



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2021-0125803
(43) 공개일자 2021년10월19일

(51) 국제특허분류(Int. Cl.)

G06F 21/45 (2013.01) G06F 21/33 (2013.01)
G06Q 10/10 (2012.01) G06Q 30/06 (2012.01)
H04L 9/06 (2006.01)

(52) CPC특허분류

G06F 21/45 (2013.01)
G06F 21/33 (2013.01)

(21) 출원번호 10-2020-0043465

(22) 출원일자 2020년04월09일

심사청구일자 2020년04월09일

(71) 출원인

건양대학교산학협력단

충청남도 논산시 대학로 121 (내동)

(72) 발명자

정승욱

대전광역시 서구 청사로 281 샘머리아파트2단지,
218동 204호

(74) 대리인

강정빈, 심찬, 송두현

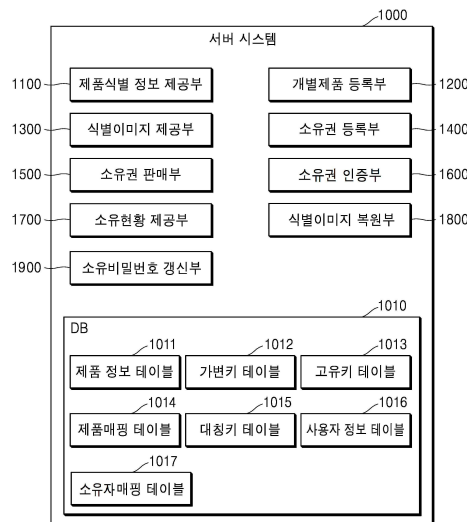
전체 청구항 수 : 총 5 항

(54) 발명의 명칭 **제품의 소유권을 인증하기 위한 방법**

(57) 요약

본 발명은 제품의 소유권을 인증하기 위한 방법에 관한 것으로서, 더욱 상세하게는 블록체인 네트워크의 분산원장에 기록되어 있는 구매한 제품에 대한 원장기록정보에 기초하여 해당 제품의 구매를 인증하고, 제품에 대한 소유비밀번호 및 식별이미지를 복구하는, 제품의 소유권을 인증하기 위한 방법에 관한 것이다.

대표도 - 도2



(52) CPC특허분류

G06Q 10/10 (2021.08)

G06Q 30/0607 (2013.01)

H04L 9/06 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호	1345317979
과제번호	NRF-2017R1D1A3B03036404
부처명	교육부
과제관리(전문)기관명	한국연구재단
연구사업명	지역대학우수과학자 지원사업
연구과제명	밀성이 향상된 블록체인 플랫폼 연구 및 개발
기 여 율	1/1
과제수행기관명	건양대학교
연구기간	2017.06.01 ~ 2020.05.31

명세서

청구범위

청구항 1

1 이상의 사용자단말 및 블록체인 네트워크와 통신을 수행하는 1 이상의 프로세서 및 1 이상의 메모리를 포함하는 서버시스템에서 수행되는 제품의 소유권을 인증하기 위한 방법으로서,

사용자단말에서 개별제품에 대한 식별이미지를 인식하여 도출한 암호화된 시리얼정보 및 소유비밀번호를 포함하는 소유권인증요청정보를 상기 사용자단말로부터 수신하는 단계;

상기 블록체인 네트워크에 포함된 스마트 컨트랙트로 하여금 상기 소유권인증요청정보에 포함된 암호화된 시리얼정보와 동일한 값을 포함하는 원장기록정보를 도출하도록 하고, 해당 원장기록정보에 포함된 개별제품식별정보를 송신하도록 요청하는 단계;

상기 소유권인증요청정보에 포함된 소유비밀번호에 기초하여 인증소유키를 도출하고, 상기 스마트 컨트랙트로부터 수신한 개별제품식별정보에 매칭되는 인증가변키를 로드하여, 상기 인증소유키 및 상기 인증가변키에 기초하여 인증고유키를 생성하는 단계;

상기 스마트 컨트랙트로 하여금 상기 암호화된 시리얼정보를 상기 인증고유키로 복호화하도록 하고, 상기 암호화된 시리얼정보와 동일한 값을 포함하는 원장기록정보를 도출하도록 하고, 해당 원장기록정보에 포함된 시리얼정보 및 상기 복호화된 시리얼정보의 일치 여부를 판별하도록 하여, 일치하는 경우에 인증성공정보를 송신하도록 요청하는 단계; 및

상기 인증성공정보를 수신하는 경우, 상기 개별제품식별정보에 기초하여 인증세부정보를 도출하고, 상기 인증세부정보를 해당 사용자단말에 제공하는 인증세부정보제공단계;를 포함하는, 제품의 소유권을 인증하기 위한 방법.

청구항 2

청구항 1에 있어서,

상기 제품의 소유권을 인증하기 위한 방법은 소유현황제공단계를 더 포함하고,

상기 소유현황제공단계는,

사용자단말로부터 소유현황제공요청정보를 수신하는 단계;

상기 스마트 컨트랙트로 하여금 해당 사용자단말에 상응하는 사용자식별정보 혹은 암호화된 시리얼정보를 포함하는 1 이상의 원장기록정보를 도출하도록 하고, 상기 1 이상의 원장기록정보에 각각 포함된 1 이상의 개별제품식별정보를 송신하도록 요청하는 단계; 및

상기 1 이상의 개별제품식별정보에 매칭되는 각각의 제품정보를 포함하는 소유현황정보를 도출하여 해당 사용자단말에 제공하는 단계;를 포함하는, 제품의 소유권을 인증하기 위한 방법.

청구항 3

청구항 1에 있어서,

상기 제품의 소유권을 인증하기 위한 방법은 식별이미지복원단계를 더 포함하고,

상기 식별이미지복원단계는,

사용자단말로부터 복원하고자 하는 식별이미지에 상응하는 개별제품식별정보 및 소유비밀번호를 포함하는 식별이미지복원요청정보를 수신하는 단계;

상기 식별이미지복원요청정보에 포함된 소유비밀번호에 기초하여 복원소유키를 도출하고, 상기 식별이미지복원요청정보에 포함된 개별제품식별정보에 매칭되는 복원가변키를 로드하여, 상기 복원소유키 및 상기 복원가변키에 기초하여 복원고유키를 도출하는 단계;

상기 스마트 컨트랙트로 하여금 상기 식별이미지복원요청정보에 포함된 개별제품식별정보와 동일한 값을 포함하는 원장기록정보를 도출하도록 하고, 해당 원장기록정보에 포함된 암호화된 시리얼정보를 상기 복원고유키로 복호화하고, 상기 복호화된 시리얼정보 및 해당 원장기록정보에 포함된 시리얼정보의 일치 여부를 판별하도록 하여, 일치하는 경우에 상기 암호화된 시리얼정보를 송신하도록 요청하는 단계; 및

수신한 상기 암호화된 시리얼정보에 기초하여 식별이미지를 생성하고, 생성된 식별이미지를 해당 사용자단말로 송신하는 단계;를 포함하는, 제품의 소유권을 인증하기 위한 방법.

청구항 4

청구항 1에 있어서,

상기 제품의 소유권을 인증하기 위한 방법은 소유비밀번호갱신단계를 더 포함하고,

상기 소유비밀번호갱신단계는,

사용자단말에서 갱신하고자 하는 소유비밀번호에 상응하는 식별이미지를 인식하여 도출한 암호화된 시리얼정보 및 신규 소유비밀번호를 포함하는 소유비밀번호갱신요청정보를 상기 사용자단말로부터 수신하는 단계;

상기 스마트 컨트랙트로 하여금 상기 소유비밀번호갱신요청정보에 포함된 암호화된 시리얼정보와 동일한 값을 포함하는 원장기록정보를 도출하도록 하고, 해당 사용자단말에 상응하는 사용자식별정보 및 해당 원장기록정보에 포함된 사용자식별정보의 일치 여부를 판별하도록 하여, 일치하는 경우에 해당 원장기록정보에 포함된 개별제품식별정보를 송신하도록 요청하는 단계; 및

상기 소유비밀번호갱신요청정보에 포함된 신규 소유비밀번호에 기초하여 신규 소유키를 도출하고, 상기 개별제품식별정보에 매칭되는 갱신고유키를 로드하여, 상기 신규 소유키 및 상기 갱신고유키에 기초하여 신규 가변키를 도출하고, 상기 신규 가변키를 상기 개별제품식별정보에 매칭하여 저장하는 단계;를 포함하는, 제품의 소유권을 인증하기 위한 방법.

청구항 5

청구항 1에 있어서,

상기 서버시스템은,

제품식별정보에 매칭된 상기 제품정보를 포함하는 제품정보테이블; 및 상기 개별제품식별정보에 매칭된 상기 제품식별정보를 포함하는 제품매핑테이블;을 포함하고,

상기 인증세부정보제공단계는,

상기 제품매핑테이블에서 상기 개별제품식별정보에 매칭된 제품식별정보를 도출하고, 상기 제품정보테이블에서 도출된 제품식별정보에 매칭된 제품정보를 도출하는 단계;를 포함하는, 제품의 소유권을 인증하기 위한 방법.

발명의 설명

기술 분야

[0001]

본 발명은 제품의 소유권을 인증하기 위한 방법에 관한 것으로서, 더욱 상세하게는 블록체인 네트워크의 분산원장에 기록되어 있는 구매한 제품에 대한 원장기록정보에 기초하여 해당 제품의 구매를 인증하고, 제품에 대한 소유비밀번호 및 식별이미지를 복구하는, 제품의 소유권을 인증하기 위한 방법에 관한 것이다.

배경 기술

- [0003] 미술품과 같은 예술작품이나 높은 인지도를 갖는 브랜드에서 생산하는 제품, 즉 명품의 경우 최초 구매 이후에도 높은 가치를 형성하기 때문에 2차 거래(중고 거래)가 활발하게 이루어지고 있는 제품에 해당한다. 따라서 예술작품이나 명품과 같이 제품에 대한 소유권을 명확하게 하기 위한 방법들이 제시되고 있다.
- [0004] 전통적으로 소유권을 인증하기 위한 방법으로는 거래계약서나, 제품을 구매할 때 지급받는 품질보증서 또는 정품인증서를 사용하여 해당 제품에 대한 소유권을 확인하는 방법이 존재하고, 통상적으로 품질보증서 또는 정품인증서를 제품과 함께 거래하는 방법을 통해 제품에 대한 소유권을 거래하고 있다.
- [0005] 그러나 상기와 같은 전통적인 방법에서 거래계약서, 품질보증서 또는 정품인증서는 위조 및 변조가 비교적 용이하기 때문에 거래계약서, 품질보증서 또는 정품인증서 등과 같이 소유권을 의미하는 문서 자체에 대한 신뢰성이 높지 않은 문제점이 존재한다. 추가적으로, 진품을 모조품으로 대체하여 정상 품질보증서와 함께 중고 판매하는 경우에 해당 모조품을 구매하는 중고 구매자는 무방비로 해당 모조품을 구매하게 되는 문제점이 발생한다.
- [0006] 또한, 상기와 같은 방법의 경우 소유권을 인증하는 매체가 종이 혹은 카드와 같은 실물 형태로 존재하기 때문에 이를 분실하거나 훼손하는 경우에 해당 제품에 대해 A/S와 같은 보증을 받는데 문제가 발생하고, 해당 제품을 중고거래 하는데 있어서도 상대적으로 낮은 가격으로 책정되는 등의 제약이 발생하는 문제점이 발생하게 된다.
- [0007] 한편, 최근에는 이러한 문제를 해결하기 위하여 제품에 대한 정품인증코드에 상응하는 식별표지를 이용하여 정품을 인증하거나, 구매이력을 확인하는 방법이 개발되었으나, 식별표지가 분실되거나, 훼손되는 경우 정상적으로 인증을 수행하기 어려운 문제점이 여전히 존재한다.
- [0008] 따라서, 구매한 제품에 대한 제품 소유권의 인증을 수행함과 동시에 해당 제품과 관련된 인증과 관련된 요소들을 복구할 수 있는 방법의 개발이 필요한 상황이다.

발명의 내용

해결하려는 과제

- [0010] 본 발명은 제품의 소유권을 인증하기 위한 방법에 관한 것으로서, 더욱 상세하게는 블록체인 네트워크의 분산원장에 기록되어 있는 구매한 제품에 대한 원장기록정보에 기초하여 해당 제품의 구매를 인증하고, 제품에 대한 소유비밀번호 및 식별이미지를 복구하는, 제품의 소유권을 인증하기 위한 방법을 제공하는 것을 목적으로 한다.

과제의 해결 수단

- [0012] 상기와 같은 과제를 해결하기 위하여 본 발명은, 1 이상의 사용자단말 및 블록체인 네트워크와 통신을 수행하는 1 이상의 프로세서 및 1 이상의 메모리를 포함하는 서버시스템에서 수행되는 제품의 소유권을 인증하기 위한 방법으로서, 사용자단말에서 개별제품에 대한 식별이미지를 인식하여 도출한 암호화된 시리얼정보 및 소유비밀번호를 포함하는 소유권인증요청정보를 상기 사용자단말로부터 수신하는 단계; 상기 블록체인 네트워크에 포함된 스마트 컨트랙트로 하여금 상기 소유권인증요청정보에 포함된 암호화된 시리얼정보와 동일한 값을 포함하는 원장기록정보를 도출하도록 하고, 해당 원장기록정보에 포함된 개별제품식별정보를 송신하도록 요청하는 단계; 상기 소유권인증요청정보에 포함된 소유비밀번호에 기초하여 인증소유키를 도출하고, 상기 스마트 컨트랙트로부터 수신한 개별제품식별정보에 매칭되는 인증가변키를 로드하여, 상기 인증소유키 및 상기 인증가변키에 기초하여 인증고유키를 생성하는 단계; 상기 스마트 컨트랙트로 하여금 상기 암호화된 시리얼정보를 상기 인증고유키로 복호화하도록 하고, 상기 암호화된 시리얼정보와 동일한 값을 포함하는 원장기록정보를 도출하도록 하고, 해당 원장기록정보에 포함된 시리얼정보 및 상기 복호화된 시리얼정보의 일치 여부를 판별하도록 하여, 일치하는 경우에 인증성공정보를 송신하도록 요청하는 단계; 및 상기 인증성공정보를 수신하는 경우, 상기 개별제품식별정보에 기초하여 인증세부정보를 도출하고, 상기 인증세부정보를 해당 사용자단말에 제공하는 인증세부정보제공단계;를 포함하는, 제품의 소유권을 인증하기 위한 방법을 제공한다.
- [0013] 본 발명의 일 실시예에서는, 상기 제품의 소유권을 인증하기 위한 방법은 소유현황제공단계를 더 포함하고, 상기 소유현황제공단계는, 사용자단말로부터 소유현황제공요청정보를 수신하는 단계; 상기 스마트 컨트랙트로 하

여금 해당 사용자단말에 상응하는 사용자식별정보 혹은 암호화된 시리얼정보를 포함하는 1 이상의 원장기록정보를 도출하도록 하고, 상기 1 이상의 원장기록정보에 각각 포함된 1 이상의 개별제품식별정보를 송신하도록 요청하는 단계; 및 상기 1 이상의 개별제품식별정보에 매칭되는 각각의 제품정보를 포함하는 소유현황정보를 도출하여 해당 사용자단말에 제공하는 단계;를 포함할 수 있다.

[0014] 상기 제품의 소유권을 인증하기 위한 방법은 소유현황제공단계를 더 포함하고, 상기 소유현황제공단계는, 사용자단말로부터 소유현황제공요청정보를 수신하는 단계; 상기 스마트 컨트랙트로 하여금 해당 사용자단말에 상응하는 사용자식별정보를 포함하는 1 이상의 원장기록정보를 도출하도록 하고, 상기 1 이상의 원장기록정보에 각각 포함된 1 이상의 개별제품식별정보를 송신하도록 요청하는 단계; 및 상기 1 이상의 개별제품식별정보에 매칭되는 각각의 제품정보를 포함하는 소유현황정보를 도출하여 해당 사용자단말에 제공하는 단계;를 포함할 수 있다.

[0015] 본 발명의 일 실시예에서는, 상기 제품의 소유권을 인증하기 위한 방법은 식별이미지복원단계를 더 포함하고, 상기 식별이미지복원단계는, 사용자단말로부터 복원하고자 하는 식별이미지에 상응하는 개별제품식별정보 및 소유비밀번호를 포함하는 식별이미지복원요청정보를 수신하는 단계; 상기 식별이미지복원요청정보에 포함된 소유비밀번호에 기초하여 복원소유키를 도출하고, 상기 식별이미지복원요청정보에 포함된 개별제품식별정보에 매칭되는 복원가변키를 로드하여, 상기 복원소유키 및 상기 복원가변키에 기초하여 복원고유키를 도출하는 단계; 상기 스마트 컨트랙트로 하여금 상기 식별이미지복원요청정보에 포함된 개별제품식별정보와 동일한 값을 포함하는 원장기록정보를 도출하도록 하고, 해당 원장기록정보에 포함된 암호화된 시리얼정보를 상기 복원고유키로 복호화하고, 상기 복호화된 시리얼정보 및 해당 원장기록정보에 포함된 시리얼정보의 일치 여부를 판별하도록 하여, 일치하는 경우에 상기 암호화된 시리얼정보를 송신하도록 요청하는 단계; 및 수신한 상기 암호화된 시리얼정보에 기초하여 식별이미지를 생성하고, 생성된 식별이미지를 해당 사용자단말로 송신하는 단계;를 포함할 수 있다.

[0016] 본 발명의 일 실시예에서는, 상기 제품의 소유권을 인증하기 위한 방법은 소유비밀번호갱신단계를 더 포함하고, 상기 소유비밀번호갱신단계는, 사용자단말에서 갱신하고자 하는 소유비밀번호에 상응하는 식별이미지를 인식하여 도출한 암호화된 시리얼정보 및 신규 소유비밀번호를 포함하는 소유비밀번호갱신요청정보를 상기 사용자단말로부터 수신하는 단계; 상기 스마트 컨트랙트로 하여금 상기 소유비밀번호갱신요청정보에 포함된 암호화된 시리얼정보와 동일한 값을 포함하는 원장기록정보를 도출하도록 하고, 해당 사용자단말에 상응하는 사용자식별정보 및 해당 원장기록정보에 포함된 사용자식별정보의 일치 여부를 판별하도록 하여, 일치하는 경우에 해당 원장기록정보에 포함된 개별제품식별정보를 송신하도록 요청하는 단계; 및 상기 소유비밀번호갱신요청정보에 포함된 신규 소유비밀번호에 기초하여 신규 소유키를 도출하고, 상기 개별제품식별정보에 매칭되는 갱신고유키를 로드하여, 상기 신규 소유키 및 상기 갱신고유키에 기초하여 신규 가변키를 도출하고, 상기 신규 가변키를 상기 개별제품식별정보에 매칭하여 저장하는 단계;를 포함할 수 있다.

[0017] 본 발명의 일 실시예에서는, 상기 서버시스템은, 제품식별정보에 매칭된 상기 제품정보를 포함하는 제품정보테이블; 및 상기 개별제품식별정보에 매칭된 상기 제품식별정보를 포함하는 제품매핑테이블;을 포함하고, 상기 인증세부정보제공단계는, 상기 제품매핑테이블에서 상기 개별제품식별정보에 매칭된 제품식별정보를 도출하고, 상기 제품정보테이블에서 도출된 제품식별정보에 매칭된 제품정보를 도출하는 단계;를 포함할 수 있다.

발명의 효과

[0019] 본 발명의 일 실시예에 따르면, 제품 생산자의 사용자단말로부터 개별제품등록요청정보를 수신하여 블록체인 네트워크의 분산원장에 원장기록정보를 기록하므로, 해당 제품의 진품을 확인할 수 있는 효과를 발휘할 수 있다.

[0020] 본 발명의 일 실시예에 따르면, 해당 제품을 구매하는 경우 구매자의 사용자식별정보가 블록체인 네트워크 상의 원장기록정보에 추가되어 기록되므로, 해당 구매자가 자신의 소유권을 확인 또는 증명할 수 있고, 이에 따라 해당 제품을 소유한 구매자의 제품에 대한 충성도를 향상시킬 수 있는 효과를 발휘할 수 있다.

[0021] 본 발명의 일 실시예에 따르면, 해당 제품을 구매하는 경우 구매자의 사용자식별정보가 블록체인 네트워크 상의 원장기록정보에 추가되어 기록되므로, 해당 제품을 중고거래 하는 경우에도 소유권을 용이하게 이전할 수 있고, 따라서 중고 구매자의 해당 제품에 대한 신뢰도를 향상시킬 수 있는 효과를 발휘할 수 있다.

[0022] 본 발명의 일 실시예에 따르면, 구매자 소유비밀번호는 서버시스템에 저장되지 않으므로, 상기 서버시스템을 통

해 소유권을 구매함에 있어서 보안을 향상시킬 수 있는 효과를 발휘할 수 있다.

- [0023] 본 발명의 일 실시예에 따르면, 서버시스템은 제품에 대한 식별이미지를 도출하여 사용자단말에 제공하므로, 해당 식별이미지가 복수의 장소에서 사용되거나, 해당 식별이미지에 대하여 복수의 오류가 발생하는 경우에 해당 제품에 대한 복제품 존재 여부를 판단할 수 있는 효과를 발휘할 수 있다.
- [0024] 본 발명의 일 실시예에 따르면, 진품을 가품으로 바꾸어 판매하는 경우에 진품을 본 발명의 방법으로는 더 이상 판매할 수 없으므로, 바꾸어 판매하고자 하는 욕구를 감소시킬 수 있는 효과를 발휘할 수 있다.
- [0025] 본 발명의 일 실시예에 따르면, 가변키 및 고유키는 대칭키테이블에 저장된 각각의 대칭키에 의해 암호화되어 각각 가변키테이블 및 고유키테이블에 저장되므로, 상기 가변키 및 상기 고유키에 대한 보안을 강화할 수 있는 효과를 발휘할 수 있다.
- [0026] 본 발명의 일 실시예에 따르면, 소유권등록단계에서는 원장기록정보에 사용자식별정보가 포함되지 않은 경우에만 소유권등록을 수행하도록 하므로, 타 판매자의 사용자단말로부터 해당 상품에 대한 중복 등록을 방지할 수 있는 효과를 발휘할 수 있다.
- [0027] 본 발명의 일 실시예에 따르면, 제품에 대한 식별이미지가 분실 혹은 훼손되는 경우, 해당 제품에 대한 소유권을 갖고 있는 사용자의 요청에 따라 식별이미지를 복원하여 해당 사용자에게 제공하므로, 식별이미지가 분실 혹은 훼손되더라도 제품의 소유권에 대한 인증 혹은 판매를 용이하게 수행할 수 있는 효과를 발휘할 수 있다.
- [0028] 본 발명의 일 실시예에 따르면, 제품의 소유권을 갖고 있는 사용자가 소유비밀번호를 분실한 경우, 해당 사용자의 요청에 따라 새로 설정한 소유비밀번호를 제품의 소유비밀번호로 설정할 수 있으므로, 소유비밀번호를 분실하더라도 용이하게 제품의 소유권을 인증하거나 판매할 수 있는 효과를 발휘할 수 있다.

도면의 간단한 설명

- [0030] 도 1은 본 발명의 일 실시예에 따른 제품의 소유권을 거래하기 위한 방법을 수행하기 위한 시스템의 구성을 개략적으로 도시한다.
- 도 2는 본 발명의 일 실시예에 따른 서버시스템의 내부 구성을 개략적으로 도시한다.
- 도 3은 본 발명의 일 실시예에 따른 서버시스템에 포함되는 각각의 테이블을 구성하는 필드들을 개략적으로 도시한다.
- 도 4는 본 발명의 일 실시예에 따른 소유권을 거래하기 위한 과정을 개략적으로 도시한다.
- 도 5는 본 발명의 일 실시예에 따른 개별제품등록단계에 포함되는 세부 단계들을 개략적으로 도시한다.
- 도 6은 본 발명의 일 실시예에 따른 소유권등록단계에 포함되는 세부 단계들을 개략적으로 도시한다.
- 도 7은 본 발명의 일 실시예에 따른 소유권판매단계에 포함되는 세부 단계들을 개략적으로 도시한다.
- 도 8은 본 발명의 일 실시예에 따른 블록체인 네트워크에서 저장되는 블록들의 연결 구조를 개략적으로 도시한다.
- 도 9는 본 발명의 일 실시예에 따른 사용자단말에 디스플레이되는 화면들을 개략적으로 도시한다.
- 도 10은 본 발명의 일 실시예에 따른 소유권판매부의 동작에 따른 사용자단말에 디스플레이되는 화면들을 개략적으로 도시한다.
- 도 11은 본 발명의 일 실시예에 따른 소유권인증단계에 포함되는 세부 단계들을 개략적으로 도시한다.
- 도 12는 본 발명의 일 실시예에 따른 소유현황제공단계에 포함되는 세부 단계들을 개략적으로 도시한다.
- 도 13은 본 발명의 일 실시예에 따른 식별이미지복원단계에 포함되는 세부 단계들을 개략적으로 도시한다.
- 도 14는 본 발명의 일 실시예에 따른 소유비밀번호갱신단계에 포함되는 세부 단계들을 개략적으로 도시한다.
- 도 15는 본 발명의 일 실시예에 따른 소유권인증부의 동작에 따른 사용자단말에 디스플레이되는 화면들을 개략적으로 도시한다.

도 16은 본 발명의 일 실시예에 따른 소유현황제공부 및 소유비밀번호갱신부의 동작에 따른 사용자단말에 디스플레이되는 화면들을 개략적으로 도시한다.

발명을 실시하기 위한 구체적인 내용

- [0031] 이하에서는, 다양한 실시예들 및/또는 양상들이 이제 도면들을 참조하여 개시된다. 하기 설명에서는 설명을 목적으로, 하나이상의 양상들의 전반적 이해를 돕기 위해 다수의 구체적인 세부사항들이 개시된다. 그러나, 이러한 양상(들)은 이러한 구체적인 세부사항들 없이도 실행될 수 있다는 점 또한 본 발명의 기술 분야에서 통상의 지식을 가진 자에게 인식될 수 있을 것이다. 이후의 기재 및 첨부된 도면들은 하나 이상의 양상들의 특정한 예시적인 양상들을 상세하게 기술한다. 하지만, 이러한 양상들은 예시적인 것이고 다양한 양상들의 원리들에서의 다양한 방법들 중 일부가 이용될 수 있으며, 기술되는 설명들은 그러한 양상들 및 그들의 균등물들을 모두 포함하고자 하는 의도이다.
- [0033] 또한, 다양한 양상들 및 특징들이 다수의 디바이스들, 컴포넌트들 및/또는 모듈들 등을 포함할 수 있는 시스템에 의하여 제시될 것이다. 다양한 시스템들이, 추가적인 장치들, 컴포넌트들 및/또는 모듈들 등을 포함할 수 있다는 점 그리고/또는 도면들과 관련하여 논의된 장치들, 컴포넌트들, 모듈들 등 전부를 포함하지 않을 수도 있다는 점 또한 이해되고 인식되어야 한다.
- [0034] 본 명세서에서 사용되는 "실시예", "예", "양상", "예시" 등은 기술되는 임의의 양상 또는 설계가 다른 양상 또는 설계들보다 양호하다거나, 이점이 있는 것으로 해석되지 않을 수도 있다. 아래에서 사용되는 용어들 '부', '컴포넌트', '모듈', '시스템', '인터페이스' 등은 일반적으로 컴퓨터 관련 엔티티(computer-related entity)를 의미하며, 예를 들어, 하드웨어, 하드웨어와 소프트웨어의 조합, 소프트웨어를 의미할 수 있다.
- [0035] 또한, "포함한다" 및/또는 "포함하는"이라는 용어는, 해당 특징 및/또는 구성요소가 존재함을 의미하지만, 하나 이상의 다른 특징, 구성요소 및/또는 이들의 그룹의 존재 또는 추가를 배제하지 않는 것으로 이해되어야 한다.
- [0036] 또한, 제1, 제2 등과 같이 서수를 포함하는 용어는 다양한 구성요소들을 설명하는데 사용될 수 있지만, 상기 구성요소들은 상기 용어들에 의해 한정되지는 않는다. 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.
- [0037] 본 명세서에 있어서 '부(部)'란, 하드웨어에 의해 실현되는 유닛(unit), 소프트웨어에 의해 실현되는 유닛, 양방을 이용하여 실현되는 유닛을 포함한다. 또한, 1 개의 유닛이 2 개 이상의 하드웨어를 이용하여 실현되어도 되고, 2 개 이상의 유닛이 1 개의 하드웨어에 의해 실현되어도 된다. 한편, '~부'는 소프트웨어 또는 하드웨어에 한정되는 의미는 아니며, '~부'는 어드레싱 할 수 있는 저장 매체에 있도록 구성될 수도 있고 하나 또는 그 이상의 프로세서들을 재생시키도록 구성될 수도 있다. 따라서, 일 예로서 '~부'는 소프트웨어 구성요소들, 객체지향 소프트웨어 구성요소들, 클래스 구성요소들 및 태스크 구성요소들과 같은 구성요소들과, 프로세스들, 함수들, 속성들, 프로시저들, 서브루틴들, 프로그램 코드의 세그먼트들, 드라이버들, 펌웨어, 마이크로코드, 회로, 데이터, 데이터베이스, 데이터 구조들, 테이블들, 어레이들 및 변수들을 포함한다. 구성요소들과 '~부'들 안에서 제공되는 기능은 더 작은 수의 구성요소들 및 '~부'들로 결합되거나 추가적인 구성요소들과 '~부'들로 더 분리될 수 있다. 뿐만 아니라, 구성요소들 및 '~부'들은 디바이스 또는 보안 멀티미디어카드 내의 하나 또는 그 이상의 CPU들을 재생시키도록 구현될 수도 있다.
- [0038] 이하에서 언급되는 '제품 생산자의 사용자단말', '판매자의 사용자단말' 및 '구매자의 사용자단말'을 포함하는 사용자단말은 네트워크를 통해 서버나 타 단말에 접속할 수 있는 컴퓨터나 휴대용 단말로 구현될 수 있다. 여기서, 컴퓨터는 예를 들어, 웹 브라우저(WEB Browser)가 탑재된 노트북, 데스크톱(desktop), 랩톱(laptop) 등을 포함하고, 휴대용 단말은 예를 들어, 휴대성과 이동성이 보장되는 무선 통신장치로서, PCS(Personal Communication System), GSM(Global System for Mobile communications), PDC(Personal Digital Cellular), PHS(Personal Handyphone System), PDA(Personal Digital Assistant), IMT(International Mobile Telecommunication)-2000, CDMA(Code Division Multiple Access)-2000, W-CDMA(W-Code Division Multiple Access), Wibro(Wireless Broadband Internet) 단말 등과 같은 모든 종류의 핸드헬드(Handheld) 기반의 무선 통신 장치를 포함할 수 있다. 또한, "네트워크"는 근거리 통신망(Local Area Network; LAN), 광역 통신망(Wide Area Network; WAN) 또는 부가가치 통신망(Value Added Network; VAN) 등과 같은 유선네트워크나 이동 통신망

(Mobile radio communication network) 또는 위성 통신망 등과 같은 모든 종류의 무선 네트워크로 구현될 수 있다.

[0039] 또한, 본 발명의 실시예들에서, 별도로 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 가지는 것으로 해석되어야 하며, 본 발명의 실시예에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[0041] 1. 제품의 소유권을 거래하기 위한 방법

[0042] 제품의 소유권을 인증하기 위한 방법을 수행하기 위해서는, 제품 생산자에 의해 해당 제품을 블록체인 네트워크에 등록하고, 해당 제품을 판매하는 판매자가 해당 제품에 대한 1차적인 소유권을 갖도록 등록하여, 최종적으로 구매자가 판매자의 소유권을 이전받고, 혹은 소유권을 이전받은 구매자가 타 구매자에게 소유권을 재이전(중고 거래) 하는 등의 제품의 소유권을 거래하기 위한 방법이 선행될 수 있다.

[0043] 이와 같이, 제품의 소유권이 구매자에게 거래된 이후에 해당 제품의 소유권을 보유한 구매자에 의해 제품의 소유권을 인증하기 위한 방법이 수행될 수 있고, 따라서, 이하에서는 제품의 소유권을 거래하기 위한 방법에 대해 우선적으로 설명하도록 한다.

[0045] 도 1은 본 발명의 일 실시예에 따른 제품의 소유권을 거래하기 위한 방법을 수행하기 위한 시스템의 구성을 개략적으로 도시한다.

[0046] 도 1에서 도시되는 바와 같이, 제품의 소유권을 거래하기 위한 방법을 수행하기 위한 시스템은 서버시스템(1000)을 포함하고, 상기 서버시스템(1000)은 복수의 사용자단말(2000) 및 블록체인 네트워크(3000)와 통신을 수행하여, 제품의 소유권을 거래하기 위한 방법을 수행할 수 있다. 도 1에서 도시한 각각의 구성요소는 일 실시예인 것으로서, 다른 실시예에서는 추가적인 구성요소를 더 포함할 수 있다.

[0047] 사용자단말(2000)은 서버시스템(1000)과 통신을 수행하여, 제품에 대한 정보를 입력하거나, 제품을 판매하기 위하여 1차적으로 제품의 소유권을 등록하고, 최종 구매자에게 제품을 판매하는, 즉 제품의 소유권을 이전하는 과정들을 수행할 수 있다. 사용자단말(2000)은 해당 사용자단말(2000)에 구비된 웹 브라우저에서 구현되는 별도의 웹페이지를 통해 상기 서버시스템(1000)과 통신을 수행하거나, 혹은 해당 사용자단말(2000)에 구비된 별도의 어플리케이션을 통해 상기 서버시스템(1000)과 통신을 수행할 수 있다.

[0048] 한편, 도 1에 도시된 제품 생산자의 사용자단말(2000.1)은 제품 생산자가 서버시스템(1000)과 통신을 수행하기 위하여 사용하는 사용자단말(2000)에 해당할 수 있고, 판매자의 사용자단말(2000.2)은 판매자가 서버시스템(1000)과 통신을 수행하기 위하여 사용하는 사용자단말(2000)에 해당할 수 있고, 구매자의 사용자단말(2000.3)은 구매자가 서버시스템(1000)과 통신을 수행하기 위하여 사용하는 사용자단말(2000)에 해당할 수 있다.

[0049] 더 구체적으로 각각의 사용자들이 사용하는 사용자단말(2000.1, 2000.2 및 2000.3)은 사용자에 따라 사용자단말(2000)의 형태나 내부 구성이 상이한 것이 아니라, 사용자단말(2000)에 포함된 웹브라우저에 의해 구현되는 서버시스템(1000)과 통신을 수행하기 위한 웹페이지 혹은 사용자단말(2000)에 포함된 서버시스템(1000)과 통신을 수행하기 위한 어플리케이션에 로그인 하기 위한 각 사용자로 설정된 계정에 따라 사용자단말(2000)의 역할이 결정될 수 있다. 따라서, 단일 사용자단말(2000)에 대해 제품 생산자, 판매자, 구매자 별로 설정된 계정의 타입에 따라서 사용자단말은 제품 생산자의 사용자단말(2000.1), 판매자의 사용자단말(2000.2) 혹은 구매자의 사용자단말(2000.3)의 역할을 수행할 수도 있다.

[0050] 한편, 제품 생산자는 실제 제품을 생산하는 사용자에게 해당하며, 제품 생산자의 사용자단말(2000.1)을 통해 서버시스템(1000)에 해당 제품에 대한 정보를 입력하고, 해당 제품을 서버시스템(1000)에 등록하여 해당 제품에 대한 식별이미지를 제공받을 수 있다.

[0051] 판매자는 제품 생산자로부터 제품을 제공받고, 판매자의 사용자단말(2000.2)을 통해 해당 제품을 구매자에게 판매하는 역할을 수행한다. 따라서 판매자는 판매자의 사용자단말(2000.2)을 통해 서버시스템(1000)에 1차적으로 소유권을 등록하고, 해당 제품을 판매하는 경우 구매자에게 등록된 소유권을 이전하는 방식으로 제품을 판매할

수 있다.

- [0052] 본 발명의 다른 실시예에서는 상술한 제품 생산자 및 판매자는 동일 주체가 될 수도 있다. 따라서, 사용자단말에서 서버시스템(1000)과 통신을 수행하기 위한 별도의 웹페이지 혹은 어플리케이션에 대한 계정 타입에는 제품 생산자에 대한 계정 타입, 판매자에 대한 계정 타입 및 구매자에 대한 계정 타입뿐만 아니라, 제품 생산자 및 판매자 모두에 대한 계정 타입이 별도로 설정될 수도 있다.
- [0053] 구매자는 판매자로부터 제품을 구매하거나, 구매한 제품에 대해 타 구매자에게 중고거래를 수행하는 주체에 해당하는 일반적인 소비자의 역할을 수행한다. 따라서 구매자는 구매자의 사용자단말(2000.3)을 통해 구매한 제품의 목록 및 해당 제품의 세부정보를 제공받거나, 제품에 대한 소유권 인증 또는 소유권을 갖고 있는 제품에 대한 소유비밀번호 혹은 식별이미지의 복구를 수행할 수 있고, 타 구매자에게 본인이 소유한 제품을 중고 판매할 수 있다.
- [0055] 한편, 서버시스템(1000)은 1 이상의 서버를 포함하고, 복수의 사용자단말(2000) 및 블록체인 네트워크(3000)와 통신을 수행하여 제품의 소유권을 거래하기 위한 각각의 단계들을 수행한다. 또한 서버시스템(1000)은 DB(1010)를 포함하고, 상기 DB(1010)에는 각각의 계정에 대한 사용자정보, 사용자단말에서 입력한 제품정보, 서버시스템(1000)에서 소정의 단계를 수행하여 도출된 정보들이 저장될 수 있다.
- [0056] 본 발명의 다른 실시예에서 상기 DB(1010)는 서버시스템(1000) 내의 별도의 서버에 포함되어 서버시스템(1000)에서 수행하는 각각의 단계에서 필요한 정보들을 제공할 수도 있다.
- [0057] 또한, 서버시스템(1000)은 블록체인 네트워크(3000)로 스마트 컨트랙트를 생성하고, 생성된 스마트 컨트랙트를 기반으로 분산원장에 서버시스템(1000)에서 도출된 정보들을 기록하도록 요청할 수 있다. 한편, 도 1에서 도시된 일 실시예에서는 서버시스템(1000)이 블록체인 네트워크(3000)의 노드(3000.1 내지 3000.N)로 참여하고 있지 않으나, 본 발명의 다른 실시예에서는 상기 서버시스템(1000)이 블록체인 네트워크(3000)의 특정 노드(3000.1 내지 3000.N)로 참여하여 직접 블록체인 네트워크(3000)의 분산원장에 정보들을 기록할 수도 있다.
- [0059] 블록체인 네트워크(3000)는 블록체인 기술에 기반하여 동작하는 복수의 노드(3000.1 내지 3000.N)들을 포함한다. 상기 블록체인 기술은 블록이 체인형태로 연결된 저장 구조를 사용하여, 스마트 컨트랙트 및 해당 스마트 컨트랙트에 의해 기록되는 정보를 블록체인 네트워크(3000)를 구성하는 복수의 노드(3000.1 내지 3000.N)들에 저장하는 분산 저장 기술이다.
- [0060] 블록체인 네트워크(3000)는 특정 노드(3000.1 내지 3000.N)에서 기록된 정보를 합의 알고리즘에 기초하여 블록 형태로 저장할 수 있고, 블록 형태로 저장되는 데이터는 블록체인 네트워크(3000)를 구성하는 복수의 노드(3000.1 내지 3000.N)들에 의해 상호 공유될 수 있다.
- [0061] 블록체인 네트워크(3000)는 구현 형태에 따라서 임의의 노드(3000.1 내지 3000.N)들이 합의 동작을 수행할 수 있는 개방형(Public) 블록체인 네트워크(3000) 또는 기설정된 노드(3000.1 내지 3000.N) 혹은 별도의 승인과정을 통해 결정되는 노드(3000.1 내지 3000.N)만이 합의 동작을 수행할 수 있는 폐쇄형(Private) 블록체인 네트워크(3000) 형태를 포함할 수 있다. 본 발명의 일 실시예에 따른 블록체인 네트워크(3000)에서 수행되는 합의 알고리즘은, Proof of Work(PoW) 알고리즘, Proof of Stake(PoS) 알고리즘, Delegated Proof of Stake(DPoS) 알고리즘, Practical Byzantine Fault Tolerance(PBFT) 알고리즘, Delegated Byzantine Fault Tolerance(DB(1010)FT) 알고리즘, Redundant Byzantine Fault Tolerance(RBFT) 알고리즘, Sieve 알고리즘, Tendermint 알고리즘, Paxos 알고리즘, Raft 알고리즘, Proof of Authority(PoA) 알고리즘, 또는 Proof of Elapsed Time(PoET) 알고리즘을 포함할 수 있다.
- [0062] 블록체인 네트워크(3000)에 포함되는 각각의 노드(3000.1 내지 3000.N)들은 계층 구조에 따른 블록체인 코어 패키지에 의해 동작할 수 있다. 상기 계층 구조는 블록체인 네트워크(3000)에서 다뤄지는 데이터의 구조를 정의하고 데이터를 관리하는 데이터 계층, 블록의 유효성을 검증하고 블록을 생성하는 마이닝을 수행하고 마이닝 과정에서 채굴자에게 지급되는 수수료의 처리를 담당하는 합의 계층, 스마트 컨트랙트를 처리 및 실행시키는 스마트 컨트랙트 계층, P2P 네트워크 프로토콜, 해시 함수, 전자서명, 인코딩 및 공통 저장소를 구현 및 관리하는 공통 계층 및 다양한 어플리케이션이 생성, 처리 및 관리 되는 응용 계층을 포함할 수 있다.
- [0063] 한편, 상술한 스마트 컨트랙트는 서버시스템(1000)에서 도출된 정보, 예를 들어 암호화된 시리얼정보, 시리얼정

보, 개별제품식별정보, 해당 제품을 소유하고 있는 사용자에게 대한 사용자식별정보 또는 해당 제품을 과거에 소유했던 사용자에게 대한 1 이상의 사용자식별정보를 포함하는 원장기록정보가 프로그래밍 가능한 언어로 작성되고 임의의 컴퓨팅 장치에서 실행될 수 있다. 즉, 스마트 컨트랙트에 포함된 코드 또는 함수가 실행되는 경우, 본 발명의 일 실시예들과 같이 해당 제품에 대한 거래가 수행될 수 있다.

- [0065] 도 2는 본 발명의 일 실시예에 따른 서버시스템(1000)의 내부 구성을 개략적으로 도시한다.
- [0066] 도 2에 도시된 바와 같이, 서버시스템(1000)은 제품의 소유권을 거래하기 위한 각각의 단계들을 수행하는 복수의 구성요소를 포함하고, 각 구성요소에서 도출된 정보 혹은 사용자단말(2000)로부터 수신한 정보들을 저장하는 DB(1010)를 포함한다.
- [0067] 구체적으로, 제품식별정보제공단계를 수행하는 제품식별정보제공부(1100)는 제품 생산자의 사용자단말(2000.1), 즉 제품 생산자의 계정 타입에 해당하는 계정으로 로그인한 사용자단말(2000)로부터 생산한 제품에 대한 제품정보를 수신하여, 상기 제품정보에 상응하는 제품식별정보를 도출하고, 상기 제품식별정보를 해당 제품 생산자의 사용자단말(2000.1)로 송신한다. 한편, 상기 제품식별정보 및 이에 해당하는 제품정보는 후술하는 DB(1010)에 포함되는 제품정보테이블(1011)에 저장될 수 있다.
- [0068] 개별제품등록단계를 수행하는 개별제품등록부(1200)는 제품 생산자의 사용자단말(2000.1)로부터 개별제품에 대한 개별제품등록요청정보를 수신하고, 상기 개별제품등록요청정보에 기초하여 원장기록정보를 도출하여 해당 원장기록정보를 블록체인 네트워크(3000)의 분산원장에 기록한다.
- [0069] 한편, 상기 개별제품등록요청정보는 개별제품을 블록체인 네트워크(3000)의 분산원장에 기록하기 위한 정보에 해당하고, 상기 개별제품은 제품식별정보제공단계에서 도출된 제품식별정보에 상응하는 제품일 수 있다. 예를 들어, 상기 제품식별정보제공단계에서 수신하는 제품정보는 '갤럭시 S20'과 같이 제품군에 대한 정보에 해당하고, 개별제품은 '갤럭시 S20'에 대한 각각의 제품에 해당한다.
- [0070] 따라서, 제품 생산자가 해당 사용자단말(2000.1)을 통해 특정 제품정보를 입력하고, 제품식별정보제공부(1100)는 상기 특정 제품정보를 수신하여 해당 제품정보에 대한 제품식별정보를 해당 사용자단말(2000.1)에 제공한다. 이어서 제품식별정보를 제공받은 제품 생산자는 제공받은 제품식별정보에 상응하는 개별제품에 대한 개별제품등록요청정보를 서버시스템(1000)으로 송신하고, 서버시스템(1000)의 개별제품등록부(1200)는 상기 개별제품등록요청정보에 기초하여 해당 개별제품에 대한 원장기록정보를 도출하여 블록체인 네트워크(3000)의 분산원장에 기록한다.
- [0071] 다음으로 식별이미지제공단계를 수행하는 식별이미지제공부(1300)는 상기 개별제품등록단계에서 도출된 원장기록정보에 기초하여 식별이미지를 생성하고, 생성된 상기 식별이미지를 해당 제품 생산자의 사용자단말(2000.1)에 제공한다. 상기 식별이미지는 해당 개별제품에 부착되거나 해당 개별제품에 대한 품질보증서 등에 함께 포함되며, 상기 식별이미지는 사용자단말(2000)에 구비된 촬영모듈에 의해 식별되어 해당 개별제품의 소유권을 확인 혹은 인증하는 데 사용되거나, 해당 개별제품의 소유권을 판매하는 데 사용될 수 있다.
- [0072] 한편, 상기 식별이미지는 소정의 식별정보를 사용자단말(2000)에서 식별할 수 있는 모든 형태의 이미지를 포함할 수 있다. 예를 들어, 바코드, PDF417 코드, Data Matrix 코드, Maxi 코드, Veri 코드, Aztec 코드 등과 같은 2차원 바코드가 상기 식별이미지에 해당될 수 있고, 바람직하게는 QR코드가 상기 식별이미지에 해당될 수 있다.
- [0073] 소유권등록단계를 수행하는 소유권등록부(1400)는 상술한 제품 생산자로부터 개별제품등록단계를 통해 분산원장에 기록된 제품을 제공받은 판매자의 사용자단말(2000.2)로부터 해당 개별제품에 대한 소유권등록요청정보를 수신하는 경우, 해당 판매자의 사용자식별정보를 상기 원장기록정보에 추가하여 분산원장에 기록한다.
- [0074] 소유권등록단계는 제품을 판매하기 위해 해당 개별제품의 소유권을 판매자로 설정하는 과정에 해당하고, 해당 개별제품을 실질적으로 구매자에게 판매하는 경우에, 소유권을 구매자에게 이전하는 과정을 통해 해당 개별제품의 구매가 이루어질 수 있다.
- [0075] 소유권판매단계를 수행하는 소유권판매부(1500)는 해당 개별제품에 대해 소유권을 갖고 있는 판매자의 사용자단말(2000.2)로부터 소유권판매요청정보를 수신하고, 상기 소유권판매요청정보에 기초하여 구매자의 사용자식별정보를 해당 개별제품의 원장기록정보에 추가하여 분산원장에 기록한다. 상기 소유권판매단계에서 구매자의 동의 없이 소유권이 이전되는 것을 방지하기 위하여, 소유권판매요청정보를 소유권판매부(1500)로 송신하기 이전에

상기 판매자의 단말 상에서 판매자 및 구매자의 구매동의 의사를 확인하는 과정이 선행될 수도 있다. 또한, 상기 소유권판매단계는 판매자 및 구매자간의 거래에서만 수행되는 것이 아니라 구매자 사이의 중고거래를 수행하는 데 있어서도 동일하게 상기 소유권판매단계가 수행되어, 구매자간의 소유권을 판매할 수 있다.

- [0076] 본 발명의 다른 실시예에서는, 소유권판매부(1500)는 구매자의 사용자단말(2000.2)을 통해 상기 소유권판매요청정보를 수신할 수도 있고, 혹은 상기 소유권판매요청정보에 포함되는 판매자가 입력해야 하는 정보의 경우 판매자의 사용자단말(2000.2)을 통해 수신하고, 상기 소유권판매요청정보에 포함되는 구매자가 입력해야 하는 정보의 경우 구매자의 사용자단말(2000.3)을 통해 개별적으로 수신할 수도 있다.
- [0077] 소유권인증부(1600)는 사용자단말(2000)로부터 상기 소유권인증요청정보를 수신하여, 해당 개별제품의 소유권을 인증하는 단계를 수행할 수 있다. 더 구체적으로 상기 소유권인증요청정보는 인증하고자 하는 개별제품에 상응하는 식별이미지 및 해당 개별제품에 대한 소유비밀번호를 포함하고, 상기 소유권인증부(1600)는 해당 개별제품의 식별이미지 및 소유비밀번호에 기초하여 해당 개별제품의 소유권을 인증할 수 있다.
- [0078] 소유현황제공단계를 수행하는 소유현황제공부(1700)는, 판매자의 사용자단말(2000.2) 혹은 구매자의 사용자단말(2000.3)로부터 소유현황제공요청정보를 수신하는 경우, 해당 사용자단말에 상응하는 사용자식별정보를 포함하는 1 이상의 원장기록정보를 도출하고, 도출된 1 이상의 원장기록정보에 기초하여 해당 판매자 혹은 해당 구매자가 소유하고 있는 제품정보를 해당 사용자단말에 제공한다.
- [0079] 식별이미지복원단계를 수행하는 식별이미지복원부(1800)는, 특정 개별제품을 소유한 구매자의 사용자단말(2000.3)로부터 해당 사용자단말에서 해당 개별제품의 개별제품식별정보 및 소유비밀번호를 포함하는 식별이미지복원요청정보를 수신하는 경우, 상기 식별이미지복원요청정보에 상응하는 원장기록정보에 기초하여 해당 개별제품에 대한 식별이미지를 다시 생성하여 해당 사용자단말에 제공한다.
- [0080] 소유비밀번호갱신단계를 수행하는 소유비밀번호갱신부(1900)는, 특정 개별제품을 소유한 구매자의 사용자단말(2000.3)로부터 해당 사용자단말에서 식별한 해당 개별제품에 대한 식별이미지 및 변경하고자 하는 소유비밀번호를 포함하는 소유비밀번호갱신요청정보를 수신하고, 상기 소유비밀번호갱신요청정보에 기초하여 해당 개별제품에 대한 가변키를 갱신하는 것으로 소유비밀번호를 변경할 수 있다.
- [0081] 본 발명에서는 상기 소유비밀번호는 서버시스템(1000)에 저장되지 않으므로, 구매자가 소유비밀번호를 잊어버린 경우, 이전에 설정한 소유비밀번호를 찾는 것이 아니라 새로 변경하는 것으로 소유비밀번호를 찾을 수 있게 된다.
- [0083] 한편, 상기 서버시스템(1000)은 DB(1010)를 포함하고, 상기 DB(1010)에는 제품정보테이블(1011), 가변키테이블(1012), 고유키테이블(1013), 제품매핑테이블(1014), 대칭키테이블(1015), 사용자정보테이블(1016) 및 소유자매핑테이블(1017)을 포함할 수 있다.
- [0084] 상기 제품정보테이블(1011)은 제품식별정보제공단계에서 수신한 제품정보가 저장되고, 더 구체적으로, 상기 제품식별정보제공단계는 수신한 제품정보에 상응하는 제품식별정보를 생성하고, 상기 제품식별정보 및 상기 제품정보를 매칭하여 상기 제품정보테이블(1011)에 저장한다.
- [0085] 상기 가변키테이블(1012)은 개별제품등록부(1200)에서 생성된 개별제품에 대한 가변키가 저장되고, 더 구체적으로 상기 가변키는 개별제품등록부(1200)에서 최초 생성되고, 이후 소유비밀번호가 변경되는 경우, 소유비밀번호에 기초하여 도출되는 소유키에 상응하여 가변될 수 있다. 또한 상기 가변키테이블(1012)에는 해당 개별제품의 개별제품식별정보에 상응하는 가변키가 매칭되어 저장된다.
- [0086] 상기 고유키테이블(1013)은 개별제품등록부(1200)에서 생성된 개별제품에 대한 고유키가 저장되고, 더 구체적으로 상기 고유키는 개별제품등록부(1200)에서 최초 생성된 후 그 값이 항상 변하지 않는 특성을 갖고 있다. 한편, 상기 고유키테이블(1013)에는 해당 개별제품의 개별제품식별정보에 상응하는 고유키가 매칭되어 저장된다.
- [0087] 상기 제품매핑테이블(1014)은 개별제품등록부(1200)에서 생성된 개별제품에 대한 개별제품식별정보가 저장되고, 더 구체적으로 상기 제품매핑테이블(1014)에는 해당 개별제품에 상응하는 제품식별정보와 개별제품식별정보가 매칭되어 저장된다. 따라서, 구매자 혹은 판매자가 소유권을 갖고 있는 개별제품에 대한 제품정보를 사용자단말(2000)을 통해 요청하는 경우, 소유현황제공부(1700)는 상기 제품매핑테이블(1014)에 저장된 구매자 혹은 판매자가 소유권을 갖고 있는 개별제품의 개별제품식별정보에 매칭되는 제품식별정보를 도출하고, 도출된 제품식별

정보에 기초하여 상기 제품정보테이블(1011)에 저장된 제품정보를 로드하여 해당 사용자단말(2000)로 해당 개별 제품에 대한 제품정보를 제공할 수 있다.

[0088] 상기 대칭키테이블(1015)에는 상기 가변키테이블(1012)에 저장되는 가변키를 암호화하는 제1대칭키가 저장되어 있고, 상기 고유키테이블(1013)에 저장되는 고유키를 암호화하는 제2대칭키가 저장되어 있다. 따라서 개별제품등록부(1200)는 생성된 가변키를 가변키테이블(1012)에 저장하는 경우, 상기 제1대칭키에 기초하여 가변키를 암호화하고, 암호화된 가변키를 상기 가변키테이블(1012)에 저장하고, 마찬가지로 개별제품등록부(1200)는 생성된 고유키를 고유키테이블(1013)에 저장하는 경우, 상기 제2대칭키에 기초하여 고유키를 암호화하고, 암호화된 고유키를 상기 고유키테이블(1013)에 저장한다.

[0089] 한편, 상기 가변키테이블(1012)에 저장된 암호화된 가변키를 복호화하는 경우 제1대칭키를 사용하여 가변키를 복호화하고, 상기 고유키테이블(1013)에 저장된 암호화된 고유키를 복호화하는 경우 제2대칭키를 사용하여 고유키를 복호화할 수 있다. 상기 가변키를 제1대칭키에 기초하여 암호화하고, 상기 고유키를 제2대칭키에 기초하여 암호화하기 위하여 일반적으로 사용하는 대칭키 기반의 암호화 방식을 사용할 수 있으나, 바람직하게는 고급 암호화 표준(Advanced Encryption Standard, AES)방식으로 암호화될 수 있다.

[0090] 상기 사용자정보테이블(1016)에는 제품 생산자, 판매자, 구매자 등과 같이 상기 서버시스템(1000)과 통신을 수행하는 사용자단말의 사용자의 계정에 대한 정보들이 저장된다. 예를 들어, 해당 사용자의 이메일정보, 계정비밀번호정보, 이름정보 등과 같이 일반적으로 회원가입과 같이 계정을 설정할 때 입력하는 정보들이 포함되고, 추가적으로 제품 생산자, 판매자 또는 구매자와 같은 사용자에 대한 타입에 대한 정보가 포함될 수 있다.

[0091] 상기 소유자매핑테이블(1017)에는 각각의 개별제품의 암호화된 시리얼정보 및 상기 암호화된 시리얼정보에 상응하는 사용자식별정보가 매칭되어 저장된다. 구체적으로, 각각의 개별제품의 암호화된 시리얼정보에 상응하는 사용자식별정보는 해당 개별제품을 현재 소유하고 있는 사용자의 사용자식별정보를 포함하고, 본 발명의 다른 실시예에서 상기 각각의 개별제품의 암호화된 시리얼정보에 상응하는 사용자식별정보는 해당 개별제품을 과거에 소유했던 1 이상의 사용자의 사용자식별정보를 더 포함할 수 있다.

[0093] 한편, 상기 서버시스템(1000)은 제1서버 및 상기 제1서버만을 대상으로 통신을 수행하는 제2서버를 포함하고, 상기 제2서버는 상기 고유키테이블(1013)을 포함하고, 상기 제1서버에서 상기 제1키도출단계를 통해 생성된 고유키를 해당 개별제품식별정보에 매칭하여 상기 고유키테이블(1013)에 저장할 수 있다.

[0095] 구체적으로, 상기 고유키테이블(1013)에 저장되는 개별제품에 대한 고유키는 상술한 바와 같이 항상 값이 변하지 않는 특성을 갖고 있고, 고유키는 해당 개별제품에 대한 시리얼정보를 암호화하고, 복호화하는 중요한 키에 해당하므로, 상기 고유키테이블(1013)이 외부로 유출되는 것을 방지하는 등의 보안성을 향상시키기 위하여 상기 고유키테이블(1013)은 상기 서버시스템(1000) 내의 별도의 제2서버에 포함되고, 상기 제2서버는 상기 서버시스템(1000) 내의 타 서버만을 대상으로 통신을 수행하고, 전술한 사용자단말(2000) 및 블록체인 네트워크(3000) 등 서버시스템(1000) 외부의 구성 요소와는 통신을 수행하지 않는 망분리 형태로 구성될 수 있다. 따라서, 상기 고유키테이블(1013)에 대한 해킹 등의 유출 가능성을 원천적으로 차단할 수 있는 효과를 발휘할 수 있다.

[0096] 본 발명의 다른 실시예에서는, 상기 고유키테이블(1013)을 포함하는 제2서버는 단순히 고유키테이블(1013)에 포함된 고유키를 상기 서버시스템(1000) 내의 타 서버에 제공하는 것이 아니라, 상기 제2서버는 고유키에 기초하여 수행하는 과정들을 직접 수행하여 상기 타 서버에 제공할 수 있다. 예를 들어, 시리얼정보를 고유키에 기초하여 암호화 하거나, 암호화된 시리얼정보를 고유키에 기초하여 복호화하는 단계들을 제2서버에서 직접 수행하고, 수행 결과를 서버시스템(1000) 내의 타 서버에 제공할 수도 있다.

[0098] 도 3은 본 발명의 일 실시예에 따른 서버시스템(1000)에 포함되는 각각의 테이블을 구성하는 필드들을 개략적으로 도시한다.

[0099] 도 3의 (A)에 도시된 바와 같이, 제품정보테이블(1011)에는 제품식별정보제공부(1100)에서 수신한 제품정보 및 상기 제품정보에 상응하여 도출된 제품식별정보가 매칭되어 저장된다. 따라서 상기 제품정보테이블(1011)에는 제품식별정보 및 해당 제품식별정보에 매칭되는 제품정보가 하나의 레코드 형태로 저장되고, 각각의 레코드는 복수의 필드로 구성된다. 상기 제품정보테이블(1011)은 사용자단말에서 해당 제품에 대한 정보를 요청하는

경우, 해당 제품에 대한 제품식별정보에 매칭되는 제품정보를 제공한다.

- [0100] 상기 제품정보는 언어정보, 제품명칭정보, 제조사정보, 출고일자정보, 제품설명정보 및 제품이미지정보 등을 포함한다. 상기 언어정보는 해당 제품정보가 작성된 언어에 대한 정보에 해당하여, 다양한 국적을 가진 제품 생산자가 서버시스템(1000)을 통해 제품정보를 등록할 수 있도록 서버시스템(1000)에 대한 접근을 용이하게 할 수 있다.
- [0101] 한편, 상기 제품정보테이블(1011)에 포함되는 제품정보는 도 3에 도시된 복수의 필드에만 한정되지 아니하고, 해당 제품의 가격정보 등 제품에 대한 다양한 정보들을 추가적으로 포함할 수 있다.
- [0103] 도 3의 (B)에 도시된 제품매핑테이블(1014)에는 제품식별정보제공단계에서 도출된 제품식별정보 및 개별제품등록단계에서 생성된 개별제품식별정보가 매칭되어 저장된다. 개별제품은 특정 제품군에 포함되는 각각의 제품에 해당하고, 각 개별제품별로 개별제품식별정보가 할당될 수 있다. 따라서, 특정 개별제품에 대해 소유권을 갖고 있는 구매자가 해당 개별제품에 대한 제품정보를 요청하는 경우, 상기 제품매핑테이블(1014)에 저장된 특정 개별제품의 개별제품식별정보에 매칭되는 제품식별정보를 도출하고, 상기 제품정보테이블(1011)에서 해당 제품식별정보에 매칭되는 제품정보를 도출하여 해당 구매자에게 제공함으로써 해당 개별제품에 대한 제품정보를 제공할 수 있다.
- [0105] 도 3의 (C)에 도시된 가변키테이블(1012)에는 개별제품등록단계에서 생성된 개별제품식별정보 및 가변키가 매칭되어 저장된다. 가변키는 소유키와 함께 해당 개별제품에 대한 고유키를 생성하기 위해 필요한 인자에 해당하고, 소유키가 변경됨에 따라 갱신될 수 있다. 더 구체적으로 상기 가변키는 최초 생성되는 경우 무작위로 생성될 수 있고, 변경된 소유키에 따라 갱신되어 상기 가변키테이블(1012)에 저장될 수 있다.
- [0107] 도 3의 (D)에 도시된 고유키테이블(1013)에는 개별제품등록단계에서 생성된 개별제품식별정보 및 고유키가 매칭되어 저장된다. 고유키는 가변키 및 소유키에 기초하여 생성되고, 시리얼정보를 암호화하거나, 암호화된 시리얼정보를 복호화하는, 즉 시리얼정보에 대한 대칭키에 해당한다. 따라서, 고유키가 무단으로 유출되는 경우 식별 이미지를 통해 식별된 암호화된 시리얼정보를 타인이 복호화할 수 있으므로 소유권이 무단으로 이전될 수 있고, 따라서 본 발명의 다른 실시예에서는 상기 고유키테이블(1013)은 서버시스템(1000) 내의 별도의 서버에 포함될 수 있다.
- [0109] 도 3의 (E)에 도시된 사용자정보테이블(1016)에는 서버시스템(1000)에 접속하는 사용자의 계정에 대한 정보가 저장된다. 상기 사용자정보테이블(1016)에 저장되는 각각의 레코드는 사용자식별정보, 이메일정보, 계정비밀번호정보, 이름정보, 전화번호정보 및 생년월일정보 등을 포함한다. 본 발명의 일 실시예에서 이메일정보, 계정비밀번호정보, 이름정보, 전화번호정보 및 생년월일정보는 사용자단말을 이용하는 주체가 입력하는 정보에 해당하고, 사용자식별정보는 서버시스템(1000)에서 자동적으로 생성되고, 상기 사용자단말을 이용하는 주체가 입력하는 정보에 매칭되어 사용자정보테이블(1016)에 저장될 수 있다.
- [0110] 한편, 소유권을 구매자에게 판매하는 경우, 소유권판매단계에서는 구매자에 대한 정보를 포함하는 소유권판매요청정보를 수신하고, 구매자에 대한 정보에 상응하는 사용자식별정보가 존재하는지 판단할 수 있다. 예를 들어, 구매자에 대한 정보에는 해당 구매자의 이메일정보 및 생년월일정보를 포함하고, 상기 소유권판매단계에서는 사용자정보테이블(1016)에 상기 이메일정보 및 상기 생년월일정보에 해당하는 사용자식별정보가 존재하는지 여부를 판단할 수 있다.
- [0111] 또한, 본 발명의 다른 실시예에서 상기 사용자정보테이블(1016)에 저장되는 각각의 레코드에는 해당 계정 타입에 대한 정보를 더 포함할 수 있고, 계정 타입에는 제품 생산자에 대한 계정 타입, 판매자에 대한 계정 타입, 구매자에 대한 계정 타입을 포함할 수 있다.
- [0113] 도 3의 (F)에 도시된 대칭키테이블(1015)에는 제1대칭키 및 제2대칭키가 저장된다. 본 발명의 일 실시예에서는 상기 가변키테이블(1012)에 저장되는 가변키는 암호화되어 저장되고, 상기 제1대칭키는 가변키를 대칭키 방식으

로 암호화하는 데 사용되고, 상기 가변키테이블(1012)에 저장된 암호화된 가변키를 복호화하는 데 사용된다. 마찬가지로, 상기 고유키테이블(1013)에 저장되는 고유키는 암호화되어 저장되고, 상기 제2대칭키는 고유키를 대칭키 방식으로 암호화하는 데 사용되고, 상기 고유키테이블(1013)에 저장된 암호화된 고유키를 복호화하는 데 사용된다. 따라서, 제2대칭키를 통해 고유키가 암호화되므로 상기 고유키테이블(1013)이 망분리된 별도의 서버에 포함되는 것과 별개로 추가적인 보안성을 향상시킬 수 있는 효과를 발휘할 수 있다.

[0114] 한편, 상기 대칭키테이블(1015)에 포함되는 제1대칭키 및 제2대칭키는 각각의 개별제품식별정보에 해당하는 가변키 및 고유키에 따라 개별적으로 구성될 수 있으나, 바람직하게는 상기 대칭키테이블(1015)에는 단일의 제1대칭키 및 단일의 제2대칭키가 저장되고, 각각의 개별제품식별정보에 해당하는 가변키 및 고유키는 단일의 제1대칭키 및 단일의 제2대칭키에 의해 암호화되거나, 복호화될 수 있다.

[0116] 도 3의 (G)에 도시된 소유자매핑테이블(1017)에는 각각의 개별제품에 대한 암호화된 시리얼정보 및 이에 상응하는 1 이상의 사용자식별정보가 저장된다. 상기 소유자매핑테이블(1017)은 후술하는 소유현황제공부(1700)에서 수행하는 소유현황제공단계에서 해당 사용자가 소유했거나 혹은 소유했던 1 이상의 개별제품에 대한 제품정보를 제공하기 위하여 사용될 수 있다.

[0118] 도 4는 본 발명의 일 실시예에 따른 소유권을 거래하기 위한 과정을 개략적으로 도시한다.

[0120] 도 4에 도시된 바와 같이, 1 이상의 사용자단말 및 블록체인 네트워크(3000)와 통신을 수행하는 1 이상의 프로세서 및 1 이상의 메모리를 포함하는 서버시스템(1000)에서 수행되는 제품의 소유권을 거래하기 위한 방법으로서, 제품 생산자의 사용자단말(2000.1)로부터 제품정보를 수신하여 상기 제품정보에 상응하는 제품식별정보를 도출하고, 상기 제품 생산자의 사용자단말(2000.1)에 상기 제품식별정보를 제공하는 제품식별정보제공단계; 상기 제품 생산자의 사용자단말(2000.1)로부터 상기 제품식별정보에 상응하는 개별제품에 대한 개별제품등록요청정보를 수신하는 단계; 상기 개별제품등록요청정보에 기초하여 개별제품에 대한 원장기록정보를 도출하고, 상기 원장기록정보를 상기 블록체인 네트워크(3000)의 분산원장에 기록하는 개별제품등록단계; 상기 원장기록정보에 기초하여 식별이미지를 생성하여 상기 제품 생산자의 사용자단말(2000.1)로 제공하는 식별이미지제공단계; 판매자의 사용자단말(2000.2)로부터 상기 판매자의 사용자단말(2000.2)에서 인식한 식별이미지 및 판매자 소유비밀번호를 포함하는 소유권등록요청정보를 수신하는 단계; 상기 소유권등록요청정보에 기초하여 상기 판매자에 해당하는 사용자식별정보를 상기 원장기록정보에 추가하여 상기 분산원장에 기록하는 소유권등록단계; 상기 판매자의 사용자단말(2000.2)로부터 상기 판매자의 사용자단말(2000.2)에서 인식한 식별이미지, 상기 판매자 소유비밀번호, 구매자 소유비밀번호 및 구매자에 대한 정보를 포함하는 소유권판매요청정보를 수신하는 단계; 및 상기 소유권판매요청정보에 기초하여 상기 구매자에 대한 정보에 상응하는 사용자식별정보를 상기 원장기록정보에 추가하여 상기 분산원장에 기록하는 소유권판매단계;를 포함한다.

[0122] 구체적으로, 제품 생산자는 해당 사용자단말(2000.1)에 디스플레이되는 인터페이스를 통해 제품정보를 입력(S10)하고, 서버시스템(1000)은 상기 제품 생산자의 사용자단말(2000.1)로부터 상기 제품정보를 수신(S11)한다. 상기 제품정보에는 상술한 바와 같이, 언어정보, 제품명칭정보, 제조사정보, 출고일자정보, 제품설명정보 및 제품이미지정보를 포함한다.

[0123] 한편, 서버시스템(1000)의 제품식별정보제공부(1100)는, 수신한 제품정보에 상응하는 제품식별정보를 도출(S12)하고, 상기 제품식별정보를 해당 제품 생산자의 사용자단말(2000.1)로 송신(S13)한다. 더 구체적으로 상기 제품식별정보는 각각의 제품정보를 식별하기 위한 정보로써, 각각의 제품식별정보가 중복되지 않도록 도출된다. 또한 제품식별정보는 해당 제품정보에 포함되는 개별제품을 서버시스템(1000)에 등록하기 위한 개별제품등록요청정보에 포함될 수 있다.

[0124] 본 발명의 다른 실시예에서 상기 제품식별정보제공부(1100)는 제품정보를 송신하는 사용자단말의 계정 타입이 제품 생산자에 해당하는 계정 타입인지 여부를 판별하고, 제품 생산자에 해당하는 계정 타입으로 판별된 경우에 제품식별정보를 도출할 수도 있다. 이와 같은 과정을 통해 제품 생산자에 해당하는 계정 타입과 상이한 계정 타입, 예를 들어 판매자에 대한 계정 타입 혹은 구매자에 대한 계정 타입의 사용자단말에서 제품정보를 송신하는

경우, 제품식별정보제공부(1100)는 제품식별정보를 도출하지 않을 수도 있다.

- [0125] 제품 생산자의 입력에 기초하여 제품 생산자의 사용자단말(2000.1)은 개별제품등록요청정보를 서버시스템(1000)으로 송신하고, 서버시스템(1000)의 개별제품등록부(1200)는 상기 개별제품등록요청정보를 수신(S14)하고, 개별제품에 대한 원장기록정보를 도출(S15)하여 상기 블록체인 네트워크(3000)의 분산원장에 상기 원장기록정보를 기록하도록 요청(S16)한다.
- [0126] 구체적으로, 상기 개별제품등록요청정보에는 등록하고자 하는 개별제품에 대한 시리얼정보가 포함될 수 있으나, 바람직하게는 상기 개별제품등록요청정보를 수신하는 경우, 상기 개별제품등록부(1200)에서 해당 개별제품에 대한 시리얼정보를 생성할 수 있다. 한편, 상기 원장기록정보는 생성된 상기 시리얼정보, 암호화된 시리얼정보 및 개별제품식별정보를 포함한다.
- [0127] 더 구체적으로 상기 개별제품등록부(1200)는 서버시스템(1000)에 기저장된 초기 소유비밀번호에 기초하여 소유키를 도출하고, 임의의 가변키를 도출한 후, 상기 소유키 및 상기 가변키에 기초하여 고유키를 도출하고, 도출된 고유키를 대칭키로 하여 상기 시리얼정보를 암호화할 수 있다. 바람직하게 상기 소유키는 초기 소유비밀번호를 해시함수에 입력함으로써 기설정된 크기로 도출되고, 상기 고유키는 상기 소유키 및 상기 가변키를 배타적 논리합(Exclusive OR, XOR)으로 연산함으로써 도출될 수 있다. 따라서 상술한 바와 같이 소유키가 변경되는 경우, 항상 고정 값을 갖는 고유키 및 변경된 소유키를 XOR 연산하여 가변키를 갱신할 수 있다.
- [0128] 한편, 상기 블록체인 네트워크(3000)는 상기 서버시스템(1000)의 개별제품등록부(1200)로부터 상기 원장기록정보의 기록 요청에 따라 분산원장에 상기 원장기록정보를 기록(S17)한다. 바람직하게 상기 요청에 따른 원장기록정보는 상기 블록체인 네트워크(3000)에 포함된 스마트 컨트랙트에 의해 블록체인 네트워크(3000)의 분산원장에 기록된다. 한편, 상기 원장기록정보는 분산원장의 트랜잭션 혹은 별도의 저장영역에 기록되고, 상기 스마트 컨트랙트에 포함되는 별도의 DB에도 기록될 수 있다. 따라서 서버시스템(1000)에서 블록체인 네트워크(3000)로 기록된 원장기록정보에 대한 조회를 쿼리하는 경우, 상기 스마트 컨트랙트는 분산원장에 기록된 원장기록정보를 도출하지 않더라도, 상기 스마트 컨트랙트에 포함되는 별도의 DB를 통해 해당 쿼리에 대한 응답정보를 서버시스템(1000)에 제공할 수도 있다.
- [0129] 한편, 식별이미지제공부(1300)는 생성된 원장기록정보에 기초하여 식별이미지를 생성하고, 해당 사용자단말(2000)에 생성된 식별이미지를 송신(S18)한다. 더 구체적으로 상기 식별이미지제공부(1300)는 상기 원장기록정보에 포함되는 암호화된 시리얼정보에 기초하여 식별이미지를 생성한다.
- [0130] 본 발명의 다른 실시예에서는 상기 식별이미지제공부(1300)는 암호화된 시리얼정보를 포함하는 식별이미지기초정보를 생성하여, 해당 사용자단말(2000)에 송신하고, 최종적으로 해당 사용자단말(2000)에서 상기 식별이미지기초정보를 통해 식별이미지를 디스플레이할 수도 있다.
- [0131] 상술한 과정(S10 내지 S18)을 통해 제품 생산자는 제조한 개별제품을 블록체인 네트워크(3000)에 등록하고, 서버시스템(1000)으로부터 제공받은 해당 개별제품에 대한 식별이미지를 출력하여, 해당 개별제품에 부착하거나 혹은 상기 식별이미지를 포함하는 품질보증서를 작성하여 개별제품과 함께 제품을 판매하는 대리점의 관리자를 포함하는 판매자에게 해당 개별제품을 공급할 수 있다.
- [0133] 한편, 식별이미지를 포함하는 개별제품을 공급받은 판매자는 판매자의 사용자단말(2000.2)을 통해 소유권등록요청정보를 서버시스템(1000)으로 송신하고, 상기 서버시스템(1000)의 소유권등록부(1400)는 상기 소유권등록요청정보를 수신(S19)한다. 이어서 상기 소유권등록요청정보를 수신한 소유권등록부(1400)는 해당 사용자단말(2000.2)의 계정에 대한 사용자식별정보를 상기 원장기록정보에 추가하여 블록체인 네트워크(3000)의 분산원장에 상기 추가된 원장기록정보를 기록하도록 요청(S20)한다. 구체적으로, 소유권등록부(1400)는 소유권등록요청정보를 송신한 사용자단말(2000.2)의 계정에 상응하는 사용자식별정보를 상기 원장기록정보에 추가하여 분산원장에 기록하도록 상기 블록체인 네트워크(3000)에 요청한다.
- [0134] 더 구체적으로 상기 소유권등록요청정보에는 해당 사용자단말(2000.2)을 통해 서버시스템(1000)에 접속한 계정의 이메일정보 혹은 이름정보와 같이 계정을 설정하기 위해 입력한 1 이상의 정보가 포함되고, 상기 소유권등록부(1400)는 상기 사용자정보테이블(1016)에 저장된 상기 계정을 설정하기 위해 입력한 1 이상의 정보에 매칭되는 사용자식별정보를 도출하고, 도출된 사용자식별정보를 상기 원장기록정보에 추가하여 분산원장에 기록하도록 요청할 수 있다. 바람직하게는, 서버시스템(1000) 및 판매자의 사용자단말(2000.2)은 세션방식으로 접속되어 있으므로, 해당 판매자의 사용자단말(2000.2)로부터 소유권등록요청정보를 수신하는 경우, 상기 소유권등록요청정

보에 계정을 설정하기 위해 입력한 1 이상의 정보가 포함되어 있지 않더라도, 자동적으로 사용자식별정보를 도출하여 분산원장에 기록을 요청할 수 있다.

[0135] 한편, 상기 블록체인 네트워크(3000)는 상기 서버시스템(1000)의 소유권등록부(1400)로부터 판매자의 사용자식별정보가 추가된 원장기록정보의 기록 요청에 따라 분산원장에 상기 원장기록정보를 기록(S21)한다. 바람직하게 상기 블록체인 네트워크(3000)에 포함된 스마트 컨트랙트에 의해 상기 요청에 따른 판매자의 사용자식별정보가 추가된 원장기록정보가 블록체인 네트워크(3000)의 분산원장에 기록된다. 한편, 상기 원장기록정보는 분산원장의 트랜잭션 혹은 별도의 저장영역에 기록되고, 상기 스마트 컨트랙트에 포함되는 별도의 DB에도 기록될 수 있다.

[0136] 더 구체적으로, 상기 스마트 컨트랙트는 상기 소유권등록부(1400)로부터의 요청에 따라 소유권등록요청정보를 송신한 판매자의 사용자단말(2000.2)의 계정 타입이 판매자에 해당하는 계정 타입인지 판별하고, 판매자에 해당하는 계정 타입인 경우에, 상기 소유권등록요청정보에 포함되는 판매자의 사용자단말(2000.2)이 식별한 식별이미지에 상응하는 원장기록정보에 판매자의 사용자식별정보를 추가하여 분산원장에 기록한다. 이러한 과정을 통해 제품 생산자 혹은 일반 구매자와 같이 상이한 계정 타입을 가진 계정으로부터 임의로 해당 개별제품의 소유권을 등록하는 것을 방지할 수 있는 효과를 발휘할 수 있다.

[0137] 한편, 본 발명의 다른 실시예에서는 소유권등록요청정보를 송신한 판매자의 사용자단말(2000.2)의 계정 타입이 판매자에 해당하는 계정 타입인지 판별하는 과정은 상기 소유권등록부(1400)에서 수행될 수 있고, 계정 타입이 판매자에 해당하는 계정 타입인 경우에 분산원장에 기록을 요청할 수 있다.

[0138] 상술한 과정(S19 내지 S21)을 통해 해당 개별제품을 판매하고자 하는 판매자는 개별제품에 대한 소유권을 상기 블록체인 네트워크(3000)의 분산원장에 기록하게 된다. 이후 구매자가 해당 개별제품을 구매하는 경우 판매자로 등록되어 있는 소유권이 상기 개별제품을 구매한 구매자로 변경되는 것으로 상기 개별제품에 대한 구매가 수행될 수 있다.

[0140] 한편 판매자가 해당 개별제품을 구매자에게 판매하는 경우, 판매자 및 구매자의 입력에 기초하여 판매자의 사용자단말(2000.2)은 소유권판매요청정보를 서버시스템(1000)에 송신하고, 상기 서버시스템(1000)의 소유권판매부(1500)는 상기 소유권판매요청정보를 수신(S22)한다. 이어서 상기 소유권판매요청정보를 수신한 소유권판매부(1500)는 해당 사용자단말의 계정에 대한 사용자식별정보를 상기 원장기록정보에 추가하여 블록체인 네트워크(3000)의 분산원장에 상기 추가된 원장기록정보를 기록하도록 요청(S23)한다. 구체적으로 소유권판매부(1500)는 소유권판매요청정보에 포함된 구매자에 대한 정보에 상응하는 구매자의 사용자식별정보를 상기 원장기록정보에 추가하여 분산원장에 기록하도록 상기 블록체인 네트워크(3000)에 요청한다.

[0141] 한편, 상기 소유권판매부(1500)는 상기 구매자에 대한 정보에 매칭되는 사용자식별정보가 상기 사용자정보테이블(1016)에 저장되어 있지 않은 경우, 해당 사용자단말로 구매자에 대한 계정을 설정(회원가입)을 안내하는 별도의 메시지를 송신할 수도 있다.

[0142] 또한, 상기 블록체인 네트워크(3000)는 상기 서버시스템(1000)의 소유권판매부(1500)로부터 구매자의 사용자식별정보가 추가된 원장기록정보의 기록 요청에 따라 분산원장에 상기 원장기록정보를 기록(S24)한다. 바람직하게 상기 블록체인 네트워크(3000)에 포함된 스마트 컨트랙트에 의해 상기 요청에 따른 구매자의 사용자식별정보가 추가된 원장기록정보가 분산원장에 기록된다.

[0143] 더 구체적으로 상기 원장기록정보에 기록되어 있던 판매자의 사용자식별정보는 상기 구매자의 사용자식별정보로 변경될 수 있으나, 바람직하게는 상기 원장기록정보에 포함되는 현 소유권 항목에는 상기 구매자의 사용자식별정보가 기록되고, 상기 원장기록정보에 포함되는 소유권 이력 항목에는 상기 판매자의 사용자식별정보가 기록되어, 해당 개별제품의 소유권의 판매 혹은 이전 이력들이 지속적으로 기록될 수 있다.

[0144] 상술한 각각의 단계에서 사용하는 스마트 컨트랙트는 단일 스마트 컨트랙트로 구성되어 원장기록정보를 분산원장에 기록 혹은 분산원장에 기록된 원장기록정보의 조회에 대한 쿼리를 처리하거나, 스마트 컨트랙트는 각각의 단계별로 별도의 스마트 컨트랙트로 구성되어 각각의 스마트 컨트랙트들은 상응하는 단계에서의 요청만을 수행할 수도 있다.

[0145] 한편, 도 4에 도시된 상기 개별제품등록단계, 상기 소유권등록단계 및 상기 소유권판매단계는 후술하는 도 5 내지 도 7에서 더욱 구체적으로 설명하도록 한다.

- [0147] 도 5는 본 발명의 일 실시예에 따른 개별제품등록단계에 포함되는 세부 단계들을 개략적으로 도시한다.
- [0149] 도 5에 도시된 바와 같이, 상기 개별제품등록단계는, 상기 개별제품등록요청정보에 기초하여 개별제품식별정보 및 시리얼정보를 생성하고, 상기 개별제품식별정보를 상기 제품식별정보에 매칭하여 제품매핑테이블(1014)에 저장하는 단계(S30); 상기 서버시스템(1000)에 기저장된 초기 소유비밀번호에 기초하여 제1소유키를 도출하고, 상기 제1소유키 및 무작위로 생성된 가변키에 기초하여 고유키를 도출하는 제1키도출단계(S31); 상기 가변키를 해당 개별제품식별정보에 매칭하여 가변키테이블(1012)에 저장하고, 상기 고유키를 해당 개별제품식별정보에 매칭하여 고유키테이블(1013)에 저장하는 단계(S32); 및 상기 시리얼정보를 상기 고유키에 기초하여 암호화하고, 암호화된 시리얼정보, 상기 시리얼정보 및 개별제품식별정보를 포함하는 상기 원장기록정보를 상기 블록체인 네트워크(3000)의 분산원장에 기록하는 단계(S33);를 포함하고, 상기 식별이미지제공단계를 통해 생성되는 식별이미지는 상기 암호화된 시리얼정보를 포함한다.
- [0151] 구체적으로, 개별제품등록부(1200)는 제품 생산자의 사용자단말(2000.1)로부터 수신한 제품식별정보를 포함하는 개별제품등록요청정보에 기초하여 개별제품식별정보 및 시리얼정보를 생성하고, 생성한 개별제품식별정보 및 상기 제품식별정보를 매칭하여 제품매핑테이블(1014)에 저장하는 단계(S30)를 수행한다.
- [0152] 본 발명의 다른 실시예에서 상기 단계(S30)에서는 개별제품등록요청정보를 송신하는 사용자단말의 계정 타입이 제품 생산자에 대한 계정 타입인지 여부를 판별하고, 제품 생산자에 대한 계정 타입으로 판별된 경우에 개별제품식별정보 및 시리얼정보를 생성할 수도 있다.
- [0153] 다음으로, 초기 소유비밀번호에 기초하여 제1소유키를 도출하고, 별도의 가변키를 생성하여 제1소유키 및 가변키 사이의 연산을 수행하여 고유키를 도출하는 제1키도출단계(S31)를 수행한다. 더 구체적으로 상기 초기 소유비밀번호는 상기 개별제품등록요청정보에 포함될 수 있으나, 바람직하게는 서버시스템(1000)에 초기 소유비밀번호가 기저장되어 있어, 상기 개별제품등록부(1200)에서 자체적으로 제1소유키를 도출할 수 있다. 한편, 상기 제1소유키는 상기 초기 소유비밀번호를 해시함수에 입력하여 도출된 결과 값에 해당하고, 바람직하게는 상기 개별제품등록부(1200)는 초기 소유비밀번호를 SHA-256 알고리즘을 통해 256 비트를 갖는 제1소유키를 도출할 수 있다.
- [0154] 한편, 상기 초기 소유비밀번호, 상기 판매자의 소유비밀번호 및 상기 구매자의 소유비밀번호의 크기는 설계변경에 따라 자유롭게 변경될 수 있으나, 바람직하게는 숫자 혹은 문자를 포함하는 다섯 자리로 구성되는 문자열에 해당할 수 있다. 상기 가변키는 상기 개별제품등록부(1200)에 의해 랜덤하게 생성되나, 상기 소유키와의 연산에 의해 고유키를 도출하기 위하여 상기 소유키의 크기와 동일한 크기로 도출될 수 있다. 상기 고유키는 상기 제1소유키 및 상기 가변키를 연산하여 도출될 수 있고, 바람직하게는 상기 제1소유키 및 상기 가변키를 XOR 연산하여 상기 고유키를 도출할 수 있다.
- [0155] 상기 개별제품등록부(1200)는 상기 단계(S31)를 통해 도출된 상기 가변키를 상기 개별제품식별정보에 매칭하여 가변키테이블(1012)에 저장하고, 상기 고유키를 상기 개별제품식별정보에 매칭하여 고유키테이블(1013)에 저장하는 단계(S32)를 수행한다. 상기 단계(S32)에서는 초기 소유비밀번호에 기초하여 도출된 제1소유키는 서버시스템(1000)의 DB(1010)에 저장하지 않기 때문에 원천적으로 제1소유키의 유출을 방지할 수 있는 효과를 발휘할 수 있다.
- [0156] 다음으로, 단계 S30에서 생성된 시리얼정보를 단계 S31에서 도출한 고유키에 기초하여 암호화하고, 암호화된 시리얼정보, 상기 시리얼정보 및 개별제품식별정보를 포함하는 원장기록정보를 상기 블록체인 네트워크(3000)에 포함되는 스마트 컨트랙트로 하여금 분산원장에 기록하도록 하는 단계(S33)를 수행한다. 더 구체적으로, 상기 고유키는 상기 시리얼정보에 대하여 대칭키의 역할을 수행하여, 상기 시리얼정보는 AES 방식으로 암호화될 수 있다.
- [0157] 한편 고유키에 의해 암호화된 시리얼정보는 상기 식별이미지제공부(1300)에서 식별이미지화 되어 해당 사용자단말에 제공될 수 있다. 따라서 식별이미지는 암호화된 시리얼정보를 포함하고, 사용자단말에 구비된 촬영모듈을 통해 식별이미지를 식별하는 경우에 상기 암호화된 시리얼정보가 도출될 수 있다.
- [0158] 본 발명의 다른 실시예에서 상기 고유키테이블(1013)이 서버시스템(1000)에 포함되는 별도의 서버에 포함되고,

해당 서버가 망분리되어 서버시스템(1000)에 포함되는 타 서버와만 통신을 수행하는 경우에, 상기 시리얼정보는 상기 별도의 서버에 송신되고, 상기 별도의 서버는 상기 고유키테이블(1013)에 포함된 고유키에 기초하여 시리얼정보를 암호화하고, 암호화된 시리얼정보를 타 서버, 바람직하게는 개별제품등록부(1200)를 포함하는 타 서버로 제공할 수도 있다. 이와 같이, 고유키를 사용하는 과정들은 고유키테이블(1013)을 포함하는 별도의 서버에서 수행하도록 하여, 고유키가 유출되지 않도록 하는 효과를 발휘할 수 있다.

[0159] 상기 개별제품등록부(1200)에서 해당 개별제품에 대한 식별이미지를 생성하여 해당 제품 생산자의 사용자단말(2000.1)로 제공하는 것으로 개별제품의 등록이 정상적으로 이루어졌음을 의미할 수 있으나, 본 발명의 또 다른 실시예에서 상기 개별제품등록부(1200)는 개별제품이 정상적으로 등록되었음을 포함하는 메시지를 추가적으로 생성하여, 해당 제품 생산자의 사용자단말(2000.1)에 제공할 수도 있다.

[0161] 도 6은 본 발명의 일 실시예에 따른 소유권등록단계에 포함되는 세부 단계들을 개략적으로 도시한다.

[0163] 도 6에 도시된 바와 같이, 상기 소유권등록단계는, 상기 블록체인 네트워크(3000)에 포함된 스마트 컨트랙트로 하여금 상기 소유권등록요청정보에 포함된 암호화된 시리얼정보와 동일한 값을 포함하는 원장기록정보에 사용자식별정보가 포함되어있는지 여부를 판별하도록 하고, 사용자식별정보가 포함되어있지 않은 경우에, 상기 스마트 컨트랙트로 하여금 상기 판매자에 해당하는 사용자식별정보를 상기 원장기록정보에 추가하여 상기 분산원장에 기록하도록 하고, 상기 원장기록정보에 포함된 개별제품식별정보를 송신하도록 요청하는 제1스마트컨트랙트실행단계(S40); 상기 제1스마트컨트랙트실행단계를 통해 수신한 상기 개별제품식별정보에 매칭되는 상기 고유키를 상기 고유키테이블(1013)에서 도출하고, 상기 소유권등록요청정보에 포함된 판매자 소유비밀번호에 기초하여 제2소유키를 도출하는 단계(S41); 및 상기 고유키 및 상기 제2소유키에 기초하여 별도의 가변키를 생성하고, 상기 가변키테이블(1012)에 저장된 가변키를 상기 별도의 가변키로 갱신하는 제1가변키갱신단계(S42);를 포함한다.

[0165] 구체적으로, 소유권등록부(1400)는 판매자의 사용자단말(2000.2)로부터 수신한 소유권등록요청정보에 기초하여 스마트 컨트랙트로 하여금 분산원장에 해당 판매자에 대한 사용자식별정보를 상기 원장기록정보에 추가하여 기록하도록 요청하는 제1스마트컨트랙트실행단계(S40)를 수행한다.

[0166] 더 구체적으로, 상기 소유권등록요청정보는 판매자의 사용자단말(2000.2)에서 식별이미지를 식별하여 도출된 해당 개별제품의 암호화된 시리얼정보를 포함하고, 상기 스마트 컨트랙트는 소유권등록부(1400)로부터 수신한 요청에 따라 상기 소유권등록요청정보에 포함된 암호화된 시리얼정보와 동일한 값을 포함하는 원장기록정보를 도출하고, 해당 원장기록정보에 사용자식별정보가 포함되어 있는지 여부를 판별한다. 사용자식별정보가 해당 원장기록정보에 포함되어 있는 경우, 이미 판매자 혹은 구매자에 의해 소유권이 등록된 경우에 해당하므로, 판매자의 식별정보를 해당 원장기록정보에 추가하여 분산원장에 기록하는 과정은 수행되지 않는다.

[0167] 한편, 상기 사용자식별정보가 해당 원장기록정보에 포함되어 있지 않은 경우, 스마트 컨트랙트는 판매자의 사용자식별정보를 해당 원장기록정보에 추가하여 분산원장에 기록하고, 기록이 정상적으로 수행되었다는 정보를 포함하는 소유권등록성공정보 및 해당 원장기록정보에 포함된 개별제품식별정보를 상기 소유권등록부(1400)로 송신한다.

[0168] 상기 제1스마트컨트랙트실행단계(S40)를 통해 스마트 컨트랙트로부터 개별제품식별정보를 수신한 상기 소유권등록부(1400)는 고유키테이블(1013)에서 상기 개별제품식별정보에 매칭되는 고유키를 도출하고, 상기 소유권등록요청정보에 더 포함된 판매자 소유비밀번호에 기초하여 판매자 제2소유키를 도출하는 단계(S41)를 수행한다.

[0169] 더 구체적으로, 고유키테이블(1013)에 저장된 고유키는 제2대칭키에 의해 암호화된 고유키에 해당하고, 따라서 대칭키테이블(1015)에 저장된 제2대칭키에 기초하여 암호화된 고유키를 복호화하여 고유키를 도출할 수 있다. 또한 상기 판매자 소유비밀번호는 판매자가 설정하고자 하는 소유비밀번호에 해당하고, 상기 소유비밀번호를 해시함수에 입력하여 제2소유키를 도출할 수 있다.

[0170] 마지막으로, 상기 소유권등록부(1400)는 도출된 상기 고유키 및 상기 제2소유키에 기초하여 새로운 가변키를 생성하고, 상기 가변키테이블(1012)에 저장된 가변키를 생성된 상기 새로운 가변키로 갱신하는 제1가변키갱신단계(S42)를 수행한다.

- [0171] 더 구체적으로, 별도로 생성되는 새로운 가변키는 항상 값이 고정되는 고유키 및 초기에 고유키를 생성하기 위하여 초기 소유비밀번호에 기초하여 도출된 소유키와는 상이한 값을 갖는 제2소유키를 연산하여 도출될 수 있다. 바람직하게 상기 새로운 가변키는 상기 고유키 및 상기 제2소유키를 XOR 연산하여 도출될 수 있다. 또한 새롭게 생성된 가변키는 상기 가변키테이블(1012)에 저장되어 있는 해당 개별제품식별정보에 해당하는 기존의 가변키를 대체하여 갱신될 수 있다.
- [0172] 본 발명의 다른 실시예에서는 상기 소유권등록부(1400)에서 상술한 단계(S40 내지 S42)들을 순차적으로 수행하여 소유권이 등록되는 경우, 상기 소유권등록부(1400)는 정상적으로 소유권이 등록되었음을 포함하는 메시지를 생성하여 해당 판매자의 사용자단말(2000.2)에 제공하는 단계를 추가적으로 수행할 수도 있다.
- [0173] 또한, 본 발명의 또 다른 실시예에서는 상기 고유키테이블(1013)이 서버시스템(1000)에 포함되는 별도의 서버에 포함되고 별도의 서버는 망분리 형태로 동작하는 경우에, 상기 별도의 서버는 고유키테이블(1013)에서 고유키를 도출하고, 상기 새로운 가변키를 도출하는 과정은 상기 별도의 서버에서 수행하고, 도출된 상기 새로운 가변키를 소유권등록부(1400)를 포함하는 서버시스템(1000) 내의 타 서버로 제공할 수도 있다.
- [0175] 도 7은 본 발명의 일 실시예에 따른 소유권판매단계에 포함되는 세부 단계들을 개략적으로 도시한다.
- [0177] 도 7에 도시된 바와 같이, 상기 소유권판매단계는, 상기 소유권판매요청정보에 포함된 구매자에 대한 정보에 상응하는 사용자식별정보가 존재하는지 판단하는 단계(S50); 상기 구매자에 대한 정보에 상응하는 사용자식별정보가 존재하는 경우, 상기 소유권판매요청정보에 포함된 판매자 소유비밀번호 및 구매자 소유비밀번호에 기초하여 각각 제3소유키 및 제4소유키를 도출하는 제2키도출단계(S51); 상기 블록체인 네트워크(3000)에 포함된 스마트 컨트랙트로 하여금 상기 소유권판매요청정보에 포함된 암호화된 시리얼정보와 동일한 값을 포함하는 원장기록정보를 도출하고, 해당 원장기록정보에 포함된 개별제품식별정보를 송신하도록 요청하는 제2스마트컨트랙트실행단계(S52); 상기 제2스마트컨트랙트실행단계를 통해 수신한 상기 개별제품식별정보에 매칭되는 가변키를 상기 가변키테이블(1012)에서 도출하고, 상기 제3소유키 및 상기 가변키에 기초하여 고유키를 도출하는 제3키도출단계(S53); 상기 소유권판매요청정보에 포함된 암호화된 시리얼정보, 상기 제3키도출단계를 통해 도출된 고유키, 상기 판매자에 해당하는 사용자식별정보 및 상기 구매자에 대한 사용자식별정보를 포함하는 소유권판매실행정보를 도출하는 단계(S54); 상기 스마트 컨트랙트로 하여금 상기 소유권판매실행정보에 포함된 고유키를 사용하여 상기 소유권판매실행정보에 포함된 암호화된 시리얼정보를 복호화하도록 하고, 상기 소유권판매실행정보에 포함된 암호화된 시리얼정보 및 판매자에 해당하는 사용자식별정보와 동일한 값을 포함하는 원장기록정보를 도출하고, 해당 원장기록정보에 포함된 시리얼정보 및 상기 복호된 시리얼정보가 일치하는지 판별하도록 하고, 일치하는 경우 상기 구매자에 대한 사용자식별정보를 해당 원장기록정보에 추가하여 상기 분산원장에 기록하도록 요청하는 제3스마트컨트랙트실행단계(S55); 및 상기 제3스마트컨트랙트실행단계를 통해 상기 구매자에 대한 사용자식별정보가 해당 원장기록정보에 추가되는 경우, 상기 제2키도출단계를 통해 도출된 제4소유키 및 상기 제3키도출단계를 통해 도출된 고유키에 기초하여 별도의 가변키를 생성하고, 상기 가변키테이블(1012)에 저장된 가변키를 상기 별도의 가변키로 갱신하는 제2가변키갱신단계(S56);를 포함한다.
- [0179] 구체적으로, 판매자의 사용자단말(2000.2)에서 송신하는 소유권판매요청정보는 판매자의 사용자단말(2000.2)에서 식별이미지를 식별하여 도출된 해당 개별제품에 대한 암호화된 시리얼정보, 판매자가 해당 개별제품에 대하여 소유권을 등록하는 과정에서 입력했던 판매자 소유비밀번호, 구매자가 설정하고자 하는 구매자 소유비밀번호 및 구매자에 대한 정보를 포함한다. 한편, 구매자에 대한 정보는 소유권판매부(1500)에서 구매자에 대한 사용자식별정보를 도출할 수 있도록 하는 정보에 해당하고, 상술한 사용자정보테이블(1016)에 포함되는 1 이상의 필드로 구성될 수 있다. 예를 들어, 상기 구매자에 대한 정보는 구매자가 계정을 설정(회원가입)하기 위해 입력한 이메일정보 및 생년월일정보를 포함할 수 있다.
- [0181] 상기 소유권판매부(1500)는 상기 소유권판매요청정보를 수신하고, 상기 소유권판매요청정보에 포함된 구매자에 대한 정보에 기초하여 사용자정보테이블(1016)에 상기 구매자에 대한 정보에 상응하는 사용자식별정보가 존재하는지를 판단하는 단계(S50)를 수행한다.

- [0182] 더 구체적으로 상기 단계 S50은 해당 개별제품을 구매하고자 하는 구매자에 대한 계정이 설정되었는지 판단하기 위한 단계에 해당한다. 따라서 구매자에 대한 정보에 상응하는 사용자식별정보가 상기 사용자정보테이블(1016)에 저장되어 있는지 판별하고, 사용자식별정보가 저장되어 있는 경우, 이후 단계(S51)를 수행할 수 있다.
- [0183] 한편, 구매자에 대한 사용자식별정보가 상기 사용자정보테이블(1016)에 저장되어 있지 않은 경우, 상기 소유권 판매요청정보를 송신한 사용자단말(2000.2)에 구매자의 계정 설정(회원가입)을 요청하는 메시지를 송신할 수도 있다.
- [0184] 이어서 구매자에 대한 사용자식별정보가 존재하는 경우, 상기 소유권판매부(1500)는 상기 소유권판매요청정보에 포함된 판매자 소유비밀번호에 기초하여 제3소유키를 도출하고, 마찬가지로 상기 소유권판매요청정보에 포함된 구매자 소유비밀번호에 기초하여 제4소유키를 도출하는 제2키도출단계(S51)를 수행한다.
- [0185] 더 구체적으로, 상기 제3소유키는 상술한 소유권등록부(1400)에서 수행하는 단계 S41에 의해 도출되는 제2소유키와 동일한 값에 해당될 수 있다. 한편, 상기 제3소유키 및 상기 제4소유키는 각각 해시함수에 상기 판매자 소유비밀번호를 입력으로 하여 도출된 값 및 상기 구매자 소유비밀번호를 입력으로 하여 도출된 값에 해당될 수 있다.
- [0186] 다음으로, 상기 소유권판매부(1500)는 상기 블록체인 네트워크(3000)에 포함되는 스마트 컨트랙트로 하여금 상기 소유권판매요청정보에 포함된 암호화된 시리얼정보와 동일한 값을 포함하는 원장기록정보를 도출하고, 해당 원장기록정보에 포함된 개별제품식별정보를 송신하도록 요청하는 제2스마트컨트랙트실행단계(S52)를 수행한다.
- [0187] 본 발명의 다른 실시예에서는 상기 제2스마트컨트랙트실행단계(S52)는 원장기록정보에 별도의 기록을 추가하거나 혹은 수정하도록 하는 것이 아니라, 원장기록정보에 기록된 특정 정보를 요청하는 과정에 해당하므로, 스마트 컨트랙트는 블록체인 네트워크(3000)의 분산원장에 기록된 원장기록정보를 조회하지 않고, 상기 스마트 컨트랙트에 포함되는 DB(1010)에 저장된 상태정보에 기초하여 해당 개별제품식별정보를 도출하여 상기 소유권판매부(1500)로 송신할 수도 있다.
- [0188] 상기 제2스마트컨트랙트실행단계(S52)를 통해 스마트 컨트랙트로부터 개별제품식별정보를 수신한 상기 소유권판매부(1500)는 가변키테이블(1012)에서 상기 개별제품식별정보에 매칭되는 가변키를 도출하고, 상기 제2키도출단계(S51)에서 도출된 상기 제3소유키 및 도출된 상기 가변키에 기초하여 고유키를 도출하는 제3키도출단계(S53)를 수행한다.
- [0189] 더 구체적으로, 상기 가변키테이블(1012)에 저장된 가변키는 제1대칭키에 의해 암호화된 가변키에 해당할 수 있고, 따라서 상기 대칭키테이블(1015)에 저장된 제1대칭키에 기초하여 암호화된 가변키를 복호화하는 것으로 상기 가변키를 도출할 수 있다. 또한 상기 고유키는 상기 가변키 및 상기 제3소유키를 연산하여 도출될 수 있으며, 바람직하게 상기 고유키는 상기 가변키 및 상기 제3소유키를 XOR 연산하여 도출된 값에 해당할 수 있다.
- [0190] 한편, 상기 소유권판매부(1500)는 소유권판매요청정보에 포함된 암호화된 시리얼정보, 상기 제3키도출단계(S53)에서 도출된 고유키, 판매자의 사용자식별정보 및 상기 단계 S50을 통해 도출된 구매자의 사용자식별정보를 포함하는 소유권판매실행정보를 도출하는 단계(S54)를 수행한다.
- [0191] 더 구체적으로, 상기 판매자의 사용자식별정보는 상기 소유권판매요청정보에 더 포함되는 판매자에 대한 정보에 기초하여 도출될 수 있으나, 바람직하게는 상기 소유권판매요청정보를 송신하는 판매자의 사용자단말(2000.2)은 서버시스템(1000)에 세션방식으로 접속되어 있으므로, 해당 판매자의 사용자단말(2000.2)로부터 소유권판매요청정보를 수신하는 경우, 자동적으로 판매자의 사용자식별정보를 도출하여 상기 소유권판매실행정보에 포함될 수 있다.
- [0192] 다음으로, 상기 제3스마트컨트랙트실행단계(S55)는 스마트 컨트랙트로 하여금 상기 단계(S54)에서 도출된 소유권판매실행정보에 포함된 암호화된 시리얼정보 및 고유키에 기초하여 암호화된 시리얼정보를 복호화하고, 암호화된 시리얼정보와 동일한 값을 포함하는 원장기록정보를 도출하여, 해당 원장기록정보에 포함된 시리얼정보가 복호화된 시리얼정보와의 동일여부 및 해당 원장기록정보에 포함된 사용자식별정보와 상기 소유권판매실행정보에 포함된 판매자의 사용자식별정보의 동일여부를 판단하도록 하여, 모두 동일한 경우에 해당 원장기록정보에 구매자의 사용자식별정보를 추가하여 분산원장에 기록하도록 한다.
- [0193] 더 구체적으로, 원장기록정보에 포함된 사용자식별정보와 상기 소유권판매실행정보에 포함된 판매자의 사용자식별정보의 동일여부는, 해당 원장기록정보에 포함되는 현 소유권 항목에 기록된 사용자식별정보 및 상기 판매자

의 식별정보의 동일여부를 판단한다. 따라서, 해당 과정을 통해 해당 개별제품에 대한 현재 소유권을 갖고 있는 사용자식별정보와 소유권을 판매하고자 하는 판매자의 사용자식별정보가 일치하는지 판별할 수 있으므로, 소유권을 갖고 있지 않은 판매자에 의해 해당 개별제품이 판매되는 것을 방지할 수 있는 효과를 발휘할 수 있다.

- [0194] 한편, 복호화된 시리얼정보 및 판매자의 사용자식별정보가 모두 동일한 경우, 스마트 컨트랙트는 구매자의 사용자식별정보를 해당 원장기록정보에 추가하여 분산원장에 기록하고, 기록이 정상적으로 수행되었다는 정보를 포함하는 소유권판매성공정보 및 해당 원장기록정보에 포함된 개별제품식별정보를 상기 소유권판매부(1500)로 송신할 수도 있다.
- [0195] 마지막으로, 상기 소유권판매부(1500)는 상기 제3스마트컨트랙트실행단계(S55)를 통해 스마트 컨트랙트로부터 상기 소유권판매성공정보 및 상기 개별제품식별정보를 수신하는 경우, 상기 제2키도출단계(S51)를 통해 도출된 제4소유키 및 상기 제3키도출단계(S53)를 통해 도출된 고유키에 기초하여 새로운 가변키를 생성하고, 상기 제3스마트컨트랙트실행단계(S55)를 통해 수신한 상기 개별제품식별정보에 매칭되는 가변키를 상기 가변키데이터베이스(1012)에서 도출하여, 상기 새로운 가변키로 갱신하는 제2가변키갱신단계(S56)를 수행한다.
- [0196] 더 구체적으로, 별도로 생성되는 새로운 가변키는 항상 값이 고정되는 고유키 및 구매자의 소유비밀번호에 기초하여 도출된 제4소유키를 연산하여 도출될 수 있다. 바람직하게 상기 새로운 가변키는 상기 고유키 및 상기 제4소유키를 XOR 연산하여 도출될 수 있다.
- [0197] 본 발명의 다른 실시예에서는 소유권판매부(1500)에서 상술한 단계(S50 내지 S56)들이 순차적으로 진행되어 소유권이 판매되는 경우, 상기 소유권판매부(1500)는 소유권 판매가 정상적으로 이루어졌음을 포함하는 메시지를 생성하여 해당 판매자의 사용자단말(2000.2)에 제공하는 단계를 추가적으로 수행할 수도 있다.
- [0198] 상술한 소유권판매부(1500)에서 수행하는 소유권판매단계는 개별제품을 판매하는 판매자 및 해당 개별제품을 구매하고자 하는 구매자 사이의 거래를 위하여 수행되는 것에 한정되지 않고, 개별제품을 구매한 구매자 및 해당 제품을 중고 구매하고자 하는 별도의 구매자 사이의 중고거래를 하는데 있어서도 수행될 수 있다.
- [0200] 도 8은 본 발명의 일 실시예에 따른 블록체인 네트워크(3000)에서 저장되는 블록들의 연결 구조를 개략적으로 도시한다.
- [0201] 도 8에 도시된 바와 같이, 블록체인 네트워크(3000)에서의 저장 단위인 블록(4000.1, 4000.2 및 4000.3)은 서로 연결되어 블록체인을 구성할 수 있다. 상기 블록(4000.1, 4000.2 및 4000.3)은 블록헤더 및 트랜잭션으로 구성될 수 있다. 블록헤더는 이전 블록헤더의 해시값, Nonce값 및 트랜잭션 그룹(머클트리)의 해시값을 포함할 수 있다. 상기 Nonce값은 블록체인 네트워크(3000)에 포함되는 노드(3000.1 내지 3000.N)가 블록(4000.1, 4000.2 및 4000.3)을 생성하기 위해 변경하는 값으로서, 블록헤더의 해시값이 사전에 설정된 난이도값 보다 작게 나온 경우, 해당 블록헤더에 대한 해시값이 결정될 수 있다. 상기 트랜잭션 그룹(머클트리)의 해시값은 1 이상의 트랜잭션에 포함된 데이터들의 Root 해시값을 의미할 수 있다.
- [0202] 도 8에서 도시된 바와 같이, 블록 #15의 블록헤더의 해시값을 도출하기 위해서 블록 #14의 블록헤더의 해시값을 입력값으로 사용하므로, 블록 #14 및 블록 #15가 연결될 수 있다. 또한 블록헤더의 해시값을 도출하는 데 있어서, 1 이상의 트랜잭션들을 대표하는 해시값인 트랜잭션 그룹(머클트리)의 해시값을 추가적인 입력값으로 사용하기 때문에, 트랜잭션에 대해 위변조가 발생하는 경우, 트랜잭션 그룹의 해시값이 변경되므로, 위변조를 방지할 수 있다. 이러한 방식으로 이웃하는 블록(4000.1, 4000.2 및 4000.3)들은 서로 연결될 수 있으며, 블록(4000.1, 4000.2 및 4000.3) 내에서의 트랜잭션 정보가 무결성 있게 저장될 수 있다.
- [0203] 블록(4000.1, 4000.2 및 4000.3)의 트랜잭션은 수행된 트랜잭션들 중에서 블록(4000.1, 4000.2 및 4000.3)에 포함된 트랜잭션들로서, 해당 트랜잭션이 블록(4000.1, 4000.2 및 4000.3) 내에 포함된 경우, 해당 트랜잭션과 관련된 동작이 블록체인 네트워크(3000)에서 수행될 수 있다.
- [0204] 도 8에 도시된 트랜잭션의 A, B, C, D, E 및 F는 상술한 사용자단말의 사용자에게 대한 사용자식별정보와 대응될 수 있다. 또한, 트랜잭션의 Contract #1 및 Contract #2는 각각의 개별제품에 대한 스마트 컨트랙트를 의미할 수 있다.
- [0205] 도시된 블록 #14에서의 트랜잭션은, A에서 B로 60포인트를 전송하여 제품을 구매하는 트랜잭션(Tx 1) 및 C에 의해 Contract #1이 생성되거나, 수행되는 트랜잭션(Tx 2)를 포함할 수 있다. 한편, 도 8에 도시되지는 않았지만

상술한 원장기록정보 또한 블록의 트랜잭션에 기록될 수도 있다.

[0206] 한편, 본 발명의 다른 실시예에서는, 블록(4000.1, 4000.2 및 4000.3)의 블록헤더는 부모 블록(이전 블록)의 해시값(ParentHash), 현재 블록의 잉클블록(블록의 난이도가 상대적으로 낮아 블록으로 채택되지 못한 블록)들의 해시값(UncleHash), 마이닝 후 해당 트랜잭션의 수수료를 받을 어카운트 주소(Coinbase), 어카운트의 상태정보가 모여있는 머클 패트리시아 트리의 루트 노드 해시값(Root), 블록의 모든 트랜잭션에 대한 머클트리의 루트노드 해시값(TxHash), 블록내 모든 트랜잭션에 대한 리시트들의 머클트리의 루트노드 해시값(ReceiptHash), 로그 정보를 사용하는데 사용하는 32바이트 블룸필터 정보(Bloom), 이전블록의 난이도와 타임스탬프로 계산되는 블록 난이도(Difficulty), 현재 블록번호(Num), 블록당 지급가능한 최대 가스(트랜잭션/스마트 컨트랙트를 처리하는데 사용되는 비용(토큰)의 개념)의 총합(GasLimit), 블록내 트랜잭션에 사용된 가스의 총합(GasUsed), 블록의 최초 생성시간(Time), 블록의 기타정보(Extra) 및/또는 작업증명에서 해시값을 계산하는데 충분한 계산횟수를 보장하기 위해 사용하는 값(MixDigest, Nonce)을 포함할 수도 있다.

[0208] 도 9는 본 발명의 일 실시예에 따른 사용자단말에 디스플레이되는 화면들을 개략적으로 도시한다.

[0209] 도 9의 (A) 내지 (C)에 도시된 각각의 도면은 서버시스템(1000)에 접속하기 위하여 사용자단말(2000)에 디스플레이되는 화면에 해당하고, 각각의 화면은 상기 사용자단말(2000)에 구비된 브라우저에서 구현되는 웹페이지 혹은 어플리케이션 상에서 디스플레이 될 수 있다.

[0210] 도 9의 (A)는 사용자단말(2000)에서 상기 웹페이지에 접속하거나 혹은 상기 어플리케이션을 실행하였을 때 초기에 표시되는 초기화면레이어(L1)에 해당한다. 상기 초기화면레이어(L1)는 사용자의 선택입력에 따라 상기 서버시스템(1000)에서 제공하는 복수의 기능을 호출할 수 있다. 한편, 복수의 기능 가운데 필수적으로 로그인을 필요로 하지 않는 기능에 대해서는 바로 해당 기능을 호출하여 제공하고, 로그인을 필수적으로 필요로 하는 기능 혹은 사용자가 로그인에 대한 선택입력을 하는 경우에 후술하는 도 9의 (B)에 도시된 로그인레이어(L2)가 표시될 수 있다.

[0211] 도 9의 (B)는 사용자단말(2000)에서 상기 초기화면레이어(L1)에서 사용자가 입력한 특정 기능에 대한 선택입력을 수신하는 경우에 표시되는 로그인레이어(L2)에 해당한다. 상기 로그인레이어(L2)를 통해 제품 생산자, 판매자 혹은 구매자 등과 같이 상기 사용자단말(2000)의 사용자는 자신의 계정의 아이디 혹은 이메일 및 계정비밀번호를 입력하여 상기 서버시스템(1000)에 접속할 수 있다.

[0212] 한편, 도 9의 (B)의 '회원가입' 항목을 선택하는 경우, 사용자단말(2000)은 회원가입에 필요한 정보들을 입력받는 별도의 레이어를 디스플레이하고, 상기 별도의 레이어를 통해 사용자는 회원가입에 필요한 정보, 구체적으로는 상술한 사용자정보테이블(1016)에 포함되는 각각의 필드에 해당하는 정보들을 입력할 수 있다. 바람직하게는 상기 사용자정보테이블(1016)에 포함되는 각각의 필드 가운데 사용자식별정보에 해당하는 필드를 제외한 모든 필드를 상기 별도의 레이어를 통해 입력 받고, 회원가입이 수행되는 경우 서버시스템(1000)에서 사용자식별정보를 자체적으로 도출하고, 입력받은 정보에 매칭하여 상기 사용자정보테이블(1016)에 저장할 수 있다.

[0213] 도 9의 (C)는 로그인레이어(L2)를 통해 접속하는 경우에 사용자단말(2000)에 디스플레이되는 메인레이어(L3)에 해당한다. 상기 메인레이어(L3)에는 상기 웹페이지 혹은 상기 어플리케이션에서 제공하는 복수의 기능들을 호출할 수 있는 '전체메뉴'에 대한 엘리먼트를 포함하고, 사용자단말(2000)에 구비된 촬영모듈을 구동하여 식별이미지를 인식할 수 있는 식별이미지레이어(L3)를 디스플레이하기 위한 식별이미지엘리먼트(E1)를 더 포함하여, 사용자가 상기 식별이미지엘리먼트(E1)를 선택 입력하는 경우, 식별이미지를 식별하기 위한 별도의 레이어가 디스플레이 될 수 있다.

[0214] 한편, 상기 메인레이어(L3)은 소유명품목록에 대한 엘리먼트(E2) 및 소유명품이전에 대한 엘리먼트(E3)를 더 포함한다. 상기 소유 명품목록에 대한 엘리먼트(E2)에 대해 사용자가 선택 입력하는 경우, 상술한 소유현황제공부(1600)가 수행되어 해당 사용자가 소유권을 갖고 있는 1 이상의 개별제품에 대한 정보가 표시되는 별도의 레이어가 디스플레이 된다. 또한, 상기 소유명품이전에 대한 엘리먼트(E3)에 대해 사용자가 선택 입력하는 경우, 상술한 소유권판매부(1500)가 수행되어 타 구매자에게 해당 개별제품의 소유권을 판매, 이전하기 위한 별도의 레이어가 디스플레이 된다.

[0216] 도 10은 본 발명의 일 실시예에 따른 소유권판매부의 동작에 따른 사용자단말에 디스플레이되는 화면들을 개략

적으로 도시한다.

- [0217] 도 10에 도시된 도면들은 상술한 도 9의 (C)에 도시된 상기 소유명품이전에 대한 엘리먼트(E3)에 대해 사용자가 선택 입력하는 경우, 디스플레이되는 화면들에 해당한다.
- [0218] 도 10의 (A)는 상기 소유명품이전에 대한 엘리먼트(E3)를 사용자가 선택 입력하는 경우, 최초로 디스플레이되는 소유권판매 식별이미지레이어(L4)를 도시한다. 상기 소유권판매 식별이미지레이어(L4)에는 식별이미지인식엘리먼트(E4)를 포함하고, 상기 식별이미지인식엘리먼트(E4) 내에 식별이미지가 촬영되는 경우에 해당 식별이미지를 인식할 수 있다. 상기 식별이미지인식엘리먼트(E4)는 사용자가 용이하게 상기 식별이미지인식엘리먼트(E4) 내에 인식하고자 하는 식별이미지가 들어오도록 촬영하기 위하여 상기 식별이미지인식엘리먼트(E4) 및 그 주변의 영역간의 불투명도 혹은 명도 등을 상이하게 하여 상기 식별이미지인식엘리먼트(E4)가 시각적으로 강조되도록 구성될 수 있고, 또는 상기 식별이미지인식엘리먼트(E4)의 외곽선을 강조하는 것으로 사용자가 용이하게 촬영할 수 있도록 할 수 있다. 한편, 상기 소유권판매 식별이미지레이어(L4)를 통해 식별이미지를 식별하는 경우, 소유권을 판매하고자 하는 개별제품에 대한 소유비밀번호를 입력하기 위한 소유권판매 소유비밀번호레이어(L5)가 표시될 수 있다.
- [0219] 도 10의 (B)는 판매하고자 하는 개별제품에 대한 식별이미지를 인식한 이후에 디스플레이되는 소유권판매 소유비밀번호레이어(L5)를 도시한다. 상기 소유권판매 소유비밀번호레이어(L5)는 해당 개별제품에 대해 소유권을 갖고 있는 판매자 혹은 구매자가 설정한 소유비밀번호를 입력할 수 있도록 0 내지 9까지 표시된 키패드 엘리먼트가 구비되어 사용자가 자신이 설정한 소유비밀번호를 입력할 수 있다.
- [0220] 한편, 본 발명의 다른 실시예에서는 상기 소유비밀번호는 숫자 및 문자의 조합으로 구성될 수 있고, 이와 같은 경우 상기 소유권판매 소유비밀번호레이어(L5)는 숫자 및 문자를 표시하는 키패드 엘리먼트가 구비될 수 있다.
- [0221] 도 10의 (C)는 상기 소유권판매 소유비밀번호레이어(L5)에서 사용자가 소유비밀번호를 입력한 이후에 표시되는 구매자정보 입력레이어(L6)를 도시한다. 상기 구매자정보 입력레이어(L6)에는 해당 개별제품을 구매하고자 하는 사용자의 이메일정보 및 생년월일정보를 입력받는 영역을 포함한다. 상기 영역을 통해 입력받는 이메일정보 및 생년월일정보는 상기 서버시스템(1000)에 포함된 사용자정보테이블(1960)에 포함된 사용자식별정보를 도출하기 위한 요소로 사용된다.
- [0222] 한편, 상기 구매자정보 입력레이어(L6)에 포함된 영역은 상기 이메일정보 및 생년월일정보를 입력받는 것으로 한정되지 아니하고, 사용자가 계정을 설정하기 위해 입력하는 1 이상의 정보를 입력받을 수 있다. 바람직하게는 상기 사용자정보테이블(1960)에 포함되는 1 이상의 필드들을 입력받을 수 있다. 또한, 사용자가 기보유한 타 서비스 계정, 예를 들어, 구글 혹은 페이스북에 대한 계정을 갖고 있는 경우, 타 계정을 통해 서버시스템에 접속할 수 있는 계정이 생성될 수 있고, 이와 같은 경우 상기 구매자정보 입력레이어(L6)에 직접 구매자에 대한 정보를 입력하지 않고, 타 계정을 통해 구매자에 대한 정보를 제공받을 수 있는 엘리먼트를 포함할 수 있다.
- [0223] 도 10의 (D)는 해당 개별제품을 구매하고자 하는 사용자가 설정하고자 하는 소유비밀번호를 입력받는 소유권설정 소유비밀번호레이어(L7)를 도시한다. 상기 소유권설정 소유비밀번호레이어(L7)는 상기 소유권판매 소유비밀번호레이어(L6)과 동일하게 소유비밀번호를 입력받을 수 있도록 키패드 엘리먼트를 포함할 수 있다.
- [0224] 도 10의 (E)는 상술한 도 10의 (A) 내지 (D)에 도시된 각각의 레이어를 통해 정상적으로 정보를 수신하는 경우, 최종적으로 해당 개별제품의 판매를 판매자 및 구매자가 승인하는 판매승인레이어(L8)를 도시한다. 상기 판매승인레이어(L8)에는 판매하고자 하는 개별제품의 제품정보가 도시될 수 있고, 상기 판매승인레이어(L8)는 판매동의레이어(L9)를 더 포함한다.
- [0225] 상기 판매동의레이어(L9)는 해당 개별제품에 대한 판매자(위임자) 및 구매자(소유자) 양 측의 거래에 대한 동의를 입력받는 레이어에 해당한다. 따라서 상기 판매동의레이어(L9)의 판매자(위임자) 및 구매자(소유자) 각각에 해당하는 영역에 대해 각각의 판매자(위임자) 및 구매자(소유자)가 거래 동의에 대한 서명을 입력할 수 있다.
- [0226] 상기 판매동의레이어(L9)를 통해 각각의 판매자(위임자) 및 구매자(소유자)가 거래 동의에 대한 서명을 입력한 후에 판매자 혹은 구매자가 상기 판매승인레이어(L8)에 표시되는 거래 동의에 대한 체크박스를 선택하여 '승인하기'에 대한 영역을 선택하는 경우, 해당 개별제품에 대한 판매가 완료되어, 완료되었음을 표시하는 별도의 메시지가 사용자단말(2000)에 표시될 수도 있다.

[0228] **2. 제품의 소유권을 인증하기 위한 방법**

[0229] 상술한 바와 같이 제품의 소유권이 구매자로 이전되어 판매가 완료된 이후에, 구매자에 의해 제품의 소유권을 인증하기 위한 방법이 수행될 수 있고, 추가적으로 식별이미지 및 소유비밀번호를 복구할 수 있는 방법이 수행될 수 있다. 이하에서는, 제품의 소유권을 인증하기 위한 방법에 대하여 상세하게 설명하도록 한다.

[0231] 도 11은 본 발명의 일 실시예에 따른 소유권인증단계에 포함되는 세부 단계들을 개략적으로 도시한다.

[0233] 도 11에 도시된 바와 같이, 1 이상의 사용자단말(2000) 및 블록체인 네트워크(3000)와 통신을 수행하는 1 이상의 프로세서 및 1 이상의 메모리를 포함하는 서버시스템(1000)에서 수행되는 제품의 소유권을 인증하기 위한 방법으로서, 사용자단말(2000)에서 개별제품에 대한 식별이미지를 인식하여 도출한 암호화된 시리얼정보 및 소유비밀번호를 포함하는 소유권인증요청정보를 상기 사용자단말(2000)로부터 수신하는 단계(S60); 상기 블록체인 네트워크(3000)에 포함된 스마트 컨트랙트로 하여금 상기 소유권인증요청정보에 포함된 암호화된 시리얼정보와 동일한 값을 포함하는 원장기록정보를 도출하도록 하고, 해당 원장기록정보에 포함된 개별제품식별정보를 송신하도록 요청하는 단계(S61); 상기 소유권인증요청정보에 포함된 소유비밀번호에 기초하여 인증소유키를 도출하고, 상기 스마트 컨트랙트로부터 수신한 개별제품식별정보에 매칭되는 인증가변키를 로드하여, 상기 인증소유키 및 상기 인증가변키에 기초하여 인증고유키를 생성하는 단계(S62); 상기 스마트 컨트랙트로 하여금 상기 암호화된 시리얼정보를 상기 인증고유키로 복호화하도록 하고, 상기 암호화된 시리얼정보와 동일한 값을 포함하는 원장기록정보를 도출하도록 하고, 해당 원장기록정보에 포함된 시리얼정보 및 상기 복호화된 시리얼정보의 일치 여부를 판별하도록 하여, 일치하는 경우에 인증성공정보를 송신하도록 요청하는 단계(S63); 및 상기 인증성공정보를 수신하는 경우, 상기 개별제품식별정보에 기초하여 인증세부정보를 도출하고, 상기 인증세부정보를 해당 사용자단말(2000)에 제공하는 인증세부정보제공단계(S64);를 포함한다.

[0235] 구체적으로, 소유권인증부(1600)에서 수행하는 소유권인증단계는 개별제품에 대한 소유권을 갖고 있는 주체에 의해 수행될 수 있다. 예를 들어, 소유권을 갖고 있는 주체는 해당 개별제품을 판매하는 판매자 혹은 판매자로부터 해당 개별제품을 구매하거나, 이전에 해당 개별제품에 대해 소유권을 갖고 있는 다른 구매자로부터 해당 개별제품을 중고 구매한 구매자가 해당될 수 있다. 따라서, 상기 소유권인증부(1600)는 개별제품에 대해 소유권을 갖고 있는 주체가 사용하는 사용자단말(2000)로부터 암호화된 시리얼정보 및 소유비밀번호를 포함하는 소유권인증요청정보를 수신하는 단계(S60)를 수행한다.

[0236] 더 구체적으로 상기 단계 S60에서 수신하는 상기 소유권인증요청정보에 포함된 암호화된 시리얼정보는 해당 개별제품에 대한 식별이미지를 사용자단말(2000)에 구비된 촬영모듈을 통해 식별한 정보에 해당하고, 소유비밀번호는 제품의 소유권을 구매할 때 설정한 소정의 크기를 갖는 비밀번호에 해당한다.

[0237] 소유권인증요청정보를 수신한 소유권인증부(1600)는 블록체인 네트워크(3000)에 포함된 스마트 컨트랙트로 하여금 상기 소유권인증요청정보에 포함된 암호화된 시리얼정보와 동일한 값을 포함하는 원장기록정보를 도출하도록 하고, 도출된 상기 원장기록정보에 포함된 해당 개별제품의 개별제품식별정보를 상기 소유권인증요청정보를 송신한 사용자단말(2000)로 송신하도록 요청하는 단계(S61)를 수행한다.

[0238] 본 발명의 다른 실시예에서 상기 단계(S61)는 스마트 컨트랙트로 하여금 원장기록정보에 별도의 기록을 추가하거나 혹은 수정하도록 하는 것이 아니라, 원장기록정보에 기록된 특정 정보에 해당하는 개별제품식별정보를 요청하는 과정에 해당하므로, 스마트 컨트랙트는 블록체인 네트워크(3000)의 분산원장에 기록된 원장기록정보를 조회하지 않고, 상기 스마트 컨트랙트에 포함되는 DB(1010)에 저장된 상태정보에 기초하여 해당 개별제품식별정보를 도출하여 상기 소유권인증부(1600)로 송신할 수도 있다.

[0239] 이후, 상기 소유권인증부(1600)는 소유권인증요청정보에 포함된 소유비밀번호에 기초하여 인증소유키를 도출하고, 가변키테이블(1012)에서 상기 스마트 컨트랙트로부터 수신한 개별제품식별정보에 매칭되는 인증가변키를 상기 가변키테이블(1012)에서 도출하고, 상기 인증소유키 및 상기 인증가변키에 기초하여 인증고유키를 생성하는 단계(S62)를 수행한다.

[0240] 더 구체적으로, 상기 인증소유키는 상기 소유권인증요청정보에 포함된 소유비밀번호를 해시함수에 입력하여 얻은 결과값에 해당할 수 있다. 또한 상기 가변키테이블(1012)에 저장된 인증가변키는 제1대칭키에 의해 암호화된

인증가변키에 해당할 수 있고, 따라서 상기 대칭키테이블(1015)에 저장된 제1대칭키에 기초하여 암호화된 인증가변키를 복호화하는 것으로 상기 인증가변키를 로드할 수 있다. 또한 상기 인증고유키는 상기 인증소유키 및 상기 인증가변키를 연산하여 도출될 수 있으며, 바람직하게 상기 인증고유키는 상기 인증소유키 및 상기 인증가변키를 XOR 연산하여 도출된 값에 해당할 수 있다.

[0241] 한편, 상술한 인증소유키, 인증가변키 및 인증고유키는 소유권인증단계를 용이하게 설명하기 위하여 사용된 용어에 해당할 뿐 인증이라는 별도의 의미에 한정되지 않는다. 따라서 상기 인증소유키는 상술한 소유비밀번호에 기초하여 도출된 소유키에 해당되고, 상기 인증가변키는 가변키테이블(1012)에 개별제품식별정보에 매칭되어 저장된 가변키에 해당되며, 마찬가지로 상기 인증고유키는 소유키 및 가변키를 연산하여 도출된 고유키에 해당될 수 있다.

[0242] 다음으로, 소유권인증부(1600)는 상기 단계 S60을 통해 수신한 암호화된 시리얼정보 및 상기 단계 S62를 통해 생성된 인증고유키를 포함하는 소유권인증수행요청정보를 상기 스마트 컨트랙트로 송신하여, 상기 스마트 컨트랙트로 하여금 상기 소유권인증수행요청정보에 포함된 암호화된 시리얼정보와 동일한 값을 갖는 원장기록정보를 도출하고, 상기 암호화된 시리얼정보를 소유권인증수행요청정보에 포함된 인증고유키로 복호화하여, 복호화된 시리얼정보 및 도출한 상기 원장기록정보에 포함된 시리얼정보의 일치 여부를 판별하도록 하여, 일치하는 경우에 인증성공정보를 송신하도록 요청하는 단계(S63)를 수행한다.

[0243] 본 발명의 다른 실시예에서는 상기 단계 S63에서 상기 소유권인증수행요청정보에 포함된 암호화된 시리얼정보와 동일한 값을 갖는 원장기록정보를 도출하는 과정은 상기 단계 S61에서 동일하게 수행하여 도출된 원장기록정보에 따라 생략될 수도 있다.

[0244] 마지막으로 상기 스마트 컨트랙트로부터 인증성공정보를 수신한 상기 소유권인증부(1600)는 단계 S61 혹은 상기 인증성공정보에 포함된 개별제품식별정보에 기초하여 인증세부정보를 도출하고, 상기 인증세부정보를 해당 사용자단말(2000)에 제공하는 인증세부정보제공단계(S64)를 수행한다.

[0246] 상기 인증세부정보제공단계(S64)를 수행하기 위하여, 상기 서버시스템(1000)은, 제품식별정보에 매칭된 상기 제품정보를 포함하는 제품정보테이블(1011); 및 상기 개별제품식별정보에 매칭된 상기 제품식별정보를 포함하는 제품매핑테이블(1014);을 포함하고, 상기 인증세부정보제공단계는(S64), 상기 제품매핑테이블(1014)에서 상기 개별제품식별정보에 매칭된 제품식별정보를 도출하고, 상기 제품정보테이블(1011)에서 도출된 제품식별정보에 매칭된 제품정보를 도출하는 단계;를 포함한다.

[0248] 더 구체적으로, 상기 인증세부정보는 상기 개별제품식별정보에 상응하는 제품정보를 포함하고, 이를 위하여 상기 제품매핑테이블(1014)에서 해당 개별제품식별정보에 매칭되는 제품식별정보를 도출하고, 상기 제품정보테이블(1011)에서 도출된 상기 제품식별정보에 매칭되는 제품정보를 도출하여 상기 인증세부정보에 포함될 수 있다. 한편, 상기 인증세부정보는 해당 사용자단말(2000)에 디스플레이되어 인증된 개별제품의 제품정보 및 인증이 정상적으로 완료되었다는 메시지가 표시될 수 있다.

[0249] 상기와 같이 소유권인증부(1600)를 통해 사용자는 소유권을 갖고 있는 개별제품에 대한 식별이미지를 인식하고, 소유비밀번호를 입력하는 것으로 해당 개별제품의 소유권에 대한 인증을 수행할 수 있고, 따라서 해당 개별제품의 소유권에 대한 인증여부를 타인에게 용이하게 제시할 수 있는 효과를 발휘할 수 있다.

[0251] 도 12는 본 발명의 일 실시예에 따른 소유현황제공단계에 포함되는 세부 단계들을 개략적으로 도시한다.

[0253] 도 12에 도시된 바와 같이, 상기 제품의 소유권을 인증하기 위한 방법은 소유현황제공단계를 더 포함하고, 상기 소유현황제공단계는, 사용자단말(2000)로부터 소유현황제공요청정보를 수신하는 단계(S70); 상기 스마트 컨트랙트로 하여금 해당 사용자단말(2000)에 상응하는 사용자식별정보를 포함하는 1 이상의 원장기록정보를 도출하도록 하고, 상기 1 이상의 원장기록정보에 각각 포함된 1 이상의 개별제품식별정보를 송신하도록 요청하는 단계(S71); 및 상기 1 이상의 개별제품식별정보에 매칭되는 각각의 제품정보를 포함하는 소유현황정보를 도출하여 해당 사용자단말(2000)에 제공하는 단계(S72);를 포함한다.

- [0255] 구체적으로, 소유현황제공부(1700)는 사용자단말(2000)로부터 소유현황제공요청정보를 수신하는 단계(S70)를 수행한다. 상기 단계 S70에서 소유현황제공요청정보에는 사용자단말(2000)에 해당하는 사용자식별정보를 포함할 수 있으나, 바람직하게는 서버시스템(1000) 및 사용자단말(2000)은 세션방식으로 접속되어 있으므로, 상기 소유현황제공요청정보에 사용자식별정보가 포함되어 있지 않더라도, 상기 서버시스템(1000)에서 자동적으로 해당 사용자식별정보를 도출할 수 있다.
- [0256] 다음으로, 소유현황제공부(1700)는 스마트 컨트랙트로 하여금 상기 사용자단말(2000)에 해당하는 사용자식별정보를 포함하는 1 이상의 원장기록정보를 도출하도록 하고, 도출된 1 이상의 원장기록정보에 포함된 각각의 개별제품식별정보를 송신하도록 요청하는 단계(S71)를 수행한다.
- [0257] 더 구체적으로, 상기 원장기록정보에는 현재 소유권을 갖고 있는 사용자의 사용자식별정보 및 이전에 소유권을 갖고 있었던 1 이상의 사용자의 사용자식별정보 즉 소유권이력정보를 포함할 수 있다. 따라서, 상기 단계 S71에서는 스마트 컨트랙트로 하여금 상기 사용자단말(2000)에 해당하는 사용자식별정보가 원장기록정보의 현재 소유권을 갖고 있는 사용자의 사용자식별정보 혹은 소유권이력정보에 포함되어 있는지 확인하여, 상기 사용자식별정보를 포함하는 1 이상의 원장기록정보를 도출하도록 할 수 있다.
- [0258] 바람직하게는 상기 소유현황제공요청정보는 사용자의 선택에 따라 현재 소유권을 갖고 있는 개별제품에 대한 현황을 요청하는 정보 혹은 과거에 소유권을 가졌던 개별제품까지 포함하는 현황을 요청하는 정보를 포함할 수 있고, 이와 같은 정보를 포함한 소유현황제공요청정보에 따라 스마트 컨트랙트는 1 이상의 원장기록정보를 도출할 수도 있다.
- [0260] 본 발명의 다른 실시예에서 상기 단계 S71에서는 상술한 소유자매핑테이블(1017)을 사용하여 스마트 컨트랙트로 하여금 해당 사용자에 대한 사용자식별정보를 포함하는 1 이상의 원장기록정보를 도출할 수도 있다.
- [0261] 구체적으로, 상기 소유자매핑테이블(1017)에는 사용자가 소유하고 있거나 혹은 소유했던 개별제품의 암호화된 시리얼정보 및 해당 사용자의 사용자식별정보가 매칭되어 저장되어 있다. 따라서, 상기 단계 S71에서는 상기 단계 S70을 통해 수신 혹은 도출된 사용자식별정보에 매핑되는 1 이상의 암호화된 시리얼정보를 상기 소유자매핑테이블(1017)에 기초하여 도출하고, 도출된 1 이상의 암호화된 시리얼정보를 스마트 컨트랙트로 송신하여, 스마트 컨트랙트로 하여금 수신한 1 이상의 암호화된 시리얼정보에 각각 상응하는 원장기록정보를 도출하도록 할 수도 있다.
- [0262] 이와 같이, 원장기록정보가 암호화된 시리얼정보를 키값으로 하는 경우에 상술한 바와 같이 소유현황제공단계에서 상기 소유자매핑테이블(1017)을 사용하는 경우 스마트 컨트랙트에서의 원장기록정보를 도출하기까지의 시간을 줄일 수 있는 효과를 발휘할 수 있다.
- [0264] 한편, 사용자단말(2000)에 상응하는 사용자식별정보가 포함된 1 이상의 원장기록정보에 각각 포함된 개별제품식별정보를 수신한 소유현황제공부(1700)는 1 이상의 개별제품식별정보에 상응하는 제품정보를 포함하는 소유현황정보를 도출하여 해당 사용자단말(2000)에 제공하는 단계(S72)를 수행한다.
- [0265] 더 구체적으로, 상기 소유현황제공부(1700)는 상기 1 이상의 개별제품식별정보에 상응하는 제품정보를 도출하기 위하여 서버시스템(1000)에 포함된 제품매핑테이블(1014)을 통해 각각의 개별제품식별정보에 매칭되는 제품식별정보를 도출하고, 제품정보테이블(1011)을 통해 도출된 각각의 제품식별정보에 매칭되는 제품정보를 도출할 수 있다.
- [0266] 한편, 개별제품식별정보는 각각의 개별제품별로 할당되는 고유한 값에 해당하고, 제품정보는 개별제품에 대한 제품명정보, 제조사정보, 제품설명정보 또는 제품이미지정보와 같이 제품군에 대한 정보에 해당하므로, 복수의 개별제품식별정보가 하나의 제품정보에 해당하는 것과 같이 1 이상의 개별제품식별정보와 1 이상의 제품정보는 일대일 대응이 되지 않을 수도 있다.
- [0267] 또한, 사용자단말(2000)에 제공되는 소유현황정보는 해당 사용자단말(2000)에 디스플레이될 수 있으며, 다양한 방식으로 디스플레이될 수 있다. 예를 들어, 최초 디스플레이되는 경우에는 리스트 형태로 소유권을 갖고 있는 개별제품에 대한 간략한 정보가 표시되고, 특정 개별제품을 사용자가 선택하는 경우에, 해당 개별제품에 대한

상세한 정보가 디스플레이될 수도 있다.

[0269] 도 13은 본 발명의 일 실시예에 따른 식별이미지복원단계에 포함되는 세부 단계들을 개략적으로 도시한다.

[0271] 도 13에 도시된 바와 같이, 상기 제품의 소유권을 인증하기 위한 방법은 식별이미지복원단계를 더 포함하고, 상기 식별이미지복원단계는, 사용자단말(2000)로부터 복원하고자 하는 식별이미지에 상응하는 개별제품식별정보 및 소유비밀번호를 포함하는 식별이미지복원요청정보를 수신하는 단계(S80); 상기 식별이미지복원요청정보에 포함된 소유비밀번호에 기초하여 복원소유키를 도출하고, 상기 식별이미지복원요청정보에 포함된 개별제품식별정보에 매칭되는 복원가변키를 로드하여, 상기 복원소유키 및 상기 복원가변키에 기초하여 복원고유키를 도출하는 단계(S81); 상기 스마트 컨트랙트로 하여금 상기 식별이미지복원요청정보에 포함된 개별제품식별정보와 동일한 값을 포함하는 원장기록정보를 도출하도록 하고, 해당 원장기록정보에 포함된 암호화된 시리얼정보를 상기 복원고유키로 복호화하고, 상기 복호화된 시리얼정보 및 해당 원장기록정보에 포함된 시리얼정보의 일치 여부를 판별하도록 하여, 일치하는 경우에 상기 암호화된 시리얼정보를 송신하도록 요청하는 단계(S82); 및 수신한 상기 암호화된 시리얼정보에 기초하여 식별이미지를 생성하고, 생성된 식별이미지를 해당 사용자단말(2000)로 송신하는 단계(S83);를 포함한다.

[0273] 구체적으로, 식별이미지복원부(1800)는 사용자단말(2000)로부터 복원하고자 하는 식별이미지에 상응하는 식별이미지복원요청정보를 수신하는 단계(S80)를 수행한다. 상기 단계 S80에서 상기 식별이미지복원요청정보는 복원하고자 하는 식별이미지에 상응하는 개별제품에 대한 개별제품식별정보 및 소유비밀번호를 포함한다.

[0274] 더 구체적으로, 상기 개별제품식별정보는 사용자가 직접 입력할 수도 있으나, 사용자가 복원하고자 하는 개별제품에 대해 선택 입력하는 것으로 상기 개별제품식별정보가 상기 식별이미지복원요청정보에 포함될 수 있다. 바람직하게는 상술한 소유현황제공부(1700)를 통해 사용자단말(2000)에 디스플레이되는 해당 사용자가 소유권을 보유한 1 이상의 개별제품 가운데 식별이미지를 복원하고자 하는 특정 개별제품을 선택하고, 식별이미지의 복원을 요청하는 선택입력에 따라 개별제품식별정보가 상기 식별이미지복원요청정보에 포함될 수 있다.

[0275] 다음으로, 상기 식별이미지복원부(1800)는 상기 식별이미지복원요청정보에 포함된 소유비밀번호에 기초하여 복원소유키를 도출하고, 가변키테이블(1012)에서 상기 식별이미지복원요청정보에 포함된 개별제품식별정보에 매칭되는 복원가변키를 로드하여, 상기 복원소유키 및 상기 복원가변키에 기초하여 복원고유키를 도출하는 단계(S81)를 수행한다.

[0276] 더 구체적으로, 상기 복원소유키는 상기 식별이미지복원요청정보에 포함된 소유비밀번호를 해시함수에 입력하여 얻은 결과값에 해당할 수 있다. 또한 상기 가변키테이블(1012)에 저장된 복원가변키는 제1대칭키에 의해 암호화된 복원가변키에 해당할 수 있고, 따라서 상기 대칭키테이블(1015)에 저장된 제1대칭키에 기초하여 암호화된 복원가변키를 복호화하는 것으로 복원가변키를 로드할 수 있다. 또한, 상기 복원고유키는 상기 복원소유키 및 상기 복원가변키를 연산하여 도출될 수 있으며, 바람직하게 상기 복원고유키는 상기 복원소유키 및 상기 복원가변키를 XOR 연산하여 도출된 값에 해당할 수 있다.

[0277] 한편, 상술한 복원소유키, 복원가변키 및 복원고유키는 식별이미지복원단계를 용이하게 설명하기 위하여 사용된 용어에 해당할 뿐 복원이라는 별도의 의미에 한정되지 않는다. 따라서 상기 복원소유키는 상술한 소유비밀번호에 기초하여 도출된 소유키에 해당되고, 상기 복원가변키는 가변키테이블(1012)에 개별제품식별정보에 매칭되어 저장된 가변키에 해당되며, 마찬가지로 상기 복원고유키는 소유키 및 가변키를 연산하여 도출된 고유키에 해당될 수 있다.

[0278] 다음으로, 상기 식별이미지복원부(1800)는 상기 단계 S80을 통해 수신한 개별제품식별정보 및 상기 단계 S81에서 도출한 복원고유키를 포함하는 식별이미지복원수행요청정보를 상기 스마트 컨트랙트로 송신하여, 스마트 컨트랙트로 하여금 상기 식별이미지복원수행요청정보에 포함된 개별제품식별정보와 동일한 값을 갖는 원장기록정보를 도출하고, 도출된 상기 원장기록정보에 포함된 암호화된 시리얼정보를 상기 식별이미지복원수행요청정보에 포함된 복원고유키로 복호화하여, 복호화된 시리얼정보 및 상기 원장기록정보에 포함된 시리얼정보의 일치 여부를 판별하도록 하여, 일치하는 경우에 상기 원장기록정보에 포함된 암호화된 시리얼정보를 송신하도록 요청하는 단계(S82)를 수행한다.

- [0279] 본 발명의 다른 실시예에서는, 상기 식별이미지복원수행요청정보는 식별이미지의 복원을 요청한 사용자단말(2000)에 상응하는 사용자식별정보를 더 포함하고, 상기 식별이미지복원수행요청정보를 수신한 스마트 컨트랙트는 도출된 원장기록정보의 현재 소유권을 갖고 있는 사용자에게 대한 사용자식별정보 및 상기 식별이미지복원수행요청정보에 포함된 사용자식별정보의 일치 여부에 대한 판단을 추가적으로 수행할 수 있다.
- [0280] 따라서, 소유비밀번호를 알고 있는 것뿐만 아니라 현재 소유권을 가진 사용자의 계정으로 사용자단말(2000)에 로그인하였는지 추가적으로 확인하여 식별이미지를 복원함으로써 타인에 의해 식별이미지가 복원되는 것을 방지할 수 있는 효과를 발휘할 수 있다.
- [0281] 마지막으로 상기 스마트 컨트랙트로부터 암호화된 시리얼정보를 수신한 식별이미지복원부(1800)는 상기 암호화된 시리얼정보에 기초하여 식별이미지를 생성하고, 해당 식별이미지를 사용자단말(2000)에 송신하는 단계(S83)를 수행한다.
- [0282] 본 발명의 다른 실시예에서 상기 단계 S83에서는 식별이미지를 생성하지 않고, 상기 암호화된 시리얼정보를 사용자단말(2000)에 제공하고, 사용자단말(2000)에서 상기 암호화된 시리얼정보에 기초하여 식별이미지를 생성할 수도 있다.
- [0284] 도 14는 본 발명의 일 실시예에 따른 소유비밀번호갱신단계에 포함되는 세부 단계들을 개략적으로 도시한다.
- [0286] 도 14에 도시된 바와 같이, 상기 제품의 소유권을 인증하기 위한 방법은 소유비밀번호갱신단계를 더 포함하고, 상기 소유비밀번호갱신단계는, 사용자단말(2000)에서 갱신하고자 하는 소유비밀번호에 상응하는 식별이미지를 인식하여 도출한 암호화된 시리얼정보 및 신규 소유비밀번호를 포함하는 소유비밀번호갱신요청정보를 상기 사용자단말(2000)로부터 수신하는 단계(S90); 상기 스마트 컨트랙트로 하여금 상기 소유비밀번호갱신요청정보에 포함된 암호화된 시리얼정보와 동일한 값을 포함하는 원장기록정보를 도출하도록 하고, 해당 사용자단말(2000)에 상응하는 사용자식별정보 및 해당 원장기록정보에 포함된 사용자식별정보의 일치 여부를 판별하도록 하여, 일치하는 경우에 해당 원장기록정보에 포함된 개별제품식별정보를 송신하도록 요청하는 단계(S91); 및 상기 소유비밀번호갱신요청정보에 포함된 신규 소유비밀번호에 기초하여 신규 소유키를 도출하고, 상기 개별제품식별정보에 매칭되는 갱신고유키를 로드하여, 상기 신규 소유키 및 상기 갱신고유키에 기초하여 신규 가변키를 도출하고, 상기 신규 가변키를 상기 개별제품식별정보에 매칭하여 저장하는 단계(S92);를 포함한다.
- [0288] 구체적으로, 소유비밀번호갱신부(1900)는 사용자단말(2000)로부터 소유비밀번호를 갱신하고자 하는 개별제품에 대한 암호화된 시리얼정보 및 갱신하고자 하는 신규 소유비밀번호를 포함하는 소유비밀번호 갱신요청정보를 수신하는 단계(S90)를 수행한다.
- [0289] 더 구체적으로 상기 단계 S90에서 수신하는 상기 소유비밀번호 갱신요청정보에 포함된 암호화된 시리얼정보는 해당 개별제품에 대한 식별이미지를 사용자단말(2000)에 구비된 촬영모듈을 통해 식별한 정보에 해당하고, 신규 소유비밀번호는 해당 개별제품에 대해 사용자가 새롭게 설정하고자 하는 소유비밀번호에 해당한다.
- [0290] 소유비밀번호 갱신요청정보를 수신한 소유비밀번호갱신부(1900)는 스마트 컨트랙트로 하여금 상기 소유비밀번호 갱신요청정보에 포함된 암호화된 시리얼정보와 동일한 값을 포함하는 원장기록정보를 도출하도록 하고, 도출된 상기 원장기록정보에 포함된 현재 소유하고 있는 사용자에게 해당하는 사용자식별정보 및 상기 소유비밀번호 갱신요청정보를 송신한 사용자단말(2000)에 상응하는 사용자식별정보의 일치 여부를 판별하도록 하여, 일치하는 경우에 상기 원장기록정보에 포함된 개별제품식별정보를 송신하도록 요청하는 단계(S91)를 수행한다.
- [0291] 더 구체적으로, 상기 소유비밀번호 갱신요청정보를 송신한 사용자단말(2000)에 상응하는 사용자식별정보는 상기 소유비밀번호 갱신요청정보에 포함될 수도 있으나, 바람직하게는 상기 사용자단말(2000) 및 서버시스템(1000)은 세션방식으로 접속되므로, 상기 서버시스템(1000)에서 자동적으로 해당 사용자단말(2000)에 대한 사용자식별정보를 도출할 수도 있다.
- [0292] 마지막으로, 소유비밀번호갱신부(1900)는 상기 단계 S90에서 수신한 신규 소유비밀번호에 기초하여 신규 소유키를 도출하고, 상기 단계 S91에서 수신한 개별제품식별정보에 매칭되는 갱신고유키를 고유키테이블(1013)에서 로드한다. 이후에 신규 소유키 및 갱신고유키에 기초하여 신규 가변키를 도출하고, 가변키테이블(1012)에 상기 개

별제품식별정보에 매칭되어 저장된 가변키를 상기 신규 가변키로 갱신하여 저장하는 단계(S92)를 수행한다.

- [0293] 더 구체적으로, 상기 신규 가변키는 항상 값이 고정되는 갱신고유키 및 사용자가 입력한 신규 소유비밀번호에 기초하여 도출된 신규 소유키를 연산하여 도출될 수 있다. 바람직하게 상기 신규 가변키는 상기 갱신고유키 및 상기 신규 소유키를 XOR 연산하여 도출될 수 있다.
- [0294] 또한 도출된 신규 가변키는 서버시스템(1000)에 포함된 가변키테이블(1012)에 저장되는 것으로 상기 가변키테이블(1012)에 저장되어 있는 기존의 가변키가 신규 가변키로 갱신될 수 있다. 더 구체적으로, 상기 가변키테이블(1012)에 저장된 1 이상의 가변키는 각각의 가변키에 해당하는 개별제품식별정보와 매칭되어 있고, 도출된 신규 가변키는 상응하는 개별제품식별정보에 매칭되어 있는 기존의 가변키를 대체하여 저장될 수 있다.
- [0296] 한편, 본 발명의 다른 실시예에서 상기 서버시스템(1000)은 제1서버 및 상기 제1서버만을 대상으로 통신을 수행하는 제2서버를 포함하여, 상기 제2서버는 상기 서버시스템(1000)의 외부와는 통신을 수행하지 않는 망분리 형태로 운영될 수 있고, 상기 고유키테이블(1013)을 포함할 수 있다.
- [0297] 따라서, 상기 단계 S92에서 고유키테이블(1013)에 저장되어 있는 갱신고유키를 로드하는 경우, 상기 제2서버에서 해당 갱신고유키를 도출하여 상기 제1서버로 해당 갱신고유키를 제공할 수 있으므로, 항상 고정된 값을 갖는 고유키에 대한 보안을 강화할 수 있는 효과를 발휘할 수 있다.
- [0298] 또한, 본 발명의 또 다른 실시예에서는, 상기 제2서버는 갱신고유키를 도출하여 상기 제1서버로 제공하는 것이 아니라, 갱신고유키에 기초하여 신규 가변키를 생성하는 과정을 직접 수행할 수도 있다. 구체적으로, 상기 단계 S92를 수행하는 경우 상기 제2서버는 상기 제1서버로부터 신규 소유키를 제공받고, 상기 제2서버의 고유키테이블(1013)에서 갱신고유키를 도출하여, 상기 신규 소유키 및 상기 갱신고유키에 기초하여 신규 가변키를 도출할 수 있다. 이와 같이 상기 제2서버에 의해 도출된 신규 가변키는 상기 제1서버로 제공되고, 상기 제1서버에서는 가변키테이블(1012)에 상기 신규 가변키를 저장하는 것으로 단계 S92를 수행할 수도 있다.
- [0299] 이와 같은 실시예에서는 갱신고유키가 제2서버내에서만 도출되어 활용되므로, 고유키에 대한 보안을 더욱 강화할 수 있는 효과를 발휘할 수 있다.
- [0301] 또한 상술한 신규 소유키, 갱신고유키 및 신규 가변키는 소유비밀번호갱신단계를 용이하게 설명하기 위하여 사용된 용어에 해당할 뿐 신규 혹은 갱신이라는 별도의 의미에 한정되지 않는다. 따라서 상기 신규 소유키는 상술한 신규 소유비밀번호에 기초하여 도출된 소유키에 해당되고, 상기 갱신고유키는 고유키테이블(1013)에 개별제품식별정보에 매칭되어 저장된 고유키에 해당되며, 마찬가지로 상기 신규 가변키는 소유키 및 고유키를 연산하여 도출된 가변키에 해당될 수 있다.
- [0303] 도 15는 본 발명의 일 실시예에 따른 소유권인증부의 동작에 따른 사용자단말에 디스플레이되는 화면들을 개략적으로 도시한다.
- [0304] 도 15에 도시된 도면들은 상술한 도 9의 (C)에 도시된 상기 식별이미지엘리먼트(E1)에 대해 사용자가 선택 입력을 하거나, 상기 소유권인증부(1600)를 호출하는 별도의 선택 입력을 사용자단말(2000)로부터 수신하는 경우에 디스플레이되는 화면들에 해당한다.
- [0305] 도 15의 (A)는 개별제품에 대한 식별이미지를 인식하여 소유권인증요청정보에 포함되는 암호화된 시리얼정보를 도출하기 위해 사용자단말(2000)에 디스플레이되는 소유권인증 식별이미지레이어(L10)를 도시한다. 상기 소유권인증 식별이미지레이어(L10)에는 식별이미지인식엘리먼트(E5)를 포함하고, 상기 식별이미지인식엘리먼트(E5) 내에 식별이미지가 촬영되는 경우에 해당 식별이미지를 인식할 수 있다. 상기 소유권인증 식별이미지레이어(L10) 및 상기 식별이미지인식엘리먼트(E5)는 상술한 도 10의 (A)와 유사하므로, 자세한 설명은 생략하도록 한다. 한편, 상기 소유권인증 식별이미지레이어(L10)를 통해 식별이미지를 식별하는 경우, 소유권을 인증하고자 하는 개별제품에 대한 소유비밀번호를 입력하기 위한 소유권인증 소유비밀번호레이어(L11)가 표시될 수 있다.
- [0306] 도 15의 (B)는 인증하고자 하는 개별제품에 대한 식별이미지를 인식한 이후에 사용자단말(2000)에 디스플레이되는 소유권인증 소유비밀번호레이어(L11)를 도시한다. 상기 소유권인증 소유비밀번호레이어(L11)는 해당 개별제품에 대해 소유권을 갖고 있는 판매자 혹은 구매자가 설정한 소유비밀번호를 입력할 수 있도록 상기 레이어

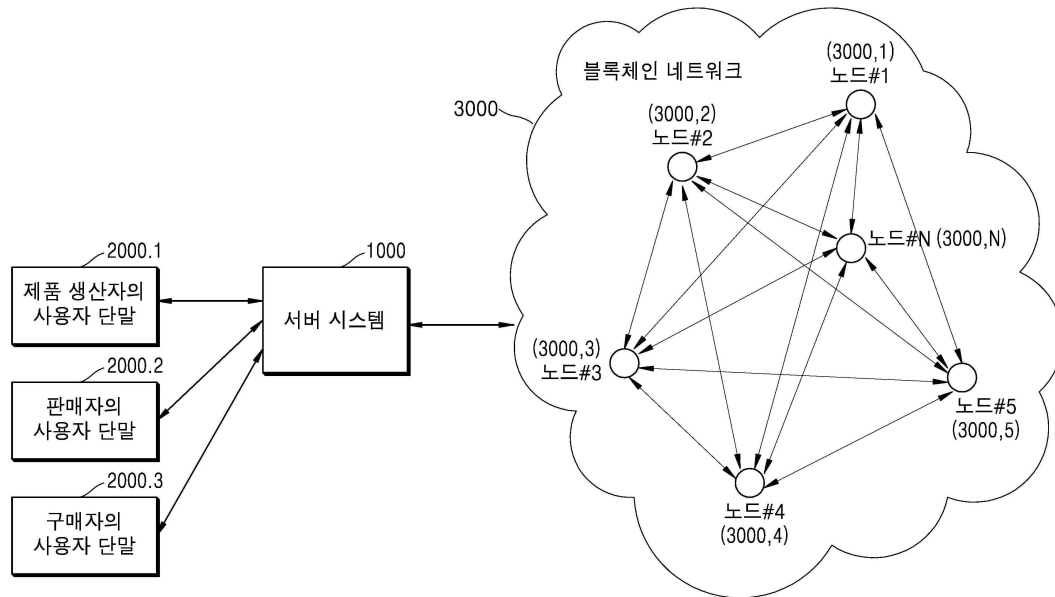
(L11)에 표시된 키패드 엘리먼트가 구비되어 사용자가 설정한 소유비밀번호를 입력할 수 있다.

- [0307] 도 15의 (C)는 식별이미지를 인식하여 도출된 암호화된 시리얼정보 및 사용자가 입력한 소유비밀번호를 포함하는 소유권인증요청정보에 기초하여 도출된 인증세부정보가 사용자단말(2000)에 디스플레이 되는 소유권인증내역레이어(L12)를 도시한다. 상기 소유권인증내역레이어(L12)에는 소유권이 정상적으로 인증되었다는 메시지를 포함하고, 인증된 개별제품에 대한 제품정보가 표시될 수 있다. 한편, 상기 소유권 인증이 정상적으로 수행되지 않는 경우, 인증에 실패하였다는 별도의 메시지가 상기 소유권인증내역레이어(L12)에 표시될 수도 있다.
- [0309] 도 16은 본 발명의 일 실시예에 따른 소유현황제공부 및 소유비밀번호갱신부의 동작에 따른 사용자단말에 디스플레이되는 화면들을 개략적으로 도시한다.
- [0310] 도 16의 (A)는 사용자단말(2000)로부터 수신한 소유현황제공요청정보에 기초하여 도출된 소유현황정보가 사용자단말(2000)에 디스플레이되는 소유현황레이어(L13)를 도시한다. 상기 소유현황레이어(L13)에는 사용자단말(2000)에 로그인된 사용자의 계정에 상응하여 소유권을 보유한 1 이상의 개별제품에 대한 정보가 디스플레이된다.
- [0311] 바람직하게 상기 소유현황레이어(L13)에는 해당 사용자가 현재 소유권을 갖고 있는 1 이상의 개별제품 및/또는 현재는 소유권을 갖고 있지 않으나, 과거에 소유권을 갖고 있었던 1 이상의 개별제품에 대한 제품정보가 디스플레이 될 수 있고, 사용자의 선택 입력에 따라 상기 소유현황레이어(L13)에 현재 소유권을 갖고 있는 1 이상의 개별제품 및/또는 과거에 소유권을 갖고 있었던 1 이상의 개별제품에 대한 제품정보가 디스플레이 될 수 있다.
- [0312] 한편, 상기 소유현황레이어(L13)에는 1 이상의 개별제품을 카테고리 혹은 브랜드별로 정렬할 수 있도록 하는 각각의 엘리먼트를 포함하고, 도 16의 (B)는 사용자가 상기 소유현황레이어(L13)에서 카테고리 별로 정렬할 수 있도록 하는 엘리먼트를 선택한 경우에 사용자단말(2000)에 디스플레이되는 소유현황레이어(L14)에 해당한다. 도 16의 (B)에 도시된 바와 같이, 카테고리 별로 정렬할 수 있도록 하는 엘리먼트를 사용자가 선택하는 경우, 상기 소유현황레이어(L14)에는 1 이상의 카테고리가 표시되고, 사용자가 특정 카테고리를 선택하는 경우 상기 소유현황레이어(L14)는 해당 카테고리에 해당하는 1 이상의 개별제품에 대한 정보를 제공할 수 있다. 한편, 도 16의 (B)에 도시되지는 않았으나 사용자가 브랜드 별로 정렬할 수 있도록 하는 엘리먼트를 선택하는 경우 상기 소유현황레이어(L14)에는 1 이상의 브랜드가 표시되고, 사용자가 특정 브랜드를 선택하는 경우 해당 브랜드에 해당하는 1 이상의 개별제품에 대한 정보를 제공할 수 있다.
- [0313] 도 16의 (C)는 상기 소유현황레이어(L13, L14)에서 사용자가 특정 개별제품을 선택하는 경우에 사용자단말(2000)에 디스플레이되는 세부소유현황레이어(L15)를 도시한다. 상기 세부소유현황레이어(L15)에는 사용자가 선택한 개별제품에 대한 제품정보가 디스플레이 되고, 해당 개별제품에 대한 소유비밀번호를 변경하기 위한 단계가 수행될 수 있도록 하는 소유비밀번호 갱신엘리먼트(E6) 및 해당 개별제품에 대한 식별이미지를 복원하기 위한 단계가 수행될 수 있도록 하는 식별이미지 복원엘리먼트(E7)를 포함한다.
- [0314] 한편, 도 16의 (D)는 상기 세부소유현황레이어(L15)에서 사용자가 소유비밀번호 갱신엘리먼트(E6)를 선택하는 경우, 소유비밀번호를 갱신하고자 하는 개별제품에 대한 식별이미지를 인식할 수 있는 비밀번호변경 식별이미지레이어(L16)를 도시한다. 상기 비밀번호변경 식별이미지레이어(L16)에는 상술한 도 10의 (A) 및 도 15의 (A)에 도시된 식별이미지인식엘리먼트(E4, E5)와 같이 식별이미지인식엘리먼트(E8)를 포함하고, 상기 식별이미지인식엘리먼트(E8) 내에 식별이미지가 촬영되는 경우에 해당 식별이미지를 인식할 수 있다. 이어서, 상기 비밀번호변경 식별이미지레이어(L16)에서 식별이미지를 인식하는 경우, 사용자단말(2000)에는 사용자가 신규 소유비밀번호를 입력할 수 있는 별도의 레이어(미도시)가 디스플레이되고, 사용자는 새로 설정하고자 하는 신규 소유비밀번호를 해당 레이어(미도시)에 입력함으로써 해당 개별제품에 대한 소유비밀번호를 변경하는 단계들이 수행될 수 있다.
- [0316] 본 발명의 일 실시예에 따르면, 제품 생산자의 사용자단말로부터 개별제품등록요청정보를 수신하여 블록체인 네트워크의 분산원장에 원장기록정보를 기록하므로, 해당 제품의 진품을 확인할 수 있는 효과를 발휘할 수 있다.
- [0317] 본 발명의 일 실시예에 따르면, 해당 제품을 구매하는 경우 구매자의 사용자식별정보가 블록체인 네트워크 상의 원장기록정보에 추가되어 기록되므로, 해당 구매자가 자신의 소유권을 확인 또는 증명할 수 있고, 이에 따라 해당 제품을 소유한 구매자의 제품에 대한 충성도를 향상시킬 수 있는 효과를 발휘할 수 있다.

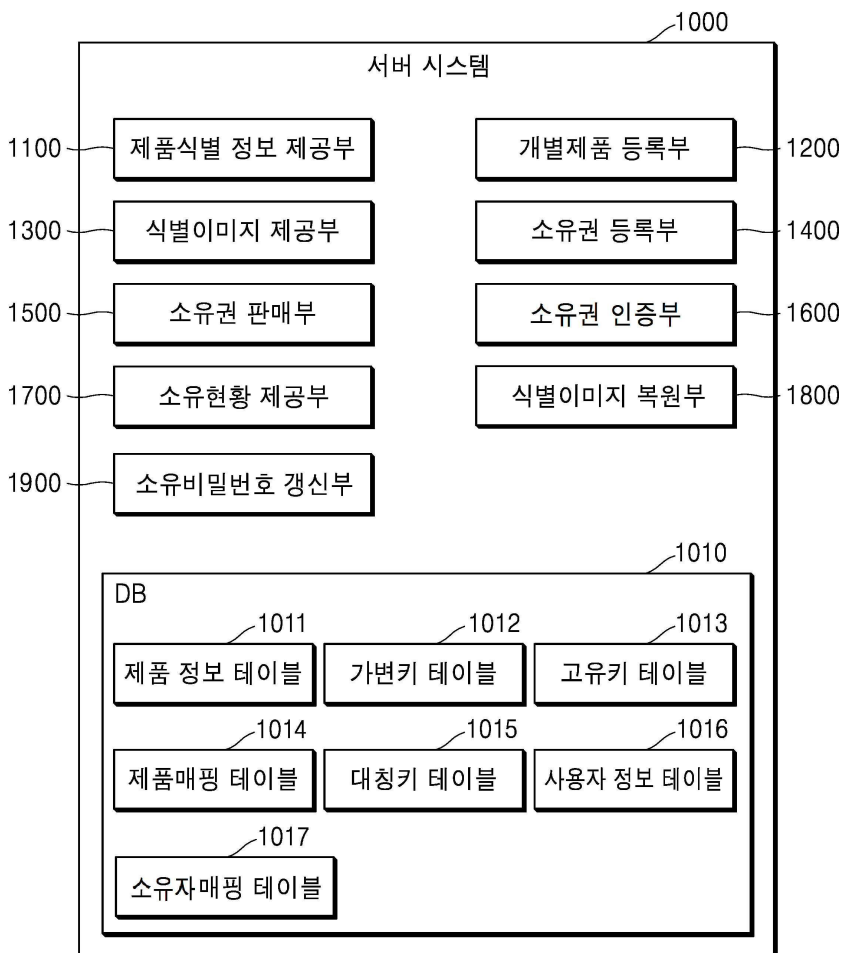
- [0318] 본 발명의 일 실시예에 따르면, 해당 제품을 구매하는 경우 구매자의 사용자식별정보가 블록체인 네트워크 상의 원장기록정보에 추가되어 기록되므로, 해당 제품을 중고거래 하는 경우에도 소유권을 용이하게 이전할 수 있고, 따라서 중고 구매자의 해당 제품에 대한 신뢰도를 향상시킬 수 있는 효과를 발휘할 수 있다.
- [0319] 본 발명의 일 실시예에 따르면, 구매자 소유비밀번호는 서버시스템에 저장되지 않으므로, 상기 서버시스템을 통해 소유권을 구매함에 있어서 보안을 향상시킬 수 있는 효과를 발휘할 수 있다.
- [0320] 본 발명의 일 실시예에 따르면, 서버시스템은 제품에 대한 식별이미지를 도출하여 사용자단말에 제공하므로, 해당 식별이미지가 복수의 장소에서 사용되거나, 해당 식별이미지에 대하여 복수의 오류가 발생하는 경우에 해당 제품에 대한 복제품 존재 여부를 판단할 수 있는 효과를 발휘할 수 있다.
- [0321] 본 발명의 일 실시예에 따르면, 진품을 가품으로 바꾸어 판매하는 경우에 진품을 본 발명의 방법으로 더 이상 판매할 수 없으므로, 바꾸어 판매하고자 하는 욕구를 감소시킬 수 있는 효과를 발휘할 수 있다.
- [0322] 본 발명의 일 실시예에 따르면, 가변키 및 고유키는 대칭키테이블에 저장된 각각의 대칭키에 의해 암호화되어 각각 가변키테이블 및 고유키테이블에 저장되므로, 상기 가변키 및 상기 고유키에 대한 보안을 강화할 수 있는 효과를 발휘할 수 있다.
- [0323] 본 발명의 일 실시예에 따르면, 소유권등록단계에서는 원장기록정보에 사용자식별정보가 포함되지 않은 경우에만 소유권등록을 수행하도록 하므로, 타 판매자의 사용자단말로부터 해당 상품에 대한 중복 등록을 방지할 수 있는 효과를 발휘할 수 있다.
- [0324] 본 발명의 일 실시예에 따르면, 제품에 대한 식별이미지가 분실 혹은 훼손되는 경우, 해당 제품에 대한 소유권을 갖고 있는 사용자의 요청에 따라 식별이미지를 복원하여 해당 사용자에게 제공하므로, 식별이미지가 분실 혹은 훼손되더라도 제품의 소유권에 대한 인증 혹은 판매를 용이하게 수행할 수 있는 효과를 발휘할 수 있다.
- [0325] 본 발명의 일 실시예에 따르면, 제품의 소유권을 갖고 있는 사용자가 소유비밀번호를 분실한 경우, 해당 사용자의 요청에 따라 새로 설정한 소유비밀번호를 제품의 소유비밀번호로 설정할 수 있으므로, 소유비밀번호를 분실하더라도 용이하게 제품의 소유권을 인증하거나 판매할 수 있는 효과를 발휘할 수 있다.
- [0327] 이상과 같이 실시예들이 비록 한정된 실시예와 도면에 의해 설명되었으나, 해당 기술분야에서 통상의 지식을 가진 자라면 상기의 기재로부터 다양한 수정 및 변형이 가능하다. 예를 들어, 설명된 기술들이 설명된 방법과 다른 순서로 수행되거나, 및/또는 설명된 시스템, 구조, 장치, 회로 등의 구성요소들이 설명된 방법과 다른 형태로 결합 또는 조합되거나, 다른 구성요소 또는 균등물에 의하여 대치되거나 치환되더라도 적절한 결과가 달성될 수 있다. 그러므로, 다른 구현들, 다른 실시예들 및 특허청구범위와 균등한 것들도 후술하는 특허청구범위의 범위에 속한다.

도면

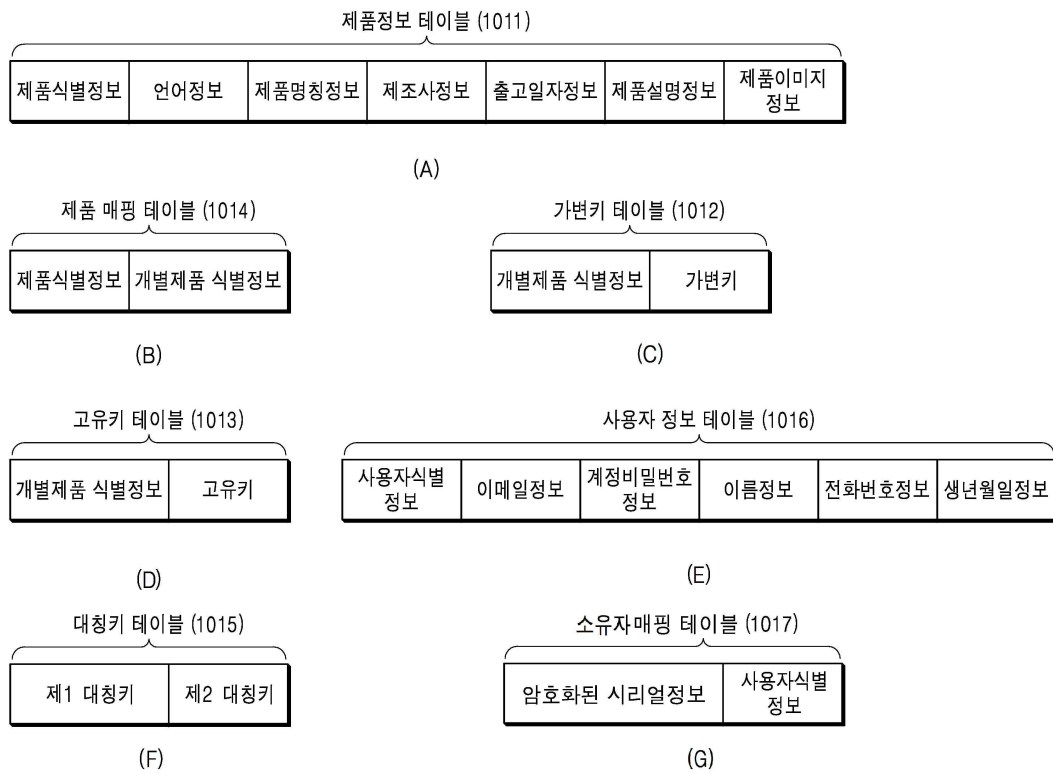
도면1



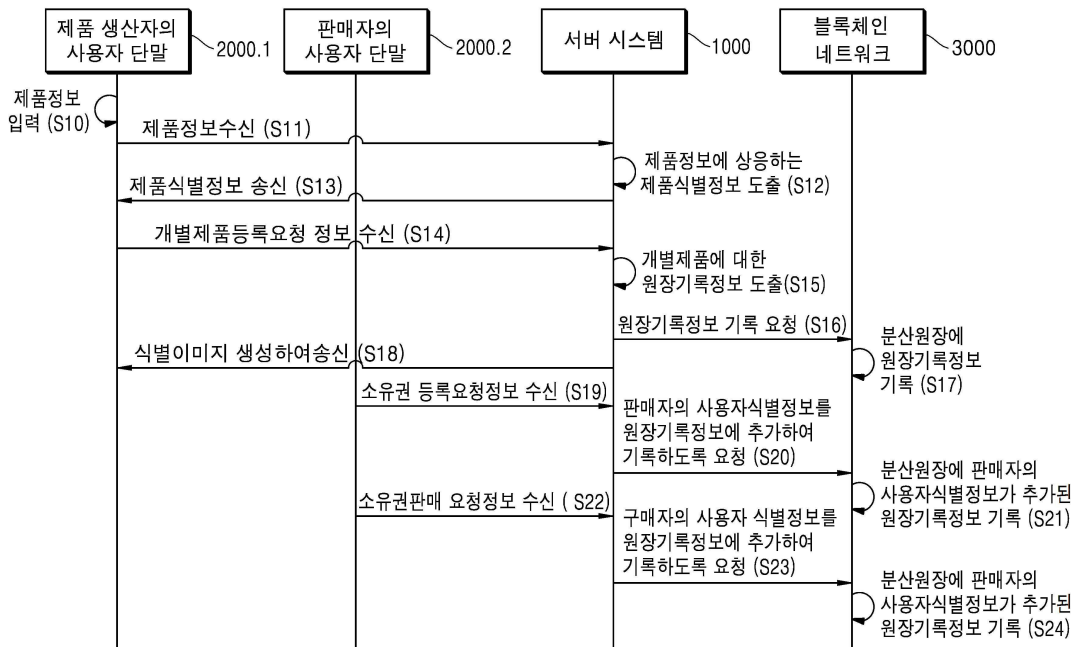
도면2



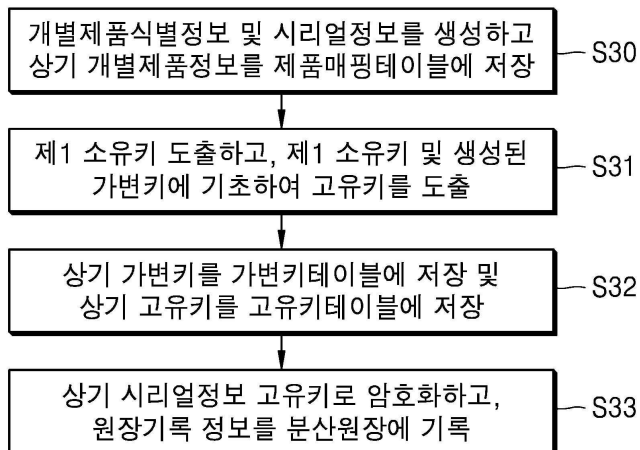
도면3



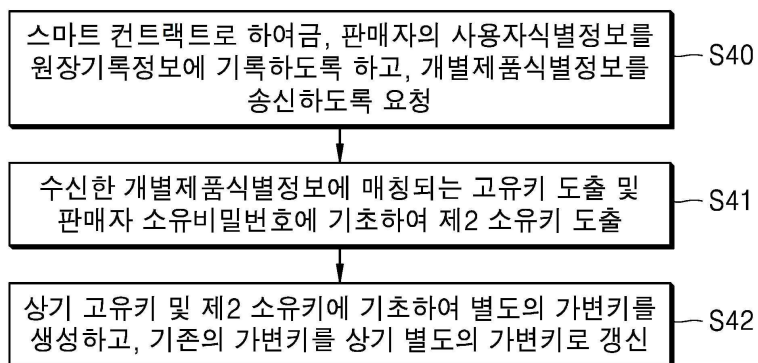
도면4



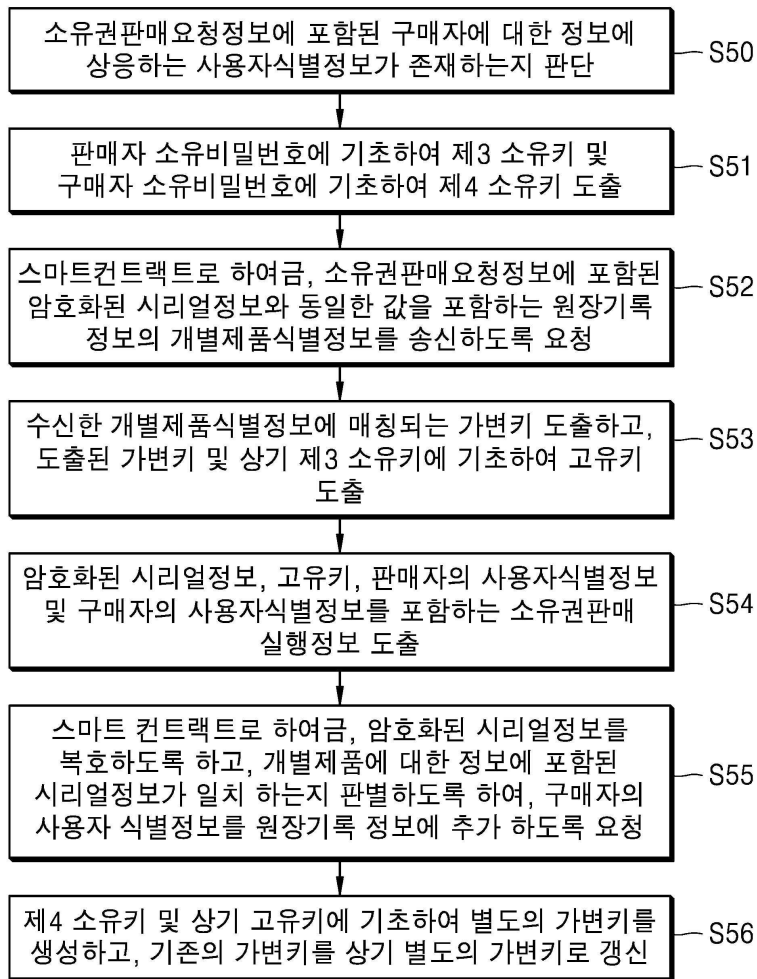
도면5



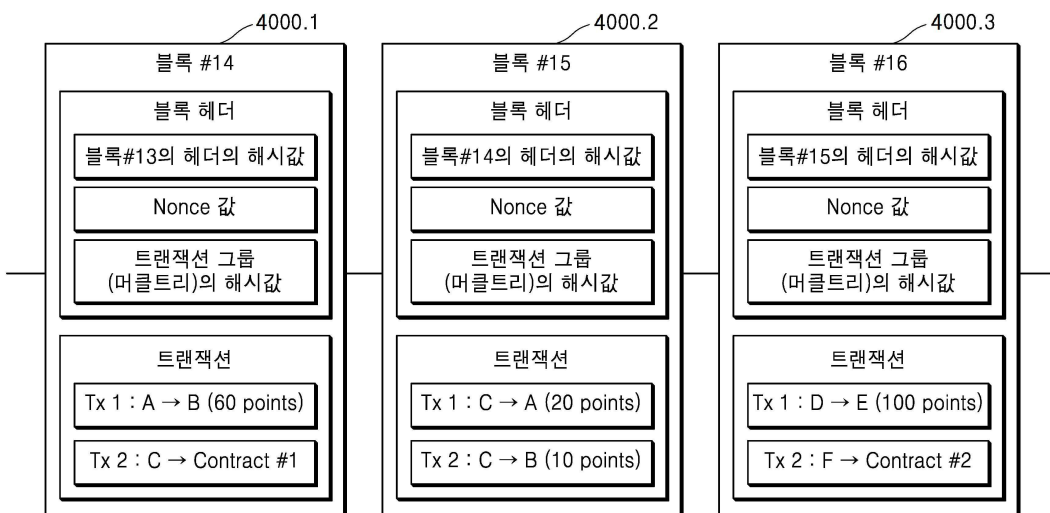
도면6



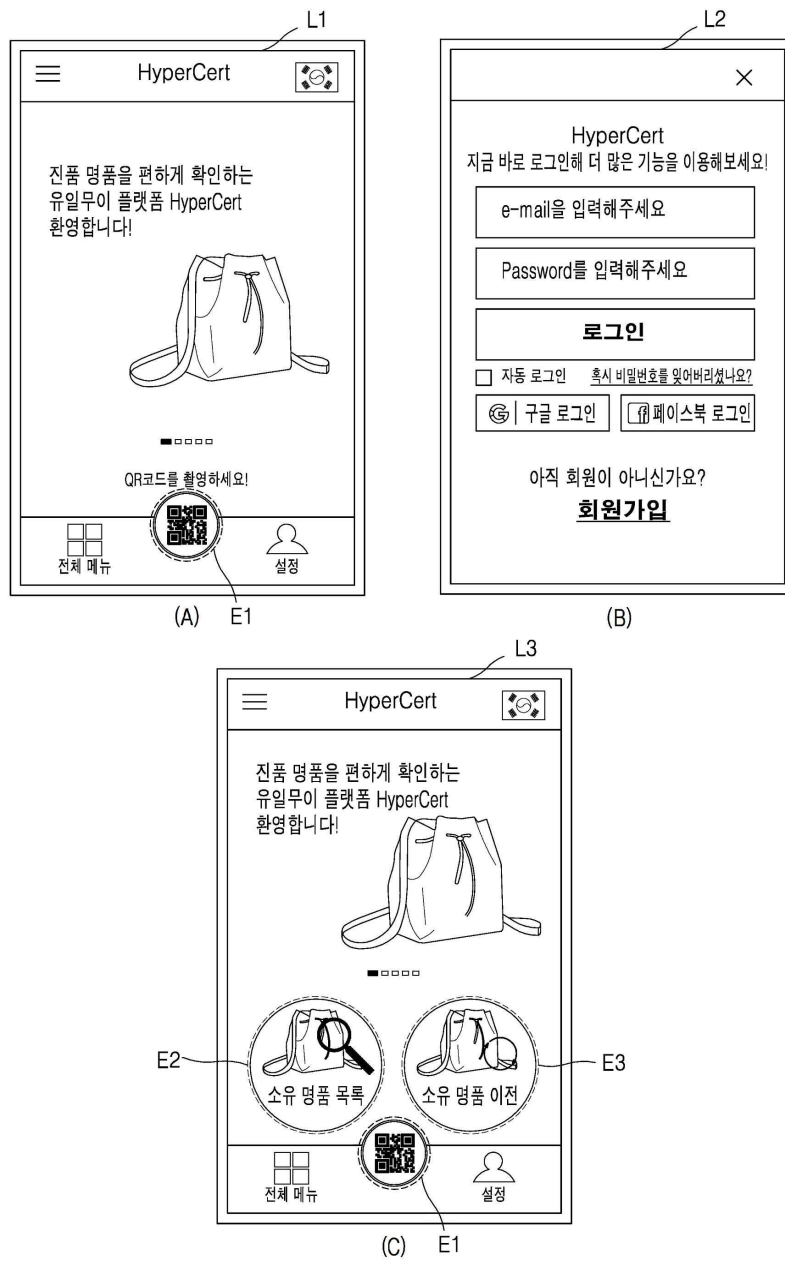
도면7



도면8



도면9



도면10

E4
L4

상품 소유권 이전



품목의 QR코드를 스캔해주세요.

L5

상품 소유권 이전

간편 패스워드를 입력해주세요.

1 3 6 4

2 5 7 9

8 0 ←

혹시 패스워드를 잊어버리셨나요?

L6

상품 소유권 이전

차기 소유자의 정보를 입력해주세요.

e-mail을 입력해주세요

생년월일 | 1996 ▼ | 06월 ▼ | 27일 ▼

위임받기

@ | 구글 계정으로 위임받기

[f] | 페이스북 계정으로 위임받기

L7

상품 소유권 이전

차기 소유자님의
간편 패스워드를 입력해주세요!

1 3 6 4

2 5 7 9

8 0 ←

L8

정품 소유권 이전

루***
ITBI 다이에그라파이트 기사이 클러치 n41664



제품정보 ■■■■■

색상	블랙
출고일	2019.01.23
제조년월	2018.10.26

위임자
 ▶

소유자

☐ 다음 사항을 확인했으며 위임에 동의합니다.

승인하기

L9

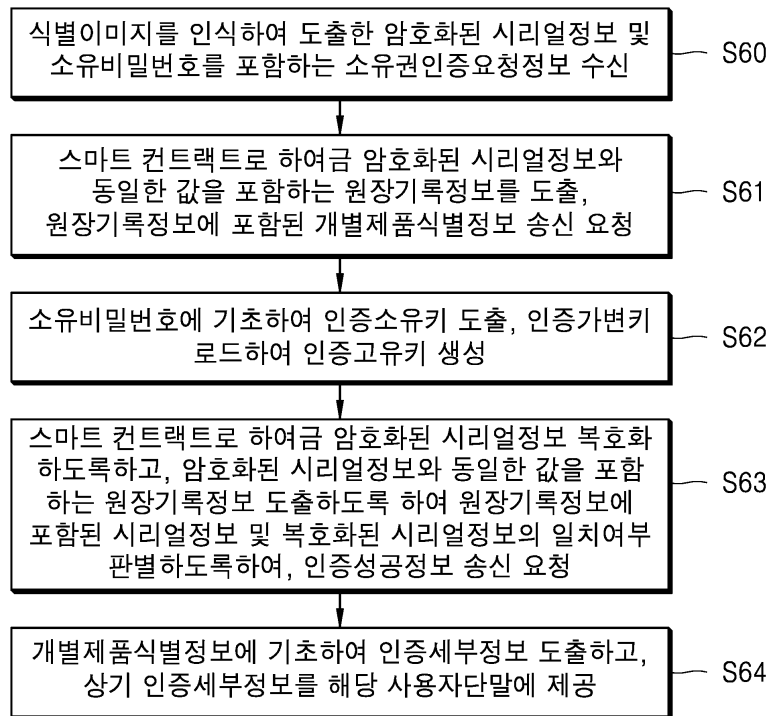
승인하기

(A)
(B)
(C)

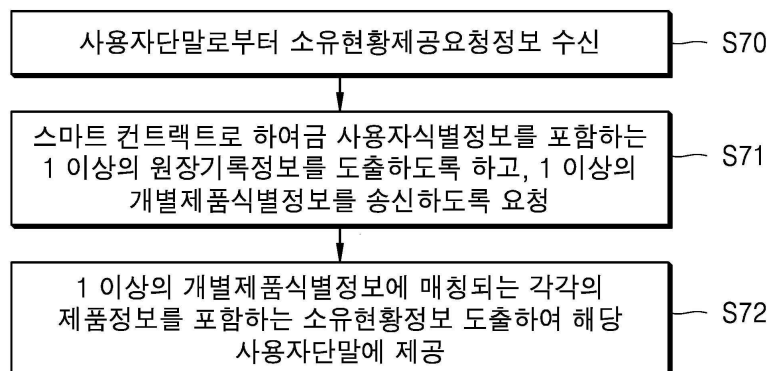
(D)
(E)

- 38 -

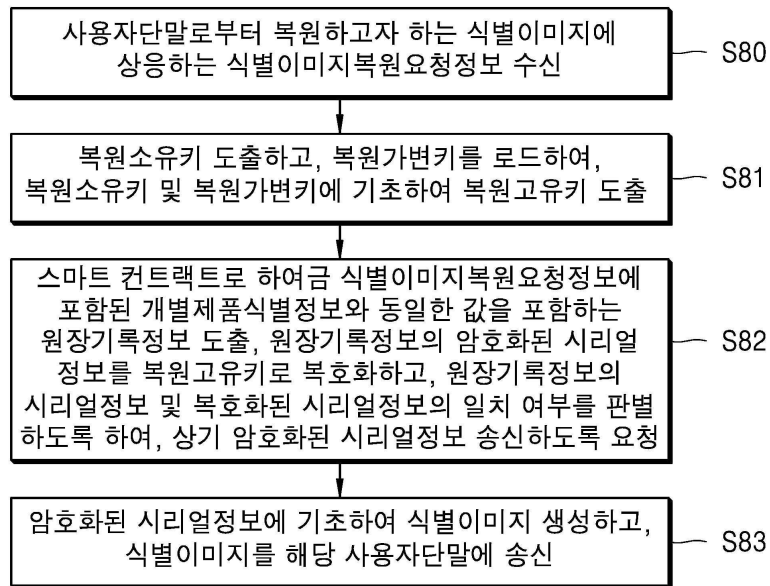
도면11



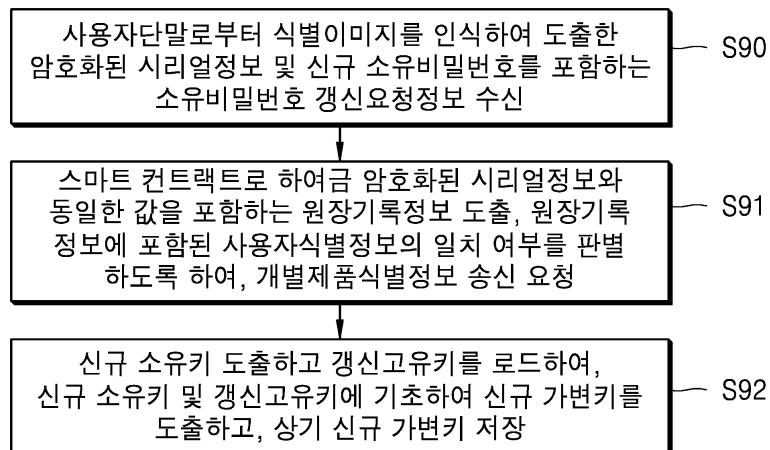
도면12



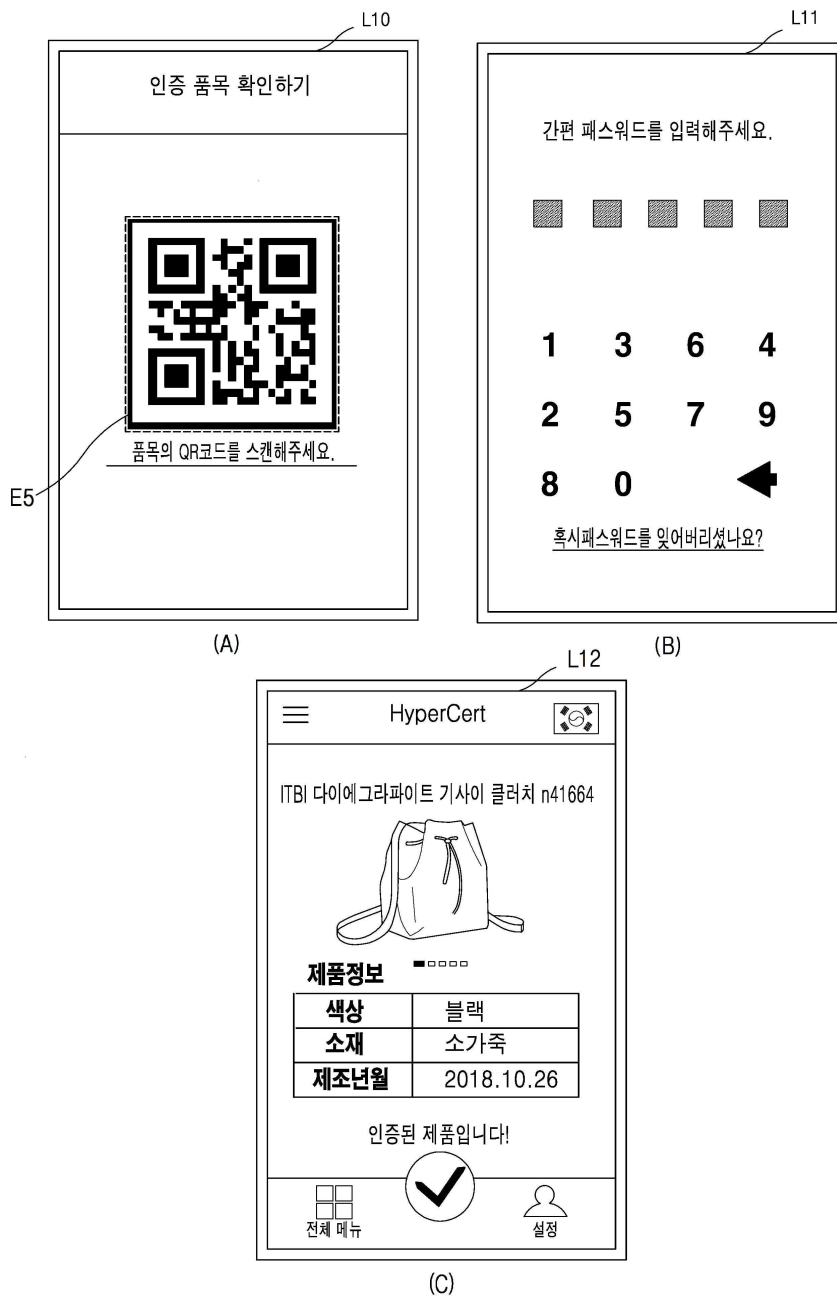
도면13



도면14



도면15



도면16

