



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2021-0059525
(43) 공개일자 2021년05월25일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) H04L 9/08 (2006.01)
(52) CPC특허분류
H04L 9/3247 (2013.01)
H04L 9/0894 (2013.01)
(21) 출원번호 10-2019-0147064
(22) 출원일자 2019년11월15일
심사청구일자 2019년11월15일

(71) 출원인
서강대학교산학협력단
서울특별시 마포구 백범로 35 (신수동, 서강대학교)
논스랩 주식회사
서울특별시 영등포구 선유서로 67 ,102동601호(양평동2가, 신동아하이팰리스)
(72) 발명자
박수용
서울특별시 마포구 독막로 18 길 5, 101동 1001호(상수동, 상수두산위브아파트)
장민오
서울시 중구 퇴계로90길 74 (래미안하이베르)115동 303호
고덕윤
서울특별시 영등포구 선유서로 67 신동아하이팰리스 102동 601호
(74) 대리인
이지연

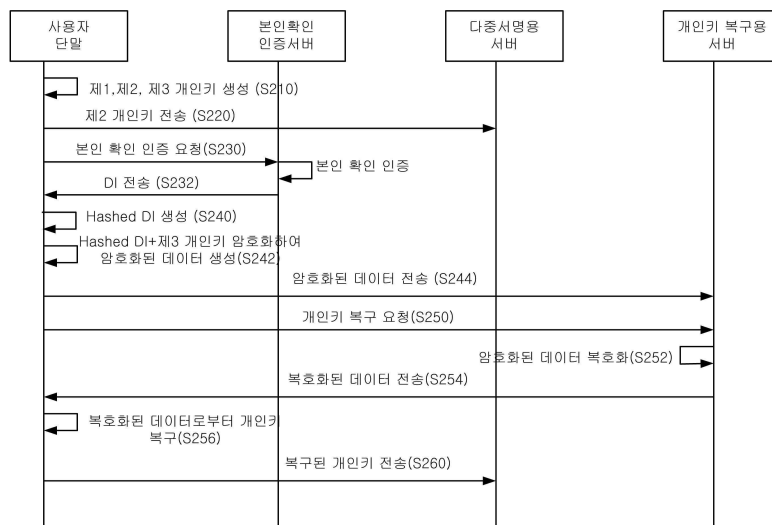
전체 청구항 수 : 총 5 항

(54) 발명의 명칭 **블록체인의 다중 서명을 기반으로 한 개인키 활용 및 복구 시스템**

(57) 요약

본 발명은 블록체인의 다중 서명을 기반으로 한 개인키 활용 및 복구 시스템에 관한 것이다. 상기 개인키 활용 및 복구 시스템은, 블록체인 네트워크의 노드를 구성하며, 제1, 제2 및 제3 개인키를 생성하는 사용자 단말; 트랜잭션들에 대한 다중 서명을 지원하는 다중 서명용 서버; 사용자들의 개인키 복구를 위한 개인키 복구용 서버; 사용자가 본인임을 확인하고 인증하는 본인 확인 인증 서버; 를 구비한다. 상기 다중 서명용 서버는 제2 개인키를 제공받아 보유하며, 상기 본인 확인 인증 서버는 사용자 단말로부터의 본인 확인 인증 요청에 따라 DI를 생성하여 사용자 단말로 제공하며, 상기 개인키 복구용 서버는, 해시된 DI(hashed DI)와 제3 개인키를 암호화한 데이터를 사용자 단말로부터 제공받아 보유하며, 사용자 단말의 개인키 복구 요청에 따라 암호화된 데이터를 복호화하여 제공한다.

대표도 - 도2



(52) CPC특허분류

H04L 9/3263 (2013.01)

H04L 2209/38 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호	1711093140
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기획평가원
연구사업명	대학ICT연구센터육성지원사업
연구과제명	적응형 블록체인 플랫폼 기술 개발 및 전문 인력 양성
기 여 율	1/1
과제수행기관명	서강대학교 산학협력단
연구기간	2019.03.01 ~ 2019.12.31

명세서

청구범위

청구항 1

블록체인 네트워크의 노드를 구성하며, 제1, 제2 및 제3 개인키를 생성하는 사용자 단말;

상기 블록체인 네트워크의 노드를 구성하여 블록체인 네트워크의 트랜잭션들에 대한 다중 서명을 지원하는 다중 서명용 서버;

사용자들의 개인키 복구를 위한 개인키 복구용 서버; 및

사용자에 대한 본인 인증에 필요한 개인 정보 데이터베이스를 보유하고, 사용자로부터의 요청에 따라 사용자가 본인임을 확인하고 인증하는 본인 확인 인증 서버;

를 구비하고, 상기 다중 서명용 서버는 사용자 단말로부터 제2 개인키를 제공받아 보유하며,

상기 본인 확인 인증 서버는 사용자 단말로부터의 본인 확인 인증 요청에 따라 중복 정보(Duplication Information)을 생성하여 사용자 단말로 제공하며,

상기 개인키 복구용 서버는, 해시된 DI(hashed DI)와 제3 개인키를 암호화한 데이터를 사용자 단말로부터 제공받아 보유하는 것을 특징으로 하는 블록체인의 다중 서명을 기반으로 하는 개인키 활용 및 복구 시스템.

청구항 2

제1항에 있어서, 상기 사용자 단말은,

본인 확인 인증 서버로 본인 확인 인증을 요청하고, 상기 요청에 따라 본인 확인 인증 서버로부터 DI 값을 돌려받고, DI 값을 해시하고, 제3 개인키와 상기 해시된 DI를 PKI 기반의 대칭키로 암호화하고, 상기 암호화된 데이터를 상기 개인키 복구용 서버로 전송하는 것을 특징으로 하는 블록체인의 다중 서명을 기반으로 하는 개인키 활용 및 복구 시스템.

청구항 3

제1항에 있어서, 상기 사용자 단말은, 상기 개인키 복구용 서버로 개인키 복구를 요청하고,

상기 요청에 따라 상기 개인키 복구용 서버는 보유한 암호화된 데이터를 복호화하고 상기 복호화된 데이터를 상기 사용자 단말로 제공하며,

상기 사용자 단말은 해시된 DI를 이용하여 상기 개인키 복구용 서버로부터 제공된 복호화된 데이터로부터 개인키를 복구하는 것을 특징으로 하는 블록체인의 다중 서명을 기반으로 하는 개인키 활용 및 복구 시스템.

청구항 4

제3항에 있어서, 상기 사용자 단말은 개인키 복구용 서버로부터 복호화된 데이터를 수신하면, 복호화된 데이터로부터 복구된 개인키를 다중 서명용 서버로 다시 분배하는 것을 특징으로 하는 블록체인의 다중 서명을 기반으로 하는 개인키 활용 및 복구 시스템.

청구항 5

제1항에 있어서, 상기 본인 확인 인증 서버는 이동 통신사의 본인 확인 인증 대행 서버로 구성된 것을 특징으로 하는 블록체인의 다중 서명을 기반으로 하는 개인키 활용 및 복구 시스템.

발명의 설명

기술 분야

[0001] 본 발명은 블록체인의 다중 서명을 기반으로 한 개인키 활용 및 복구 시스템에 관한 것으로서, 더욱 구체적으로는 이동 통신사의 본인 확인 인증 서버를 통한 본인 인증을 통해 다중 서명을 위한 개인키를 복구할 수 있도록 구성된 것을 특징으로 한 개인키 활용 및 복구 시스템에 관한 것이다.

배경 기술

[0002] 2008년 Satoshi Nakamoto라는 익명의 개발자가 작성한 "Bitcoin: A peer-to-peer electronic cash system"의 등장과 함께 비트코인이 출현하였고 이로 인해 블록체인 기술이 시작되었다. 블록체인 기술은, 기존의 중앙화된 방식의 시스템과는 달리, 탈중앙화된 분산 시스템으로서, 모든 데이터를 참여하는 모든 사용자들이 공유하기 때문에 투명성, 무결성 및 보안성이 보장되었으며, 각각의 데이터를 블록형태로 암호화하여 원장에 저장함으로써 '블록체인'이라 불리게 되었다.

[0003] 블록체인은 사용자가 암호자산을 통제하기 위해서 개인만 소지해야 하는 개인키를 활용해야 하며 데이터의 위변조, 인증을 수행하는 기술인 전자서명 중 특수 전자서명을 활용한다.

[0004] 일반적으로 전자서명 방식은 한 문서에 한 사람이 서명을 하는 환경에 기초하여 설계되어 있기 때문에, 서류 결재, 서명 운동, 계약의 경우와 같이 여러 사람이 한 문서에 서명하는 경우 단순서명을 반복해서 적용하여 문서를 해결할 수 있다. 하지만 이러한 방식은 서명의 길이가 늘어나도 서명을 검증할 때 서명자의 수만큼 검증과정을 거쳐야 하기 때문에, 서명자가 많은 경우 시간이 오래 걸린다는 단점이 있다.

[0005] 또한, 일반적으로 암호화폐 기반의 블록체인에서 사용하는 전자서명 방식은 한 사람이 하나의 키를 소유하기 때문에, 소유한 키를 분실하게 되면 다시 찾을 수 없게 된다. 이 경우, 키 분실과 함께 디지털 자산은 영원히 분실되어 송금할 수 없게 되는 문제점이 발생한다. 이러한 문제를 해결하기 위하여 개인키를 중앙 서비스 주체가 보유하는 경우, 보안적으로 취약할 뿐만 아니라, 서비스 주체에서 임의의 송금에 대한 부인 방지가 어려워지는 문제가 발생하게 된다.

[0006] 이러한 단순서명 방식의 문제를 해결하기 위해 나온 개념이 바로 다중서명 방식이다. 다중서명 주소는 하나의 주소에 n 개의 개인키가 설정되어 있다. 이 다중서명 주소에서 인출을 할 때는 n 개의 개인키 중에서 m 개의 서명이 있어야 가능하다. 이를 M-of-N 거래라고도 일컫는다. 다중서명이 산업에서 더욱 더 활용되기 위해서 트랜잭션뿐만 아니라 서명에 필요한 개인키를 활용 및 복구하는 부분을 해결할 필요가 있다.

[0007] 한편, 블록체인의 다중 서명 방식에서는, 사용자가 자신의 개인키를 분실하거나 훼손한 경우, 개인키를 안전하게 복구할 수 있는 방안이 마련되어 있지 않는 문제점이 있다.

선행기술문헌

특허문헌

[0008] (특허문헌 0001) 한국공개특허공보 제 10-2018-0041050호

(특허문헌 0002) 한국등록특허공보 제 10-0523357호

발명의 내용

해결하려는 과제

[0009] 전술한 문제점을 해결하기 위한 본 발명의 목적은 블록체인의 다중 서명을 통해 신뢰할 수 있는 제3자를 설정하고, 신뢰할 수 있는 제3자로부터 본인인증을 하고 이를 통하여 개인키를 안전하게 복구할 수 있도록 하는 개인키 활용 및 복구 시스템을 제공하는 것이다.

과제의 해결 수단

[0010] 전술한 기술적 과제를 달성하기 위한 본 발명의 특징에 따른 블록체인의 다중 서명을 기반으로 한 개인키 활용 및 복구 시스템은, 블록체인 네트워크의 노드를 구성하며, 제1, 제2 및 제3 개인키를 생성하는 사용자 단말; 상기 블록체인 네트워크의 노드를 구성하여 블록체인 네트워크의 트랜잭션들에 대한 다중 서명을 지원하는 다중 서명용 서버; 사용자들의 개인키 복구를 위한 개인키 복구용 서버; 사용자에게 본인 인증에 필요한 개인 정

보 데이터베이스를 보유하고, 사용자로부터의 요청에 따라 사용자가 본인임을 확인하고 인증하는 본인 확인 인증 서버; 를 구비하고,

- [0011] 상기 다중 서명용 서버는 사용자 단말로부터 제2 개인키를 제공받아 보유하며, 상기 본인 확인 인증 서버는 사용자 단말로부터의 본인 확인 인증 요청에 따라 중복 정보(Duplication Information)을 생성하여 사용자 단말로 제공하며,
- [0012] 상기 개인키 복구용 서버는, 해시된 DI(hashed DI)와 제3 개인키를 암호화한 데이터를 사용자 단말로부터 제공받아 보유하는 것이 바람직하다.
- [0013] 전술한 특징에 따른 블록체인의 다중 서명을 기반으로 하는 개인키 활용 및 복구 시스템에 있어서, 상기 사용자 단말은, 본인 확인 인증 서버로 본인 확인 인증을 요청하고, 상기 요청에 따라 본인 확인 인증 서버로부터 DI 값을 돌려받고, DI 값을 해시하고, 제3 개인키와 상기 해시된 DI를 PKI 기반의 대칭키로 암호화하고, 상기 암호화된 데이터를 상기 개인키 복구용 서버로 전송하는 것이 바람직하다.
- [0014] 전술한 특징에 따른 블록체인의 다중 서명을 기반으로 하는 개인키 활용 및 복구 시스템에 있어서, 상기 사용자 단말은, 상기 개인키 복구용 서버로 개인키 복구를 요청하고, 상기 요청에 따라 상기 개인키 복구용 서버는 보유된 암호화된 데이터를 복호화하고 상기 복호화된 데이터를 상기 사용자 단말로 제공하며, 상기 사용자 단말은 해시된 DI를 이용하여 상기 개인키 복구용 서버로부터 제공된 복호화된 데이터로부터 개인키를 복구하는 것이 바람직하다.
- [0015] 전술한 특징에 따른 블록체인의 다중 서명을 기반으로 하는 개인키 활용 및 복구 시스템에 있어서, 상기 사용자 단말은 개인키 복구용 서버로부터 복호화된 데이터를 수신하면, 복호화된 데이터로부터 복구된 개인키를 다중 서명용 서버로 다시 분배하는 것이 바람직하다.
- [0016] 전술한 특징에 따른 블록체인의 다중 서명을 기반으로 하는 개인키 활용 및 복구 시스템에 있어서, 상기 본인 확인 인증 서버는 이동 통신사의 본인 확인 인증 대행 서버로 구성된 것이 바람직하다.

발명의 효과

- [0017] 본 발명에 따른 시스템은 블록체인 네트워크에서 각 사용자가 자신의 개인키를 분실하거나 훼손시킨 경우, 개인키를 안전하게 복구할 수 있게 된다. 종래에는 사용자 본인만 소유해야 하는 개인키를 분실하는 경우, 별도의 복구 방법이 없어 블록체인에 저장된 자산을 찾을 수 없었지만, 본 발명에 의하여 본인 확인 및 인증을 통해 PKI 기반 대칭키 암호화를 적용시킴으로써, 개인키를 분실하여도 복구할 수 있게 된다.
- [0018] 또한, 개인키 복구용 서버는 암호화된 데이터를 복호화하더라도, Hashed DI의 값을 알 수 없기 때문에, 개인키에 대한 유출이 발생될 우려가 없다. 만약, 개인키 복구용 서버가 개인키를 통해 추후에 DI 값을 알고자 하여도 이미 DI값은 해시 알고리즘을 통해 사용자로부터 전달되었기 때문에 유출할 수 없게 된다. 또한, Hashed DI를 기반으로 대칭키를 복호화하게 되면, 사용자는 분실한 개인키를 찾을 수 있기 때문에 이전과 같이 블록체인 네트워크에서 개인키를 활용하여 자산을 관리할 수 있게 된다.

도면의 간단한 설명

- [0019] 도 1은 본 발명의 바람직한 실시예에 따른 블록체인 다중서명을 기반으로 한 개인키 활용 및 복구 시스템을 개략적으로 도시한 구성도이다.
- 도 2는 본 발명에 따른 블록체인의 다중 서명을 기반으로 한 개인키 활용 및 복구 방법을 전체적으로 도시한 흐름도이다.
- 도 3은 본 발명에 따른 블록체인의 다중 서명을 기반으로 한 개인키 활용 및 복구 방법에 있어서, 사용자 단말에서의 다중 서명을 위한 개인키 분배 및 생성 과정을 순차적으로 도시한 흐름도이다.
- 도 4는 본 발명에 따른 블록체인의 다중 서명을 기반으로 한 개인키 활용 및 복구 방법에 있어서, 본인 확인 인증 서버를 통해 중복 정보(DI)를 획득하는 과정을 도시한 흐름도이다.
- 도 5는 본 발명에 따른 블록체인의 다중 서명을 기반으로 한 개인키 활용 및 복구 방법에 있어서, 사용자 단말이 개인키를 복구하는 과정을 도시한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

- [0020] 본 발명에 따른 개인키 활용 및 복구 시스템은 블록체인 기반 다중 서명(Multi-Signature), 이동통신사의 모바일 본인 인증 서비스, PKI(Public Key Infrastructure) 기반 대칭키를 활용하여 개인키를 활용 및 복구하는 것을 특징으로 한다.
- [0021] 이하, 첨부된 도면을 참조하여 본 발명의 바람직한 실시예에 따른 블록체인의 다중 서명을 기반으로 한 개인키 활용 및 복구 시스템 및 개인키 활용 및 복구 방법에 대하여 구체적으로 설명한다.
- [0022] 도 1은 본 발명의 바람직한 실시예에 따른 블록체인 다중서명을 기반으로 한 개인키 활용 및 복구 시스템을 개략적으로 도시한 구성도이다. 도 1을 참조하면, 본 발명의 개인키 활용 및 복구 시스템(1)은 사용자 단말(10), 다중 서명용 서버(20), 복구용 서버(30) 및 본인 확인 인증 서버(40)를 구비한다.
- [0023] 상기 사용자 단말(10)은 블록체인 네트워크의 인증서버로부터 개인키와 공개키를 제공받고 블록체인 네트워크의 노드를 구성하며, 상기 다중 서명용 서버(20)와 연동되어 블록체인의 M of N 다중 서명을 한다. 따라서, 상기 사용자 단말(10)은 제1, 제2 및 제3 개인키를 생성하고, 제2 개인키는 상기 다중 서명용 서버로 제공한다.
- [0024] 상기 사용자 단말은 최초에 3개의 개인키(Private Key), 즉 제1, 제2 및 제3 개인키를 생성하고, 최초에는 제1 개인키와 제3 개인키는 사용자 단말에 저장하고 제2 개인키는 다중 서명용 서버에 전달한다. 한편, 사용자 단말은 개인키를 따로 저장하기 위하여 제3 개인키를 활용하게 되는데, 본인 확인 인증 서버에 본인 확인 및 인증을 요청하고, 상기 요청에 따라 복인 확인되고 인증되면 상기 본인 확인 인증 서버로부터 복제 정보(Duplication Information; 이하 'DI'라 한다.)를 제공받는다.
- [0025] 상기 사용자 단말은 상기 DI를 복호화할 수 없는 해시(hash) 알고리즘을 통해 암호화하며, Hashed DI와 제3 개인키를 PKI 기반 대칭키로 암호화한 후 상기 복구용 서버로 제공한다.
- [0026] 상기 다중 서명용 서버(20)는 블록체인 네트워크를 구성하는 노드들에 대한 개인키를 제공받아 보유하면서 다중 서명을 해주는 서버로서, 상기 사용자 단말(10)로부터 초기 생성된 3개의 개인키 중 제2 개인키를 제공받아 보유하고 다중 서명을 해 주게 되는데, 블록체인 네트워크를 관리하는 회사의 서버, 일반적인 회사의 서버 또는 비트코인의 거래소의 서버 등이 될 수 있다. 일반적으로 상기 다중 서명용 서버는, 거래소 서버가 될 수 있는데, 다중 서명 기반으로 트랜잭션을 생성하기 위하여 제2 개인키를 소유하게 된다.
- [0027] 따라서, 상기 다중 서명용 서버(20)는 사용자 단말로부터 초기에 제2 개인키를 제공받아 보유하거나, 사용자 단말이 제1 개인키를 분실하고 복구한 경우에는 사용자 단말로부터 복구된 제2 개인키를 다시 제공받아 보유하게 된다.
- [0028] 상기 복구용 서버(30)는 사용자 단말로부터 제공받은 암호화된 데이터들을 보유하는 것을 특징으로 하며, 상기 암호화된 데이터들은 제3 개인키와 본인 확인 인증 서버로부터 받은 Hashed DI를 PKI 기반 대칭키로 저장하게 된다. 상기 Hashed DI는 사용자 단말이 본인 확인 및 인증을 통해야만 받을 수 있는 데이터이기 때문에 다중 서명용 서버가 소유하고 있을 수 없으며 사용자가 개인키 분실시 개인키 복구를 요청하면 Hashed DI를 통해 복구할 수 있게 된다.
- [0029] 상기 본인 확인 인증 서버(40)는 사용자에 대한 개인 정보를 포함하는 DB를 구비하는 이동 통신사와 연동되는 본인 확인 인증 대행사의 서버가 될 수 있는데, 사용자로부터 본인 확인 인증을 요청받게 되면, 이동 통신사에서 저장 및 관리하고 있는 사용자에 대한 개인 정보 데이터베이스를 기반으로 하여 사용자에 대한 본인 확인하고 DI값을 리턴하게 된다. 일반적으로 모바일 본인 확인 및 인증 과정에서는 DI(Connecting Information)과 DI(Duplication Information)이 있는데, 상기 CI는 각 웹 사이트마다 중복되는 정보이나, 상기 DI는 보안성이 높고 고유한 값이므로 상기 DI값을 사용자 단말에게 제공하게 된다. 상기 DI는 중복 정보로서 64 bytes로 된 정보이며, 기본적으로 중복 가입 체크를 하고 이에 따라 한 사람의 명의로 여러 개의 계정을 만들어 악용하는 것을 방지하기 위하여 사용되는 정보이다.
- [0030] 상기 본인 확인 인증 대행사는, 본인 확인 및 인증에 필요한 개인 정보를 보유하고 있는 이동 통신사들을 대신 하여, 모바일 본인 인증을 통해 지점을 방문하지 않아도 본인임을 비대면으로 인증해 줄 수 있는 주체이다.
- [0031] 이하, 첨부된 도면을 이용하여 본 발명에 따른 블록체인의 다중 서명을 기반으로 한 개인키 활용 및 복구 방법을 구체적으로 설명한다.
- [0032] 도 2는 본 발명에 따른 블록체인의 다중 서명을 기반으로 한 개인키 활용 및 복구 방법을 전체적으로 도시한 흐름도이며, 도 3은 도 2에서 사용자 단말에서의 다중 서명을 위한 개인키 분배 및 생성 과정을 순차적으로 도시한 흐름도이며, 도 4는 본인 확인 인증 서버를 통해 중복 정보(DI)를 획득하는 과정을 도시한 흐름도이며, 도 5

는 사용자 단말이 개인키를 복구하는 과정을 도시한 흐름도이다.

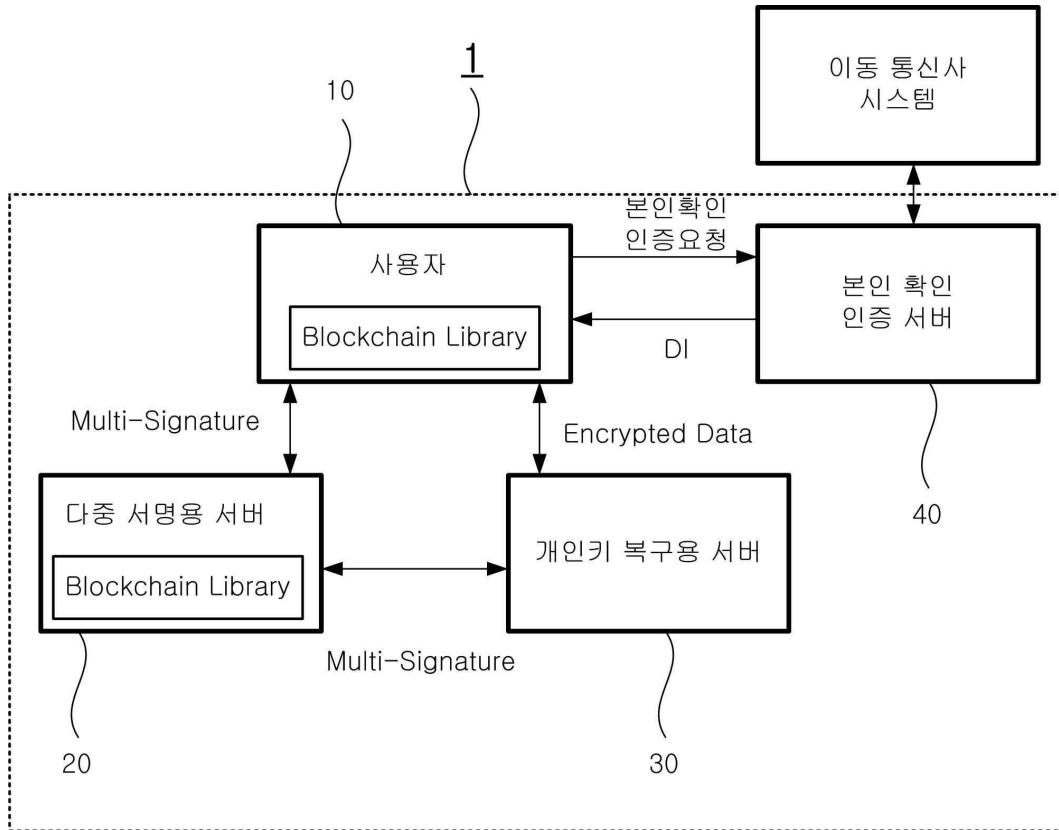
- [0033] 도 2 및 도 3을 참조하여 본 발명에 따른 개인키 활용 및 복구 방법에서의 개인키 생성 및 분배 과정을 설명한다. 도 3을 참조하면, 개인키 생성 및 분배 과정은, 먼저 사용자가 자신의 단말을 이용하여 블록체인 네트워크에 하나의 노드로 참가하기 위하여 블록체인 네트워크의 인증 서버에 의해 인증되고, 다중 서명을 위하여 제1, 제2 및 제3 개인키를 생성하게 되고(단계 210), 제2 개인키는 다중 서명을 위하여 다중 서명용 서버로 제공한다(단계 220). 이때, 제1, 제2 및 제3 개인키는 모두 동일한 값으로 구성된다.
- [0034] 다음, 도 2 및 도 4를 참조하여 본 발명에 따른 개인키 활용 및 복구 방법에서의 다중 서명 기반의 본인 확인 및 인증 과정을 설명한다. 도 4를 참조하면, 본인 확인 및 인증 방법은, 사용자 단말이 본인 확인 인증 서버에 본인 확인 인증을 요청하고(단계 230), 본인 확인 인증 요청에 따라 본인 확인 인증 서버는 본인 확인 인증을 수행하고 DI를 사용자 단말로 제공한다(단계 232).
- [0035] 다음, 사용자 단말은 DI를 해시알고리즘을 이용하여 암호화하여 Hashed DI 를 생성하고(단계 240), Hashed DI 와 제3 개인키를 PKI 기반 대칭키를 이용하여 암호화시키고(단계 242), 암호화된 데이터를 복구용 서버로 제공한다(단계 244).
- [0036] 다음, 도 2 및 도 5를 참조하여 본 발명에 따른 개인키 활용 및 복구 방법에서의 다중 서명 기반의 개인키 복구 과정을 설명한다. 도 5를 참조하면, 개인키 복구 과정은, 사용자가 개인키를 분실하여 복구하고자 하는 경우, 사용자 단말은 복구용 서버로 Hashed DI를 전송하고 개인키의 복구를 요청한다(단계 250). 사용자 단말로부터의 개인키 복구 요청에 따라, 복구용 서버는 암호화된 데이터를 복호화시키고(단계 252) 복호화된 데이터를 사용자 단말로 제공한다(단계 254).
- [0037] 사용자 단말은 Hashed DI를 통해 복구용 서버로부터 제공된 복호화된 데이터로부터 개인키를 복구하고, 복구화된 개인키를 다중 서명용 서버로 다시 제공한다(단계 260).
- [0038] 이상에서 본 발명에 대하여 그 바람직한 실시예를 중심으로 설명하였으나, 이는 단지 예시일 뿐 본 발명을 한정하는 것이 아니며, 본 발명이 속하는 분야의 통상의 지식을 가진 자라면 본 발명의 본질적인 특성을 벗어나지 않는 범위에서 이상에 예시되지 않은 여러 가지의 변형과 응용이 가능함을 알 수 있을 것이다. 그리고, 이러한 변형과 응용에 관계된 차이점들은 첨부된 청구 범위에서 규정하는 본 발명의 범위에 포함되는 것으로 해석되어야 할 것이다.

부호의 설명

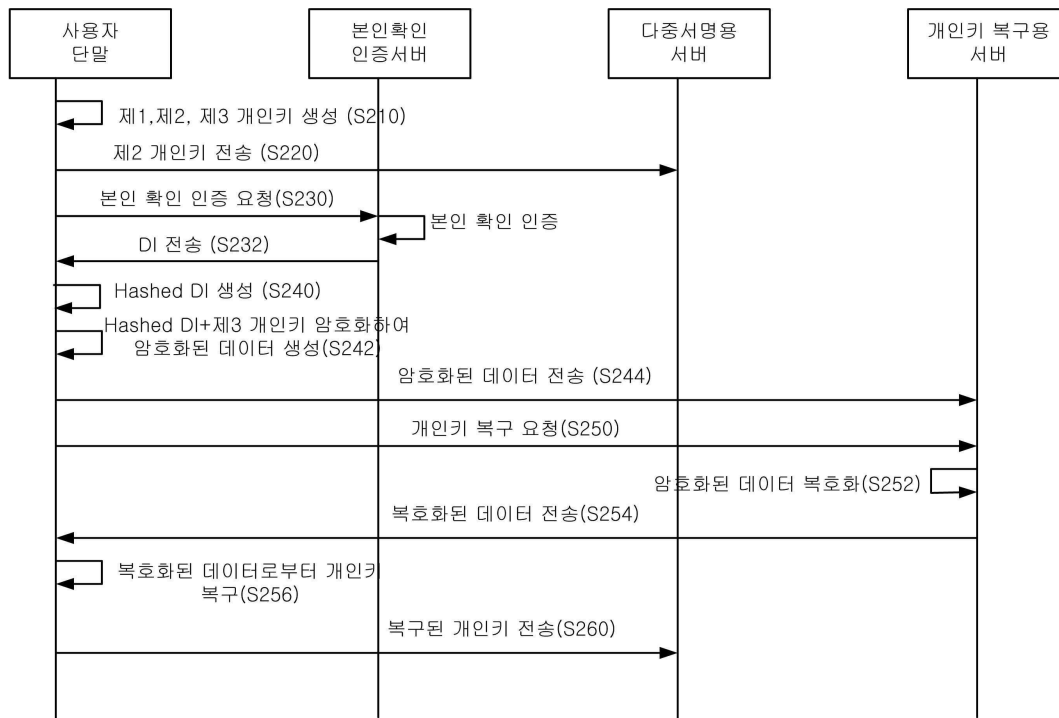
- [0039] 1 : 개인키 활용 및 복구 시스템
 10 : 사용자 단말
 20 : 다중 서명용 서버
 30 : 복구용 서버
 40 : 본인 확인 인증 서버

도면

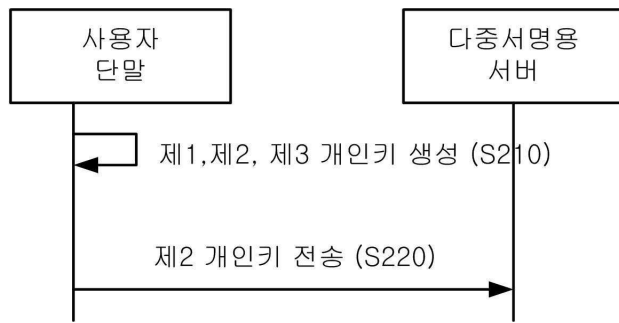
도면1



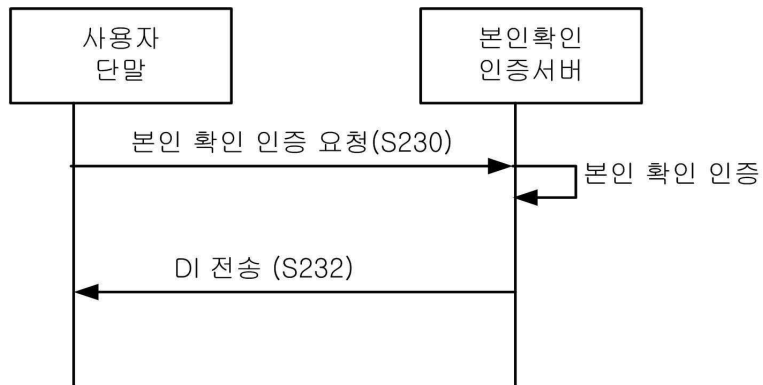
도면2



도면3



도면4



도면5

