

명세서

발명의 명칭: 금융 서비스를 지원하는 장치 및 그 통합 시스템

기술분야

- [1] 본 발명은 금융 서비스를 지원하는 장치에 관한 것이다. 또한 본 발명은 QR code, blockchain, DeFi(분산 금융), NFT(대체 불가능 토큰), metaverse 등의 기술을 금융 서비스에 접목시킨 통합 시스템을 제안한다.
- [2] 또한 본 발명은 블록체인 기반의 금융 서비스 제공 방법 및 장치에 관한 것으로서, 더욱 상세하게는 처리 시간의 지연 없이 실시간으로 수행되는 블록체인 기반의 암호화폐를 통해 결제를 수행하거나 환전하는 서비스를 제공하는 방법 및 장치에 관한 것이다.
- [3] 또한 본 발명은 계좌 개설 과정에서, 신분증의 위조/변조를 판단하고, 신분증 소지자의 안면과 및 신분증 사진의 안면을 비교하여 신분증 소지자의 신원을 인증하는 ATM 기기 및 그 동작 방법에 관한 것이다.
- [4] 또한 본 발명은 QR 코드를 이용한 전자출입관리 시스템에 관한 것이다.

배경기술

- [5] 최근 다양한 보험 서비스나 은행 서비스 등 금융 서비스와 관련된 상품이 증가함에 따라 많은 사람들이 각 상품에 대한 비교 또는 분석 등을 통해 자신에게 필요한 상품을 찾아 가입하고 있다. 이와 같은 과정에서 사람들은 각 상품의 내용을 직접 확인하고 비용 등을 산출하여 확인하기 위해 가입을 진행하지는 않더라도 자신의 상황과 관련된 정보를 이용하여 각 상품을 조회하는 과정을 갖게 된다.
- [6] 특히, 금융 서비스의 상품을 조회하는 과정에서는 개인의 민감한 정보인 개인정보를 이용하게 될 수 있고, 이를 위해 개인은 각 상품을 조회할 때마다 동일한 안내 문구, 약관 등을 확인 후 매번 동의 여부 의사를 체크 등의 방식으로 제공하게 된다.
- [7] 이와 같은 과정은 금융 서비스 또는 해당 금융 서비스를 제공하는 제공자(예를 들어, 보험 회사와 같은 서비스 제공 업체 등 금융 서비스 제공 업체 등)가 달라질 경우, 거의 동일한 안내 문구 및 약관 등을 확인 후 동의 여부 의사를 제공해야하고, 동일한 제공자의 서비스일지라도 서로 다른 보험 서비스 등 금융 서비스일 경우, 다시 동일한 동의 여부 의사를 제공해야하는 과정이 반복될 수 있다.
- [8] 이는, 보험 서비스나 등 금융 서비스의 종류가 증가할수록 사람들에게 번거롭고 반복적인 과정을 수행해야만 해당 서비스의 상품을 조회할 수 있고, 가입하는 과정까지의 번거로움이나 수고가 매우 증가할 수 있다. 이와 관련하여 금융 서비스를 자신의 상황을 고려하여 추천하는 기술 등은 상당히 제안되고 있으나, 금융 서비스에 사용되는 양식의 통합과 관련된 기술 등은 다소 부족한

문제가 있다.

- [9] 또한 IT 기술과 비즈니스 모델의 진화, 스마트 결제의 트렌드가 확산됨에 따라 비공식적인 암호화폐(crypto currency)가 출현하게 되었다. 대표적인 암호화폐로 비트코인이 최근 몇 년간 이슈화되고 있으며, 이와 같은 이유는 기존의 디지털 화폐와 달리 중앙 은행이 발행하는 법정 통화의 대체를 목적으로 한다는 점이 있을 수 있다. 또한, 거래소의 파산이나 탈세, 자금 세탁, 마약 거래 등의 불법 행위에 활용되는 점도 그 원인의 하나라고 할 수 있다.
- [10] 구체적으로, 비트코인은 전 세계 사용자의 컴퓨터를 개별적으로 연결한 네트워크에 기반하고 있으며, 발행 기관이 존재하지 않고 익명성이 보장되며, 비트코인이 온오프라인 공간에서 지급 결제 수단으로 사용됨에 따라 국적을 초월한 발행 및 유통 시스템으로 환전이나 신용카드 없이 인터넷만 연결되어 있으면 직접 거래가 가능하다는 점은 편리함과 비용 절감이라는 점에서 유용한 교환 및 지불 수단이라고 할 수 있다.
- [11] 또한, 비트코인은 일본에서 2014년 시내에서 전용의 ATM을 이용하여 암호화폐와 법정 통화를 교환하는 거래를 허용함을 기반으로 환전 후 남은 금액을 비트코인으로 변환하는 기술로까지 발전하였다. 더불어, 향후 암호화폐는 법정 통화와의 교환성 향상, 온오프라인 사용처 확대 등 서로 다른 유형의 장점을 흡수하는 융합을 통해 효용성이 증가하고 사용자수가 확대될 것으로 전망되고 있다.
- [12] 그러나, 실제로 일반 수령이 가능한 교환가치가 있으며, 가치 척도와 가치 보장의 기능을 가지는 일반적인 통화나 결제 수단으로 사용되기 보다는 자산으로서 보유하고 있는 상황에 비추어보면 암호화폐는 통화 또는 그에 준하는 자금이나 지불 수단으로의 역할을 뒷받침하기 위한 연구 및 조사가 미비한 것이 현 실정이다.
- [13] 특히, 암호화폐를 통해 결제를 수행하거나 암호화폐를 이용하여 환전을 수행하는 경우, 암호화폐를 위한 전용의 ATM을 이용할 수 있다. 이때, 암호화폐를 결제나 환전에 사용하는 과정에서 확인(confirm) 절차가 수행되어야 하며, 이와 같은 확인 절차가 수행이 완료되는 경우에 암호화폐를 통한 결제나 환전이 최종적으로 완료될 수 있다. 다만, 암호화폐를 결제나 환전에 사용하는 과정에서 수행되는 확인 절차가 처리되기 위해서는 시간이 소요될 수 있고, 이로 인해 사용자는 암호화폐의 실시간 사용이 어려운 문제가 있다.

발명의 상세한 설명

기술적 과제

- [14] 본 발명은 금융 서비스에 QR코드, 블록체인, DeFi, 메타버스, NFT(대체 불가능 토큰) 등의 기술을 접목시키는데 그 목적이 있다.
- [15] 또한, 본 발명은 사용자 단말에 대응하는 QR 코드를 특정 위치에 설치된 키오스크마다 생성하고 관리할 수 있는 전자출입관리 시스템을 제안하는데 그

목적이 있다.

- [16] 또한, 본 발명은 사용자 단말에 대응하는 QR 코드의 스푸핑(Spoofing) 행위를 방지할 수 있는 전자출입관리 시스템을 제공하는데 그 목적이 있다.
- [17] 또한, 본 발명은 원본 QR 코드의 위변조 방지 및 무결성을 보장할 수 있는 전자출입관리 시스템을 제공하는데 그 목적이 있다.
- [18] 본 발명은 신분증의 위조/변조를 판단할 수 있고, 촬영 영상으로부터 사용자 안면을 인식하여, 인식된 사용자 안면과 신분증 내의 사용자 사진의 일치율을 계산할 수 있는 ATM 기기 및 그 동작 방법을 제공하는데 그 목적이 있다.
- [19] 또한, 본 발명은 처리 시간의 지연 없이 실시간으로 수행되는 블록체인 기반의 암호화폐를 통해 결제를 수행하거나 환전하는 서비스를 제공하는 방법 및 장치를 제공하는데 그 목적이 있다.

과제 해결 수단

- [20] 본 발명의 일 실시예는 금융 서비스를 지원하는 통합 시스템에 있어서, 금융 서비스를 지원하는 온라인 플랫폼이 실행되는 제1 단말; 및 상기 온라인 플랫폼을 운용하는 서버; 를 포함하고, 상기 서버는: 제1 사용자 정보를 상기 제1 단말로부터 수신하고, 상기 제1 사용자 정보에 기반하여 상기 제1 단말의 제1 사용자에게 대한 인증 절차를 수행하고, 상기 인증 절차의 결과에 기반하여 상기 제1 사용자에게 상기 금융 서비스를 제공할 지 여부를 결정하고, 상기 결정에 따라 상기 금융 서비스를 제공하기 위한 정보를 상기 제1 단말에게 전송하는, 통합 시스템을 제안한다.
- [21] 상기 통합 시스템은, 상기 온라인 플랫폼이 실행되는 제2 단말; 을 더 포함하고, 상기 금융 서비스는 DeFi(Decentralized Finance) 서비스를 포함하고, 상기 제1 단말은: 상기 제1 사용자 정보를 상기 제2 단말에 전달하고, 상기 제1 사용자 정보에 상응하는 블록체인 기반의 암호화 정보를 상기 제2 단말로부터 수신하고, 상기 암호화 정보를 복호화 할 수 있다.
- [22] 상기 통합 시스템은, 입력 모듈과 출력 모듈이 구비된 키오스크를 더 포함할 수 있다.
- [23] 상기 금융 서비스는 환전 서비스를 더 포함하고, 상기 키오스크는: 상기 입력 모듈을 통하여 촬영되는 제1 사용자의 신분증을 수집하고, 상기 신분증을 분석하여 상기 환전 서비스를 제공할지 여부를 결정할 수 있다.
- [24] 상기 키오스크는: 상기 신분증에 객체 추출 알고리즘을 적용하여 객체 정보를 획득하고, 상기 객체 정보에 기반하여 상기 환전 서비스를 제공할지 여부를 결정할 수 있다.
- [25] 상기 서버는: 상기 키오스크에 대한 정보 및 상기 제1 사용자 정보를 기반으로 상기 제1 QR 코드를 생성하고, 상기 제1 QR 코드를 상기 제1 단말에게 송신하고, 상기 제1 단말은 상기 서버로부터 수신한 제1 QR 코드를 표시하고, 상기 키오스크는 상기 제1 단말에 출력된 제1 QR 코드를 기반으로 출입 인증 여부를

판단할 수 있다.

- [26] 상기 키오스크는, 상기 신분증을 수집하기 위한 스캐너를 더 포함하고, 상기 제1 사용자 정보는, 상기 제1 사용자의 핸드폰번호 및 상기 제1 사용자의 신상정보를 포함할 수 있다.
- [27] 상기 서버는: 출입인증요청 신호를 상기 키오스크로부터 수신하면, 상기 제1 사용자 단말의 현재 위치좌표를 상기 제1 단말에게 요청하고, 상기 제1 단말의 현재 위치좌표 및 현재 표준시간 정보를 기반으로 제2 QR 코드를 생성하고, 상기 제2 QR 코드를 상기 키오스크 및 상기 제1 단말에게 송신하고, 상기 제1 단말은: 상기 제1 QR 코드와 상기 제2 QR 코드를 기반으로 제1 오버레이 QR 코드를 생성하고, 상기 제1 오버레이 QR 코드를 상기 키오스크에게 송신하고, 상기 키오스크는: 상기 제1 QR 코드와 상기 제2 QR 코드를 기반으로 제2 오버레이 QR 코드를 생성하고, 상기 제1 오버레이 QR 코드와 상기 제2 오버레이 QR 코드를 비교하여 출입인증여부를 판단할 수 있다.
- [28] 상기 제1 오버레이 QR 코드 및 상기 제2 오버레이 QR 코드는, 상기 제1 QR 코드 및 상기 제2 QR 코드의 위치 검출용 패턴을 동일 축(axis) 상에 위치시키고, 상기 제1 QR 코드 및 상기 제2 QR 코드의 각 셀을 비교하여 동일한 셀은 흑색 셀로 설정하고, 동일하지 않은 셀은 백색 셀로 설정하여 생성될 수 있다.
- [29] 상기 통합 시스템은, 기 설정된 복수의 특정 위치에 설치되는 복수의 키오스크를 포함하고, 상기 제1 단말은, 상기 복수의 단말 각각에 대응하는 복수의 제1 QR 코드를 구분하여 저장할 수 있다.
- [30] 본 발명의 일 실시예에 따른 시스템은 기 설정된 특정 위치에 설치되어, 사용자 정보를 입력받고, 사용자 단말에 출력된 제1 QR 코드를 기반으로 출입 인증 여부를 판단하는 키오스크, 관리자 서버로부터 수신한 상기 제1 QR 코드를 출력하는 사용자 단말 및 상기 키오스크로부터 상기 사용자 정보를 수신하고, 상기 키오스크 정보 및 상기 사용자 정보를 기반으로 상기 제1 QR 코드를 생성하고, 상기 제1 QR 코드를 상기 사용자 단말에게 송신하는 관리자 서버를 포함할 수 있다.
- [31] 이 때, 상기 키오스크는, 신분증에서 사용자의 신상정보를 추출하는 신분증 스캐너를 더 포함하고, 상기 사용자 정보는, 상기 사용자의 핸드폰번호 및 상기 사용자의 신상정보일 수 있다.
- [32] 이 때, 상기 관리자 서버는 상기 키오스크로부터 출입인증요청 신호를 수신하면, 상기 사용자 단말의 현재 위치좌표를 요청하고, 상기 사용자 단말의 현재 위치좌표 및 현재 표준시간 정보를 기반으로 제2 QR 코드를 생성하고, 상기 제2 QR 코드를 상기 키오스크 및 상기 사용자 단말에게 송신하고, 상기 사용자 단말은, 상기 제1 QR 코드와 상기 제2 QR 코드를 기반으로 제1 오버레이 QR 코드를 생성하고, 상기 제1 오버레이 QR 코드를 상기 키오스크에게 송신하고, 상기 키오스크는, 상기 제1 QR 코드와 상기 제2 QR 코드를 기반으로 제2 오버레이 QR 코드를 생성하고, 상기 제1 오버레이 QR 코드와 상기 제2

오버레이 QR 코드를 비교하여 출인인증 여부를 판단할 수 있다.

- [33] 이 때, 상기 제1 오버레이 QR 코드 및 상기 제2 오버레이 QR 코드는, 상기 제1 QR 코드 및 상기 제2 QR 코드의 위치 검출용 패턴을 동일 축 상에 위치시키고, 상기 제1 QR 코드 및 상기 제2 QR 코드의 각 셀을 비교하여 동일한 셀은 흑색 셀로 설정하고, 동일하지 않은 셀은 백색 셀로 설정하여 생성될 수 있다.
- [34] 이 때, 상기 키오스크는, 기 설정된 하나 이상의 특정 위치에 하나 이상 설치되고, 상기 사용자 단말은, 상기 키오스크 각각에 대응하는 하나 이상의 제1 QR 코드를 구분하여 저장할 수 있다.
- [35] 본 발명의 일 실시예에 따른 키오스크는 상기 서비스를 이용하는 사용자로부터 입력된 거래 금액에 대한 암호화폐의 수량을 산출하고, 상기 산출된 암호화폐의 수량에서 수수료를 제외한 나머지 수량의 암호화폐를 복수의 암호화폐 거래소들 중 가장 높은 거래가를 가지는 암호화폐 거래소로 전송하는 입출력부, 상기 사용자의 신분증 또는 여권의 위변조 여부 판별을 통해 본인인 것으로 확인되는 경우 상기 거래 금액에 대응되는 수량의 암호화폐를 매도하고, 상기 암호화폐로 변환되는 거래 금액에 대응되는 환전용 암호화폐를 환전용 암호화폐 거래소에서 매도하는 환전용 암호화폐 운영부 및 상기 환전용 암호화폐의 매도를 통해 획득된 금액을 상기 서비스 제공 장치가 설치된 가맹점을 운영하는 운영자의 계좌로 송금하는 금액 송금부를 포함한다.
- [36] 여기서, 상기 입출력부는 상기 사용자로부터 언어의 종류 및 통화의 종류를 선택받고, 상기 선택된 종류의 언어 및 상기 선택된 통화의 종류를 기반으로 상기 금융 서비스를 제공할 수 있다.
- [37] 여기서, 상기 입출력부는 상기 산출된 수량의 암호화폐를 송금할 지갑주소를 식별코드로 출력하고, 상기 식별코드를 리딩 또는 스캔한 상기 사용자의 사용자 단말을 통하여 상기 지갑주소로 상기 출력된 수량의 암호화폐가 입금되었는지의 여부를 확인하고, 상기 암호화폐가 입금된 경우 입금 이벤트를 생성하여 출력할 수 있다.
- [38] 여기서, 상기 서비스 제공 장치는 미리 연동된 스캐너를 통해 상기 신분증 또는 여권을 스캔하고, 스캔된 상기 신분증 또는 여권의 위변조 여부를 판별하여 상기 사용자의 본인여부를 확인하고, 상기 금융 서비스의 확인(CONFIRM) 절차가 정상적으로 완료되는 경우 상기 신분증 또는 여권에 대한 정보를 삭제할 수 있다.
- [39] 여기서, 상기 서비스 제공 장치는 상기 환전용 암호화폐의 낙폭이 미리 설정된 기준보다 높은 경우, 서킷 브레이크가 수행될 수 있다.
- [40] 본 발명의 일 실시예에 따른 시스템의 동작 방법은, 상기 서비스 제공 장치의 입출력부를 통해 상기 서비스를 이용하는 사용자로부터 입력된 거래 금액에 대한 암호화폐의 수량을 산출하고, 상기 산출된 암호화폐의 수량에서 수수료를 제외한 나머지 수량의 암호화폐를 복수의 암호화폐 거래소들 중 가장 높은 거래가를 가지는 암호화폐 거래소로 전송하는 단계, 상기 서비스 제공 장치의

환전용 암호화폐 운영부를 통해 상기 사용자의 신분증 또는 여권의 위변조 여부를 판별을 통해 본인인 것으로 확인되는 경우 상기 거래 금액에 대응되는 수량의 암호화폐를 매도하고, 상기 암호화폐로 변환되는 거래 금액에 대응되는 환전용 암호화폐를 환전 암호화폐 거래소에서 매도하는 단계 및 상기 서비스 제공 장치의 금액 송금부를 통해 상기 환전용 암호화폐의 매도를 통해 획득된 금액을 상기 서비스 제공 장치가 설치된 가맹점을 운영하는 운영자의 계좌로 송금하는 단계를 포함한다.

- [41] 여기서, 상기 동작 방법은 상기 입출력부를 통해 상기 사용자로부터 언어의 종류 및 통화의 종류를 선택받고, 상기 선택된 종류의 언어 및 상기 선택된 통화의 종류를 기반으로 상기 금융 서비스를 제공하는 단계를 포함할 수 있다.
- [42] 여기서, 상기 동작 방법은 상기 입출력부를 통해 상기 산출된 수량의 암호화폐를 송금할 지갑주소를 식별코드로 출력하고, 상기 식별코드를 리딩 또는 스캔한 상기 사용자의 사용자 단말을 통하여 상기 지갑주소로 상기 출력된 수량의 암호화폐가 입금되었는 지의 여부를 확인하고, 상기 암호화폐가 입금된 경우 입금 이벤트를 생성하여 출력하는 단계를 포함할 수 있다.
- [43] 여기서, 상기 동작 방법은 상기 서비스 제공 장치와 미리 연동된 스캐너를 통해 상기 신분증 또는 여권을 스캔하고, 스캔된 상기 신분증 또는 여권의 위변조 여부를 판별하여 상기 사용자의 본인여부를 확인하고, 상기 금융 서비스의 확인(CONFIRM) 절차가 정상적으로 완료되는 경우 상기 신분증 또는 여권에 대한 정보를 삭제하는 단계를 포함할 수 있다.
- [44] 여기서, 상기 동작 방법은 상기 서비스 제공 장치를 통해 상기 환전용 암호화폐의 낙폭이 미리 설정된 기준보다 높은 경우, 서킷 브레이크가 수행되는 단계를 포함할 수 있다.
- [45] 다양한 실시예들에 따라서, 결제, 입출금, 환전, 충전 및 해외 송금 기능을 지원하는 ATM(Automated Teller Machine) 기기는, 디스플레이, 통신 인터페이스, 카메라 모듈, 신분증 스캐너, 및 프로세서를 포함하고, 상기 프로세서는, 사용자로부터 계좌 개설 요청을 수신하는 것에 응답하여, 상기 신분증 스캐너를 이용하여 상기 사용자의 신분증을 스캔함으로써, 상기 신분증의 위조/변조 여부를 판단하고, 상기 신분증이 위조/변조되지 않은 것으로 판단하는 경우, 상기 신분증이 유효한지를 문의하기 위하여 상기 통신 인터페이스를 이용하여 상기 신분증으로부터 추출된 신분증 식별 정보 및 사용자 사진을 외부 서버에게 송신하고, 상기 외부 서버로부터 상기 신분증이 유효함을 나타내는 응답을 수신하는 경우, 상기 카메라 모듈을 이용하여 촬영된 프리뷰 영상(preview image)을 상기 디스플레이 상에 표시하고, 안면 인식(face recognition)을 위한 인공지능 모델을 이용하여 상기 프리뷰 영상 내에서 사용자 안면을 인식하고, 상기 사용자 안면이 페이크 영상(fake image)인지를 판단하기 위한 라이브니스 검출(liveness detection)을 수행하고, 상기 라이브니스 검출을 수행한 결과 상기 사용자 안면이 페이크 영상이 아닌 것으로 판단하는 경우, 상기 프리뷰

영상으로부터 특정 영상을 캡처(capture)하고, 안면들 사이의 일치율을 산출하기 위한 인공지능 모델을 이용하여 상기 캡처된 특정 영상 내의 상기 사용자 안면과 상기 사용자 사진 내의 기준 안면 사이의 일치율을 계산하고, 및 상기 일치율이 미리 정해진 제1 임계치 이상에 해당하는 경우, 상기 사용자에게 대한 계좌 개설과 관련된 QR코드를 생성하고, 상기 통신 인터페이스를 통하여 상기 QR코드를 상기 사용자의 사용자 장치에게 송신하도록 설정될 수 있다.

[46] 상기 프로세서는, 상기 신분증의 종류를 판단하고, 및 미리 등록된 복수의 외부 서버들 중에서 상기 신분증의 종류에 대응하는 상기 외부 서버로 상기 신분증 식별 정보 및 상기 사용자 사진을 송신하도록 설정될 수 있다.

[47] 상기 프로세서는, 상기 외부 서버로부터 상기 신분증이 유효함을 나타내는 응답을 수신하는 경우, 상기 미리 정해진 가이드 영역을 통하여 상기 프리뷰 영상의 상기 일부 영상을 표시하면서, 상기 미리 정해진 가이드 영역 이외의 상기 디스플레이 내의 나머지 영역을 비활성화하고, 및 상기 나머지 영역을 비활성화한 시점으로부터 미리 정해진 시간 동안 상기 미리 정해진 가이드 영역 내에 표시된 상기 일부 영상으로부터 상기 사용자 안면이 인식되지 않은 경우, 상기 나머지 영역의 상태를 비활성화 상태에서 활성화 상태로 전환하고, 상기 디스플레이의 전체 영역에 표시된 상기 프리뷰 영상으로부터 상기 사용자 안면을 인식하도록 설정될 수 있다.

[48] 상기 프로세서는, 상기 사용자 안면과 상기 기준 안면 사이의 상기 일치율을 계산하는 동안, 상기 프리뷰 영상의 표시를 중단하고, 상기 캡처된 특정 영상을 상기 디스플레이 상에 표시하도록 설정될 수 있다.

[49] 상기 프로세서는, 상기 일치율이 상기 미리 정해진 제1 임계치 미만이고, 미리 정해진 제2 임계치 이상에 해당하는 경우, 상기 캡처된 특정 영상의 표시를 중단하고, 상기 카메라 모듈을 이용하여 새로이 촬영된 프리뷰 영상을 상기 디스플레이 상에 표시하고, 상기 새로이 촬영된 프리뷰 영상을 이용하여 상기 기준 안면과의 일치율을 새로이 계산하도록 설정될 수 있다.

[50] 상기 프로세서는, 상기 일치율이 상기 미리 정해진 제2 임계치 미만에 해당하는 경우, 상기 ATM 기기와 연동되는 콜센터가 상기 사용자의 신원 정보를 인증하도록 하는 요청을 상기 콜센터에 등록하고, 상기 콜센터로부터 상기 사용자의 신원 인증 성공 응답을 수신하는 경우, 상기 사용자가 특정 서버에 등록된 위험 인물 리스트에 포함되었는지 여부를 확인하고, 및 상기 사용자가 상기 위험 인물 리스트에 포함되어 있지 않은 경우, 상기 QR코드를 생성하고, 상기 QR코드를 상기 사용자의 사용자 장치에게 송신하도록 설정될 수 있다.

발명의 효과

[51] 본 발명에 의하면, 암호화폐가 다양한 유형의 금융상품 및 통화로서의 기능을 할 수 있도록 사용자가 선택한 종류의 법정통화와 암호화폐 간의 실시간 시세와 현지통화 간의 환율에 근거하여 현지의 상품을 구매할 수 있도록 하되, 신분증의

진위여부 및 성인인증을 한 후 가맹점 또는 자판기로의 접근을 허용하며, 회원별 및 연령별로 회원의 마일리지나 구매가능 상품을 관리하고, 각 가맹점을 노드로 하는 프라이빗 블록체인을 생성하여 재고관리 및 회원관리를 포함한 분산장부를 공유하도록 함으로써, 전자지갑, 다른 유형의 암호화폐 통합 및 교환 서비스, 온라인 암호화폐 거래소, 암호화폐 ATM 등 새로운 비즈니스 모델로 진화할 수 있는 토대를 마련하여, 암호화폐 관련 사업으로의 확대 및 발전에 기여할 수 있다.

- [52] 특히, 사용자가 암호화폐를 기반으로 제공 가능한 결제 서비스 또는 환전 서비스를 이용하는 과정에서 처리 시간에 소요되는 시간을 감소시킬 수 있으며, 이를 통해 암호화폐 기반의 결제 서비스 및 환전 서비스가 최대한 실시간으로 제공될 수 있는 효과가 있다.
- [53] 또한, 본 발명에 의하면, 계좌 개설 과정 중에 제출된 신분증의 위조/변조 여부를 1차적으로 자체 검증하고, 신분증으로부터 추출된 식별 정보와 사용자 사진을 외부 서버에게 송신하여 2차적으로 위조/변조 여부를 검증할 수 있으며, 촬영 영상으로부터 인식된 사용자 안면이 페이크 영상(fake image)인지 여부를 판단한 후, 인식된 사용자 안면과 사용자 사진의 일치율을 계산함으로써, 신뢰도 있는 신원 확인 결과를 제공할 수 있다.
- [54] 또한, 본 발명에 의하면, 사용자 단말에 대응하는 QR 코드를 특정 위치에 설치된 키오스크마다 생성하여 보관할 수 있다.
- [55] 또한, 본 발명에 의하면, 사용자 단말에 대응하는 QR 코드의 스푸핑(Spoofing) 행위를 방지할 수 있는 전자출입관리 시스템을 제공할 수 있다.
- [56] 또한, 본 발명에 따르면, 원본 QR 코드의 위변조 방지 및 무결성을 보장할 수 있는 전자출입관리 시스템을 제공할 수 있다.

도면의 간단한 설명

- [57] 도 1 및 도 2는 본 발명의 일 실시예에 따른 통합 시스템을 나타내는 도면이다.
- [58] 도 3은 본 발명의 일 실시예에 따른 통합 시스템을 나타내는 블록도이다.
- [59] 도 4는 본 발명의 일 실시예에 따른 키오스크의 동작을 설명하기 위한 도면이다.
- [60] 도 5 및 도 6은 본 발명의 일 실시예에 따른 통합 시스템의 동작을 나타내는 흐름도이다.
- [61] 도 7은 본 발명의 일 실시예에 따른 제어 모듈을 나타내는 블록도이다.
- [62] 도 8은 본 발명의 일 실시예에 따른 통합 시스템의 동작을 나타내는 흐름도이다.

발명의 실시를 위한 형태

- [63] 도 1은 본 발명의 일 실시예에 따른 통합 시스템을 나타내는 도면이다.
- [64] 도 1을 참조하면, 본 발명의 일 실시예에 따른 통합 시스템(10)은 서버(20), 제1 단말(30) 및/또는 제2 단말(40)을 포함할 수 있다.

- [65] 서버(20)는 본 발명의 금융 서비스 플랫폼을 운용하는 장치로써, 상기 금융 서비스 플랫폼은 웹사이트 및/또는 모바일 앱을 통하여 제공되는 온라인 서비스이거나, 키오스크(50)를 통하여 제공되는 서비스를 위한 플랫폼일 수 있다.
- [66] 예를 들어, 제1 단말(30) 및/또는 제2 단말(40)은 휴대성과 이동성이 보장되는 무선 통신 장치로서, 네비게이션, 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(WCode Division Multiple Access), Wibro(Wireless Broadband Internet) 단말, 스마트폰(smartphone), 스마트 패드(smartpad), 태블릿 PC(Tablet PC) 등과 같은 모든 종류의 핸드헬드(Handheld) 기반의 무선 통신 장치를 포함할 수 있다.
- [67] 또한, 제1 단말(30) 및/또는 제2 단말(40)은 네트워크를 통하여 원격지의 서버나 단말에 접속할 수 있는 컴퓨터로 구현될 수 있다. 예를 들어, 컴퓨터는 네비게이션, 웹 브라우저(WEB Browser)가 탑재된 노트북, 데스크톱(Desktop), 랩톱(Laptop) 등을 포함할 수 있다. 이때, 제1 단말(30) 및/또는 제2 단말(40)은 네트워크를 통해 원격지의 서버나 단말에 접속할 수 있는 단말로 구현될 수 있다.
- [68] 또한 본 발명의 금융 서비스 플랫폼은 QR(Quick Response) 코드, 블록체인(blockchain), DeFi(Decentralized Finance), NFT(non-fungible token), 메타버스(metaverse) 등의 기술을 이용하여 금융 서비스의 고객인 사용자에게 금융 서비스를 제공하는데 그 목적이 있다.
- [69] DeFi(탈 중앙화 금융 or 분산 경제)는 중개, 거래소 또는 은행 과 같은 중앙 금융 중개자에 의존하지 않고, 대신 블록 체인에서 스마트 계약을 활용하는 블록 체인 기반의 금융 형태이다. DeFi를 통해 사람들은 다른 사람에게 자금을 빌리고, 파생 상품을 사용하여 자산의 가격 변동을 예측할 수 있다. 또한, 암호 화폐를 거래하고, 위험에 대비하며, 저축과 같은 계정에서 이자를 얻을 수 있다.
- [70] DeFi는 블록체인에서 금융 기능을 수행하는 DApp(Decentralized Application, 분산형 애플리케이션)으로 알려진 애플리케이션을 중심으로 전개된다. 중앙의 중개자와 거래가 이루어지지 않고 스마트 계약 프로그램에 의해 참여자 간에 중재되어 직접 거래가 이루어진다. 이런 시스템을 바탕으로, DApp에서 다수를 연결하고 함께 작동하여 복잡한 금융 서비스를 만들 수 있다. 예를 들어 스테이블 코인 보유자는 Aave와 같은 유동성 풀에 자산을 위탁할 수 있다. 다른 사람들은 일반적으로 대출 금액보다 더 많은 추가 담보를 제공해야 풀에서 빌릴 수 있는 것에 비하면 큰 이점이라 할 수 있다. 프로토콜은 자산에 대한 순간적 수요에 따라 이자율을 자동으로 조정한다. Aave는 또한 "플래시 론"을 시장에 내놓았는데, 이는 임의의 금액이 담보화 되지 않은 대출로 몇 분 내에 회수되고

상환된다. 차익 거래, 담보 스왑 및 자기 청산과 같은 대출에 대한 합법적인 용도가 있을 수 있지만 DeFi 플랫폼은 암호 화폐 현물 가격의 단기 조작에 플래시 대출을 사용하는 등 악용되기도 했다. "분권화"는 곧 중앙 거래소가 없다는 것을 의미한다. DeFi 프로그램은 개발자 및 프로그래머 커뮤니티에서 오픈 소스 소프트웨어를 사용하여 실행된다.

- [71] DeFi 프로토콜의 한 예시는 이더리움 블록 체인에서 실행된다. 더 자세히 말하면, 이더리움 블록 체인에서 발행되는 수백 개의 디지털 토큰 거래를 허용하는 분산형 거래소이다. Uniswap의 알고리즘은 사용자가 유동성을 제공하는 사람들에게 거래 수수료를 내게 함으로써, 토큰에 대한 유동성 풀을 형성하도록 장려한다. 개발 팀은 Uniswap에 배포할 소프트웨어를 작성한다. 그러나 플랫폼은 궁극적으로 사용자가 관리한다. 또한, 위치 규제 기관이 Uniswap과 같은 플랫폼의 합법성을 취할지는 명확하지 않다.
- [72] NFT(대체 불가능 토큰)는 블록체인에 저장된 데이터 단위로, 고유하면서 상호 교환할 수 없는 토큰을 의미할 수 있다. 또한 NFT는 사진, 비디오, 오디오 및 기타 유형의 디지털 파일을 나타내는데 사용될 수 있다.
- [73] 메타버스(metaverse) 또는 확장 가상 세계는 가상, 초월 의미인 '메타'(meta)와 세계, 우주 의미인 '유니버스'(universe)를 합성한 신조어다. '가상 우주'라고 번역하기도 했다. 이는 3차원에서 실제 생활과 법적으로 인정되는 활동인 직업, 금융, 학습 등이 연결된 가상 세계를 뜻한다. 구체적으로, 정치와 경제, 사회, 문화의 전반적 측면에서 현실과 비현실이 공존하는 생활형, 게임형 가상 세계라는 의미로 폭넓게 사용한다.
- [74] 도 2는 본 발명의 일 실시예에 따른 통합 시스템을 나타내는 도면이다.
- [75] 도 2를 참조하면 본 발명의 일 실시예에 따른 통합 시스템(10)은 서버(20), 제1 단말(30) 및/또는 키오스크(50)를 포함할 수 있으며, 도 2에 도시되어 있지 않으나 제2 단말(40)과 같은 다른 단말을 더 포함할 수도 있다.
- [76] 키오스크(50)는 제1 단말(30) 및/또는 제2 단말(40)의 사용자의 신분을 확인(또는 본인 확인 또는 신분 확인)할 필요가 있는 위치 또는 장치 내부(예; ATM 기기 내부), 출입을 관리하고자 하는 장소의 출입구 등에 설치되어 실시될 수 있다. 또한, 본 발명의 일 실시예는 출입자의 신원정보를 기반으로 출입 허용 여부를 판단하여 출입구의 잠금장치를 제어할 수도 있고, 또는 출입자의 신원정보를 기재하는 출입명부를 생성할 수도 있다.
- [77] 이 때, 키오스크(50)는 기 설정된 특정 위치에 하나 이상 설치될 수 있고, 출입하려고 하는 출입자로부터 사용자 정보를 입력받을 수 있고, 제1 단말(30)에 출력된 제1 QR 코드를 기반으로 출입 인증 여부를 판단할 수 있다.
- [78] 이 때, 키오스크(50)는 사전적 의미의 키오스크에 한정되지 않고, 컴퓨터, 스마트폰, 핸드폰, 스마트 TV, 셋톱박스(set-top box), 태블릿 PC 등 통신이 가능하고 제1 단말(30) 및/또는 제2 단말(40)에 출력된 QR 코드를 인식할 수 있는 모든 장치가 포함될 수 있다. 여기서 컴퓨터는 노트북 컴퓨터(laptop computer),

데스크톱 등을 포함할 수 있다.

- [79] 도 3은 본 발명의 일 실시예에 따른 통합 시스템을 나타내는 블록도이다.
- [80] 도 3을 참조하면, 서버(20)는 제1 제어 모듈(110), 제1 통신 모듈(120), 제1 입력 모듈(130), 제1 출력 모듈(140) 및/또는 저장 모듈(150)을 포함할 수 있으며, 상기 서버(20)는 본 발명의 일 실시예에 따른 금융 서비스 플랫폼을 운용하는 서버일 수 있다.
- [81] 제1 단말(30) 및/또는 제2 단말(40) 각각은 제2 제어 모듈(160), 제2 통신 모듈(170), 제2 입력 모듈(180), 제2 출력 모듈(190) 및/또는 내부 배터리(미도시)를 포함할 수 있다.
- [82] 키오스크(50)는 제2 제어 모듈(210), 제2 통신 모듈(220), 제2 입력 모듈(230), 제2 출력 모듈(240) 및/또는 내부 배터리(미도시)를 포함할 수 있다.
- [83] 제어 모듈(110, 160, 210)은 본 발명의 일 실시예에 따른 동작/단계/과정을 구현할 수 있도록 서버(20), 제1 단말(30), 제2 단말(40) 및/또는 키오스크(50)을 직/간접적으로 제어할 수 있다. 또한 제어 모듈(110, 160, 210)은 적어도 하나의 프로세서를 포함할 수 있으며, 프로세서는 적어도 하나의 중앙 처리 유닛(CPU) 및/또는 적어도 하나의 그래픽 처리 디바이스(GPU)를 포함할 수 있다.
- [84] 또한 제어 모듈(110, 160, 210)은 API(Application Programming Interface), IoT(Internet of Things), IIoT(Industrial Internet of Things), ICT(Information & Communication Technology) 기술에 기반하여 제어 정보(예; 명령어) 등을 생성하거나 및/또는 관리할 수 있다.
- [85] 통신 모듈(120, 170, 220)은 서버(20), 제1 단말(30), 제2 단말(40) 및/또는 키오스크(50) 등과 각종 데이터, 신호, 정보를 송수신할 수 있다. 또한, 통신 모듈(120, 170, 220)은 무선 통신 모듈(예: 셀룰러 통신 모듈, 근거리 무선 통신 모듈, 또는 GNSS(global navigation satellite system) 통신 모듈) 또는 유선 통신 모듈(예: LAN(local area network) 통신 모듈, 또는 전력선 통신 모듈)을 포함할 수 있다. 또한, 통신 모듈(120, 170, 220)은 제1 네트워크(예: 블루투스, WiFi direct 또는 IrDA(Infrared Data Association) 같은 근거리 통신 네트워크) 또는 제2 네트워크(예: 셀룰러 네트워크, 인터넷, 또는 컴퓨터 네트워크(예: LAN 또는 WAN)와 같은 원거리 통신 네트워크)를 통하여 외부 전자 장치와 통신할 수 있다. 이런 여러 종류의 통신 모듈들은 하나의 구성 요소(예: 단일 칩)로 통합되거나, 또는 서로 별도의 복수의 구성 요소들(예: 복수 칩들)로 구현될 수 있다.
- [86] 또한 본 발명의 통신 모듈(120, 170, 220)은 통신표준 기술에 기반하여 동작할 수 있다.
- [87] 입력 모듈(130, 180)은 서버(20), 제1 단말(30), 제2 단말(40) 및/또는 키오스크(50)의 구성요소(예: 제어 모듈(110) 등)에 사용될 명령 또는 데이터를 서버(20) 및/또는 제1 단말(30)의 외부(예: 사용자(예; 제1 사용자, 제2 사용자 등), 서버(20)의 관리자 등)로부터 수신할 수 있다. 또한, 입력 모듈(130, 180)은

서버(20), 제1 단말(30), 제2 단말(40) 및/또는 키오스크(50)에 설치된 터치인식가능 디스플레이, 터치패드, 버튼형 인식 모듈, 음성인식센서, 마이크, 마우스, 또는 키보드 등을 포함할 수 있다. 여기서 터치인식가능 디스플레이, 터치패드, 버튼형 인식 모듈은 감압식 및/또는 정전식 방식을 통하여 사용자의 신체(예; 손가락)를 통한 터치를 인식할 수 있다.

- [88] 출력 모듈(140, 190, 240)은 서버(20), 제1 단말(30), 제2 단말(40) 및/또는 키오스크(50)의 제어 모듈(110, 160, 210)에 의해 생성되거나 통신 모듈(120, 170, 220)을 통하여 획득된 신호(예; 음성 신호), 정보, 데이터, 이미지, 및/또는 각종 객체(object) 등을 표시하는 모듈이다. 예를 들면, 출력 모듈(140, 190, 240)은 스크린, 표시부(displaying unit), 스피커 및/또는 발광장치(예; LED 램프) 등을 포함할 수 있다.
- [89] 저장 모듈(150)은 서버(20), 제1 단말(30), 제2 단말(40) 및/또는 키오스크(50)의 동작을 위한 기본 프로그램, 응용 프로그램, 설정 정보 등의 데이터를 저장한다. 또한, 저장 모듈은 플래시 메모리 타입(Flash Memory Type), 하드 디스크 타입(Hard Disk Type), 멀티미디어 카드 마이크로 타입(Multimedia Card Micro Type), 카드 타입의 메모리(예를 들면, SD 또는 XD 메모리 등), 자기 메모리, 자기 디스크, 광디스크, 램(Random Access Memory, RAM), SRAM(Static Random Access Memory), 롬(Read-Only Memory, ROM), PROM(Programmable Read-Only Memory), EEPROM(Electrically Erasable Programmable Read-Only Memory) 중 적어도 하나의 저장매체를 포함할 수 있다.
- [90] 또한, 저장 모듈(150)은 서버(20), 제1 단말(30), 제2 단말(40) 및/또는 키오스크(50)을 사용하는 고객(제1 사용자)의 개인정보, 관리자(제2 사용자)의 개인정보 등을 저장할 수 있다. 여기서 개인정보는 이름, 아이디(ID; identifier), 패스워드, 도로명 주소, 전화 번호, 휴대폰 번호, 이메일 주소, 및/또는 서버(20)에 의해 생성되는 리워드(reward)(예; 포인트 등)를 나타내는 정보 등을 포함할 수 있다. 또한, 제어 모듈(110, 160, 210)은 상기 저장 모듈(150)에 저장된 각종 이미지, 프로그램, 콘텐츠, 데이터 등을 이용하여 다양한 동작을 수행할 수 있다.
- [91] 도 4는 본 발명의 일 실시예에 따른 키오스크의 동작을 설명하기 위한 도면이다.
- [92] 도 5는 본 발명의 일 실시예에 따른 통합 시스템의 동작을 나타내는 흐름도이다.
- [93] 도 4 및 도 5를 참조하면, 본 발명의 목적을 달성하기 위하여, 본 발명의 일 실시예에 따른 키오스크(50)는 사용자로부터 정보를 입력받고, 정보를 출력할 수 있는 터치가능한 디스플레이(301), 제1 단말(30)에 출력된 QR 코드를 인식할 수 있는 QR 코드 리더기(303), 사용자의 신분증을 스캔하여 사용자 정보를 추출할 수 있는 스캐너(305), 출입인증결과가 인쇄된 종이를 출력할 수 있는 결과출력부(307), 사용자의 얼굴 등을 촬영할 수 있는 카메라(309), 사용자의 체온을 측정할 수 있는 적외선 열감지 카메라(311) 및 촬영을 위한

조명장치(313)를 포함할 수 있다.

- [94] 이 때, 본 발명의 일 실시예에 따른 키오스크(50)는 사용자가 QR 코드를 신규 생성할 때, 카메라(309)를 통하여 사용자의 얼굴을 촬상하고, 인공지능 기반의 안면인식 모듈을 통하여, 상기 촬상 이미지와 상기 스캐너(305)를 통해 추출된 사진을 비교하고, 그 결과값을 사용자 정보에 포함시킴으로써, QR 코드를 사용할 때, QR 코드를 사용하는 사용자가 진정 사용자인지 판단할 수 있다. 또한, 이때, 상기 인공지능 기반의 안면인식 모듈은 마스크착용 여부 또한 확인할 수 있도록 구성될 수 있어, 보다 엄격한 출입 인증 여부를 판단할 수도 있다.
- [95] 또한, 출입을 원하는 사용자가 전염병의 우려가 있는 경우, 즉, 체온이 기 설정된 임계온도(ex. 37.5도)를 초과하는 경우에는 전염병에 노출되었을 가능성이 높기 때문에 키오스크(50)는 적외선 열감지 카메라(311)를 통하여 출입을 원하는 사용자의 체온을 측정하고, 상기 사용자의 체온을 기반으로 출입 인증 여부를 판단할 수도 있다.
- [96] 또한, 본 발명의 일 실시예에 따른 키오스크(50)는 사용자가 제1 단말(30)에 출력된 QR 코드를 QR 코드 리더기(303)에 인식시키면, 디스플레이(301)에 사용자 정보와 출입인증결과(320)를 출력할 수 있다.
- [97] 이 때, 상기 제1 QR 코드는 상기 사용자 정보를 기반으로 서버(20)에서 생성된 것으로, 서버(20)로부터 제1 단말(30)에게 송신된 것일 수 있다.
- [98] 이 때, 상기 사용자 정보는 출입자의 신상을 파악할 수 있는 모든 정보를 포함할 수 있으며, 예를 들면, 상기 출입자의 핸드폰 번호 및 이름, 생년월일, 주소 등 중 적어도 하나 이상을 포함할 수 있다. 사용자는 키오스크(50)의 입력 모듈을 이용하여 사용자 정보를 입력할 수 있다.
- [99] 다만, 사용자가 본인의 신상정보를 직접 입력하는 경우, 수기로 기재하는 것과 크게 다를 바가 없고, 거짓 신상정보를 입력할 우려가 있으므로, 사용자의 신원정보를 정확하게 추출하기 위하여, 키오스크(50)는 사용자의 신분증을 식별할 수 있는 스캐너(305)를 포함할 수 있다.
- [100] 이 때, 스캐너(305)는 주민등록증, 운전면허증 및 여권 등과 같이 사용자의 신원을 확인할 수 있는 신분증을 스캔하여, 사용자의 신원정보를 추출할 수 있다. 이 때, 상기 스캐너(305)는 OCR(Optical Character Reader)을 포함할 수 있으며, 이를 통해 사용자의 신분증에서 사용자의 이름, 주소, 생년월일, 성별, 국적 및 여권번호 중 적어도 하나 이상을 사용자 정보로써 추출할 수 있다.
- [101] 또한, 키오스크(50)는 제1 단말(30)에 출력된 QR 코드를 인식할 수 있는 QR 코드 리더기(303)를 더 포함할 수 있다. 따라서, 키오스크(50)는 제1 단말(30)에 출력된 제1 QR 코드를 해석하고, 상기 제1 QR 코드에 상응하는 사용자 정보를 서버(20)에 요청할 수 있으며, 서버(20)로부터 수신한 사용자 정보를 기반으로 출입 인증 여부를 판단할 수 있다.
- [102] 이 때, 상기 키오스크가 설치된 장소를 고정적으로 출입하고자 하는 사람과 1회성으로 출입하고자 하는 사람이 있을 수 있음에도, 일괄적으로 제1

단말(30)에 어플 등을 설치하고 상기 제1 QR 코드를 저장하게 하는 것은 비효율적일 수 있다. 따라서, 고정적으로 출입하고자 하는 사람에게 제공할 고정 QR 코드와 1회성으로 출입하고자 하는 사람(타지역에서 온 방문자 또는 관광 온 외국인 등)에게 제공할 1회성 QR 코드를 구분하여 출력할 수 있다.

- [103] 상술한 구성을 위하여, 키오스크(50)는 디스플레이(301)를 통해 고정 QR 코드와 1회성 QR 코드를 선택할 수 있는 메뉴를 제공하고, 선택에 따라 아래 과정을 선택적으로 진행할 수 있다. 이 때, 사용자 정보를 입력받고 QR 코드를 생성하는 과정을 동일하나, 생성된 QR 코드를 제공하는 방식에서 차이가 있다.
- [104] 먼저, 고정적 QR 코드를 선택한 경우, 키오스크(50)는 제1 QR 코드를 다운받을 수 있는 URL을 포함하는 고정 QR 코드를 종이에 인쇄하여 출력하거나, 키오스크(50)의 디스플레이(301)에 출력하여, 사용자가 상기 고정 QR 코드를 통해 상기 제1 QR 코드를 다운받을 수 있도록 할 수 있다. 따라서, 이 때는, 서버(20)에서 제1 단말(30)로 직접 제1 QR 코드를 송신할 필요가 없다.
- [105] 또한, 1회성 QR 코드를 선택한 경우, 키오스크(50)는 상기 1회성 QR 코드를 종이에 인쇄하여 출력할 수 있다. 이 때, 상기 1회성 QR 코드는 상기 제1 QR 코드와 동일한 것일 수 있다. 상기 1회성 QR 코드가 인쇄된 종이를 소지한 사용자는 해당 종이를 출입하고자 하는 장소에 설치된 키오스크(50)에 인식시킴으로써, 출입인증을 받을 수 있다. 따라서, 1회성을 출입하고자 하는 사람은 상기 제1 QR 코드를 단말에 다운받거나, 다수의 QR 코드를 저장 및 관리할 어플 등을 설치할 필요가 없다.
- [106] 제1 단말(30)은 서버(20)로부터 수신한 제1 QR 코드를 제2 출력 모듈(190)을 통하여 출력할 수 있다. 또한, 제1 단말(30)은 통신 모듈(170)을 통하여 서버(20)로부터 상기 제1 QR 코드를 수신할 수 있다.
- [107] 또한, 제1 단말(30) 및/또는 제2 단말(40)은 컴퓨터, 스마트폰, 핸드폰, 태블릿 PC, 디지털 카메라, 캠코더, 전자책 단말기, 디지털 방송용 단말기, PDA(Personal Digital Assistants), PMP(Portable Multimedia Player), 네비게이션, MP3 플레이어, 착용형 기기(wearable device), 오디오, DVD 플레이어 등 통신이 가능한 장치를 모두 포함할 수 있다.
- [108] 출입자 명부만을 기록하기 위해서는 사용자마다 하나의 QR 코드만을 생성하고 관리하면 되지만, 출입 허용 여부를 판단하기 위해서는 각 출입장소마다 별개의 QR 코드를 생성하는 것이 보안상 유리하다. 따라서, 키오스크(50)는 기 설정된 특정 장소에 하나 이상 설치될 수 있고, 상기 제1 단말(30)은 상기 키오스크(50) 각각에 대응하는 하나 이상의 제1 QR 코드를 구분하여 생성요청할 수 있고, 각각 구분하여 저장 및 관리할 수 있다. 이를 통해, 사용자는 출입하고자 하는 장소의 입구에 설치된 키오스크(50)에 해당 키오스크(50)에 대응하는 제1 QR 코드를 인식시킴으로써, 출입명부 기록 또는 출입인증을 할 수 있다.
- [109] 본 발명의 일 실시예에 따른 서버(20)는 키오스크(50)로부터 상기 사용자

정보를 수신하고, 키오스크 정보 및 상기 사용자 정보를 기반으로 상기 제1 QR 코드를 생성할 수 있고, 상기 제1 QR 코드를 상기 제1 단말(30)에게 송신할 수 있다.

- [110] 이 때, 상기 키오스크 정보는 상기 키오스크(50) 고유의 식별자일 수 있고, 상기 키오스크(50)이 위치하고 있는 장소에 대한 식별값 또는 상기 키오스크(50)의 현재 좌표값일 수 있다. 이 때, 서버(20)는 상기 식별값 또는 상기 좌표값과 상기 사용자 정보를 기반으로 상기 제1 QR 코드를 생성하고, 이를 제1 단말(30)에게 송신하며, 상기 제1 QR 코드와 사용자 정보는 서버(20)의 저장 모듈(150)에 저장될 수 있다.
- [111] 이 때, 상기 사용자 정보는 유출 방지를 위하여 암호화하여 저장할 수 있으며, 키오스크(50)로부터 상기 제1 QR 코드에 대응하는 출입인증요청을 수신하면, 상기 제1 QR 코드에 대응하는 암호화된 사용자 정보를 복호화하여 키오스크(50)에게 송신할 수 있다.
- [112] 본 발명의 일 실시예에 따른 통합 시스템(10)은 상술한 구성을 통하여 사용자의 출입을 관리할 수 있으며, 시스템(10)의 동작흐름과 관련하여 후술하도록 한다.
- [113] 도 6은 본 발명의 일 실시예에 따른 통합 시스템의 동작을 나타내는 흐름도이다.
- [114] 도 6을 참조하면, 본 발명의 일 실시예에 따른 제1 단말(30)은 제1 QR 코드를 생성하기 위하여 키오스크(50)로 사용자 정보를 입력한다(S401).
- [115] 이 때, 단계(S401)는 상술한 바와 같이 사용자가 직접 입력할 수도 있고, 사용자를 인증할 수 있는 신분증을 키오스크(50)의 스캐너(305)에 삽입 및/또는 거치 등으로 사용자 정보를 입력할 수도 있다. 이 때, 상기 신분증은 사용자의 신원을 확인할 수 있는 신분증을 모두 포함할 수 있고, 예를 들면, 주민등록증, 운전면허증 및 여권 등일 수 있다. 상기 스캐너(305)에 신분증을 삽입 및/또는 거치하는 경우, 키오스크(50)는 상기 신분증을 스캔하여 사용자 정보를 추출 또는 생성할 수 있다.
- [116] 이 때, 스캐너(305)는 주민등록증, 운전면허증 및 여권 등의 신분증의 부정사용(복사) 방지를 위하여 위변조 판별기능을 포함할 수 있다. 본 발명의 일 실시예에 따라 신분증을 기반으로 QR 코드를 생성하는 이유는 상기 제1 단말(30)이 본인 명의의 단말이 아닌 경우에도 생성할 수 있도록 하기 위함이다.
- [117] 종래에는 사용자의 신원을 특정하기 위한 방법으로 통신사의 본인인증이 주로 적용되고 있으며, 특히, 웹사이트의 회원가입 등에서 적용되고 있고, 블록체인 전자신분증(DID)의 경우에는 통신사의 본인인증을 유일한 본인확인 수단으로 사용하고 있다.
- [118] 이와 관련하여, 네이버 등과 같은 QR 코드 발급기관에서도 QR 코드 발급을 위하여, 우선적으로 QR 코드 발급기관에 회원가입시 입력한 제1 개인정보를 추출하고, 제1 단말(30)이 가입한 통신사의 본인인증을 통해 제2 개인정보를 추출한 후, 상기 제1 개인정보와 상기 제2 개인정보의 비교결과에 기반하여 QR

코드를 발급하고 있다.

- [119] 그러나, 종래 QR 코드 발급방식은 가족 명의로 개통한 단말인 경우나, 영업 등의 이유로 회사 명의로 개통한 단말의 경우에는 QR 코드를 발급하기 어렵다는 문제점이 있었다. 또한, QR 코드 발급기관들은 QR 코드를 발급받기 원하는 사용자가 회원가입을 위해 입력한 개인정보와 통신사의 본인인증 결과를 기반으로 QR 코드를 발급하기 때문에, 허위정보에 대한 판단과 책임소재가 모호하다는 문제점이 있다.
- [120] 또한, 코로나(COVID-19)와 같은 전염병 확산을 방지하기 위한 대책에서 내외국인의 차이가 없어야 함에도, 통신사의 본인인증의 경우 외국인은 신청할 수 없어 상술한 방식으로는 QR 코드를 발급받기 어렵다는 문제점도 있다.
- [121] 이에, 본 발명의 일 실시예에 따른 통합 시스템(10)은 QR 코드 발급기관의 회원가입 등과 같은 사전행위 없이도, 신분증의 위변조 판별기술을 기반으로 QR 코드를 발급할 수 있어, 내외국인에 대한 구별없이 QR 코드를 쉽게 발급할 수 있다.
- [122] 또한, 본 발명의 일 실시예에 따른 통합 시스템(10)은 상기 스캐너(305)와 안면인식 기술, 홍채 인식 기술, 정맥 인식 기술 등 바이오 인증 수단과 결합되어, QR 코드를 발급하고자 하는 사용자를 정확하게 특정할 수도 있다.
- [123] 다만, 제1 단말(30)이 가입한 통신사의 본인인증 방식도 배제할 순 없으므로, 신분증에 의한 본인확인과 바이오 인증을 결합하여 QR 코드를 생성하는 제1 방식과, 제1 단말(30)의 통신사 본인인증과 QR 코드 발급기관의 회원정보를 기반으로 QR 코드를 생성하는 제2 방식을 선택적으로 적용할 수 있도록 구성하여, QR 코드 발급의 어려움을 해소할 수 있으며, 보다 정확한 본인인증이 가능해질 수 있다. 이를 통해 출입명부를 허위로 기재하는 등의 문제점을 해결할 수도 있다. 그리고, 본 발명의 일 실시예에 따른 키오스크(50)는 상기 사용자 정보와 본 키오스크(50)의 위치 정보를 관리사 서버에게 송신한다(S403). 이 때, 단계(S403)는 제1 QR 코드에 상기 사용자 정보와 키오스크(50)에 관한 정보를 모두 반영하기 위한 것으로, 상기 키오스크(50)의 위치 정보는 상기 키오스크(50)을 식별할 수 있는 식별값 또는 상기 키오스크(50)의 좌표값일 수 있다.
- [124] 그리고, 본 발명의 일 실시예에 따른 서버(20)는 상기 사용자 정보 및 상기 키오스크(50)의 위치 정보를 기반으로 제1 QR 코드를 생성한다(S405).
- [125] 이 때, 서버(20)는 상기 제1 QR 코드와 상기 제1 QR 코드에 상응하는 상기 사용자 정보 및 상기 키오스크(50)의 위치 정보를 암호화하여 저장할 수도 있다.
- [126] 그리고, 본 발명의 일 실시예에 따른 서버(20)는 상기 제1 QR 코드를 제1 단말(30)에게 송신한다(S407).
- [127] 상술한 S401 내지 S407 단계는 사용자가 키오스크(50)이 설치된 장소에 처음 출입하기 위하여 상기 키오스크(50)에 대한 제1 QR 코드를 생성하는 과정을 설명한 것이며, 이하에서는 S409 내지 S417 단계를 통하여, 사용자가 상기 제1

QR 코드를 사용하는 과정을 설명하도록 한다.

- [128] 본 발명의 일 실시예에 따른 키오스크(50)이 설치된 장소에 출입하고자 하는 사용자는 제1 단말(30)에 제1 QR 코드를 출력하고, 상기 제1 QR 코드를 키오스크(50)에 있는 QR 코드 리더기(303)에 인식시킨다(S409).
- [129] 그리고, 본 발명의 일 실시예에 따른 키오스크(50)는 상기 제1 QR 코드를 해석한다(S411). 이 때, 단계(S411)는 제1 QR 코드에 포함된 사용자 정보 및 키오스크(50)의 위치 정보를 추출하여, 제1 QR 코드가 본 키오스크(50)에 대응하는 것인지를 확인하고, 후술하는 S413 및 S415 단계를 통해 상기 제1 QR 코드가 서버(20)에 의하여 생성된 것인지 확인하기 위한 것이다.
- [130] 그리고, 본 발명의 일 실시예에 따른 키오스크(50)는 상기 제1 QR 코드를 기반으로 서버(20)에 출입인증요청을 송신하고(S413), 서버(20)는 상기 제1 QR 코드에 대응하는 사용자 정보를 키오스크(50)에게 송신한다(S415).
- [131] 그리고, 본 발명의 일 실시예에 따른 키오스크(50)는 상기 단계(S411)를 통해 추출한 사용자 정보와 서버(20)로부터 수신한 사용자 정보를 비교하여, 사용자의 출입 인증 여부를 판단한다(S417).
- [132] 이 때, 상기 단계(S417)를 통하여, 상기 제1 QR 코드가 제1 단말(30) 및 키오스크(50)에 대응하는 정보를 기반으로 서버(20)에서 생성된 것인지 판단할 수 있다.
- [133] 본 발명의 일 실시예에 따른 전자출입관리 시스템(10)은 상술한 동작을 통하여 사용자의 신원정보를 정확하게 추출할 수 있고, 출입 허용 여부를 판단하거나 출입명부를 작성할 수 있다. 그러나, 상술한 동작은 상기 제1 QR 코드가 상기 제1 QR 코드를 생성한 제1 단말(30)에서 출력되지 않고, 종이에 인쇄되거나, 스크린 샷으로 저장된 파일을 다른 제1 단말(30)에서 출력되는 경우에 발생할 수 있는 스푸핑(Spoofing) 문제를 해결하기 위한 구성이 없다는 문제점이 있다.
- [134] 상술한 스푸핑 문제점을 해결하기 위한 방안으로 도 5를 참조하여 후술하도록 한다.
- [135] 도 6은 본 발명의 일 실시예에 따른 통합 시스템의 동작을 나타내는 흐름도이다.
- [136] 상기 동작은 제1 QR 코드 및 제2 QR 코드를 기반으로 스푸핑을 방지하는데 그 목적이 있을 수 있다. 스푸핑(Spoofing)이란, 의도적인 행위를 위해 타인의 신분으로 위장하는 것으로, 승인받은 사용자인 것처럼 시스템에 접근하거나 네트워크 상에서 허가된 주소로 가장하여 접근 제어를 우회하는 공격행위를 의미한다. 본 발명을 예로 들면, 상기 제1 QR 코드가 서버(20)를 통해 생성된 진정한 것이라고 할지라도, 상기 제1 QR 코드를 키오스크(50)에 인식시키는 사용자가 상기 제1 QR 코드에 대응하는 사용자가 아닌 경우가 발생할 수 있기 때문이다.
- [137] 일반적인 QR 코드 리더기(303)에서는 QR 코드가 제1 단말(30)에서 출력되는 것인지, 종이에 인쇄된 것인지, 또는 다른 제1 단말(30)에서 출력되는 것인지

구분할 수 없다. 따라서, 본 발명은 일반적인 QR 코드 리더기(303)를 통해서도 스푸핑을 방지할 수 있는 구성을 포함하여, 스푸핑 문제를 해결하고자 한다.

- [138] 도 5를 참조하면, 본 발명의 일 실시예에 따른 키오스크(50)이 설치된 장소에 출입하고자 하는 사용자는 제1 단말(30)에 제1 QR 코드를 출력하고, 상기 제1 QR 코드를 키오스크(50)로 있는 QR 코드 리더기(303)에 인식시킨다(S501).
- [139] 그리고, 키오스크(50)는 상기 제1 QR 코드를 해석한다(S503).
- [140] 이 때, 단계(S503)는 상기 제1 QR 코드에 포함된 사용자 정보 및 키오스크(50)의 위치 정보를 추출하여, 상기 제1 QR 코드가 본 키오스크(50)에 대응하는 것인지를 확인하기 위한 것이다.
- [141] 그리고, 키오스크(50)는 상기 제1 QR 코드를 기반으로 서버(20)에 출입인증요청을 송신한다(S505).
- [142] 그리고, 키오스크(50)는 상기 제1 QR 코드에 대응하는 제1 단말(30)로 상기 제1 단말(30)의 현재 위치좌표를 요청한다(S507).
- [143] 그리고, 제1 단말(30)은 현재 위치좌표를 서버(20)에게 송신한다(S509).
- [144] 이 때, 단계(S507 및 S509)는 상기 제1 QR 코드가 진정한 사용자의 제1 단말(30)에서 출력되는 것인지 확인하기 위한 것이다. 이 때, 서버(20)는 1차적으로, 제1 단말(30)의 현재 위치좌표와 키오스크(50)의 위치를 비교하여 임계치 이상 거리차이가 발생하는 경우, 제1 QR 코드가 상기 제1 단말(30)에서 출력되지 않은 것으로 판단할 수도 있다.
- [145] 그리고, 본 발명의 일 실시예에 따른 서버(20)는 현재 표준시간 정보 및 제1 단말(30)로부터 수신한 현재 위치좌표를 기반으로 제2 QR 코드를 생성한다(S511).
- [146] 이 때, 단계(S511)는 현재 표준시간 정보 및 제1 단말(30)로부터 수신한 현재 위치좌표를 기반으로 제2 QR 코드를 생성하는데, 이는 제2 QR 코드를 무작위로 생성하되, 인증을 요청하는 시점의 정보를 반영하여 조작을 방지하기 위한 것이다.
- [147] 또한, 단계(S511)에서 제2 QR 코드는 상기 제1 QR 코드와 동일한 버전 및 동일한 크기로 생성할 수 있다. 이는 후술하는 바와 같이 제1 QR 코드와 제2 QR 코드를 병합하여 오버레이 QR 코드를 생성할 때 용이하게 하기 위함이다.
- [148] 그리고, 본 발명의 일 실시예에 따른 서버(20)는 상기 제1 QR 코드에 대응하는 사용자 정보와 상기 제2 QR 코드를 키오스크(50)에게 송신하고(S515), 상기 제2 QR 코드를 제1 단말(30)에게 송신한다(S517).
- [149] 그리고, 본 발명의 일 실시예에 따른 키오스크(50)는 상기 제1 QR 코드 및 제2 QR 코드를 병합하여, 제2 오버레이 QR 코드를 생성하고(S517), 본 발명의 일 실시예에 따른 제1 단말(30)은 상기 제1 QR 코드 및 제2 QR 코드를 병합하여, 제1 오버레이 QR 코드를 생성한다(S519).
- [150] 이 때, 상기 제1 오버레이 QR 코드 및 상기 제2 오버레이 QR 코드는 상기 제1 QR 코드 및 상기 제2 QR 코드를 중첩시켜 생성될 수 있다. 보다 상세하게

- 살펴보면, 상기 제1 오버레이 QR 코드 및 상기 제2 오버레이 QR 코드는 상기 제1 QR 코드 및 상기 제2 QR 코드의 위치 검출용 패턴을 동일 축상에 위치시키고, 상기 제1 QR 코드 및 상기 제2 QR 코드의 각 셀을 비교하여 동일한 셀은 흑색 셀로 설정하고, 동일하지 않은 셀은 백색 셀로 설정하여 생성될 수 있다.
- [151] 상기 제1 오버레이 QR 코드 및 상기 제2 오버레이 QR 코드는 랜덤하게 생성되며, 동일하게 생성되는 것이 목적으로써, 상기 제1 QR 코드와 상기 제2 QR 코드를 다양한 방식으로 조합하여 생성될 수 있다.
- [152] 그리고, 제1 단말(30)은 상기 제2 오버레이 QR 코드를 키오스크(50)에 있는 QR 코드 리더기(303)에 인식시킨다(S521).
- [153] 이 때, S521 단계는 S501 단계와 별개의 단계로 구성되어 있지만, 상기 S501 단계의 연장선상에 있는 것으로써, 사용자가 제1 단말(30)의 디스플레이에 출력된 제1 QR 코드를 QR 코드 리더기(303)에 인식시키고 있는 동안에, S503 내지 S519 단계가 수행되고 제1 단말(30)의 디스플레이에 제1 오버레이 QR 코드가 출력됨으로써, 자연스럽게 인식시킬 수 있다.
- [154] 그리고, 키오스크(50)는 상기 단계(S503)를 통해 추출한 사용자 정보와 서버(20)로부터 수신한 사용자 정보를 비교하여, 사용자의 출입 인증 여부를 판단함으로써, 상기 제1 QR 코드가 제1 단말(30) 및 키오스크(50)에 대응하는 정보를 기반으로 서버(20)에서 생성된 것인지 판단하고, 상기 제1 오버레이 QR 코드 및 상기 제2 오버레이 QR 코드의 동일여부를 비교하여 스푸핑 여부를 판단한다(S523).
- [155] 만약, 상기 제1 QR 코드가 종이에 인쇄된 경우, 제1 오버레이 QR 코드를 키오스크(50)에 인식시킬 수 없으므로, 스푸핑으로 판단하여 출입인증을 승인하지 않을 수 있다.
- [156] 또한 본 발명의 일 실시예는 다음과 같은 특징을 더 포함할 수 있다.
- [157] 사용자는 키오스크(50)의 입력 모듈(230)을 통해 신분증(예; 주민등록증, 운전면허증, 사원증, 학생증, 명함 등), 여권(passport)을 입력하거나 인식시킬 수 있으며, 상기 입력 및/또는 인식된 신분증, 여권에 상응하는 이미지 및/또는 영상을 서버(20)에게 전달할 수 있다.
- [158] 서버(20)는 신분증, 여권 위변조 판별 결과 정상인 경우에 한해 신분증, 여권상의 사진과 키오스크(50)에 설치한 카메라의 실시간(Liveness) 얼굴 활상 사진을 객체 인식 알고리즘 및/또는 인공지능(AI) 안면 인식 알고리즘으로 일치 여부를 비교할 수 있다. 이는 기존의 사전 회원 가입시 활상한 얼굴 사진을 등록, 이후 출입 또는 서비스 사용인증을 위한 단순 얼굴사진 비교 방식에 비해 사전 회원등록 없이 내국인은 물론 외국인도 포함한 불특정 다수인을 대상으로 즉시 회원등록이 가능한 강력한 비대면 본인인증 방식을 제공하기 위함이다. 이 기술은 국가 공인기관에서 발급한 신분증이 아닌 학생증, 명함 등 사진이 있는 매체를 스캐너에 인식하여 취득한 사진과 키오스크(50)에 설치한 카메라로 활상한 얼굴사진을 AI 안면인식 알고리즘으로 일치 여부를 판단, 출입과

신분증대체(FACE ID) 수단으로 활용할 수 있다. 이를 통해 공인 신분증도 없고 본인확인 부제로 금융시스템이 열악한 국가에서도 본인인증 방식을 제공하거나, FACE ID를 이용하여 출입, 금융서비스와 연계할 수 있게 하기 위함이다.

- [159] 상기 객체 인식 알고리즘은 HOG(Histogram of Oriented Gradient), Haar-like feature, Co-occurrence HOG, LBP(local binary pattern), FAST(features from accelerated segment test) 등과 같은 오브젝트 특징 추출을 위한 다양한 알고리즘에 기반하는 것으로써, 이미지, 동영상, 이미지 정보, 및/또는 동영상 정보에 포함된 오브젝트의 윤곽선 또는 상기 오브젝트에서 추출할 수 있는 글씨(또는 정보를 나타내는 윤곽선(또는 외형))를 획득할 수 있다.
- [160] 또한 키오스크(50)에 비대면 본인인증을 위한 바이오 인증 수단으로 지문, 홍채, 손바닥정맥 등도 활용할 수 있지만, 고객의 동의를 전제로 사전 등록 없이는 비교 인증할 수 없는 불편함이 있기에, 본원발명의 구성을 통해 즉시 인증(immediately certification)을 위해 안면 인식(facial recognition)이 효율적이라 볼 수 있다.
- [161] 한편 서버(200)가 소정의 기준에 따라 상이한 오브젝트 검출 모드로 동작하는 것과 관련하여, 이하 다시 설명한다.
- [162] 일 예로, 상기 이미지 정보 및/또는 동영상 정보가 검출 대상 오브젝트가 단일 오브젝트임을 나타내고, 상기 RGB 가지수 정보가 소정의 임계치(예; 0~150 사이의 정수값)보다 높은 값을 나타내는 경우, 서버(200)는 제1 오브젝트 검출 모드로 동작하거나 제1 오브젝트 검출 모드로 설정될 수 있다. 제1 오브젝트 검출 모드로 동작하거나 제1 오브젝트 검출 모드로 설정된 서버(200)는 로지스틱 회귀분석(Logistic Regression), SVM(Support Vector Machine), Latent SVM(Latent Support Vector Machine) 등의 다양한 인식기들을 이용하여 이미지, 동영상, 이미지 정보, 및/또는 동영상 정보에 포함된 오브젝트를 검출함으로써 오브젝트 정보를 생성(및/또는 획득)할 수 있다.
- [163] 다른 예로, 상기 이미지 정보 및/또는 동영상 정보가 검출 대상 오브젝트가 단일 오브젝트임을 나타내고, 상기 RGB 가지수 정보가 상기 소정의 임계치(예; 0~150 사이의 정수값) 이하의 값을 나타내는 경우, 서버(200)는 제2 오브젝트 검출 모드로 동작하거나 제2 오브젝트 검출 모드로 설정될 수 있다. 제2 오브젝트 검출 모드로 동작하거나 제2 오브젝트 검출 모드로 설정된 서버(200)는 가변 부분 모델(deformable part model)에서 이미지 부분 모델을 이미지-모션 혼합 특징 기반 부분 모델로 대체함으로써, 규칙적인 움직임을 보이는 오브젝트에 대한 모델링을 수행하여 이동 중인 오브젝트와 배경을 분리시킬 수 있다. 그래서, 오브젝트 검출 장치는, 예를 들어 회전하는 자동차 바퀴, 걷고 있는 사람의 다리 등의 규칙적인 움직임을 보이는 오브젝트를 검출함으로써 오브젝트 정보를 생성(및/또는 획득)할 수 있다.
- [164] 또 다른 예로, 상기 이미지 정보 및/또는 동영상 정보가 검출 대상 오브젝트가

복수의 오브젝트임을 나타내는 경우(이때는 상기 RGB 가지수 정보와 상기 소정의 임계치 사이의 비교를 고려하지 않음), 서버(200)는 제3 오브젝트 검출 모드로 동작하거나 제3 오브젝트 검출 모드로 설정될 수 있다. 제3 오브젝트 검출 모드로 동작하거나 제3 오브젝트 검출 모드로 설정된 서버(200)는 이미지, 동영상, 이미지 정보, 및/또는 동영상 정보에 포함된 오브젝트를 추출하여 오브젝트 정보를 획득할 수 있다. 제3 오브젝트 검출 모드로 동작하거나 제3 오브젝트 검출 모드로 설정된 서버(200)는 HOG(Histogram of Oriented Gradient), Haar-like feature, Co-occurrence HOG, LBP(local binary pattern), FAST(features from accelerated segment test) 등과 같은 오브젝트 특징 추출을 위한 다양한 알고리즘을 통하여, 이미지, 동영상, 이미지 정보, 및/또는 동영상 정보에 포함된 오브젝트의 윤곽선 또는 상기 오브젝트에서 추출할 수 있는 글씨(또는 정보를 나타내는 윤곽선(또는 외형))를 획득할 수 있다. 또한 제3 오브젝트 검출 모드로 동작하거나 제3 오브젝트 검출 모드로 설정된 서버(200)는 이미지, 동영상, 이미지 정보, 및/또는 동영상 정보에 포함된 오브젝트를 영상 분석을 통해 인식(또는 식별)하고, 상기 인식된 오브젝트에 대응되는 영역을 마스킹 처리하여 마스킹 영상 정보를 생성할 수 있다. 이때, 마스킹 처리 과정은, 예를 들면, 차분영상 방법, GMM(Gaussian Mixture Models)을 이용하는 MOG(Model of Gaussian) 알고리즘, 코드북(Codebook) 알고리즘 등과 같은 오브젝트와 배경을 분리하기 위한 배경 모델링을 통해 오브젝트에 해당하는 오브젝트 후보 영역을 추출하는 방법을 이용함으로써 오브젝트 정보를 추출 및/또는 획득할 수 있다.

- [165] 도 7은 본 발명의 일 실시예에 따른 제어 모듈을 나타내는 블록도이다.
- [166] 도 7을 참조하면, 서버(20)의 제1 제어 모듈(110)은 인공지능 모듈(610) 및 블록체인 모듈(620)을 포함할 수 있다.
- [167] 인공지능 모듈(610)은 인공지능망에 기반하여 사용자의 동선을 분석하고 스푸핑 여부를 판단할 수 있다. 또한, 인공지능 모듈(610)은 저장 모듈(150)에 저장된 빅데이터(big data)에 기계 학습(machine learning)을 이용하여 사용자의 동선을 분석하고 스푸핑 여부를 판단할 수 있다.
- [168] 또한, 인공지능 모듈(610)은 서버(20)의 저장 모듈(150)에 저장된 빅데이터를 입력변수로 하여 인공지능망을 학습시킬 수 있다. 예를 들면, 인공지능 모듈(610)은 머신러닝의 한 분야인 딥러닝(Deep Learning) 기법을 이용하여 정확한 상관 관계가 도출될 수 있도록 학습을 수행할 수 있다.
- [169] 또한 인공지능 모듈은 딥러닝을 통하여 상기 함수에서의 복수 개의 입력들의 가중치(weight)를 학습을 통하여 산출할 수 있다. 또한, 이러한 학습을 위하여 활용되는 인공지능망 모델로는 RNN(Recurrent Neural Network), DNN(Deep Neural Network) 및 DRNN(Dynamic Recurrent Neural Network) 등 다양한 모델들을 활용할 수 있을 것이다.
- [170] 여기서 RNN은 현재의 데이터와 과거의 데이터를 동시에 고려하는 딥 러닝 기법으로서, 순환 신경망(RNN)은 인공 신경망을 구성하는 유닛 사이의 연결이

방향성 사이클(directed cycle)을 구성하는 신경망을 나타낸다. 나아가, 순환 신경망(RNN)을 구성할 수 있는 구조에는 다양한 방식이 사용될 수 있는데, 예컨대, 완전순환망(Fully Recurrent Network), 홉필드망(Hopfield Network), 엘만망(Elman Network), ESN(Echo state network), LSTM(Long short term memory network), 양방향(Bi-directional) RNN, CTRNN(Continuous-time RNN), 계층적 RNN, 2차 RNN 등이 대표적인 예이다. 또한, 순환 신경망(RNN)을 학습시키기 위한 방법으로서, 경사 하강법, Hessian Free Optimization, Global Optimization Method 등의 방식이 사용될 수 있다.

- [171] 블록체인 모듈(620)은, QR 코드가 블록체인 기술에 기반하여 다른 네트워크 노드(예; 제1 단말(30))에게 전달될 수 있도록, 상기 QR 코드를 나타내는 정보에 기반하여 QR 코드 블록 데이터를 생성할 수 있다. 상기 블록체인 모듈(620)에 의해 생성되는 QR 코드 블록 데이터는 통신 모듈(120)을 통하여 제1 단말(30)에게 전달될 수 있다. 또한 상기 서버(20)는 상기 그룹화된 (QR 코드를 나타내는) 정보 및/또는 QR 코드 블록 데이터에 포함된 적어도 하나의 요소들을 블록체인에 저장할 수 있다.
- [172] 일반적으로 블록 체인(block chain)은 P2P(peer-to-peer) 네트워크에 의해 생성되고 관리되는 위조 및/또는 변조 불가능한 분산 저장소이다. 블록 체인은 트랜잭션(쌍방간의 조깅 수 없는 단위 작업)으로 생성된 데이터 블록들을 체인(chain) 형태로 잇따라 연결한 모음을 의미한다. 이전 블록에 다음 블록을 연이어 암호화하고 과반수가 넘는 사용자가 동의한 데이터를 실제 데이터로 인정하기 때문에, 한번 기록된 데이터는 위조 및/또는 변조가 불가능하다. 블록 체인의 대표적인 응용사례는 암호화폐의 거래 과정을 기록하는 분산화된 전자 화폐인 비트코인(bitcoin)이 있다. 블록 체인에는 일정 시간 동안 사용자들 간에 발생하는 확정된 거래 내역이 저장될 수 있다. 그리고, 많은 사용자들은 블록 체인 사본을 각자 갖고 있으며, 거래 내역은 모두에게 공개될 수 있다. 이와 같이, 과반수가 넘는 사용자가 동의한 거래 내역만 실제 데이터로 인정되고, 영구적으로 보관할 블록으로 묶여 저장될 수 있다.
- [173] 한편, 본 발명의 서버(20), 제1 단말(30), 제2 단말(40) 및/또는 키오스크(50) 각각은 블록체인을 포함하거나 블록 데이터를 제어할 수 있는 블록체인 노드일 수 있다. 예를 들면, 서버(20)는 키오스크(50)로부터 수신되는 QR 코드, 사용자 정보, 사용자 단말 정보, 키오스크 정보 등을 그룹화 및/또는 해시(hash)하여 블록체인에 저장한 후, QR 코드, 사용자 정보, 사용자 단말 정보, 키오스크 정보 등에 대한 위조 및/또는 변조를 검증하거나 판단할 수 있다. 일 예로, 블록체인 모듈(620)은 QR 코드를 나타내는 정보에 기반하여 머클 해쉬(Merkle hash)를 포함하는 QR 코드 블록 데이터를 생성하고, 상기 생성된 머클 해쉬가 포함되도록 복수의 QR 코드를 나타내는 정보를 그룹화할 수 있다.
- [174] 서버(20)는 저장 모듈(150)에 저장할 내용(예; QR 코드를 나타내는 정보)에 기반하여 머클 해쉬를 포함하는 QR 코드 블록 데이터(을)를 블록체인

트랜잭션으로 만들어 블록체인 네트워크에 참여한 다른 블록체인 노드에게 전송할 수 있다. 상기 블록체인 트랜잭션에 저장할 QR 코드를 나타내는 정보는 머클 해쉬 식별자, 그룹 식별자 및/또는 이전 그룹의 식별자를 포함할 수 있다.

- [175] 서버(20)는 미리 결정된 시간 및 상기 저장된 QR 코드를 나타내는 정보의 개수 중 적어도 하나에 기반하여 상기 블록체인에 저장된 적어도 하나의 요소와 상기 그룹화된 QR 코드를 나타내는 정보에 포함된 적어도 하나의 요소를 비교하여 상기 저장된 QR 코드를 나타내는 정보의 무결성을 검증할 수 있다. 상기 서버(20)는 상기 저장된 QR 코드를 나타내는 정보가 무결성하지 않는 경우, 출력 모듈(140)을 통해 상기 무결성 여부를 출력할 수 있다.
- [176] 서버(20)는 상기 저장 모듈(150)에 저장된 QR 코드를 나타내는 정보가 위조 및/또는 변조되거나 손상된 경우, 상기 서버(20)를 관리하는 관리자(예; 제2 사용자)가 이러한 사항을 알 수 있도록 출력 모듈(140)을 통해 상기 무결성 여부를 출력할 수 있다. 상기 제어 모듈(110)은 상기 저장된 블록체인의 무결성 여부를 판단하기 위한 증명서(certificate)를 생성하여 다른 블록체인 노드에게 전송할 수 있다. 상기 증명서는, 상기 저장된 적어도 하나의 QR 코드를 나타내는 정보의 정보, 상기 그룹화된 QR 코드를 나타내는 정보 및 상기 저장된 블록체인의 정보를 포함할 수 있다. 상기 증명서는 서버(20)가 매칭 점수를 나타내는 정보의 무결성 여부를 판단하는데 이용될 수 있다.
- [177] 제어 모듈(110)은 상기 저장된 블록체인에 대한 적어도 하나의 요소의 요청이 i) 본 발명의 QR 코드를 나타내는 정보 제공 서비스를 제공하거나 지원하는 웹사이트 및/또는 모바일앱을 통하여, 및/또는 ii) 다른 블록체인 노드로부터 수신되면 상기 요청된 적어도 하나의 요소를 i) 상기 웹사이트 및/또는 모바일앱을 통하여 출력하거나, 및/또는 ii) 다른 블록체인 노드에게 전송할 수 있다.
- [178] 또한 본 발명의 일 실시예에 따른 통합 시스템은 다음과 같은 특징을 더 포함할 수 있다.
- [179] 본 발명의 일 실시예에 따른 통합 시스템(10)은 블록체인 기반의 키오스크(50), 서버(20), 제1 단말(30) 및 스캐너(305)를 포함할 수 있다. 다만, 이와 같이 도 1에 도시된 통합 시스템(10)은 본 발명의 일 실시예에 불과할 수 있으며, 본 발명의 해석이 도 1에 의해 한정되는 형태로 해석되지 않을 수 있다.
- [180] 이때, 도 1에 도시된 복수의 구성 요소들은 일반적으로 네트워크(network)를 기반으로 서로 연결될 수 있다. 예를 들어, 도 1에 도시된 바와 같이, 키오스크(50)는 본 발명의 일 실시예에 따른 시스템(10)의 동작 방법을 사용하는 가맹점에 설치된 가맹점 단말을 의미할 수 있으며, 네트워크를 기반으로 서버(20)와 연결될 수 있다. 또한, 서버(20)는 네트워크를 기반으로 키오스크(50), 제1 단말(30) 및 스캐너(305)와 연결될 수 있다. 또한, 제1 단말(30)은 네트워크를 기반으로 서버(20)와 연결될 수 있다. 또한, 스캐너(305)는 네트워크를 기반으로 서버(20) 및 제1 단말(30)과 연결될 수 있다.

- [181] 여기서, 네트워크는 복수의 단말들 및 서버들과 같은 각각의 노드 상호 간에 정보 교환이 가능한 연결 구조를 의미할 수 있다. 예를 들어, 네트워크는 RF(radio frequency), 3GPP(3rd Generation Partnership Project) 네트워크, LTE(long term evolution) 네트워크, 5GPP(5th Generation Partnership Project) 네트워크, WIMAX(World Interoperability for Microwave Access) 네트워크, 인터넷(Internet), LAN(Local Area Network), Wireless LAN(Wireless Local Area Network), WAN(Wide Area Network), PAN(Personal Area Network), 블루투스(Bluetooth) 네트워크 NFC 네트워크, 위성 방송 네트워크, 아날로그 방송 네트워크, DMB(Digital Multimedia Broadcasting) 네트워크 등이 포함되나 이에 한정되지는 않을 수 있다.
- [182] 한편, 본 발명의 일 실시예에 따른 키오스크(50)는 블록체인 기반의 금융 서비스와 관련된 웹페이지(web page), 앱페이지(app page), 프로그램(program) 또는 애플리케이션(application)을 기반으로 암호화폐를 사용자 별로 생성된 지갑주소를 통하여 입금 받을 수 있고, 암호화폐에 대응되는 가치의 가격을 가지는 상품에 대한 지불 처리를 수행하는 장치를 의미할 수 있다. 이때, 키오스크(50)는 키오스크(kiosk)뿐만 아니라, 신분증 또는 여권의 진위여부를 확인할 수 있고, 네트워크 통신을 통하여 암호화폐의 입금을 확인하여 결제 대금의 지불을 처리할 수 있는 단말 또는 장치를 의미할 수 있다.
- [183] 또한, 키오스크(50)는 사용자가 언어의 종류를 선택하는 경우, 사용자가 선택한 언어에 대응되도록 화면 또는 소리로 출력되는 언어의 종류를 변경할 수 있다.
- [184] 또한, 키오스크(50)는 사용자가 통화의 종류를 선택하는 경우, 사용자가 선택한 종류의 통화와 암호화폐의 실시간 시세를 조회 및 출력 가능한 장치를 의미할 수 있다.
- [185] 또한, 본 발명의 일 실시예에 따른 키오스크(50)는 신분증 또는 여권 등과 같이 사용자의 신분을 확인할 수 있는 서면에 대한 진위여부를 스캐너(305)로부터 서버(20)를 통하여 판별하는 것은 물론, 성인인증을 함으로써 거래의 주체가 될 수 있는지 여부를 판별하는 장치를 의미할 수 있다.
- [186] 또한, 키오스크(50)는 사용자가 구매하고자 하는 상품의 가격의 금액이나 환전하고자 하는 금액에 대응하는 암호화폐의 수량을 사용자가 선택한 종류의 통화로 환산한 암호화폐의 시세로 계산할 수 있고, 계산된 암호화폐의 수량을 입금 받을 지갑주소를 사용자 별로 생성하여 식별코드로 출력하는 장치를 의미할 수 있다.
- [187] 그리고, 키오스크(50)는 식별코드로 출력된 지갑주소에 사용자의 제1 단말(30)을 통해 입금이 되었는지의 여부를 확인할 수 있고, 입금이 된 경우 입금 영수증을 발행하고, 결제완료처리를 하는 장치를 의미할 수 있다. 이때, 키오스크(50)는 암호화폐의 현 시세를 조회하거나, 지갑주소에 입금이 되었는지를 확인하거나 하는 등의 프로세스를 자체적으로 수행하는 경우에는 별도의 서버(20)가 요구되지 않을 수도 있으나, 실시예에 따라 각각의 역할을

- 분배하여 별도로 또는 통합하여 다르게 구현될 수도 있음은 자명하다 할 것이다.
- [188] 또한, 키오스크(50)는 상품의 가격을 결제하는 트랜잭션 관련 데이터를 모두 서버(20)로 전송함으로써, 서버(20)에서 프라이빗 블록체인으로 분산장부, 재고관리, 회원관리가 가능하도록 하는 서버를 의미할 수도 있다.
- [189] 여기서, 키오스크(50)는 네트워크를 통하여 원격지의 서버나 단말에 접속할 수 있는 컴퓨터로 구현될 수 있다. 예를 들어, 컴퓨터는 네비게이션, 웹 브라우저(WEB Browser)가 탑재된 노트북, 데스크톱(Desktop), 랩톱(Laptop) 등을 포함할 수 있다. 이때, 키오스크(50)는 네트워크를 통해 원격지의 서버나 단말에 접속할 수 있는 단말로 구현될 수도 있다.
- [190] 다시 말해, 키오스크(50)는 예를 들어, 휴대성과 이동성이 보장되는 무선 통신 장치로서, 네비게이션, 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(WCode Division Multiple Access), Wibro(Wireless Broadband Internet) 단말, 스마트폰(smartphone), 스마트 패드(smartpad), 타블렛 PC(Tablet PC) 등과 같은 모든 종류의 핸드헬드(Handheld) 기반의 무선 통신 장치를 포함할 수 있다.
- [191] 또한, 서버(20)는 블록체인 기반의 금융 서비스 웹 페이지, 앱 페이지, 프로그램 또는 애플리케이션을 제공하는 서버를 의미할 수 있다. 그리고, 서버(20)는 키오스크(50)에서 사용자의 입금을 받을 계정인 지갑주소를 생성하여 식별코드를 제공한 경우, 생성된 지갑주소에 입금이 되었는지를 확인하는 서버일 수 있다.
- [192] 다만, 상술한 바와 같이 키오스크(50)에서 자체적으로 처리하는 경우 서버는 존재하지 않을 수도 있고, 복수의 키오스크들을 관리하는 역할만을 수행할 수도 있다.
- [193] 그리고, 서버(20)는 제1 단말(30)에서 생성된 지갑주소로 암호화폐를 입금한 경우, 환전 수수료를 공제하는 서버일 수 있고, 블록체인 내의 노드의 장부를 업데이트하는 역할을 수행하는 서버를 의미할 수도 있다.
- [194] 또한, 서버(20)는 키오스크(50)와 미리 연동된 스캐너(305)에서 진위여부 판별 및 성인인증 등의 프로세스를 수행하는 경우, 진위여부 및 성인여부 등을 판별하여 키오스크(50)로 피드백하는 서버일 수도 있다. 그리고, 서버(20)는 복수의 지점들에 존재하는 키오스크 각각에서 판매된 상품의 종류 및 개수 등을 로그로 저장하고 회원관리를 하는 서버일 수도 있다.
- [195] 여기서, 서버(20)는 네트워크를 통하여 원격지의 서버나 단말에 접속할 수 있는 컴퓨터로 구현될 수 있다. 예를 들어, 컴퓨터는 네비게이션, 웹 브라우저(WEB Browser)가 탑재된 노트북, 데스크톱(Desktop), 랩톱(Laptop) 등을 포함할 수 있다. 제1 단말(30)은 블록체인 기반의 금융 서비스 관련 웹 페이지, 앱 페이지, 프로그램 또는 애플리케이션을 이용하는 사용자의 단말일 수 있다.

- [196] 그리고, 제1 단말(30)은 암호화폐를 이용하여 상품을 구매하고자 하는 외국인 또는 내국인의 단말일 수 있다. 또한, 제1 단말(30)은 키오스크(50)에서 지갑주소를 생성하여 지갑주소의 정보 및 암호화폐의 수량 정보를 포함한 식별코드를 출력한 경우, 출력된 식별코드를 스캔 또는 리딩하여 해당전자지갑으로 사용자가 보유한 암호화폐를 송금하는 단말일 수 있다. 이때, 암호화폐의 종류는 비트코인 등일 수 있으나, 이에 한정하지는 않는다.
- [197] 또한, 스캐너(305)는 금융 서비스를 제공하는 가맹점에 출입하고자 하는 회원 또는 사용자의 신분증 또는 여권의 진위여부 및 성인여부 등을 확인하고자 신분증을 스캔하는 장치일 수 있다. 이때, 스캐너(305)는 가맹점의 도어개폐장치(미도시)와 연동되어 회원임이 확인된 경우, 도어개폐장치로 도어개방 또는 액세스 허가 신호를 출력하는 장치일 수 있다. 이때, 스캐너(305)는 본 발명의 일 실시예에 따라 키오스크(50)와 일체로 형성될 수도 있다.
- [198] 예를 들어, IoT 자판기의 경우에는 일체로 형성될 수 있고, 키오스크(50)와 액세스하는 위치가 이격되어 있는 경우(예를 들어, 무인편의점과 같은 장소)는 별도로 설치될 수도 있으나, 이에 한정되지는 않고 다양한 실시예가 가능할 수 있음은 자명하다 할 것이다. 여기서, 스캐너(305)는, 네트워크를 통하여 원격지의 서버나 단말에 접속할 수 있는 컴퓨터로 구현될 수 있다. 상술한 바와 같이 유사하게 컴퓨터는 예를 들어, 네비게이션, 웹 브라우저(WEB Browser)가 탑재된 노트북, 데스크톱(Desktop), 랩톱(Laptop) 등을 포함할 수 있다.
- [199] 상술한 바와 같은 본 발명의 일 실시예에 따른 통합 시스템(10)에 포함된 키오스크(50)는 상기에서 설명된 블록체인 기반 금융 서비스를 제공하기 위해 기본적인 기능 또는 역할들을 수행할 수 있으며, 이를 수행하기 위한 복수의 구성 요소들을 포함할 수 있다.
- [200] 다만, 일반적으로 블록체인 기반의 금융 서비스 제공 방법을 통해 암호화폐로 결제 서비스를 사용하거나 환전 서비스를 사용하는 경우, 암호화폐의 사용과 관련하여 확인(confirm) 절차가 반드시 수반되어야 할 수 있다. 이와 같이, 암호화폐의 사용과 관련하여 반드시 수반되어야 하는 확인 절차는 처리되기까지 일정한 시간이 소요되거나 일정하지 않은 시간이 소요될 수 있다.
- [201] 본 발명의 일 실시예에 따른 금융 서비스 제공 시스템(1)에서 키오스크(50)는 암호화폐의 사용과 관련하여 수행되는 확인 절차의 처리 시간을 감소시키기 위해 환전용 암호화폐를 사용할 수 있다. 이하에서는 본 발명의 일 실시예에 따른 암호화폐 키오스크(50)가 환전용 암호화폐를 사용하여 처리 시간의 지연을 최소화하여 금융 서비스를 제공하는 방법이 설명될 수 있다. 더불어, 본 발명에서 사용되는 환전용 암호화폐는 'DPEC(Digital Payment Exchange Coin)' 또는 'D코인'이라 칭할 수 있으며, 이에 반드시 한정되는 것은 아닐 수 있다.
- [202] 구체적으로, 본 발명의 일 실시예에 따른 키오스크(50)는 사용자에게 언어의 종류가 선택되는 경우, 선택된 언어의 종류를 기반으로 금융 서비스를 제공할 수

- 있다. 예를 들어, 키오스크(50)는 사용자에게 의해 한국어가 선택된 경우, 키오스크(50)의 입출력부(예를 들어, 스크린, 화면 등과 같은 디스플레이 장치를 의미할 수 있음)를 통해 출력되는 언어가 한국어로 변환되도록 동작할 수 있다.
- [203] 또한, 키오스크(50)는 사용자에게 의해 통화의 종류가 선택되는 경우, 선택된 종류의 통화를 기반으로 금융 서비스를 제공할 수 있다. 예를 들어, 키오스크(50)는 사용자에게 의해 한국의 통화 종류인 원화가 선택된 경우, 키오스크(50)의 입출력부를 통해 입력 가능한 통화의 종류가 원화로 변환되도록 동작할 수 있다.
- [204] 이후, 키오스크(50)는 금융 서비스를 이용하는 사용자로부터 결제 서비스 또는 환전 서비스를 원하는 거래 금액을 입력 받을 수 있고, 입력된 거래 금액에 대한 암호화폐의 수량을 산출할 수 있다. 이때, 키오스크(50)는 사용자에게 의해 미리 선택된 언어의 종류 및 통화의 종류를 기반으로 동작할 수 있다. 이후, 키오스크(50)는 산출된 수량의 암호화폐를 송금할 지갑주소를 식별코드로 출력할 수 있고, 식별코드를 리딩 또는 스캔한 사용자의 사용자 단말을 통하여 지갑주소로 출력된 수량의 암호화폐가 입금되었는지의 여부를 확인할 수 있고, 암호화폐가 입금된 경우 입금 이벤트를 생성하여 출력할 수 있다.
- [205] 이후, 키오스크(50)는 입금 이벤트가 출력된 경우, 산출된 암호화폐의 수량에서 수수료를 제외한 나머지 수량의 암호화폐를 복수의 암호화폐 거래소들 중 가장 높은 거래가를 가지는 암호화폐 거래소로 전송할 수 있다. 이때, 키오스크(50)는 네트워크를 통해 암호화폐를 암호화폐 거래소로 전송할 수 있다.
- [206] 이와 동시에 키오스크(50)는 사용자의 지갑주소의 거래 내역 존재 여부를 확인할 수 있다. 이때, 키오스크(50)는 서버(20)를 통해 사용자의 지갑주소의 거래 내역 존재 여부를 확인할 수도 있다. 이후, 키오스크(50)는 사용자의 지갑주소의 거래 내역 존재 여부에 기초하여 자체적인 확인 절차를 수행할 수 있다.
- [207] 예를 들어, 키오스크(50)는 사용자의 지갑주소의 거래 내역이 존재하는 경우, 제로 확인(zero-confirmation)을 결정할 수 있다. 반면, 키오스크(50)는 사용자의 지갑주소의 거래 내역이 존재하지 않는 경우, 제로 확인(zero-confirmation)을 결정하기 전에 미리 정의된 일련의 확인 절차를 수행할 수 있다. 여기서, 미리 정의된 일련의 확인 절차는 키오스크(50) 내에 미리 정의된 프로그램 명령에 의해 수행될 수 있다.
- [208] 한편, 키오스크(50)에서 사용자의 지갑주소의 거래 내역 여부에 기초하여 자체적인 확인 절차를 수행하는 것으로 설명되었으나, 반드시 이에 한정되는 것은 아닐 수 있다. 즉, 키오스크(50)는 사용자의 지갑주소의 거래 내역 여부가 아닌 미리 설정된 기간에 상응하는 최근 거래 내역 여부에 기초하여 자체적인 확인 절차를 수행할 수도 있다. 또는, 키오스크(50)는 사용자의 지갑주소의 거래 내역 여부가 아닌 사용자의 지갑주소에 대한 정상 여부에 기초하여 자체적인 확인 절차를 수행할 수도 있으며, 이때 지갑주소에 대한 정상 여부에 대한

기준은 미리 정의될 수 있다.

- [209] 상기에서 설명된 바와 같이 본 발명의 일 실시예에 따른 키오스크(50)는 자체적인 확인 절차를 기반으로 거래 이벤트의 진행 여부를 결정하는 것을 의미할 수 있으며, 이는 암호화폐를 기반으로 수행되는 결제 및 환전 서비스를 제공하기 위해 필수적으로 수반되어야 하는 일반적인 확인 절차의 시간을 감소시키는 데 큰 효과를 가질 수 있다.
- [210] 이때, 키오스크(50)는 복수의 암호화폐 거래소들 중 거래가를 고려할 뿐 아니라, 암호화폐 거래소의 가격 변동성에 대한 안정성까지 고려할 수도 있다. 예를 들어, 키오스크(50)는 주기적으로 복수의 암호화폐 거래소들의 낙폭 등과 같이 안정성을 판단할 수 있는 요소를 확인할 수 있고, 이를 통해 암호화폐를 전송할 암호화폐 거래소를 결정할 수도 있다.
- [211] 이후, 키오스크(50)는 키오스크(50)와 미리 연동된 스캐너(305)를 통해 신분증 또는 여권을 스캔할 수 있다. 이후, 키오스크(50)는 스캔된 신분증 또는 여권의 위변조 여부를 판별하여 사용자의 본인여부를 확인할 수 있고, 금융 서비스의 확인 절차가 정상적으로 완료되는 경우 신분증 또는 여권에 대한 정보를 삭제할 수 있다. 여기서, 신분증 또는 여권에 대한 정보가 삭제되는 시점은 키오스크(50)에 미리 설정될 수 있다.
- [212] 이와 같은 방법을 통해, 키오스크(50)는 사용자의 신분증 또는 여권의 위변조 여부 판별을 통해 본인인 것으로 확인되는 경우, 거래 금액에 대응되는 수량의 암호화폐를 매도할 수 있고, 암호화폐로 변환되는 거래 금액에 대응되는 환전용 암호화폐를 환전용 암호화폐 거래소에서 매도할 수 있다. 이후, 키오스크(50)는 환전용 암호화폐의 매도를 통해 획득된 금액을 키오스크(50)가 설치된 가맹점을 운영하는 운영자의 계좌로 송금할 수 있다.
- [213] 한편, 본 발명의 일 실시예에 따른 키오스크(50)는 환전용 암호화폐의 낙폭에 따른 위험성을 미리 방지하여 금융 서비스가 제공될 수 있도록 동작할 수 있다. 구체적으로, 키오스크(50)는 환전용 암호화폐의 낙폭이 미리 설정된 기준보다 높은 경우, 서킷 브레이크를 수행함으로써 추가적인 거래 서비스 또는 환전 서비스가 수행되지 않도록 동작할 수 있다.
- [214] 도 3을 참조하면, 키오스크(50)의 제3 출력 모듈(240)은 제3 입력 모듈(230)을 통하여 사용자에게 의해 언어의 종류가 선택되는 경우, 선택된 언어로 화면을 변경할 수 있다. 이때, 무인 가맹점이나 자판기의 경우 사용자가 입력을 하지만, 유인 가맹점의 경우 키오스크(50)를 조작하는 사람에 의해 언어가 입력될 수 있다. 이와 같이, 제3 출력 모듈(240)은 사용자의 언어의 종류 및 통화의 종류를 선택받을 수 있고, 제3 출력 모듈(240)은 선택된 종류의 통화로 암호화폐의 현재 시세를 화면에 출력하고, 제3 출력 모듈(240)은 입력 받은 거래 금액을 결제하거나 환전하기 위한 암호화폐의 수량을 출력할 수 있고, 제3 출력 모듈(240)은 암호화폐를 송금할 지갑주소를 식별코드로 출력할 수 있다.
- [215] 예를 들어, 키오스크(50)는 IoT 자판기이고 한국에 위치하고, 미국에서 A가

한국에 여행을 와서 영화표를 구매한다고 가정하자. 이때, 영화표는 1 장 당 만원권이고, 1 장에 1 암호화폐이며, 다른 권종은 없다고 가정한다. 그리고, 1 암호화폐의 달러화 현재시세는 10 달러라고 하면, 제3 출력 모듈(240)은 암호화폐의 현재시세가 1 암호화폐 = 10 달러를 표시하고, 1 장당 1 암호화폐라는 것을 출력할 수 있다. 또한, A가 10장을 선택한 경우, 100달러에 대응하는 10 암호화폐를 입금할 전자지갑 주소가 생성되면, 제3 출력 모듈(240)은 입금자 A, 10 암호화폐의 정보를 담은 식별코드를 출력할 수 있다. 이때, 식별코드는 QR 코드일 수 있으나, 실시에에 따라 바코드 등의 다른 식별코드로 구현될 수 있음은 자명하다 할 것이다.

- [216] 다시 말해, 제3 출력 모듈(240)은 제3 입력 모듈(230)을 통하여 선택된 종류의 통화로 암호화폐의 시세를 검색하고, 사용자가 결제하거나 환전하고자 하는 거래 금액과 검색된 암호화폐의 시세를 제3 출력 모듈(240)로 출력할 수 있고, 제3 입력 모듈(230)을 통하여 입력 받은 거래 금액에 대응하는 암호화폐의 수량을 환전하기 위한 암호화폐가 입금될 지갑주소를 생성할 수 있고, 생성된 지갑주소를 입출력부(110)를 통하여 식별코드로 출력할 수 있다. 이때, 제3 제어 모듈(210)은 사용자로부터 제3 입력 모듈(230)을 통하여 입력된 거래 금액에 대한 암호화폐의 수량을 산출하고, 제3 제어 모듈(210) 및/또는 제3 통신 모듈(220)은 산출된 암호화폐의 수량에서 수수료를 제외한 나머지 수량의 암호화폐를 복수의 암호화폐 거래소들 중 가장 높은 거래가를 가지는 암호화폐 거래소로 전송할 수 있다.
- [217] 제3 제어 모듈(210)에서 식별코드를 리딩 또는 스캔한 사용자의 사용자 단말을 통하여 지갑주소로 출력된 수량의 암호화폐가 입금되었는지의 여부를 확인할 수 있고, 암호화폐가 입금된 경우 입금 이벤트를 생성하여 출력하여 지불완료처리가 되도록 제어할 수 있다. 이때, 제3 제어 모듈(210)은 자체적으로 지갑주소에 접근하여 입금여부를 확인할 수도 있지만, 상술한 바와 같이 구현예에 따라 서버(20)에서 확인된 입금여부에 대한 결과값만을 얻을 수도 있다.
- [218] 한편, 제3 제어 모듈(210)은 사용자의 지갑주소의 거래 내역 존재 여부에 기초하여 자체적인 확인 절차를 가질 수 있다.
- [219] 또한, 제3 제어 모듈(210)은 사용자의 신분증 또는 여권의 위변조 여부 판별을 통해 본인인 것으로 확인되는 경우 상기 거래 금액에 대응되는 수량의 암호화폐를 매도하고, 상기 암호화폐로 변환되는 거래 금액에 대응되는 환전용 암호화폐를 환전용 암호화폐 거래소에서 매도할 수 있다.
- [220] 이후, 제3 제어 모듈(210)은 환전용 암호화폐의 매도를 통해 획득된 금액을 상기 서비스 제공 장치가 설치된 가맹점을 운영하는 운영자의 계좌로 송금할 수 있다. 추가적으로, 제3 제어 모듈(210)은 영수증을 출력하는 기능을 더 수행할 수 있다. 예를 들어, 입금 이벤트가 출력된 경우 입력 받은 거래 금액 및 블록체인 수수료를 합산한 금액의 영수증을 출력할 수 있다. 이때, 제3 제어 모듈(210)은

키오스크(50)의 시리얼 넘버, 트랜잭션 일시, 지갑주소, 코인수량, 상품 수량, 및 선택된 종류의 통화로 환산한 트랜잭션 금액을 포함한 영수증 인쇄 목록을 인쇄하여 출력할 수 있다. 이때, 코인수량의 코인은 특정 암호화폐를 지칭하는 것은 아니고, 암호화폐의 단위를 일컫는 용어로 정의하기로 한다. 여기서, 식별코드는 지갑주소 및 입금할 코인의 수량의 정보를 포함할 수 있다.

- [221] 상술한 바와 같은 과정에서 제3 제어 모듈(210)은 키오스크(50)의 각 구성요소를 제어할 수 있고, 입출력 신호를 전달하며 전반적인 입출력관리 및 명령신호를 제어하는 역할을 수행할 수 있다.
- [222] 한편, 스캐너(305)는 신분증 또는 여권의 위변조 여부를 판별한 결과 위변조가 되지 않은 원본인 경우 본인확인을 완료할 수 있다. 이때, 스캐너(305)는 위변조 여부 뿐만 아니라 성인인증을 수행할 수도 있다. 이에 따라, 위변조 여부는 적외선(IR) 및 홀로그램(OVD)를 통하여 판별될 수 있고, 스캐너(305)는 스캔된 여권 또는 신분증의 주민등록번호 또는 생년월일의 OCR을 이용하여 성인인증을 확인할 수 있다.
- [223] 이때, 스캐너(305)에서 수행되는 신분증 위변조 여부와 성인인증을 하기 위한 방법은 신분증에 기입된 신분 정보의 유효성 검사, 적외선 램프로부터 주사된 적외선 투과 값을 산출하고 비교하는 적외선 검사, 자외선 램프로부터 주사된 자외선 반사 값을 산출하고 비교하는 자외선 검사의 단계를 거쳐 판별하는 방법을 이용할 수 있고, 이에 따라 획득한 이미지 데이터가 자동적으로 저장되므로 신분증 복사본을 준비할 필요가 없고, OCR(Optical Character Reader) 처리를 통해 획득한 정보는 데이터베이스에 자동 저장되므로 개인정보 입력을 위한 입력과정이 불필요해질 수 있다.
- [224] 스캐너(305)는 키오스크(50)와 연동되도록 출입 구역에 설치되어 회원이 가맹점에 접근 가능하도록 가맹점의 도어개폐를 제어할 수 있고, 사용자의 신분증 또는 여권의 위변조 여부를 판별하여 본인확인을 완료할 수 있다. 이때, 성인인증을 통하여 도어오픈을 허용할 수도 있고, 성인일지라도 회원이 아니면 접근하지 못하도록 도어오픈을 불허할 수도 있는데, 이는 어떠한 객체에게 가맹점으로의 접근을 허용할지에 대한 다양한 실시예에 따라 달라질 수 있는 구성이므로 상술한 조건에 한정되지 않음은 자명하다 할 것이다.
- [225] 한편, 키오스크(50)는 블록체인의 복수의 노드들 중 하나의 노드일 수 있다. 이때, 암호화폐 중 비트코인에 대해 살펴보면 전자서명(암호화 프로토콜)과 인터넷을 이용한 전자적 지불수단의 일종이며 금 등의 실물자산과 국가 등의 발행주체의 신용력에 의존하는 대신 인터넷을 통해 접속된 분산형(Peer to Peer, 이하 P2P라 한다) 네트워크에서 데이터 송수신을 통해 참가자(채굴자)가 Proof of Work라고 하는 특수한 계산작업을 (신규생성 비트코인의 교부를 인센티브로서) 자주적이고 경쟁적으로 행하여 정당성이 인정된 블록체인 공개거래기록을 연속적으로 보존하는 것으로 이중지불의 위험이 방지되는 점이 최대의 특징이다.

- [226] 법정통화의 송금이 원칙적으로 금융기관과 송금업자 등의 매개기관을 통해 행할 필요가 있는 것에 비해, 비트코인의 경우 사용자의 전자지갑이 P2P네트워크에서의 접속 포인트로서 기능하고 비트코인을 사용자의 전자지갑 간 직접 거래하는 것이 가능하다. 비트코인은 특정한 발행주체가 존재하지 않는 점에서 중앙 은행이 발행하는 전통적인 화폐와 법정통화 그 자체는 아닌 점은 명확하지만 비트코인에 지불가치, 교환가치가 있다고 사인이 인정한 점, 게다가 그 자체가 근거로써, 채권채무관계의 해소를 위한 지불 및 결제수단과 격지자 간의 자금이동에 이용할 수 있고, 통화와 결제성 자금에 유사한 기능을 다하고 있다. 일반인이 비트코인을 이용할 경우, 자신의 PC등에 인스톨한 전자지갑주소, 또는 비트코인거래소의 사이트에 개설한 주소를 통해서 엔과 미국 달러 등의 전통적 화폐를 지불하고 비트코인을 구입한 다음, 비트코인이 사용가능한 온라인마켓 등에서 상품을 구입하거나, 서비스를 받는 대가로 사용하거나 다른 이용자와의 간에 판매를 하거나 혹은 전통적 화폐로 재환금 등을 할 수 있다.
- [227] 한편, 블록체인은 P2P(Peer-to-Peer) 네트워크, 암호화, 분산 장부, 분산 합의와 같이 크게 4가지의 기반 기술로 구성되어 있고, 본 발명에서는 블록체인 기술을 이용하여 비대면 암호화폐 결제를 수행하도록 한다. 각각의 기술들은 블록체인의 가치라 할 수 있는 탈중앙화, 데이터의 무결성 유지 등을 위해 상호 보완적인 관계를 취하고 있으며 블록체인 동작 메커니즘의 근간을 이루고 있다. 그리고, 블록체인 환경에서의 응용 기술인 스마트 컨트랙트는 프로그램의 실행 코드 및 그 결과에 대한 무결성, 신뢰성을 제공해주는 기술로서 자동화된 거래, 제어 등의 분야에서 주목받고 있다. 우선, 블록체인의 참여자들 간 연결 및 통신은 P2P 네트워크를 기반으로 하여 이루어진다. P2P 네트워크는 기존 클라이언트-서버 방식에서 탈피한 동등한 계층의 참여자들로 이루어지는 네트워크로서 크게 structured P2P(구조적 P2P)와 unstructured P2P(비구조적 P2P)로 분류된다. 특히 unstructured P2P는 서버를 중심으로 참여자들 간의 망이 이루어지는 중앙 집중형 방식과 데이터의 flooding 알고리즘을 기반으로 하는 분산형 P2P 네트워크로 다시 구분할 수 있다. 블록 체인은 기술의 특징이자 이념인 탈중앙화 분산 네트워크를 위해 flooding 기반의 unstructured P2P 네트워크를 사용한다. 또한 P2P 네트워크의 통신은 UDP를 통하여 이루어지는 것이 일반적이지만, 블록체인에서는 TCP/IP를 사용하고 있다. 따라서 블록체인의 참여자들은 자신과 물리적으로 가장 인접한 참여자들의 IP를 유지하고 있으며(비트코인의 경우, 3개의 IP를 유지) 이를 사용하여 메시지 및 데이터를 주고받는다.
- [228] 두 번째로, 블록체인에서 사용되는 암호화 기술은 ① 데이터의 무결성 검증을 위한 머클 트리(Merkle Tree), ② 거래의 부인방지를 위한 공개키 기반 디지털 서명 기법이 사용되고 있다. 머클 트리는 해시 트리의 일종으로 모든 비리프노드의 이름이 자식 노드들의 해시로 구성된 트리를 일컫는다. 즉, 리프

노드들은 파일이나 특정 값 등의 데이터를 가리키며 상위 노드는 이 리프 노드의 해시로 구성된다. 이러한 방식으로 구성된 머클 트리의 루트 노드는 트리를 구성하는 모든 리프 노드들의 데이터의 해시값으로 이루어져 있으며 사용자는 루트 노드의 해시를 검증하는 것만으로 데이터들의 위변조를 검증할 수 있다. 따라서 블록체인에서는 리프 노드에 참여자들 간의 거래, 정보 등을 삽입함으로써 머클 트리의 기초를 구성하며 상위 노드를 만들 때 사용될 수 있는 해시 함수는 여러 가지가 있으나 블록체인에서는 SHA-256 함수를 사용하여 머클 트리를 활용하고 있다.

- [229] 공개키 기반의 디지털 서명 방식은 사전에 비밀 키를 나누어 가지지 않은 참여자 간의 안전한 통신을 이루어지게 하는 암호화 기술로 본인 인증 등의 분야에서 널리 사용되고 있다. 공개 키 기반 구조에서는 공개 키와 비밀 키 두 개의 키 쌍이 존재하며, 공개 키는 모든 참여자들이 알 수 있지만 이에 대응되는 비밀키는 해당 소유자만이 알 수 있도록 유지되어야 한다. 이러한 공개 키 기반 디지털 서명 방식을 블록체인에서는 거래의 유효성을 검증하는데 사용하고 있다. 거래를 발생시키려는 사용자가 자신의 비밀 키를 사용하여 해당 거래에 대해 서명을 하고 이에 대응되는 자신의 공개 키와 함께 블록체인 네트워크에 거래정보를 전송한다. 이 거래 정보를 받은 다른 모든 참여자들은 거래에 담긴 송신자의 공개 키를 이용하여 해당 거래의 유효성을 검증하고 이를 통해 그 거래는 블록체인의 참여자가 보냈음을 확인한다.
- [230] 세 번째로, 분산 장부는 참여자들 간의 합의에 의해 복제되고 공유, 동기화된 정보의 기록 저장소이다. 특히 분산 장부가 P2P 네트워크상에서 적용되기 위해서는 분산 장부의 기록에 대한 참여자들의 합의가 필요하다는 특징을 가지며 이는 블록체인에서도 그 특징을 유지하고 있다. 블록체인에서 분산 장부는 발생하는 모든 거래, 정보들을 참여자들의 검증과정을 거쳐 기록하며, 모든 참여자가 동일한 정보를 유지한다. 거래나 정보를 검증할 시에는 먼저 참여자 개개인이 유지하고 있는 분산 장부에 이미 기록되어 있는 정보와의 연결성을 확인하고 참여자들 간의 합의를 거쳐 적법한 거래나 정보만이 블록체인의 분산 장부에 저장된다.
- [231] 거래나 정보를 저장 시에는 이들을 일정 시간동안 누적하여 블록이라는 단위로 저장하고 이 블록 간의 연결성을 부여한 상태에서 분산 장부에 저장한다. 이러한 분산 장부는 블록체인이 제공하는 데이터 무결성 보장의 바탕이 된다. 블록체인에 참여하고 있는 모든 사용자들은 동일한 분산 장부의 데이터를 유지하고 있기 때문에 외부에서 공격자가 특정 데이터를 위변조하거나 이중거래 등을 시도하기 위해서는 참여자들이 유지하고 있는 분산 장부들 중 절반 이상의 장부들에 대해 공격을 시도해야 하기 때문에 높은 비용과 컴퓨팅 리소스가 필요로 한다.
- [232] 네 번째로, 분산 합의는 분산 컴퓨팅과 멀티 에이전트 시스템 등의 분야에서 결함이 있는 프로세스가 있는 경우, 전반적인 시스템의 신뢰성을 달성하기

위하여 프로세스나 에이전트 간의 특정 데이터 값에 대한 동의를 이끌어내는 프로토콜이다. 이를 위한 분산 합의 프로토콜은 다음과 같은 성질을 지니고 있다.

- [233] 우선, 유효성(Validity), 즉 모든 올바른 프로세스들이 동일한 데이터를 제안했다면, 모든 프로세스들은 제안된 데이터에 결정(유효, 무효)을 내리고, 두 번째로, 무결성(Integrity), 즉 모든 올바른 프로세스들이 하나의 데이터를 채택하였다면 그 데이터는 다른 프로세스에 의해 제안된 데이터이며, 세 번째로, 동의(Agreement), 모든 올바른 프로세스들은 반드시 어떤 데이터에 대해 동의하여야 하며, 네 번째로, 종료(Termination), 모든 올바른 프로세스들은 어떤 데이터들에 대해 결정을 내려야 한다.
- [234] 블록체인에서는 위와 같은 분산 합의 프로토콜 설계하고 이를 통해 발생하는 거래나 정보에 대해 참여자 간의 합의를 이끌어낸다. 합의를 거쳐 적합한 거래나 정보만이 블록체인에서 유지되기 때문에 핵심이 되는 부분 중 하나이다.
- [235] 또한, 어떠한 방식의 분산 합의 프로토콜을 사용하고 있는가에 따라 블록체인의 특징이 구별되어지고 시스템의 신뢰성 또한 영향을 받는다. 대표적인 블록체인 서비스라고 할 수 있는 비트코인의 경우 작업 증명(Proof-of-work)이라는 분산 합의 프로토콜을 사용하고 있다. 이 작업 증명 프로토콜은 참여자들이 블록으로 저장되기 위한 거래 및 데이터들과 SHA-256 해시 함수를 사용하여 시행착오 방식으로 특정 해시 값을 찾아내는 작업을 함으로써 참여자 간의 블록 정보에 대한 합의를 이끌어내는 프로토콜이다. 이때, 블록체인은 지분증명(Proof-of-stake)이라는 투표 기반합의 알고리즘을 사용할 수 있으며, 보안성은 작업 증명 합의보다 낮아졌지만 합의 속도, 전력낭비 문제를 해결할 수 있다.
- [236] 또한, 본 발명의 일 실시예에서는 스마트 컨트랙트를 이용할 수 있다. 스마트 컨트랙트는 전자 상거래를 위한 컴퓨터 프로토콜로, 계약 조건을 실행하는 컴퓨터 트랜잭션 프로토콜로 정의되고 있으며, 거래의 신뢰를 위한 중개인을 최소화하는 한편 계약 조건을 충족시키고 악의적인 예외를 최소화하는데 그 목적이 있다. 블록체인에서는 이와 같은 스마트 컨트랙트를 지원하는데 이를 통하여 중개 혹은 중앙 기관 없이 거래 당사자 간의 자동화된 직접 거래를 가능케 하며, 그 조건과 결과를 모두 분산 장부에 유지함으로써 거래 정보의 신뢰성과 무결성을 보장한다. 즉, 사용자는 자신이 원하는 조건을 담은 프로토콜 스마트 컨트랙트를 프로그래밍하여 블록체인에 저장하고, 특정 조건이 만족되면 해당 스마트 컨트랙트는 다른 블록체인 참여자들에 의해 검증 및 실행이 된다. 실행 결과는 다시금 블록체인에 저장되어 거래 결과에 대한 정보의 무결성과 신뢰성 또한 보장한다. 특히, 컴퓨팅 파워를 가진 기기 간의 자동, 자율적 협업 및 제어가 블록체인의 스마트 컨트랙트로 가능하다. 후술할 블록체인과 대비되는 개념으로 상술한 블록체인은 퍼블릭 블록체인(Public Blockchain)으로 정의할 수 있다.

- [237] 이에 더하여, 본 발명은 프라이빗 블록체인을 더 이용할 수 있는데, 프라이빗 블록체인이란 각 가맹점을 노드로 하여 트랜잭션 데이터, 회원 데이터, 구매 데이터 등을 공유하는 네트워크로 정의될 수 있다. 이는, 공개되지 않고 각 가맹점 간에서만 보유하는 네트워크로 구성되며, 그 기능은 상술한 블록체인의 기능을 모두 포함할 수 있다. 그리고, 프라이빗 블록체인은, 본 발명의 일 실시예에 따른 한 회사가 모든 것을 통제하는 기업형 블록체인으로, 암호 감사(Cryptographic auditability)의 기능이 추가된 기존의 중앙집중식 데이터베이스로 정의될 수 있고, 중앙관리의 역할은 유지하되 기존의 중앙집중방식의 보안성을 개선하고 프로세스처리의 한계 등을 해결할 목적으로 도입될 수 있으며, 특정한 기관, 업체들의 목적 및 특성에 맞도록 설계된 블록체인이기 때문에, 블록체인이 가지는 공개성 및 분산성 등의 특성을 모두 구현하지 않아도 가능하나, 해당 특성을 모두 구현할 수 있음은 상술한 바와 같다. 이때, 프라이빗 블록체인은 네트워크상 운용노드가 각 가맹점으로 제한되어 있기 때문에 코인을 발행할 경제적 토대가 마련되지 않는 경우 발행할 필요는 없으나 발행되는 것을 제한하는 것은 아니다. 또한, 프라이빗 블록체인은 데이터를 분산하여 관리하는데 적합한 방식일 수 있다.
- [238] 또한 본 발명의 일 실시예에 따른 통합 시스템(10)은 복수의 키오스크를 포함할 수 있으며, 다음과 같은 특징을 더 포함할 수 있다.
- [239] ① 복수의 키오스크는 상기 복수의 키오스크의 트랜잭션을 관리하는 서버(20)와 연동될 수 있다. 그리고, 서버(20)는 복수의 키오스크 내에 발생하는 트랜잭션 및 구매 데이터를 복수의 키오스크를 각각의 노드로 하는 프라이빗 블록체인에 반영할 수 있고, 트랜잭션 및 구매 데이터로부터 채고 데이터를 업데이트 및 관리할 수 있고, 프라이빗 블록체인은 복수의 키오스크 간의 분산 장부를 공유하는 P2P 네트워크일 수 있다. 이때, 프라이빗 블록체인에서 공유하는 분산 장부는 상술한 블록체인의 분산 장부의 기능을 포함할 수 있다.
- [240] 이때, 서버(20)는 복수의 키오스크에서 암호화폐로 결제할 수 있는 회원을 등급별 및 연령별로 관리할 수 있고, 회원의 마일리지와 구매내역정보를 업데이트하여 프라이빗 블록체인을 관리할 수 있다.
- [241] ② 그리고, 서버(20)는 회원관리를 가맹점에 출입시의 신분증 또는 여권 스캔을 통하여 관리할 수 있고, 블록체인과 트랜잭션을 블록체인 엔진 관리를 통하여 실시할 수 있으며, 스마트 컨트랙트 관리는 체인코드를 이용한 자율거래 계약을 관리함으로써 실시할 수 있다. 예를 들어, 웹 서버, 인증 서버, API 서버, 지갑 서버, 관리자 서버 등과 같은 다양한 서버들은 서로 서비스 요청을 통해 동작을 수행할 수 있으며, 이들은 데이터베이스를 기반으로 동작을 수행할 수 있다.
- [242] ③ 키오스크(50)는 상술한 서버(20)에 의해 관리될 수 있으며, 입출력부(110)를 통하여 거래를 수행하거나 환전을 수행하는데 사용되는 언어의 종류가 선택되는 경우, 입력된 언어로 화면을 변경할 수 있다. 이때, 언어를 선택할 수 있는 사용자 인터페이스는 암호화폐 결제의 모든 프로세스의 화면에 배치될 수

있다.

- [243] ①과 같은 키오스크(50)는 사용자가 메인 화면을 클릭 또는 터치하는 경우, 결제를 수행하는 화면으로 이동할 수 있다.
- [244] ④ 키오스크(50)는 제3 입력 모듈(230)을 통하여 선택된 종류의 통화로 암호화폐의 시세를 검색하고, 검색된 암호화폐의 시세를 제3 출력 모듈(240)로 출력할 수 있다. 이때, 제3 출력 모듈(240)은 상품의 수량, 상품의 가격, 암호화폐 수량, 암호화폐 거래 및 환전 수수료, 가암호화폐 합계 등의 정보를 표시할 수 있지만, 나열된 것들로 한정되는 것은 아니다.
- [245] ⑤ 키오스크(50)는 제3 입력 모듈(230)을 통하여 입력 받은 거래 금액에 대응되는 암호화폐가 입금될 지갑주소를 생성하고, 생성된 지갑주소를 제3 출력 모듈(240)을 통하여 식별코드로 출력할 수 있다. 이때, 결제가 수행될 때마다 새로운 지갑주소를 생성하여 고객별로 입금 주소를 부여할 수 있으나, 회원인 경우 회원의 고유 코드를 이용할 수도 있다. 이에 따라, 지갑주소로 사용자(고객)는 제1 단말(30)로 QR 코드를 포함한 식별코드를 스캔 또는 리딩하여 암호화폐를 전송하게 되고, 이때 키오스크(50)는 QT 서버(미도시)를 통하여 입금여부를 지속적으로 체크하게 되고, 입금이 되는 경우 바로 배출화면으로 이동하게 되지만, 제1 단말(30)에서 입금(암호화폐 전송)은 하였지만, QT 서버에서는 계속 체크 중인 경우에는 키오스크(50)는 시리얼 넘버(기계 번호), 지갑주소, 암호화폐 수량, 상품 가격, 금액 등을 인쇄하는 입금영수증 인쇄 프로세스를 진행할 수 있다.
- [246] 이에 따라, 키오스크(50)의 제3 제어 모듈(210)은 제3 제어 모듈(210)에서 식별코드를 리딩 또는 스캔한 사용자의 제1 단말(30)을 통하여 지갑주소로 출력된 수량의 암호화폐가 입금되었는지의 여부를 확인할 수 있고, 암호화폐가 입금된 경우 입금 이벤트를 생성하여 출력하여 결제완료처리를 제어할 수 있다.
- [247] 물론, 제3 제어 모듈(210)은 상술한 구성 이외에도 각 구성요소의 제어를 담당할 수 있음은 자명하다 할 것이다. 이때, 상품의 가격은 암호화폐의 검색된 실시간 시세에 대응하는 선택된 통화의 금액에 기초한 결제금액이다. 즉, 암호화폐는 변동성이 크기 때문에 실시간 시세를 조회 및 환전하도록 거래하는 것이 중요한데 조회 당시 또는 트랜잭션 당시의 금액을 기준으로 환가를 할 수 있으며, 이는 실시예에 따라 어느 시점을 기준으로 할 것인지에 대한 변동이 존재할 수 있음은 물론이라 할 것이다.
- [248] 상술한 바와 같이 ① 내지 ⑤를 참조하여 설명된 본 발명의 일 실시예에 따른 시스템(10)의 동작 방법이 수행되는 동안 도 1 및 도 2를 참조하여 설명된 환전용 암호화폐를 기반으로 금융 서비스가 수행될 수 있는 것은 자명한 것으로 볼 수 있다.
- [249] 또한, 본 발명의 일 실시예에 따른 금융 서비스는 환전 서비스를 포함할 수 있으며, 키오스크(50)는 상기 환전 서비스를 제공하는 ATM(Automated Teller Machine)에 적용될 수 있다.

- [250] 먼저, (a) 키오스크(50)는 사용자가 각국의 언어 중 자신이 사용하고자 하는 언어를 선택할 수 있도록 화면을 출력할 수 있고, 화면에서 사용자가 언어를 선택하면 (b) 와 같이 숫자 키패드를 출력할 수 있고, 사용자에게 의해 환전할 거래 금액을 입력 받을 수 있다. 환전할 거래 금액의 통화 종류를 설정하면 이에 대응하는 수량의 암호화폐와 수수료가 표시되며, 총 지불될 암호화폐의 개수가 표시될 수 있다. 사용자가 이 화면에서 다음 버튼을 선택하게 되면 (c) 와 같은 화면으로 전환되는데, 고객(사용자)에게 화면의 QR 코드로 암호화폐를 보내달라고 요청하는 화면이 출력될 수 있다.
- [251] 이때, 사용자는 자신의 지갑에서 QR 코드를 스캔하여 암호화폐를 전송할 수 있고(스캔 이체), 사용자가 이체를 한 것을 키오스크(50)는 확인하고, 해당 수량의 암호화폐가 입금되면 키오스크(50)는 영수증을 인쇄할 수 있다. 이때, 암호화폐의 수수료 퍼센트는 조정 가능하다.
- [252] 즉, 키오스크(50)는 암호화폐가 입금되고(0 CONFIRM), 블록체인에서 1 확인만(전체 6 확인) 발생하면, 사업장의 외부지갑(거래소)으로 서버에서 자동으로 블록체인 수수료를 제외하고 전송할 수 있고, 거래소 사업장 계정에서 전송 받은 금액을 매도 주문 처리하며(계약), 매도체결 금액(원/KRW)을 키오스크(50)의 운영자 계좌로 이체할 수 있다. 또한 1 확인까지 시간이 최소 10분에서 20분 이상 소요될 수 있으므로, 즉시처리를 위해서는 사고 대비 본인확인을 위한 신분증 또는 여권의 인식을 선행 후 확인이 완료되면 자동삭제 처리할 수 있도록 구성될 수 있다.
- [253] 이때, (e) 본인확인 절차는 즉시 환전을 위한 절차로 확인을 위해서는 시간이 필요하기 때문에 그사이 발생할 수 있는 사고 리스크를 사전에 방어하고 사고가 발생하면 당사자를 추적할 수 있도록 진행될 수 있다. 이때, 확인 절차가 정상적으로 종료되면 신분증 또는 여권 정보는 자동 삭제될 수 있고, 본 발명의 일 실시예에 따른 키오스크(50)는 외국인을 위한 시내 환금기(KIOSK) 텍스 리펀드 신청 시 본인 신용카드 정보를 남기는 것(100일 내 출국)에 비하여 개인정보 보호에 더욱 강력한 절차를 수행할 수 있다.
- [254] 이후, (f) 키오스크(50)에서 출금 중일 때의 화면을 도시하는데, 본 발명의 일 실시예에 따른 키오스크(50)와 연동되도록 키오스크(50)에 설치된 현장에 CCTV가 더 설치될 수 있다. 즉, 출금 시비가 발생하는 것을 방지하기 위함 일 수 있다. 이때, 현장 키오스크(50) 운영 사업자가 CCTV를 통하여 현금 장입에 대한 관리를 할 수 있으며, 관리 프로그램에서 잔고 확인이 가능하도록 구성될 수 있다. ATM 사용 수수료는 환전금액의 3%로 부과할 수 있으나 변동 가능성은 상술한 바와 같다.
- [255] 도 8은 본 발명의 일 실시예에 따른 통합 시스템의 동작을 나타내는 흐름도이다.
- [256] 도 8을 참조하면, 키오스크는 상기 키오스크의 입출력부를 통해 금융 서비스를 이용하는 사용자로부터 입력된 거래 금액에 대한 암호화폐의 수량을 산출할 수

있다(S720).

- [257] 또한 키오스크는 산출된 암호화폐의 수량에서 수수료를 제외한 나머지 수량의 암호화폐를 복수의 암호화폐 거래소들 중 가장 높은 거래가를 가지는 암호화폐 거래소로 전송할 수 있다(S720).
- [258] 이때, 키오스크는 입출력부를 통해 사용자로부터 언어의 종류 및 통화의 종류를 선택 받을 수 있고, 선택된 종류의 언어 및 선택된 통화의 종류를 기반으로 금융 서비스를 제공할 수 있다. 또한, 키오스크는 입출력부를 통해 산출된 수량의 암호화폐를 송금할 지갑주소를 식별코드로 출력할 수 있고, 식별코드를 리딩 또는 스캔한 사용자의 사용자 단말을 통하여 지갑주소로 출력된 수량의 암호화폐가 입금되었는지의 여부를 확인할 수 있고, 암호화폐가 입금된 경우 입금 이벤트를 생성하여 출력할 수 있다.
- [259] 이때, 키오스크는 도 1을 참조하여 설명된 바와 같이 사용자의 지갑주소의 거래 내역 존재 여부에 기초하여 자체적인 확인 절차를 가질 수 있으며, 이에 대한 구체적인 설명은 도 1을 참조하여 설명된 바와 동일하여 생략될 수 있다.
- [260] 이후, 키오스크는 키오스크와 미리 연동된 스캐너를 통해 신분증 또는 여권을 스캔할 수 있고, 스캔된 신분증 또는 여권의 위변조 여부를 판별하여 사용자의 본인여부를 확인할 수 있고, 금융 서비스의 확인 절차가 정상적으로 완료되는 경우 신분증 또는 여권에 대한 정보를 삭제할 수 있다.
- [261] 이후, 키오스크는 키오스크의 환전용 암호화폐 운영부를 통해 사용자의 신분증 또는 여권의 위변조 여부를 판별을 통해 본인인 것으로 확인되는 경우 거래 금액에 대응되는 수량의 암호화폐를 매도할 수 있다(S740).
- [262] 암호화폐로 변환되는 거래 금액에 대응되는 환전용 암호화폐를 환전 암호화폐 거래소에서 매도할 수 있다(S740).
- [263] 이후, 키오스크는 키오스크의 금액 송금부를 통해 환전용 암호화폐의 매도를 통해 획득된 금액을 키오스크가 설치된 가맹점을 운영하는 운영자의 계좌로 송금할 수 있다(S750).
- [264] 상술한 바와 같은 방법을 통해 블록체인 기반의 금융 서비스를 제공하는 키오스크는 환전용 암호화폐의 낙폭이 미리 설정된 기준보다 높은 경우, 서킷 브레이크가 수행함으로써 암호화폐 결제 서비스 또는 암호화폐 환전 서비스가 수행되지 않도록 방지할 수 있다.
- [265]
- [266] 한편, 본 발명의 일 실시예에 따른 블록체인 기반의 금융 서비스를 제공하는 키오스크가 구현되는 측면에 있어서, 키오스크가 키오스크를 직접적으로 운영하거나 운용하는 사용자가 없는 무인 ATM으로 구현되는 경우, 사용자의 신분 확인을 위해 신분증 또는 여권 등을 통해 스캔 절차가 필수적으로 필요할 수 있다. 이와 같은 스캔 절차는 금융 서비스가 수행되는 동안에 임시로 저장될 수 있으며, 이를 통해 부당한 목적(자금 세탁 등)의 암호화폐 사용 등을 방지하거나 부당한 목적으로 암호화폐가 사용되는 경우에 이를 해소하기 위한

정보를 확보하기 위한 절차를 의미할 수 있다.

- [267] 반면, 본 발명의 일 실시예에 따른 키오스크가 키오스크를 운영하거나 운용하는 사용자가 있는 가맹점과 같은 곳에서 사용되는 장치로 구현되는 경우, 암호화폐를 이용한 서비스를 위해서는 비용이 우선적으로 지불될 수 있도록 선결제 절차가 필요할 수도 있다. 이와 같은 본 발명의 일 실시예에 따른 키오스크의 기술적 특징에 따라 키오스크가 구현되는 방식 및 적용되는 절차가 서로 달라질 수 있는 것을 통상의 기술자에게 자명한 사실에 해당할 수 있으며, 이에 대한 구체적인 설명은 생략될 수 있다.
- [268] 본 명세서와 도면에 개시된 본 발명의 실시예들은 본 발명의 기술 내용을 쉽게 설명하고 본 발명의 이해를 돕기 위해 특정 예를 제시한 것일 뿐이며, 본 발명의 범위를 한정하고자 하는 것은 아니다. 즉 본 발명의 기술적 사상에 바탕을 둔 다른 변형예들이 실시 가능하다는 것은 본 발명의 속하는 기술 분야에서 통상의 지식을 가진 자에게 자명한 것이다. 또한 상기 각각의 실시예는 필요에 따라 서로 조합되어 운용할 수 있다. 예컨대, 본 발명의 모든 실시예는 일부분들이 서로 조합되어 본 발명의 시스템(10), 서버(20), 제1 단말(30) 및/또는 제2 단말(40)에 의해 구현될 수 있다.
- [269] 또한, 본 발명의 시스템(10), 서버(20), 제1 단말(30) 및/또는 제2 단말(40)을 제어하는 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다.
- [270] 이와 같이, 본 발명의 다양한 실시예들은 특정 관점에서 컴퓨터 리드 가능 기록 매체(computer readable recording medium)에서 컴퓨터 리드 가능 코드(computer readable code)로서 구현될 수 있다. 컴퓨터 리드 가능 기록 매체는 컴퓨터 시스템에 의해 리드될 수 있는 데이터를 저장할 수 있는 임의의 데이터 저장 디바이스이다. 컴퓨터 리드 가능 기록 매체의 예들은 읽기 전용 메모리(read only memory: ROM)와, 랜덤-접속 메모리(random access memory: RAM)와, 콤팩트 디스크- 리드 온니 메모리(compact disk-read only memory: CD-ROM)들과, 마그네틱 테이프(magnetic tape)들과, 플로피 디스크(floppy disk)들과, 광 데이터 저장 디바이스들, 및 캐리어 웨이브(carrier wave)들(인터넷을 통한 데이터 송신 등)을 포함할 수 있다. 컴퓨터 리드 가능 기록 매체는 또한 네트워크 연결된 컴퓨터 시스템들을 통해 분산될 수 있고, 따라서 컴퓨터 리드 가능 코드는 분산 방식으로 저장 및 실행된다. 또한, 본 발명의 다양한 실시예들을 성취하기 위한 기능적 프로그램들, 코드, 및 코드 세그먼트(segment)들은 본 발명이 적용되는 분야에서 숙련된 프로그래머들에 의해 쉽게 해석될 수 있다.
- [271] 또한 본 발명의 다양한 실시예들에 따른 장치 및 방법은 하드웨어, 소프트웨어 또는 하드웨어 및 소프트웨어의 조합의 형태로 실현 가능하다는 것을 알 수 있을 것이다. 이러한 소프트웨어는 예를 들어, 삭제 가능 또는 재기록 가능 여부와 상관없이, ROM 등의 저장 장치와 같은 휘발성 또는 비휘발성 저장 장치, 또는 예를 들어, RAM, 메모리 칩, 장치 또는 집적 회로와 같은 메모리, 또는 예를 들어

콤팩트 디스크(compact disk: CD), DVD, 자기 디스크 또는 자기 테이프 등과 같은 광학 또는 자기적으로 기록 가능함과 동시에 기계(예를 들어, 컴퓨터)로 읽을 수 있는 저장 매체에 저장될 수 있다. 본 발명의 다양한 실시예들에 따른 방법은 제어부 및 메모리를 포함하는 컴퓨터 또는 휴대 단말에 의해 구현될 수 있고, 이러한 메모리는 본 발명의 실시예들을 구현하는 명령들을 포함하는 프로그램 또는 프로그램들을 저장하기에 적합한 기계로 읽을 수 있는 저장 매체의 한 예임을 알 수 있을 것이다.

- [272] 따라서, 본 발명은 본 명세서의 청구항에 기재된 장치 또는 방법을 구현하기 위한 코드를 포함하는 프로그램 및 이러한 프로그램을 저장하는 기계(컴퓨터 등)로 읽을 수 있는 저장 매체를 포함한다. 또한, 이러한 프로그램은 유선 또는 무선 연결을 통해 전달되는 통신 신호와 같은 임의의 매체를 통해 전자적으로 이송될 수 있고, 본 발명은 이와 균등한 것을 적절하게 포함한다.

청구범위

- [청구항 1] 금융 서비스를 지원하는 통합 시스템에 있어서,
금융 서비스를 지원하는 온라인 플랫폼이 실행되는 제1 단말; 및 상기
온라인 플랫폼을 운용하는 서버;를 포함하고,
상기 서버는:
제1 사용자 정보를 상기 제1 단말로부터 수신하고,
상기 제1 사용자 정보에 기반하여 상기 제1 단말의 제1 사용자에게 대한
인증 절차를 수행하고,
상기 인증 절차의 결과에 기반하여 상기 제1 사용자에게 상기 금융
서비스를 제공할 지 여부를 결정하고,
상기 결정에 따라 상기 금융 서비스를 제공하기 위한 정보를 상기 제1
단말에게 전송하는, 통합 시스템.
- [청구항 2] 청구항 1에 있어서,
상기 통합 시스템은, 상기 온라인 플랫폼이 실행되는 제2 단말;을 더
포함하고,
상기 금융 서비스는 DeFi(Decentralized Finance) 서비스를 포함하고,
상기 제1 단말은:
상기 제1 사용자 정보를 상기 제2 단말에 전달하고,
상기 제1 사용자 정보에 상응하는 블록체인 기반의 암호화 정보를 상기
제2 단말로부터 수신하고,
상기 암호화 정보를 복호화 하는, 통합 시스템.
- [청구항 3] 청구항 2에 있어서,
상기 통합 시스템은, 입력 모듈과 출력 모듈이 구비된 키오스크를 더
포함하는, 통합 시스템.
- [청구항 4] 청구항 3에 있어서,
상기 금융 서비스는 환전 서비스를 더 포함하고,
상기 키오스크는:
상기 입력 모듈을 통하여 촬영되는 제1 사용자의 신분증을 수집하고,
상기 신분증을 분석하여 상기 환전 서비스를 제공할지 여부를 결정하는,
통합 시스템.
- [청구항 5] 청구항 4에 있어서,
상기 키오스크는:
상기 신분증에 객체 추출 알고리즘을 적용하여 객체 정보를 획득하고,
상기 객체 정보에 기반하여 상기 환전 서비스를 제공할지 여부를
결정하는, 통합 시스템.
- [청구항 6] 청구항 5에 있어서,
상기 서버는:

상기 키오스크에 대한 정보 및 상기 제1 사용자 정보를 기반으로 상기 제1 QR 코드를 생성하고,
 상기 제1 QR 코드를 상기 제1 단말에게 송신하고,
 상기 제1 단말은 상기 서버로부터 수신한 제1 QR 코드를 표시하고,
 상기 키오스크는 상기 제1 단말에 출력된 제1 QR 코드를 기반으로 출입 인증 여부를 판단하는, 통합 시스템.

[청구항 7] 청구항 6에 있어서,
 상기 키오스크는, 상기 신분증을 수집하기 위한 스캐너를 더 포함하고,
 상기 제1 사용자 정보는, 상기 제1 사용자의 핸드폰번호 및 상기 제1 사용자의 신상정보를 포함하는, 통합 시스템.

[청구항 8] 청구항 7에 있어서,
 상기 서버는:
 출입인증요청 신호를 상기 키오스크로부터 수신하면, 상기 제1 사용자 단말의 현재 위치좌표를 상기 제1 단말에게 요청하고,
 상기 제1 단말의 현재 위치좌표 및 현재 표준시간 정보를 기반으로 제2 QR 코드를 생성하고,
 상기 제2 QR 코드를 상기 키오스크 및 상기 제1 단말에게 송신하고,
 상기 제1 단말은:
 상기 제1 QR 코드와 상기 제2 QR 코드를 기반으로 제1 오버레이 QR 코드를 생성하고,
 상기 제1 오버레이 QR 코드를 상기 키오스크에게 송신하고,
 상기 키오스크는:
 상기 제1 QR 코드와 상기 제2 QR 코드를 기반으로 제2 오버레이 QR 코드를 생성하고,
 상기 제1 오버레이 QR 코드와 상기 제2 오버레이 QR 코드를 비교하여 출입인증여부를 판단하는, 통합 시스템.

[청구항 9] 청구항 8에 있어서,
 상기 제1 오버레이 QR 코드 및 상기 제2 오버레이 QR 코드는,
 상기 제1 QR 코드 및 상기 제2 QR 코드의 위치 검출용 패턴을 동일 축(axis) 상에 위치시키고, 상기 제1 QR 코드 및 상기 제2 QR 코드의 각 셀을 비교하여 동일한 셀은 흑색 셀로 설정하고, 동일하지 않은 셀은 백색 셀로 설정하여 생성되는, 통합 시스템.

[청구항 10] 청구항 9에 있어서,
 상기 통합 시스템은, 기 설정된 복수의 특정 위치에 설치되는 복수의 키오스크를 포함하고,
 상기 제1 단말은, 상기 복수의 단말 각각에 대응하는 복수의 제1 QR 코드를 구분하여 저장하는, 통합 시스템.