(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2024년05월31일
(11) 등록번호 10-2671054
(24) 등록일자 2024년05월27일

(51) 국제특허분류(Int. Cl.)
G06Q 20/38 (2012.01) *G06Q 20/06* (2012.01)
G06Q 20/32 (2012.01) *G06Q 20/36* (2012.01)
G06Q 20/40 (2012.01) *H04L 65/40* (2022.01)
H04L 9/08 (2006.01) *H04L 9/32* (2006.01)
(52) CPC특허분류
G06Q 20/3821 (2013.01)
G06Q 20/065 (2013.01)
(21) 출원번호 10-2020-0144950
(22) 출원일자 2020년11월03일
심사청구일자 2021년06월09일
(65) 공개번호 10-2022-0041692
(43) 공개일자 2022년04월01일
(30) 우선권주장
1020200124440 2020년09월25일 대한민국(KR)
(56) 선행기술조사문헌
KR1020160030294 A*
KR1020160098756 A*
KR1020180007459 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
라인플러스 주식회사
경기도 성남시 분당구 황새울로360번길 42, 20층 (서현동, 에이케이플라자 분당점)
(72) 발명자
소홍섭
경기도 성남시 분당구 황새울로 360번길 42, 11층(서현동,에이케이플라자분당점)
류인선
경기도 성남시 분당구 황새울로 360번길 42, 11층(서현동,에이케이플라자분당점)
(뒷면에 계속)
(74) 대리인
양성보

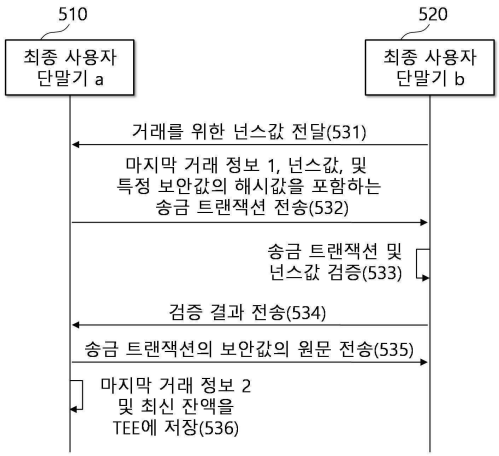
전체 청구항 수 : 총 18 항 심사관 : 박성웅

(54) 발명의 명칭 **중앙은행 디지털 화폐를 위한 결제 방법 및 시스템**

(57) 요 약

오프라인 상황(사용자의 단말기가 네트워크를 통해 서버에 연결될 수 없는 상황)에서도 이중 지불 없이 중앙은행 디지털 화폐(Central Bank Digital Currency, CBDC)를 이용하여 결제를 처리할 수 있는 결제 방법 및 시스템을 제공한다.

대 표 도 - 도5



(52) CPC특허분류
G06Q 20/322 (2013.01)
G06Q 20/367 (2020.05)
G06Q 20/3829 (2013.01)
G06Q 20/40145 (2013.01)
H04L 67/104 (2022.05)
H04L 9/0877 (2013.01)
H04L 9/3263 (2013.01)
H04L 9/50 (2022.05)
H04L 2209/56 (2013.01)
(72) 발명자
김황욱
경기도 성남시 분당구 황새울로 360번길 42, 11층 (서현동,에이케이플라자분당점)
이철웅
경기도 성남시 분당구 황새울로 360번길 42, 11층 (서현동,에이케이플라자분당점)

명 세 서

청구범위

청구항 1

컴퓨터 장치의 결제 방법에 있어서,

상기 컴퓨터 장치는 보안 영역, HSM(Hardware Security Module) 및 적어도 하나의 프로세서를 포함하고,

상기 결제 방법은,

상기 적어도 하나의 프로세서에 의해, 오프라인 상황에서 근거리 통신을 통해 송금을 받을 최종 사용자의 단말기로부터 넌스값을 전달받는 단계;

상기 적어도 하나의 프로세서에 의해, 상기 보안 영역에 저장된 제1 마지막 거래 정보, 상기 전달받은 넌스값 및 보안값의 해시값을 포함하는 송금 트랜잭션을 상기 HSM의 비밀키를 이용하여 서명하여 상기 단말기로 전송하는 단계;

상기 적어도 하나의 프로세서에 의해, 상기 단말기로부터 검증 성공 메시지를 수신하는 경우, 상기 보안값의 원문을 상기 단말기로 전송하는 단계; 및

상기 적어도 하나의 프로세서에 의해, 상기 송금 트랜잭션에 따른 제2 마지막 거래 정보 및 전자 지갑의 최신 잔액을 상기 보안 영역에 저장하는 단계

를 포함하고,

상기 보안 영역은 TEE(Trusted Execution Environment) 보안 영역 또는 WBC(White-Box Cryptographic) 보안 영역을 포함하는 것을 특징으로 하는 결제 방법.

청구항 2

삭제

청구항 3

제1항에 있어서,

상기 오프라인 상황이 온라인 상황으로 변화함에 응답하여 상기 단말기에서 상기 송금 트랜잭션 및 상기 보안값의 원문을 CBDC 원장으로 전송함으로써 상기 오프라인 상황에서 발생한 거래가 동기화되는 것을 특징으로 하는 결제 방법.

청구항 4

제1항에 있어서,

상기 결제 방법은,

상기 적어도 하나의 프로세서에 의해, 상기 단말기와 인증서를 교환하여 상기 단말기를 인증하는 단계

를 더 포함하는 것을 특징으로 하는 결제 방법.

청구항 5

제4항에 있어서,

상기 인증서는 상기 인증서가 발급된 디바이스의 디바이스 고유정보, 상기 디바이스가 포함하는 HSM의 공개정보, 발급 기관 정보 및 유효기간을 포함하도록 발급되어 상기 디바이스가 포함하는 보안 영역에 저장되는 것

을 특징으로 하는 결제 방법.

청구항 6

제5항에 있어서,

상기 단말기에서 상기 컴퓨터 장치의 인증서가 포함하는 상기 HSM의 공개정보를 이용하여 상기 송금 트랜잭션의 서명 검증이 처리되는 것

을 특징으로 하는 결제 방법.

청구항 7

제1항에 있어서,

상기 송금 트랜잭션을 상기 HSM의 비밀키를 이용하여 서명하여 상기 단말기로 전송하는 단계는,

상기 HSM의 공개정보를 상기 단말기로 더 전송하고,

상기 단말기에서 상기 HSM의 공개정보를 이용하여 상기 송금 트랜잭션의 서명 검증이 처리되는 것

을 특징으로 하는 결제 방법.

청구항 8

컴퓨터 장치의 결제 방법에 있어서,

상기 컴퓨터 장치는 제1 보안 영역, HSM(Hardware Security Module) 및 적어도 하나의 프로세서를 포함하고,

상기 결제 방법은,

상기 적어도 하나의 프로세서에 의해, 오프라인 상황에서 근거리 통신을 통해 송금을 하는 최종 사용자의 단말기로 넌스값을 전달하는 단계;

상기 적어도 하나의 프로세서에 의해, 상기 단말기로부터 상기 단말기의 HSM의 비밀키를 이용하여 서명된 송금 트랜잭션을 수신하는 단계 - 상기 송금 트랜잭션은 상기 단말기의 제2 보안 영역에 저장된 제1 마지막 거래 정보, 상기 전달한 넌스값 및 보안값의 해시값을 포함함 -;

상기 적어도 하나의 프로세서에 의해, 상기 수신된 송금 트랜잭션을 서명 검증하는 단계;

상기 적어도 하나의 프로세서에 의해, 상기 수신된 송금 트랜잭션이 포함하는 넌스값을 검증하는 단계;

상기 적어도 하나의 프로세서에 의해, 상기 서명 검증 및 상기 넌스값의 검증이 성공하는 경우, 상기 단말기로 검증 성공 메시지를 전송하는 단계;

상기 적어도 하나의 프로세서에 의해, 상기 수신된 송금 트랜잭션 및 제2 마지막 거래를 상기 제1 보안 영역에 저장하는 단계; 및

상기 적어도 하나의 프로세서에 의해, 상기 단말기에서 상기 검증 성공 메시지를 수신함에 응답하여 전송하는 상기 보안값의 원문을 수신하는 단계

를 포함하고,

상기 제1 보안 영역 및 상기 제2 보안 영역 각각은 TEE(Trusted Execution Environment) 보안 영역 또는 WBC(White-Box Cryptographic) 보안 영역을 포함하는 것을 특징으로 하는 결제 방법.

청구항 9

삭제

청구항 10

제8항에 있어서,

상기 오프라인 상황이 온라인 상황으로 변화함에 응답하여 상기 오프라인 상황에서 발생한 거래를 동기화하기 위해, 상기 결제 방법은,

상기 적어도 하나의 프로세서에 의해, 상기 제1 보안 영역에 저장된 상기 송금 트랜잭션 및 상기 보안값의 원문을 CBDC 원장으로 전송하는 단계

를 더 포함하는 것을 특징으로 하는 결제 방법.

청구항 11

제8항에 있어서,

상기 결제 방법은,

상기 적어도 하나의 프로세서에 의해, 상기 단말기와 인증서를 교환하여 상기 단말기를 인증하는 단계

를 더 포함하는 것을 특징으로 하는 결제 방법.

청구항 12

제11항에 있어서,

상기 인증서는 상기 인증서가 발급된 디바이스의 디바이스 고유정보, 상기 디바이스가 포함하는 HSM의 공개정보, 발급 기관 정보 및 유효기간을 포함하도록 발급되어 상기 디바이스가 포함하는 보안 영역에 저장되는 것

을 특징으로 하는 결제 방법.

청구항 13

제12항에 있어서,

상기 서명 검증하는 단계는,

상기 단말기가 포함하는 HSM의 공개정보, 상기 발급 기관 정보 및 상기 유효기간을 이용하여 상기 송금 트랜잭션을 서명 검증하는 것

을 특징으로 하는 결제 방법.

청구항 14

제8항에 있어서,

상기 서명된 송금 트랜잭션을 수신하는 단계는,

상기 단말기가 포함하는 HSM의 공개정보를 상기 단말기로부터 더 수신하고,

상기 서명 검증하는 단계는,

상기 수신된 HSM의 공개정보를 이용하여 상기 송금 트랜잭션을 서명 검증하는 것

을 특징으로 하는 결제 방법.

청구항 15

컴퓨터 장치와 결합되어 제1항, 제3항 내지 제8항 또는 제10항 내지 제14항 중 어느 한 항의 방법을 컴퓨터 장치에 실행시키기 위해 컴퓨터 판독 가능한 기록매체에 저장된 컴퓨터 프로그램.

청구항 16

제1항, 제3항 내지 제8항 또는 제10항 내지 제14항 중 어느 한 항의 방법을 컴퓨터 장치에 실행시키기 위한 컴퓨터 프로그램이 기록되어 있는 컴퓨터 판독 가능한 기록매체.

청구항 17

컴퓨터 장치에서 판독 가능한 명령을 실행하도록 구현되는 적어도 하나의 프로세서;

보안 영역; 및

HSM(Hardware Security Module)

을 포함하고,

상기 적어도 하나의 프로세서에 의해,

오프라인 상황에서 근거리 통신을 통해 송금을 받을 최종 사용자의 단말기로부터 넌스값을 전달받고,

상기 보안 영역에 저장된 제1 마지막 거래 정보, 상기 전달받은 넌스값 및 보안값의 해시값을 포함하는 송금 트랜잭션을 상기 HSM의 비밀키를 이용하여 서명하여 상기 단말기로 전송하고,

상기 단말기로부터 검증 성공 메시지를 수신하는 경우, 상기 보안값의 원문을 상기 단말기로 전송하고,

상기 송금 트랜잭션에 따른 제2 마지막 거래 정보 및 전자 지갑의 최신 잔액을 상기 보안 영역에 저장하고,

상기 보안 영역은 TEE(Trusted Execution Environment) 보안 영역 또는 WBC(White-Box Cryptographic) 보안 영역을 포함하는 것

을 특징으로 하는 컴퓨터 장치.

청구항 18

제17항에 있어서,

상기 오프라인 상황이 온라인 상황으로 변화함에 응답하여 상기 단말기에서 상기 송금 트랜잭션 및 상기 보안값의 원문을 CBDC 원장으로 전송함으로써 상기 오프라인 상황에서 발생한 거래가 동기화되는 것

을 특징으로 하는 컴퓨터 장치.

청구항 19

컴퓨터에서 판독 가능한 명령을 실행하도록 구현되는 적어도 하나의 프로세서;

제1 보안 영역; 및

HSM(Hardware Security Module)

을 포함하고,

상기 적어도 하나의 프로세서에 의해,

오프라인 상황에서 근거리 통신을 통해 송금을 하는 최종 사용자의 단말기로 넌스값을 전달하고,

상기 단말기로부터 상기 단말기의 HSM의 비밀키를 이용하여 서명된 송금 트랜잭션을 수신하고, - 상기 송금 트랜잭션은 상기 단말기의 제2 보안 영역에 저장된 제1 마지막 거래 정보, 상기 전달한 넌스값 및 보안값의 해시값을 포함함 -;

상기 수신된 송금 트랜잭션을 서명 검증하고,

상기 수신된 송금 트랜잭션이 포함하는 넌스값을 검증하고,

상기 서명 검증 및 상기 넌스값의 검증이 성공하는 경우, 상기 단말기로 검증 성공 메시지를 전송하고,

상기 수신된 송금 트랜잭션 및 제2 마지막 거래를 상기 제1 보안 영역에 저장하고,

상기 단말기에서 상기 검증 성공 메시지를 수신함에 응답하여 전송하는 상기 보안값의 원문을 수신하고,

상기 제1 보안 영역 및 상기 제2 보안 영역 각각은 TEE(Trusted Execution Environment) 보안 영역 또는 WBC(White-Box Cryptographic) 보안 영역을 포함하는 것

을 특징으로 하는 컴퓨터 장치.

청구항 20

제19항에 있어서,

상기 적어도 하나의 프로세서에 의해,

상기 오프라인 상황이 온라인 상황으로 변화함에 응답하여 상기 오프라인 상황에서 발생한 거래를 동기화하기 위해,

상기 제1 보안 영역에 저장된 상기 송금 트랜잭션 및 상기 보안값의 원문을 CBDC 원장으로 전송하는 것

을 특징으로 하는 컴퓨터 장치.

발명의 설명

기 술 분 야

[0001] 아래의 설명은 중앙은행 디지털 화폐를 위한 결제 방법 및 시스템에 관한 것이다.

배 경 기 술

[0002] 중앙은행 디지털 화폐(Central Bank Digital Currency, CBDC)는 중앙은행이 발행하는 전자적 형태의 화폐로서, CBDC 구현방식은 중앙은행 또는 은행이 CBDC 계좌 및 관련 거래정보를 보관 및 관리하는 단일원장방식(계좌방식)과, 다수의 거래참가자가 동일한 거래기록을 관리하는 분산원장방식으로 분류할 수 있다.

[0003] [선행문헌번호]

[0004] 한국등록특허 제10-1862637호

발명의 내용

해결하려는 과제

[0005] 오프라인 상황(사용자의 단말기가 네트워크를 통해 서버에 연결될 수 없는 상황)에서도 이중 지불 없이 중앙은행 디지털 화폐(Central Bank Digital Currency, CBDC)를 이용하여 결제를 처리할 수 있는 결제 방법 및 시스템을 제공한다.

과제의 해결 수단

[0006] 컴퓨터 장치의 결제 방법에 있어서, 상기 컴퓨터 장치는 보안 영역, HSM(Hardware Security Module) 및 적어도 하나의 프로세서를 포함하고, 상기 결제 방법은, 상기 적어도 하나의 프로세서에 의해, 오프라인 상황에서 근거리 통신을 통해 송금을 받을 최종 사용자의 단말기로부터 넌스값을 전달받는 단계; 상기 적어도 하나의 프로세서에 의해, 상기 보안 영역에 저장된 제1 마지막 거래 정보, 상기 전달받은 넌스값 및 보안값의 해시값을 포함하는 송금 트랜잭션을 상기 HSM의 비밀키를 이용하여 서명하여 상기 단말기로 전송하는 단계; 상기 적어도 하나의 프로세서에 의해, 상기 단말기로부터 검증 성공 메시지를 수신하는 경우, 상기 보안값의 원문을 상기 단말기로 전송하는 단계; 및 상기 적어도 하나의 프로세서에 의해, 상기 송금 트랜잭션에 따른 제2 마지막 거래 정보 및 전자 지갑의 최신 잔액을 상기 보안 영역에 저장하는 단계를 포함하는 것을 특징으로 하는 결제 방법을 제공한다.

[0007] 일측에 따르면, 상기 보안 영역은 TEE(Trusted Execution Environment) 보안 영역 또는 WBC(White-Box Cryptographic) 보안 영역을 포함하는 것을 특징으로 할 수 있다.

[0008] 다른 측면에 따르면, 상기 오프라인 상황이 온라인 상황으로 변화함에 응답하여 상기 단말기에서 상기 송금 트랜잭션 및 상기 보안값의 원문을 CBDC 원장으로 전송함으로써 상기 오프라인 상황에서 발생한 거래가 동기화되는 것을 특징으로 할 수 있다.

[0009] 또 다른 측면에 따르면, 상기 결제 방법은, 상기 적어도 하나의 프로세서에 의해, 상기 단말기와 인증서를 교환하여 상기 단말기를 인증하는 단계를 더 포함할 수 있다.

[0010] 또 다른 측면에 따르면, 상기 인증서는 상기 인증서가 발급된 디바이스의 디바이스 고유정보, 상기 디바이스가 포함하는 HSM의 공개정보, 발급 기관 정보 및 유효기간을 포함하도록 발급되어 상기 디바이스가 포함하는 보안 영역에 저장되는 것을 특징으로 할 수 있다.

[0011] 또 다른 측면에 따르면, 상기 단말기에서 상기 컴퓨터 장치의 인증서가 포함하는 상기 HSM의 공개정보를 이용하

여 상기 송금 트랜잭션의 서명 검증이 처리되는 것을 특징으로 할 수 있다.

[0012] 또 다른 측면에 따르면, 상기 송금 트랜잭션을 상기 HSM의 비밀키를 이용하여 서명하여 상기 단말기로 전송하는 단계는, 상기 HSM의 공개정보를 상기 단말기로 더 전송하고, 상기 단말기에서 상기 HSM의 공개정보를 이용하여 상기 송금 트랜잭션의 서명 검증이 처리되는 것을 특징으로 할 수 있다.

[0013] 컴퓨터 장치의 결제 방법에 있어서, 상기 컴퓨터 장치는 제1 보안 영역, HSM(Hardware Security Module) 및 적어도 하나의 프로세서를 포함하고, 상기 결제 방법은, 상기 적어도 하나의 프로세서에 의해, 오프라인 상황에서 근거리 통신을 통해 송금을 하는 최종 사용자의 단말기로 넌스값을 전달하는 단계; 상기 적어도 하나의 프로세서에 의해, 상기 단말기로부터 상기 단말기의 HSM의 비밀키를 이용하여 서명된 송금 트랜잭션을 수신하는 단계 - 상기 송금 트랜잭션은 상기 단말기의 제2 보안 영역에 저장된 제1 마지막 거래 정보, 상기 전달한 넌스값 및 보안값의 해시값을 포함함 -; 상기 적어도 하나의 프로세서에 의해, 상기 수신된 송금 트랜잭션을 서명 검증하는 단계; 상기 적어도 하나의 프로세서에 의해, 상기 수신된 송금 트랜잭션이 포함하는 넌스값을 검증하는 단계; 상기 적어도 하나의 프로세서에 의해, 상기 서명 검증 및 상기 넌스값의 검증이 성공하는 경우, 상기 단말기로 검증 성공 메시지를 전송하는 단계; 상기 적어도 하나의 프로세서에 의해, 상기 수신된 송금 트랜잭션 및 제2 마지막 거래를 상기 제1 보안 영역에 저장하는 단계; 및 상기 적어도 하나의 프로세서에 의해, 상기 단말기에서 상기 검증 성공 메시지를 수신함에 응답하여 전송하는 상기 보안값의 원문을 수신하는 단계를 포함하는 것을 특징으로 하는 결제 방법을 제공한다.

[0014] 일측에 따르면, 상기 제1 보안 영역 및 상기 제2 보안 영역 각각은 TEE(Trusted Execution Environment) 보안 영역 또는 WBC(White-Box Cryptographic) 보안 영역을 포함하는 것을 특징으로 할 수 있다.

[0015] 다른 측면에 따르면, 상기 오프라인 상황이 온라인 상황으로 변화함에 응답하여 상기 오프라인 상황에서 발생한 거래를 동기화하기 위해, 상기 결제 방법은, 상기 적어도 하나의 프로세서에 의해, 상기 제1 보안 영역에 저장된 상기 송금 트랜잭션 및 상기 보안값의 원문을 CBDC 원장으로 전송하는 단계를 더 포함하는 것을 특징으로 할 수 있다.

[0016] 다른 측면에 따르면, 상기 결제 방법은, 상기 적어도 하나의 프로세서에 의해, 상기 단말기와 인증서를 교환하여 상기 단말기를 인증하는 단계를 더 포함할 수 있다.

[0017] 또 다른 측면에 따르면, 상기 인증서는 상기 인증서가 발급된 디바이스의 디바이스 고유정보, 상기 디바이스가 포함하는 HSM의 공개정보, 발급 기관 정보 및 유효기간을 포함하도록 발급되어 상기 디바이스가 포함하는 보안 영역에 저장되는 것을 특징으로 할 수 있다.

[0018] 또 다른 측면에 따르면, 상기 서명 검증하는 단계는, 상기 단말기가 포함하는 HSM의 공개정보, 상기 발급 기관 정보 및 상기 유효기간을 이용하여 상기 송금 트랜잭션을 서명 검증하는 것을 특징으로 할 수 있다.

[0019] 또 다른 측면에 따르면, 상기 서명된 송금 트랜잭션을 수신하는 단계는, 상기 단말기가 포함하는 HSM의 공개정보를 상기 단말기로부터 더 수신하고, 상기 서명 검증하는 단계는, 상기 수신된 HSM의 공개정보를 이용하여 상기 송금 트랜잭션을 서명 검증하는 것을 특징으로 할 수 있다.

[0020] 컴퓨터 장치와 결합되어 상기 방법을 컴퓨터 장치에 실행시키기 위해 컴퓨터 판독 가능한 기록매체에 저장된 컴퓨터 프로그램을 제공한다.

[0021] 상기 방법을 컴퓨터 장치에 실행시키기 위한 프로그램이 기록되어 있는 컴퓨터 판독 가능한 기록매체를 제공한다.

[0022] 컴퓨터에서 판독 가능한 명령을 실행하도록 구현되는 적어도 하나의 프로세서; 보안 영역; 및 HSM(Hardware Security Module)을 포함하고, 상기 적어도 하나의 프로세서에 의해, 오프라인 상황에서 근거리 통신을 통해 송금을 받을 최종 사용자의 단말기로부터 넌스값을 전달받고, 상기 보안 영역에 저장된 제1 마지막 거래 정보, 상기 전달받은 넌스값 및 보안값의 해시값을 포함하는 송금 트랜잭션을 상기 HSM의 비밀키를 이용하여 서명하여 상기 단말기로 전송하고, 상기 단말기로부터 검증 성공 메시지를 수신하는 경우, 상기 보안값의 원문을 상기 단말기로 전송하고, 상기 송금 트랜잭션에 따른 제2 마지막 거래 정보 및 전자 지갑의 최신 잔액을 상기 보안 영역에 저장하는 것을 특징으로 하는 컴퓨터 장치를 제공한다.

[0023] 컴퓨터에서 판독 가능한 명령을 실행하도록 구현되는 적어도 하나의 프로세서; 제1 보안 영역; 및 HSM(Hardware Security Module)을 포함하고, 상기 적어도 하나의 프로세서에 의해, 오프라인 상황에서 근거리 통신을 통해 송금을 하는 최종 사용자의 단말기로 넌스값을 전달하고, 상기 단말기로부터 상기 단말기의 HSM의 비밀키를 이용

하여 서명된 송금 트랜잭션을 수신하고, - 상기 송금 트랜잭션은 상기 단말기의 제2 보안 영역에 저장된 제1 마지막 거래 정보, 상기 전달한 넌스값 및 보안값의 해시값을 포함함 -; 상기 수신된 송금 트랜잭션을 서명 검증하고, 상기 수신된 송금 트랜잭션이 포함하는 넌스값을 검증하고, 상기 서명 검증 및 상기 넌스값의 검증이 성공하는 경우, 상기 단말기로 검증 성공 메시지를 전송하고, 상기 수신된 송금 트랜잭션 및 제2 마지막 거래를 상기 제1 보안 영역에 저장하고, 상기 단말기에서 상기 검증 성공 메시지를 수신함에 응답하여 전송하는 상기 보안값의 원문을 수신하는 것을 특징으로 하는 컴퓨터 장치를 제공한다.

발명의 효과

[0024] 오프라인 상황(사용자의 단말기가 네트워크를 통해 서버에 연결될 수 없는 상황)에서도 이중 지불 없이 중앙은행 디지털 화폐(Central Bank Digital Currency, CBDC)를 이용하여 결제를 처리할 수 있다.

도면의 간단한 설명

[0025] 도 1은 본 발명의 일실시예에 따른 네트워크 환경의 예를 도시한 도면이다.

도 2는 본 발명의 일실시예에 따른 컴퓨터 장치의 예를 도시한 블록도이다.

도 3은 본 발명의 일실시예에 따른 최종 사용자 단말기의 내부 구성의 예를 도시한 도면이다.

도 4는 본 발명의 일실시예에 따른 온라인 결제 방법의 예를 도시한 흐름도이다.

도 5는 본 발명의 일실시예에 따른 오프라인 결제 방법의 예를 도시한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0026] 이하, 실시예를 첨부한 도면을 참조하여 상세히 설명한다.

[0027] 본 발명의 실시예들에 따른 결제 시스템은 적어도 하나의 컴퓨터 장치에 의해 구현될 수 있다. 이때, 컴퓨터 장치에는 본 발명의 일실시예에 따른 컴퓨터 프로그램이 설치 및 구동될 수 있고, 컴퓨터 장치는 구동된 컴퓨터 프로그램의 제어에 따라 본 발명의 실시예들에 따른 결제 방법을 수행할 수 있다. 상술한 컴퓨터 프로그램은 컴퓨터 장치와 결합되어 결제 방법을 컴퓨터에 실행시키기 위해 컴퓨터 판독 가능한 기록매체에 저장될 수 있다.

[0028] 도 1은 본 발명의 일실시예에 따른 네트워크 환경의 예를 도시한 도면이다. 도 1의 네트워크 환경은 복수의 전자 기기들(110, 120, 130, 140), 복수의 서버들(150, 160) 및 네트워크(170)를 포함하는 예를 나타내고 있다. 이러한 도 1은 발명의 설명을 위한 일례로 전자 기기의 수나 서버의 수가 도 1과 같이 한정되는 것은 아니다. 또한, 도 1의 네트워크 환경은 본 실시예들에 적용 가능한 환경들 중 하나의 예를 설명하는 것일 뿐, 본 실시예들에 적용 가능한 환경이 도 1의 네트워크 환경으로 한정되는 것은 아니다.

[0029] 복수의 전자 기기들(110, 120, 130, 140)은 컴퓨터 장치로 구현되는 고정형 단말이거나 이동형 단말일 수 있다. 복수의 전자 기기들(110, 120, 130, 140)의 예를 들면, 스마트폰(smart phone), 휴대폰, 네비게이션, 컴퓨터, 노트북, 디지털방송용 단말, PDA(Personal Digital Assistants), PMP(Portable Multimedia Player), 태블릿 PC 등이 있다. 일례로 도 1에서는 전자 기기(110)의 예로 스마트폰의 형상을 나타내고 있으나, 본 발명의 실시예들에서 전자 기기(110)는 실질적으로 무선 또는 유선 통신 방식을 이용하여 네트워크(170)를 통해 다른 전자 기기들(120, 130, 140) 및/또는 서버(150, 160)와 통신할 수 있는 다양한 물리적인 컴퓨터 장치들 중 하나를 의미할 수 있다.

[0030] 통신 방식은 제한되지 않으며, 네트워크(170)가 포함할 수 있는 통신망(일례로, 이동통신망, 유선 인터넷, 무선 인터넷, 방송망)을 활용하는 통신 방식뿐만 아니라 기기들간의 근거리 무선 통신 역시 포함될 수 있다. 예를 들어, 네트워크(170)는, PAN(personal area network), LAN(local area network), CAN(campus area network), MAN(metropolitan area network), WAN(wide area network), BBN(broadband network), 인터넷 등의 네트워크 중 하나 이상의 임의의 네트워크를 포함할 수 있다. 또한, 네트워크(170)는 버스 네트워크, 스타 네트워크, 링 네트워크, 메쉬 네트워크, 스타-버스 네트워크, 트리 또는 계층적(hierarchical) 네트워크 등을 포함하는 네트워크 토폴로지 중 임의의 하나 이상을 포함할 수 있으나, 이에 제한되지 않는다.

[0031] 서버(150, 160) 각각은 복수의 전자 기기들(110, 120, 130, 140)과 네트워크(170)를 통해 통신하여 명령, 코드, 파일, 컨텐츠, 서비스 등을 제공하는 컴퓨터 장치 또는 복수의 컴퓨터 장치들로 구현될 수 있다. 예를

들어, 서버(150)는 네트워크(170)를 통해 접속한 복수의 전자 기기들(110, 120, 130, 140)로 서비스(일례로, 결제 서비스, 가상 거래소 서비스, 리스크 모니터링 서비스, 인스턴트 메시징 서비스, 게임 서비스, 그룹 통화 서비스(또는 음성 컨퍼런스 서비스), 메시징 서비스, 메일 서비스, 소셜 네트워크 서비스, 지도 서비스, 번역 서비스, 금융 서비스, 검색 서비스, 컨텐츠 제공 서비스 등)를 제공하는 시스템일 수 있다.

[0032] 도 2는 본 발명의 일실시예에 따른 컴퓨터 장치의 예를 도시한 블록도이다. 앞서 설명한 복수의 전자 기기들(110, 120, 130, 140) 각각이나 서버들(150, 160) 각각은 도 2를 통해 도시된 컴퓨터 장치(200)에 의해 구현될 수 있다.

[0033] 이러한 컴퓨터 장치(200)는 도 2에 도시된 바와 같이, 메모리(210), 프로세서(220), 통신 인터페이스(230) 그리고 입출력 인터페이스(240)를 포함할 수 있다. 메모리(210)는 컴퓨터에서 판독 가능한 기록매체로서, RAM(random access memory), ROM(read only memory) 및 디스크 드라이브와 같은 비소멸성 대용량 기록장치(permanent mass storage device)를 포함할 수 있다. 여기서 ROM과 디스크 드라이브와 같은 비소멸성 대용량 기록장치는 메모리(210)와는 구분되는 별도의 영구 저장 장치로서 컴퓨터 장치(200)에 포함될 수도 있다. 또한, 메모리(210)에는 운영체제와 적어도 하나의 프로그램 코드가 저장될 수 있다. 이러한 소프트웨어 구성요소들은 메모리(210)와는 별도의 컴퓨터에서 판독 가능한 기록매체로부터 메모리(210)로 로딩될 수 있다. 이러한 별도의 컴퓨터에서 판독 가능한 기록매체는 플로피 드라이브, 디스크, 테이프, DVD/CD-ROM 드라이브, 메모리 카드 등의 컴퓨터에서 판독 가능한 기록매체를 포함할 수 있다. 다른 실시예에서 소프트웨어 구성요소들은 컴퓨터에서 판독 가능한 기록매체가 아닌 통신 인터페이스(230)를 통해 메모리(210)에 로딩될 수도 있다. 예를 들어, 소프트웨어 구성요소들은 네트워크(170)를 통해 수신되는 파일들에 의해 설치되는 컴퓨터 프로그램에 기반하여 컴퓨터 장치(200)의 메모리(210)에 로딩될 수 있다.

[0034] 프로세서(220)는 기본적인 산술, 로직 및 입출력 연산을 수행함으로써, 컴퓨터 프로그램의 명령을 처리하도록 구성될 수 있다. 명령은 메모리(210) 또는 통신 인터페이스(230)에 의해 프로세서(220)로 제공될 수 있다. 예를 들어 프로세서(220)는 메모리(210)와 같은 기록 장치에 저장된 프로그램 코드에 따라 수신되는 명령을 실행하도록 구성될 수 있다.

[0035] 통신 인터페이스(230)는 네트워크(170)를 통해 컴퓨터 장치(200)가 다른 장치(일례로, 앞서 설명한 저장 장치들)와 서로 통신하기 위한 기능을 제공할 수 있다. 일례로, 컴퓨터 장치(200)의 프로세서(220)가 메모리(210)와 같은 기록 장치에 저장된 프로그램 코드에 따라 생성한 요청이나 명령, 데이터, 파일 등이 통신 인터페이스(230)의 제어에 따라 네트워크(170)를 통해 다른 장치들로 전달될 수 있다. 역으로, 다른 장치로부터의 신호나 명령, 데이터, 파일 등이 네트워크(170)를 거쳐 컴퓨터 장치(200)의 통신 인터페이스(230)를 통해 컴퓨터 장치(200)로 수신될 수 있다. 통신 인터페이스(230)를 통해 수신된 신호나 명령, 데이터 등은 프로세서(220)나 메모리(210)로 전달될 수 있고, 파일 등은 컴퓨터 장치(200)가 더 포함할 수 있는 저장 매체(상술한 영구 저장 장치)로 저장될 수 있다.

[0036] 입출력 인터페이스(240)는 입출력 장치(250)와의 인터페이스를 위한 수단일 수 있다. 예를 들어, 입력 장치는 마이크, 키보드 또는 마우스 등의 장치를, 그리고 출력 장치는 디스플레이, 스피커와 같은 장치를 포함할 수 있다. 다른 예로 입출력 인터페이스(240)는 터치스크린과 같이 입력과 출력을 위한 기능이 하나로 통합된 장치와의 인터페이스를 위한 수단일 수도 있다. 입출력 장치(250) 중 적어도 하나는 컴퓨터 장치(200)와 하나의 장치로 구성될 수도 있다. 예를 들어, 스마트폰과 같이 터치스크린, 마이크, 스피커 등이 컴퓨터 장치(200)에 포함된 형태로 구현될 수 있다.

[0037] 또한, 다른 실시예들에서 컴퓨터 장치(200)는 도 2의 구성요소들보다 더 적은 혹은 더 많은 구성요소들을 포함할 수도 있다. 그러나, 대부분의 종래기술적 구성요소들을 명확하게 도시할 필요성은 없다. 예를 들어, 컴퓨터 장치(200)는 상술한 입출력 장치(250) 중 적어도 일부를 포함하도록 구현되거나 또는 트랜시버(transceiver), 데이터베이스 등과 같은 다른 구성요소들을 더 포함할 수도 있다.

[0038] 중앙은행 디지털 화폐(Central Bank Digital Currency, CBDC)를 이용하는 결제의 처리를 위해, 최종 사용자 단말기는 수시로 서버와 통신하여 원장의 정보를 갱신해야 한다. 한편, 최종 사용자 단말기가 네트워크에 연결될 수 없는 상황과 같은 오프라인 상황에서도 최종 사용자들간의 결제가 이루어져야 한다. 이때, 이중 지불이 발생되지 않아야 하며, 최종 사용자들이 인증될 수 있어야 한다.

[0039] 도 3은 본 발명의 일실시예에 따른 최종 사용자 단말기의 내부 구성의 예를 도시한 도면이다. 본 실시예에 따른 제1 최종 사용자 단말기(310) 및 제2 최종 사용자 단말기(320)는 서버(330)와 통신하면서 결제를 처리할 수

있으나, 오프라인 상황에서는 최종 사용자 단말기들(제1 최종 사용자 단말기(310) 및 제2 최종 사용자 단말기(320))간의 통신을 통해 최종 사용자 단말기들간의 오프라인 결제를 처리할 수 있다. 이후, 서버(330)와의 통신이 가능해지면, 최종 사용자 단말기들은 서버(330)와의 통신을 통해 오프라인 결제의 내용을 서버(330)와 동기화할 수 있다. 서버(330)는 CBDC 플랫폼 및 최종 사용자 단말기들 사이에서 CBDC를 이용한 결제를 처리하는 서비스 제공자의 서버 장치일 수 있다. 이후 본 명세서에서 특별한 한정 없이 사용하는 용어 "서버"는 서비스 제공자의 서버를 의미할 수 있다.

[0040] 오프라인 결제 시의 이중 지불의 방지를 위해, 제1 최종 사용자 단말기(310)는 도 3에 도시된 바와 같이 P2P 통신모듈(311), HSM(Hardware Security Module, 312) 및 TEE(Trusted Execution Environment) 보안 영역(313)을 포함할 수 있다. 제2 최종 사용자 단말기(320) 역시 제1 최종 사용자 단말기(310)와 동일 또는 유사한 내부 구성을 가질 수 있다. 이러한 제1 최종 사용자 단말기(310) 및 제2 최종 사용자 단말기(320)는 도 2를 통해 설명한 컴퓨터 장치(200)에 의해 구현될 수 있으며, 도 3의 실시예에서 오프라인 결제를 위해 필수적이지 않은 구성요소들은 생략되었다.

[0041] P2P 통신모듈(311)은 블루투스나 NFC(Near Field Communication)와 같이 근거리 통신을 목적으로 하는 통신모듈을 포함할 수 있다. 사용자가 네트워크를 통해 서버와 통신할 수 없는 상황(일례로, 일시적인 네트워크 장애나 재난 등에 의한 장애가 발생한 상황과 같은 오프라인 상황)에서도 최종 사용자들간의 결제가 이루어지도록 하기 위해서는 적어도 최종 사용자들의 단말기들(일례로, 도 3의 제1 최종 사용자 단말기(310) 및 제2 최종 사용자 단말기(320))간의 통신은 가능해야 하기 때문에, P2P 통신모듈(311)이 요구될 수 있다.

[0042] HSM(312)은 물리적으로 복제와 추출이 불가능한 비밀키(private key)를 관리하고 보호하기 위한 모듈을 포함할 수 있다. 일반적으로 암호화 API에서 암호키와 같은 비밀키를 메모리 등에 탑재하여 활용하는 방식 대신에, HSM(312)은 데이터에 대한 암복호화시 데이터를 HSM(312) 내부에 보내어 결과값을 받는 방식을 활용할 수 있다. 따라서 비밀키는 내부적으로 관리하여 외부에 유출이 되지 않고 암호 연산 자체가 HSM(312) 내부에서 수행될 수 있기 때문에 비밀키의 유출을 원천적으로 방지할 수 있다. 일례로, 도 2의 컴퓨터 장치(200)가 이러한 HSM(312)을 위한 물리적인 장치를 더 포함할 수 있다.

[0043] TEE 보안 영역(313)은 하드웨어로 독립된 보안 영역을 제공하여 안전한 실행 환경에서 응용 프로그램의 무결성과 데이터의 기밀성 등의 보안 기능을 제공할 수 있다. 일례로, 도 2의 컴퓨터 장치(200)가 포함하는 프로세서(220)가 TEE 보안 영역(313)의 제공을 위한 TEE 기능을 포함할 수 있다.

[0044] 또한, 실시예에 따라 하드웨어적으로 구성되는 TEE 보안 영역(313)은 소프트웨어 기술로 대체될 수도 있다. 예를 들어, WBC(White-Box Cryptographic)는 데이터를 안전하게 보관할 수 있고, 신뢰할 수 없는 단말에서 암호화 알고리즘이 실행되더라도 보관한 데이터가 드러나지 않도록 할 수 있는 소프트웨어 기술이다.

[0045] 이후에 설명되는 TEE 기반의 보안 영역이 하드웨어 보안 영역과 소프트웨어 보안 영역 중 어느 하나를 포함하는 "보안 영역"으로 확장될 수 있음을 쉽게 이해할 수 있을 것이다.

[0046] 근거리 통신을 위한 블루투스나 NFC, 보안을 위한 HSM, TEE 등에 대해서는 이미 잘 알려져 있기 때문에 자세한 설명은 생략한다.

[0047] 오프라인 상황에서의 결제를 처리하기 위해, 본 실시예들에 따른 결제 방법에서는 아래 (1) 내지 (5)의 조건을 만족한다고 가정한다.

[0048] (1) 최종 사용자 단말기 각각(일례로, 제1 최종 사용자 단말기(310) 및 제2 최종 사용자 단말기(320) 각각)은 유일한 비밀키를 갖는 HSM 디바이스일 수 있다. 다시 말해, 둘 이상의 최종 사용자 단말기가 동일한 비밀키를 갖지 않는다.

[0049] (2) 최종 사용자 단말기에서 서명한 최신 정보는 TEE에 기록되고 서명할 때마다 TEE에 기록된 정보를 활용하여 서명이 처리될 수 있다. 예를 들어, 제1 최종 사용자 단말기(310)에서 서명한 최신 정보는 TEE 보안 영역(313)에 기록될 수 있으며, 제1 최종 사용자 단말기(310)는 TEE 보안 영역(313)에 기록된 서명된 최신 정보를 이용하여 다음 서명을 처리할 수 있다.

[0050] (3) 서버와 동기화된 최종 잔액에 대한 정보는 TEE에 기록된다. 예를 들어, 제1 최종 사용자 단말기(310)는 서버와의 통신을 통해 동기화된 최종 잔액에 대한 정보를 TEE 보안 영역(313)에 기록할 수 있다.

[0051] (4) KYC(Know Your Customer) 인증을 완료한 사용자의 전자 지갑이 사용될 수 있도록 한다. 실시예에 따라 외국인도 이용할 수 있도록 KYC 인증이 선택적으로 처리될 수도 있다. 만약, KYC 인증을 하지 않은 전자 지갑을

사용 가능하도록 허용하는 경우에는 결제 가능한 금액의 상한을 제한하는 것과 같은 제약이 전자 지갑에 적용되도록 설정할 수 있다.

[0052] (5) HSM을 사용할 유일한 디바이스에 PKI 기반의 인증서를 CA(Certification Authority)에서 발급받는다. 이때, 인증서가 이중 발급되지 않도록 하며, 인증서는 TEE(일례로, TEE 보안 영역(313))에 저장될 수 있다. 인증서 정보에는 디바이스 고유정보와 HSM의 공개정보, 발급 기관 정보 및 유효기간이 포함될 수 있다. 일례로, 디바이스 고유정보는 최종 사용자 단말기를 고유하게 식별할 수 있는 정보를 포함할 수 있으며, 퍼블릭 정보는 HSM에 저장된 비밀키에 대응하여 공개되는 정보(일례로, 공개키)를 포함할 수 있다.

[0053] 앞서 도 3의 실시예에서는 제1 최종 사용자 단말기(310)가 P2P 통신모듈(311), HSM(312) 및 TEE 보안 영역(313)을 모두 포함하는 실시예를 설명하였으나, TEE를 지원하는 디바이스(일례로, 스마트폰)와 스마트 HSM(일례로, ledger Nano, Trezor, YubiKey 등)이 결합된 형태 또는 네트워크를 지원하는 디바이스(일례로, POS(Point Of Sales)나 스마트폰 등)와 TEE 및 HSM을 갖춘 디바이스(일례로, 보안 저장장치를 가진 HSM 카드)가 결합된 형태로 구현될 수도 있다.

[0054] 스마트폰의 경우는 휴대용 충전장치나 건전지로 충전할 수 있는 장비를 저렴한 가격에 구매할 수 있어서 손쉽게 무전력을 대비할 수 있다. 또한, 별도의 개발된 최종 사용자 단말기의 경우에도 마이크로-USB나 USB-C로 충전 가능한 내장 배터리를 구비하도록 하여 휴대용 충전장치나, 건전지로 충전할 수 있도록 함으로써 무전력에 대비할 수 있다. 또한, 최종 사용자 단말기가 카드형의 소형 디바이스로 개발될 경우 건전지 교체가 가능하게 할 수 있으며, 저전력으로 오래 사용할 수 있는 설계가 필요하다.

[0055] 한편, 최종 사용자 단말기(일례로, 제1 최종 사용자 단말기(310) 또는 제2 최종 사용자 단말기(320))를 발급받을 때, 또는 보유한 최종 사용자 단말기의 사용을 설정하는 경우, 중개업자(일례로, 중앙은행을 제외한 다른 금융기관들)에게서 KYC 인증 및/또는 아이디/비밀번호 인증 등의 인증 과정을 진행할 수 있다.

[0056] 또한, 인증이 완료된 최종 사용자 단말기에는 인증서가 발급될 수 있다. 이미 설명한 바와 같이 인증서에는 디바이스 고유정보, HSM의 공개정보, 발급 기관 정보 및 유효기간 등이 서명되어 포함될 수 있다. 유효기간은 인증서를 주기적으로 재발급 받게 하여 최신 정보가 유지되도록 하기 위해 활용될 수 있다.

[0057] 또한, 사용자가 최종 사용자 단말기를 사용할 때, 비밀번호, 또는 지문, 홍채, 얼굴인식 등의 생체인증을 통해 디바이스 사용자 인증이 처리될 수 있다. 예를 들어, 최종 사용자 단말기에 설치 및 구동된 결제 프로그램은 사용자가 최종 사용자 단말기를 이용한 결제를 진행하고자 할 때, 최종 사용자 단말기가 디바이스 사용자 인증을 진행하여 사용자를 먼저 인증하도록 최종 사용자 단말기를 제어할 수 있다.

[0058] 온라인 접속 시 또는 오프라인에서 사용자들간의 인증을 진행할 때, 인증서와 함께 디바이스 고유정보 및 HSM의 공개정보, 그리고 발급 기관 정보와 유효기간 등과 같이 CA로부터 인증 받을 때 사용된 정보가 함께 서버나 다른 사용자의 최종 사용자 단말기로 전송되어 사용자의 최종 사용자 단말기에 대한 인증이 이루어질 수 있다.

[0059] 도 4는 본 발명의 일실시예에 따른 온라인 결제 방법의 예를 도시한 흐름도이다. 본 실시예에 따른 온라인 결제 방법은 최종 사용자 단말기를 구현하는 컴퓨터 장치(200)에 의해 수행될 수 있다. 이때, 컴퓨터 장치(200)의 프로세서(220)는 메모리(210)가 포함하는 운영체제의 코드나 적어도 하나의 컴퓨터 프로그램의 코드에 따른 제어 명령(instruction)을 실행하도록 구현될 수 있다. 여기서, 프로세서(220)는 컴퓨터 장치(200)에 저장된 코드가 제공하는 제어 명령에 따라 컴퓨터 장치(200)가 도 4의 방법이 포함하는 단계들(410 내지 470)을 수행하도록 컴퓨터 장치(200)를 제어할 수 있다.

[0060] 단계(410)에서 컴퓨터 장치(200)는 컴퓨터 장치(200)에 발급된 인증서, 컴퓨터 장치(200)의 디바이스 고유정보 및 HSM의 공개정보, 그리고 발급 기관 정보와 유효기간 등과 같이 CA로부터 인증 받을 때 사용된 정보를 서비스 제공자의 서버로 전송할 수 있다. 이 경우, 서비스 제공자의 서버는 전송된 인증서, 디바이스 고유정보 및 HSM의 공개정보, 그리고 발급 기관 정보, 유효기간 등과 같이 CA로부터 인증 받을 때 사용된 정보를 이용하여 최종 사용자 단말기로서의 컴퓨터 장치(200)를 인증할 수 있다.

[0061] 단계(420)에서 컴퓨터 장치(200)는 서버를 통해 사용자의 전자 지갑의 최신 잔액과 마지막 거래 정보(sequence number)를 조회할 수 있다.

[0062] 단계(430)에서 컴퓨터 장치(200)는 조회된 최신 잔액과 마지막 거래 정보를 TEE에 저장할 수 있다. 이미 설명한 바와 같이, 하드웨어적으로 구성되는 TEE 기반의 보안영역은 WBC와 같은 소프트웨어 기술로 대체될 수도 있다.

[0063] 단계(440)에서 컴퓨터 장치(200)는 송금 정보를 수신할 수 있다. 일례로, 컴퓨터 장치(200)는 사용자로부터 송금 금액과 받는 사람 정보를 입력받을 수 있다.

[0064] 단계(450)에서 컴퓨터 장치(200)는 HSM을 이용하여 마지막 거래 정보와 송금 정보를 서명할 수 있다. 예를 들어, HSM이 포함하는 비밀키를 통해 마지막 거래 정보와 송금 정보가 서명될 수 있다.

[0065] 단계(460)에서 컴퓨터 장치(200)는 서명한 정보를 서버로 전송할 수 있다. 서버는 전송된 정보에 따라 받는 사람의 전자 지갑으로 송금 금액을 전달하고, 사용자의 전자 지갑에서 송금 금액을 차감하는 방식으로 해당 결제를 처리할 수 있다.

[0066] 단계(470)에서 컴퓨터 장치(200)는 처리 결과를 확인할 수 있다. 이때, 컴퓨터 장치(200)는 처리가 완료되면, 전자 지갑의 최신 잔액과 마지막 거래 정보를 TEE에 저장할 수 있다.

[0067] 도 5는 본 발명의 일실시예에 따른 오프라인 결제 방법의 예를 도시한 흐름도이다. 본 실시예는 서비스 사용자의 서버와의 통신이 불가능한 경우, 금액을 보내는 최종 사용자 A의 최종 사용자 단말기 a(510)와 금액을 받는 최종 사용자 B의 최종 사용자 단말기 b(520)는 근거리 네트워크를 이용한 P2P 통신(이하, 근거리 통신)을 통해 결제를 처리하는 예를 설명한다. 우선, 최종 사용자 단말기 a(510)와 최종 사용자 단말기 b(520)는 근거리 통신을 통해 인증서를 교환하여 서로 인증 받은 디바이스임을 확인할 수 있다. 이러한 최종 사용자 단말기 a(510)와 최종 사용자 단말기 b(520) 각각은 컴퓨터 장치(200)에 의해 구현될 수 있으며, 각각 TEE 보안 영역과 HSM을 포함할 수 있다.

[0068] 단계(531)에서 최종 사용자 단말기 b(520)는 최종 사용자 단말기 a(510)로 거래를 위한 넌스(nonce)값을 전달할 수 있다. 넌스값은 랜덤하게 생성되는 값일 수 있다.

[0069] 단계(532)에서 최종 사용자 단말기 a(510)는 마지막 거래 정보 1, 넌스값 및 특정 보안값의 해시값을 포함하는 송금 트랜잭션을 최종 사용자 단말기 b(520)로 전송할 수 있다. 여기서, 마지막 거래 정보 1은 TEE에 저장된 시퀀스 넘버를 포함할 수 있으며, 특정 보안값은 랜덤하게 생성되는 값일 수 있다. 이때, 송금 트랜잭션은 HSM의 비밀키로 서명될 수 있으며, HSM의 공개정보로서의 퍼블릭 키와 함께 최종 사용자 단말기 b(520)로 전송될 수 있다. 실시예에 따라 최종 사용자 단말기 a(510)가 HSM의 공개정보로서의 퍼블릭 키를 최종 사용자 단말기 b(520)로 전송할 필요 없이, 최종 사용자 단말기 b(520)가 최종 사용자 단말기 a(510)의 인증서로부터 HSM의 공개정보로서의 퍼블릭 키를 얻을 수도 있다.

[0070] 단계(533)에서 최종 사용자 단말기 b(520)는 수신된 송금 트랜잭션 및 넌스값을 검증할 수 있다. 일례로, 최종 사용자 단말기 b(520)는 퍼블릭 키를 이용하여 수신된 송금 트랜잭션에 대한 서명 검증을 처리할 수 있으며, 송금 트랜잭션에 포함된 넌스값이 단계(510)에서 전달한 넌스값과 동일한지 확인할 수 있다. 이때, 수신된 송금 트랜잭션에 대한 서명 검증이 실패하거나, 수신된 넌스값이 단계(510)에서 전달한 넌스값과 다르거나 또는 이미 처리된 넌스값이 수신된 경우, 최종 사용자 단말기 b(520)는 최종 사용자 단말기 a(510)로 실패 메시지를 전송할 수 있다. 또한, 최종 사용자 단말기 b(520)는 수신된 송금 트랜잭션을 마지막 거래 정보 2와 함께 저장할 수 있다. 여기서, 마지막 거래 정보 2는 마지막 거래 정보 1과 달리 현재의 거래에 대한 정보일 수 있다.

[0071] 단계(534)에서 최종 사용자 단말기 b(520)는 최종 사용자 단말기 a(510)로 검증 결과를 전송할 수 있다. 일례로, 최종 사용자 단말기 b(520)는 검증 성공 메시지나 검증 실패 메시지를 최종 사용자 단말기 a(510)로 전송할 수 있다.

[0072] 단계(535)에서 최종 사용자 단말기 a(510)는 검증 결과가 성공인 경우, 최종 사용자 단말기 b(520)로 송금 트랜잭션의 보안값의 원문을 전송할 수 있다. 만약, 최종 사용자 단말기 b(520)가 최종 사용자 단말기 b(520)로부터 일정 시간 내에 검증 성공 메시지를 수신하지 못하는 경우, 거래는 취소될 수 있다. 이 경우, 최종 사용자 단말기 b(520)는 보안값의 원문을 전달받지 못하게 된다.

[0073] 단계(536)에서 최종 사용자 단말기 a(510)는 마지막 거래 정보 2와 최신 잔액을 TEE에 저장할 수 있다. 최신 잔액은 최종 사용자 A의 전자 지갑의 최신 잔액일 수 있다.

[0074] 이후 통신이 복구되면, 최종 사용자 단말기 b(520)는 최종 사용자 단말기 a(510)로부터 수신한 송금 트랜잭션과 보안값의 원문을 CBDC 원장으로 전송하여 최종 사용자 단말기 a(510)에서 최종 사용자 단말기 b(520)로의 오프라인 상황에서 발생한 거래를 순서대로 원장과 동기화시킬 수 있다. 만약, 단계(550)에서 최종 사용자 단말기 b(520)가 보안값의 원문을 전달받지 못하는 경우, 원장과의 동기화가 실패되고, 실질적으로 해당 거래가 취소될 수 있다. 금번 거래를 통해 마지막 거래 정보가 갱신되어야 하기 때문에 마지막 거래 정보 2는 마지막 거래 정

보 1과 달리 현재의 거래에 대한 정보일 수 있다. 실시예에 따라 단계(536)에서 최종 사용자 단말기 a(510)의 TEE에 저장되는 마지막 거래 정보 2와 단계(533)에서 최종 사용자 단말기 b(520)의 TEE에 저장되는 마지막 거래 정보 2는 적어도 일부의 내용이 상이한 정보일 수 있다.

[0075] 실시예에 따라 다음 (a) 내지 (c)와 같은 제약사항들이 적용될 수도 있다.

[0076] (a) 오프라인 상황에서 수신한 거래 금액은 온라인에서 CBDC 원장 서비스와의 동기화 없이는 사용할 수 없다.

[0077] (b) 최종 사용자 단말기에서 사용 가능한 금액이 제한될 수 있다.

[0078] (c) 오프라인에서 사용 가능한 금액의 한도, 거래 횟수, 오프라인 상황에서 거래를 진행할 수 있는 유효시간 중 적어도 하나를 설정하여 한도나 횟수 또는 시간이 초과되는 경우 거래를 제한할 수 있다.

[0079] 본 실시예에 따르면, HSM과 연동된 전자 지갑의 모든 거래는 해당 HSM을 포함하는 최종 사용자 단말기에서 처리된다. 예를 들어, HSM의 비밀키가 복제될 수 없기 때문에 연동된 전자 지갑의 모든 거래는 해당 HSM을 포함하는 최종 사용자 단말기에서 처리됨이 보장될 수 있다. 또한, 전자 지갑의 인증을 통해 인증서에 기록된 디바이스 고유정보와 HSM의 공개정보가 동일한지 여부를 확인하기 때문에 다른 디바이스에서 사용될 수 없다. 또한, 본 실시예에 따르면, 완료된 거래는 TEE에 저장되므로 강제로 수정할 수 없다. 이때, 거래가 하나의 최종 사용자 단말기에서만 진행되므로 TEE에 저장되는 정보는 항상 최신의 정보가 저장된다. 따라서, 이중 지불이 방지될 수 있다.

[0080] 또한, 본 실시예에서는 하드웨어적으로 구성되는 TEE 기반의 보안영역에 대해서 설명하고 있으나, 이러한 TEE는 WBC와 같은 소프트웨어 기술로 대체될 수도 있다.

[0081] 이처럼, 본 발명의 실시예들에 따르면, 오프라인 상황(사용자의 단말기가 네트워크를 통해 서버에 연결될 수 없는 상황)에서도 이중 지불 없이 중앙은행 디지털 화폐(Central Bank Digital Currency, CBDC)를 이용하여 결제를 처리할 수 있다.

[0082] 이상에서 설명된 시스템 또는 장치는 하드웨어 구성요소, 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 어플리케이션을 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.

[0083] 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 기록매체에 저장될 수 있다.

[0084] 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. 매체는 컴퓨터로 실행 가능한 프로그램을 계속 저장하거나, 실행 또는 다운로드를 위해 임시 저장하는 것일 수도 있다. 또한, 매체는 단일 또는 수개 하드웨어가 결합된 형태의 다양한 기록수단 또는 저장수단일 수 있는데, 어떤 컴퓨터 시스템에 직접 접속되는 매체에 한정되지 않고, 네트워크 상에 분산 존재하는 것일 수도 있다. 매체의 예시로는, 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체, CD-ROM 및 DVD와 같은 광기록 매체, 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical medium), 및 ROM, RAM, 플래시 메모리 등을 포함하여 프로그램 명령어가 저장되도록 구성된

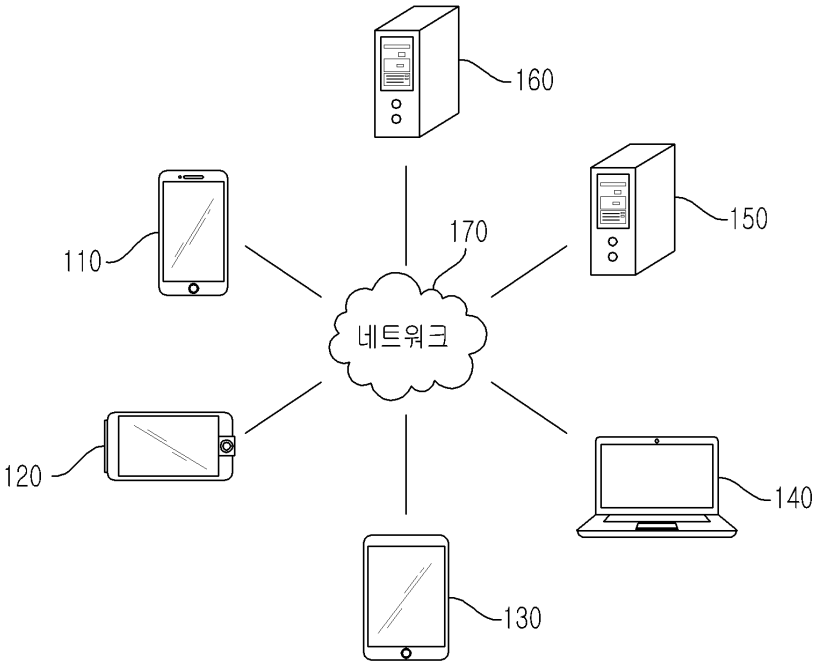
것이 있을 수 있다. 또한, 다른 매체의 예시로, 애플리케이션을 유통하는 앱 스토어나 기타 다양한 소프트웨어를 공급 내지 유통하는 사이트, 서버 등에서 관리하는 기록매체 내지 저장매체도 들 수 있다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다.

[0085] 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.

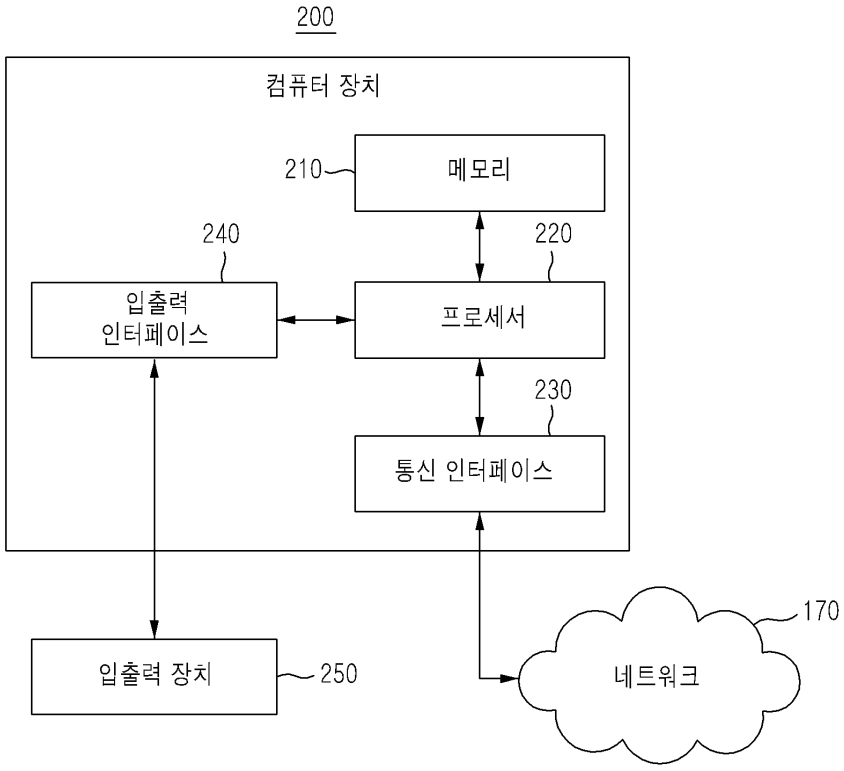
[0086] 그러므로, 다른 구현들, 다른 실시예들 및 청구범위와 균등한 것들도 후술하는 청구범위의 범위에 속한다.

도면

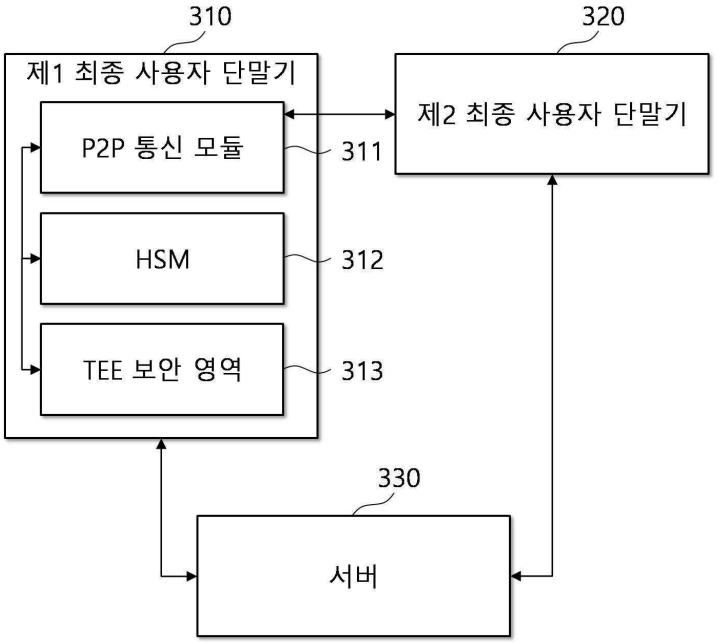
도면1



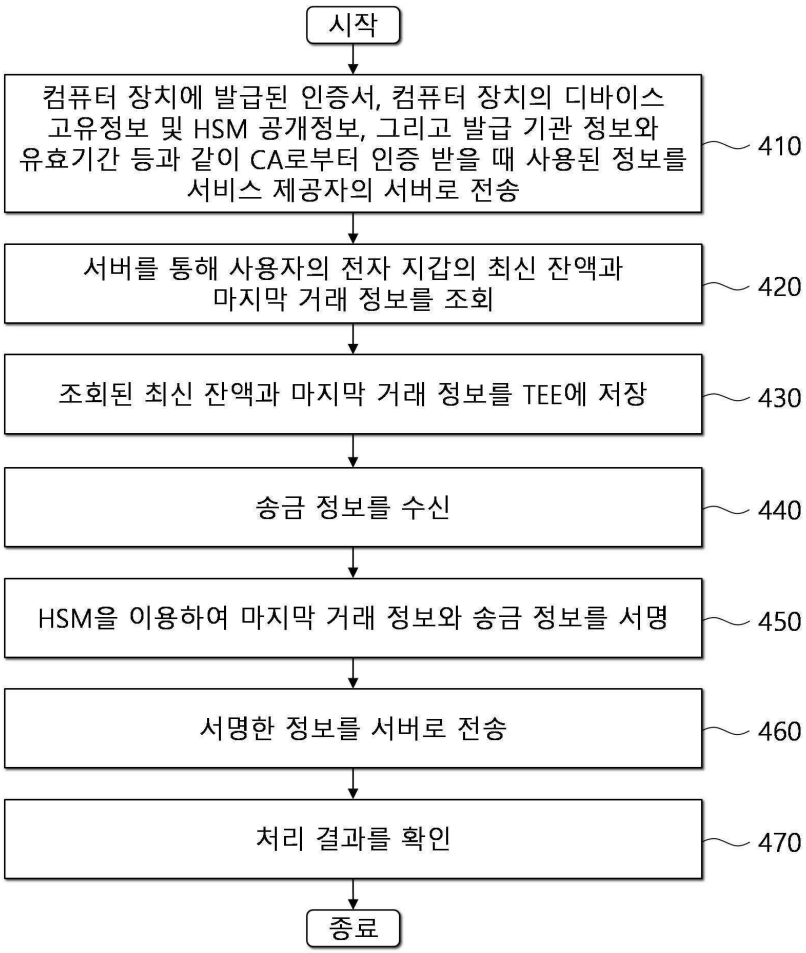
도면2


200
컴퓨터 장치
210
메모리
240
220
입출력
인터페이스
프로세서
230
통신 인터페이스
170
입출력 장치
250
네트워크

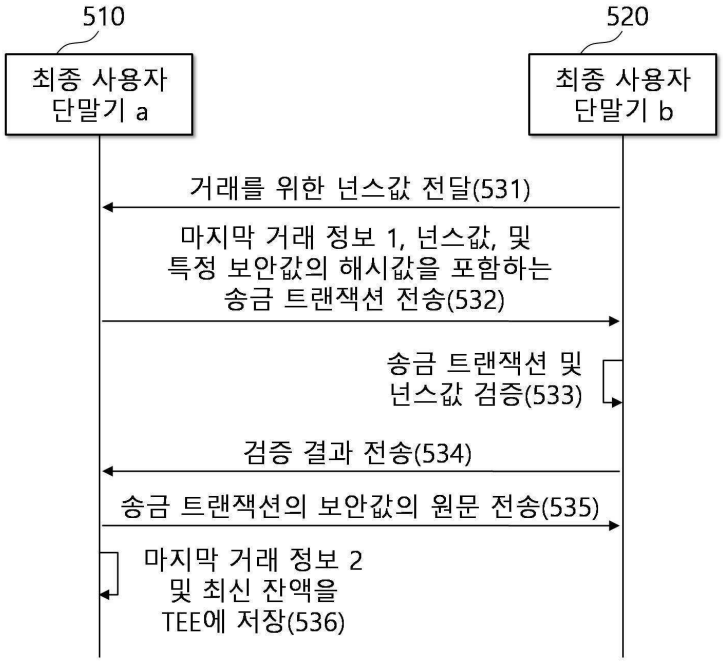
도면3


310
320
제1 최종 사용자 단말기
제2 최종 사용자 단말기
P2P 통신 모듈
311
HSM
312
TEE 보안 영역
313
330
서버

도면4


시작
컴퓨터 장치에 발급된 인증서, 컴퓨터 장치의 디바이스 고유정보 및 HSM 공개정보, 그리고 발급 기관 정보와 유효기간 등과 같이 CA로부터 인증 받을 때 사용된 정보를 서비스 제공자의 서버로 전송
410
서버를 통해 사용자의 전자 지갑의 최신 잔액과 마지막 거래 정보를 조회
420
조회된 최신 잔액과 마지막 거래 정보를 TEE에 저장
430
송금 정보를 수신
440
HSM을 이용하여 마지막 거래 정보와 송금 정보를 서명
450
서명한 정보를 서버로 전송
460
처리 결과를 확인
470
종료

도면5


510
520
최종 사용자 단말기 a
최종 사용자 단말기 b
거래를 위한 넌스값 전달(531)
마지막 거래 정보 1, 넌스값, 및 특정 보안값의 해시값을 포함하는 송금 트랜잭션 전송(532)
송금 트랜잭션 및 넌스값 검증(533)
검증 결과 전송(534)
송금 트랜잭션의 보안값의 원문 전송(535)
마지막 거래 정보 2 및 최신 잔액을 TEE에 저장(536)