(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2022년07월27일
(11) 등록번호 10-2426078
(24) 등록일자 2022년07월22일

(51) 국제특허분류(Int. Cl.)
G06Q 20/38 (2012.01) *G06Q 20/36* (2012.01)
G06Q 20/40 (2012.01) *H04L 9/08* (2006.01)
H04L 9/30 (2006.01)
(52) CPC특허분류
G06Q 20/3829 (2013.01)
G06Q 20/3678 (2013.01)
(21) 출원번호 10-2020-0149623
(22) 출원일자 2020년11월10일
심사청구일자 2020년11월10일
(65) 공개번호 10-2022-0063591
(43) 공개일자 2022년05월17일
(56) 선행기술조사문헌
KR101796690 B1*
KR1020180115701 A*
KR1020200028961 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
포항공과대학교 산학협력단
경상북도 포항시 남구 청암로 77 (지곡동)
(72) 발명자
박찬익
경상북도 포항시 남구 지곡로 155, 6동 1105호
박해성
경상북도 포항시 남구 청암로 77, 11동 207호
(74) 대리인
특허법인이상

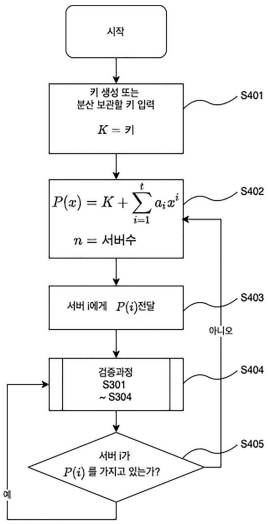
전체 청구항 수 : 총 17 항 심사관 : 심송학

(54) 발명의 명칭 **공개 검증 가능한 블록체인 지갑 키 보관 방법 및 장치**

(57) 요 약

복원 임계값 개수 이상의 키 보관 서버들이 부분 키를 정확하게 보관하도록 공개 검증 방식으로 검증하고 관리하는 블록체인 지갑 키 보관 방법 및 장치가 개시된다. 블록체인 지갑 키 보관 방법은 사용자 단말에 탑재된 사용자 프로그램에 의해 수행되는 공개 검증 가능한 블록체인 지갑 키 보관 방법으로서, 사용자 프로그램에 탑재된 키 분산/복원 실행부에 의해 사용자 암호키를 분할하여 확정 값과 함께 부분 키를 생성하는 단계와, 부분 키를 확정 값과 함께 분산 키 보관 서버의 공개키로 암호화하는 단계와, 공개키로 암호화된 부분 키를 분산 키 보관 서버로 전달하는 단계를 포함한다.

대 표 도 - 도4



(52) CPC특허분류
G06Q 20/40 (2013.01)
H04L 9/0825 (2013.01)
H04L 9/3066 (2013.01)
H04L 9/50 (2022.05)

이 발명을 지원한 국가연구개발사업
과제고유번호 1711125876
과제번호 2020-0-00936-002
부처명 과학기술정보통신부
과제관리(전문)기관명 정보통신기획평가원
연구사업명 블록체인융합기술개발(R&D)
연구과제명 5G 초저지연 서비스를 위한 무선 단말용 블록체인 기술 개발
기 여 율 1/2
과제수행기관명 포항공과대학교 산학협력단
연구기간 2021.01.01 ~ 2021.12.31
이 발명을 지원한 국가연구개발사업
과제고유번호 1711152571
과제번호 2021-0-00484-002
부처명 과학기술정보통신부
과제관리(전문)기관명 정보통신기획평가원
연구사업명 데이터경제를위한블록체인기술개발(R&D)
연구과제명 노드 간 메시지 전달과 합의를 위한 최적 경로 네트워크 프로토콜 기술개발
기 여 율 1/2
과제수행기관명 포항공과대학교 산학협력단
연구기간 2022.01.01 ~ 2022.12.31

명 세 서

청구범위

청구항 1

사용자 단말에 탑재된 사용자 프로그램에 의해 수행되는 공개 검증 가능한 블록체인 지갑 키 보관 방법으로서,

사용자 프로그램에 탑재된 키 분산/복원 실행부에 의해 사용자 암호키를 분할하여 확정 값과 함께 부분 키를 생성하는 단계;

상기 부분 키를 상기 확정 값과 함께 분산 키 보관 서버의 공개키로 암호화하는 단계;

상기 공개키로 암호화된 부분 키를 상기 분산 키 보관 서버로 전달하는 단계;

상기 분산 키 보관 서버가 유효한 부분 키를 소유하고 있는지 감시하는 단계;

상기 분산 키 보관 서버에 저장된 부분 키의 유효성을 검증하는 단계;

상기 검증하는 단계에서의 검증 결과, 특정 분산 키 보관 서버가 유효한 부분 키를 소유하지 않은 경우, 유효한 부분 키를 재생성하는 단계; 및

상기 특정 분산 키 보관 서버로 재생성한 유효한 부분 키를 전송하거나, 상기 분산 키 보관 서버를 재구성한 후 재구성된 분산 키 보관 서버로 상기 재생성한 유효한 부분 키를 전송하는 단계를 포함하는 블록체인 지갑 키 보관 방법.

청구항 2

청구항 1에 있어서,

상기 생성하는 단계는 상기 부분 키의 생성 시 복원 임계값을 t로 하고, 암호키를 K로 대입하여 t-1차 다항식을 구성하고, 상기 t-1차 다항식에 기반하여 추후 검증을 위한 확정 값을 생성하는, 블록체인 지갑 키 보관 방법.

청구항 3

청구항 2에 있어서,

상기 확정 값(C)은 아래의 [수학식 2]로 표현되고,

[수학식 2]

$$C=(H,H^{K},\bigcup_{i=1}^{t-1}H^{a_i},\bigcup_{i=1}^{n}X_i^{P(i)})$$

상기 [수학식 2]에서 상기 P(i)는 t-1차 다항식을, 상기 K는 암호키를, 상기 H는 타원곡선 암호화에서 H를 기준점으로 사용하는 큰 소수(prime number) 또는 타원 곡선(elliptic curve)의 한 점을, H^{K}는 K를 타원곡선 상에서 H 값을 기준으로 곱 연산한 것을 각각 나타내는, 블록체인 지갑 키 보관 방법.

청구항 4

청구항 2에 있어서,

상기 생성하는 단계는, 상기 확정 값을 생성한 후 상기 t-1차 다항식 상에서의 한 점 (i, P(i))으로 i번째 부분 키를 생성하는, 블록체인 지갑 키 보관 방법.

청구항 5

삭제

청구항 6

청구항 1에 있어서,

상기 검증하는 단계는,

상기 분산 키 보관 서버의 보관 서비스 프로그램으로 검증 요청을 전송하는 단계;

상기 분산 키 보관 서버로부터 무작위로 생성한 제1 상수 값을 받는 단계;

상기 부분 키의 검증 확인 요청값으로 무작위로 생성한 제2 상수 값을 상기 보관 서비스 프로그램에 전달하는 단계;

상기 분산 키 보관 서버로부터 상기 제1 상수 값, 상기 제2 상수 값 및 기저장된 부분 키 값을 이용하여 생성한 증명 값을 받는 단계; 및

상기 제1 상수 값, 상기 제2 상수 값 및 상기 증명 값을 이용하여 상기 분산 키 보관 서버가 유효한 부분 키를 저장하고 있는지 여부를 검증하는 단계;

를 포함하는 블록체인 지갑 키 보관 방법.

청구항 7

청구항 6에 있어서,

상기 증명 값은 아래의 [수학식 4]로부터 도출되고,

[수학식 3]

$$r=w\text{-}P(i)\times c$$

상기 [수학식 3]에서 r는 증명 값을, w는 제1 상수 값을, c는 제2 상수 값을, P(i)는 t-1차 다항식을 각각 나타내는, 블록체인 지갑 키 보관 방법.

청구항 8

청구항 6에 있어서,

상기 여부를 검증하는 단계는, 동형이산로그(discrete logarithm equality) 수학식인 하기의 [수학식 4]로부터 도출되는 값을 검증 과정에서 확정 값과 함께 이용하며,

[수학식 4]

$$\log_{g_1} h_1=\log_{g_2} h_2(h_1=g_1^{P(i)},h_2=g_2^{P(i)},g_1=H,g_2=X_i)$$

상기 [수학식 4]에서 $g_2^{P(i)}$는 $g_2 = X_i$에서 부분 키 P(i)를 공개키로 곱한 것을 의미하고, $g_1^{P(i)}$는 타원 곡선 위의 한 점(H)로 곱한 값인, 블록체인 지갑 키 보관 방법.

청구항 9

청구항 8에 있어서,

상기 여부를 검증하는 단계는, 상기 수학식 4를 만족하는 경우, 상기 분산 키 보관 서버로부터 부분 키를 받지 않고 상기 분산 키 분산 서버에 유효한 부분 키가 저장되어 있음을 수학적으로 검증하는 단계를 포함하는, 블록체인 지갑 키 보관 방법.

청구항 10

청구항 9에 있어서,

상기 수학적으로 검증하는 단계는 하기의 [수학식 5] 및 [수학식 6]를 이용하여 검증하며,

[수학식 5]

$$H^{w}=H^{r}h_1^{c}$$

[수학식 6]

$$X_i^{w}=X_i^{r}h_2^{c}$$

상기 [수학식 5] 및 [수학식 6]에서 Xi는 공개된 값인 분산 키 보관 서버의 공개키를, c는 확정 값을, w는 제1 상수 값을, c는 제2 상수 값을, r은 증명 값을 각각 나타내는, 블록체인 지갑 키 보관 방법.

청구항 11

사용자 프로그램을 포함하는 공개 검증 가능한 블록체인 지갑 키 보관 장치로서,

사용자 프로그램에 포함된 키 분산/복원 실행부와 감시/검증 실행부; 및

상기 키 분산/복원 실행부와 상기 감시/검증 실행부의 프로그램 명령을 저장하는 메모리를 포함하고, 상기 프로그램 명령에 의해,

사용자 암호키를 분할하여 확정 값과 함께 부분 키를 생성하고,

상기 부분 키를 상기 확정 값과 함께 분산 키 보관 서버의 공개키로 암호화하고,

상기 공개키로 암호화된 부분 키를 상기 분산 키 보관 서버로 전달하고,

상기 분산 키 보관 서버가 유효한 부분 키를 소유하고 있는지 감시하고, 상기 분산 키 보관 서버에 저장된 부분 키의 유효성을 검증하고,

상기 유효성의 검증에서 특정 분산 키 보관 서버가 유효한 부분 키를 소유하지 않은 경우에 유효한 부분 키를 재생성하고,

상기 특정 분산 키 보관 서버로 재생성한 유효한 부분 키를 전송하거나, 상기 분산 키 보관 서버를 재구성한 후 재구성된 분산 키 보관 서버로 상기 재생성한 유효한 부분 키를 전송하는, 블록체인 지갑 키 보관 장치.

청구항 12

청구항 11에 있어서,

상기 감시/검증 실행부는 상기 확정 값을 생성한 후 t-1차 다항식 상에서의 한 점 (i, P(i))으로 i번째 부분 키를 생성하며, 여기서 t는 다항식의 최고차항을 결정하는 장치 설정값인, 블록체인 지갑 키 보관 장치.

청구항 13

삭제

청구항 14

청구항 11에 있어서,

상기 감시/검증 실행부는 상기 유효한 부분 키의 검증을 위해 상기 분산 키 보관 서버의 보관 서비스 프로그램으로 검증 요청을 전송하고, 상기 분산 키 보관 서버로부터 무작위로 생성한 제1 상수 값을 받고, 상기 부분 키의 검증 확인 요청값으로 무작위로 생성한 제2 상수 값을 상기 보관 서비스 프로그램에 전달하고, 상기 분산 키 보관 서버로부터 상기 제1 상수 값, 상기 제2 상수 값 및 기저장된 부분 키 값을 이용하여 생성한 증명 값을 받고, 상기 제1 상수 값, 상기 제2 상수 값 및 상기 증명 값을 이용하여 상기 분산 키 보관 서버가 유효한 부분 키를 저장하고 있는지를 검증하는, 블록체인 지갑 키 보관 장치.

청구항 15

청구항 14에 있어서,

상기 감시/검증 실행부는 상기 유효한 부분 키의 검증 과정에서 상기 유효한 부분 키의 검증 과정에서 동형이산

로그(discrete logarithm equality) 수학식으로부터 도출되는 값을 상기 확정 값과 함께 이용하는, 블록체인 지갑 키 보관 장치.

청구항 16

청구항 15에 있어서,

상기 감시/검증 실행부는 상기 검증 과정에서 상기 동형이산로그 수학식을 만족하는 경우, 상기 분산 키 보관 서버로부터 부분 키를 받지 않고 상기 분산 키 분산 서버에 유효한 부분 키가 저장되어 있음을 수학적으로 검증하는, 블록체인 지갑 키 보관 장치.

청구항 17

청구항 16에 있어서,

상기 수학적으로 검증하는 것은 하기의 [수학식 5] 및 [수학식 6]를 이용하여 검증하며,

[수학식 5]

$$H^{w}=H^{r}h_{1}^{c}$$

[수학식 6]

$$X_{i}^{w}=X_{i}^{r}h_{2}^{c}$$

상기 [수학식 5] 및 [수학식 6]에서 Xi는 공개된 값인 분산 키 보관 서버의 공개키를, c는 확정 값을, w는 제1 상수 값을, c는 제2 상수 값을, r은 증명 값을 각각 나타내는, 블록체인 지갑 키 보관 장치.

청구항 18

청구항 15에 있어서,

상기 감시/검증 실행부는 상기 검증 과정을 통해 유효한 부분 키를 저장하고 있지 않은 재분배 대상 서버의 정보를 저장하는, 블록체인 지갑 키 보관 장치.

청구항 19

청구항 18에 있어서,

상기 감시/검증 실행부는 복원 임계값 이하의 서버 개수에 대하여 유효한 부분 키의 저장 여부에 대한 검증이 각각 완료되면, 유효한 부분 키를 저장하고 있지 않은 분산 키 보관 서버의 정보에 기초하여 분산 키를 재분배하는, 블록체인 지갑 키 보관 장치.

발명의 설명

기 술 분 야

[0001] 본 발명은 분산 암호화 키 보관 기술에 관한 것으로, 보다 상세하게는 복원 임계값 개수 이상의 키 보관 서버들이 부분 키를 정확하게 보관하도록 공개 검증 방식으로 검증하고 관리하는 블록체인 지갑 키 보관 방법 및 장치에 관한 것이다.

배 경 기 술

[0002] 블록체인 서비스는 탈중앙화 특성을 가지므로, 블록체인 기반 서비스에서 사용자 계정 정보 즉, 사용자 암호화 키의 관리는 전적으로 사용자 책임이다. 반면, 전통적 인터넷 온라인 서비스 대부분의 경우 온라인 서비스 제공자가 사용자 계정 정보 즉, 암호화 키의 백업 및 복원 기능을 지원하고 있다. 따라서, 블록체인 기반 서비스 확산을 위해서 사용자 암호화 키 분실에 대응하여 키 백업 및 복원 기능을 제공하는 암호화 키 보관(custody) 문제는 반드시 해결해야 하는 문제이다.

[0003] 현재 블록체인 사용자 암호화 키 보관 서비스 대부분들은 대부분 비밀 값 공유 기법을 이용하여 암호 키를 분할하고 분산 보관한다. 즉, 부분 키를 키 보관 서비스 제공자들에게 분산 보관함으로써, 사용자 암호화키 유출을

방지하면서도, 사용자 암호화키가 분실되었을 경우 복원 임계값 개수 이상의 부분 키 정보를 통해 사용자 암호화 키를 복원한다.

[0004] 따라서, 블록체인 사용자 암호화 키 보관 서비스에서는 복원 임계값 이상의 키 보관 서비스들이 정확한 부분 키 정보를 저장하고 있어야 하며, 사용자 입장에서 이를 검증하기 위해서는 복원 임계값 개수 이상의 부분 키 정보를 수집하여 사용자 암호화 키를 복원하는 과정을 진행해야 한다. 이런 과정은 실행 오버헤드가 크며, 또한 빈번한 암호화 키 복원 과정에서 암호화 키 유출 가능성을 높이는 문제를 가진다. 더욱이, 특정 키 보관 서비스 제공자에 대한 집중적 검증을 진행하기는 불가능하다.

발명의 내용

해결하려는 과제

[0005] 본 발명은 상술한 문제점을 해결하기 위해 도출된 것으로, 본 발명의 목적은 부분 키 보관 서버들을 효과적으로 감시 및 검증하는 방법을 지원하는 분산 키 보관 시스템을 제공하는데 있다.

[0006] 본 발명의 다른 목적은 PVSS(public verifiable secret sharing) 기법을 활용하여 각 부분 키 유효성을 감시하는, 공개적 검증 가능한 블록체인 지갑 키 보관 방법 및 장치를 제공하는데 있다.

[0007] 본 발명의 또 다른 목적은 항상 복원 임계 값 개수 이상의 부분 키를 읽을 수 있도록 유지하기 위해서, 개별 키 보관 서버 즉 분산 키 보관 서버에서 해당 부분 키 정보를 정상적으로 보관하고 있는지를 검증하고, 만일 특정 키 보관 서버에서 정상적으로 부분 키 정보를 보관하고 있지 않다면, 정상 동작하는 또 다른 키 보관 서버에 재저장함으로써, 항상 일정 개수 이상의 부분 키 보관 서버들이 정상 동작하도록 유지하는, 공개 검증 가능한 블록체인 지갑 키 보관 방법 및 장치를 제공하는데 있다.

과제의 해결 수단

[0008] 상술한 기술적 과제를 해결하기 위한 본 발명의 일 측면에 따른 블록체인 지갑 키 보관 시스템은, 사용자 프로그램과 키 보관 서비스 프로그램을 운영하는 복수의 분산 키 보관 서버를 포함한다. 분산 키 보관 서버는 서비스 제공자로서 사용자 응용 프로그램으로부터 암호화 키 보관 요청을 수신하는 보관 서비스 프로그램과 이를 통해 부분 키를 기록하는 데이터베이스를 포함한다. 사용자 프로그램은 응용 프로그램의 일종으로 암호화키를 분할하고 복원하는 키 분산/복원 실행부와 분산 키 보관 서버에 대한 키 보관 검증을 진행하는 감시/검증 실행부를 포함한다.

[0009] 일실시예에서, 키 분산/복원 실행부에서는 비밀 키 공유 기법을 통해 사용자 암호화 키를 분할하는 방법을 사용하는 환경에서 PVSS(public verifiable secret sharing) 기법을 활용하여 공개 검증 가능한 블록체인 지갑 키 보관 방안을 제시한다. 그리고 감시/검증 실행부는 특정 분산 키 보관 서버가 유효한 부분 키를 소유하는지 감시하고 유효한 부분 키를 소유하지 않았을 때, 해당 서버에 유효한 부분 키를 재생성해 전달해 주거나, 필요한 경우, 부분 키 재생성 및 서비스 서버 재구성을 통해 일정 수준의 사용자 암호화 키 보관 서비스의 신뢰성을 유지하는 것을 포함한다.

[0010] 일실시예에서, 상기 사용자 암호화 키 보관 서비스의 신뢰성을 유지하는 것은, 복원 신뢰 수준을 일정 수준으로 유지하는 것으로서, 유효한 부분키를 유지하지 않는 분산 키 보관 서버가 발견되는 경우, 해당 부분 키를 다시 생성하여 분산 키 보관 서버에 유효한 부분 키 정보를 다시 전달하는 것을 포함한다.

[0011] 상술한 기술적 과제를 해결하기 위한 본 발명의 다른 측면에 따른 블록체인 지갑 키 보관 방법은, 사용자 단말에 탑재된 사용자 프로그램에 의해 수행되는 공개 검증 가능한 블록체인 지갑 키 보관 방법으로서, 사용자 프로그램에 탑재된 키 분산/복원 실행부에 의해 사용자 암호키를 분할하여 확정 값과 함께 부분 키를 생성하는 단계; 부분 키를 확정 값과 함께 분산 키 보관 서버의 공개키로 암호화하는 단계; 및 공개키로 암호화된 부분 키를 분산 키 보관 서버로 전달하는 단계를 포함한다.

[0012] 일실시예에서, 블록체인 지갑 키 보관 방법은, 상기 전달하는 단계 후에, 분산 키 보관 서버가 유효한 부분 키를 소유하고 있는지 감시하거나 검증하는 단계를 더 포함한다.

[0013] 일실시예에서, 상기 검증하는 단계는, 분산 키 보관 서버의 보관 서비스 프로그램으로 검증 요청을 전송하는 단계; 분산 키 보관 서버로부터 무작위로 생성한 제1 상수 값을 받는 단계; 부분 키의 검증 확인 요청값으로 무작위로 생성한 제2 상수 값을 보관 서비스 프로그램에 전달하는 단계; 분산 키 보관 서버로부터 제1 상수 값, 제2

상수 값 및 기저장된 부분 키 값을 이용하여 생성한 증명 값을 받는 단계; 및 제1 상수 값, 제2 상수 값 및 증명 값을 이용하여 분산 키 보관 서버가 유효한 부분 키를 저장하고 있는지 여부를 검증하는 단계를 포함한다.

[0014] 일실시예에서, 상기 여부를 검증하는 단계는, 분산 키 보관 서버로부터 부분 키를 받지 않고 분산 키 분산 서버에 유효한 부분 키가 저장되어 있음을 수학적으로 검증하는 단계를 포함한다.

[0015] 상술한 기술적 과제를 해결하기 위한 본 발명의 또 다른 측면에 따른 블록체인 지갑 키 보관 장치는, 사용자 프로그램을 포함하는 공개 검증 가능한 블록체인 지갑 키 보관 장치로서, 사용자 프로그램에 탑재되는 키 분산/복원 실행부와 감시/검증 실행부를 포함한다. 감시/검증 실행부는 사용자 암호키를 분할하여 확정 값과 함께 부분 키를 생성하고, 부분 키를 확정 값과 함께 분산 키 보관 서버의 공개키로 암호화하고, 상기 공개키로 암호화된 부분 키를 상기 분산 키 보관 서버로 전달한다. 여기서 확정 값은 하기의 [수학식 1]의 다항식에서 각 차수 x^i의 상수 a_i에 대한 묶음값들로 정의된다.

[0016] 일실시예에서, 감시/검증 실행부는 확정 값을 생성한 후 상기 다항식 상에서의 한 점 (i, P(i))으로 i번째 부분 키를 생성한다.

[0017] 일실시예에서, 감시/검증 실행부는 부분 키를 받아 저장하는 분산 키 보관 서버가 유효한 부분 키를 소유하고 있는지를 감지하거나 검증한다.

[0018] 일실시예에서, 감시/검증 실행부는 유효한 부분 키의 검증을 위해 분산 키 보관 서버의 보관 서비스 프로그램으로 검증 요청을 전송하고; 분산 키 보관 서버로부터 무작위로 생성한 제1 상수 값을 받고; 부분 키의 검증 확인 요청값으로 무작위로 생성한 제2 상수 값을 보관 서비스 프로그램에 전달하고; 분산 키 보관 서버로부터 제1 상수 값, 제2 상수 값 및 기저장된 부분 키 값을 이용하여 생성한 증명 값을 받고; 제1 상수 값, 제2 상수 값 및 증명 값을 이용하여 분산 키 보관 서버가 유효한 부분 키를 저장하고 있는지를 검증한다.

[0019] 일실시예에서, 감시/검증 실행부는 유효한 부분 키의 검증 과정에서 동형이산로그(discrete logarithm equality) 수학식으로부터 도출되는 값을 확정 값과 함께 이용한다.

[0020] 일실시예에서, 감시/검증 실행부는 상기 검증 과정에서 동형이산로그 수학식을 만족하는 경우, 분산 키 보관 서버로부터 부분 키를 받지 않고 분산 키 분산 서버에 유효한 부분 키가 저장되어 있음을 수학적으로 검증한다.

[0021] 일실시예에서, 감시/검증 실행부는 상기 검증 과정을 통해 유효한 부분 키를 저장하고 있지 않은 재분배 대상 서버의 정보를 저장한다.

[0022] 일실시예에서, 감시/검증 실행부는 복원 임계값 이하의 서버 개수에 대하여 유효한 부분 키의 저장 여부에 대한 검증이 각각 완료되면, 유효한 부분 키를 저장하고 있지 않은 분산 키 보관 서버의 정보에 기초하여 분산 키를 재분배할 수 있다.

발명의 효과

[0023] 상술한 공개 검증 가능한 블록체인 지갑 키 보관 방법 및 장치를 사용하는 경우에는, 사용자 암호화 키를 분할하고 각 부분 키를 복수개의 분산 키 보관 서버들에 분산 저장하는 분산 키 보관 시스템에서, 개별 키 보관 시스템에서 보관하고 있는 부분 키 정보가 정상적 정보인지, 즉 복구 가능한지 여부를 해당 부분 키 정보를 노출하지 않으면서 공개적으로 검증할 수 있다.

[0024] 또한, 키 보관 서비스 서버 즉, 분산 키 보관 서버가 문제가 생겨 복원 임계값 미만의 부분 키들만 읽을 수 있는 경우, 암호화 키 복원이 불가능한데, 본 발명에서는 암호화 키 복구가 불가능할 경우를 대비하여, 예방적으로 분산 키 보관 서버의 동작 여부를 미리 검증하여, 다른 키 보관 서버를 이용하거나 부분 키 복구 과정을 진행시키는 등으로 대응함으로써, 항상 복원 임계값 이상의 부분 키 읽기가 가능하게 유지할 수 있고, 아울러 암호화 키 복구가 불가능한 상황을 사전에 예방할 수 있는 효과가 있다.

[0025] 본 발명에 의하면, 부분 키 보관 서버의 정상 동작 여부를 검증하는 방법을 제시하고, 필요시 암호화 키 재분할 및 재배치하는 방안을 제공할 수 있다.

도면의 간단한 설명

[0026] 도 1은 본 발명의 일실시예에 따른 감시 및 검증 가능한 분산 키 보관 시스템의 구성을 보여주는 도면이다.

도 2a 및 도 2b는 도 1의 시스템의 주요 작동 과정을 예시한 도면들이다.

도 3은 도 1의 시스템에서 사용자 프로그램상의 감시/검증 실행부와 분산 키 보관 서버의 보관 서비스 프로그램 간의 동작 프로토콜을 나타낸 도면이다.

도 4는 도 1의 시스템에 채용할 수 있는 블록체인 지갑 키 보관 방법에 대한 흐름도이다.

도 5는 본 발명의 다른 실시예에 따른 블록체인 지갑 키 보관 방법에 대한 흐름도이다.

도 6은 도 5의 방법의 검증 과정에 대한 상세 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0027] 본 발명은 다양한 변경을 가할 수 있고 여러 가지 실시예를 가질 수 있는 바, 특정 실시예들을 도면에 예시하고 상세하게 설명하고자 한다. 그러나, 이는 본 발명을 특정한 실시 형태에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다.

[0028] 제1, 제2 등의 용어는 다양한 구성요소들을 설명하는데 사용될 수 있지만, 상기 구성요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 사용된다. 예를 들어, 본 발명의 권리 범위를 벗어나지 않으면서 제1 구성요소는 제2 구성요소로 명명될 수 있고, 유사하게 제2 구성요소도 제1 구성요소로 명명될 수 있다. 및/또는 이라는 용어는 복수의 관련된 기재된 항목들의 조합 또는 복수의 관련된 기재된 항목들 중의 어느 항목을 포함한다.

[0029] 어떤 구성요소가 다른 구성요소에 "연결되어" 있다거나 "접속되어" 있다고 언급된 때에는, 그 다른 구성요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성요소가 존재할 수도 있다고 이해되어야 할 것이다. 반면에, 어떤 구성요소가 다른 구성요소에 "직접 연결되어" 있다거나 "직접 접속되어" 있다고 언급된 때에는, 중간에 다른 구성요소가 존재하지 않는 것으로 이해되어야 할 것이다.

[0030] 본 출원에서 사용한 용어는 단지 특정한 실시예를 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 출원에서, "포함하다" 또는 "가지다" 등의 용어는 명세서상에 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] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가지고 있다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥 상 가지는 의미와 일치하는 의미를 가진 것으로 해석되어야 하며, 본 출원에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[0032] 본 발명의 바람직한 실시예를 설명하기에 앞서 본 기술분야의 몇 가지 주요 용어와 표현을 본 실시예와 관련하여 설명하면 다음과 같다.

[0033] [암호 키]

[0034] 암호 키란 암호화 및 복호화를 수행하기 위해 암호화 기법 및 프로그램에서 사용하는 키를 말한다. 암호 키의 종류는 크게 대칭 키, 비 대칭 키 방식으로 나눌 수 있다. 대칭키 방식은 키 하나로 암호화 및 복호화하는 방법을 말한다. 비 대칭키 방식은 개인키와 공개키의 두 개의 키 쌍을 이용해 암호화 및 복호화하는 방법을 말한다. 본 실시예에서는 비 대칭 키 암호화 방식에서 개인이 소유한 개인 키를 암호키라고 칭한다. 특히, 블록체인에서 사용하는 개인 키를 칭하고 이를 보관하는 방법 및 장치를 제안한다.

[0036] [비밀 값 공유]

[0037] 비밀 값 공유(secret sharing)는 특정한 비밀 값을 나누어 보관하는 방법으로서, 암호 키를 여러 부분 키로 나누어 분산 저장하는 방법을 지칭한다. 대표적인 방법으로는 샤미르(Shamir)의 비밀 값 공유와 Blakley의 비밀 값 공유 방법이 있다.

[0038] 본 실시예에서는 Shamir의 방법([문헌 1] 참조)을 이용하여 비밀 값을 공유한다. Shamir의 비밀 값 공유 방법은 다항식을 이용한다. 이 방법을 이용하기 위해서는 't'라는 장치 설정값이 필요하다. t는 다항식의 최고차항을

결정하며, 이는 비밀 값을 복구할 때 필요한 부분 키의 개수를 의미한다.

[0039] 본 실시예에서는 또한 t를 복원 임계값으로 정의한다. 따라서 비밀 키 K를 부분 키로 만들어 보관하기 위해 t-1 차의 다항식 P(x)를 생성한다. 다항식은 다음의 [수학식 1]과 같이 표현되고, 부분 키는 P(x)의 한 점인 (x,P(x))가 된다.

수학식 1

[0040] $$P(x)=K+\sum_{i=1}^{t-1}a_i x^i$$

[0041] [문헌 1] Adi Shamir. How to share a secret, Communications of the ACM, 1979, Vol 22. 612-613pp.

[0043] [공개 검증 가능한 키 공유(Publicly Verifiable Secret Sharing, PVSS)]

[0044] 기존 Shamir의 비밀 값 공유 방법은, 비밀 키로부터 부분 키들을 생성하고 보관할 때, 각 부분 키가 특정한 키로부터 생성된 부분 값임을 확인할 방법이 없다. 이를 해결하기 위해 PVSS[문헌2]에서는 다항식 P(x)를 생성할 때 만들어지는 확정(commitment) 값 C를 이용한다.

[0045] 확정 값 C는 [수학식 1]의 다항식에서 각 차수 x^i의 상수 a_i에 대한 묶음값들로 정의되며, 확정값 C를 통해 한 점이 특정 다항식 P(x) 상의 점인지 검증할 수 있다. 이에 대하여는 본 실시예의 상세한 설명에서 자세히 설명될 것이다.

[0046] 확정값 C를 활용한다면, 어떤 부분 값을 나타내는 한 점 (x,y)가 특정 다항식 P(x)로부터 계산된 점인지는 누구든지 확인할 수 있다. 상기의 PVSS 특징이 본 실시예에 적용되는 방식은 본 실시예의 예제와 함께 아래에서 자세히 설명하기로 한다.

[0047] [문헌 2] Markus Stadler. Publicly Verifiable Secret Sharing. EUROCRYPT'96: Proceedings of the 15th annual international conference on Theory and application of cryptographic techniques, 1996, ISBN 978-3-540-61186-8,190-199pp.

[0049] [비밀 값 공유 기반 키 보관 서비스]

[0050] 비밀 값 공유 기반 키 보관 서비스는 비밀 값 공유 기법을 이용하여 암호화키를 분할하여 분산 보관한다. 즉, 사용자 암호화 키를 분할하고, 개별 부분 키를 복수개의 키 보관 서버 혹은 서비스 제공자들에 분산 저장하고, 사용자 암호화 키가 분실되었을 경우, 복원 임계값 개수 이상의 부분 키 정보를 키 보관 서버들을 통해 읽어옴으로써 사용자 암호화 키를 복구한다.

[0051] 비밀값 공유 기반 키 보관 서비스가 정상적으로 동작하기 위해서는 항상 복원 임계값 개수 이상의 키 보관 서버들이 정확한 부분 키 정보를 저장하고 있음을 전제로 한다. 하지만, 사용자 입장에서는 이를 검증할 방법이 없다. 다시 말해 암호 키를 부분 키로 나누어 서버들이 보관할 때, 각 서버가 유효한 부분 키를 소유중인지 사용자 관점에서 유효성을 검증하기 위해서는 복원 임계값 개수 이상의 부분 키 값을 읽은 후 사용자 암호화 키를 복원해 보아야 한다. 이는 사용자 컴퓨팅 자원이나 네트워크 자원에 매우 큰 오버헤드를 가지며, 또한 빈번한 복원 과정에서 암호화 키 유출 가능성을 높이는 문제가 있다.

[0053] [키 보관 방법 (중앙 집중식 서비스- one point failure)]

[0054] 중앙집중식 암호화키 관리 서비스는 암호화 키 생성부터 보관까지 담당하는 서비스로 이루어져 있다. 예를 들어 아마존 키 보관 서비스(https://aws.amazon.com/ko/kms/), 네이버 키 보관 서비스(https://www.ncloud.com/product/security/kms) 등이 존재한다. 따라서 해당 컴퓨터가 암호 키의 원본을 가지고 있으므로, 두 가지 문제가 발생하게 된다.

[0055] 첫번째로 해당 컴퓨터가 악의적인 공격에 의해 해킹당했을 경우이다. 해당 컴퓨터의 자료가 탈취당한 경우, 사용자의 암호 키 원본을 소유하는 중이므로 보안에 민감한 암호 키를 그대로 탈취당하게 된다.

[0056] 두번째로 해당 컴퓨터가 악의적인 공격 또는 여러 이유로 서비스 불가 상태가 되었을 경우이다. 서비스 불가는 해당 컴퓨터의 고장 또는 암호 키를 저장하고 있는 데이터베이스의 복구 불가능한 상태 등 저장된 키를 소실 상

태를 뜻한다.

[0057] 본 실시예에서는 분산 키 보관 방법을 사용하므로 기본적으로 중앙 집중식 키 보관 서비스의 문제점을 가지지 않는다.

[0059] 이하, 본 발명의 바람직한 실시예를, 첨부한 도면들을 참조하여 보다 상세하게 설명한다.

[0060] 도 1은 본 발명의 일실시예에 따른 감시 및 검증 가능한 분산 키 보관 시스템의 구성을 보여주는 도면이다. 그리고 도 2a 및 도 2b는 도 1의 시스템의 주요 작동 과정을 예시한 도면들이다.

[0061] 도 1, 도 2a 및 도 2b를 참조하면, 본 실시예에 따른 공개적 검증 가능한 블록체인 지갑 키 보관 장치는 복수의 분산 키 보관 서버(200a~200n) 및 분산 키 보관 서버와 연동하는 사용자 프로그램(100)을 포함한다.

[0062] 사용자 프로그램은 컴퓨팅 장치, 모바일 단말 등의 사용자 단말에 탑재되고 사용자 암호화 키를 분할하여 복수개의 부분 키를 생성한다.

[0063] 각 분산 키 보관 서버들은 사용자 프로그램(100)으로부터 전송된 부분 키를 각 데이터베이스(212a~212n)에 저장하는 보관 서비스 프로그램(210a~210n)을 포함한다.

[0064] 각 분산 키 보관 서버(200a~200n)는 공개키 인프라(Public Key Infrastructure, PKI)에서 정의하는 공개키/비밀키 쌍을 사용한다. 그리고 사용자 프로그램(100)은 부분 키를 각 분산 키 보관 서버의 공개키로 암호화하여 각 서버에 전달한다. 따라서 본 실시예에서는 사용자 프로그램(100)과 분산 키 보관 서버 간에 안전한 통신을 지원한다.

[0065] 각 분산 키 보관 서버(200a~200n)의 보관 서비스 프로그램(210a~210n), 데이터베이스(212a~212n), 및 보관되는 부분 키(112a~112n)의 기능은 동일하므로, 이하 에서는 일반적으로 i(임의의 자연수)번째 분산 키 보관 서버(200i)에 설치된 보관 서비스 프로그램(210i), 데이터베이스(212i) 및 부분 키(112i)를 기준으로 그 기능에 대해 설명하기로 한다. 그리고 이하에서는 설명 및 도시의 편의를 위해 분산 키 보관 서버(200i), 데이터베이스(212i), 및 부분키(112i)를 분산 키 보관서버(200), 데이터베이스(212) 및 부분 키(112)로 기재하기로 한다.

[0066] 먼저, 도 2a에 도시된 바와 같이, 사용자 프로그램(100)은 키 분산/복원 실행부(122)와 감시/검증 실행부(124)를 포함한다. 키 분산/복원 실행부(122)는 사용자 암호화 키(110)를 PVSS 기법을 이용하여 분할함으로써 복수개 부분 키(112a~112n)들을 생성한다. 개별 부분 키(112)는 분산 키 보관 서버(200)의 공개키로 부분 키를 암호화하여 전송되며, 결과적으로 복수의 분산 키 보관 서버들에게 개별적으로 부분 키들을 분산 저장한다.

[0067] 또한 키 분산/복원 실행부(122)는 필요한 경우 분산 키 보관 서버(200)로부터 부분 키(112)를 전달받아 사용자의 암호 키(110)를 원상태로 복원하는 역할을 한다. 이때 사용자 암호화 키 분할 때 설정한 복원 임계값에 따라, 읽어야 하는 부분 키 개수가 결정된다.

[0068] 사용자 프로그램(100)은 감시/검증 실행부(124)를 통해 각 분산 키 보관 서버가 정상적으로 부분 키를 보관하고 있는지 검증하고, 사용자에게 필요하다면 부분키 재생성 및 분산 키 보관 서버 재구성을 통해 항상 복원 임계값을 상회하는 일정 개수 이상의 분산 키 보관 서버에서 정확한 부분 키 정보를 저장하게 함으로써, 사용자 암호화 키 보관 서비스 신뢰성을 보장한다.

[0069] 구체적으로, 도 2b에 도시된 바와 같이, 키 분산/복원 실행부(122)는 PVSS 기법을 이용하여 사용자 암호키(110)를 분할하여 부분 키(112a~112n)를 생성하고, 확정 값 C를 함께 생성한다. PVSS 과정을 통해 부분 키를 생성하는 과정을 보다 자세히 서술하면 다음의 (1) 내지 (5)와 같다.

[0070] (1) 먼저 복원 임계값은 t 로 표현한다.

[0071] (2) 암호키(110)를 K로 대입하여 t-1차 다항식을 구성한다. t-1차 다항식 P(x)는 [수학식 1]과 같다.

[0072] [수학식 1]

[0073] $$P(x)=K+\sum_{i=1}^{t-1} a_i x^i$$

[0074] (3) P(x)에 기반하여 추후 검증을 위한 확정 값 C를 생성한다. 확정 값 C는 [수학식 2]와 같다.

수학식 2

[0075] $$C=(H,H^{K},\bigcup_{i=1}^{t-1}H^{a_i},\bigcup_{i=1}^{n}X_i^{P(i)})$$

[0076] [수학식 2]에서, H는 일반적인 암호화에서 사용하는 큰 소수(prime number) 또는 타원 곡선(Elliptic Curve)에서 한 점이다. H^K는 K를 타원곡선 상에서 H값을 기준으로 곱 연산한 것을 의미하며, H^K와 H값으로 K를 유추할 수 없다.

[0077] 본 실시예에서는 타원곡선 암호화를 사용하는 것으로 H를 기준점으로 사용하는 것으로 서술하나, 이에 한정되지 않고, 암호학 특성을 따르는 다른 경우도 가능하다.

[0078] (4) P(x) 상에서의 한 점 (i,P(i))으로 i번째 부분 키(112i)를 생성한다.

[0079] (5) 특정 부분 키(112)는 해당 확정 값 C와 함께 특정 분산 키 보관 서버(200)의 공개키로 암호화하여 해당 분산 키 보관 서버(200)로 전달된다. 이때 분산 키 보관 서버의 공개키를 X, 특정 데이터 D를 해당 공개키로 암호화한 것을 $E_X(D)$로 나타내기로 한다. 따라서, $E_{X_i}(P(i))$는 부분 키 Pi를 공개키로 암호화한 정보를 나타낸다.

[0080] 도 3은 도 1의 시스템에서 사용자 프로그램상의 감시/검증 실행부와 분산 키 보관 서버의 보관 서비스 프로그램 간의 동작 프로토콜을 나타낸 도면이다.

[0081] 도 3은 사용자 프로그램(100) 상의 감시/검증 실행부(124)와 분산 키 보관 서버에 탑재된 보관 서비스 프로그램(210i) 간의 동작 프로토콜을 서술한다.

[0082] 즉, 분산 키 보관 서버가 유효한 부분 키를 소유하고 있는지 감시/검증을 하기 위한 동작 순서는 감시/검증 실행부와 보관 서비스 프로그램 간 4단계 통신 순서로 진행될 수 있다.

[0083] 구체적으로, 첫째, 검증 요청(S301)으로써, 감시/검증 실행부(124)는 분산 키 보관 서버(200)의 보관 서비스 프로그램(210i)으로 검증요청을 전송한다(S301).

[0084] 둘째, 보관 서비스 프로그램(210i)은 검증 요청(S301)에 대한 응답으로 무작위로 생성한 상수 값 w(이하 제1 상수 값이라고도 한다)를 감시/검증 실행부(124)로 전달한다(S302). 보관 서비스 프로그램(210i)은 상수 값 w를 서버의 저장부나 데이터베이스에 저장한다.

[0085] 셋째, 감시/검증 실행부(124)는 무작위로 생성한 상수 값 c(이하 제2 상수 값이라고도 한다)를 검증 확인 요청 값으로 보관 서비스 프로그램(210i)에게 전달한다(S303). 감시/검증 실행부(124)는 보관 서비스 프로그램(210i)로부터 받은 제1 상수값과 보관 서비스 프로그램(210i)로 전송한 제2 상수값을 사용자 단말의 저장부나 데이터베이스에 저장한다.

[0086] 넷째, 보관 서비스 프로그램(210i)은 저장한 상수 값 w와 수신한 상수 값 c, 그리고 자체적으로 데이터베이스에 저장된 부분 키(112) 값을 이용하여 증명 값 r을 생성하고, 감시/검증 실행부(124)로 전달한다(S304).

[0087] i 번째 부분키를 저장하는 보관 서비스 프로그램(210i)에서 증명 값 r은 다음과 같은 [수학식 3]으로부터 도출한다.

수학식 3

[0088] $$r=w-P(i)*c$$

[0089] 이때 감시/검증 실행부(124)는 두 상수값 w 와 c, 그리고 증명값 r을 이용하여, 보관 서비스 프로그램(210i)을 실행하는 분산 키 보관 서버(200i)가 유효한 부분 키(112i)를 정확하게 저장하고 있는지 여부를 검증할 수 있다.

[0090] 보다 자세히 설명하면, 감시/검증 실행부(124)에서 무작위 상수 값 w, c와 확정 값 C, 증명 값 r 및 공개키 X_i

를 이용하여 유효한 부분 키를 소유하는지 검증하는 방법은 다음과 같은 동형이산로그(discrete logarithm equality) 수학식으로부터 도출된다.

수학식 4

[0091] $$\log_{g_1} h_1 = \log_{g_2} h_2 (h_1 = g_1^{P(i)}, h_2 = g_2^{P(i)}, g_1 = H, g_2 = X_i)$$

[0092] 위의 [수학식 4]는 PVSS의 특징으로써, $g_2^{P(i)}$의 경우 $g_2 = X_i$이므로 부분 키 P(i)를 공개키로 곱한 것을 의미하고, $g_1^{P(i)}$의 경우 타원곡선 위의 한 점 H로 곱한 값이며 검증 과정에서 확정 값 C와 함께 이용하게 된다.

[0093] 위의 [수학식 4]를 만족한다면, 감시/검증 실행부(124)는 분산 키 보관 서버(200i)로부터 부분 키(112i)를 받지 않고 공개된 값인 분산 키 보관 서버의 공개키 X_i, 확정 값 C, 두 상수 값 w와 c 그리고 증명 값 r을 이용하여 해당 분산 키 보관 서버가 유효한 값을 가지고 있음을 수학적으로 검증할 수 있다. 이러한 검증 과정은 아래와 같은 [수학식 5] 및 [수학식 6]으로 증명할 수 있다.

수학식 5

[0094] $$H^w = H^r h_1^c$$

수학식 6

[0095] $$X_i^w = X_i^r h_2^c$$

[0096] 위의 [수학식 5]와 [수학식 6]을 모두 만족시킨다면, 감시/검증 실행부(124)는 분산 키 보관 서버(200i)로부터 받은 증명 값 r을 통해 해당 서버가 유효한 부분 키를 소유하는지 증명할 수 있다.

[0097] [수학식 5]는 아래와 같은 [수학식 7] 내지 [수학식 10]의 수학적 계산 과정으로 확인 가능하다.

수학식 7

[0098] $$H^w = H^r h_1^c = H^r (H^{P(i)})^c$$

[0099] 이때, [수학식 7]에서 P(i)를 모르더라도 $H^{P(i)}$는 다음의 [수학식 8]과 같이 구할 수 있다.

수학식 8

[0100] $$H^{P(i)} = H^{K + \sum_{j=1}^{t-1} a_j^t} = H^K \times (H^{a_1})^1 \times (H^{a_2})^2 \times \ldots \times (H^{a_{t-1}})^{t-1}$$

[0101] 위의 [수학식 8]에서 $H^{a_1}, H^{a_2}, \ldots, H^{a_{t-1}}$은 확정 값 C에 포함되어 있으므로, $H^{P(i)}$를 계산해낼 수 있다. 이때 $H^{P(i)}$와 r값에 문제가 없다면 아래와 같은 [수학식 9]가 성립한다.

수학식 9

[0102] $$H^{w}=H^{w-P(i)\times c}H^{P(i)\times c}=H^{w}\times H^{-P(i)\times c+P(i)\times c}=H^{w}$$

[0103] 또한, 위의 [수학식 5]의 확인 과정과 유사하게 [수학식 6]도 아래의 [수학식 10]을 통해 확인 가능하다.

수학식 10

[0104] $$X_i^{w}=X_i^{r}h_2^{c}=X_i^{r}(X_i^{P(i)})^{c}$$

[0105] 위의 [수학식 10]에서 $X_i^{P(i)}$는 부분 키를 분산 키 보관 서버(200i)의 공개 키로 곱한 데이터로서, 최초 사용자 프로그램에서 부분 키 전달 시에 포함된 확정 값 C에서 추출하거나 검증과정에서 증명 값 r과 함께 분산 키 보관 서버에 요청할 수 있다. 이때 $X_i^{P(i)}$와 r값에 문제가 없다면 아래와 같은 [수학식 11]이 성립한다.

수학식 11

[0106] $$X_i^{w}=X_i^{(w-P(i)\times c)}X_i^{P(i)\times c}=X_i^{w}\times X_i^{-P(i)\times c+P(i)\times c}=x_i^{w}$$

[0107] 위에서 살핀 바와 같이, [수학식 5]와 [수학식 6] 모두를 만족한다면, 감시/감증 실행부는 분산 키 보관 서버는 유효한 부분키를 소유하고 있다고 판단할 수 있다.

[0108] 이와 같이, 본 실시예에 따르면 보관 서비스 프로그램(210i)을 통해 해당 서버가 특정 암호 키에 대한 유효한 부분 키를 소유하고 있는지 확인할 수 있으며, 이는 최초 암호 키에 대한 확정 값 C와 공개키 X_i를 알고 있는 감시/검증 실행부(124)를 통해 실행될 수 있다.

[0109] 이때, 암호키 특성상 공개키 X_i는 누구에게 든 공개되어 있고, 암호 키에 대한 확정 값 C로는 암호 키를 추측할 수 없으므로, 감시/검증 기능을 중요한 정보의 공유 없이 외부 주체에게 위임할 수 있음을 의미하고 이는 공개적으로 검증 가능함을 뜻한다.

[0110] 도 4는 도 1의 시스템에 채용할 수 있는 블록체인 지갑 키 보관 방법에 대한 흐름도이다.

[0111] 도 4를 참조하면, 본 실시예에 따른 블록체인 지갑 키 보관 방법은, 사용자 프로그램 상의 블록체인 지갑 키 보관 방법으로서, 일련의 단계들(S401 내지 S405)의 과정을 반복적으로 진행하여 전체 부분 키 중 유효한 부분 키가 몇 개가 되는지, 즉 몇 개의 분산 키 보관 서버가 정상적으로 부분 키 정보를 유지하고 있는지 모니터링할 수 있다.

[0112] 그리고, 감시/검증 실행부에서 어떤 분산 키 보관 서버에서 정상적으로 부분 키를 유지하지 못한다고 판단할 때는(S405), P(x) 상에서의 한 점 (i,P(i))으로 i 번째 부분 키를 생성하는 단계(S402)로 되돌아가서 해당 부분 키를 확정 값과 함께 해당 혹은 새로운 분산 키 보관 서버의 공개키로 암호화하여 해당 혹은 새로운 분산 키 보관 서버로 전달하고, 그 후에 검증과정을 진행하는 일련의 과정을 통해 비정상적 행위가 감지된 분산 키 보관 서버에게 유효한 부분 키를 다시 저장하게 하거나, 새로운 분산 키 보관 서버에 유효한 부분 키를 저장하거나, 또는 부분 키 전체를 새로 생성하여 모든 분산 키 보관 서버(200a~200n)에 재전달 할 수 있다.

[0113] 이와 같이, 본 발명에 따르면 암호 키로부터 부분 키 생성(S401), 분배(S402~S403), 검증(S404) 및 재분배(S405)과정을 거쳐 분산 키 보관 시스템에 대한 모니터링 및 안정성을 확보할 수 있다.

[0114] 도 5는 본 발명의 다른 실시예에 따른 블록체인 지갑 키 보관 방법에 대한 흐름도이다. 도 6은 도 5의 방법의 검증 과정에 대한 상세 흐름도이다.

[0115] 도 5를 참조하면, 본 실시예에 따른 블록체인 지갑 키 보관 방법은, 사용자 단말의 사용자 프로그램에서 수행되는 일련의 과정으로서, 먼저 장치 설정값(t)에 따라 다항식의 최고 차항을 결정한 후 분산 키 보관 서버들에 보

관하고자 하는 암호 키로부터 부분 키를 생성한다(S501). 그리고, 생성한 부분 키들을 분산 키 보관 서버들에 분배한다(S502).

[0116] 다음, 이후에 수행할 검증 과정의 모든 대상 서버에 대하여 검증이 완료되었는지를 판단할 수 있다(S503).

[0117] 모든 대상 서버의 검증이 완료되지 않았으면(S503의 아니오), 사용자 프로그램의 감시/검증 실행부는 특정 분산 키 보관 서버에 유효한 부분 키가 저장되어 있는지를 검증한다(S504). 해당 서버에 유효한 부분 키가 저장되어 있으면(S505의 예), 다시 상기의 판단 단계(S503)로 되돌아가 나머지 다른 서버들에 대한 검증 과정을 순차적으로 반복 진행한다.

[0118] 그리고 상기의 단계(S504)의 검증 결과, 해당 서버에 유효한 부분 키가 저장되어 있지 않으면(S505의 아니오), 부분 키의 재분배 과정을 수행할 수 있다 (S506). 그런 다음, 상기의 판단 단계(S503)로 되돌아가 나머지 다른 서버들에 대한 검증 과정을 순차적으로 반복 진행한다.

[0119] 한편, 모든 대상 서버에 대하여 검증 과정을 완료한 것으로 판단되면(S503의 예), 모든 검증 대상 서버들에 대한 1회 검증 완료한 것으로 현재의 프로세스를 종료할 수 있다.

[0120] 물론, 본 실시예에 따른 검증 과정은 분산 저장한 암호키의 일부 부분 키를 각각 보관하고 있는 모든 검증 대상 서버에 대하여 일정 회수 반복하도록 설정되거나 일정 시간 주기적으로 혹은 간헐적으로 반복 수행되도록 구현될 수 있다.

[0121] 한편, 전술한 검증 과정(S504)을 분산 키 보관 서버의 측면에서 바라보면 도 6에 도시한 바와 같다.

[0122] 먼저, 분산 키 보관 서버는 사용자 단말로부터 검증 요청을 수신한다(S541).

[0123] 다음, 검증 요청에 응하여 무작위로 제1 상수 값을 생성하고, 제1 상수 값을 사용자 단말에 전달한다(S542). 제1 상수 값은 서버의 저장부나 데이터베이스에 저장된다.

[0124] 다음, 사용자 단말에서 무작위로 생성된 제2 상수 값을 사용자 단말로부터 부분 키의 검증 확인 요청값으로 수신한다(S543).

[0125] 다음, 제1 상수 값, 제2 상수 값과 기저장된 부분 키 값을 이용하여 생성한 증명 값을 사용자 단말로 전달한다(S544).

[0126] 전술한 과정들(S541 내지 S544)에 의하면, 네트워크를 통해 분산 키 보관 서버에 연결되는 사용자 단말은 제1 상수 값, 제2 상수 값 및 증명 값을 이용하여 분산 키 보관 서버가 유효한 부분 키를 정확하게 저장하고 있는지 여부를 검증할 수 있고, 다수의 분산 키 보관 서버들은 사용자 단말의 사용자 프로그램과 연동하여 그것의 암호키 혹은 블록체인 지갑 키 보관 방법을 지원할 수 있다.

[0127] 한편, 본 실시예에 따른 블록체인 지갑 키 보관 방법은 다양한 컴퓨터 수단을 통해 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 컴퓨터 판독 가능 매체에 기록되는 프로그램 명령은 본 발명을 위해 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수 있다.

[0128] 컴퓨터 판독 가능 매체의 예에는 롬(rom), 램(ram), 플래시 메모리(flash memory) 등과 같이 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러(compiler)에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터(interpreter) 등을 사용해서 컴퓨터에 의해 실행될 수 있는 고급 언어 코드를 포함한다. 상술한 하드웨어 장치는 본 발명의 동작을 수행하기 위해 적어도 하나의 소프트웨어 모듈로 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[0129] 이상과 같이 실시예들을 참조하여 설명하였지만, 해당 기술 분야의 숙련된 당업자는 하기의 청구범위에 기재된 본 발명의 사상 및 영역으로부터 벗어나지 않는 범위 내에서 본 발명을 다양하게 수정 및 변경시킬 수 있음을 이해할 수 있을 것이다.

부호의 설명

[0130] 100: 사용자 프로그램

110: 사용자 키

112a ~ 112n: 사용자 부분 키

122: 사용자 키 분산 및 복원 실행 부

124: 부분 키 감시 및 검증 실행 부

130: 사용자

200a ~ 200n: 분산 키 보관 서버

210a ~ 210n: 키 보관 서비스 프로그램

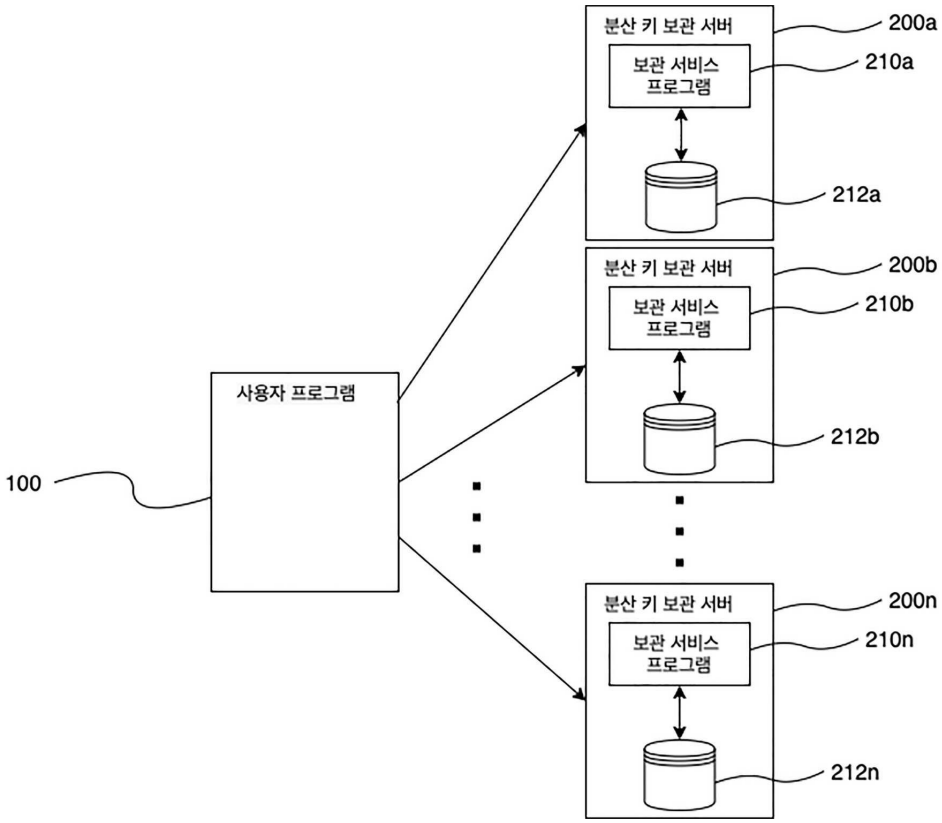
212a ~ 212n: 데이터베이스

S301 ~ S304: 사용자 부분 키 보관 검증 과정

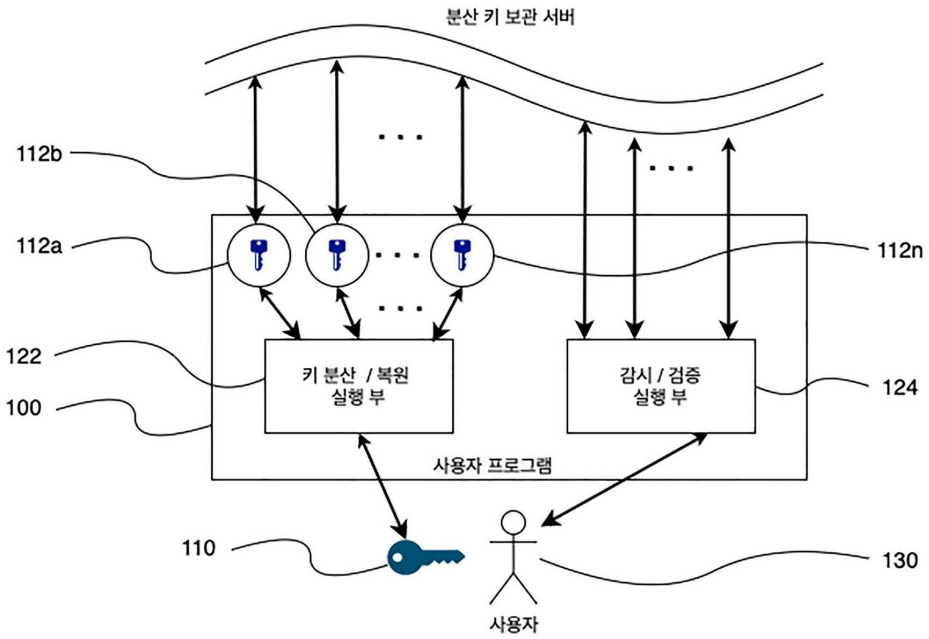
S401 ~ S404: 사용자 프로그램 진행 과정

도면

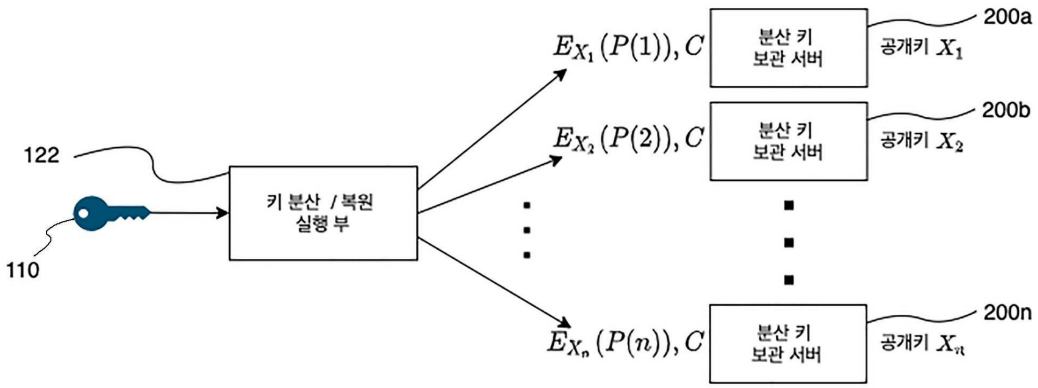
도면1



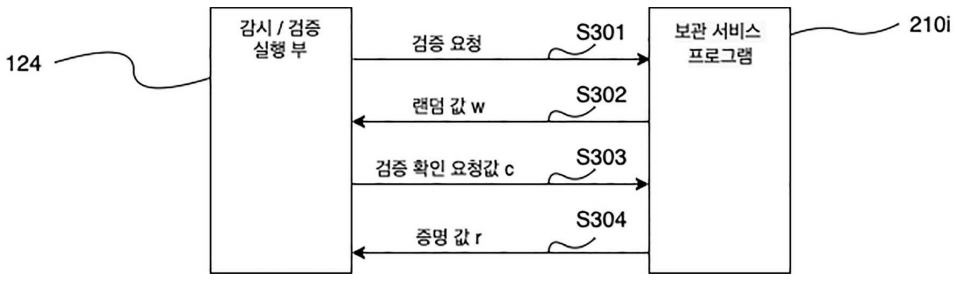
도면2a



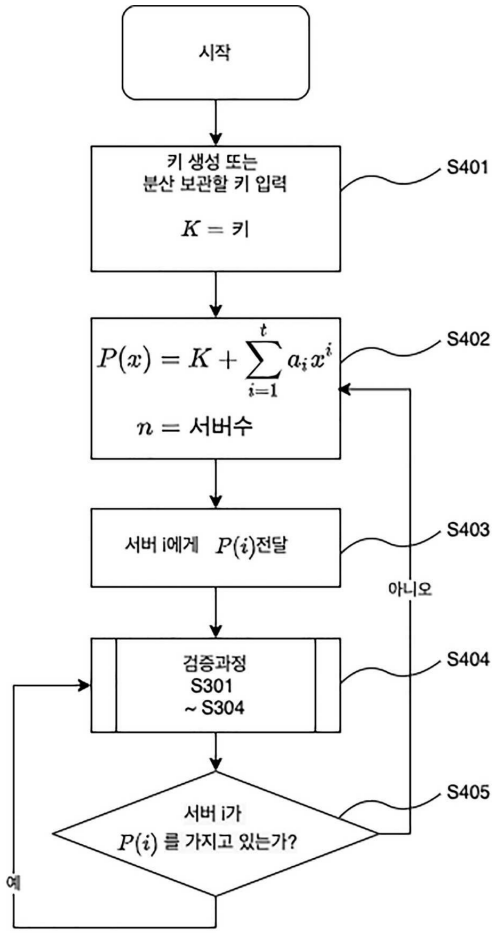
도면2b



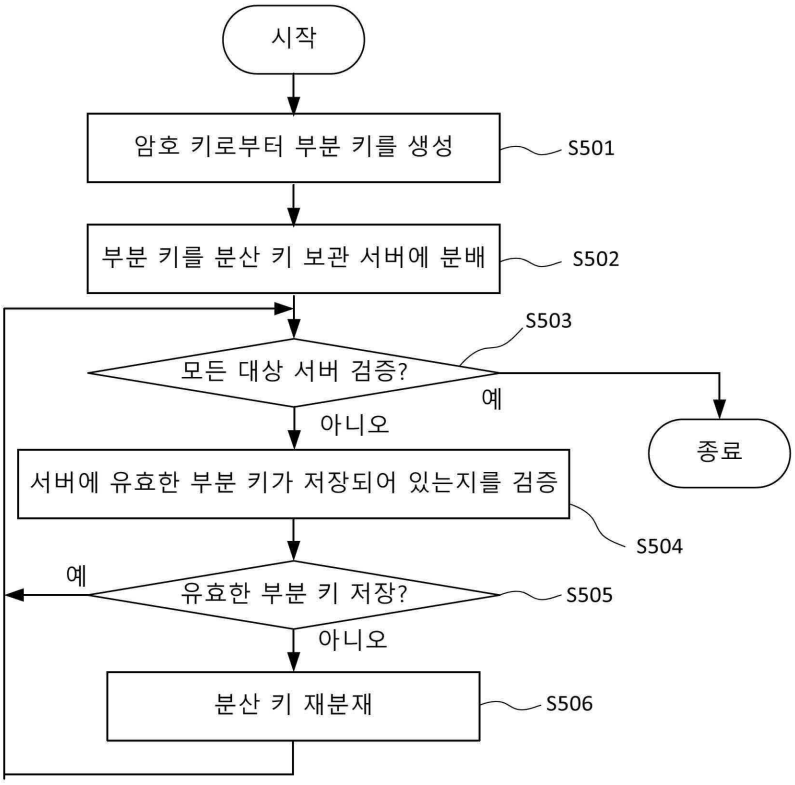
도면3



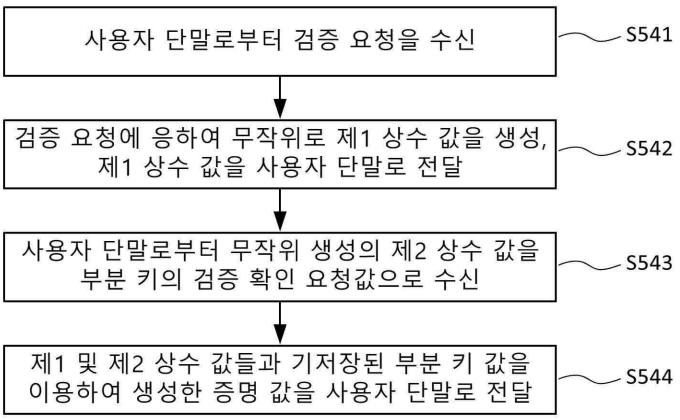
도면4


시작
키 생성 또는
분산 보관할 키 입력
K = 키
S401
$P(x) = K + \sum_{i=1}^{t} a_i x^i$
n = 서버수
S402
서버 i에게 $P(i)$전달
S403
아니오
검증과정
S301
~ S304
S404
서버 i가
$P(i)$ 를 가지고 있는가?
S405
예

도면5


시작
암호 키로부터 부분 키를 생성
S501
부분 키를 분산 키 보관 서버에 분배
S502
S503
모든 대상 서버 검증?
예
아니오
종료
서버에 유효한 부분 키가 저장되어 있는지를 검증
S504
예
유효한 부분 키 저장?
S505
아니오
분산 키 재분재
S506

도면6


사용자 단말로부터 검증 요청을 수신
S541
검증 요청에 응하여 무작위로 제1 상수 값을 생성,
제1 상수 값을 사용자 단말로 전달
S542
사용자 단말로부터 무작위 생성의 제2 상수 값을
부분 키의 검증 확인 요청값으로 수신
S543
제1 및 제2 상수 값들과 기저장된 부분 키 값을
이용하여 생성한 증명 값을 사용자 단말로 전달
S544