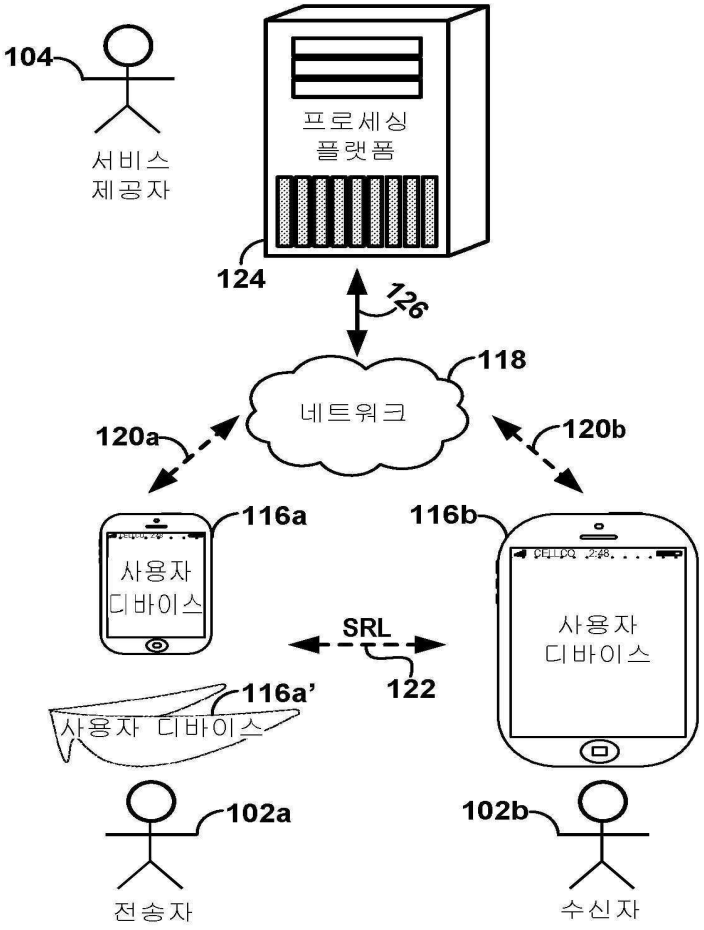
[0694] [0605] 유사하게, 동작들이 특정 순서로 도면들에 도시될 수 있지만, 원하는 결과들을 달성하기 위해, 그런 동작들이 도시된 특정 순서로 또는 순차적 순서로 수행되거나, 또는 모든 예시된 동작들이 수행될 필요가 없다는 것이 인식될 것이다. 추가로, 도면들은 흐름도 형태로 하나 이상의 예시적 프로세스들을 개략적으로 도시할 수 있다. 그러나, 도시되지 않은 다른 동작들이 개략적으로 예시된 예시적인 방법들 및 프로세스들에 통합될 수 있다. 예컨대, 하나 이상의 부가적인 동작들은 예시된 동작들 중 임의의 동작 이전에, 이후에, 동시에, 또는 중간에 수행될 수 있다. 부가적으로, 동작들은 다른 구현들에서 재배열되거나 재정렬될 수 있다. 특정 상황들에서, 멀티태스킹 및 병렬 프로세싱이 유리할 수 있다. 게다가, 위에서 설명된 구현들에서 다양한 시스템 컴포넌트들의 분리는 모든 구현들에서 그런 분리를 요구하는 것으로 이해되지 않아야 하고, 그리고 설명된 프로그램 컴포넌트들 및 시스템들이 일반적으로 단일 소프트웨어 제품으로 함께 통합될 수 있거나 다수의 소프트웨어 제품들로 패키징될 수 있다는 것이 이해되어야 한다. 부가적으로, 다른 구현들은 하기의 청구항들의 범위 내에 있다. 일부 경우들에서, 청구항들에 열거된 액션들은 상이한 순서로 수행될 수 있고 그럼에도 불구하고 원하는 결과들을 달성할 수 있다. 이로써, 하기의 청구항들은 본 개시내용의 부가적인 양상들로서 본 상세한 설명부에 참조로 명시적으로 통합된다.

도면

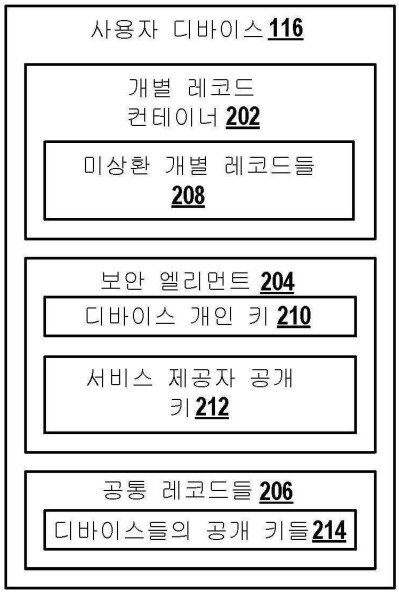
도면1a


전송자
102a
수신자
102b
서비스 제공자
104
100
FROM: 전송자 공개 키 106a
레코드 ID 108
콘텐츠 110
TO: 수신자 공개 키 106b
전송자 서명 112a
105a
100m1
FROM: 전송자 공개 키 106a
레코드 ID 108
콘텐츠 110
TO: 수신자 공개 키 106b
전송자 서명 112a
105a
프로세싱만을 위한 배서 114
수신자 서명 112b
105b

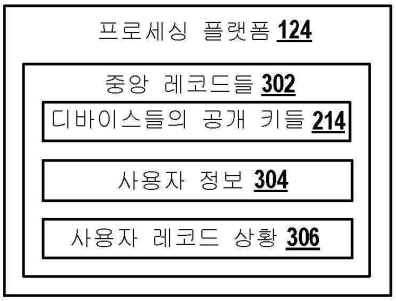
도면1b


104
서비스 제공자
프로세싱 플랫폼
124
126
118
네트워크
120a
120b
116a
116b
사용자 디바이스
SRL
122
116a'
사용자 디바이스
사용자 디바이스
102a
102b
전송자
수신자

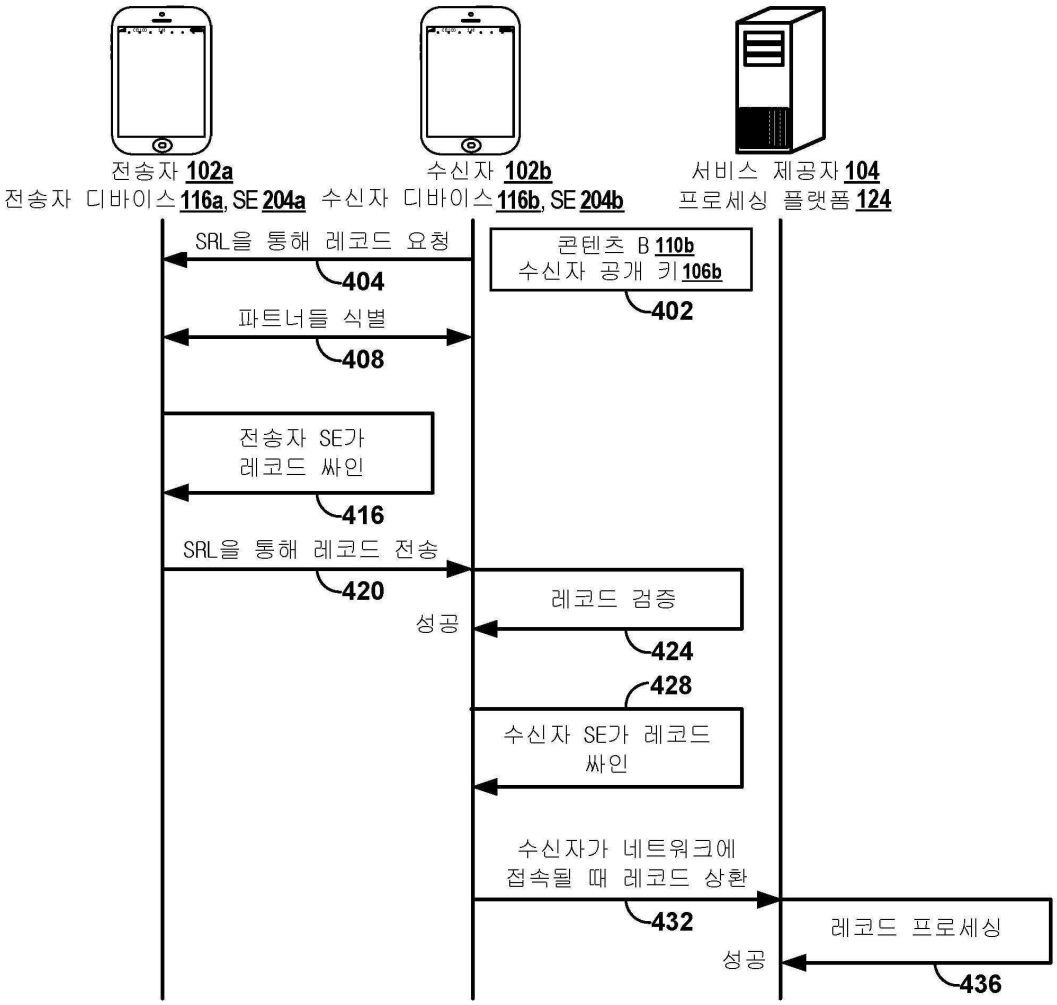
도면2


사용자 디바이스 116
개별 레코드 컨테이너 202
미상환 개별 레코드들 208
보안 엘리먼트 204
디바이스 개인 키 210
서비스 제공자 공개 키 212
공통 레코드들 206
디바이스들의 공개 키들 214

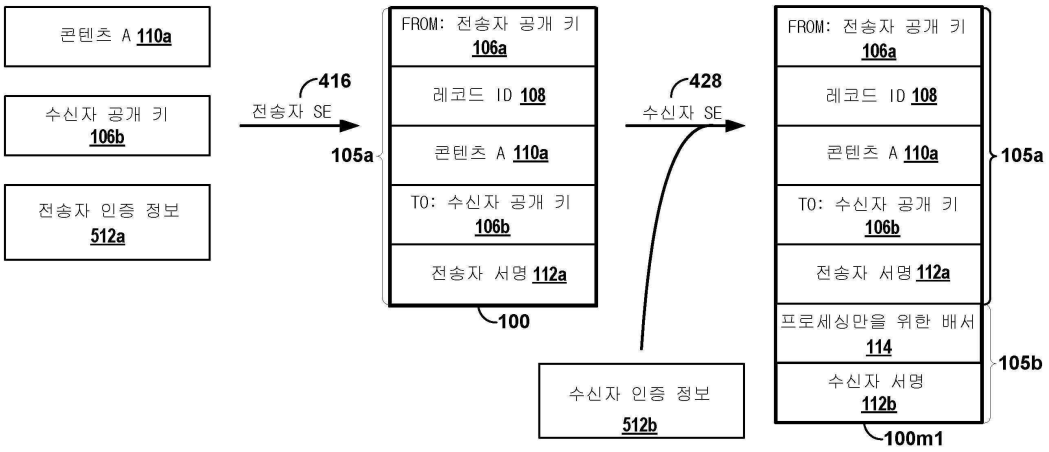
도면3


프로세싱 플랫폼 124
중앙 레코드들 302
디바이스들의 공개 키들 214
사용자 정보 304
사용자 레코드 상황 306

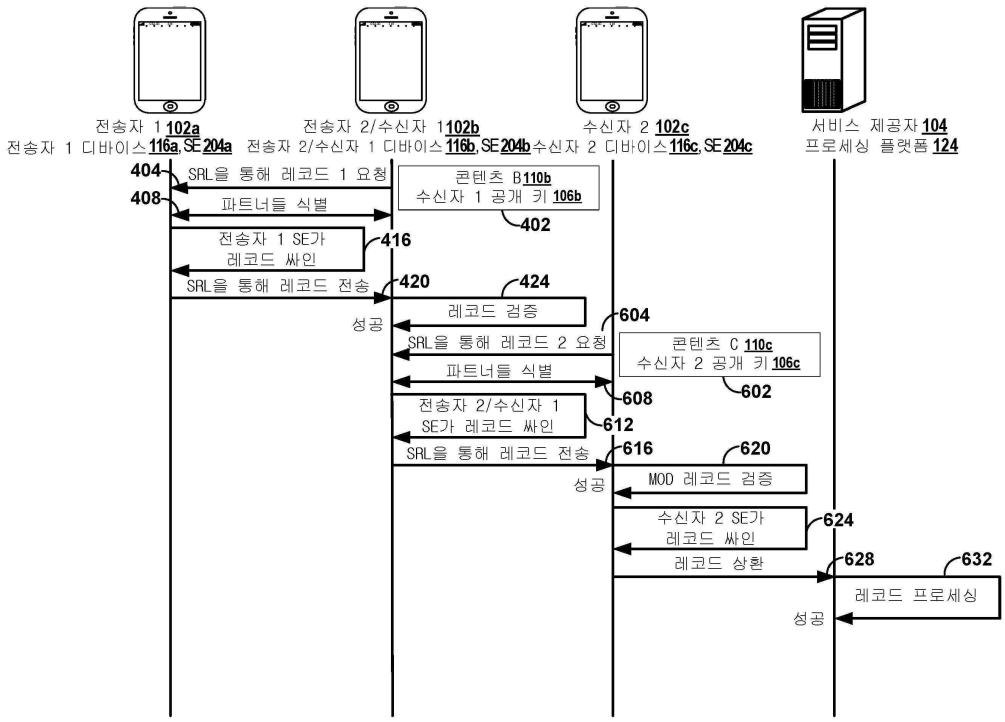
도면4


전송자 102a
전송자 디바이스 116a, SE 204a
수신자 102b
수신자 디바이스 116b, SE 204b
서비스 제공자 104
프로세싱 플랫폼 124
SRL을 통해 레코드 요청
404
콘텐츠 B 110b
수신자 공개 키 106b
402
파트너들 식별
408
전송자 SE가
레코드 싸인
416
SRL을 통해 레코드 전송
420
성공
레코드 검증
424
428
수신자 SE가 레코드
싸인
수신자가 네트워크에
접속될 때 레코드 상환
432
성공
레코드 프로세싱
436

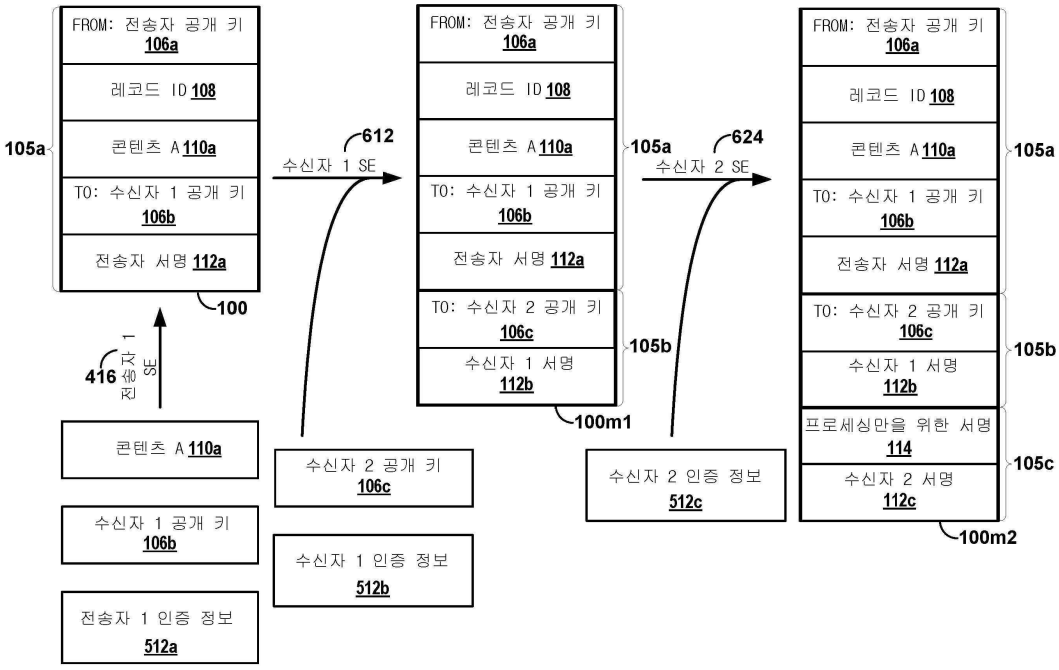
도면5


콘텐츠 A 110a
수신자 공개 키
106b
전송자 인증 정보
512a
416
전송자 SE
105a
FROM: 전송자 공개 키
106a
레코드 ID 108
콘텐츠 A 110a
TO: 수신자 공개 키
106b
전송자 서명 112a
100
428
수신자 SE
수신자 인증 정보
512b
FROM: 전송자 공개 키
106a
레코드 ID 108
콘텐츠 A 110a
TO: 수신자 공개 키
106b
전송자 서명 112a
105a
프로세싱만을 위한 배서
114
수신자 서명
112b
105b
100m1

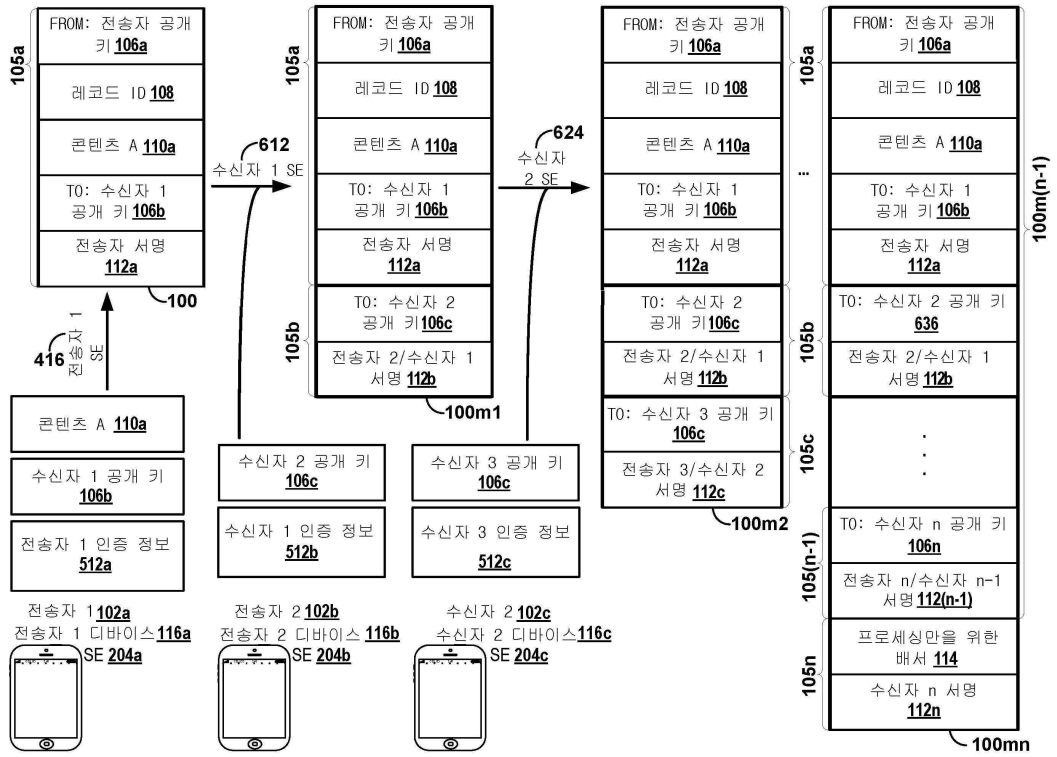
도면6


전송자 1 102a
전송자 1 디바이스 116a, SE 204a
전송자 2/수신자 1 102b
전송자 2/수신자 1 디바이스 116b, SE 204b
수신자 2 102c
수신자 2 디바이스 116c, SE 204c
서비스 제공자 104
프로세싱 플랫폼 124
404
SRL을 통해 레코드 1 요청
콘텐츠 B 110b
수신자 1 공개 키 106b
408
파트너들 식별
402
전송자 1 SE가 레코드 싸인
416
SRL을 통해 레코드 전송
420
424
레코드 검증
성공
604
SRL을 통해 레코드 2 요청
콘텐츠 C 110c
수신자 2 공개 키 106c
602
파트너들 식별
608
전송자 2/수신자 1 SE가 레코드 싸인
612
SRL을 통해 레코드 전송
616
620
MOD 레코드 검증
성공
수신자 2 SE가 레코드 싸인
624
레코드 상환
628
632
레코드 프로세싱
성공

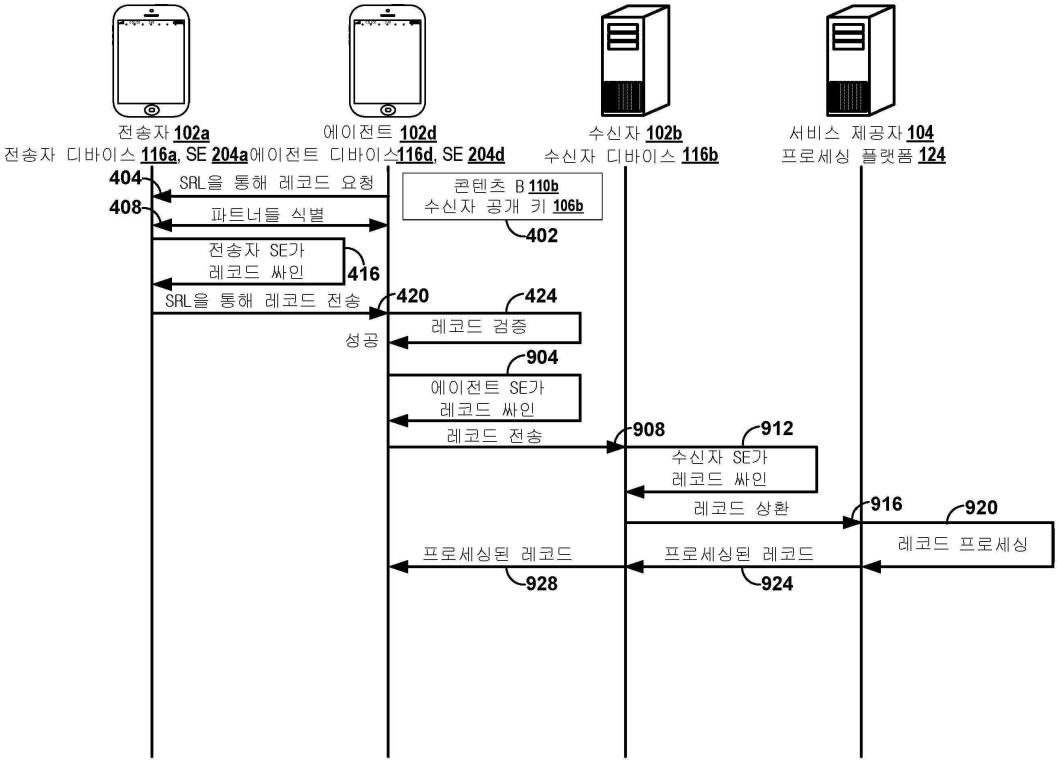
도면7


FROM: 전송자 공개 키 106a
레코드 ID 108
콘텐츠 A 110a
TO: 수신자 1 공개 키 106b
전송자 서명 112a
105a
100
612
수신자 1 SE
416
전송자 1 SE
콘텐츠 A 110a
수신자 1 공개 키 106b
전송자 1 인증 정보 512a
수신자 2 공개 키 106c
수신자 1 인증 정보 512b
FROM: 전송자 공개 키 106a
레코드 ID 108
콘텐츠 A 110a
TO: 수신자 1 공개 키 106b
전송자 서명 112a
TO: 수신자 2 공개 키 106c
수신자 1 서명 112b
105b
100m1
624
수신자 2 SE
수신자 2 인증 정보 512c
FROM: 전송자 공개 키 106a
레코드 ID 108
콘텐츠 A 110a
TO: 수신자 1 공개 키 106b
전송자 서명 112a
TO: 수신자 2 공개 키 106c
수신자 1 서명 112b
프로세싱만을 위한 서명 114
수신자 2 서명 112c
105c
100m2

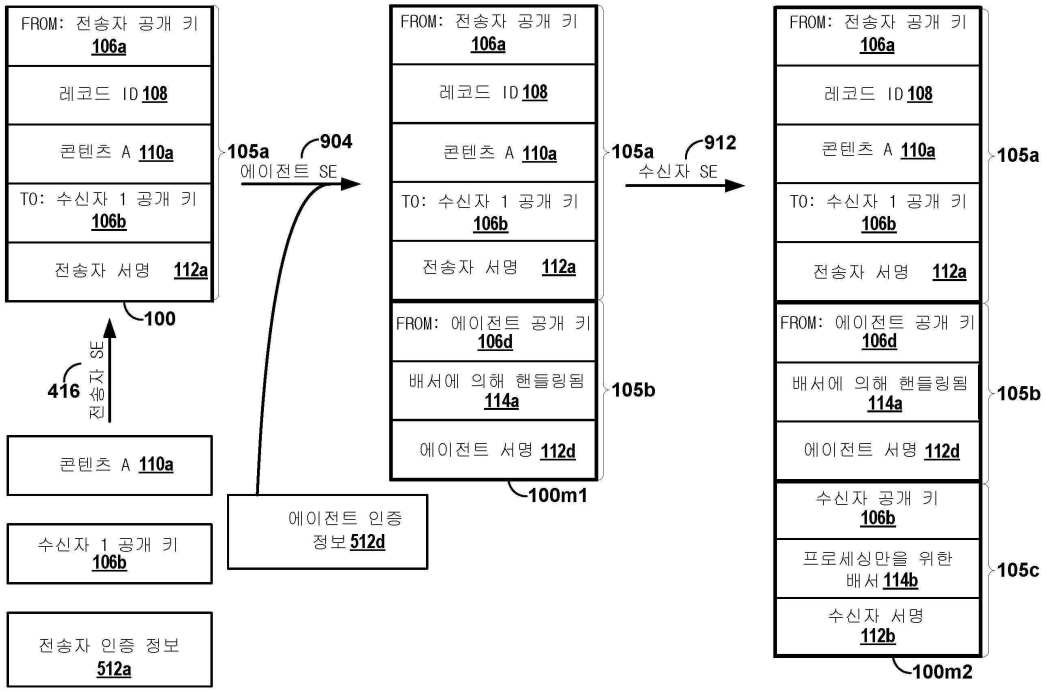
도면8


FROM: 전송자 공개 키 106a
레코드 ID 108
콘텐츠 A 110a
TO: 수신자 1 공개 키 106b
전송자 서명 112a
100
105a
105b
105c
105(n-1)
105n
612
수신자 1 SE
624
수신자 2 SE
416
전송자 1 SE
TO: 수신자 2 공개 키 106c
전송자 2/수신자 1 서명 112b
100m1
TO: 수신자 3 공개 키 106c
전송자 3/수신자 2 서명 112c
100m2
TO: 수신자 2 공개 키 636
TO: 수신자 n 공개 키 106n
전송자 n/수신자 n-1 서명 112(n-1)
프로세싱만을 위한 배서 114
수신자 n 서명 112n
100mn
100m(n-1)
콘텐츠 A 110a
수신자 1 공개 키 106b
전송자 1 인증 정보 512a
수신자 2 공개 키 106c
수신자 1 인증 정보 512b
수신자 3 공개 키 106c
수신자 3 인증 정보 512c
전송자 1 102a
전송자 1 디바이스 116a
SE 204a
전송자 2 102b
전송자 2 디바이스 116b
SE 204b
수신자 2 102c
수신자 2 디바이스 116c
SE 204c

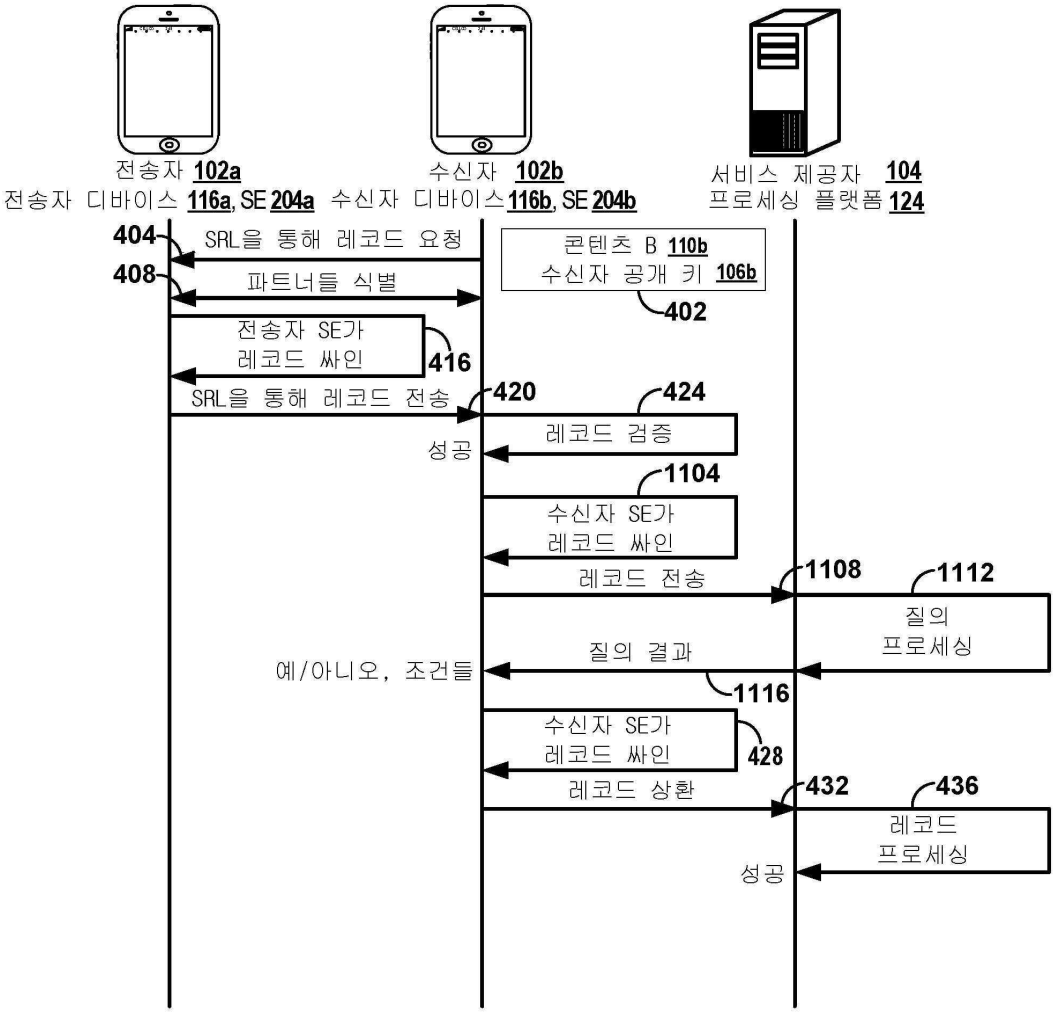
도면9


전송자 102a
전송자 디바이스 116a, SE 204a
에이전트 102d
에이전트 디바이스 116d, SE 204d
수신자 102b
수신자 디바이스 116b
서비스 제공자 104
프로세싱 플랫폼 124
404
SRL을 통해 레코드 요청
408
파트너들 식별
콘텐츠 B 110b
수신자 공개 키 106b
402
전송자 SE가 레코드 싸인
416
SRL을 통해 레코드 전송
420
424
레코드 검증
성공
904
에이전트 SE가 레코드 싸인
레코드 전송
908
912
수신자 SE가 레코드 싸인
레코드 상환
916
920
레코드 프로세싱
프로세싱된 레코드
928
프로세싱된 레코드
924

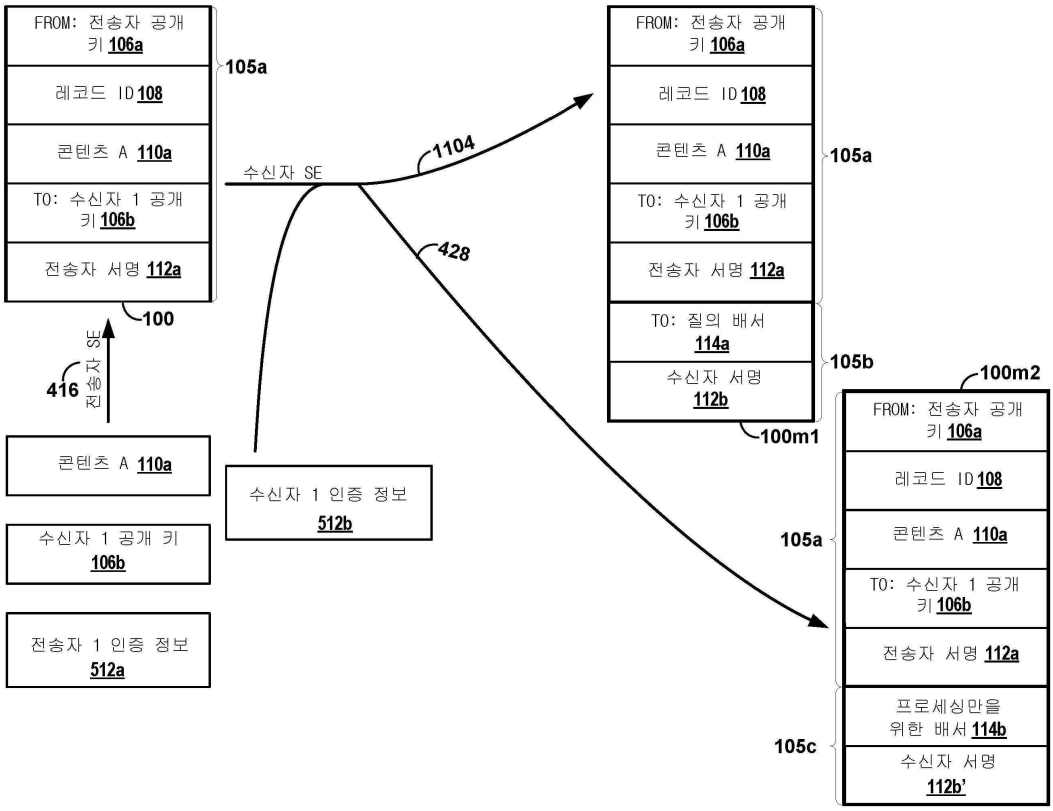
도면10


FROM: 전송자 공개 키 106a
레코드 ID 108
콘텐츠 A 110a
TO: 수신자 1 공개 키 106b
전송자 서명 112a
100
105a
904
에이전트 SE
416
전송
SE
콘텐츠 A 110a
수신자 1 공개 키 106b
전송자 인증 정보 512a
에이전트 인증 정보 512d
FROM: 전송자 공개 키 106a
레코드 ID 108
콘텐츠 A 110a
TO: 수신자 1 공개 키 106b
전송자 서명 112a
FROM: 에이전트 공개 키 106d
배서에 의해 핸들링됨 114a
에이전트 서명 112d
100m1
105b
912
수신자 SE
FROM: 전송자 공개 키 106a
레코드 ID 108
콘텐츠 A 110a
TO: 수신자 1 공개 키 106b
전송자 서명 112a
FROM: 에이전트 공개 키 106d
배서에 의해 핸들링됨 114a
에이전트 서명 112d
수신자 공개 키 106b
프로세싱만을 위한 배서 114b
수신자 서명 112b
100m2
105a
105b
105c

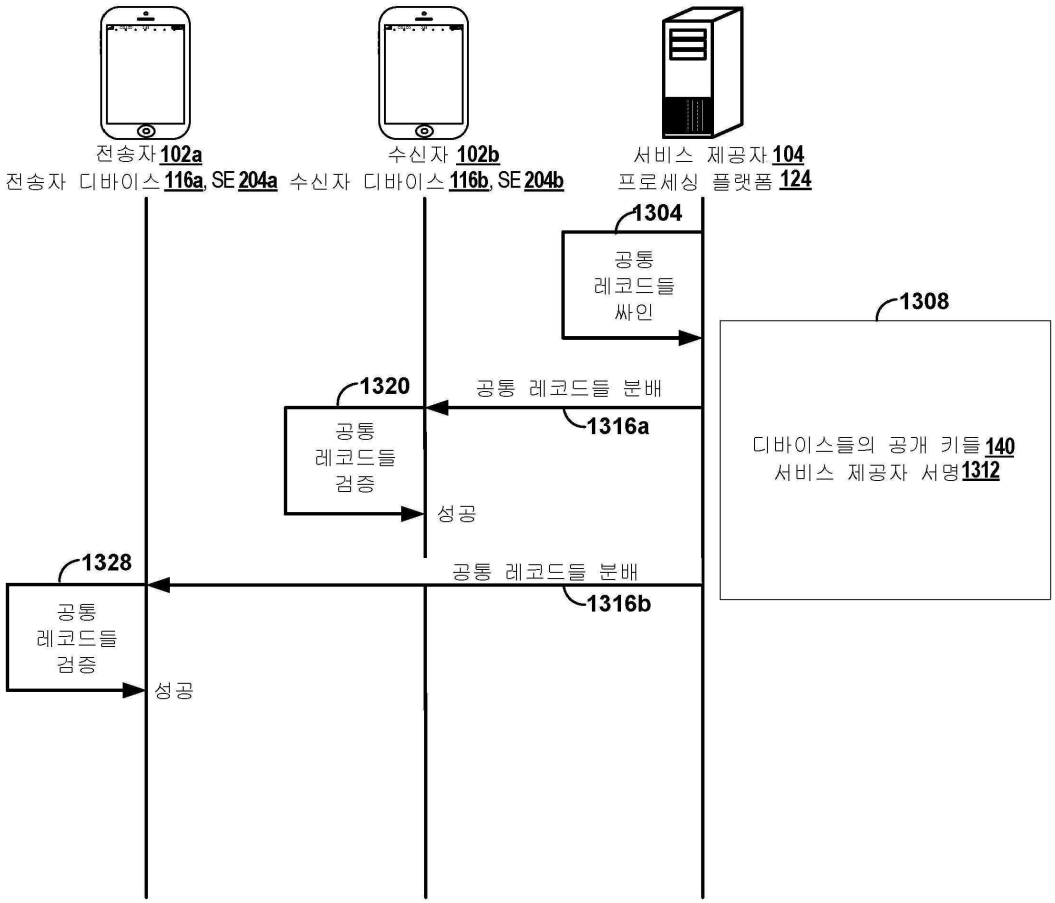
도면11


전송자 102a
전송자 디바이스 116a, SE 204a
수신자 102b
수신자 디바이스 116b, SE 204b
서비스 제공자 104
프로세싱 플랫폼 124
404
SRL을 통해 레코드 요청
콘텐츠 B 110b
수신자 공개 키 106b
402
408
파트너들 식별
전송자 SE가
레코드 싸인
416
SRL을 통해 레코드 전송
420
424
레코드 검증
성공
1104
수신자 SE가
레코드 싸인
1108
1112
레코드 전송
질의
프로세싱
질의 결과
예/아니오, 조건들
1116
수신자 SE가
레코드 싸인
428
432
436
레코드 상환
레코드
프로세싱
성공

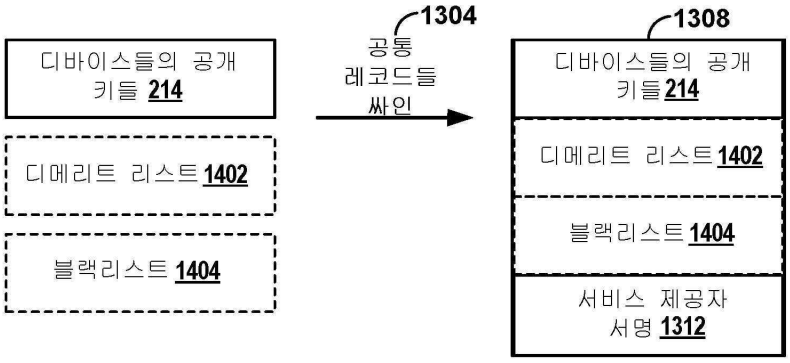
도면12


FROM: 전송자 공개 키 106a
레코드 ID 108
콘텐츠 A 110a
TO: 수신자 1 공개 키 106b
전송자 서명 112a
105a
100
416
SE 전송
콘텐츠 A 110a
수신자 1 공개 키 106b
전송자 1 인증 정보 512a
수신자 SE
1104
428
수신자 1 인증 정보 512b
FROM: 전송자 공개 키 106a
레코드 ID 108
콘텐츠 A 110a
TO: 수신자 1 공개 키 106b
전송자 서명 112a
105a
TO: 질의 배서 114a
수신자 서명 112b
105b
100m1
100m2
FROM: 전송자 공개 키 106a
레코드 ID 108
콘텐츠 A 110a
105a
TO: 수신자 1 공개 키 106b
전송자 서명 112a
프로세싱만을 위한 배서 114b
105c
수신자 서명 112b'

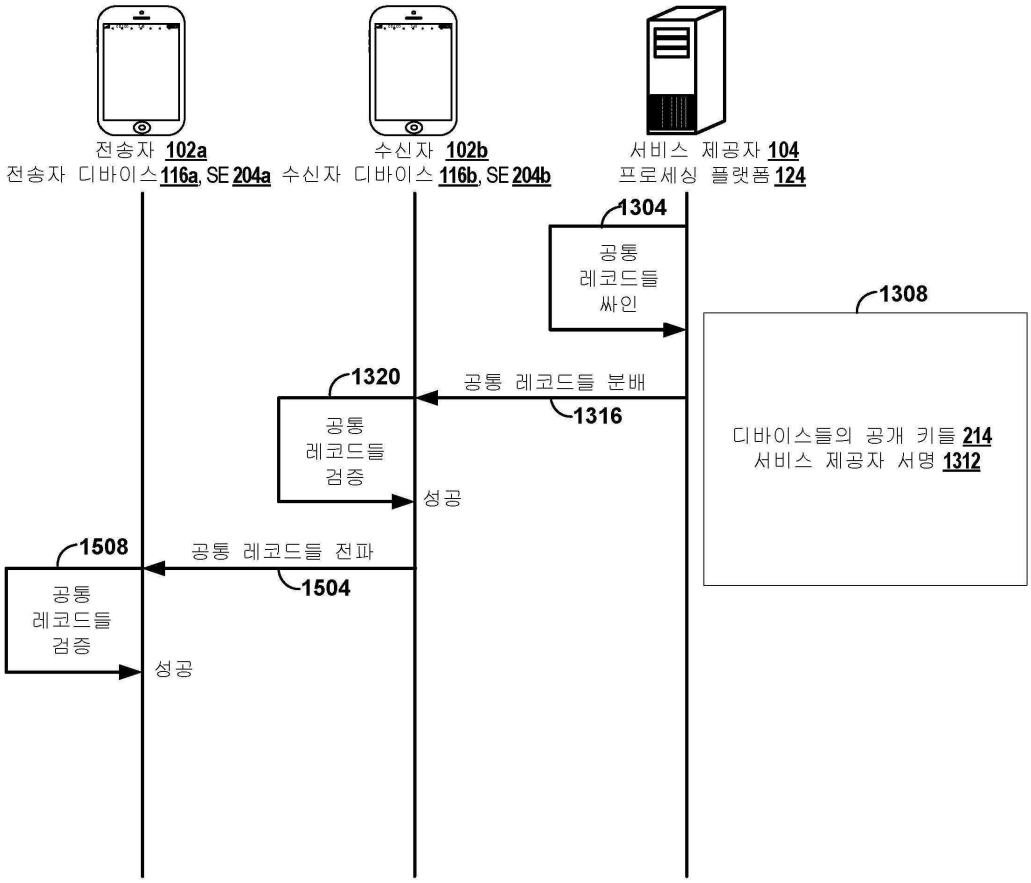
도면13


전송자 102a
전송자 디바이스 116a, SE 204a
수신자 102b
수신자 디바이스 116b, SE 204b
서비스 제공자 104
프로세싱 플랫폼 124
1304
공통 레코드들 싸인
1308
디바이스들의 공개 키들 140
서비스 제공자 서명 1312
1320
공통 레코드들 분배
1316a
공통 레코드들 검증
성공
1328
공통 레코드들 분배
1316b
공통 레코드들 검증
성공

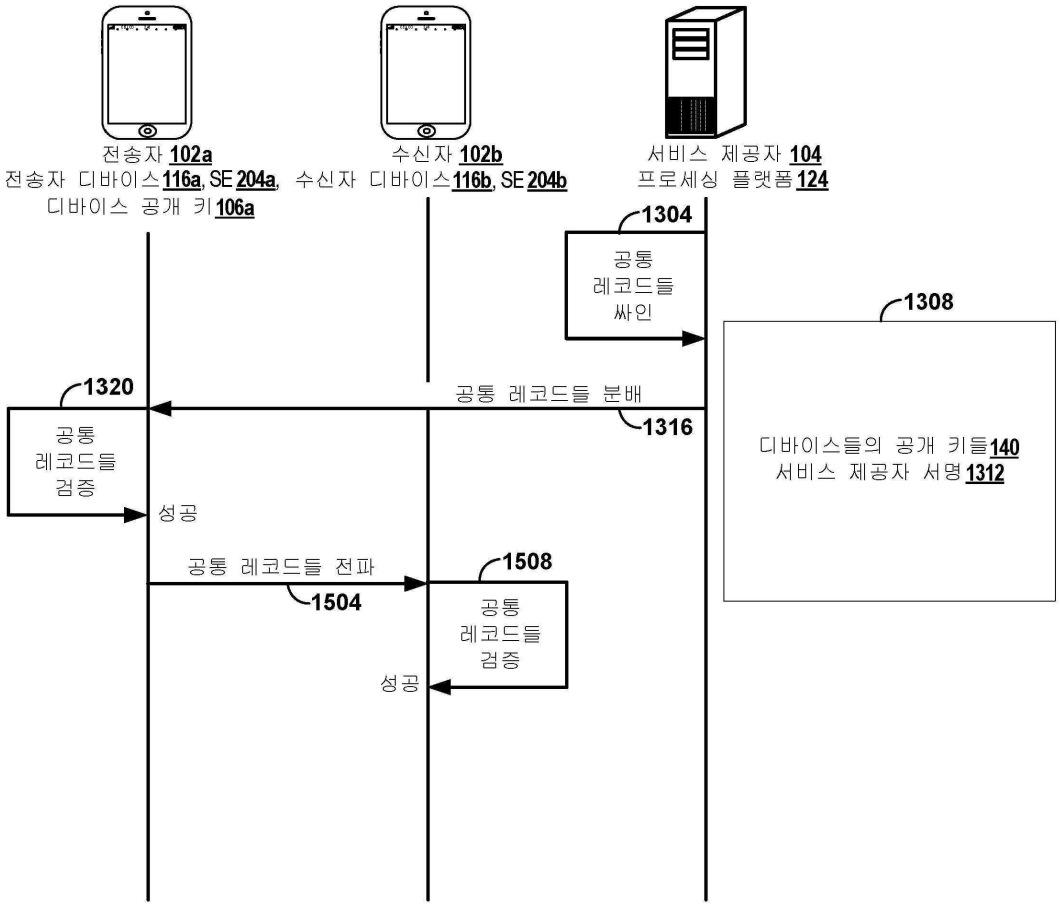
도면14


디바이스들의 공개 키들 214
디메리트 리스트 1402
블랙리스트 1404
1304
공통 레코드들 싸인
1308
디바이스들의 공개 키들 214
디메리트 리스트 1402
블랙리스트 1404
서비스 제공자 서명 1312

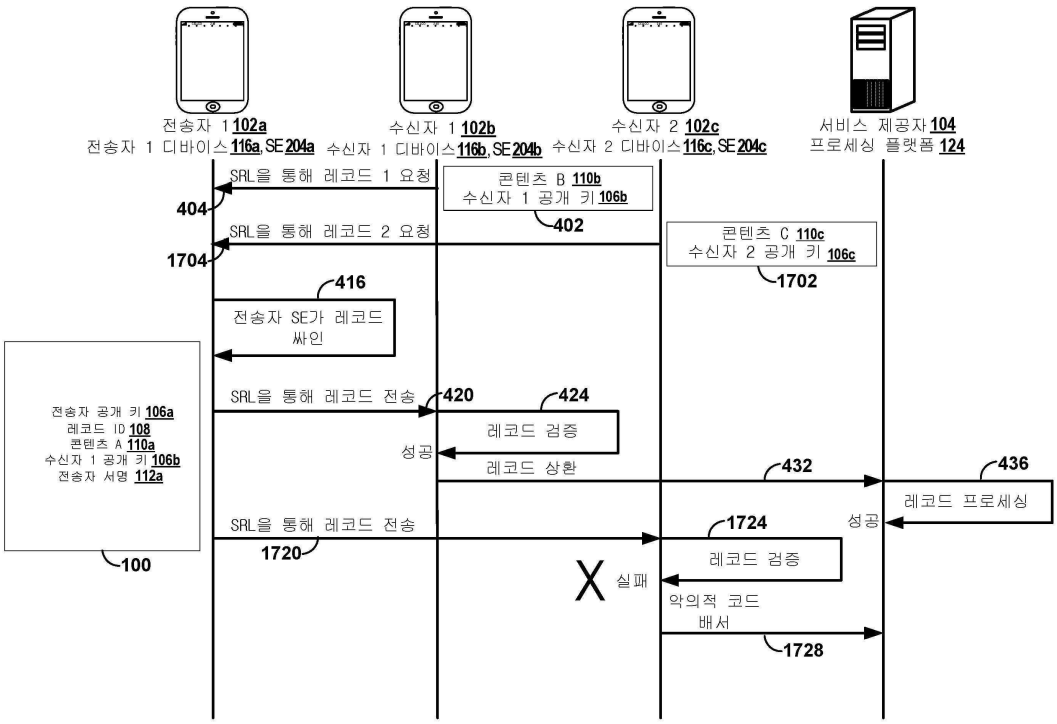
도면15


전송자 102a
전송자 디바이스 116a, SE 204a
수신자 102b
수신자 디바이스 116b, SE 204b
서비스 제공자 104
프로세싱 플랫폼 124
1304
공통 레코드들 싸인
1308
디바이스들의 공개 키들 214
서비스 제공자 서명 1312
1320
공통 레코드들 분배
1316
공통 레코드들 검증
성공
1508
공통 레코드들 전파
1504
공통 레코드들 검증
성공

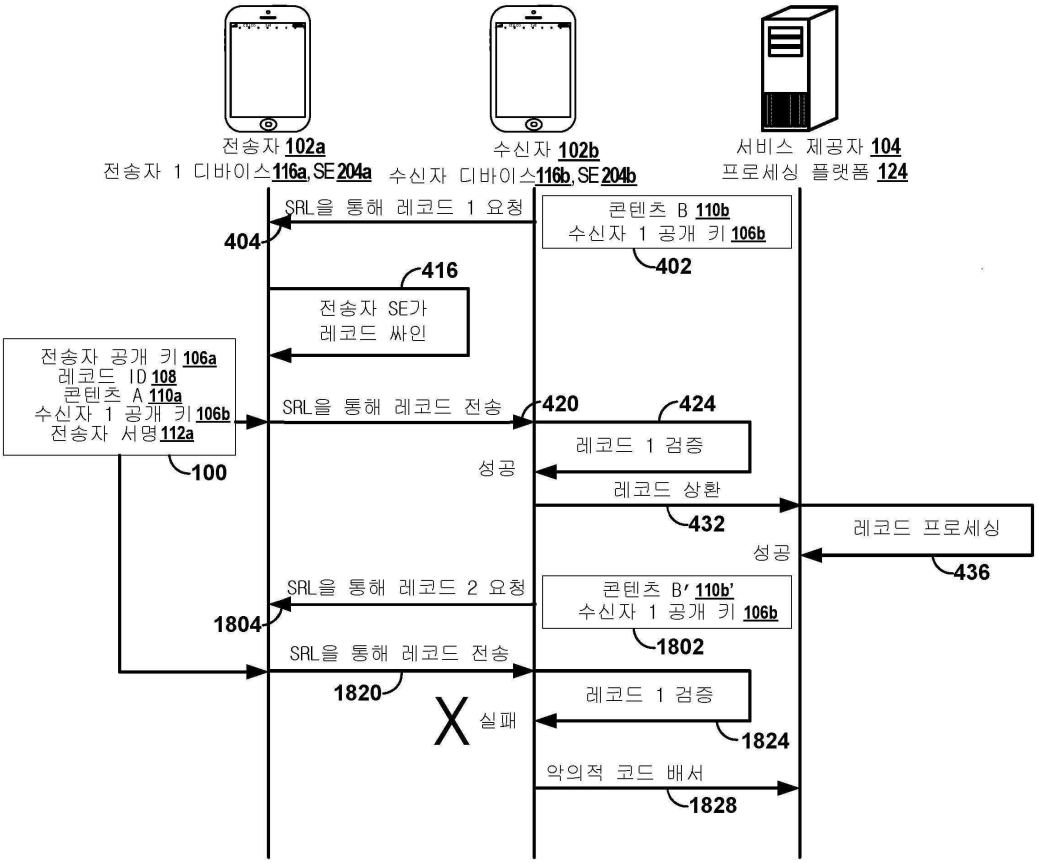
도면16


전송자 102a
전송자 디바이스 116a, SE 204a,
디바이스 공개 키 106a
수신자 102b
수신자 디바이스 116b, SE 204b
서비스 제공자 104
프로세싱 플랫폼 124
1304
공통
레코드들
싸인
1308
디바이스들의 공개 키들 140
서비스 제공자 서명 1312
1320
공통
레코드들
검증
성공
공통 레코드들 분배
1316
공통 레코드들 전파
1504
1508
공통
레코드들
검증
성공

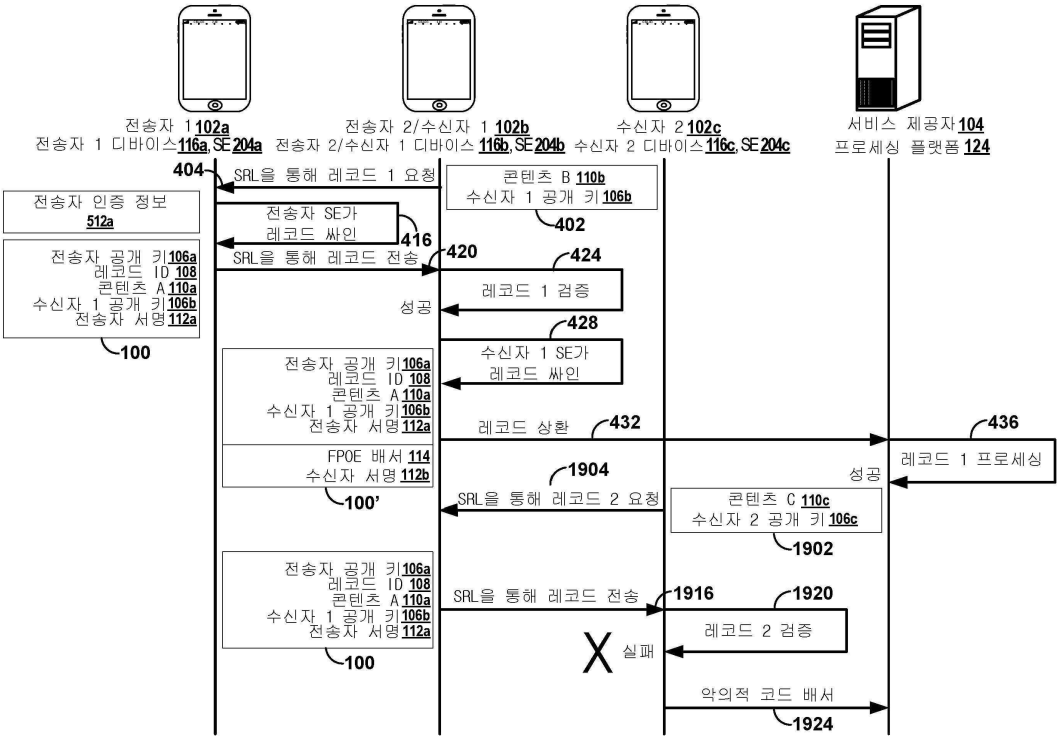
도면17


전송자 1 102a
전송자 1 디바이스 116a, SE 204a
수신자 1 102b
수신자 1 디바이스 116b, SE 204b
수신자 2 102c
수신자 2 디바이스 116c, SE 204c
서비스 제공자 104
프로세싱 플랫폼 124
SRL을 통해 레코드 1 요청
404
콘텐츠 B 110b
수신자 1 공개 키 106b
402
SRL을 통해 레코드 2 요청
1704
콘텐츠 C 110c
수신자 2 공개 키 106c
1702
416
전송자 SE가 레코드
싸인
전송자 공개 키 106a
레코드 ID 108
콘텐츠 A 110a
수신자 1 공개 키 106b
전송자 서명 112a
100
SRL을 통해 레코드 전송
420
424
레코드 검증
성공
레코드 상환
432
436
레코드 프로세싱
성공
SRL을 통해 레코드 전송
1720
1724
레코드 검증
X 실패
악의적 코드
배서
1728

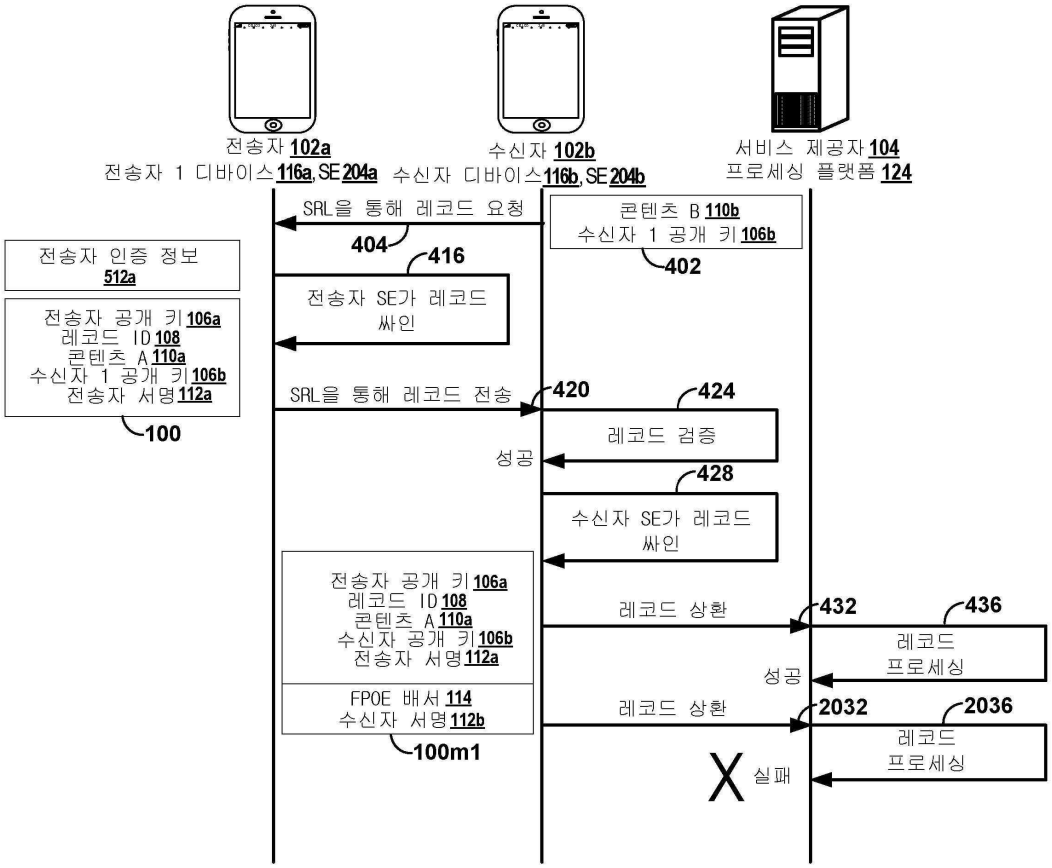
도면18


전송자 102a
전송자 1 디바이스 116a, SE 204a
수신자 102b
수신자 디바이스 116b, SE 204b
서비스 제공자 104
프로세싱 플랫폼 124
SRL을 통해 레코드 1 요청
404
콘텐츠 B 110b
수신자 1 공개 키 106b
402
416
전송자 SE가
레코드 싸인
전송자 공개 키 106a
레코드 ID 108
콘텐츠 A 110a
수신자 1 공개 키 106b
전송자 서명 112a
100
SRL을 통해 레코드 전송
420
424
레코드 1 검증
성공
레코드 상환
432
레코드 프로세싱
성공
436
SRL을 통해 레코드 2 요청
1804
콘텐츠 B′ 110b′
수신자 1 공개 키 106b
1802
SRL을 통해 레코드 전송
1820
레코드 1 검증
X
실패
1824
악의적 코드 배서
1828

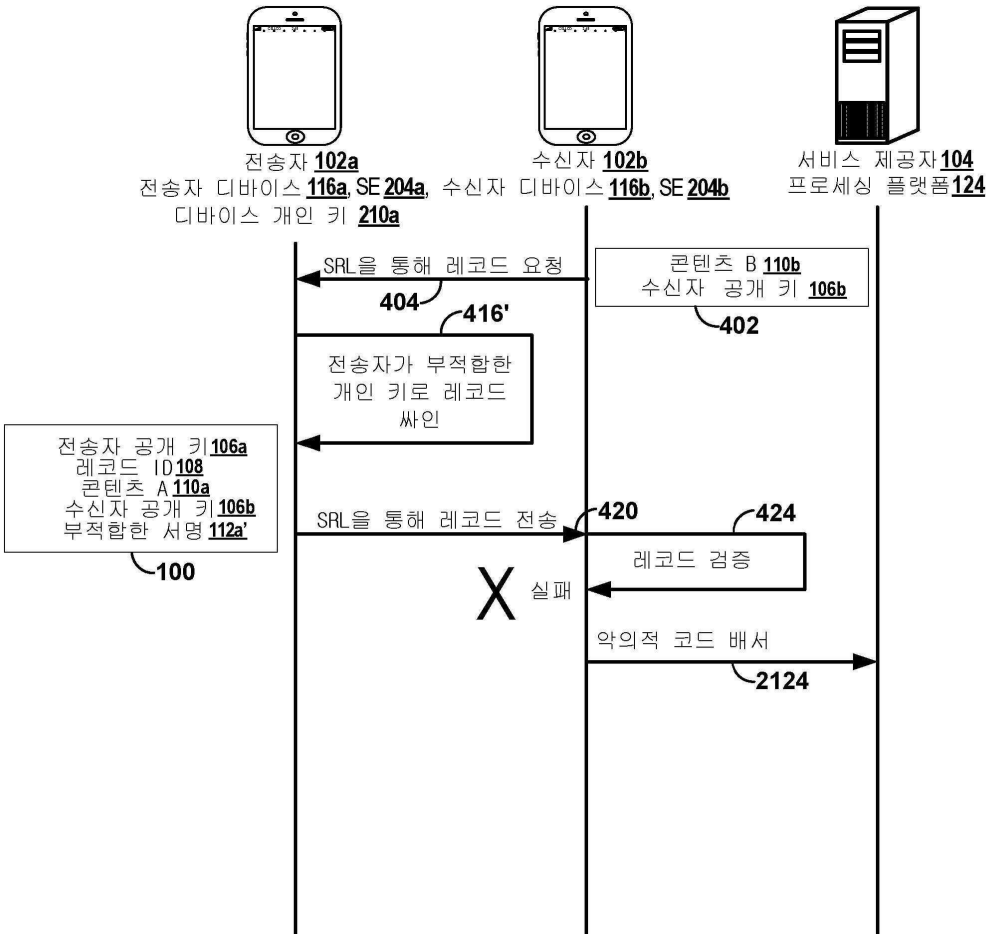
도면19


전송자 1 102a
전송자 1 디바이스 116a, SE 204a
전송자 2/수신자 1 102b
전송자 2/수신자 1 디바이스 116b, SE 204b
수신자 2 102c
수신자 2 디바이스 116c, SE 204c
서비스 제공자 104
프로세싱 플랫폼 124
404
SRL을 통해 레코드 1 요청
콘텐츠 B 110b
수신자 1 공개 키 106b
402
전송자 인증 정보
512a
전송자 SE가
레코드 싸인
416
전송자 공개 키 106a
레코드 ID 108
콘텐츠 A 110a
수신자 1 공개 키 106b
전송자 서명 112a
100
SRL을 통해 레코드 전송
420
424
레코드 1 검증
성공
428
수신자 1 SE가
레코드 싸인
전송자 공개 키 106a
레코드 ID 108
콘텐츠 A 110a
수신자 1 공개 키 106b
전송자 서명 112a
레코드 상환
432
436
레코드 1 프로세싱
성공
FPOE 배서 114
수신자 서명 112b
100′
1904
SRL을 통해 레코드 2 요청
콘텐츠 C 110c
수신자 2 공개 키 106c
1902
전송자 공개 키 106a
레코드 ID 108
콘텐츠 A 110a
수신자 1 공개 키 106b
전송자 서명 112a
100
SRL을 통해 레코드 전송
1916
1920
레코드 2 검증
X
실패
악의적 코드 배서
1924

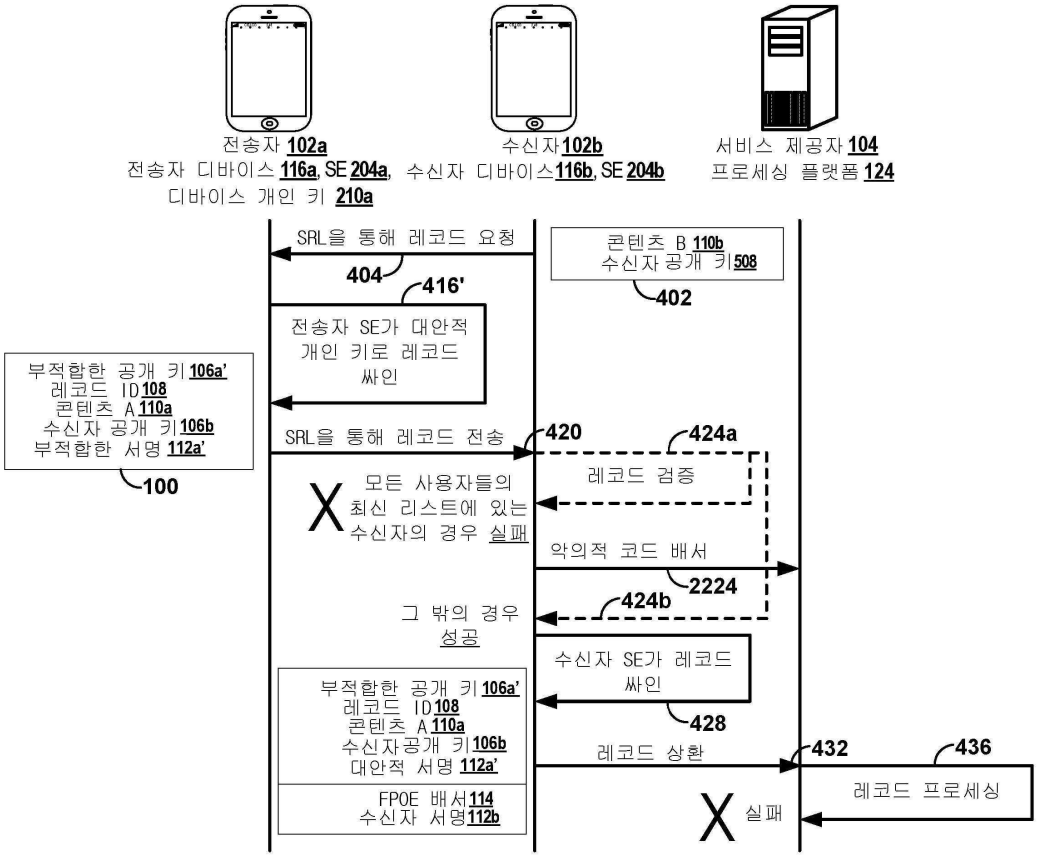
도면20


전송자 102a
전송자 1 디바이스 116a, SE 204a
수신자 102b
수신자 디바이스 116b, SE 204b
서비스 제공자 104
프로세싱 플랫폼 124
SRL을 통해 레코드 요청
404
416
콘텐츠 B 110b
수신자 1 공개 키 106b
402
전송자 인증 정보 512a
전송자 SE가 레코드 싸인
전송자 공개 키 106a
레코드 ID 108
콘텐츠 A 110a
수신자 1 공개 키 106b
전송자 서명 112a
100
SRL을 통해 레코드 전송
420
424
레코드 검증
성공
428
수신자 SE가 레코드 싸인
전송자 공개 키 106a
레코드 ID 108
콘텐츠 A 110a
수신자 공개 키 106b
전송자 서명 112a
레코드 상환
432
436
레코드 프로세싱
성공
FPOE 배서 114
수신자 서명 112b
100m1
레코드 상환
2032
2036
레코드 프로세싱
X
실패

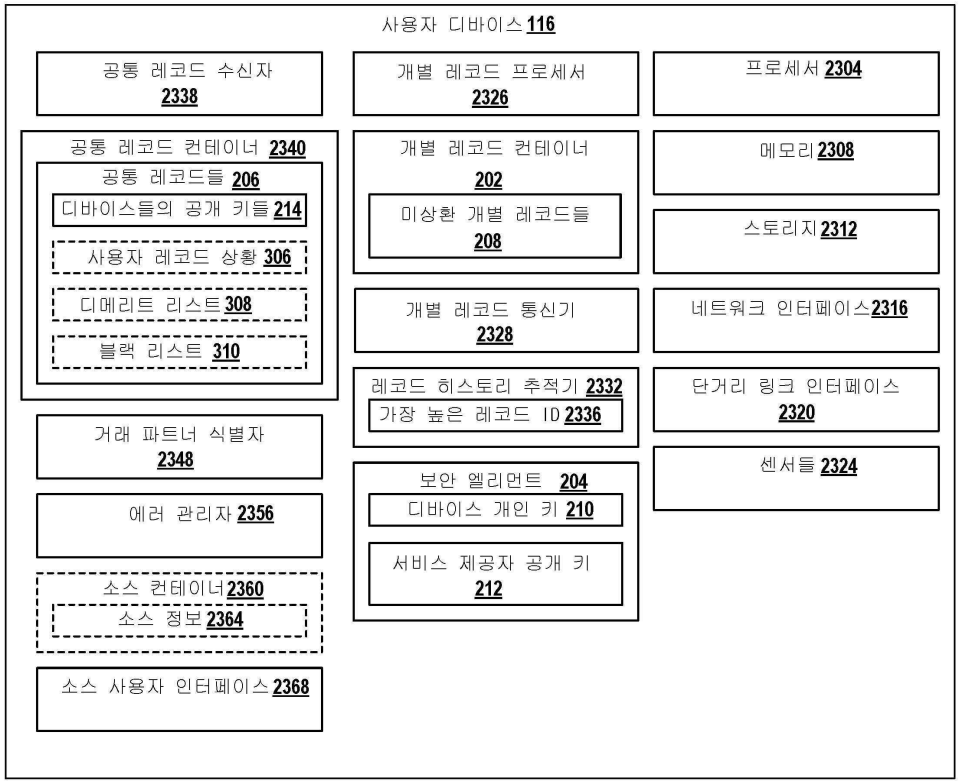
도면21


전송자 102a
전송자 디바이스 116a, SE 204a,
디바이스 개인 키 210a
수신자 102b
수신자 디바이스 116b, SE 204b
서비스 제공자 104
프로세싱 플랫폼 124
SRL을 통해 레코드 요청
404
416'
전송자가 부적합한
개인 키로 레코드
싸인
콘텐츠 B 110b
수신자 공개 키 106b
402
전송자 공개 키 106a
레코드 ID 108
콘텐츠 A 110a
수신자 공개 키 106b
부적합한 서명 112a'
100
SRL을 통해 레코드 전송
420
424
레코드 검증
X
실패
악의적 코드 배서
2124

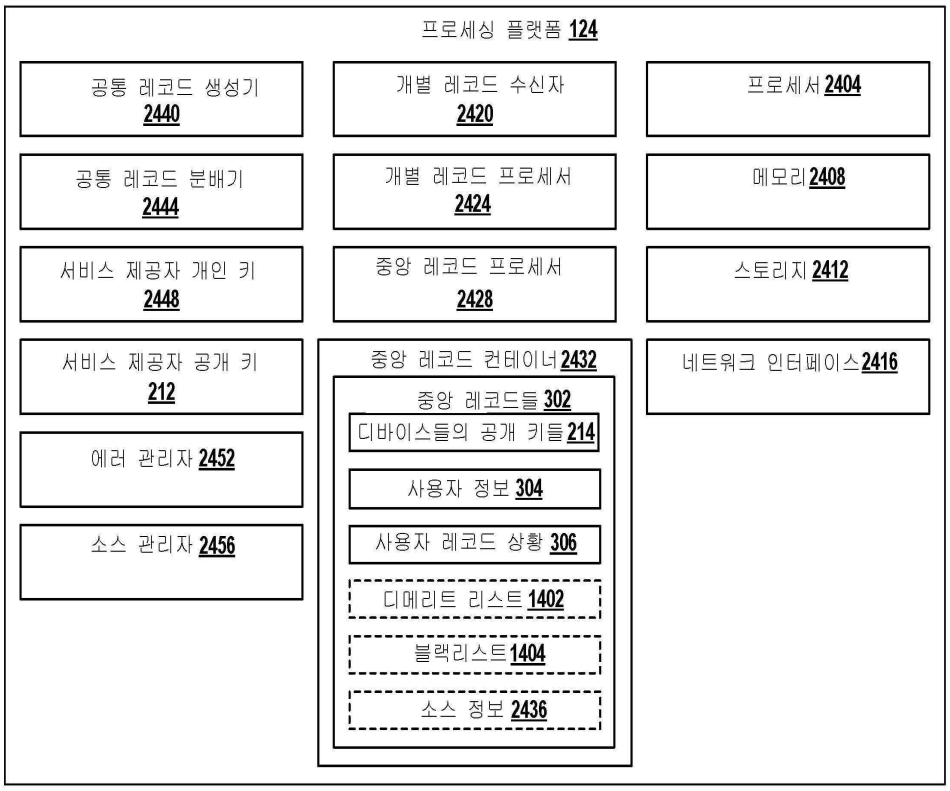
도면22


전송자 102a
전송자 디바이스 116a, SE 204a,
디바이스 개인 키 210a
수신자 102b
수신자 디바이스 116b, SE 204b
서비스 제공자 104
프로세싱 플랫폼 124
SRL을 통해 레코드 요청
404
416'
전송자 SE가 대안적 개인 키로 레코드 싸인
콘텐츠 B 110b
수신자 공개 키 508
402
부적합한 공개 키 106a'
레코드 ID 108
콘텐츠 A 110a
수신자 공개 키 106b
부적합한 서명 112a'
100
SRL을 통해 레코드 전송
420
424a
레코드 검증
X
모든 사용자들의 최신 리스트에 있는 수신자의 경우 실패
악의적 코드 배서
2224
424b
그 밖의 경우 성공
수신자 SE가 레코드 싸인
428
부적합한 공개 키 106a'
레코드 ID 108
콘텐츠 A 110a
수신자공개 키 106b
대안적 서명 112a'
FPOE 배서 114
수신자 서명 112b
레코드 상환
432
436
레코드 프로세싱
X
실패

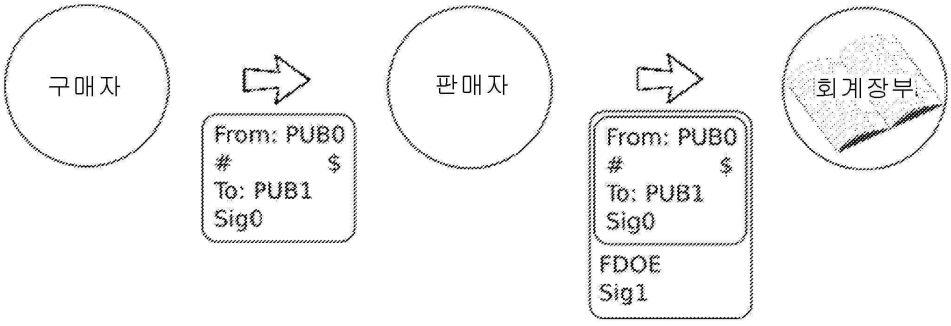
도면23


사용자 디바이스 116
공통 레코드 수신자 2338
개별 레코드 프로세서 2326
프로세서 2304
공통 레코드 컨테이너 2340
공통 레코드들 206
디바이스들의 공개 키들 214
사용자 레코드 상황 306
디메리트 리스트 308
블랙 리스트 310
개별 레코드 컨테이너 202
미상환 개별 레코드들 208
메모리 2308
스토리지 2312
개별 레코드 통신기 2328
네트워크 인터페이스 2316
레코드 히스토리 추적기 2332
가장 높은 레코드 ID 2336
단거리 링크 인터페이스 2320
센서들 2324
보안 엘리먼트 204
디바이스 개인 키 210
서비스 제공자 공개 키 212
거래 파트너 식별자 2348
에러 관리자 2356
소스 컨테이너 2360
소스 정보 2364
소스 사용자 인터페이스 2368

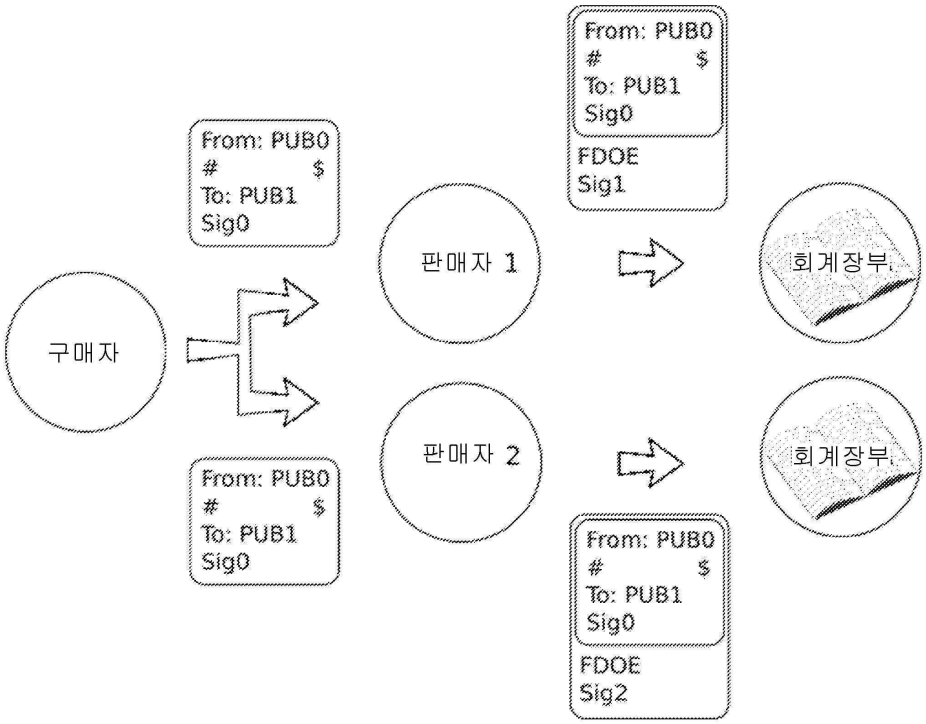
도면24


프로세싱 플랫폼 124
공통 레코드 생성기 2440
개별 레코드 수신자 2420
프로세서 2404
공통 레코드 분배기 2444
개별 레코드 프로세서 2424
메모리 2408
서비스 제공자 개인 키 2448
중앙 레코드 프로세서 2428
스토리지 2412
서비스 제공자 공개 키 212
중앙 레코드 컨테이너 2432
네트워크 인터페이스 2416
중앙 레코드들 302
디바이스들의 공개 키들 214
사용자 정보 304
사용자 레코드 상황 306
디메리트 리스트 1402
블랙리스트 1404
소스 정보 2436
에러 관리자 2452
소스 관리자 2456

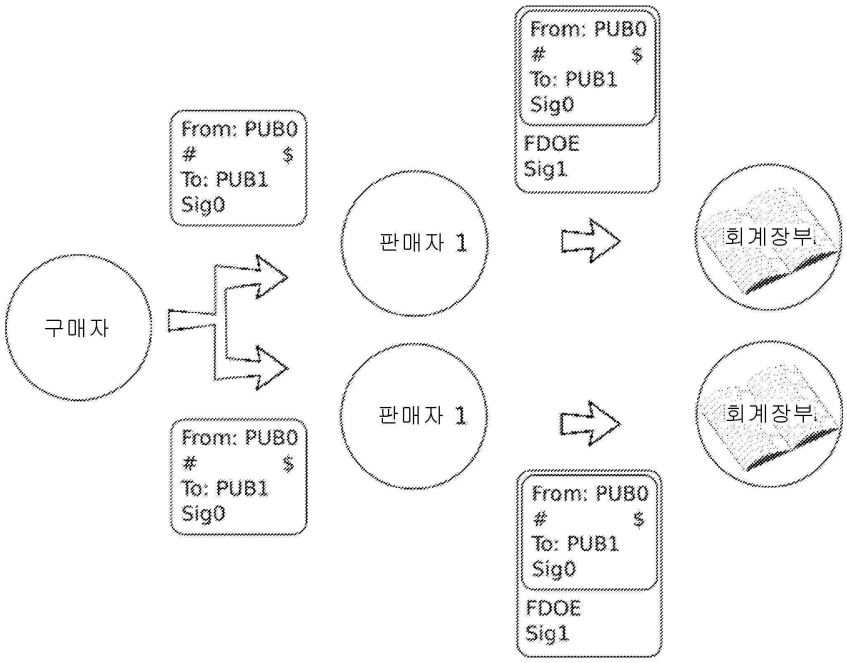
도면25


구매자
From: PUB0
#
$
To: PUB1
Sig0
판매자
From: PUB0
#
$
To: PUB1
Sig0
FDOE
Sig1
회계장부

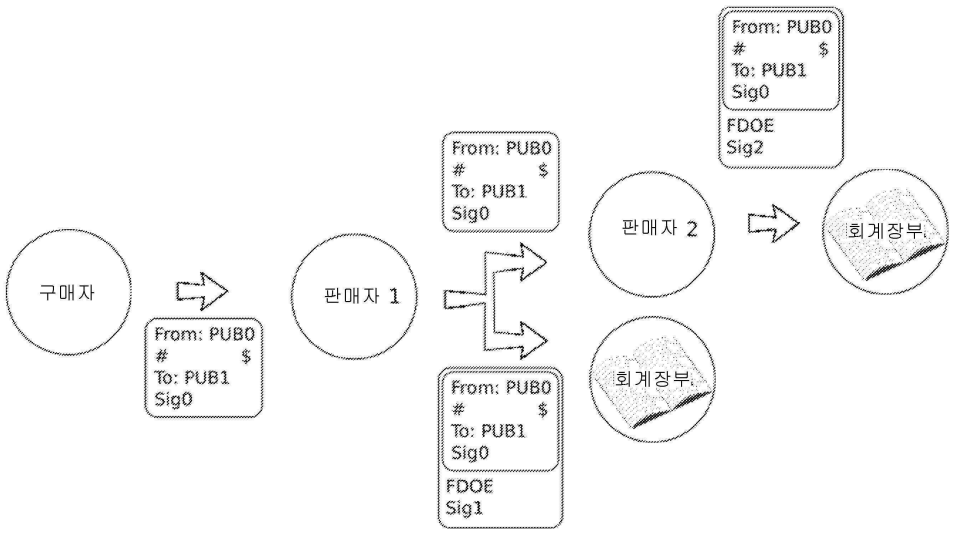
도면26


From: PUB0
#
$
To: PUB1
Sig0
구매자
From: PUB0
#
$
To: PUB1
Sig0
판매자 1
From: PUB0
#
$
To: PUB1
Sig0
FDOE
Sig1
회계장부
판매자 2
회계장부
From: PUB0
#
$
To: PUB1
Sig0
FDOE
Sig2

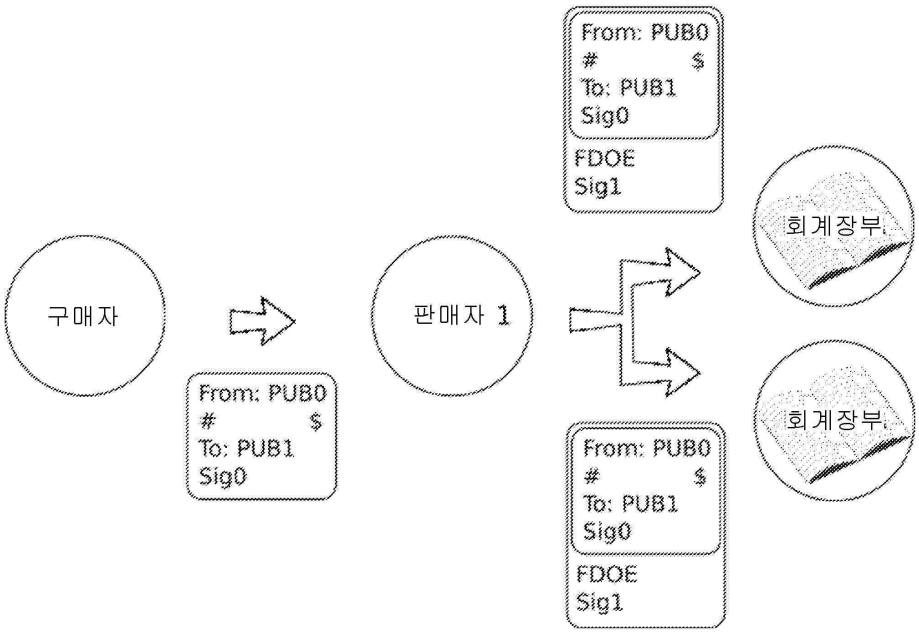
도면27


From: PUB0
#
$
To: PUB1
Sig0
구매자
From: PUB0
#
$
To: PUB1
Sig0
판매자 1
From: PUB0
#
$
To: PUB1
Sig0
FDOE
Sig1
회계장부
판매자 1
회계장부
From: PUB0
#
$
To: PUB1
Sig0
FDOE
Sig1

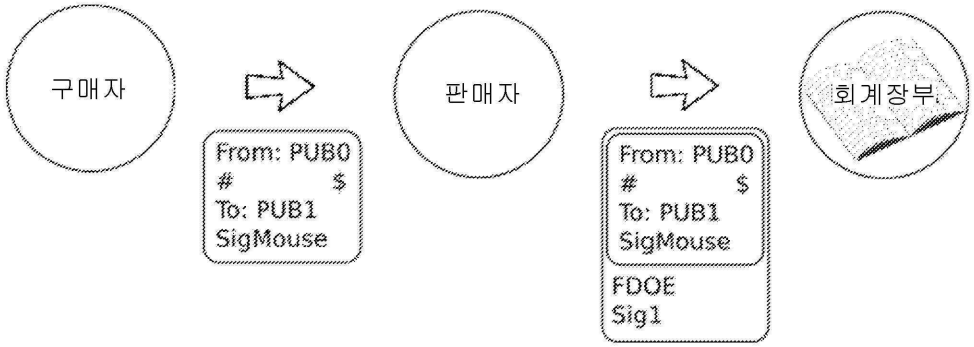
도면28



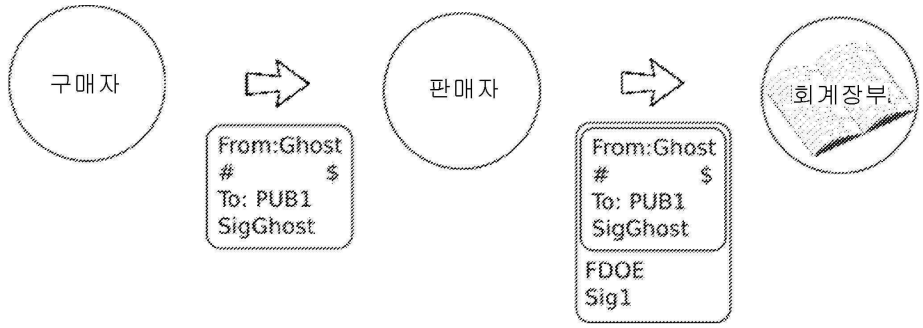
도면29



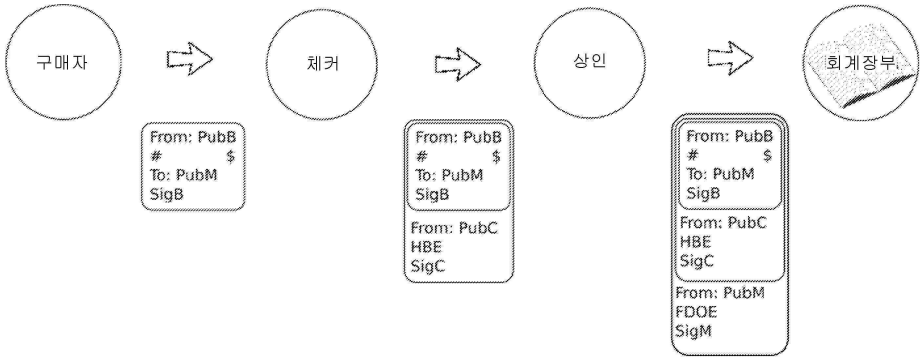
도면30



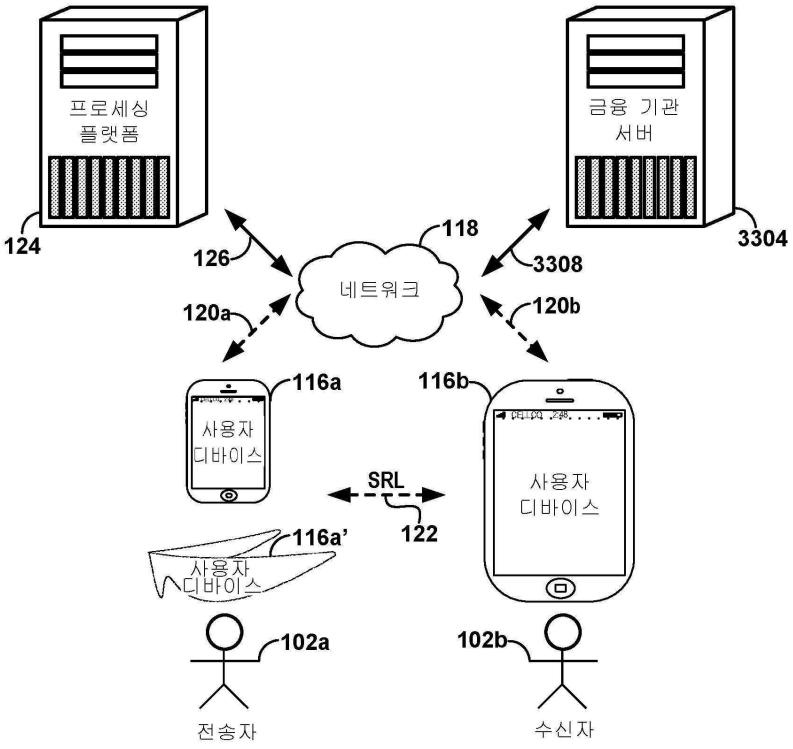
도면31



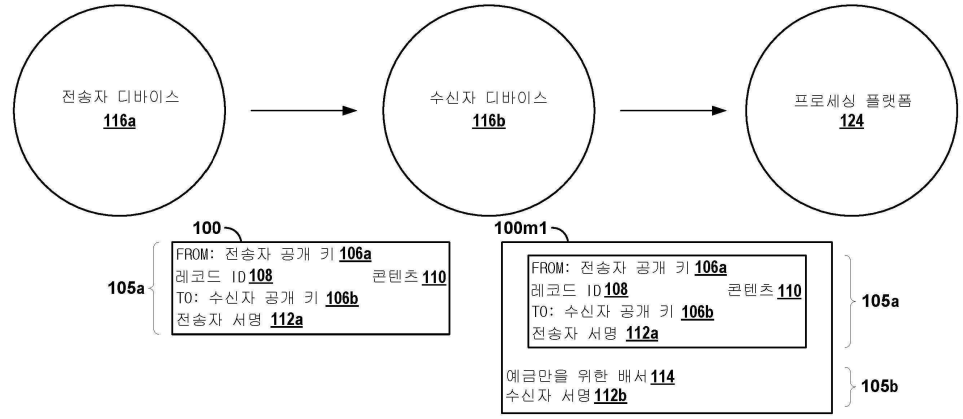
도면32



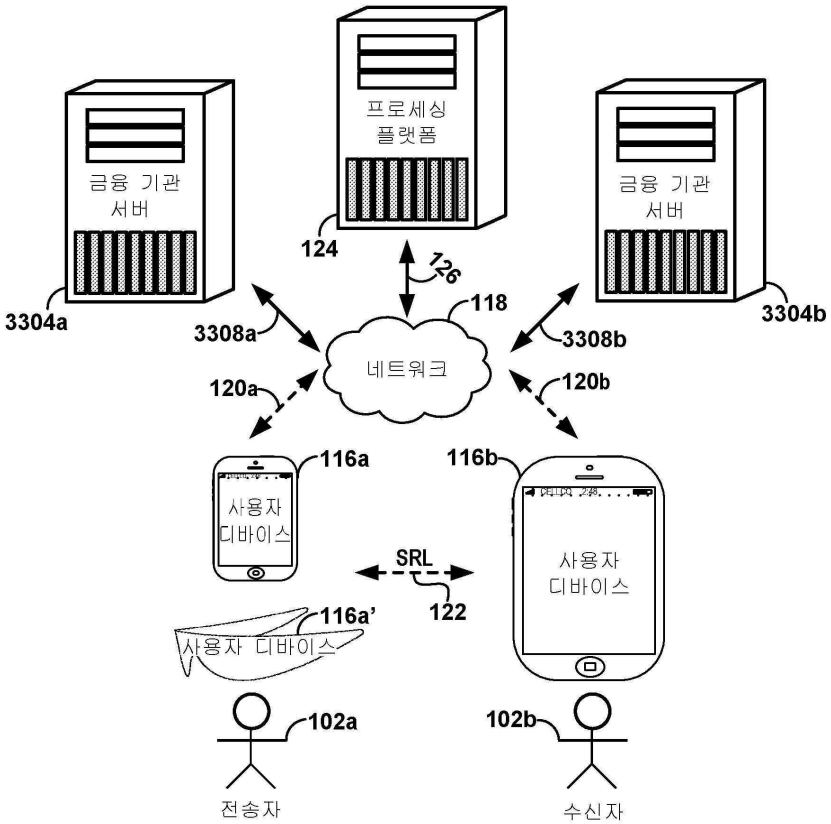
도면33a



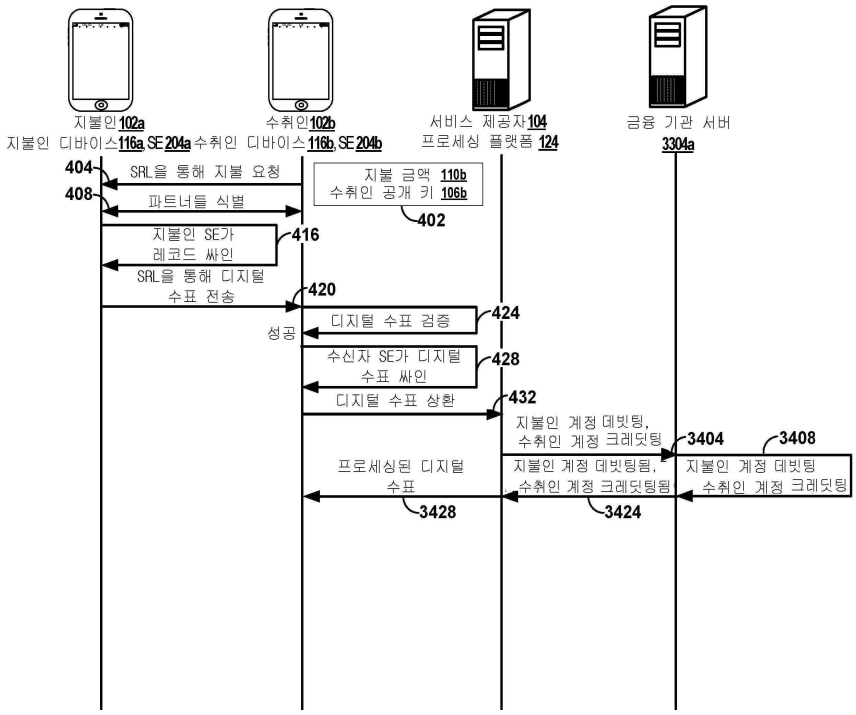
도면33b


전송자 디바이스
116a
수신자 디바이스
116b
프로세싱 플랫폼
124
100
FROM: 전송자 공개 키 106a
레코드 ID 108
콘텐츠 110
TO: 수신자 공개 키 106b
전송자 서명 112a
105a
100m1
FROM: 전송자 공개 키 106a
레코드 ID 108
콘텐츠 110
TO: 수신자 공개 키 106b
전송자 서명 112a
105a
예금만을 위한 배서 114
수신자 서명 112b
105b

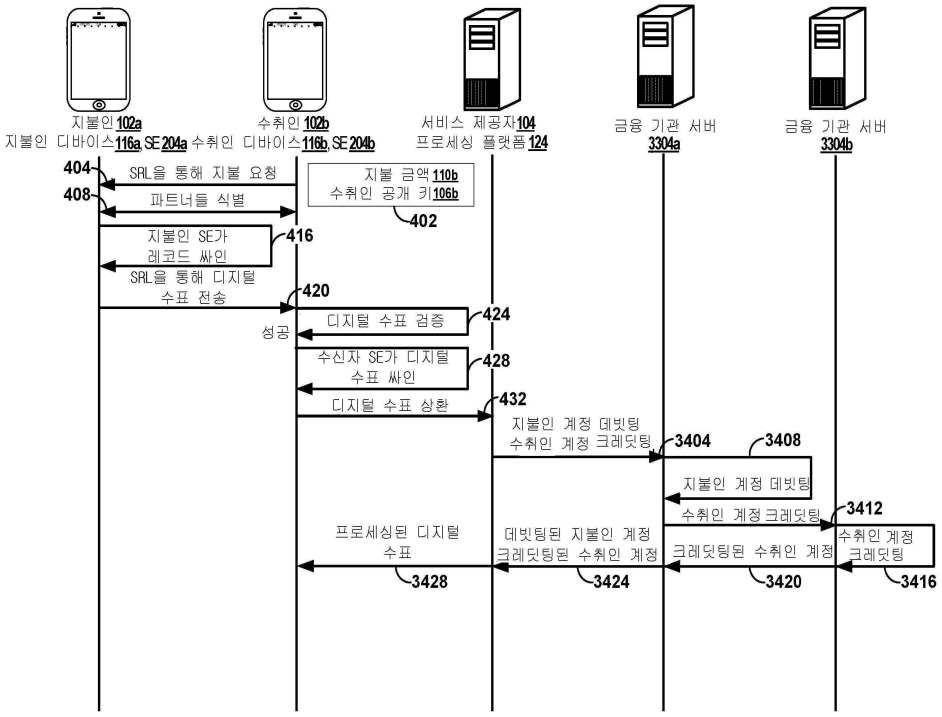
도면33c


금융 기관 서버
3304a
프로세싱 플랫폼
124
126
118
금융 기관 서버
3304b
3308a
3308b
네트워크
120a
120b
116a
사용자 디바이스
116b
사용자 디바이스
SRL
122
116a'
사용자 디바이스
102a
전송자
102b
수신자

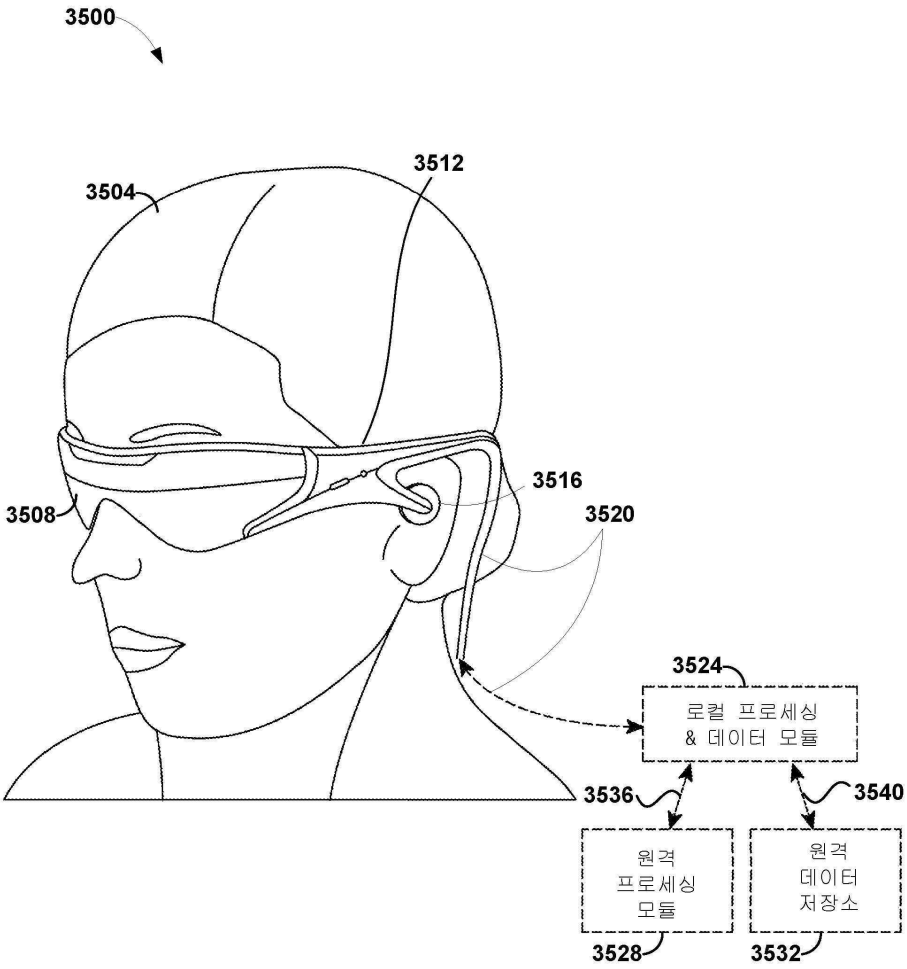
도면34a


지불인 102a
지불인 디바이스 116a, SE 204a
수취인 102b
수취인 디바이스 116b, SE 204b
서비스 제공자 104
프로세싱 플랫폼 124
금융 기관 서버
3304a
404
SRL을 통해 지불 요청
408
파트너들 식별
지불 금액 110b
수취인 공개 키 106b
402
416
지불인 SE가
레코드 싸인
SRL을 통해 디지털
수표 전송
420
디지털 수표 검증
424
성공
수신자 SE가 디지털
수표 싸인
428
디지털 수표 상환
432
지불인 계정 데빗팅,
수취인 계정 크레딧팅
3404
3408
지불인 계정 데빗팅
수취인 계정 크레딧팅
지불인 계정 데빗팅됨,
수취인 계정 크레딧팅됨
3424
프로세싱된 디지털
수표
3428

도면34b


지불인 102a
지불인 디바이스 116a, SE 204a
수취인 102b
수취인 디바이스 116b, SE 204b
서비스 제공자 104
프로세싱 플랫폼 124
금융 기관 서버
3304a
금융 기관 서버
3304b
404
SRL을 통해 지불 요청
408
파트너들 식별
지불 금액 110b
수취인 공개 키 106b
402
416
지불인 SE가
레코드 싸인
SRL을 통해 디지털
수표 전송
420
디지털 수표 검증
424
성공
수신자 SE가 디지털
수표 싸인
428
디지털 수표 상환
432
지불인 계정 데빗팅
수취인 계정 크레딧팅
3404
3408
지불인 계정 데빗팅
3412
수취인 계정 크레딧팅
수취인 계정
크레딧팅
3416
데빗팅된 지불인 계정
크레딧팅된 수취인 계정
3424
크레딧팅된 수취인 계정
3420
프로세싱된 디지털
수표
3428

도면35


3500
3512
3504
3516
3508
3520
3524
로컬 프로세싱
& 데이터 모듈
3536
3540
원격
프로세싱
모듈
원격
데이터
저장소
3528
3532