



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2022-0131676
(43) 공개일자 2022년09월29일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) H04L 9/08 (2006.01)
H04L 9/14 (2006.01)
(52) CPC특허분류
H04L 9/3252 (2013.01)
H04L 9/0852 (2013.01)
(21) 출원번호 10-2021-0036631
(22) 출원일자 2021년03월22일
심사청구일자 2021년03월22일

(71) 출원인
계명대학교 산학협력단
대구광역시 달서구 달구벌대로 1095, 계명대학교
산학협력관 201호(신당동)
(72) 발명자
나동준
대구광역시 달성군 현풍읍 테크노상업로 49, 104
동 602호(제일풍경채더퍼스트)
박세진
대구광역시 동구 팔공로 260(봉무동, 협성휴포레
이시아폴리스)
(74) 대리인
특허법인 무한

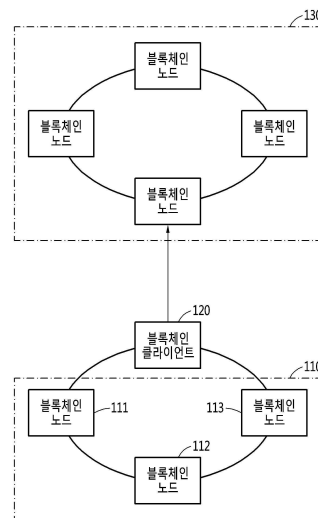
전체 청구항 수 : 총 17 항

(54) 발명의 명칭 다중 서명과 슈노르 서명을 이용한 블록 체인 시스템의 서명 검증 방법 및 시스템

(57) 요약

다중 서명과 슈노르 서명을 이용한 블록 체인 시스템의 서명 검증 방법 및 시스템이 개시된다. 서명 검증 방법은 사용자들 각각의 서명들을 결합하여 슈노르 서명을 생성하는 단계; 블록 체인 시스템에 등록된 다중 공개 키를 로드하는 단계; 상기 다중 공개 키에 포함된 공개 키들을 결합하여 검증 공개 키를 생성하는 단계; 및 상기 검증 공개 키로 상기 슈노르 서명을 검증하는 단계를 포함할 수 있다.

대표도 - 도1



(52) CPC특허분류

H04L 9/14 (2022.08)

H04L 9/50 (2022.05)

H04L 2209/26 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호	1711116985
과제번호	2020-0-00936-001
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기획평가원
연구사업명	정보통신·방송연구개발사업
연구과제명	5G 초저지연 서비스를 위한 무선 단말용 블록체인 기술 개발
기 여 율	1/1
과제수행기관명	계명대학교 산학협력단
연구기간	2020.04.01 ~ 2020.12.31

명세서

청구범위

청구항 1

사용자들 각각의 서명들을 결합하여 슈노르 서명을 생성하는 단계;
블록 체인 시스템에 등록된 다중 공개 키를 로드하는 단계;
상기 다중 공개 키에 포함된 공개 키들을 결합하여 검증 공개 키를 생성하는 단계; 및
상기 검증 공개 키로 상기 슈노르 서명을 검증하는 단계
를 포함하는 서명 검증 방법.

청구항 2

제1항에 있어서,
상기 다중 공개 키는,
상기 사용자들 각각의 서명들로 구성된 멀티 시그 서명을 복호화할 수 있는지 여부에 따라 검증된 후 상기 블록 체인 시스템에 기 등록되는 서명 검증 방법.

청구항 3

제1항에 있어서,
상기 슈노르 서명을 생성하는 단계는,
상기 사용자들 각각의 개인 키를 이용하여 다중 서명을 생성하는 단계; 및
상기 다중 서명을 슈노르 시그니처에 따라 결합하여 슈노르 서명을 생성하는 단계
를 포함하는 서명 검증 방법.

청구항 4

제1항에 있어서,
상기 검증 공개 키는,
상기 다중 공개 키에 포함된 상기 사용자들 각각의 공개 키들을 슈노르 시그니처에 따라 결합하여 생성되는 서명 검증 방법.

청구항 5

사용자들 각각의 서명들이 포함된 다중 서명을 생성하는 단계;
상기 사용자들 각각의 공개 키들이 포함된 다중 공개 키를 생성하는 단계; 및
상기 다중 서명 및 상기 다중 공개 키를 블록 체인 시스템에 전송하는 단계
를 포함하고,
상기 블록 체인 시스템은,
상기 다중 서명을 이용하여 상기 다중 공개 키를 검증하고, 검증된 다중 공개 키를 저장하는 서명 검증을 위한 공개 키 등록 방법.

청구항 6

제5항에 있어서,

상기 블록 체인 시스템은,

상기 다중 공개 키를 사용하여 상기 다중 서명을 복호화할 수 있는 경우, 상기 다중 공개 키를 검증된 것으로 결정하는 서명 검증을 위한 공개 키 등록 방법.

청구항 7

제5항에 있어서,

상기 블록 체인 시스템은,

상기 다중 공개 키를 사용하여 상기 다중 서명을 복호화할 수 없는 경우, 상기 다중 공개 키를 검증 실패한 것으로 결정하는 서명 검증을 위한 공개 키 등록 방법.

청구항 8

제5항에 있어서,

상기 다중 공개 키에 포함된 상기 사용자들 각각의 공개 키들을 슈노르 시그니처에 따라 결합하여 검증 공개 키를 생성하는 단계

를 더 포함하고,

상기 검증 공개 키는,

상기 사용자들 각각의 서명들을 결합하여 생성한 슈노르 서명을 검증하기 위하여 사용되는 서명 검증을 위한 공개 키 등록 방법.

청구항 9

제1항 내지 제8항 중 어느 한 항의 방법을 실행하기 위한 프로그램이 기록된 컴퓨터에서 판독 가능한 기록 매체.

청구항 10

다중 공개 키가 등록된 블록 체인 시스템; 및

사용자들 각각의 서명들을 결합하여 슈노르 서명을 생성하고, 상기 다중 공개 키에 포함된 공개 키들을 결합하여 검증 공개 키를 생성하며, 상기 검증 공개 키로 상기 슈노르 서명을 검증하는 블록 체인 클라이언트

를 포함하는 서명 검증 시스템.

청구항 11

제10항에 있어서,

상기 다중 공개 키는,

상기 사용자들 각각의 서명들로 구성된 멀티 시그 서명을 복호화할 수 있는지 여부에 따라 검증된 후 상기 블록 체인 시스템에 기 등록되는 서명 검증 시스템.

청구항 12

제10항에 있어서,

상기 블록 체인 클라이언트는,

상기 사용자들 각각의 개인 키를 이용하여 다중 서명을 생성하고, 상기 다중 서명을 슈노르 시그니처에 따라 결합하여 슈노르 서명을 생성하는 서명 검증 시스템.

청구항 13

제10항에 있어서,

상기 검증 공개 키는,

상기 다중 공개 키에 포함된 상기 사용자들 각각의 공개 키들을 슈노르 시그니처에 따라 결합하여 생성되는 서명 검증 시스템.

청구항 14

사용자들 각각의 서명들이 포함된 다중 서명을 생성하고, 상기 사용자들 각각의 공개 키들이 포함된 다중 공개 키를 생성하는 블록 체인 클라이언트; 및

상기 다중 서명을 이용하여 상기 다중 공개 키를 검증하고, 검증된 다중 공개 키를 저장하는 블록 체인 시스템을 포함하는 서명 검증 시스템.

청구항 15

제14항에 있어서,

상기 블록 체인 시스템은,

상기 다중 공개 키를 사용하여 상기 다중 서명을 복호화할 수 있는 경우, 상기 다중 공개 키를 검증된 것으로 결정하는 서명 검증 시스템.

청구항 16

제14항에 있어서,

상기 블록 체인 시스템은,

상기 다중 공개 키를 사용하여 상기 다중 서명을 복호화할 수 없는 경우, 상기 다중 공개 키를 검증 실패한 것으로 결정하는 서명 검증 시스템.

청구항 17

제14항에 있어서,

상기 블록 체인 시스템은,

상기 다중 공개 키에 포함된 상기 사용자들 각각의 공개 키들을 슈노르 시그니처에 따라 결합하여 검증 공개 키를 생성하고,

상기 검증 공개 키는,

상기 사용자들 각각의 서명들을 결합하여 생성한 슈노르 서명을 검증하기 위하여 사용되는 서명 검증 시스템.

발명의 설명

기술 분야

[0001] 본 발명은 서명 검증 방법 및 장치에 관한 것으로, 보다 구체적으로는 블록 체인 기반의 다중서명 방식에 슈노르 서명을 결합하여 등록 및 인증하는 방법 및 장치에 관한 것이다.

배경 기술

[0002] 종래의 블록 체인 기술은 사용자의 데이터를 저장하는 기능만 수행하였다. 그러나, 블록 체인 플랫폼의 다양화와 기술의 발전으로 인해 여러 블록 체인이 만들어지며 블록 체인이 나뉜 인터-체인 구조가 만들어지며 블록 체인 간 통신을 위한 인증 방법이 필요하게 되었다.

[0003] 종래의 블록 체인 간 데이터 전송은 제3의 신뢰된 기관을 통해서만 수행되며 블록 체인-블록 체인 간 데이터 통신을 위해서는 블록 체인 내 노드를 모두 인증하여 상호 신뢰가 필요하다.

[0004] 상호 신뢰를 위한 인증인 다중 서명은 여러 사람이 서명을 하는 방식으로 해당 데이터에 대한 생성, 처리, 전송, 저장, 수신 행위를 한 복수의 사용자를 보증하기 위한 인증을 보장한다.

[0005] 다중 서명 방식은 PKI를 기반으로 하여 개인 키를 이용한 복수의 서명 생성과 복수의 공개 키를 사용한 검증이 필요하다. 그러므로, 블록 체인 간 데이터 통신을 위한 인증을 위해 복수의 사용자의 공개 키를 관리하는 시스템 구축과 다중 전자서명의 검증 방법이 요구되나, 복수의 공개 키의 등록 시 검증과 전자 서명에 대한 검증에 시간이 소요되는 문제가 있다.

[0006] 따라서, 복수의 공개 키를 사용하여 검증하는 속도를 향상시키는 방법이 요청되고 있다.

발명의 내용

해결하려는 과제

[0007] 본 발명은 복수의 사용자 공개 키를 블록 체인에 등록하고, 저장한 복수의 사용자 공개 키들을 결합하여 생성한 검증 공개 키와 사용자들의 서명을 결합하여 생성한 슈노르 서명을 이용하여 사용자들의 다중 서명을 검증함으로써, 복수의 사용자가 서명한 데이터의 블록 체인 간 데이터 통신을 위한 인증을 빠르게 검증하는 방법 및 장치를 제공한다.

[0008] 또한, 본 발명은 블록 체인 간 데이터 통신을 위한 인증을 위해 다중 서명을 하는 방식으로 검증된 사용자의 공개 키들을 블록 체인 시스템에 저장함으로써, 인증 후 저장된 복수의 공개 키의 위변조를 하지 못하도록 하는 방법 및 장치를 제공한다.

과제의 해결 수단

[0009] 본 발명의 일실시예에 따른 서명 검증 방법은 사용자들 각각의 서명들을 결합하여 슈노르 서명을 생성하는 단계; 블록 체인 시스템에 등록된 다중 공개 키를 로드하는 단계; 상기 다중 공개 키에 포함된 공개 키들을 결합하여 검증 공개 키를 생성하는 단계; 및 상기 검증 공개 키로 상기 슈노르 서명을 검증하는 단계를 포함할 수 있다.

[0010] 본 발명의 일실시예에 따른 서명 검증 방법의 상기 다중 공개 키는, 상기 사용자들 각각의 서명들로 구성된 멀티 시그 서명을 복호화할 수 있는지 여부에 따라 검증된 후 상기 블록 체인 시스템에 기 등록될 수 있다.

[0011] 본 발명의 일실시예에 따른 서명 검증 방법의 상기 슈노르 서명을 생성하는 단계는, 상기 사용자들 각각의 개인 키를 이용하여 다중 서명을 생성하는 단계; 및 상기 다중 서명을 슈노르 시그니처에 따라 결합하여 슈노르 서명을 생성하는 단계를 포함할 수 있다.

[0012] 본 발명의 일실시예에 따른 서명 검증 방법의 상기 검증 공개 키는, 상기 다중 공개 키에 포함된 상기 사용자들 각각의 공개 키들을 슈노르 시그니처에 따라 결합하여 생성될 수 있다.

[0013] 본 발명의 일실시예에 따른 서명 검증을 위한 공개 키 등록 방법은 사용자들 각각의 서명들이 포함된 다중 서명을 생성하는 단계; 상기 사용자들 각각의 공개 키들이 포함된 다중 공개 키를 생성하는 단계; 및 상기 다중 서명 및 상기 다중 공개 키를 블록 체인 시스템에 전송하는 단계를 포함하고, 상기 블록 체인 시스템은, 상기 다중 서명을 이용하여 상기 다중 공개 키를 검증하고, 검증된 다중 공개 키를 저장할 수 있다.

[0014] 본 발명의 일실시예에 따른 서명 검증을 위한 공개 키 등록 방법의 상기 블록 체인 시스템은, 상기 다중 공개 키를 사용하여 상기 다중 서명을 복호화할 수 있는 경우, 상기 다중 공개 키를 검증된 것으로 결정할 수 있다.

[0015] 본 발명의 일실시예에 따른 서명 검증을 위한 공개 키 등록 방법의 상기 블록 체인 시스템은, 상기 다중 공개 키를 사용하여 상기 다중 서명을 복호화할 수 없는 경우, 상기 다중 공개 키를 검증 실패한 것으로 결정할 수 있다.

[0016] 본 발명의 일실시예에 따른 서명 검증을 위한 공개 키 등록 방법은 상기 다중 공개 키에 포함된 상기 사용자들 각각의 공개 키들을 슈노르 시그니처에 따라 결합하여 검증 공개 키를 생성하는 단계를 더 포함하고, 상기 검증 공개 키는, 상기 사용자들 각각의 서명들을 결합하여 생성한 슈노르 서명을 검증하기 위하여 사용될 수 있다.

[0017] 본 발명의 일실시예에 따른 서명 검증 시스템은 다중 공개 키가 등록된 블록 체인 시스템; 및 사용자들 각각의 서명들을 결합하여 슈노르 서명을 생성하고, 상기 다중 공개 키에 포함된 공개 키들을 결합하여 검증 공개 키를 생성하며, 상기 검증 공개 키로 상기 슈노르 서명을 검증하는 블록 체인 클라이언트를 포함할 수 있다.

[0018] 본 발명의 일실시예에 따른 서명 검증 시스템의 상기 다중 공개 키는, 상기 사용자들 각각의 서명들로 구성된

멀티 시그 서명을 복호화할 수 있는지 여부에 따라 검증된 후 상기 블록 체인 시스템에 기 등록될 수 있다.

- [0019] 본 발명의 일실시예에 따른 서명 검증 시스템의 상기 블록 체인 클라이언트는, 상기 사용자들 각각의 개인 키를 이용하여 다중 서명을 생성하고, 상기 다중 서명을 슈노르 시그니처에 따라 결합하여 슈노르 서명을 생성할 수 있다.
- [0020] 본 발명의 일실시예에 따른 서명 검증 시스템의 상기 검증 공개 키는, 상기 다중 공개 키에 포함된 상기 사용자들 각각의 공개 키들을 슈노르 시그니처에 따라 결합하여 생성될 수 있다.
- [0021] 본 발명의 일실시예에 따른 서명 검증 시스템은 사용자들 각각의 서명들이 포함된 다중 서명을 생성하고, 상기 사용자들 각각의 공개 키들이 포함된 다중 공개 키를 생성하는 블록 체인 클라이언트; 및 상기 다중 서명을 이용하여 상기 다중 공개 키를 검증하고, 검증된 다중 공개 키를 저장하는 블록 체인 시스템을 포함할 수 있다.
- [0022] 본 발명의 일실시예에 따른 서명 검증 시스템의 상기 블록 체인 시스템은, 상기 다중 공개 키를 사용하여 상기 다중 서명을 복호화할 수 있는 경우, 상기 다중 공개 키를 검증된 것으로 결정할 수 있다.
- [0023] 본 발명의 일실시예에 따른 서명 검증 시스템의 상기 블록 체인 시스템은, 상기 다중 공개 키를 사용하여 상기 다중 서명을 복호화할 수 없는 경우, 상기 다중 공개 키를 검증 실패한 것으로 결정할 수 있다.
- [0024] 본 발명의 일실시예에 따른 서명 검증 시스템의 상기 블록 체인 시스템은, 상기 다중 공개 키에 포함된 상기 사용자들 각각의 공개 키들을 슈노르 시그니처에 따라 결합하여 검증 공개 키를 생성하고, 상기 검증 공개 키는, 상기 사용자들 각각의 서명들을 결합하여 생성한 슈노르 서명을 검증하기 위하여 사용될 수 있다.

발명의 효과

- [0025] 본 발명의 일실시예에 의하면, 복수의 사용자 공개 키를 블록 체인에 등록하고, 저장한 복수의 사용자 공개 키들을 결합하여 생성한 검증 공개 키와 사용자들의 서명을 결합하여 생성한 슈노르 서명을 이용하여 사용자들의 다중 서명을 검증함으로써, 복수의 사용자가 서명한 데이터의 블록 체인 간 데이터 통신을 위한 인증을 빠르게 검증할 수 있다.
- [0026] 또한, 본 발명의 일실시예에 의하면, 블록 체인 간 데이터 통신을 위한 인증을 위해 다중 서명을 하는 방식으로 검증된 사용자의 공개 키들을 블록 체인 시스템에 저장함으로써, 인증 후 저장된 복수의 공개 키의 위변조를 하지 못하도록 할 수 있다.
- [0027] 그리고, 본 발명의 일실시예에 의하면, 블록 체인 간 멀티 시그와 슈노르 시그니처 방법을 결합함으로써, 블록 체인-블록 체인 간 상호 인증의 검증속도가 향상된 서명 검증 시스템을 제공할 수 있다.

도면의 간단한 설명

- [0028] 도 1은 본 발명의 제1실시예에 따른 서명 검증 시스템을 도시한 도면이다.
- 도 2는 본 발명의 제1실시예에 따른 서명 검증 시스템의 공개 키 등록 과정을 도시한 도면이다.
- 도 3은 본 발명의 제1실시예에 따른 서명 검증 시스템의 서명 검증 과정을 도시한 도면이다.
- 도 4는 본 발명의 제2실시예에 따른 서명 검증 시스템을 도시한 도면이다.
- 도 5는 본 발명의 제2실시예에 따른 서명 검증 시스템의 공개 키 등록 과정을 도시한 도면이다.
- 도 6은 본 발명의 제2실시예에 따른 서명 검증 시스템의 서명 검증 과정을 도시한 도면이다.
- 도 7은 본 발명의 일실시예에 따른 공개 키 등록 방법을 도시한 플로우차트이다.
- 도 8은 본 발명의 일실시예에 따른 서명 검증 방법을 도시한 플로우차트이다.

발명을 실시하기 위한 구체적인 내용

- [0029] 이하에서, 첨부된 도면을 참조하여 실시예들을 상세하게 설명한다. 그러나, 실시예들에는 다양한 변경이 가해질 수 있어서 특허출원의 권리 범위가 이러한 실시예들에 의해 제한되거나 한정되는 것은 아니다. 실시예들에 대한 모든 변경, 균등물 내지 대체물이 권리 범위에 포함되는 것으로 이해되어야 한다.
- [0030] 실시예에서 사용한 용어는 단지 설명을 목적으로 사용된 것으로, 한정하려는 의도로 해석되어서는 안된다. 단

수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 명세서에서, "포함하다" 또는 "가지다" 등의 용어는 명세서 상에 기재된 특징, 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

- [0031] 또한, 첨부 도면을 참조하여 설명함에 있어, 도면 부호에 관계없이 동일한 구성 요소는 동일한 참조부호를 부여하고 이에 대한 중복되는 설명은 생략하기로 한다. 실시예를 설명함에 있어서 관련된 공지 기술에 대한 구체적인 설명이 실시예의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우 그 상세한 설명을 생략한다.
- [0032] 이하, 본 발명의 실시예를 첨부된 도면을 참조하여 상세하게 설명한다.
- [0033] 도 1은 본 발명의 제1실시예에 따른 서명 검증 시스템을 도시한 도면이다.
- [0034] 서명 검증 시스템은 도 1에 도시된 바와 같이 제1 블록 체인 시스템(110), 블록 체인 클라이언트(120), 및 제2 블록 체인 시스템(130)을 포함할 수 있다.
- [0035] 제1 블록 체인 시스템(110)은 공개 키가 저장되는 제2 블록 체인 시스템(130)과 블록 체인 클라이언트(120)를 통한 데이터 통신을 수행할 수 있다. 이때, 제1 블록 체인 시스템(110)은 블록 체인 노드(111, 112, 113)들로 구성되며, 블록 체인 노드(111, 112, 113)들 각각은 사용자 단말과 연결될 수 있다.
- [0036] 블록 체인 노드(111, 112, 113)들에 접속 가능한 사용자 단말을 사용하는 사용자들 중 적어도 하나의 사용자를 제2 블록 체인 시스템(130)에 등록하는 경우, 서명 검증을 위한 공개 키 등록 과정이 수행될 수 있다.
- [0037] 이때, 블록 체인 노드(111, 112, 113)들 각각은 사용자 단말로부터 사용자의 개인 키와 공개 키를 수신하여 저장할 수 있다. 또한, 블록 체인 노드(111, 112, 113)들 각각은 사용자의 개인 키를 이용하여 생성한 사용자의 서명, 및 사용자의 공개 키를 블록 체인 클라이언트(120)로 전송할 수 있다.
- [0038] 블록 체인 클라이언트(120)는 사용자들 각각의 서명들이 포함된 다중 서명을 생성할 수 있다. 또한, 블록 체인 클라이언트(120)는 사용자들 각각의 공개 키들이 포함된 다중 공개 키를 생성할 수 있다. 그리고, 블록 체인 클라이언트(120)는 생성한 다중 서명 및 다중 공개 키를 제2 블록 체인 시스템(130)에 전송할 수 있다.
- [0039] 제2 블록 체인 시스템(130)의 블록 체인 노드들은 블록 체인 클라이언트(120)로부터 수신한 다중 서명을 이용하여 다중 공개 키를 검증할 수 있다. 그리고, 제2 블록 체인 시스템(130)의 블록 체인 노드들은 검증된 다중 공개 키를 저장할 수 있다.
- [0040] 구체적으로, 블록 체인 시스템(130)의 블록 체인 노드들은 클라이언트(120)가 전송한 다중 공개 키를 사용하여 다중 서명에 대한 복호화를 시도할 수 있다. 블록 체인 클라이언트(120)가 전송한 다중 공개 키를 사용하여 다중 서명을 복호화할 수 있는 경우, 제2 블록 체인 시스템(130)의 블록 체인 노드들은 다중 공개 키를 검증된 것으로 결정할 수 있다. 또한, 블록 체인 클라이언트(120)가 전송한 다중 공개 키를 사용하여 다중 서명을 복호화할 수 없는 경우, 제2 블록 체인 시스템(130)의 블록 체인 노드들은 다중 공개 키를 검증 실패한 것으로 결정할 수 있다.
- [0041] 그리고, 제2 블록 체인 시스템(130)의 블록 체인 노드들은 다중 공개 키에 포함된 사용자들 각각의 공개 키들을 슈노르 시그니처에 따라 결합하여 검증 공개 키를 생성할 수 있다. 이때, 검증 공개 키는 사용자들 각각의 서명들을 결합하여 생성한 슈노르 서명을 검증하기 위하여 사용될 수 있다. 또한, 실시예에 따라 제2 블록 체인 시스템(130)의 블록 체인 노드들이 검증 공개 키를 생성하지 않고, 다중 공개 키만을 저장할 수도 있다.
- [0042] 서명 검증 방법이 수행되는 경우, 블록 체인 클라이언트(120)는 사용자들 각각의 서명들을 결합하여 슈노르 서명을 생성할 수 있다. 이때, 블록 체인 클라이언트(120)는 사용자들 각각의 개인 키를 이용하여 사용자들 각각의 서명들이 포함된 다중 서명을 생성할 수 있다. 그리고, 블록 체인 클라이언트(120)는 다중 서명을 슈노르 시그니처에 따라 결합하여 슈노르 서명을 생성할 수 있다.
- [0043] 다음으로, 블록 체인 클라이언트(120)는 제2 블록 체인 시스템(130)에 등록된 다중 공개 키를 로드할 수 있다. 이때, 블록 체인 클라이언트(120)는 다중 공개 키에 포함된 공개 키들을 결합하여 검증 공개 키를 생성할 수 있다. 이때, 블록 체인 클라이언트(120)는 다중 공개 키에 포함된 사용자들 각각의 공개 키들을 슈노르 시그니처에 따라 결합하여 검증 공개 키를 생성할 수 있다.
- [0044] 또한, 제2 블록 체인 시스템(130)의 블록 체인 노드들이 검증 공개 키를 생성한 경우, 블록 체인 클라이언트(120)는 제2 블록 체인 시스템(130)에서 생성되어 저장된 검증 공개 키를 로드할 수 있다.

- [0045] 그 다음으로, 블록 체인 클라이언트(120)는 검증 공개 키로 슈노르 서명을 검증할 수 있다.
- [0046] 서명 검증 시스템은 복수의 사용자 공개 키를 블록 체인에 등록하고, 저장한 복수의 사용자 공개 키들을 결합하여 생성한 검증 공개 키와 사용자들의 서명을 결합하여 생성한 슈노르 서명을 이용하여 사용자들의 다중 서명을 검증함으로써, 복수의 사용자가 서명한 데이터의 블록 체인 간 데이터 통신을 위한 인증을 빠르게 검증할 수 있다.
- [0047] 또한, 서명 검증 시스템은 블록 체인 간 데이터 통신을 위한 인증을 위해 다중 서명을 하는 방식으로 검증된 사용자의 공개 키들을 블록 체인 시스템에 저장함으로써, 인증 후 저장된 복수의 공개 키의 위변조를 하지 못하도록 할 수 있다.
- [0048] 그리고, 본 발명은 블록 체인 간 멀티 시그와 슈노르 시그니처 방법을 결합함으로써, 블록 체인-블록 체인 간 상호 인증의 검증속도가 향상된 서명 검증 시스템을 제공할 수 있다.
- [0049] 도 2는 본 발명의 제1실시예에 따른 서명 검증 시스템의 공개 키 등록 과정을 도시한 도면이다.
- [0050] 블록 체인 노드(111)는 제1 사용자의 사용자 단말로부터 제1 사용자의 개인 키(211)와 공개 키(212)를 수신하여 저장할 수 있다. 그리고, 블록 체인 노드(111)는 제1 사용자의 개인 키(211)를 이용하여 제1 사용자의 서명 1(241)을 생성할 수 있다.
- [0051] 블록 체인 노드(112)는 제2 사용자의 사용자 단말로부터 제2 사용자의 개인 키(221)와 공개 키(222)를 수신하여 저장할 수 있다. 그리고, 블록 체인 노드(112)는 제2 사용자의 개인 키(221)를 이용하여 제2 사용자의 서명 2(242)를 생성할 수 있다.
- [0052] 블록 체인 노드(113)는 제3 사용자의 사용자 단말로부터 제3 사용자의 개인 키(231)와 공개 키(232)를 수신하여 저장할 수 있다. 그리고, 블록 체인 노드(113)는 제3 사용자의 개인 키(231)를 이용하여 제3 사용자의 서명 3(243)을 생성할 수 있다.
- [0053] 블록 체인 클라이언트(120)는 블록 체인 노드(111)로부터 제1 사용자의 공개 키(212) 및 제1 사용자의 서명 1(241)을 수신할 수 있다. 또한, 블록 체인 클라이언트(120)는 블록 체인 노드(112)로부터 제2 사용자의 공개 키(222) 및 제2 사용자의 서명 2(242)를 수신할 수 있다. 그리고, 블록 체인 클라이언트(120)는 블록 체인 노드(113)로부터 제3 사용자의 공개 키(232) 및 제3 사용자의 서명 3(243)을 수신할 수 있다.
- [0054] 이때, 블록 체인 클라이언트(120)는 도 2에 도시된 바와 같이 서명 1(241), 서명 2(242), 및 서명 3(243)이 포함된 다중 서명인 멀티 시그(multi-sig)(240)를 생성할 수 있다. 또한, 블록 체인 클라이언트(120)는 공개 키(212), 공개 키(222), 및 공개 키(232)가 포함된 다중 공개 키를 생성할 수 있다. 그리고, 블록 체인 클라이언트(120)는 생성한 멀티 시그(240) 및 다중 공개 키를 제2 블록 체인 시스템(130)에 전송할 수 있다.
- [0055] 제2 블록 체인 시스템(130)의 블록 체인 노드들은 멀티 시그(240)를 이용하여 다중 공개 키를 검증할 수 있다. 이때, 제2 블록 체인 시스템(130)의 블록 체인 노드들은 다중 공개 키를 사용하여 멀티 시그(240)의 복호화를 시도할 수 있다.
- [0056] 다중 공개 키를 사용하여 멀티 시그(240)를 복호화할 수 있는 경우, 제2 블록 체인 시스템(130)의 블록 체인 노드들은 다중 공개 키가 검증된 것으로 결정하고, 검증된 다중 공개 키에 포함된 공개 키(212), 공개 키(222), 및 공개 키(232)를 저장할 수 있다. 이때, 제2 블록 체인 시스템(130)의 블록 체인 노드들은 공개 키(212), 공개 키(222), 및 공개 키(232)를 슈노르 시그니처에 따라 결합하여 검증 공개 키(250)를 생성하고 저장할 수 있다.
- [0057] 다중 공개 키를 사용하여 멀티 시그(240)를 복호화할 수 없는 경우, 제2 블록 체인 시스템(130)의 블록 체인 노드들은 다중 공개 키를 검증 실패한 것으로 결정하고 공개 키(212), 공개 키(222), 및 공개 키(232)를 저장하지 않을 수 있다.
- [0058] 도 3은 본 발명의 제1실시예에 따른 서명 검증 시스템의 서명 검증 과정을 도시한 도면이다.
- [0059] 블록 체인 클라이언트(120)는 서명 1(241), 서명 2(242), 및 서명 3(243)을 결합하여 슈노르 서명(300)을 생성할 수 있다.
- [0060] 다음으로, 블록 체인 클라이언트(120)는 제2 블록 체인 시스템(130)에 등록된 다중 공개 키를 로드할 수 있다. 이때, 블록 체인 클라이언트(120)는 다중 공개 키에 포함된 공개 키(221, 222, 232)들을 결합하여 검증 공개 키

(250)를 생성할 수 있다. 이때, 블록 체인 클라이언트(120)는 공개 키(212), 공개 키(222), 및 공개 키(232)를 슈노르 시그니처에 따라 결합하여 검증 공개 키(250)를 생성할 수 있다.

[0061] 또한, 제2 블록 체인 시스템(130)의 블록 체인 노드들이 검증 공개 키(250)를 생성한 경우, 블록 체인 클라이언트(120)는 제2 블록 체인 시스템(130)에서 생성되어 저장된 검증 공개 키(250)를 로드할 수 있다.

[0062] 그 다음으로, 블록 체인 클라이언트(120)는 검증 공개 키(250)로 슈노르 서명(300)을 검증할 수 있다. 구체적으로, 블록 체인 클라이언트(120)는 검증 공개 키(250)를 이용하여 슈노르 서명(300)의 복호화를 시도할 수 있다.

[0063] 그리고, 검증 공개 키(250)를 사용하여 슈노르 서명(300)을 복호화할 수 있는 경우, 블록 체인 클라이언트(120)는 슈노르 서명(300)이 검증된 것으로 결정할 수 있다. 반면, 검증 공개 키(250)를 사용하여 슈노르 서명(300)을 복호화할 수 없는 경우, 블록 체인 클라이언트(120)는 슈노르 서명(300)에 대한 검증이 실패한 것으로 결정할 수 있다.

[0064] 도 4는 본 발명의 제2실시예에 따른 서명 검증 시스템을 도시한 도면이다.

[0065] 서명 검증 시스템은 도 4에 도시된 바와 같이 사용자 단말(411, 412, 413)들, 블록 체인 클라이언트(420), 및 블록 체인 시스템(430)을 포함할 수 있다.

[0066] 블록 체인 시스템(430)에 사용자 단말(411, 412, 413)들 각각을 사용하는 사용자들 중 적어도 하나의 사용자를 등록하는 경우, 서명 검증을 위한 공개 키 등록 과정이 수행될 수 있다.

[0067] 이때, 사용자 단말(411, 412, 413)들 각각은 사용자의 개인 키와 공개 키를 저장할 수 있다. 또한, 사용자 단말(411, 412, 413)들 각각은 사용자의 개인 키를 이용하여 생성한 사용자의 서명, 및 사용자의 공개 키를 블록 체인 클라이언트(420)로 전송할 수 있다.

[0068] 블록 체인 클라이언트(420)는 사용자들 각각의 서명들이 포함된 다중 서명을 생성할 수 있다. 또한, 블록 체인 클라이언트(420)는 사용자들 각각의 공개 키들이 포함된 다중 공개 키를 생성할 수 있다. 그리고, 블록 체인 클라이언트(420)는 생성한 다중 서명 및 다중 공개 키를 블록 체인 시스템(430)에 전송할 수 있다.

[0069] 블록 체인 시스템(430)의 블록 체인 노드들은 블록 체인 클라이언트(420)로부터 수신한 다중 서명을 이용하여 다중 공개 키를 검증할 수 있다. 그리고, 블록 체인 시스템(430)의 블록 체인 노드들은 검증된 다중 공개 키를 저장할 수 있다.

[0070] 구체적으로, 블록 체인 시스템(430)의 블록 체인 노드들은 클라이언트(420)가 전송한 다중 공개 키를 사용하여 다중 서명에 대한 복호화를 시도할 수 있다. 블록 체인 클라이언트(420)가 전송한 다중 공개 키를 사용하여 다중 서명을 복호화할 수 있는 경우, 블록 체인 시스템(430)의 블록 체인 노드들은 다중 공개 키를 검증된 것으로 결정할 수 있다. 또한, 블록 체인 클라이언트(420)가 전송한 다중 공개 키를 사용하여 다중 서명을 복호화할 수 없는 경우, 블록 체인 시스템(430)의 블록 체인 노드들은 다중 공개 키를 검증 실패한 것으로 결정할 수 있다.

[0071] 그리고, 블록 체인 시스템(430)의 블록 체인 노드들은 다중 공개 키에 포함된 사용자들 각각의 공개 키들을 슈노르 시그니처에 따라 결합하여 검증 공개 키를 생성할 수 있다. 이때, 검증 공개 키는 사용자들 각각의 서명들을 결합하여 생성한 슈노르 서명을 검증하기 위하여 사용될 수 있다. 또한, 실시예에 따라 블록 체인 시스템(430)의 블록 체인 노드들이 검증 공개 키를 생성하지 않고, 다중 공개 키만을 저장할 수도 있다.

[0072] 서명 검증 방법이 수행되는 경우, 블록 체인 클라이언트(420)는 사용자 단말(411, 412, 413)들로부터 수신한 사용자들 각각의 서명들을 결합하여 슈노르 서명을 생성할 수 있다. 이때, 블록 체인 클라이언트(420)는 사용자들 각각의 개인 키를 이용하여 사용자들 각각의 서명들이 포함된 다중 서명을 생성할 수 있다. 그리고, 블록 체인 클라이언트(420)는 다중 서명을 슈노르 시그니처에 따라 결합하여 슈노르 서명을 생성할 수 있다.

[0073] 다음으로, 블록 체인 클라이언트(420)는 블록 체인 시스템(430)에 등록된 다중 공개 키를 로드할 수 있다. 이때, 블록 체인 클라이언트(420)는 다중 공개 키에 포함된 공개 키들을 결합하여 검증 공개 키를 생성할 수 있다. 이때, 블록 체인 클라이언트(420)는 다중 공개 키에 포함된 사용자들 각각의 공개 키들을 슈노르 시그니처에 따라 결합하여 검증 공개 키를 생성할 수 있다.

[0074] 또한, 블록 체인 시스템(430)의 블록 체인 노드들이 검증 공개 키를 생성한 경우, 블록 체인 클라이언트(420)는 블록 체인 시스템(430)에서 생성되어 저장된 검증 공개 키를 로드할 수 있다.

- [0075] 그 다음으로, 블록 체인 클라이언트(420)는 검증 공개 키로 슈노르 서명을 검증할 수 있다.
- [0076] 서명 검증 시스템은 복수의 사용자 공개 키를 블록 체인에 등록하고, 저장한 복수의 사용자 공개 키들을 결합하여 생성한 검증 공개 키와 사용자들의 서명을 결합하여 생성한 슈노르 서명을 이용하여 사용자들의 다중 서명을 검증함으로써, 복수의 사용자가 서명한 데이터를 검증할 수 있다.
- [0077] 또한, 서명 검증 시스템은 데이터 인증을 위해 다중 서명을 하는 방식으로 검증된 사용자의 공개 키들을 블록 체인 시스템에 저장함으로써, 인증 후 저장된 복수의 공개 키의 위변조를 하지 못하도록 할 수 있다.
- [0078] 도 5는 본 발명의 제2실시예에 따른 서명 검증 시스템의 공개 키 등록 과정을 도시한 도면이다.
- [0079] 사용자 단말(411)은 제1 사용자의 개인 키(511)와 공개 키(512)를 저장하고, 제1 사용자의 개인 키(511)를 이용하여 제1 사용자의 서명 1(513)을 생성할 수 있다. 또한, 사용자 단말(412)은 제2 사용자의 개인 키(521)와 공개 키(522)를 저장하고, 제2 사용자의 개인 키(521)를 이용하여 제2 사용자의 서명 2(523)을 생성할 수 있다. 그리고, 사용자 단말(413)은 제3 사용자의 개인 키(531)와 공개 키(532)를 저장하고, 제3 사용자의 개인 키(531)를 이용하여 제3 사용자의 서명 3(533)을 생성할 수 있다.
- [0080] 블록 체인 클라이언트(420)는 사용자 단말(411)로부터 제1 사용자의 공개 키(512) 및 제1 사용자의 서명 1(513)을 수신할 수 있다. 또한, 블록 체인 클라이언트(420)는 사용자 단말(412)로부터 제2 사용자의 공개 키(522) 및 제2 사용자의 서명 2(523)을 수신할 수 있다. 그리고, 블록 체인 클라이언트(420)는 사용자 단말(413)로부터 제3 사용자의 공개 키(532) 및 제3 사용자의 서명 3(533)을 수신할 수 있다.
- [0081] 이때, 블록 체인 클라이언트(420)는 도 2에 도시된 바와 같이 서명 1(513), 서명 2(523), 및 서명 3(533)이 포함된 다중 서명인 멀티 시그(multi-sig)(530)를 생성할 수 있다. 또한, 블록 체인 클라이언트(420)는 공개 키(512), 공개 키(522), 및 공개 키(532)가 포함된 다중 공개 키를 생성할 수 있다. 그리고, 블록 체인 클라이언트(420)는 생성한 멀티 시그(530) 및 다중 공개 키를 블록 체인 시스템(430)에 전송할 수 있다.
- [0082] 블록 체인 시스템(430)의 블록 체인 노드들은 멀티 시그(530)를 이용하여 다중 공개 키를 검증할 수 있다. 이때, 블록 체인 시스템(430)의 블록 체인 노드들은 다중 공개 키를 사용하여 멀티 시그(530)의 복호화를 시도할 수 있다.
- [0083] 다중 공개 키를 사용하여 멀티 시그(530)를 복호화할 수 있는 경우, 블록 체인 시스템(430)의 블록 체인 노드들은 다중 공개 키가 검증된 것으로 결정하고, 검증된 다중 공개 키에 포함된 공개 키(512), 공개 키(522), 및 공개 키(532)를 저장할 수 있다.
- [0084] 다중 공개 키를 사용하여 멀티 시그(530)를 복호화할 수 없는 경우, 블록 체인 시스템(430)의 블록 체인 노드들은 다중 공개 키를 검증 실패한 것으로 결정하고 공개 키(512), 공개 키(522), 및 공개 키(532)를 저장하지 않을 수 있다.
- [0085] 도 6은 본 발명의 제2실시예에 따른 서명 검증 시스템의 서명 검증 과정을 도시한 도면이다.
- [0086] 블록 체인 클라이언트(420)는 블록 체인 시스템(430)에 등록된 다중 공개 키를 로드할 수 있다. 이때, 블록 체인 클라이언트(420)는 다중 공개 키에 포함된 공개 키(521, 222, 232)들을 결합하여 검증 공개 키(610)를 생성할 수 있다. 이때, 블록 체인 클라이언트(420)는 공개 키(512), 공개 키(522), 및 공개 키(532)를 슈노르 시그니처에 따라 결합하여 검증 공개 키(620)를 생성할 수 있다.
- [0087] 다음으로, 블록 체인 클라이언트(420)는 서명 1(513), 서명 2(523), 및 서명 3(533)을 결합하여 슈노르 서명(620)을 생성할 수 있다.
- [0088] 그 다음으로, 블록 체인 클라이언트(420)는 검증 공개 키(610)로 슈노르 서명(620)을 검증할 수 있다. 구체적으로, 블록 체인 클라이언트(420)는 검증 공개 키(610)를 이용하여 슈노르 서명(620)의 복호화를 시도할 수 있다.
- [0089] 그리고, 검증 공개 키(610)를 사용하여 슈노르 서명(620)을 복호화할 수 있는 경우, 블록 체인 클라이언트(420)는 슈노르 서명(620)이 검증된 것으로 결정할 수 있다. 반면, 검증 공개 키(610)를 사용하여 슈노르 서명(620)을 복호화할 수 없는 경우, 블록 체인 클라이언트(420)는 슈노르 서명(620)에 대한 검증이 실패한 것으로 결정할 수 있다.
- [0090] 도 7은 본 발명의 일실시예에 따른 공개 키 등록 방법을 도시한 플로우차트이다.

- [0091] 단계(710)에서 블록 체인 클라이언트(120), 또는 블록 체인 클라이언트(420)는 사용자들 각각의 서명들이 포함된 다중 서명을 생성할 수 있다. 또한, 블록 체인 클라이언트(120), 또는 블록 체인 클라이언트(420)는 사용자들 각각의 공개 키들이 포함된 다중 공개 키를 생성할 수 있다.
- [0092] 단계(720)에서 블록 체인 클라이언트(120)는 단계(710)에서 생성한 다중 서명 및 다중 공개 키를 제2 블록 체인 시스템(130)에 전송할 수 있다. 또한, 단계(720)에서 블록 체인 클라이언트(420)는 단계(710)에서 생성한 다중 서명 및 다중 공개 키를 블록 체인 시스템(430)에 전송할 수 있다.
- [0093] 단계(730)에서 제2 블록 체인 시스템(130)의 블록 체인 노드들, 또는 블록 체인 시스템(430)의 블록 체인 노드들은 단계(720)에서 수신한 다중 서명을 이용하여 다중 공개 키를 검증할 수 있다.
- [0094] 구체적으로, 제2 블록 체인 시스템(130)의 블록 체인 노드들, 또는 블록 체인 시스템(430)의 블록 체인 노드들은 단계(720)에서 수신한 다중 공개 키를 사용하여 다중 서명에 대한 복호화를 시도할 수 있다.
- [0095] 단계(740)에서 제2 블록 체인 시스템(130)의 블록 체인 노드들, 또는 블록 체인 시스템(430)의 블록 체인 노드들은 단계(730)에서 다중 공개 키의 검증이 성공하였는지 여부를 확인할 수 있다. 단계(720)에서 수신한 다중 공개 키를 사용하여 다중 서명을 복호화할 수 있는 경우, 제2 블록 체인 시스템(130)의 블록 체인 노드들, 또는 블록 체인 시스템(430)의 블록 체인 노드들은 다중 공개 키가 검증된 것으로 판단하고 단계(760)를 수행할 수 있다. 단계(720)에서 수신한 다중 공개 키를 사용하여 다중 서명을 복호화할 수 있는 경우, 제2 블록 체인 시스템(130)의 블록 체인 노드들, 또는 블록 체인 시스템(430)의 블록 체인 노드들은 다중 공개 키에 대한 검증이 실패한 것으로 판단하고 단계(750)를 수행할 수 있다.
- [0096] 단계(750)에서 제2 블록 체인 시스템(130)의 블록 체인 노드들, 또는 블록 체인 시스템(430)의 블록 체인 노드들은 검증 실패를 알리는 메시지를 사용자 단말에게 전송하고, 단계(720)에서 수신한 다중 공개 키를 저장하지 않을 수 있다.
- [0097] 단계(760)에서 제2 블록 체인 시스템(130)의 블록 체인 노드들, 또는 블록 체인 시스템(430)의 블록 체인 노드들은 단계(720)에서 수신한 다중 공개 키를 저장할 수 있다.
- [0098] 단계(770)에서 제2 블록 체인 시스템(130)의 블록 체인 노드들, 또는 블록 체인 시스템(430)의 블록 체인 노드들은 다중 공개 키에 포함된 사용자들 각각의 공개 키들을 슈노르 시그니처에 따라 결합하여 검증 공개 키를 생성할 수 있다. 이때, 검증 공개 키는 사용자들 각각의 서명들을 결합하여 생성한 슈노르 서명을 검증하기 위하여 사용될 수 있다. 또한, 실시예에 따라 단계(770)는 생략될 수도 있다.
- [0099] 도 8은 본 발명의 일실시예에 따른 서명 검증 방법을 도시한 플로우차트이다.
- [0100] 단계(810)에서 블록 체인 클라이언트(120), 또는 블록 체인 클라이언트(420)는 사용자들 각각의 서명들을 결합하여 슈노르 서명을 생성할 수 있다. 이때, 블록 체인 클라이언트(120), 또는 블록 체인 클라이언트(420)는 사용자들 각각의 개인 키를 이용하여 사용자들 각각의 서명들이 포함된 다중 서명을 생성할 수 있다. 그리고, 블록 체인 클라이언트(120), 또는 블록 체인 클라이언트(420)는 다중 서명을 슈노르 시그니처에 따라 결합하여 슈노르 서명을 생성할 수 있다.
- [0101] 단계(820)에서 블록 체인 클라이언트(120)는 제2 블록 체인 시스템(130)에 등록된 다중 공개 키를 로드할 수 있다. 또는, 블록 체인 클라이언트(420)는 블록 체인 시스템(430)에 등록된 다중 공개 키를 로드할 수 있다.
- [0102] 단계(830)에서 블록 체인 클라이언트(120), 또는 블록 체인 클라이언트(420)는 다중 공개 키에 포함된 사용자들 각각의 공개 키들을 슈노르 시그니처에 따라 결합하여 검증 공개 키를 생성할 수 있다. 제2 블록 체인 시스템(130)의 블록 체인 노드들이 검증 공개 키를 생성한 경우, 블록 체인 클라이언트(120)는 제2 블록 체인 시스템(130)에서 생성되어 저장된 검증 공개 키를 로드할 수 있다. 또한, 블록 체인 시스템(430)의 블록 체인 노드들이 검증 공개 키를 생성한 경우, 블록 체인 클라이언트(420)는 블록 체인 시스템(430)에서 생성되어 저장된 검증 공개 키를 로드할 수 있다.
- [0103] 단계(840)에서 블록 체인 클라이언트(120), 또는 블록 체인 클라이언트(420)는 단계(830)에서 생성, 또는 로드한 검증 공개 키로 단계(810)에서 생성한 슈노르 서명을 검증할 수 있다.
- [0104] 본 발명은 복수의 사용자 공개 키를 블록 체인에 등록하고, 저장한 복수의 사용자 공개 키들을 결합하여 생성한 검증 공개 키와 사용자들의 서명을 결합하여 생성한 슈노르 서명을 이용하여 사용자들의 다중 서명을 검증함으로써, 복수의 사용자가 서명한 데이터의 블록 체인 간 데이터 통신을 위한 인증을 빠르게 검증할 수 있다.

- [0105] 또한, 본 발명은 블록 체인 간 데이터 통신을 위한 인증을 위해 다중 서명을 하는 방식으로 검증된 사용자의 공개 키들을 블록 체인 시스템에 저장함으로써, 인증 후 저장된 복수의 공개 키의 위변조를 하지 못하도록 할 수 있다.
- [0106] 그리고, 본 발명은 블록 체인 간 멀티 시그와 슈노르 시그니처 방법을 결합함으로써, 블록 체인-블록 체인 간 상호 인증의 검증속도가 향상된 서명 검증 시스템을 제공할 수 있다.
- [0107] 한편, 본 발명에 따른 서명 검증 장치 또는 서명 검증 방법은 컴퓨터에서 실행될 수 있는 프로그램으로 작성되어 마그네틱 저장매체, 광학적 판독매체, 디지털 저장매체 등 다양한 기록 매체로도 구현될 수 있다.
- [0108] 본 명세서에 설명된 각종 기술들의 구현들은 디지털 전자 회로조직으로, 또는 컴퓨터 하드웨어, 펌웨어, 소프트웨어로, 또는 그들의 조합들로 구현될 수 있다. 구현들은 데이터 처리 장치, 예를 들어 프로그램가능 프로세서, 컴퓨터, 또는 다수의 컴퓨터들의 동작에 의한 처리를 위해, 또는 이 동작을 제어하기 위해, 컴퓨터 프로그램 제품, 예를 들어 기계 판독가능 저장 장치(컴퓨터 판독가능 매체)에서 유형적으로 구체화된 컴퓨터 프로그램으로서 구현될 수 있다. 상술한 컴퓨터 프로그램(들)과 같은 컴퓨터 프로그램은 컴파일된 또는 인터프리트된 언어들을 포함하는 임의의 형태의 프로그래밍 언어로 기록될 수 있고, 독립형 프로그램으로서 또는 모듈, 구성요소, 서브루틴, 또는 컴퓨팅 환경에서의 사용에 적절한 다른 유닛으로서 포함하는 임의의 형태로 전개될 수 있다. 컴퓨터 프로그램은 하나의 사이트에서 하나의 컴퓨터 또는 다수의 컴퓨터들 상에서 처리되도록 또는 다수의 사이트에 걸쳐 분배되고 통신 네트워크에 의해 상호 연결되도록 전개될 수 있다.
- [0109] 컴퓨터 프로그램의 처리에 적절한 프로세서들은 예로서, 범용 및 특수 목적 마이크로프로세서들 둘 다, 및 임의의 종류의 디지털 컴퓨터의 임의의 하나 이상의 프로세서들을 포함한다. 일반적으로, 프로세서는 판독 전용 메모리 또는 랜덤 액세스 메모리 또는 둘 다로부터 명령어들과 데이터를 수신할 것이다. 컴퓨터의 요소들은 명령어들을 실행하는 적어도 하나의 프로세서 및 명령어들과 데이터를 저장하는 하나 이상의 메모리 장치들을 포함할 수 있다. 일반적으로, 컴퓨터는 데이터를 저장하는 하나 이상의 대량 저장 장치들, 예를 들어 자기, 자기-광 디스크들, 또는 광 디스크들을 포함할 수 있거나, 이것들로부터 데이터를 수신하거나 이것들에 데이터를 송신하거나 또는 양쪽으로 되도록 결합될 수도 있다. 컴퓨터 프로그램 명령어들과 데이터를 구체화하는데 적절한 정보 캐리어들은 예로서 반도체 메모리 장치들, 예를 들어, 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(Magnetic Media), CD-ROM(Compact Disk Read Only Memory), DVD(Digital Video Disk)와 같은 광 기록 매체(Optical Media), 플롭티컬 디스크(Floptical Disk)와 같은 자기-광 매체(Magneto-Optical Media), 롬(ROM, Read Only Memory), 램(RAM, Random Access Memory), 플래시 메모리, EPROM(Erasable Programmable ROM), EEPROM(Electrically Erasable Programmable ROM) 등을 포함한다. 프로세서 및 메모리는 특수 목적 논리 회로조직에 의해 보충되거나, 이에 포함될 수 있다.
- [0110] 또한, 컴퓨터 판독가능 매체는 컴퓨터에 의해 액세스될 수 있는 임의의 가용매체일 수 있고, 컴퓨터 저장매체를 모두 포함할 수 있다.
- [0111] 본 명세서는 다수의 특정한 구현물의 세부사항들을 포함하지만, 이들은 어떠한 발명이나 청구 가능한 것의 범위에 대해서도 제한적인 것으로서 이해되어서는 안되며, 오히려 특정한 발명의 특정한 실시형태에 특유할 수 있는 특징들에 대한 설명으로서 이해되어야 한다. 개별적인 실시형태의 문맥에서 본 명세서에 기술된 특정한 특징들은 단일 실시형태에서 조합하여 구현될 수도 있다. 반대로, 단일 실시형태의 문맥에서 기술한 다양한 특징들 역시 개별적으로 혹은 어떠한 적절한 하위 조합으로도 복수의 실시형태에서 구현 가능하다. 나아가, 특징들이 특정한 조합으로 동작하고 초기에 그와 같이 청구된 바와 같이 묘사될 수 있지만, 청구된 조합으로부터의 하나 이상의 특징들은 일부 경우에 그 조합으로부터 배제될 수 있으며, 그 청구된 조합은 하위 조합이나 하위 조합의 변형물로 변경될 수 있다.
- [0112] 마찬가지로, 특정한 순서로 도면에서 동작들을 묘사하고 있지만, 이는 바람직한 결과를 얻기 위하여 도시된 그 특정한 순서나 순차적인 순서대로 그러한 동작들을 수행하여야 한다거나 모든 도시된 동작들이 수행되어야 하는 것으로 이해되어서는 안 된다. 특정한 경우, 멀티태스킹과 병렬 프로세싱이 유리할 수 있다. 또한, 상술한 실시형태의 다양한 장치 컴포넌트의 분리는 그러한 분리를 모든 실시형태에서 요구하는 것으로 이해되어서는 안되며, 설명한 프로그램 컴포넌트와 장치들은 일반적으로 단일의 소프트웨어 제품으로 함께 통합되거나 다중 소프트웨어 제품에 패키징 될 수 있다는 점을 이해하여야 한다.
- [0113] 한편, 본 명세서와 도면에 개시된 본 발명의 실시 예들은 이해를 돕기 위해 특정 예를 제시한 것에 지나지 않으며, 본 발명의 범위를 한정하고자 하는 것은 아니다. 여기에 개시된 실시 예들 이외에도 본 발명의 기술적 사상

에 바탕을 둔 다른 변형 예들이 실시 가능하다는 것은, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 자명한 것이다.

부호의 설명

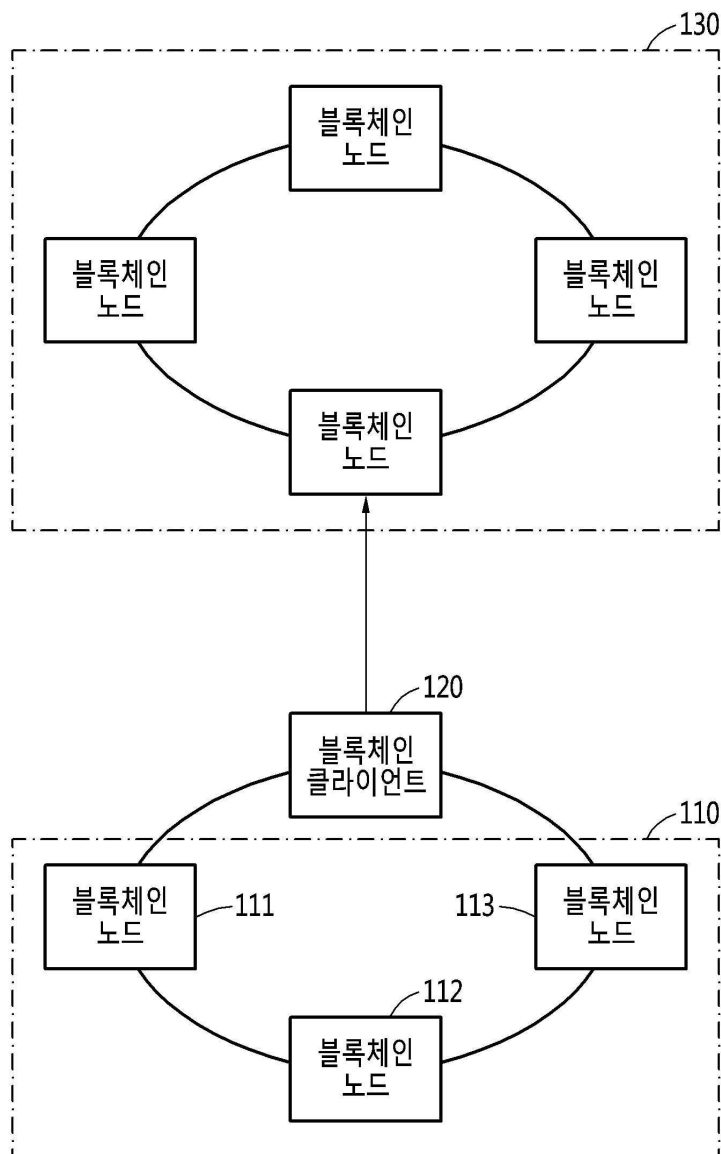
110: 제1 블록 체인 시스템

120: 블록 체인 클라이언트

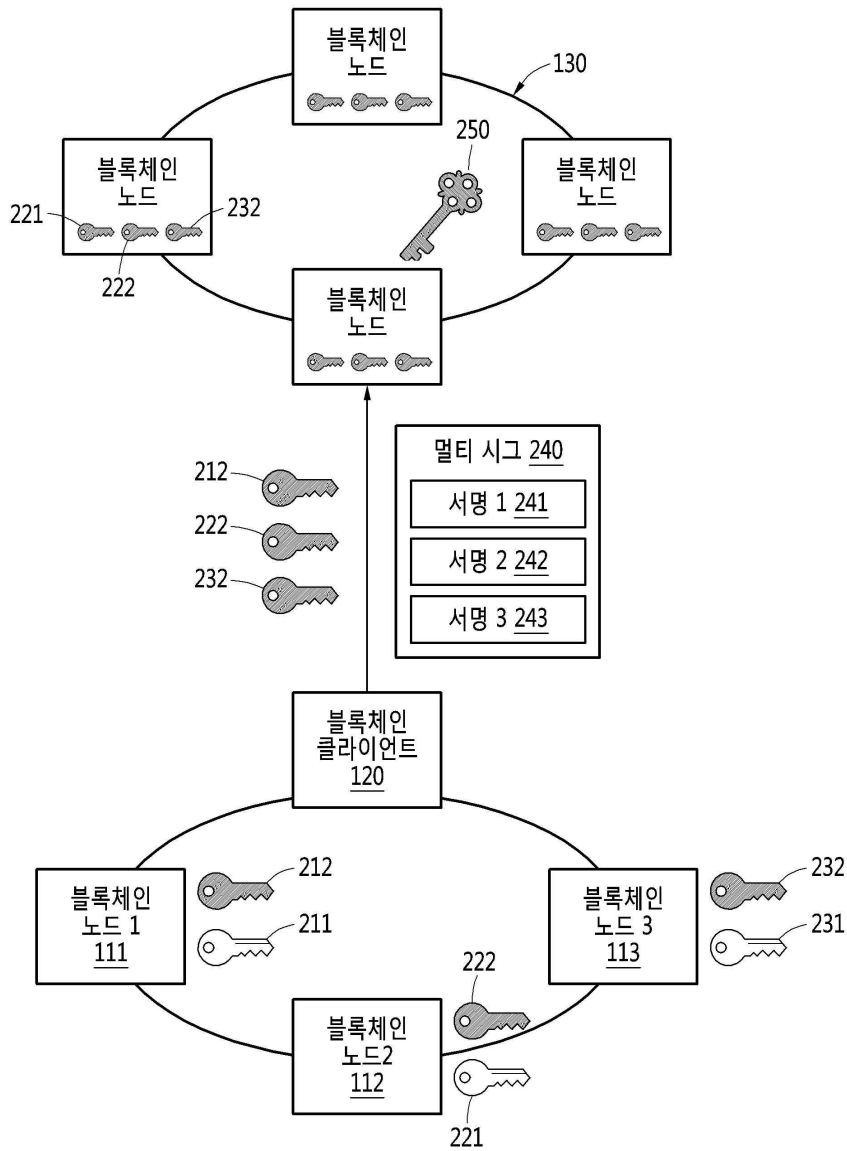
130: 제2 블록 체인 시스템

도면

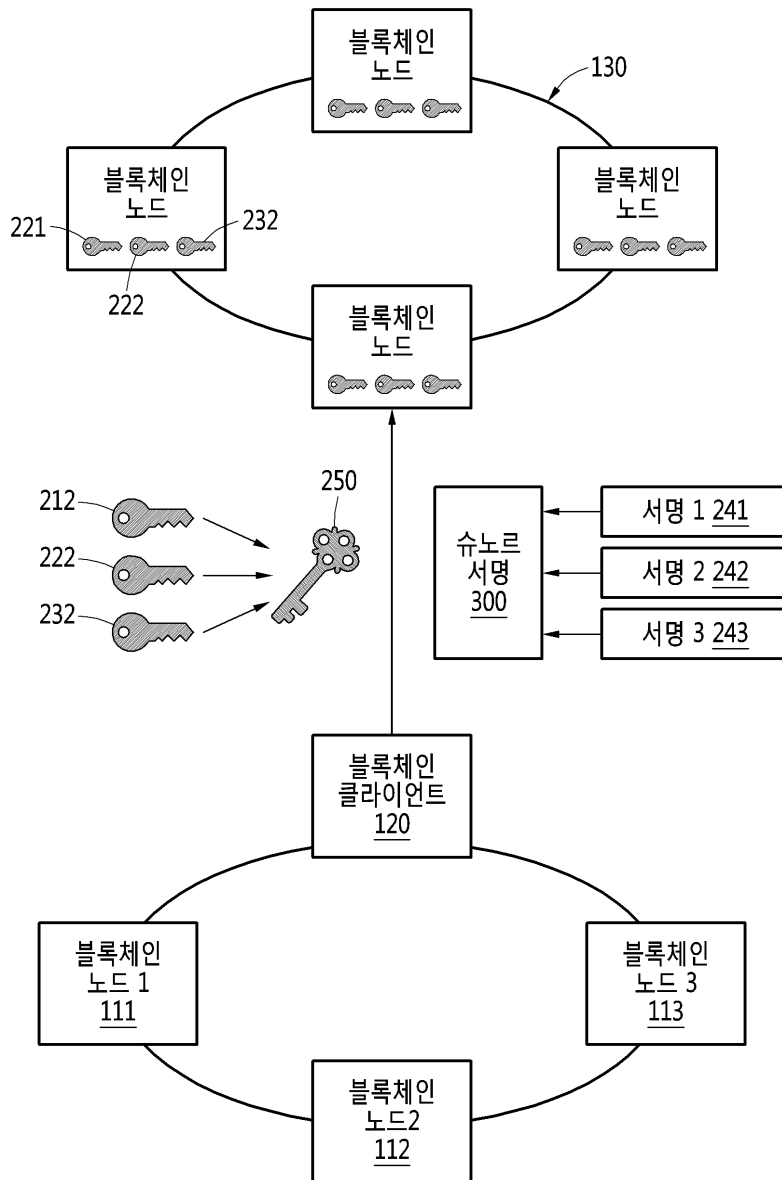
도면1



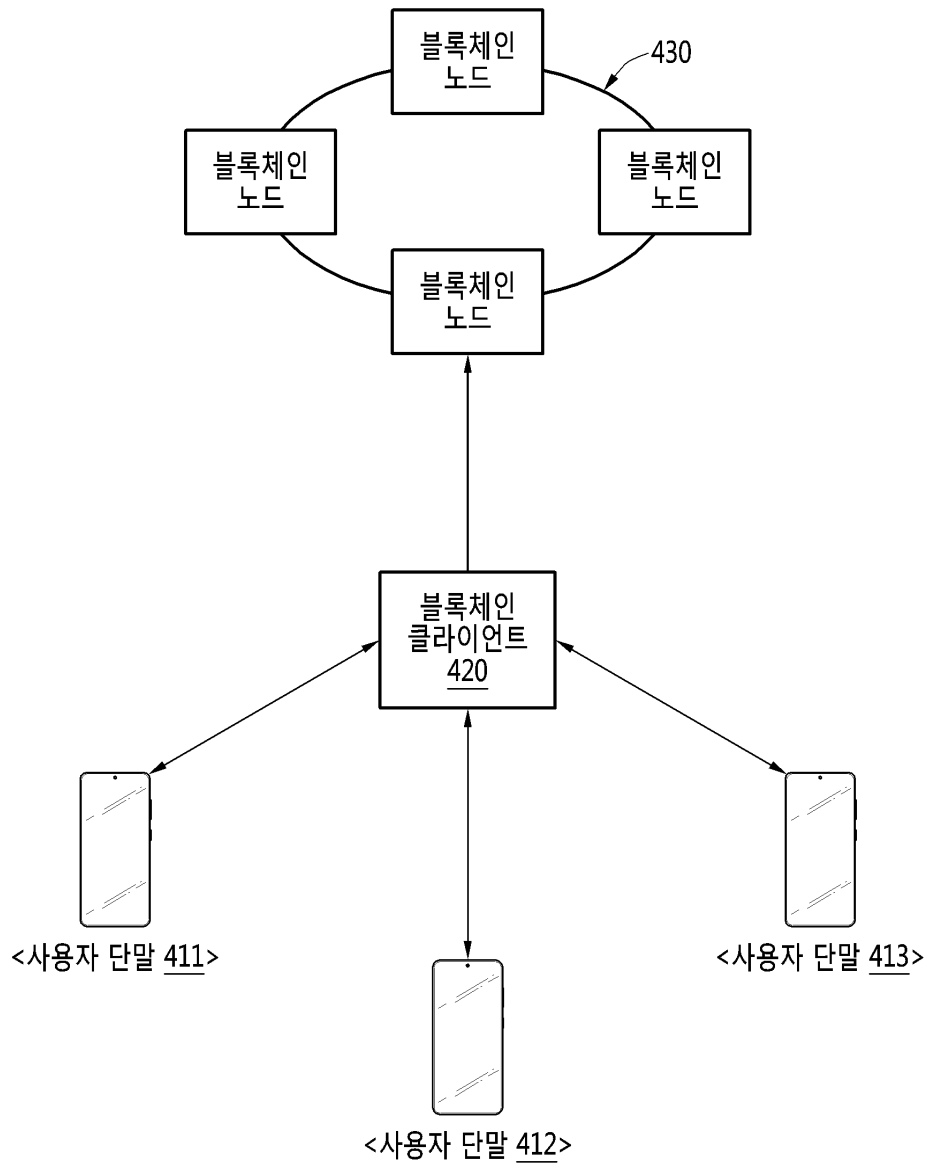
도면2



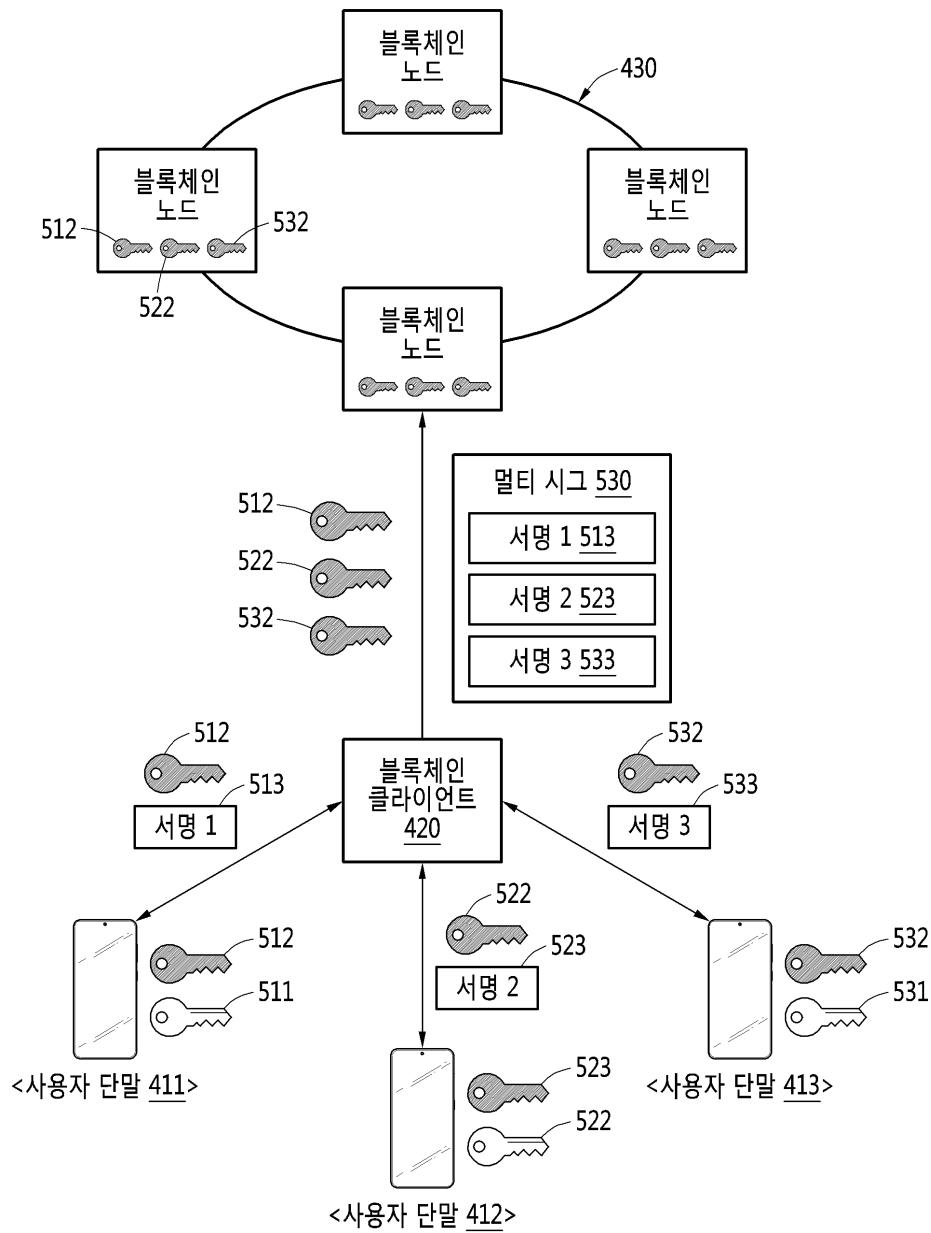
도면3



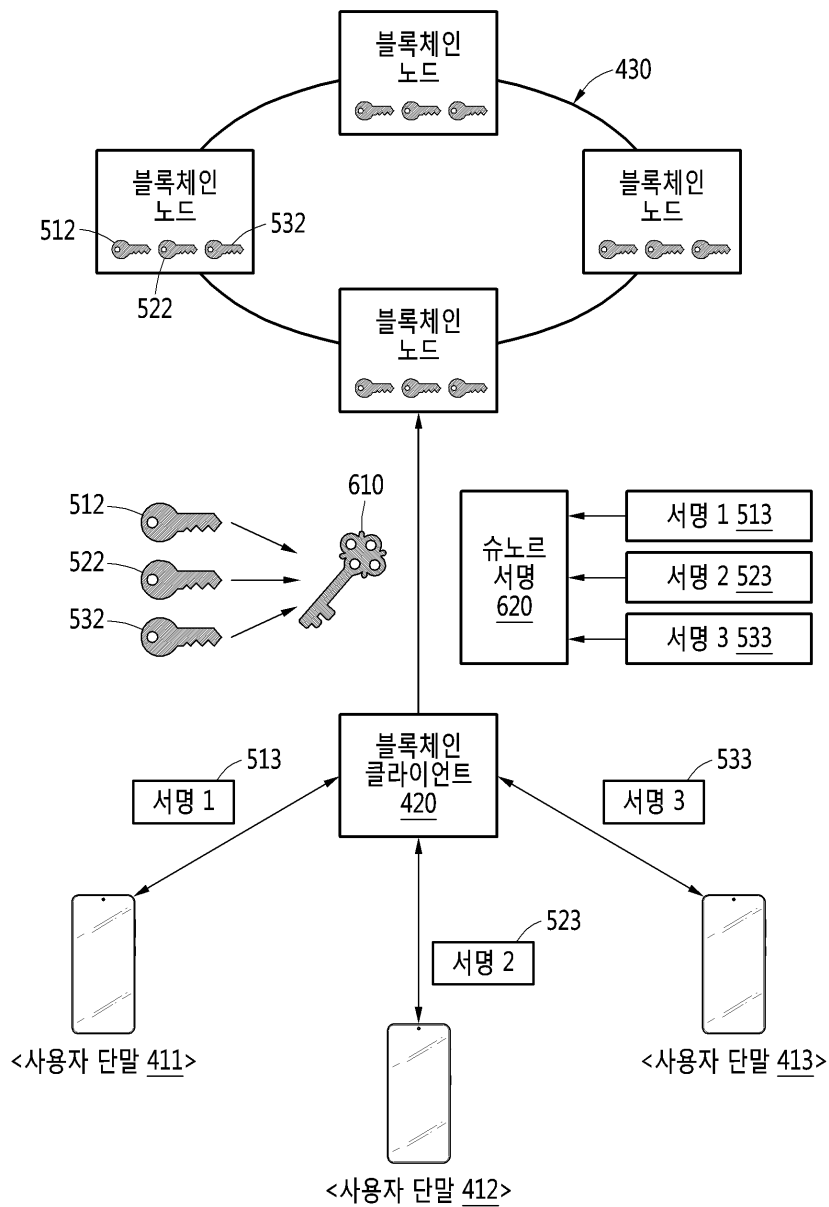
도면4



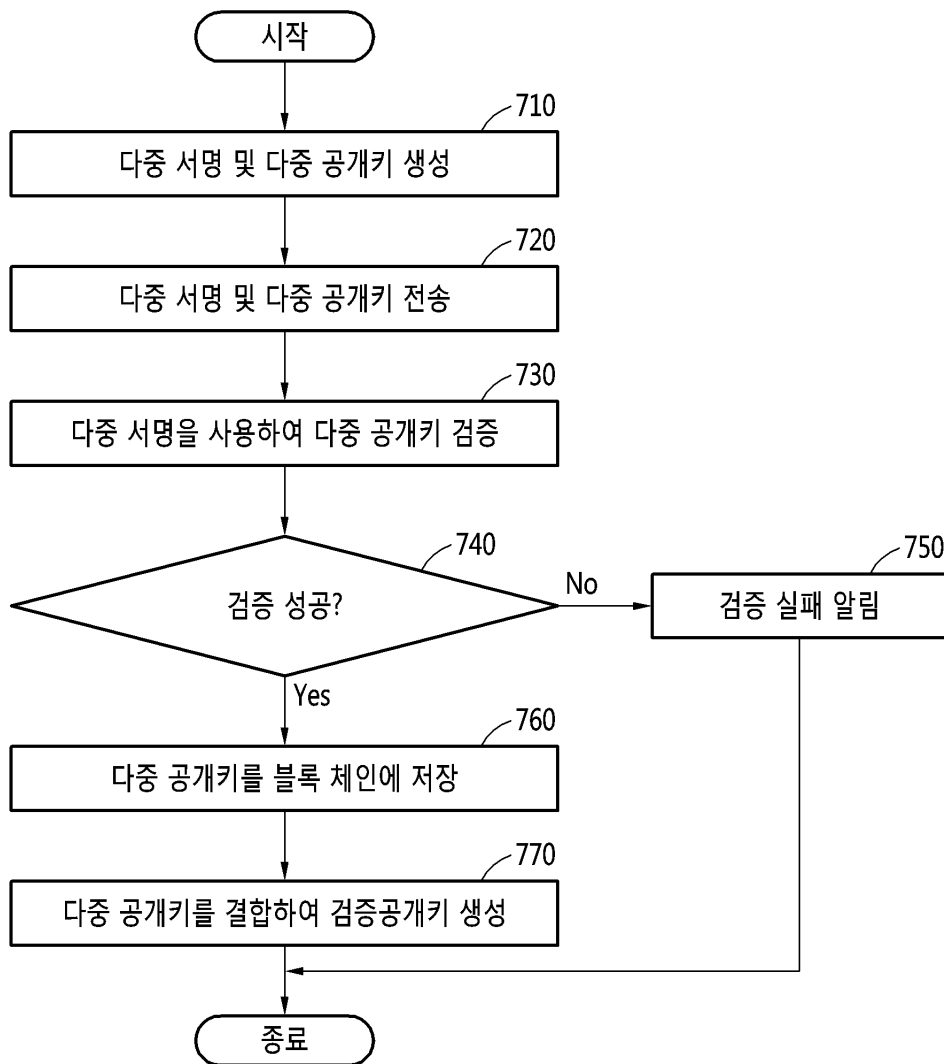
도면5



도면6



도면7



도면8

