(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2023-0171674
(43) 공개일자 2023년12월21일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *H04L 67/1097* (2022.01)
H04L 9/00 (2022.01) *H04L 9/40* (2022.01)
(52) CPC특허분류
H04L 9/3213 (2013.01)
H04L 63/0876 (2013.01)
(21) 출원번호 10-2022-0072129
(22) 출원일자 2022년06월14일
심사청구일자 2022년06월14일

(71) 출원인
창원대학교 산학협력단
경상남도 창원시 의창구 창원대학로 20(퇴촌동)
(72) 발명자
정성욱
경상남도 창원시 의창구 북면 무동로267번길 10, 205동 902호(창원무동 STX KAN 2차아파트)
황성욱
경상남도 창원시 성산구 원이대로579번길 13, 103동 1003호(용호동, 용지 아이파크)
손성무
경상남도 창원시 의창구 창이대로417번길 9-9, 203호(사림동)
(74) 대리인
양성보

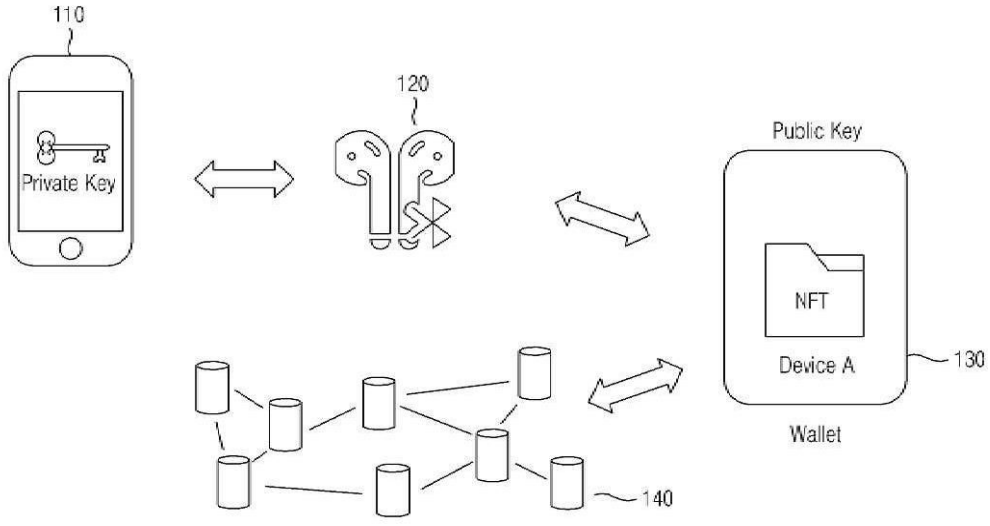
전체 청구항 수 : 총 14 항

(54) 발명의 명칭 **NFT를 활용한 블루투스 장치 인증 방법 및 시스템**

(57) 요 약

NFT를 활용한 블루투스 장치 인증 방법 및 시스템이 제시된다. 본 발명에서 제안하는 NFT를 활용한 블루투스 장치 인증 방법은 마스터 장치와 슬레이브 장치가 페어링하고, 상기 페어링 과정에 상기 마스터 장치를 통해 상기 슬레이브 장치의 NFT를 사용자 지갑에 생성하고, 공개키와 개인키를 쌍으로 생성하여 상기 마스터 장치 내부에 저장하는 단계 및 상기 저장된 공개키와 개인키 쌍을 검증하기 위해 상기 마스터 장치가 API를 사용하여 복수의 노드와 통신하고, 각 노드는 분산 원장에 저장되어 있는 장부를 통해 상기 NFT의 존재 유무를 검증함으로써 상기 슬레이브 장치를 인증하는 단계를 포함한다.

대 표 도



(52) CPC특허분류
H04L 67/1097 (2022.05)
H04L 9/3263 (2013.01)
H04L 9/50 (2022.05)

이 발명을 지원한 국가연구개발사업

과제고유번호	1365003599
과제번호	KMI2021-01312
부처명	기상청
과제관리(전문)기관명	한국기상산업기술원
연구사업명	기후예측 및 위험 대응 강화 연구
연구과제명	차세대 전산과학 기술접합을 위한 기반 기술 개발
기 여 율	1/1
과제수행기관명	창원대학교 산학협력단
연구기간	2022.01.01 ~ 2022.12.31

명 세 서

청구범위

청구항 1

마스터 장치와 슬레이브 장치가 페어링하고, 상기 페어링 과정에 상기 마스터 장치를 통해 상기 슬레이브 장치의 NFT를 사용자 지갑에 생성하고, 공개키와 개인키를 쌍으로 생성하여 상기 마스터 장치 내부에 저장하는 단계; 및

상기 저장된 공개키와 개인키 쌍을 검증하기 위해 상기 마스터 장치가 API를 사용하여 복수의 노드와 통신하고, 각 노드는 분산 원장에 저장되어 있는 장부를 통해 상기 NFT의 존재 유무를 검증함으로써 상기 슬레이브 장치를 인증하는 단계

를 포함하는 블루투스 장치 인증 방법.

청구항 2

제1항에 있어서,

상기 마스터 장치와 슬레이브 장치가 페어링하고, 상기 페어링 과정에 상기 마스터 장치를 통해 상기 슬레이브 장치의 NFT를 사용자 지갑에 생성하고, 공개키와 개인키를 쌍으로 생성하여 상기 마스터 장치 내부에 저장하는 단계는,

상기 지갑 내부에 상기 슬레이브 장치에 대응되는 NFT가 리스트로 존재하고, 상기 NFT는 상기 슬레이브 장치에 내장된 고유한 MAC 주소를 포함하는

블루투스 장치 인증 방법.

청구항 3

제1항에 있어서,

상기 마스터 장치와 슬레이브 장치가 페어링하고, 상기 페어링 과정에 상기 마스터 장치를 통해 상기 슬레이브 장치의 NFT를 사용자 지갑에 생성하고, 공개키와 개인키를 쌍으로 생성하여 상기 마스터 장치 내부에 저장하는 단계는,

상기 슬레이브 장치가 상기 마스터 장치와 최초로 페어링하는 과정에서 상기 마스터 장치에 NFT를 생성하고, 상기 NFT에 상응하는 동일한 MAC 주소가 이미 존재할 경우 상기 NFT 생성은 거절되는 장치 등록 단계를 포함하는

블루투스 장치 인증 방법.

청구항 4

제3항에 있어서,

상기 장치 등록 단계는,

상기 마스터 장치가 상기 슬레이브 장치를 검색하고, 검색된 슬레이브 장치는 자신의 MAC 주소를 마스터 장치로 전송하며,

상기 마스터 장치는 이더리움에 지갑생성을 요청하고, 상기 이더리움은 지갑을 생성하여 개인키를 마스터 장치에게 전달하며,

지갑 생성 후 상기 마스터장치는 이더리움에 상기 슬레이브 장치의 MAC 주소를 기반으로 하는 NFT 생성을 요청하고,

어떤 사용자의 지갑에 NFT를 생성할지 결정하기 위해 개인키를 요청하여 키를 전달한 후 이더리움에서 NFT를 생성하는

블루투스 장치 인증 방법.

청구항 5

제1항에 있어서,

상기 저장된 공개키와 개인키 쌍을 검증하기 위해 상기 마스터 장치가 API를 사용하여 복수의 노드와 통신하고, 각 노드는 분산 원장에 저장되어 있는 장부를 통해 상기 NFT의 존재 유무를 검증함으로써 상기 슬레이브 장치를 인증하는 단계는,

제1 사용자의 슬레이브 장치를 제2 사용자에게 양도하는 경우 제1 사용자의 슬레이브 장치의 NFT를 제2 사용자의 지갑으로 전송하는 장치 양도 단계를 포함하는

블루투스 장치 인증 방법.

청구항 6

제5항에 있어서,

상기 장치 양도 단계는,

양도하기 위한 제1 사용자의 슬레이브 장치가 제1 사용자의 슬레이브 장치의 NFT를 수신할 제2 사용자의 마스터 장치의 공개키 주소를 이더리움에 요청하고, 이더리움에서 제1 사용자의 마스터 장치에 개인키를 요청하면, 제1 사용자의 마스터 장치가 개인키를 이더리움에 전달하고, 제1 사용자의 슬레이브 장치의 NFT를 수신할 제2 사용자의 공개키 주소를 이용하여 상기 공개키의 개인키가 맞다면 입력된 공개키 주소로 NFT를 전송하는

블루투스 장치 인증 방법.

청구항 7

제1항에 있어서,

상기 저장된 공개키와 개인키 쌍을 검증하기 위해 상기 마스터 장치가 API를 사용하여 복수의 노드와 통신하고, 각 노드는 분산 원장에 저장되어 있는 장부를 통해 상기 NFT의 존재 유무를 검증함으로써 상기 슬레이브 장치를 인증하는 단계는,

상기 슬레이브 장치가 상기 마스터 장치와 최초로 페어링한 후 재연결 시에 개인키를 확인하지 않고 페어링만 되어 있다면 상기 슬레이브 장치가 상기 마스터 장치와 즉시 연결되는 장치 연결 단계; 및

상기 슬레이브 장치 사용 중 오류가 발생하는 경우 상기 슬레이브 장치의 초기화를 제공하는 장치 초기화 단계

를 더 포함하는 블루투스 장치 인증 방법.

청구항 8

상호 간 페어링하는 마스터 장치 및 슬레이브 장치 -상기 페어링 과정에 상기 마스터 장치를 통해 상기 슬레이브 장치의 NFT를 사용자 지갑에 생성하고, 공개키와 개인키를 쌍으로 생성하여 상기 마스터 장치 내부에 저장함-; 및

상기 저장된 공개키와 개인키 쌍을 검증하기 위해 상기 마스터 장치가 API를 사용하여 복수의 노드와 통신하고, 각 노드는 분산 원장에 저장되어 있는 장부를 통해 상기 NFT의 존재 유무를 검증함으로써 상기 슬레이브 장치를 인증하는 NBAS(NFT-based Bluetooth Device Authentication System)

를 포함하는 블루투스 장치 인증 시스템.

청구항 9

제8항에 있어서,

상기 마스터 장치 및 슬레이브 장치는,

상기 지갑 내부에 상기 슬레이브 장치에 대응되는 NFT가 리스트로 존재하고, 상기 NFT는 상기 슬레이브 장치에 내장된 고유한 MAC 주소를 포함하는

블루투스 장치 인증 시스템.

청구항 10

제8항에 있어서,

상기 마스터 장치 및 슬레이브 장치는,

상기 슬레이브 장치가 상기 마스터 장치와 최초로 페어링하는 과정에서 상기 마스터 장치에 NFT를 생성하고, 상기 NFT에 상응하는 동일한 MAC 주소가 이미 존재할 경우 상기 NFT 생성은 거절되는 장치 등록 과정을 수행하는

블루투스 장치 인증 시스템.

청구항 11

제10항에 있어서,

상기 마스터 장치 및 슬레이브 장치는,

상기 마스터 장치가 상기 슬레이브 장치를 검색하고, 검색된 슬레이브 장치는 자신의 MAC 주소를 마스터 장치로 전송하며,

상기 마스터 장치는 이더리움에 지갑생성을 요청하고, 상기 이더리움은 지갑을 생성하여 개인키를 마스터 장치에게 전달하며,

지갑 생성 후 상기 마스터장치는 이더리움에 상기 슬레이브 장치의 MAC 주소를 기반으로 하는 NFT 생성을 요청하고,

어떤 사용자의 지갑에 NFT를 생성할지 결정하기 위해 개인키를 요청하여 키를 전달한 후 이더리움에서 NFT를 생성하는

블루투스 장치 인증 시스템.

청구항 12

제8항에 있어서,

상기 NBAS는,

제1 사용자의 슬레이브 장치를 제2 사용자에게 양도하는 경우 제1 사용자의 슬레이브 장치의 NFT를 제2 사용자의 지갑으로 전송하는 장치 양도 과정을 수행하는

블루투스 장치 인증 시스템.

청구항 13

제12항에 있어서,

상기 NBAS는,

양도하기 위한 제1 사용자의 슬레이브 장치가 제1 사용자의 슬레이브 장치의 NFT를 수신할 제2 사용자의 마스터 장치의 공개키 주소를 이더리움에 요청하고, 이더리움에서 제1 사용자의 마스터 장치에 개인키를 요청하면, 제1 사용자의 마스터 장치가 개인키를 이더리움에 전달하고, 제1 사용자의 슬레이브 장치의 NFT를 수신할 제2 사용자의 공개키 주소를 이용하여 상기 공개키의 개인키가 맞다면 입력된 공개키 주소로 NFT를 전송하는

블루투스 장치 인증 시스템.

청구항 14

제1항에 있어서,

상기 NBAS는,

상기 슬레이브 장치가 상기 마스터 장치와 최초로 페어링한 후 재연결 시에 개인키를 확인하지 않고 페어링만 되어 있다면 상기 슬레이브 장치가 상기 마스터 장치와 즉시 연결되는 장치 연결 과정을 수행하고,

상기 슬레이브 장치 사용 중 오류가 발생하는 경우 상기 슬레이브 장치의 초기화를 제공하는 장치 초기화 과정

을 수행하는

블루투스 장치 인증 시스템.

발명의 설명

기 술 분 야

[0001] 본 발명은 NFT를 활용한 블루투스 장치 인증 방법 및 시스템에 관한 것이다.

배 경 기 술

[0002] 근거리 무선통신기술인 블루투스는 전력 효율이 뛰어나고 고품질 데이터를 지속적으로 전송하는데 최적 화된 통신 기술이다. 오늘날 블루투스는 노트북, 휴대폰, 이어폰, 마우스, 키보드, 헬스기기 등의 다양한 휴대 기기 분야에서 광범위하게 적용되고 있다. 애플, 삼성, 샤오미 등 다양한 IT 기업들은 무선이어폰 시장을 장악하기 위해 경쟁하고 있으며, 헬스케어와 피트니스 기업들은 블루투스 기술이 적용된 센서를 활용하여 사용자의 생체 데이터와 운동 데이터를 수집한 후 스마트폰으로 전송하는 웨어러블 기기들을 선보이고 있다.

[0003] 블루투스 기기는 대부분 소형의 휴대장치 형태로 인하여 분실이 자주 발생하는 문제점이 있다. 무선 이어폰의 경우 많은 사용자들이 분실을 경험하게 되는데 분실된 블루투스 이어폰을 습득하는 경우 간단한 초기화를 통해서 사용이 가능하여 습득자가 사용하거나 중고거래 시장에 판매하는 경우가 빈번하다. 특히 해외 제조사인 경우, 국내에서 블루투스 기기의 위치추적 기능을 제공하지 않고 있어 분실대책이 전무한 상태이다. 국내 제조사의 경우, 블루투스 무선 이어폰을 분실할 시 위치 추적기능을 지원한다. 그러나 평소 해당 기능이 활성화되어 있어야 하며, 잃어버린 기기 주변에 위치 추적 기능이 활성화된 같은 제조사의 다른 제품이 있어야 분실 기기의 추적이 가능하다. 또한 위치 추적 이전에 제3자가 습득할 경우에는 분실 대책으로서 한계가 있다[1].

발명의 내용

해결하려는 과제

[0004] 본 발명이 이루고자 하는 기술적 과제는 분실이 잦은 블루투스 기기에서 NFT(Non-Fungible Token)를 이용하여 합법적인 사용자를 인증하는 NBAS(NFT-based Bluetooth Device Authentication System)을 제공하는데 있다.

과제의 해결 수단

[0005] 일 측면에 있어서, 본 발명에서 제안하는 NFT를 활용한 블루투스 장치 인증 방법은 마스터 장치와 슬레이브 장치가 페어링하고, 상기 페어링 과정에 상기 마스터 장치를 통해 상기 슬레이브 장치의 NFT를 사용자 지갑에 생성하고, 공개키와 개인키를 쌍으로 생성하여 상기 마스터 장치 내부에 저장하는 단계 및 상기 저장된 공개키와 개인키 쌍을 검증하기 위해 상기 마스터 장치가 API를 사용하여 복수의 노드와 통신하고, 각 노드는 분산 원장에 저장되어 있는 장부를 통해 상기 NFT의 존재 유무를 검증함으로써 상기 슬레이브 장치를 인증하는 단계를 포함한다.

[0006] 상기 마스터 장치와 슬레이브 장치가 페어링하고, 상기 페어링 과정에 상기 마스터 장치를 통해 상기 슬레이브 장치의 NFT를 사용자 지갑에 생성하고, 공개키와 개인키를 쌍으로 생성하여 상기 마스터 장치 내부에 저장하는 단계는 상기 지갑 내부에 상기 슬레이브 장치에 대응되는 NFT가 리스트로 존재하고, 상기 NFT는 상기 슬레이브 장치에 내장된 고유한 MAC 주소를 포함한다.

[0007] 상기 마스터 장치와 슬레이브 장치가 페어링하고, 상기 페어링 과정에 상기 마스터 장치를 통해 상기 슬레이브 장치의 NFT를 사용자 지갑에 생성하고, 공개키와 개인키를 쌍으로 생성하여 상기 마스터 장치 내부에 저장하는 단계는 상기 슬레이브 장치가 상기 마스터 장치와 최초로 페어링하는 과정에서 상기 마스터 장치에 NFT를 생성하고, 상기 NFT에 상응하는 동일한 MAC 주소가 이미 존재할 경우 상기 NFT 생성은 거절되는 장치 등록 단계를 포함한다.

[0008] 상기 장치 등록 단계는 상기 마스터 장치가 상기 슬레이브 장치를 검색하고, 검색된 슬레이브 장치는 자신의 MAC 주소를 마스터 장치로 전송하며, 상기 마스터 장치는 이더리움에 지갑생성을 요청하고, 상기 이더리움은 지갑을 생성하여 개인키를 마스터 장치에게 전달하며, 지갑 생성 후 상기 마스터장치는 이더리움에 상기 슬레이브 장치의 MAC 주소를 기반으로 하는 NFT 생성을 요청하고, 어떤 사용자의 지갑에 NFT를 생성할지 결정하기 위해

개인키를 요청하여 키를 전달한 후 이더리움에서 NFT를 생성한다.

[0009] 상기 저장된 공개키와 개인키 쌍을 검증하기 위해 상기 마스터 장치가 API를 사용하여 복수의 노드와 통신하고, 각 노드는 분산 원장에 저장되어 있는 장부를 통해 상기 NFT의 존재 유무를 검증함으로써 상기 슬레이브 장치를 인증하는 단계는 제1 사용자의 슬레이브 장치를 제2 사용자에게 양도하는 경우 제1 사용자의 슬레이브 장치의 NFT를 제2 사용자의 지갑으로 전송하는 장치 양도 단계를 포함한다.

[0010] 상기 장치 양도 단계는 양도하기 위한 제1 사용자의 슬레이브 장치가 제1 사용자의 슬레이브 장치의 NFT를 수신할 제2 사용자의 마스터 장치의 공개키 주소를 이더리움에 요청하고, 이더리움에서 제1 사용자의 마스터 장치에 개인키를 요청하면, 제1 사용자의 마스터 장치가 개인키를 이더리움에 전달하고, 제1 사용자의 슬레이브 장치의 NFT를 수신할 제2 사용자의 공개키 주소를 이용하여 상기 공개키의 개인키가 맞다면 입력된 공개키 주소로 NFT를 전송한다.

[0011] 상기 저장된 공개키와 개인키 쌍을 검증하기 위해 상기 마스터 장치가 API를 사용하여 복수의 노드와 통신하고, 각 노드는 분산 원장에 저장되어 있는 장부를 통해 상기 NFT의 존재 유무를 검증함으로써 상기 슬레이브 장치를 인증하는 단계는 상기 슬레이브 장치가 상기 마스터 장치와 최초로 페어링한 후 재연결 시에 개인키를 확인하지 않고 페어링만 되어 있다면 상기 슬레이브 장치가 상기 마스터 장치와 즉시 연결되는 장치 연결 단계 및 상기 슬레이브 장치 사용 중 오류가 발생하는 경우 상기 슬레이브 장치의 초기화를 제공하는 장치 초기화 단계를 더 포함한다.

[0012] 또 다른 일 측면에 있어서, 본 발명에서 제안하는 NFT를 활용한 블루투스 장치 인증 시스템은 상호 간 페어링하는 마스터 장치 및 슬레이브 장치 -상기 페어링 과정에 상기 마스터 장치를 통해 상기 슬레이브 장치의 NFT를 사용자 지갑에 생성하고, 공개키와 개인키를 쌍으로 생성하여 상기 마스터 장치 내부에 저장함- 및 상기 저장된 공개키와 개인키 쌍을 검증하기 위해 상기 마스터 장치가 API를 사용하여 복수의 노드와 통신하고, 각 노드는 분산 원장에 저장되어 있는 장부를 통해 상기 NFT의 존재 유무를 검증함으로써 상기 슬레이브 장치를 인증하는 NBAS(NFT-based Bluetooth Device Authentication System)를 포함한다.

발명의 효과

[0013] 본 발명의 실시예들에 따른 NBAS(NFT-based Bluetooth Device Authentication System)는 분실이 잦은 블루투스 기기에서 NFT(Non-Fungible Token)를 이용하여 합법적인 사용자를 인증할 수 있다. 제안하는 시스템에서 사용자는 블루투스 기기를 기기의 고유 정보인 MAC 주소를 기반으로 탈중앙화된 형태의 이더리움 블록체인 상에 디지털 지갑을 생성하고, 디지털 지갑에 블루투스 장치의 MAC 주소를 이용하여 NFT를 생성하고 보관할 수 있다. 지갑의 소유자는 개인키를 사용하여 NFT의 소유를 증명함으로써 블루투스 장치의 합법적인 소유자임을 인증할 수 있다. 제안하는 NFT를 이용하는 인증 방식은 중앙화된 형태의 기존 인증 방식에 비하여 다양한 블루투스 기기들이 존재하는 환경에서도 별도의 관리체계를 필요로하지 않는다는 장점이 있다.

도면의 간단한 설명

[0014] 도 1은 본 발명의 일 실시예에 따른 NFT를 활용한 블루투스 장치 인증 시스템의 구성을 나타내는 도면이다.

도 2는 본 발명의 일 실시예에 따른 1명의 사용자가 복수의 슬레이브 장치를 소지하는 경우의 NBAS 구성도이다.

도 3은 본 발명의 일 실시예에 따른 NBAS의 인증 과정을 설명하기 위한 도면이다.

도 4는 본 발명의 일 실시예에 따른 NFT를 활용한 블루투스 장치 인증 방법을 설명하기 위한 흐름도이다.

도 5는 본 발명의 일 실시예에 따른 슬레이브 장치를 이더리움에 등록하는 과정을 설명하기 위한 도면이다.

도 6은 본 발명의 일 실시예에 따른 NFT 내부 데이터 구조를 나타내는 도면이다.

도 7은 본 발명의 일 실시예에 따른 장치 양도 과정을 설명하기 위한 도면이다.

도 8은 본 발명의 일 실시예에 따른 NBAS의 전체적인 개발구성을 나타낸다.

도 9 내지 도 11은 본 발명의 일 실시예에 따른 모의 실험 결과를 나타낸 그래프이다.

발명을 실시하기 위한 구체적인 내용

[0015] 블루투스 이어폰과 같은 대부분의 블루투스 장치는 무선이라는 편리성으로 다양하게 사용되지만 소형 무선기기

라는 특성으로 자주 분실되는 단점이 있다. 그러나 대부분의 블루투스 장치에서는 합법적인 소유자에 대한 인증 기능 제공이 미흡하며, 분실된 블루투스 장치를 습득한 제3자는 해당 기기를 손쉽게 자신의 스마트기기 등에 연결하여 사용할 수 있다.

[0016] 본 발명에서는 분실이 잦은 블루투스 기기에서 NFT(Non-Fungible Token)를 이용하여 합법적인 사용자를 인증하는 NBAS(NFT-based Bluetooth Device Authentication System)에 대해서 제안하였다. 기존의 중앙화된 형태의 인증 방식으로는 다양한 기업에서 만든 블루투스 기기들을 통합하고 인증하는데 어려움이 존재한다. 제안하는 시스템에서 사용자는 블루투스 기기를 기기의 고유 정보인 MAC 주소를 기반으로 탈중앙화된 형태의 이더리움[2] 블록체인 상에 디지털 지갑을 생성하고, 디지털 지갑에 블루투스 장치의 MAC 주소를 이용하여 NFT를 생성하고 보관한다. 지갑의 소유자는 개인키를 사용하여 NFT의 소유를 증명함으로써 블루투스 장치의 합법적인 소유자임을 인증하게 된다. 등록된 블루투스 기기는 최초 페어링 과정에서 개인키의 소유 유무를 확인하도록 하여 보안성을 강화하도록 하였다. 따라서 새로운 기기에서 분실된 기기를 사용하는 경우에 개인키 인증 절차를 거친 후 페어링이 가능하므로 제3자에 의한 분실된 블루투스 기기의 재사용을 방지하도록 하였다. 그리고 블루투스 기기를 분실했을 때 소유자가 분실 메시지를 이더리움에 등록하는 기능을 제공하여 습득자가 분실 메시지를 활용하여 사용자에게 되돌려 줄 수 있도록 하였다. NFT를 이용하는 인증 방식은 중앙화된 형태의 기존 인증 방식에 비하여 다양한 블루투스 기기들이 존재하는 환경에서도 별도의 관리체계를 필요로하지 않는다는 장점이 있다. 이더리움에서 NBAS(NFT-based Bluetooth Device Authentication System)의 평균 페이링 시간은 10.25sec로 마스터 장치와 슬레이브 장치간에 최초 페어링 때 한 번만 등록하고 그 후에는 재연결 기능을 사용한다. 재연결 평균시간은 0.00741sec로 기존 블루투스 장 치의 재연결시간과 유사하다. NBAS에서 미등록 장치에 대한 거절시간은 1.58sec로 측정되었다. 이하, 본 발명의 실시 예를 첨부된 도면을 참조하여 상세하게 설명한다.

[0018] 블루투스 장치의 보안 모드는 비보안 모드, 서비스 수준 강제 보안 모드, 링크 수준 강제 보안 모드로 나뉜다. 보안 기능을 제공하지 않는 비보안 모드를 제외한 두 가지 보안 모드에서는 마스터 장치와 슬레이브 장치 간에 일차적으로 키 공유 과정을 통하여 링크키를 공유하여 상호 간에 인증 및 암호화 기능을 제공하게 된다. 예를 들어, 키 공유 후 인증을 요구한 기기에서 제공한 128 비트 난수값과 블루투스 주소값, 공유된 링크키를 이용하여 128 비트 난수값을 생성하여 32비트는 인증에 활용하고 나머지 96비트(Authenticated Ciphering Offset)는 암호 키 생성에 활용할 수 있다[3].

[0019] 종래기술에서는 오토바이 사용자의 키분실 대비책으로 블루투스를 활용하는 SA-RT(Situation Awareness Rating Technique)방식을 적용한 오토바이 2차 인증 시스템을 구축하였다. 해당 시스템은 아두이노 기반 HC-05와 SIM800L 모듈을 사용하여 열쇠 분실 문제를 해결하고 열쇠가 분실된 오토바이를 확보 할 수 있도록 하였다.

[0020] NFT는 블록체인 네트워크의 기술적 장점인 신뢰성과 무결성을 활용한 기술이다. NFT는 자산에 대한 특징을 블록체인 네트워크에 기록함으로써 자산에 대한 원본 보장이 가능하다. NFT는 블록체인 네트워크의 계정에 의해 발급된다. NFT를 발급하는 생성자 계정은 토큰을 발급하는 트랜잭션에 디지털 서명을 한다. 이때 디지털 서명은 블록체인 기술의 측면에서 계정의 소유자가 개인키를 활용하여 트랜잭션에 서명하였는지를 확인할 수 있음을 의미한다. 이렇게 디지털 서명된 트랜잭션은 서명에 사용된 암호화 알고리즘으로 인하여 조작이 불가능하다.

[0021] 종래기술에 따르면, IoT장치에 기기 고유의 NFT를 생성하여 저장하는 방식으로 IoT장치의 하드웨어와 소프트웨어에 대한 신뢰성을 제공하는 방식을 제안하였다. 제조사는 IoT장치에 내장된 SRAM PUFs(Physical Unclonable Functions)를 사용하여 스마트 NFT를 생성하고 장치를 프로그래밍한다. 제조부터 최종 사용자 적용까지 IoT장치의 하드웨어와 소프트웨어 신뢰성을 보장하여 사용자 BCA(BlockChain Account), 장치의 작동 모드와 관련된 상태, 공개, 소유자 및 사용자와 공유하는 비밀과 관련된 데이터 등의 정보들을 스마트 계약 기능과 가스 소비를 통해 제공한다[6].

[0023] 도 1은 본 발명의 일 실시예에 따른 NFT를 활용한 블루투스 장치 인증 시스템의 구성을 나타내는 도면이다.

[0024] NFT를 활용한 블루투스 장치 인증 시스템은 마스터 장치(110), 슬레이브 장치(120) 및 NBAS(NFT-based Bluetooth Device Authentication System)(140)를 포함한다.

[0025] 사용자는 자신의 마스터 장치(예를 들어, 스마트폰)(110)를 소지한다. 마스터 장치(110)는 슬레이브 장치(예를 들어, 무선 이어폰)(120)와 페어링 된다. 사용자는 페어링 과정에 마스터 장치(110)를 통해 슬레이브 장치(120)의 NFT를 지갑(130)에 생성하게 된다. 공개키와 개인키를 쌍으로 생성하여 마스터 장치 내부에 개인키를 저장

한다. 이때 슬레이브 장치의 NFT는 장치에 내장된 고유한 MAC 주소를 포함한다.

[0026] 본 발명의 실시예에 따른 NBAS(140)은 상기 저장된 공개키와 개인키 쌍을 검증하기 위해 상기 마스터 장치가 API를 사용하여 복수의 노드와 통신하고, 각 노드는 분산 원장에 저장되어 있는 장부를 통해 상기 NFT의 존재 유무를 검증함으로써 상기 슬레이브 장치를 인증한다.

[0028] 도 2는 본 발명의 일 실시예에 따른 1명의 사용자가 복수의 슬레이브 장치를 소지하는 경우의 NBAS 구성도이다.

[0029] 또 다른 실시예에 따르면, 일반적으로 1명의 사용자(210)는 복수의 슬레이브 장치(다시 말해, 블루투스 장치)(220)를 소유할 수 있다. 도 2는 1명의 사용자가 복수의 슬레이브 장치를 소지하는 경우의 NBAS 구성도를 나타낸 것이다. 슬레이브 장치들(220)은 사용자의 지갑(230) 내부에 NFT 리스트로 저장되며 페어링 단계에서 마스터 장치에 저장된 개인키(241)를 통해 인증되게 된다.

[0031] 도 3은 본 발명의 일 실시예에 따른 NBAS의 인증 과정을 설명하기 위한 도면이다.

[0032] 본 발명의 실시예에 따른 NBAS의 인증 과정은 개인키와 공개키 쌍을 검증하는 과정으로 도 3에서와 같이 이루어진다. 본 발명의 실시예에 따른 개인키는 Web3 Secret Storage Definition에서 정의한 표준 양식 PBKDF2-SHA-256을 활용하여 마스터 장치(311)에 저장된다.

[0033] 마스터 장치(311)가 슬레이브 장치(321)에게 수행하기 위한 기능 선택(321)하여 전송하면, 마스터 장치(311)는 이더리움에서 제공하는 블록체인 API(323)를 사용하여 노드(314)와 통신한다. 각 노드들은 분산 원장에 저장되어 있는 장부(API 리스트)(323)를 통하여 NFT의 존재 유무를 검증하는 방식으로 인증하게 된다.

[0035] 도 4는 본 발명의 일 실시예에 따른 NFT를 활용한 블루투스 장치 인증 방법을 설명하기 위한 흐름도이다.

[0036] 제안하는 NFT를 활용한 블루투스 장치 인증 방법은 마스터 장치와 슬레이브 장치가 페어링하고, 상기 페어링 과정에 상기 마스터 장치를 통해 상기 슬레이브 장치의 NFT를 사용자 지갑에 생성하고, 공개키와 개인키를 쌍으로 생성하여 상기 마스터 장치 내부에 저장하는 단계(420) 및 상기 저장된 공개키와 개인키 쌍을 검증하기 위해 상기 마스터 장치가 API를 사용하여 복수의 노드와 통신하고, 각 노드는 분산 원장에 저장되어 있는 장부를 통해 상기 NFT의 존재 유무를 검증함으로써 상기 슬레이브 장치를 인증하는 단계(430)를 포함한다.

[0037] 본 발명의 실시예에 따르면, 사용자의 마스터 장치는 먼저 수행하기 위한 기능을 선택(410)한다. 본 발명의 실시예에 따른 NBAS는 장치 등록(420), 장치 연결 단계(431), 장치 양도 단계(432), 초기화 단계(440)를 수행할 수 있다.

[0038] 단계(420)에서는 마스터 장치와 슬레이브 장치가 페어링하고, 상기 페어링 과정에 상기 마스터 장치를 통해 상기 슬레이브 장치의 NFT를 사용자 지갑에 생성하고, 공개키와 개인키를 쌍으로 생성하여 상기 마스터 장치 내부에 저장한다.

[0039] 장치 등록(421)을 위해 먼저, 상기 마스터 장치가 상기 슬레이브 장치를 검색하고, 검색된 슬레이브 장치는 자신의 MAC 주소를 마스터 장치로 전송한다. 상기 마스터 장치는 이더리움에 지갑생성을 요청하고(423), 지갑이 존재하는 경우 상기 슬레이브 장치의 NFT를 사용자 지갑에 생성한다(424). 지갑이 존재하지 않는 경우 공개키와 개인키를 쌍으로 생성하여 상기 마스터 장치 내부에 저장한다(426).

[0040] 단계(430)에서는 상기 저장된 공개키와 개인키 쌍을 검증하기 위해 상기 마스터 장치가 API를 사용하여 복수의 노드와 통신하고, 각 노드는 분산 원장에 저장되어 있는 장부를 통해 상기 NFT의 존재 유무를 검증함으로써 상기 슬레이브 장치를 인증한다. 단계(430)는 장치 연결 단계(431), 장치 양도 단계(432) 초기화 단계(440) 포함한다.

[0041] 상기 이더리움은 지갑을 생성하여 개인키를 마스터 장치에게 전달하며, 지갑 생성 후 상기 마스터장치는 이더리움에 상기 슬레이브 장치의 MAC 주소를 기반으로 하는 NFT 생성을 요청한다. 이후, 어떤 사용자의 지갑에 NFT를 생성할지 결정하기 위해 개인키를 요청하여 키를 전달한 후 이더리움에서 NFT를 생성한다.

[0042] 본 발명의 실시예에 따른 장치 연결 단계(431)은 상기 슬레이브 장치가 상기 마스터 장치와 최초로 페어링한 후 재연결 시에 개인키를 확인하지 않고 페어링만 되어 있다면 상기 슬레이브 장치가 상기 마스터 장치와 즉시 연

결된다(431).

[0043] 본 발명의 실시예에 따른 장치 양도 단계(432)는 제1 사용자의 슬레이브 장치를 제2 사용자에게 양도하는 경우 제1 사용자의 슬레이브 장치의 NFT를 제2 사용자의 지갑으로 전송한다.

[0044] 양도하기 위한 제1 사용자의 슬레이브 장치가 제1 사용자의 슬레이브 장치의 NFT를 수신할 제2 사용자의 마스터 장치의 공개키 주소를 이더리움에 요청하고, 이더리움에서 제1 사용자의 마스터 장치에 개인키를 요청하면, 제1 사용자의 마스터 장치가 개인키를 이더리움에 전달하고, 제1 사용자의 슬레이브 장치의 NFT를 수신할 제2 사용자의 공개키 주소를 이용하여 상기 공개키의 개인키를 검증한다(434). 상기 공개키와 개인키가 맞다면 입력된 공개키 주소로 NFT를 전송하고(435), 아닌 경우 장치 양도를 수행하지 않는다(436).

[0045] 본 발명의 실시예에 따른 초기화 단계(440)는 상기 슬레이브 장치 사용 중 오류가 발생하는 경우 상기 슬레이브 장치의 초기화를 제공한다. 초기화를 진행하여도 이미 등록된 MAC 주소를 통해 NFT와 연결되며 개인키 확인 과정없이 초기화를 진행할 수 있다.

[0046] 본 발명의 실시예에 따른 장치 등록 단계와 장치 양도 단계에서는 마스터 장치에 저장된 개인키 확인 과정을 거치게 된다. 장치 재연결은 페어링이 완료되었다면 이후로는 마스터 장치와 자동연결되기 때문에 추가적인 인증 프로세스를 거치지 않는다.

[0048] 도 5는 본 발명의 일 실시예에 따른 슬레이브 장치를 이더리움에 등록하는 과정을 설명하기 위한 도면이다.

[0049] 먼저 마스터 장치에서 슬레이브 장치를 검색하고(510), 검색된 슬레이브 장치는 자신의 MAC 주소를 마스터 장치로 전송한다(520). 마스터 장치는 이더리움에 지갑생성을 요청한다(530). 이더리움은 지갑을 생성하고, 개인키를 마스터 장치에게 전달한다(540). 지갑 생성 후 마스터 장치는 이더리움에 슬레이브 장치 MAC 주소를 기반으로 하는 NFT 생성을 요청한다(550). 이더리움은 마스터 장치에게 어떤 지갑에 NFT를 생성할지 결정하기 위해 개인키를 요청한다(560). 마스터 장치는 이더리움에게 개인키를 전달한 후(570) 이더리움에서 NFT를 생성한다(580).

[0051] 도 6은 본 발명의 일 실시예에 따른 NFT 내부 데이터 구조를 나타내는 도면이다.

[0052] 이더리움에서 공개키는 개인키와 쌍을 이루며 사용자의 지갑을 생성한다. 지갑 내부에는 개별 장치에 대응되는 NFT들이 리스트로 존재하며 개인키를 이용하여 소유를 증거하게 된다. 도 6은 NFT 내부 데이터 구조를 보인 것으로, 슬레이브 장치의 MAC 주소가 포함되며 사용자가 정의한 데이터가 포함된다.

[0054] 도 7은 본 발명의 일 실시예에 따른 장치 양도 과정을 설명하기 위한 도면이다.

[0055] 슬레이브 장치(다시 말해, 블루투스 장치)의 최초 등록 및 페어링 과정이 끝나면 사용자는 장치를 재연결한다. 장치의 재연결은 이더리움 네트워크과 통신하지 않고 페어링이 완료된 후라면 개인키 확인없이 자동으로 재연결하게 된다. 슬레이브 장치를 양도(hand-over)하는 경우에는 양도할 장치의 NFT를 수신할 상대방의 공개키 주소를 필요로 한다.

[0056] 도 7을 참조하여 장치 양도 과정을 설명한다.

[0057] 마스터 장치에서 소유 중인 블루투스 장치의 NFT 전송을 요청한다(710). 전송 대상은 장치를 양도받을 사용자 마스터 장치의 공개키이다. 이더리움에서 개인키를 요청하고(720), 개인키를 이더리움에 전달한다(730). 공개키의 개인키가 맞다면 입력된 공개키 주소로 NFT를 전송한다(740).

[0058] 본 발명의 실시예에 따른 NBAS에서 슬레이브 장치의 초기화는 블루투스 연결 과정에서 생기는 오류나 사용자가 기기 초기화를 원하는 경우에 블루투스 통신을 위한 페어링 쌍을 초기화하는 기능이다. NBAS에서의 초기화는 기존의 블루투스 장치에서 초기화와 달리 MAC 주소를 초기화하지 않는다.

[0059] 표 1에서는 기존 블루투스 장치에서의 초기화 기능과 NBAS에서의 초기화 기능의 차이점을 비교 제시한 것이다.

[0060] <표 1>

Bluetooth	NBAS
Pairing Key Pair	Pairing Key Pair
Do not Use of MAC Address	Use of MAC Address

[0061]

[0062] 제안하는 NBAS 시스템은 MAC 주소를 인증 시스템의 요소로 활용하기 때문에 초기화를 하여도 이더리움에 저장된 MAC 주소는 초기화되지 않고 유지되게 된다.

[0064] 본 발명의 실시예에 따른 NBAS 모의 실험환경을 구축하고 다양한 실험을 수행한다. 모의 실험 환경은 합법적인 블루투스 장치 소유자 스마트폰 A(사용자 마스터 장치), 미등록 스마트폰 B(미등록 마스터 장치)와 블루투스 장치 C(슬레이브 장치)로 구성된다. 이더리움에서의 노드 개수가 증가하면 속도가 저하될 수 있으나[7], 본 발명에서는 NBAS에서 블루투스 장치의 인증 보안의 효용성을 확인하기 위한 테스트베드를 구성하여 성능을 측정한다.

[0065] 표 2에서는 실험 환경 구축에 사용된 언어 등 세부 구현 환경을 제시한다. 자바스크립트를 사용해 모의 시스템을 구축하고 솔리디티를 통해 스마트 컨트랙트를 배포한다. 구축 환경으로 리액트 네이티브, 트러플, 노드 JS를 사용한다.

[0066] <표 2>

Environment	React-native, Truffle, Nodejs
Library	Ethereumjs-tx.js, Ethereumjs-wallet.js, Ethereumjs-util 6.0.0, Ethers 4.0.23, React 16.6.3, React-native-bluetooth-serial 1.0.0, React-native-secure-key-store 2.0.0
Language	Javascript, Solidity

[0067]

[0068] 본 발명의 실시예에 따르면, Node-bluetooth.js 라이브러리를 사용하여 블루투스 세부 기능을 구현한다. 마스터 장치는 블루투스 장치 검색, 페어링된 장치 출력, 블루투스 연결, 데이터 통신등의 역할을 수행한다. 마스터 장치는 내부적으로 개인키를 저장하며 사용자가 지정한 암호문으로 암호화 된다. 개인키를 통해 사용자를 증명하고 이더리움과 통신한다. web3.js는 HTTP, IPC 또는 WebSocket형태로 로컬 또는 원격 이더리움 노드와 상호작용할 수 있는 용도로 사용한다. 데이터를 주고받는 형태는 JSON 형태이며 기능에 따라 직렬화를 진행한다. INFURA를 사용하여 이더리움 노드와 통신하고 ethereumjs-tx.js라이브러리를 사용해 서명 및 스마트 컨트랙트 함수를 호출한다. 퍼블릭 블록체인의 종류는 비트코인, 이더리움, 폴리곤 등이 있다[8]. 이 중 본 연구에서는 개발 환경이 우수하고 다양한 라이브러리를 지원하는 이더리움을 사용하였다. 일반적인 블록체인 기술에서는 토큰이 대체 가능한 형태이다. 하지만 NFT는 대체 불가능한 토큰이기 때문에 고유한 원본성과 소유권을 나타내는데 사용될 수 있는 장점이 있다[5]. 따라서 제안하는 NBAS에서 MAC address를 NFT에 저장함으로써 원본성 및 소유권을 나타낼 수 있다. 스마트 컨트랙트는 솔리디티를 사용하여 이벤트, 구조체, 배열, 7개의 매핑 및 메서드로 구현하며, ERC721에서 권장하는 인터페이스를 따른다. 배포는 트러플을 사용하고 주소는 0xf1fe23dd1a73663e07b7ceffccbbc7dfe6197529이다.

[0070] 도 8은 본 발명의 일 실시예에 따른 NBAS의 전체적인 개발구성을 나타낸다.

[0071] 본 발명의 일 실시예에 따른 NBAS은 블루투스 레이어(810), 네트워크 레이어(820) 및 이더리움 레이어(830)를 포함한다.

[0073] 도 9 내지 도 11은 본 발명의 일 실시예에 따른 모의 실험 결과를 나타낸 그래프이다.

[0074] 도 9는 전체 100회 수행하였을 때, 기존 블루투스 장치의 페어링 시간과 NBAS 페어링 시간을 비교한 것이다.

[0075] 도 10의 기존 블루투스 장치 재연결 시간은 평균 0.007sec로 측정되었다. NBAS의 경우 최초 페어링 이후 재연결 시에는 마스터 장치 내부에 NBAS를 통한 기존 페어링 장치들의 정보가 저장됨으로 추가적으로 이더리움 네트워크상에 접속할 필요가 없다. 따라서 NBAS에서도 재연결될 때 시간은 기존의 블루투스 장치의 재연결 시간과 비슷하게 측정되었다.

[0076] 본 발명의 실시예에 따른 NBAS는 NFT를 활용하여 미승인된 장치의 승인을 거절함으로써 기존 블루투스 장치의 분실, 도난에 대한 보안성을 제공한다. 도 11과 같이 미승인된 장치에서 이더리움에 등록된 슬레이브 장치에 페어링을 요청하는 경우 미승인 장치의 접근은 페어링이 제 한되며 NBAS의 거절 시간은 평균 1.58sec로 측정되었다. 이는 NBAS와 기존 블루투스 페어링을 구분짓는 중요한 특징으로 NBAS는, 미승인 장치의 페어링 을 효과적으로 제한함을 보여준다.

[0077] 이와 같이, 본 발명에서는 기존의 블루투스 장치에서 분실 취약점을 해결하기 위한 방안으로 NFT기반으로 블루투스 장치를 인증하는 NBAS를 제안하였다. 블루투스 장치의 초기 페어링 단계에서 슬레이브 장치의 고유정보를 NFT화하여 등록하고 생성한 합법적인 소유자만 해당 NFT에 접근하는 절차를 제안하였다. NBAS의 초기 페어링 시간은 평균 10.25sec이고 재연결 시간은 평균 0.007sec으로 측정되었다. 또한 NBAS는 미등록장치를 평균 1.58sec로 거절함을 보여주었다. 이는 장치 등록 후 다른 소유자 혹은 다른 기기에서 접근을 효과적으로 제한하며 보안성을 강화 하였음을 보여준다. 제안하는 시스템은 다양한 형태의 블루투스 장치가 존재하는 환경에서 보안을 강화하고 분실된 블루투스 장치의 무분별한 사용을 방지 하는 해결책으로 활용될 수 있을 것으로 기대된다.

[0078] 이상에서 설명된 장치는 하드웨어 구성요소, 소프트웨어 구성요소, 및/또는 하드웨어 구성요소 및 소프트웨어 구성요소의 조합으로 구현될 수 있다. 예를 들어, 실시예들에서 설명된 장치 및 구성요소는, 예를 들어, 프로세서, 콘트롤러, ALU(arithmetic logic unit), 디지털 신호 프로세서(digital signal processor), 마이크로컴퓨터, FPGA(field programmable gate array), PLU(programmable logic unit), 마이크로프로세서, 또는 명령(instruction)을 실행하고 응답할 수 있는 다른 어떠한 장치와 같이, 하나 이상의 범용 컴퓨터 또는 특수 목적 컴퓨터를 이용하여 구현될 수 있다. 처리 장치는 운영 체제(OS) 및 상기 운영 체제 상에서 수행되는 하나 이상의 소프트웨어 애플리케이션을 수행할 수 있다. 또한, 처리 장치는 소프트웨어의 실행에 응답하여, 데이터를 접근, 저장, 조작, 처리 및 생성할 수도 있다. 이해의 편의를 위하여, 처리 장치는 하나가 사용되는 것으로 설명된 경우도 있지만, 해당 기술분야에서 통상의 지식을 가진 자는, 처리 장치가 복수 개의 처리 요소(processing element) 및/또는 복수 유형의 처리 요소를 포함할 수 있음을 알 수 있다. 예를 들어, 처리 장치는 복수 개의 프로세서 또는 하나의 프로세서 및 하나의 콘트롤러를 포함할 수 있다. 또한, 병렬 프로세서(parallel processor)와 같은, 다른 처리 구성(processing configuration)도 가능하다.

[0079] 소프트웨어는 컴퓨터 프로그램(computer program), 코드(code), 명령(instruction), 또는 이들 중 하나 이상의 조합을 포함할 수 있으며, 원하는 대로 동작하도록 처리 장치를 구성하거나 독립적으로 또는 결합적으로(collectively) 처리 장치를 명령할 수 있다. 소프트웨어 및/또는 데이터는, 처리 장치에 의하여 해석되거나 처리 장치에 명령 또는 데이터를 제공하기 위하여, 어떤 유형의 기계, 구성요소(component), 물리적 장치, 가상 장치(virtual equipment), 컴퓨터 저장 매체 또는 장치에 구체화(embody)될 수 있다. 소프트웨어는 네트워크로 연결된 컴퓨터 시스템 상에 분산되어서, 분산된 방법으로 저장되거나 실행될 수도 있다. 소프트웨어 및 데이터는 하나 이상의 컴퓨터 판독 가능 기록 매체에 저장될 수 있다.

[0080] 실시예에 따른 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 실시예를 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다.

[0081] 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 형

태로 결합 또는 조합되거나, 다른 구성요소 또는 균등물에 의하여 대치되거나 치환되더라도 적절한 결과가 달성될 수 있다.

[0082] 그러므로, 다른 구현들, 다른 실시예들 및 특허청구범위와 균등한 것들도 후술하는 특허청구범위의 범위에 속한다.

[0084] <참고 문헌>

[0085] [1] Scarfone, Karen, and John Padgette, "Guide to bluetooth security", NIST Special Publication vol. 800, no. 121, 2008.

[0086] [2] H. J. Lee and J. Y. Cho, "A Study on Matters of Crypto-Currency," The Jounal of Comparative Private Law, vol. 25, no. 2, pp. 657-696, May. 2018.

[0087] [3] A. I. Mondal and B. K. Mandal, "Architecture of Bluetooth Security for Pairing Key and Better Authentication," in Proceeding of the 5th International Conference on Information System and Computer Networks, Mathura, India, pp. 1-6, 2021.

[0088] [4] N. Anggrini, I. M. Shofi, M. Nurzamazami, N. Hakiem, F. Fahrianto, and T. Rosyadi, "Motorcycle Secondary Authentication System Using Arduino-Based HC-05 and SIM8001 Module," in Proceeding of the 8th International Conference on Cyber and IT Service Management, Pangkal, Indonesia, pp. 1-7, 2020.

[0089] [5] J. Lee and G. -S. Jo, "Understanding and Utilizing the Latest NFT Technology," Korea Institute of Information Technology Magazine, vol. 19, no. 1, pp. 7-11, Dec. 2021.

[0090] [6] J. Arcenegui, R. Arjona, R. Roman, and I. Baturone, "Secure combination of IoT and blockchain by physically binding IoT devices to smart non-fungible tokens using PUFs," MDPI Sensors, vol. 21, no. 9, pp. 3119, 2021, DOI: 10.3390/s21093119.

[0091] [7] R. Dennis and J. P. Disso, "An analysis into the scalability of bitcoin and ethereum," in Proceeding of the third International Congress on Information and Communication Technology, London, U.K, vol. 797, pp. 619-627, 2019.

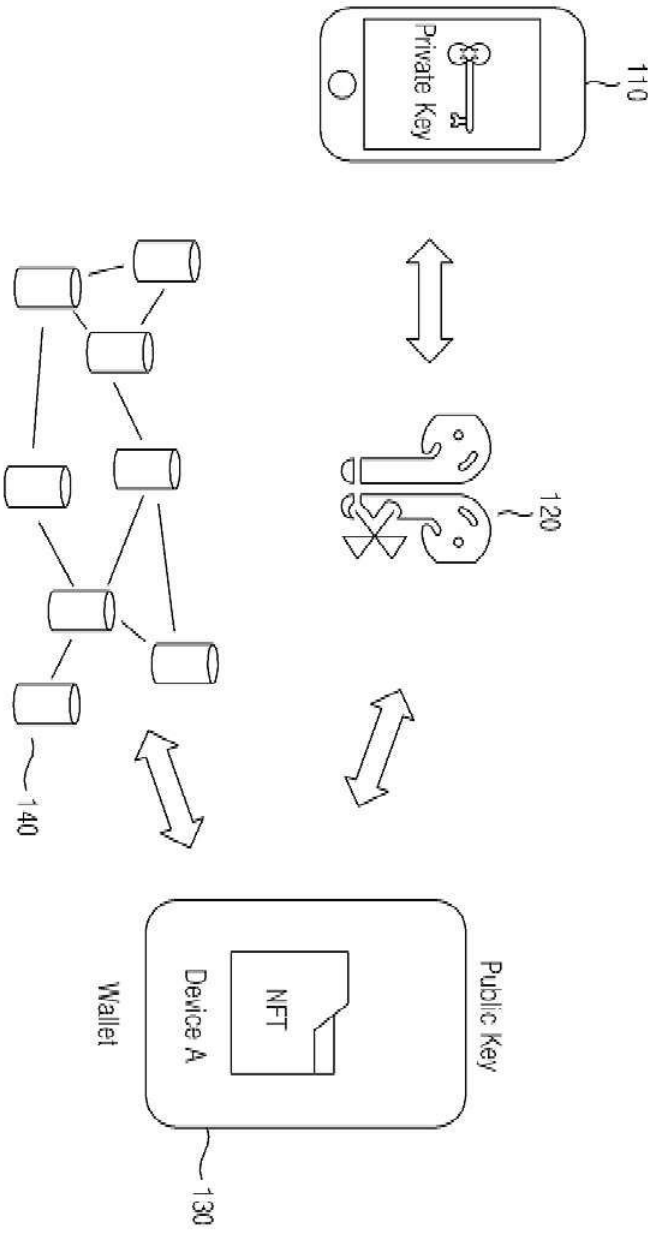
[0092] [8] F. Irresberger, K. John, P. Muller, and F. Saleh, "The public blockchain ecosystem: An empirical analysis," NYU Stern School of Business, Apr. 2021.

[0093] [9] S. Gajbhiye, M. Samta, S. Karmkar, and S. Sharma, "Design, implementation and security analysis of Bluetooth pairing protocol in NS2," in Proceeding of the International Conference on Advances in Computing, Communications and Informatics, Jaipur, India, pp. 1711-1717, 2016.

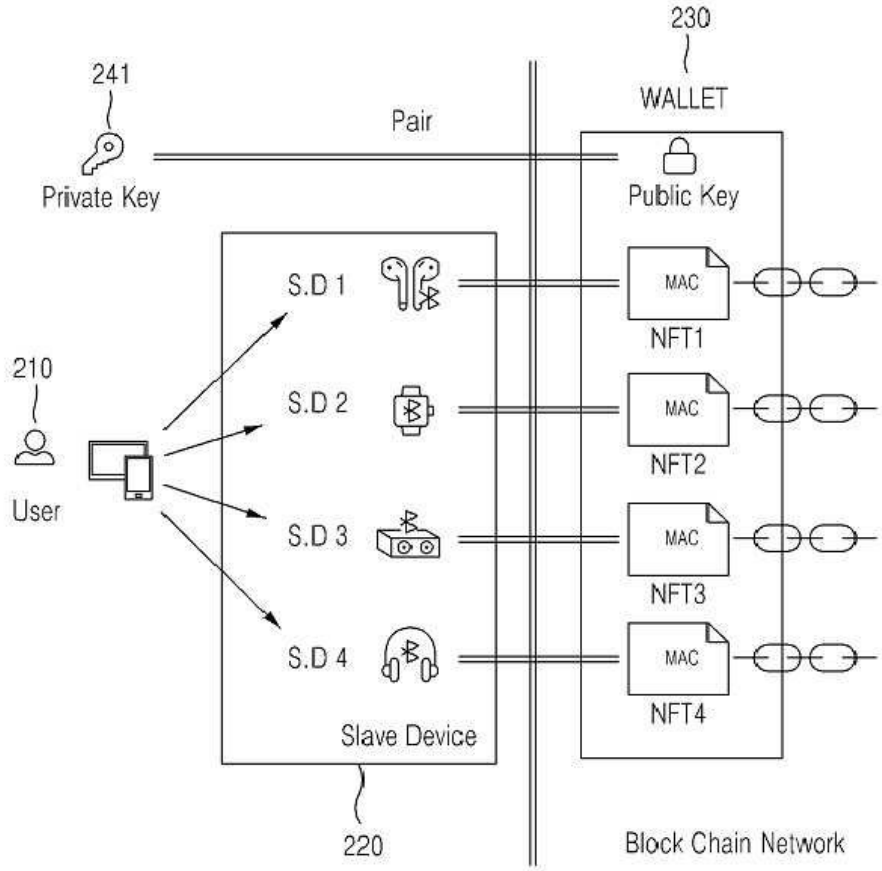
[0094] [10] Ethereum Development Documentation [Internet]. Available: https://ethereum.org/en/developers/docs/blocks/.

도면

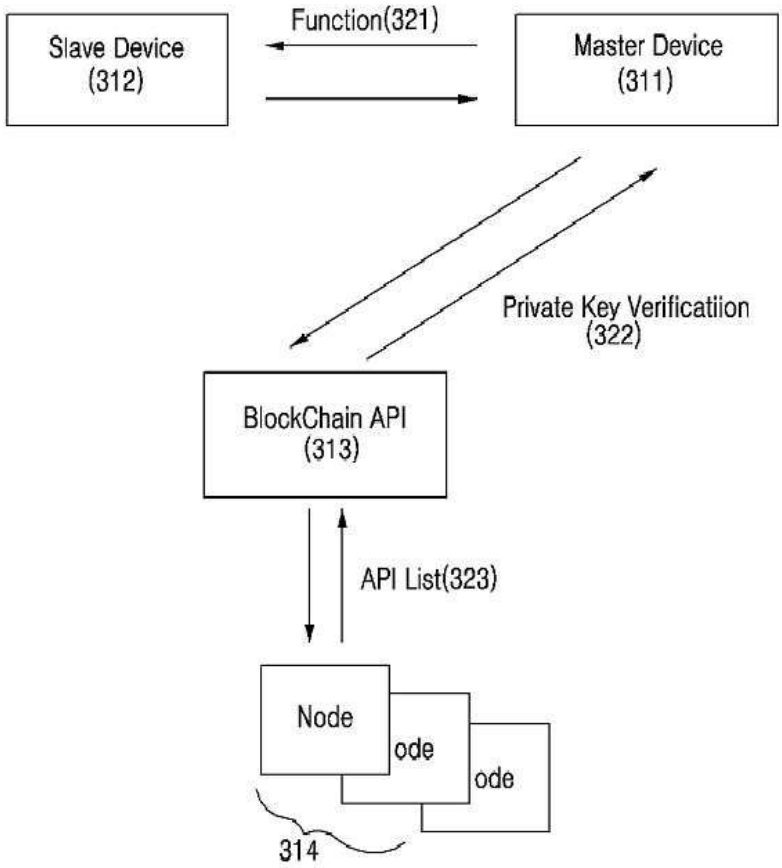
도면1



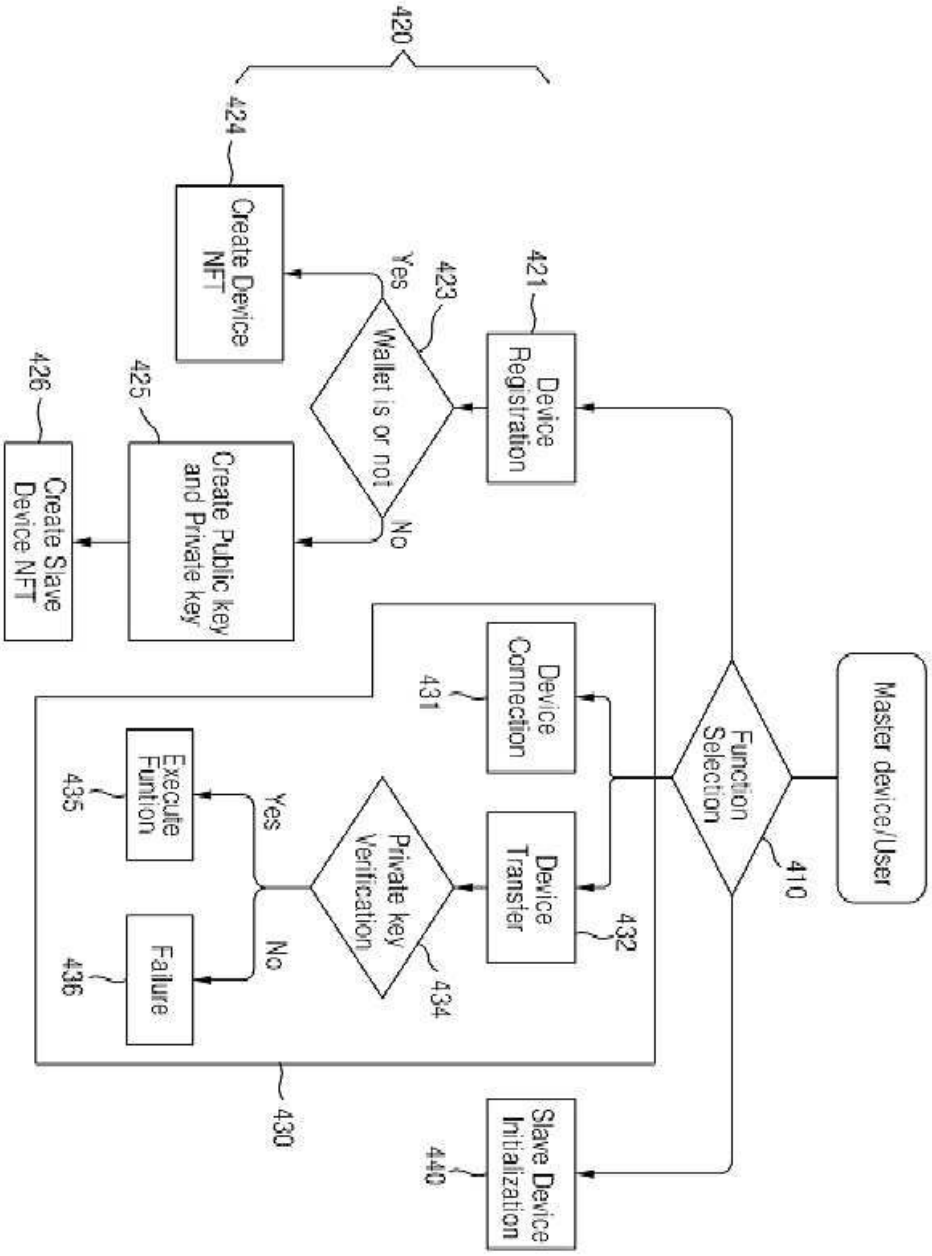
도면2


230
WALLET
241
Pair
Private Key
Public Key
S.D 1
S.D 2
S.D 3
S.D 4
MAC
NFT1
MAC
NFT2
MAC
NFT3
MAC
NFT4
210
User
Slave Device
220
Block Chain Network

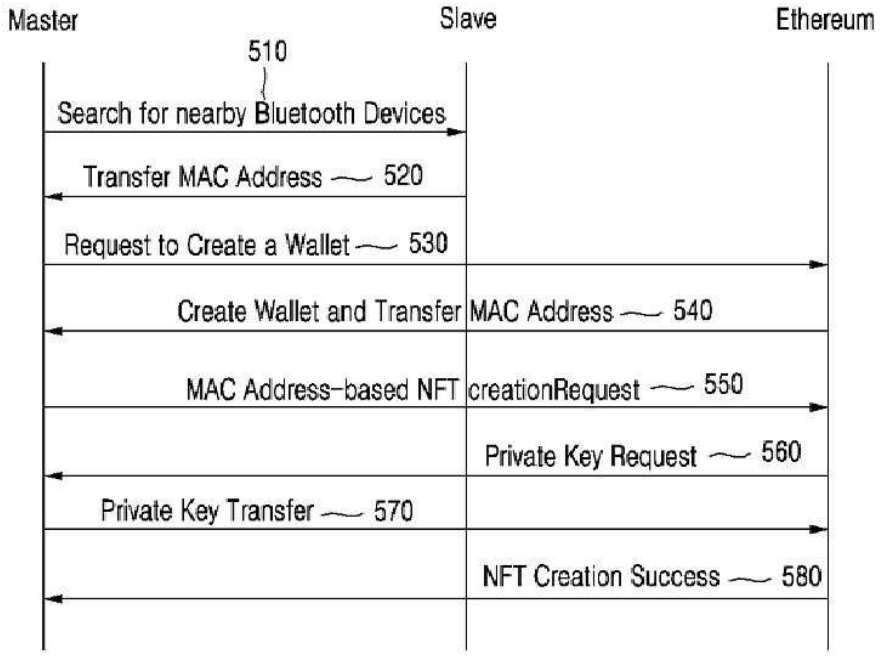
도면3


Slave Device
(312)
Function(321)
Master Device
(311)
Private Key Verificatiion
(322)
BlockChain API
(313)
API List(323)
Node
ode
ode
314

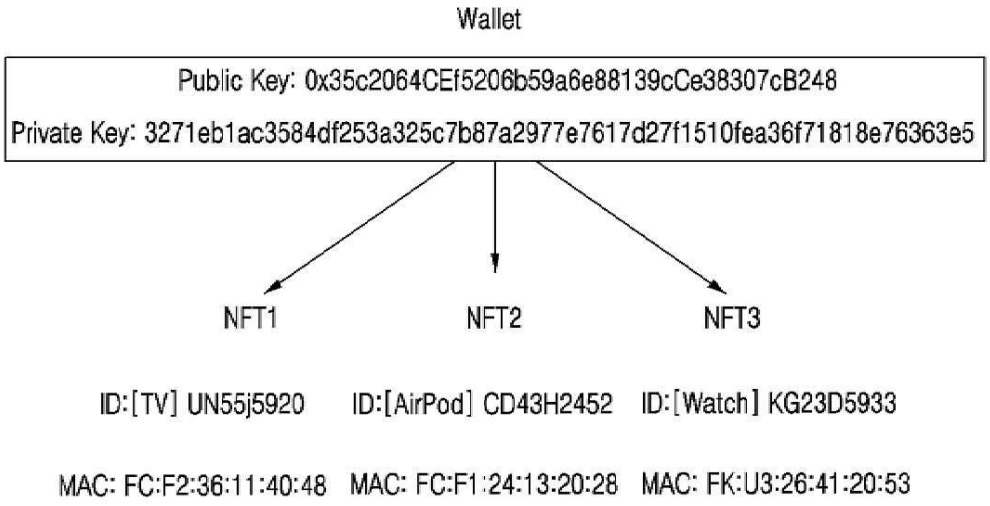
도면4


Master device/User
410
Function Selection
Device Registration
421
Wallet is or not
423
Yes
No
Create Device NFT
424
420
Create Public key and Private key
425
Create Slave Device NFT
426
Device Connection
431
Device Transfer
432
Private key Verification
434
Execute Funtion
435
Failure
436
430
Slave Device Initialization
440

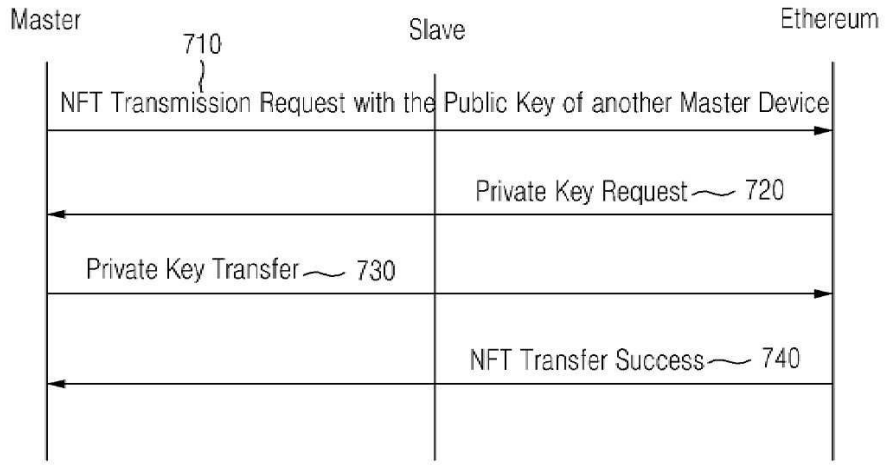
도면5


Master
Slave
Ethereum
510
Search for nearby Bluetooth Devices
Transfer MAC Address 520
Request to Create a Wallet 530
Create Wallet and Transfer MAC Address 540
MAC Address-based NFT creationRequest 550
Private Key Request 560
Private Key Transfer 570
NFT Creation Success 580

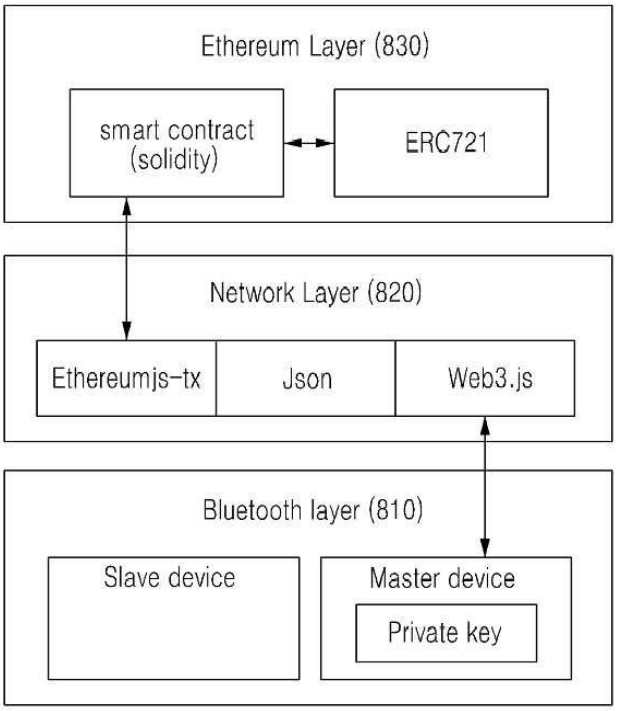
도면6


Wallet
Public Key: 0x35c2064CEf5206b59a6e88139cCe38307cB248
Private Key: 3271eb1ac3584df253a325c7b87a2977e7617d27f1510fea36f71818e76363e5
NFT1
NFT2
NFT3
ID:[TV] UN55j5920
ID:[AirPod] CD43H2452
ID:[Watch] KG23D5933
MAC: FC:F2:36:11:40:48
MAC: FC:F1:24:13:20:28
MAC: FK:U3:26:41:20:53

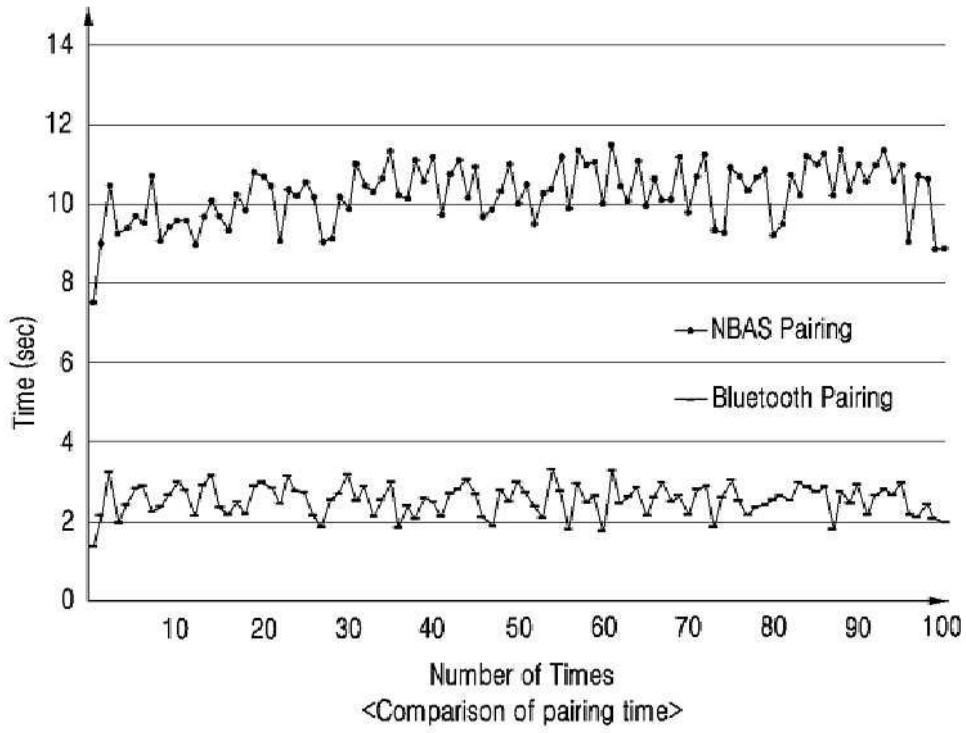
도면7


Master
710
Slave
Ethereum
NFT Transmission Request with the Public Key of another Master Device
Private Key Request
720
Private Key Transfer
730
NFT Transfer Success
740

도면8

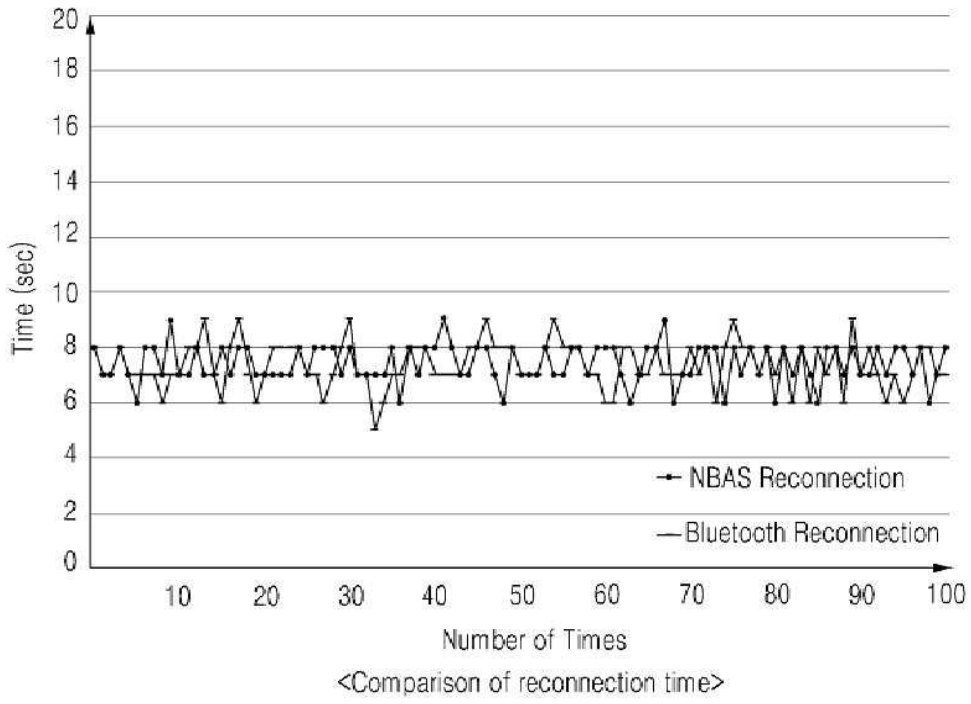

Ethereum Layer (830)
smart contract (solidity)
ERC721
Network Layer (820)
Ethereumjs-tx
Json
Web3.js
Bluetooth layer (810)
Slave device
Master device
Private key

도면9



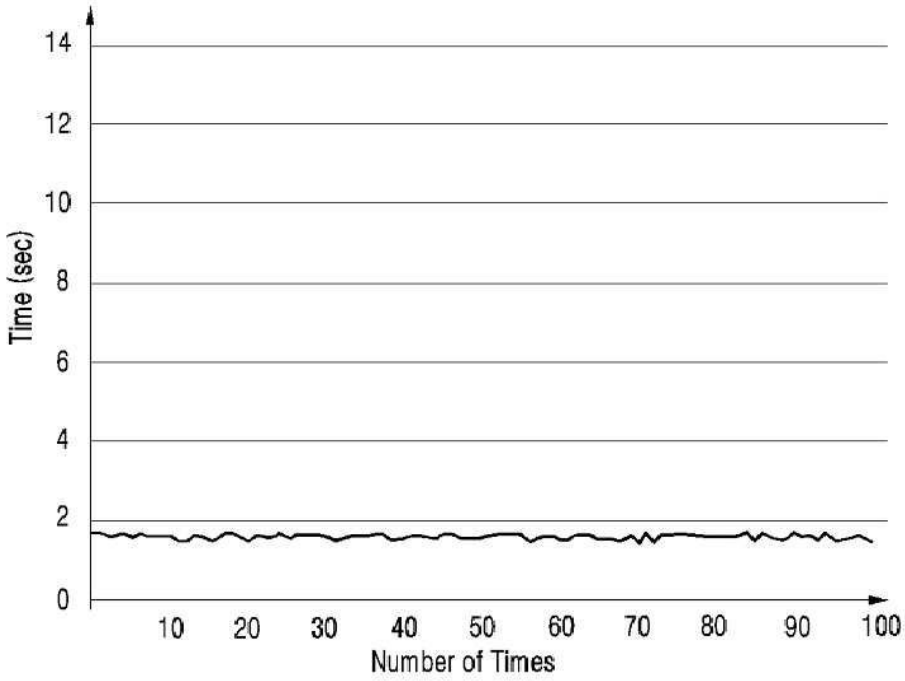
<Comparison of pairing time>

도면10



<Comparison of reconnection time>

도면11



<Rejection time for unauthorized device pairing>