



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2020-0065507
(43) 공개일자 2020년06월09일

(51) 국제특허분류(Int. Cl.)
G06Q 20/36 (2012.01) G06Q 20/06 (2012.01)
G06Q 20/38 (2012.01) H04L 9/06 (2006.01)
(52) CPC특허분류
G06Q 20/3674 (2013.01)
G06Q 20/065 (2013.01)
(21) 출원번호 10-2018-0152040
(22) 출원일자 2018년11월30일
심사청구일자 없음

(71) 출원인
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
인호
서울특별시 용산구 이촌로88길 15, 3동 106호 (이촌동, 왕궁아파트)
이대건
서울특별시 용산구 이촌로 347, 16동 401호 (서빙고동, 신동아아파트)
박재용
서울특별시 송파구 송이로33길 7, 301호 (문정동)
(74) 대리인
특허법인엠에이피에스

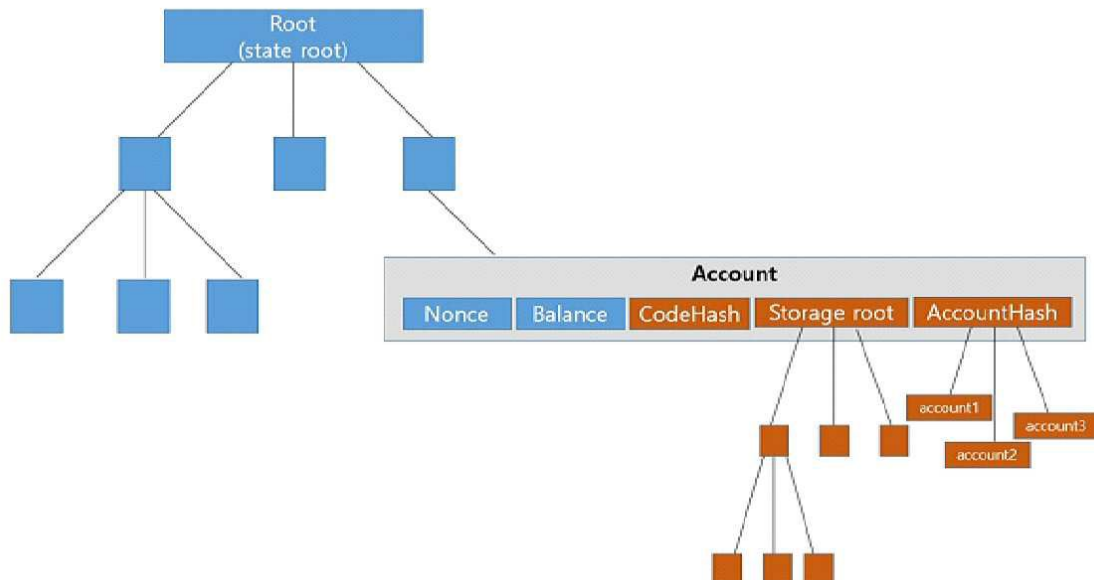
전체 청구항 수 : 총 3 항

(54) 발명의 명칭 **블록체인의 개인키 권한 조절 시스템 및 그 방법**

(57) 요약

본 발명은 블록체인의 개인키 권한 조절 시스템 및 그 방법에 관한 것으로서, 블록체인의 트랜잭션들이 결과를 저장하는 상태 데이터베이스를 포함하는 블록체인 시스템에 의해 수행되는 블록 체인의 개인키 권한 조절 방법에 있어서, a)상기 상태 데이터베이스에 스마트 계약의 주소를 저장하는 어카운트해쉬(AccountHash)를 추가하는 단계; 및 b) 상기 어카운트해쉬에 스마트 계약 주소가 저장된 경우, 트랜잭션이 요청이 해당 어카운트로부터 발생하면 다중서명지갑에서 기설정된 조건에 따라 금액을 지불하고, 상기 어카운트해쉬에 스마트계약 주소가 저장되지 않은 경우, 일반 결제를 진행하는 단계를 포함하는 것이다.

대표도 - 도2



(52) CPC특허분류

G06Q 20/3827 (2013.01)

H04L 9/06 (2013.01)

H04L 9/0819 (2013.01)

H04L 2209/38 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호 20150009360041001

부처명 과학기술정보통신부

연구관리전문기관 정보통신기술진흥센터

연구사업명 SW중심대학지원사업

연구과제명 SW중심대학 지원사업

기 여 율 1/1

주관기관 고려대학교 산학협력단

연구기간 2018.01.01 ~ 2018.12.31

명세서

청구범위

청구항 1

블록체인의 트랜잭션들이 결과를 저장하는 상태 데이터베이스를 포함하는 블록 체인의 개인키 권한 조절 시스템에 있어서,

블록 체인의 개인키 권한 조절 방법을 수행하기 위한 프로그램이 기록된 메모리; 및

상기 프로그램을 실행하기 위한 프로세서를 포함하며,

상기 프로세서는, 상기 프로그램의 실행에 의해,

상기 상태 데이터베이스에 스마트 계약의 주소를 저장하는 어카운트해쉬(AccountHash)를 추가하고,

상기 어카운트해쉬에 스마트 계약 주소가 저장된 경우, 트랜잭션이 요청이 해당 어카운트로부터 발생하면 다중 서명지갑에서 기설정된 조건에 따라 금액을 지불하고,

상기 어카운트해쉬에 스마트계약 주소가 저장되지 않은 경우, 일반 결제를 진행하는 것인, 블록체인의 개인키 권한 조절 시스템.

청구항 2

블록체인의 트랜잭션들이 결과를 저장하는 상태 데이터베이스를 포함하는 블록체인 시스템에 의해 수행되는 블록 체인의 개인키 권한 조절 방법에 있어서,

a)상기 상태 데이터베이스에 스마트 계약의 주소를 저장하는 어카운트해쉬(AccountHash)를 추가하는 단계; 및

b) 상기 어카운트해쉬에 스마트 계약 주소가 저장된 경우, 트랜잭션이 요청이 해당 어카운트로부터 발생하면 다중서명지갑에서 기설정된 조건에 따라 금액을 지불하고, 상기 어카운트해쉬에 스마트계약 주소가 저장되지 않은 경우, 일반 결제를 진행하는 단계를 포함하는 것인, 블록체인의 개인키 권한 조절 방법.

청구항 3

제2항에 있어서,

상기 b) 단계는,

사용자가 자신의 제1 개인키를 스마트 계약과 연결 요청하고, 기저장된 제2 개인키로 상기 제1 개인키의 등록을 승인하는 단계; 및

상기 제1 개인키의 연결 성공시, 상기 제1 개인키에 대한 어카운트의 어카운트해쉬 값에 스마트 계약의 주소를 저장하고, 상기 스마트 계약의 주소의 어카운트해쉬는 상기 제1 개인키에 대한 어카운트를 포함하는 단계를 더 포함하는 것인, 블록체인의 개인키 권한 조절 방법.

발명의 설명

기술 분야

[0001] 본 발명은 블록체인의 개인키 권한 조절 시스템 및 그 방법에 관한 것이다.

배경 기술

[0002] 블록체인(Blockchain) 기술은 2008년 10월 31일 사토시 나카모토(본명: Craig Steven Wright)가 인터넷에 발표한 논문에서 처음 소개되었다. 이 논문에서 비트코인(Bitcoin)을 “P2P 네트워크를 이용해 이중 지불을 막을 수 있으며, 전적으로 거래 당사자 사이에서만 오가는 전자화폐” 라고 소개했다. 즉, 블록체인 기술은 이중 지불과 복제를 막기 위하여 P2P 네트워크를 이용, 거래를 관리하는 중앙 기관이 없이 다수의 비트 코인 사용자가 거래 기록을 함께 관리하는 것이다.

- [0003] 이러한 블록 체인 기술은 최초 블록부터 연결리스트의 형태로 블록들을 연쇄적으로 저장하는 시스템이다. 블록 체인을 이용하는 각 클라이언트마다 P2P 방식으로 블록들을 동기화하여 보유한다. 블록체인에 저장되는 거래의 단위인 각각의 트랜잭션(Transaction)은 공개키 암호 방식 기반으로 그 유효성을 증명한다.
- [0004] 블록체인은 최초의 블록체인 기반 어플리케이션인 비트코인을 시작으로 여러 가지 기술들이 접목되어 여러 분야에서 블록체인을 활용하려는 시도가 계속되고 있다.
- [0005] 한편, 트랜잭션(Transaction)은 블록체인 거래의 단위이며, 스마트 계약 등록, 스마트 계약 함수 실행 등 모든 작업이 트랜잭션으로 이루어진다. 트랜잭션의 수행 결과는 상태DB에 저장된다.
- [0006] 스마트 계약(Smart contract)은 2014년 개발된 이더리움이 최초로 튜링 완전 언어로 작성한 프로그램을 블록체인 시스템에서 실행될 수 있도록 한 것으로서, 블록체인에 올려놓은 프로그램을 스마트 계약(Smart contract)이라고 하고, 토큰, ICO, 다중 서명 지갑 등이 있다.
- [0007] 블록체인 계좌에는 2세대 블록체인 이더리움 이후에 블록체인을 개인키로 생성된 일반계좌와 블록체인의 스마트 계약 기능을 위한 계약 계좌가 존재한다. 일반 계좌는 개인키로부터 생성된 계좌이고, 계약 계좌는 스마트 계약을 블록체인에 등록시 일정한 규칙에 의해 생성되는 계좌이다. 일반 계좌는 개인이 트랜잭션을 생성할 때 사용되며, 계약 계좌는 스마트 계약을 사용할 때 트랜잭션의 수신자가 된다.
- [0008] 다중서명 지갑은 블록체인의 스마트 계약 기술로 생성한 지갑으로 여러 개의 개인키가 소유 및 사용 주체가 되는 지갑이다. 일반적으로 관리자 권한이 있는 하나 또는 여러 개의 개인키가 각의 개인키의 권한 및 출금 한도를 설정할 수 있으며, 여러 개의 개인키로 다중 서명을 해야 큰 금액의 출금이 가능하다. 다중서명 지갑은 프로그램 코드로 작성되기 때문에 지갑에서 돈을 사용할 때 다양한 기능이나 조건을 추가할 수 있다.
- [0009] 도 1은 종래 기술의 블록체인에서 이더리움 기반의 트랜잭션 유효성 검사 과정을 설명하는 도면이다.
- [0010] 도 1을 참고하면, 상태DB(State Database)는 블록체인에서 빠른 서비스를 제공하기 위해 블록체인에 있는 모든 트랜잭션들의 결과를 누적한 데이터베이스이다. 상태 DB에 대표적으로 저장되는 값들에는 모든 계좌의 잔고나 스마트 계약의 프로그램 코드가 있다. 또한 트랜잭션을 생성하거나 실행할 때 [계좌 잔고 $\geq$ 트랜잭션 수수료 + 트랜잭션 값]인지 검사하는 과정에서 계좌 잔고를 상태DB에서 조회하여 빠르게 트랜잭션의 유효성을 검증한다.
- [0011] 개인키에 대한 해킹(거래소 해킹 등), 개인키의 유출 등의 문제는 블록체인의 활성화를 위해 반드시 해결되어야 하는 문제이다. 해당 문제들은 다중서명지갑 스마트 계약을 사용하여 해결할 수 있지만 과정이 복잡해지고 시스템에 기존 프로세스 대비 복잡해진다는 문제점이 있다.
- [0012] 일반 개인키 결제는 (보내는 금액, 받는 사람)의 정보만 있으면 트랜잭션을 생성할 수 있지만, 스마트 컨트랙트 결제는 최소 정보(보내는 금액, 받는사람, 컨트랙트주소)가 필요하다.
- [0013] 스마트 컨트랙트 결제 방식은 보내는 금액은 숫자로 조정할 수 있고, 받는 사람은 결제 시스템에서 지정해줄 수 있지만, 컨트랙트 주소는 추가적인 입력과정이 필요하여 결제를 복잡하게 만드는 문제점이 있다. 또한, 일반적인 다중서명지갑은 다른 계좌에 송금하는 것도 개인키 결제보다 복잡하지만 다른 스마트 컨트랙트를 배포하거나 다른 함수를 호출하려면 프로그램코드를 컴파일해야 해서 더욱 복잡해지는 문제점이 있다.
- [0014] 이러한 다중서명 지갑은 복잡한 결제 절차로 인하여 실제로 많이 사용되지 않고 있고, 만일 실제로 다중서명 지갑이 많이 사용될 경우에 거래소 해킹과 같은 사건 등으로 사용자 피해가 감소될 수 있을 것이다.

발명의 내용

해결하려는 과제

- [0015] 본 발명은 전술한 문제점을 해결하기 위하여, 본 발명의 일 실시예에 따라 개인키로 요청한 결제를 자동으로 스마트 계약에서 처리하는 블록체인의 개인키 권한 조절 시스템 및 그 방법을 제공하는 것에 목적이 있다.
- [0016] 다만, 본 실시예가 이루고자 하는 기술적 과제는 상기된 바와 같은 기술적 과제로 한정되지 않으며, 또 다른 기술적 과제들이 존재할 수 있다.

과제의 해결 수단

- [0017] 상기한 기술적 과제를 달성하기 위한 기술적 수단으로서 본 발명의 일 실시예에 따른 블록체인의 개인키 권한

조절 시스템은, 블록체인의 트랜잭션들이 결과를 저장하는 상태 데이터베이스를 포함하는 블록 체인의 개인키 권한 조절 시스템에 있어서, 블록 체인의 개인키 권한 조절 방법을 수행하기 위한 프로그램이 기록된 메모리; 및 상기 프로그램을 실행하기 위한 프로세서를 포함하며, 상기 프로세서는, 상기 프로그램의 실행에 의해, 상기 상태 데이터베이스에 스마트 계약의 주소를 저장하는 어카운트해쉬(AccountHash)를 추가하고, 상기 어카운트해쉬에 스마트 계약 주소가 저장된 경우, 트랜잭션이 요청이 해당 어카운트로부터 발생하면 다중서명지갑에서 기 설정된 조건에 따라 금액을 지불하고, 상기 어카운트해쉬에 스마트계약 주소가 저장되지 않은 경우, 일반 결제를 진행하는 것이다.

[0018] 상기한 기술적 과제를 달성하기 위한 기술적 수단으로서 본 발명의 일 실시예에 따른 블록체인의 개인키 권한 조절 방법은, 블록체인의 트랜잭션들이 결과를 저장하는 상태 데이터베이스를 포함하는 블록체인 시스템에 의해 수행되는 블록 체인의 개인키 권한 조절 방법에 있어서, a)상기 상태 데이터베이스에 스마트 계약의 주소를 저장하는 어카운트해쉬(AccountHash)를 추가하는 단계; 및 b) 상기 어카운트해쉬에 스마트 계약 주소가 저장된 경우, 트랜잭션이 요청이 해당 어카운트로부터 발생하면 다중서명지갑에서 기 설정된 조건에 따라 금액을 지불하고, 상기 어카운트해쉬에 스마트계약 주소가 저장되지 않은 경우, 일반 결제를 진행하는 단계를 포함하는 것이다.

발명의 효과

[0019] 진술한 본 발명의 과제 해결 수단에 의하면 개인키의 권한을 다중서명지갑과 같은 스마트 계약으로 조절할 수 있고, 스마트 계약으로 이루어지는 상대적으로 복잡한 결제 프로세스를 일반적인 개인키 결제와 같이 단순하게 이루어질 수 있게 함으로써 보편적이고 안전한 결제 시스템 구축이 가능해진다.

[0020] 또한, 본 발명은 개인키의 권한이 스마트 계약으로 조절되는데, 스마트 계약은 프로그래밍 언어로 자유롭게 작성가능하기 때문에 개인키 권한과 관련된 다양한 문제 해결에 사용될 수 있다. 따라서, 본 발명의 일 실시예에 따른 블록체인의 개인키 권한 조절 방법을 기존의 블록 체인 시스템에 적용하면, 사용자 입장에서 일반 개인키가 컨트랙트 생성하거나 함수 호출하는 것과 같은 과정이 요구되므로 접근성이 향상되고, 블록체인 시스템 내부적으로 개인키를 보호할 수 있다.

도면의 간단한 설명

[0021] 도 1은 종래 기술의 블록체인에서 이더리움 기반의 트랜잭션 유효성 검사 과정을 설명하는 도면이다
 도 2는 본 발명의 일 실시예에 따른 블록체인의 개인키 권한 조절 시스템의 구조를 나타낸 도면이다.
 도 3은 본 발명의 일 실시예에 따른 블록체인의 개인키 권한 조절 방법 중 개인키와 스마트 계약을 연결 요청하는 과정을 설명하는 도면이다.
 도 4는 본 발명의 일 실시예에 따른 블록체인의 개인키 권한 조절 방법 중 개인키와 스마트 계약을 연결 성광 과정을 설명하는 도면이다.
 도 5는 본 발명의 일 실시예에 따른 블록체인의 개인키 권한 조절 방법 중 주소의 개인키를 사용하여 계약 계좌에서 지불하는 트랜잭션 생성하는 과정을 설명하는 도면이다.
 도 6은 도 5의 주소의 개인키를 사용하여 계약 계좌에서 지불하는 트랜잭션 생성하는 과정을 단순화하여 나타낸 도면이다.
 도 7은 본 발명의 일 실시예에 따른 블록체인의 개인키 권한 조절 방법과 기존 블록 체인 시스템을 비교한 결과를 나타낸 도면이다.

발명을 실시하기 위한 구체적인 내용

[0022] 아래에서는 첨부한 도면을 참조하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 본 발명의 실시예를 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시예에 한정되지 않는다. 그리고 도면에서 본 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였으며, 명세서 전체를 통하여 유사한 부분에 대해서는 유사한 도면 부호를 붙였다.

[0023] 명세서 전체에서, 어떤 부분이 다른 부분과 "연결"되어 있다고 할 때, 이는 "직접적으로 연결"되어 있는 경우뿐 아니라, 그 중간에 다른 소자를 사이에 두고 "전기적으로 연결"되어 있는 경우도 포함한다. 또한 어떤 부분이

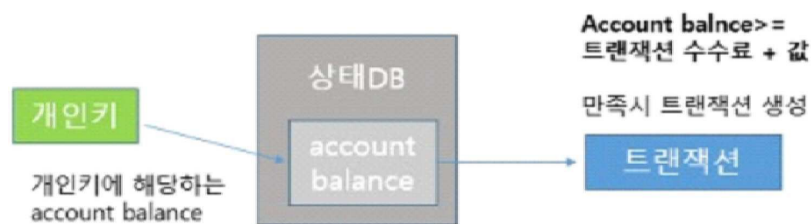
어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있는 것을 의미하며, 하나 또는 그 이상의 다른 특징이나 숫자, 단계, 동작, 구성요소, 부분품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

- [0024] 이하의 실시예는 본 발명의 이해를 돕기 위한 상세한 설명이며, 본 발명의 권리 범위를 제한하는 것이 아니다. 따라서 본 발명과 동일한 기능을 수행하는 동일 범위의 발명 역시 본 발명의 권리 범위에 속할 것이다.
- [0025] 이하 첨부된 도면을 참고하여 본 발명의 일 실시예를 상세히 설명하기로 한다.
- [0026] 도 2는 본 발명의 일 실시예에 따른 블록체인의 개인키 권한 조절 시스템의 구조를 나타낸 도면이다.
- [0027] 도 2를 참조하면, 블록체인의 개인키 권한 조절 시스템은 기존의 이더리움 기반의 블록체인의 상태DB(State DataBase)에 다중 서명 지갑의 주소를 입력할 AccountHash를 추가한다.
- [0028] 개인키로 생성된 account의 경우, AccountHash를 추가하면 다중서명지갑과 같은 스마트 계약의 주소(contract address)를 저장할 수 있다. 만약 accountHash에 스마트 계약의 주소가 저장되어 있다면, 트랜잭션 요청이 해당 account로부터 발생할 때, 해당 다중서명지갑에서 조건하에 금액을 지불하는 것을 시도한다. 만약 해당 AccountHash가 비어있으면 일반적인 결제가 진행된다.
- [0029] 계약주소(Contract address)의 경우, AccountHash는 계약에 따라 사용할 수도 있고, 사용하지 않을 수도 있다. 그러나 본 발명에서 제안하는 블록체인의 개인키 권한 조절 방법에 의하면 해당 계약으로 리스크를 최소화할 account들의 주소들이 포함된다. 만약 accountHash에 포함되는 account로부터 결제요청, 즉 트랜잭션 생성 요청이 전송되면 한도 등의 조건이 맞을 경우에 계약주소에서 트랜잭션 생성비용과 금액을 지불한다.
- [0030] 여기에서 안전하게 보관하는 개인키의 권한이 결제에 사용할 개인키 보다 권한이 큰 것으로 가정한다.
- [0031] 도 3은 본 발명의 일 실시예에 따른 블록체인의 개인키 권한 조절 방법 중 개인키와 스마트 계약을 연결 요청하는 과정을 설명하는 도면이고, 도 4는 본 발명의 일 실시예에 따른 블록체인의 개인키 권한 조절 방법 중 개인키와 스마트 계약을 연결 성공 과정을 설명하는 도면이다.
- [0032] 도 3 및 도 4를 참조하면, 본 발명의 일 실시예에 따른 블록체인의 개인키 권한 조절 방법은 소유자가 주소(계좌)를 다중 서명지갑에 등록, 권한 수정 및 삭제할 수 있다.
- [0033] 즉, 도 3에 도시된 바와 같이, 다중 서명 지갑과 같은 스마트 계약에게 자신의 주소를 등록 요청하고, 안전하게 보관되어 있는 자신의 다른 키로 등록을 승인하면, 해당 주소가 상태 DB의 자신의 주소(Key)의 accountHash값에 스마트 계약의 주소를 저장하고, 상태 DB에서 스마트 계약의 주소(Key)의 accountHash에 account를 추가한다.
- [0034] 등록 요청시 해당 주소의 한도를 설정할 수 있으며, 각각 주소의 한도는 다중 서명 지갑을 블록체인에 배포할 때 설정한 단일 주소의 최대 한도를 초과할 수 없다. 같은 과정으로 한도를 높이는 것과 같은 권한 상승이 일어난다. 언급된 스마트 계약과 관련된 내용들은 고정적인 것이 아니며 스마트 계약으로 프로그래밍하는 것에 따라 다르게 설정할 수 있다.
- [0035] 도 4에 도시된 바와 같이, 자신이 실제로 사용할 개인키를 스마트 계약과 연결을 요청하는데, 안전하게 보관된 개인키로 연결을 승인한다. 연결에 성공하면 account3의 accountHash값은 스마트 계약의 주소를 저장하고, 스마트 계약 주소의 accountHash는 account3를 포함하게 되어 연결 요청이 연결 성공으로 변화한다.
- [0036] 도 5는 본 발명의 일 실시예에 따른 블록체인의 개인키 권한 조절 방법 중 주소의 개인키를 사용하여 계약 계좌에서 지불하는 트랜잭션 생성하는 과정을 설명하는 도면이고, 도 6은 도 5의 주소의 개인키를 사용하여 계약 계좌에서 지불하는 트랜잭션 생성하는 과정을 단순화하여 나타낸 도면이다.
- [0037] 기존 블록체인 시스템에서 트랜잭션을 생성할 때는 생성하는 개인키에 해당하는 개인키의 잔고(balance)가 보내는 금액과 수수료의 합보다 큰 것을 검사한다.
- [0038] 그러나, 도 5에 도시된 바와 같이, 본 발명의 일 실시예에 따른 블록체인의 개인키 권한 조절 방법에서는 트랜잭션을 생성할 때, 상태 DB에서 개인키에 해당하는 주소를 조회한다. 해당 주소의 잔고(balance)를 조회하기 전에 accountHash의 값이 다중 서명 지갑 계약과 같은 스마트 계약을 가리킬 때, 스마트 계약 주소를 확인한다. 스마트 계약 주소의 accountHash에 요청한 계좌 주소가 등록된 것이 확인되고, 스마트 계약의 내부 조건이 충족되면 다중 서명 지갑 계약의 잔고(balance)에서 지불하는 트랜잭션을 생성한다.

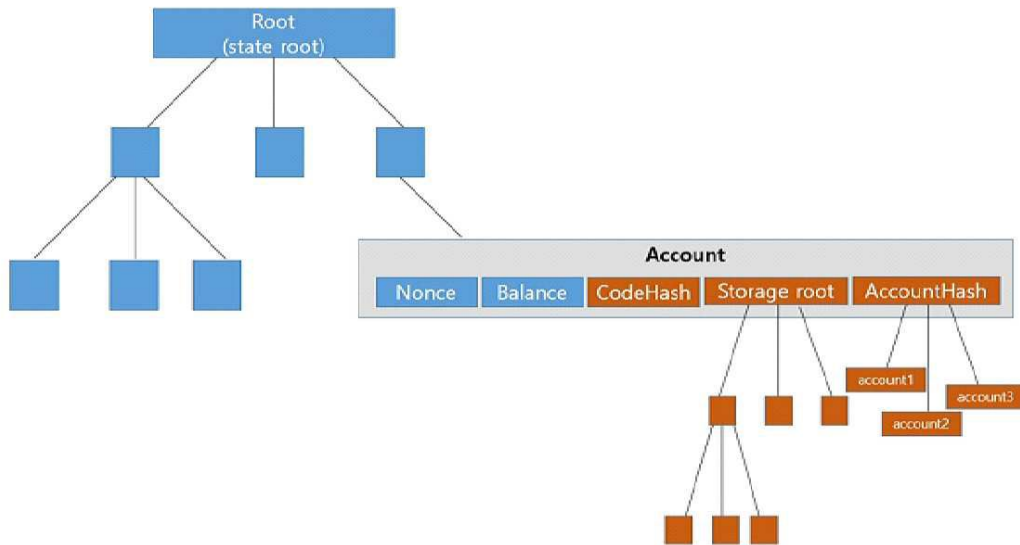
- [0039] 기존의 상태DB의 유효성검사는 보내는금액(msg.value)과 수수료의 합이 계좌잔고보다 같거나 작아야 유효성검사를 통과했지만, 제안한 방법에서는 보내는 금액(msg.value)과 수수료의 합이 트랜잭션잔고보다 같거나 작아야 한다.
- [0040] 도 7은 본 발명의 일 실시예에 따른 블록체인의 개인키 권한 조절 방법과 기존 블록 체인 시스템을 비교한 결과를 나타낸 도면이다.
- [0041] 도 7을 참조하면, 본 발명의 일 실시예에 따른 블록체인의 개인키 권한 조절 방법은 일반 개인키 결제보다 사용자입장에서 과정의 추가 없이 권한을 조절할 수 있고, 작성한 스마트 컨트랙트의 조건에 따라 결제할 수 있게 된다. 또한 본 발명은 스마트 컨트랙트 결제보다 결제의 과정이 단순화되어 개인키 결제와 같은 과정으로 결제가 진행될 수 있다.
- [0042] 이와 같이, 본 발명은 개인키의 권한을 다중서명지갑과 같은 스마트 계약으로 조절할 수 있고, 스마트 계약으로 이루어지는 상대적으로 복잡한 결제 프로세스를 일반적인 개인키 결제와 같이 단순하게 이루어질 수 있게 함으로써 보편적이고 안전한 결제 시스템 구축이 가능해진다.
- [0043] 또한, 본 발명은 개인키의 권한이 스마트 계약으로 조절되는데, 스마트 계약은 프로그래밍 언어로 자유롭게 작성가능하기 때문에 개인키 권한과 관련된 다양한 문제 해결에 사용될 수 있다. 따라서, 본 발명의 일 실시예에 따른 블록체인의 개인키 권한 조절 방법을 기존의 블록 체인 시스템에 적용하면, 사용자 입장에서 일반 개인키가 컨트랙트 생성하거나 함수 호출하는 것과 같은 과정이 요구되므로 접근성이 향상되고, 블록체인 시스템 내부적으로 개인키를 보호할 수 있다.
- [0044] 이상에서 설명한 본 발명의 실시예에 따른 블록체인의 개인키 권한 조절 방법은, 컴퓨터에 의해 실행되는 프로그램 모듈과 같은 컴퓨터에 의해 실행 가능한 명령어를 포함하는 기록 매체의 형태로도 구현될 수 있다. 이러한 기록 매체는 컴퓨터 판독 가능 매체를 포함하며, 컴퓨터 판독 가능 매체는 컴퓨터에 의해 액세스될 수 있는 임의의 가용 매체일 수 있고, 휘발성 및 비휘발성 매체, 분리형 및 비분리형 매체를 모두 포함한다. 또한, 컴퓨터 판독가능 매체는 컴퓨터 저장 매체를 포함하며, 컴퓨터 저장 매체는 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈 또는 기타 데이터와 같은 정보의 저장을 위한 임의의 방법 또는 기술로 구현된 휘발성 및 비휘발성, 분리형 및 비분리형 매체를 모두 포함한다.
- [0045] 전술한 본 발명의 설명은 예시를 위한 것이며, 본 발명이 속하는 기술분야의 통상의 지식을 가진 자는 본 발명의 기술적 사상이나 필수적인 특징을 변경하지 않고서 다른 구체적인 형태로 쉽게 변형이 가능하다는 것을 이해할 수 있을 것이다. 그러므로 이상에서 기술한 실시예들은 모든 면에서 예시적인 것이며 한정적이 아닌 것으로 이해해야만 한다. 예를 들어, 단일형으로 설명되어 있는 각 구성 요소는 분산되어 실시될 수도 있으며, 마찬가지로 분산된 것으로 설명되어 있는 구성 요소들도 결합된 형태로 실시될 수 있다.
- [0046] 본 발명의 범위는 상기 상세한 설명보다는 후술하는 특허청구범위에 의하여 나타내어지며, 특허청구범위의 의미 및 범위 그리고 그 균등 개념으로부터 도출되는 모든 변경 또는 변형된 형태가 본 발명의 범위에 포함되는 것으로 해석되어야 한다.

도면

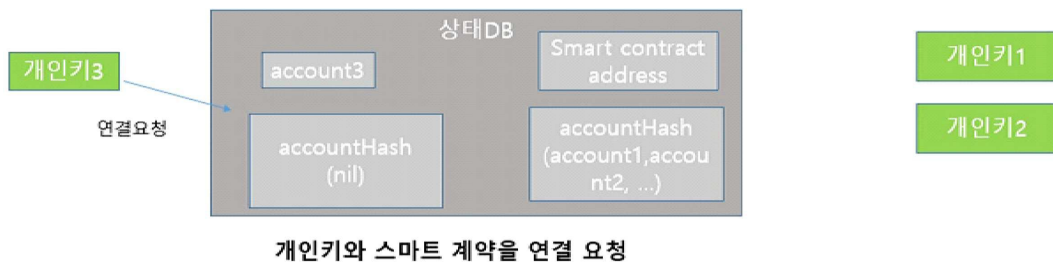
도면1



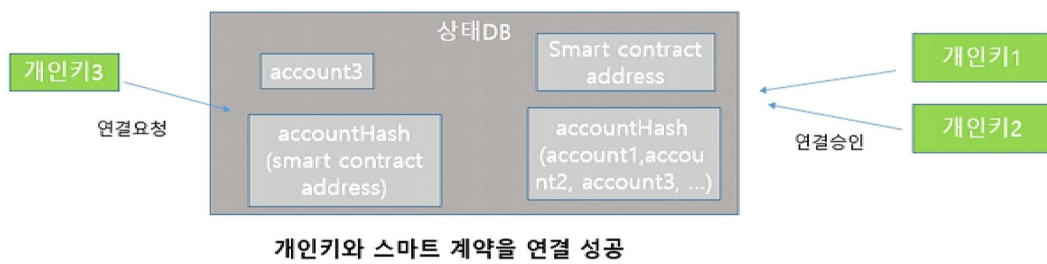
도면2



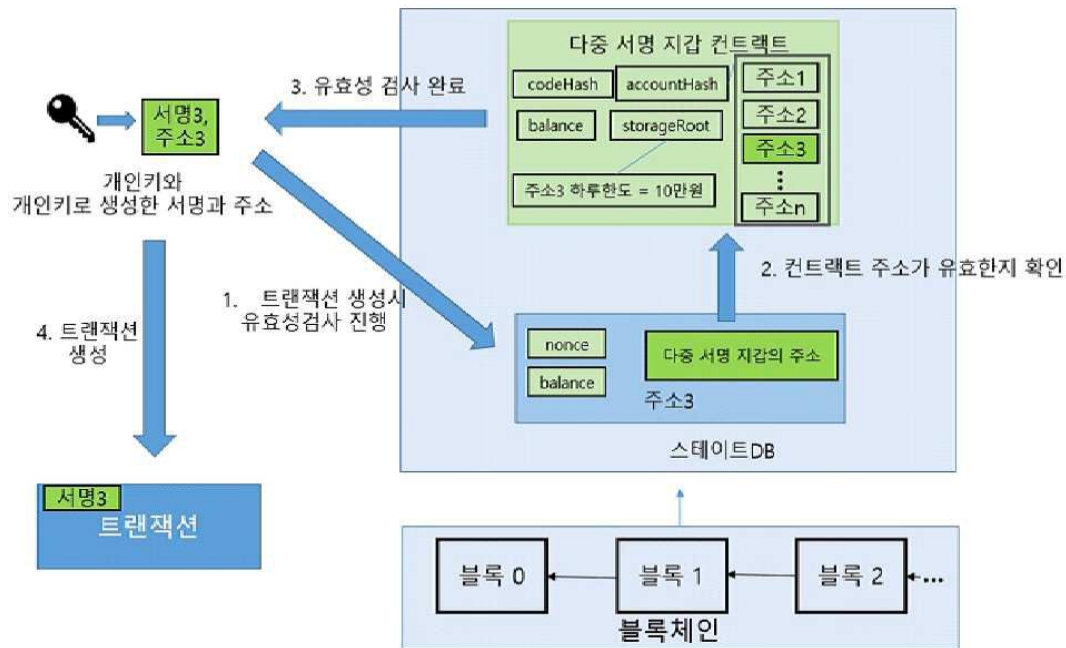
도면3



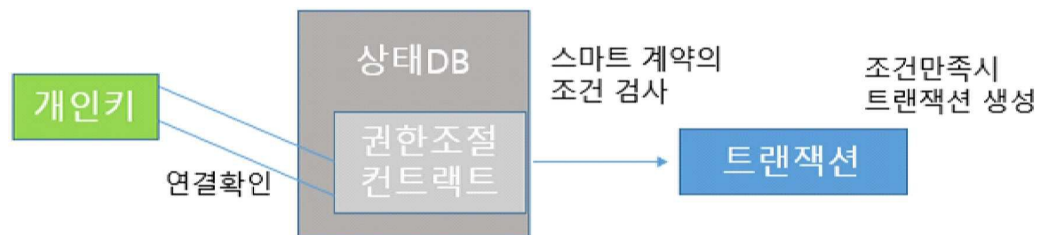
도면4



도면5



도면6



새로운 프로세스의 트랜잭션 생성과정

도면7

기존시스템	->제안하는 발명의 개선점
개인키결제	권한조절가능
스마트컨트랙트결제	개인키결제처럼 간편화됨