November 2022

DEVICE AND METHOD FOR ACCEPTING CENTRAL BANK DIGITAL CURRENCY(CBDC) IN PAYMENT NETWORKS

PAMELA GHOSH
VISA

VANESA MEYER
VISA

WANYUN GU
VISA

TITLE: “DEVICE AND METHOD FOR ACCEPTING CENTRAL BANK DIGITAL CURRENCY(CBDC) IN PAYMENT NETWORKS”

VISA

PAMELA GHOSH

VANESA MEYER

WANYUN GU

TECHNICAL FIELD

[0001] This disclosure relates generally to the field of digital transactions using the Central Bank Digital Currency (CBDC). More particularly, the present disclosure relates to a device and method for accepting CBDC in payment networks.

BACKGROUND

[0002] Central bank digital currencies (CBDCs) will play a role in the digital infrastructure for payments. CBDC is a digital form of central bank liability issued by a central bank and intended as a legal tender. While a CBDC is a digital representation of a fiat currency, it will be backed by a certain monetary reserve.

[0003] CBDC simplifies the implementation of monetary policy by making it easier to propagate money through the economy. CBDC can enable participation by people, small business owners, etc., in the formal financial system and advance social impact in the long term. However, the adoption of CBDC depends on how soon the banking industry can innovate and adopt newer infrastructure and on how soon merchants/acquirers can start accepting CBDC as a reliable payment source.

[0004] Apart from existing financial players in 4-party model, there is an important role for private sector fintechs and developers to play in the new ecosystem. CBDC should be a platform for developers to build digital currency wallets and to utilize digital currencies in existing and new payment flows. For central banks, it will be difficult to build a vibrant developer ecosystem on their own where they can provide a range of value-added services to help global developers to build new applications while efficiently vetting these applications and ensure they meet high standards for compliance, user experience, and cybersecurity. Thus, there is a need for an improved device and method for facilitating the CBDC transactions in payments networks, so that a greater number of users are inspired to adopt or accept the CBDC as the payment mode.

SUMMARY

[0005] The present disclosure relates to a device and method for accepting CBDC in payment networks. In the present disclosure, initially an interaction module may receive an onboarding

request from an authorizing entity computer. Further, the interaction module may transmit a request to a blockchain network to generate a wallet identifier and a private key for the authorizing entity. The generation of the wallet identifier leads to the creation of an account associated with the authorizing entity operating with the authorizing entity computer. Upon transmitting the request, the interaction module may receive the wallet identifier and the private key from the blockchain network. The received wallet identifier and the private key may be stored by the interaction module in a secure vault. Furthermore, the interaction module may receive a request from the authorizing entity computer to add an amount to the account associated with the authorizing entity. Moreover, the interaction module may transmit the request to a central entity via the blockchain network to add the amount to the account associated with the authorizing entity. Finally, the central entity may add the requested amount in the account associated with the authorizing entity.

[0006] In some embodiments of the present disclosure, the interaction module may receive a request from the authorizing entity computer, a request to generate a user account associated with the authorizing entity. Further, the interaction module may transmit a request to the blockchain network to generate a wallet identifier and private key for the user. The generation of the wallet identifier leads to creation of an account of the user associated with the authorizing entity account. The interaction module may further receive the generated wallet identifier and the private key from the blockchain network. Also, the interaction module may generate a card identifier associated with the wallet identifier. Upon generation, the interaction module may transmit the card identifier and the wallet identifier to the authorizing entity computer. The authorizing entity computer finally transmits the card identifier and the wallet identifier to a user device associated with the user.

[0007] In some embodiments of the present disclosure, the interaction module, may receive an authorization request message which comprises the card identifier and a first amount, from a network computer. The interaction module may access a user account in a local ledger using the wallet identifier to determine if the first amount is less than or equal to a second amount in the user account. Further, the interaction module may transmit an instruction message to the blockchain network to move the first amount from the user account to the authorizing entity account. Finally, the interaction module may transmit an authorization status message to the network computer.

[0008] In some embodiments of the present disclosure, the interaction module may receive a notification that the transfer has been settled. Further, the interaction module may generate a settlement message for the authorizing entity. The settlement message may include settlements to be performed for all CBDC transactions made during a particular time-period. The interaction module may then transmit the settlement message to the authorizing entity. Further, the authorizing entity upon receiving the settlement message, requests the interaction module to burn CBDC for Fiat currency such as Indian Rupees and the like. Finally, the interaction module may burn CBDC to obtain Fiat currency for the authorization entity. The authorization entity may perform a normal fiat currency settlement between the authorizing entity and the acquirer bank using the Fiat currency from the liquidity pool.

[0009] In the present disclosure, the interaction module which is also referred to as a CBDC payment module provides an enhanced methodology for CBDC adoption among existing financial players like merchant and acquirers for acceptance and issuers for issuance without any significant change in their infrastructure. In some embodiments, the CBDC payment module may be delegated by the payment network such as Visa and the like. The CBDC payment module is intended to increase the acceptance of CBDC in current payment network without much impact on existing banking infrastructure. Also, the CBDC payment module provides a key management service to a small and medium bank. The CBDC payment module may alternatively enable consumers and businesses to make transactions using digital currency (for example, CBDC's digital currency) instead of cash that is free of credit and liquidity risk, unlike bank and non-bank money. Moreover, the CBDC payment module may reduce barriers to financial inclusion and reduce transaction costs. CBDC payments module onboards Retail Banks (RB) for CBDC Management Services, provides Application Programming Interface (APIs) for Retail Bank to create retail user wallet under Issuer/RB entity, facilitates CBDC payments through Visa network, leading to acceptance of CBDC linked debit cards by all the merchants and acquirer network who accepts the payment network such as Visa today, and also internally manages authorization and settlement flows for CBDC acceptance through CBDC linked debit cards.

[0010] These and other features and characteristics of the present invention, as well as the methods of operation and functions of the related elements of structures and the combination of parts and economies of manufacture, will become more apparent upon consideration of the following description and the appended claims with reference to the accompanying drawings, all of which form a part of this specification, wherein like reference numerals designate corresponding parts in the various figures. It is to be expressly understood, however, that the drawings are for the purpose of illustration and description only and are not intended as a definition of the limits of the invention. As used in the specification and the claims, the singular form of "a," "an," and "the" include plural referents unless the context clearly dictates otherwise.

BRIEF DESCRIPTION OF THE DRAWINGS

[0011] Additional advantages and details of non-limiting embodiments are explained in greater detail below with reference to the exemplary embodiments that are illustrated in the accompanying schematic figures, in which:

[0012] **FIG. 1** discloses a schematic diagram of a system for facilitating CBDC payments using an interaction module, in accordance with some embodiments of the present disclosure;

[0013] **FIG.2** discloses an exemplary architecture of Certificate Authority (CA) for wallet providers, in accordance with some embodiments of the present disclosure; and

[0014] **FIG.3** discloses a process flow between the wallet providers and the central bank using the delegated CA, in accordance with some embodiments of the present disclosure.

[0015] **FIG. 4** illustrates an exemplary scenario of wallet provisioning in Offline payment system, in accordance with some embodiments of the present disclosure.

[0016] **FIG. 5** illustrates an exemplary scenario of a receiver claiming funds sent by a sender using a secure hardware, in accordance with some embodiments of the present disclosure.

[0017] **FIG. 6** illustrates an exemplary scenario of adding funds into receiver's offline balance using a secure hardware, in accordance with some embodiments of the present disclosure. and

[0018] **FIG. 7** illustrates an exemplary scenario of receiver forwarding withdraw message to a bank to add funds to receiver's online balance, in accordance with some embodiments of the present disclosure.

DESCRIPTION OF THE DISCLOSURE

[0019] In the present document, the word "exemplary" is used herein to mean "serving as an example, instance, or illustration." Any embodiment or implementation of the present subject matter described herein as "exemplary" is not necessarily to be construed as preferred or advantageous over other embodiments.

[0020] While the disclosure is susceptible to various modifications and alternative forms, specific embodiment thereof has been shown by way of example in the drawings and will be described in detail below. It should be understood, however that it is not intended to limit the disclosure to the particular forms disclosed, but on the contrary, the disclosure is to cover all modifications, equivalents, and alternative falling within the spirit and the scope of the disclosure.

[0021] The terms "comprises", "comprising", or any other variations thereof, are intended to cover a non-exclusive inclusion, such that a setup, device or method that comprises a list of components or steps does not include only those components or steps but may include other components or steps not expressly listed or inherent to such setup or device or method. In other words, one or more elements in a device or system or apparatus proceeded by "comprises… a" does not, without more constraints, preclude the existence of other elements or additional elements in the device or system or apparatus.

[0022] The terms "an embodiment", "embodiment", "embodiments", "the embodiment", "the embodiments", "one or more embodiments", "some embodiments", and "one embodiment" mean "one or more (but not all) embodiments of the invention(s)" unless expressly specified otherwise.

[0023] The terms "including", "comprising", "having" and variations thereof mean "including but not limited to", unless expressly specified otherwise.

[0024] For purposes of the description hereinafter, the terms “end,” “upper,” “lower,” “right,” “left,” “vertical,” “horizontal,” “top,” “bottom,” “lateral,” “longitudinal,” and derivatives thereof shall relate to the invention as it is oriented in the drawing figures. However, it is to be understood that the invention may assume various alternative variations and step sequences, except where expressly specified to the contrary. It is also to be understood that the specific devices and processes illustrated in the attached drawings, and described in the following specification, are simply exemplary embodiments or aspects of the invention. Hence, specific dimensions and other physical characteristics related to the embodiments or aspects disclosed herein are not to be considered as limiting.

[0025] As used herein, the terms “communication” and “communicate” may refer to the reception, receipt, transmission, transfer, provision, and/or the like of information (e.g., data, signals, messages, instructions, commands, and/or the like). For one unit (e.g., a device, a system, a component of a device or system, combinations thereof, and/or the like) to be in communication with another unit means that the one unit is able to directly or indirectly receive information from and/or transmit information to the other unit. This may refer to a direct or indirect connection (e.g., a direct communication connection, an indirect communication connection, and/or the like) that is wired and/or wireless in nature. Additionally, two units may be in communication with each other even though the information transmitted may be modified, processed, relayed, and/or routed between the first and second unit. For example, a first unit may be in communication with a second unit even though the first unit passively receives information and does not actively transmit information to the second unit. As another example, a first unit may be in communication with a second unit if at least one intermediary unit (e.g., a third unit located between the first unit and the second unit) processes information received from the first unit and communicates the processed information to the second unit. In some non-limiting embodiments, a message may refer to a network packet (e.g., a data packet and/or the like) that includes data. It will be appreciated that numerous other arrangements are possible.

[0026] As used herein, the term “merchant” may refer to an individual or entity that provides goods and/or services, or access to goods and/or services, to customers based on a transaction, such as a payment transaction. The term “merchant” or “merchant system” may also refer to one or more computer systems operated by or on behalf of a merchant, such as a server computer

executing one or more software applications. A "point-of-sale (POS) system," as used herein, may refer to one or more computers and/or peripheral devices used by a merchant to engage in payment transactions with customers, including one or more card readers, near-field communication (NFC) receivers, RFID receivers, and/or other contactless transceivers or receivers, contact-based receivers, payment terminals, computers, servers, input devices, and/or other like devices that can be used to initiate a payment transaction.

[0027] As used herein, the term "user" may include an individual. In some embodiments, a user may be associated with one or more personal accounts and/or mobile devices. The user may also be referred to as a cardholder, account holder, or consumer in some embodiments.

[0028] As used herein, the term "user device" may be a device that is operated by a user. Examples of user devices may include a mobile phone, a smart phone, a card, a personal digital assistant (PDA), a laptop computer, a desktop computer, a server computer, a thin-client device, a tablet PC, etc. Additionally, user devices may be any type of wearable technology device, such as a watch, earpiece, glasses, etc. The user device may include one or more processors capable of processing user input. The user device may also include one or more input sensors for receiving user input. As is known in the art, there are a variety of input sensors capable of detecting user input, such as accelerometers, cameras, microphones, etc. The user input obtained by the input sensors may be from a variety of data input types, including, but not limited to, audio data, visual data, or biometric data. The user device may comprise any electronic device that may be operated by a user, which may also provide remote communication capabilities to a network. Examples of remote communication capabilities include using a mobile phone (wireless) network, wireless data network (e.g., 3G, 4G or similar networks), Wi-Fi, Wi-Max, or any other communication medium that may provide access to a network such as the Internet or a private network. A user device may also be a credit, debit, or prepaid card.

[0029] As used herein, the term "resource provider" can be any suitable entity that provides resources (e.g., goods, services, access to secure data, access to locations, or the like) during a transaction. For example, a resource providing entity can be a merchant, a venue operator, a building owner, a governmental entity, etc. A "merchant" may typically be an entity that engages in transactions and can sell goods or services or provide access to goods or services.

[0030] As used herein, the term “access device” may be any suitable device for providing access to an external computer system. An access device may be in any suitable form. Some examples of access devices include point of sale (POS) devices, cellular phones, PDAs, personal computers (PCs), tablet PCs, hand-held specialized readers, set-top boxes, electronic cash registers (ECRs), automated teller machines (ATMs), virtual cash registers (VCRs), kiosks, security systems, access systems, Websites, and the like. An access device may use any suitable contact or contactless mode of operation to send or receive data from, or associated with, a mobile device. In some embodiments, where an access device may comprise a POS terminal, any suitable POS terminal may be used and may include a reader, a processor, and a computer-readable medium. A reader may include any suitable contact or contactless mode of operation. For example, exemplary card readers can include radio frequency (RF) antennas, optical scanners, bar code readers, or magnetic stripe readers to interact with a mobile device.

[0031] As used herein, the term "Access data" may include any suitable data that can be used to access a resource or create data that can access a resource. In some embodiments, access data may be account information for a payment account. Account information may include a PAN (primary account number), payment token, expiration date, verification values (e.g., CVV, CVV2, dCVV, dCVV2), etc. In other embodiments, access data may be data that can be used to activate account data. For example, in some cases, account information may be stored on a mobile device, but may not be activated until specific information is received by the mobile device. In other embodiments, access data could include data that can be used to access a location. Such access data may be ticket information for an event, data to access a building, transit ticket information, etc. In yet other embodiments, access data may include data used to obtain access to sensitive data. Examples of access data may include codes or other data that are needed by a server computer to grant access to the sensitive data.

[0032] As used herein, the term “authorizing entity” may be an entity that authorizes a request, typically using an authorizing computer to do so. An authorizing entity may be an issuer, a governmental agency, a document repository, an access administrator, etc. An “issuer” may typically include a business entity (e.g., a bank) that maintains an account for a user. An issuer

may also issue payment credentials stored on a user device, such as a cellular telephone, smart card, tablet, or laptop to the user.

[0033] As used herein, the term "network computer" may be a computer in a network. An authorizing computer may be an example of a network computer.

[0034] As used herein, the term "authorization request message" may be an electronic message that is sent to a payment processing network and/or an issuer of a payment card to request authorization for a transaction. An authorization request message according to some embodiments may comply with ISO 8583, which is a standard for systems that exchange electronic transaction information associated with a payment made by a user using a payment device or payment account. The authorization request message may include an issuer account identifier that may be associated with a payment device or payment account. An authorization request message may also comprise additional data elements corresponding to "identification information" including, by way of example only: a service code, a CVV (card verification value), a dCVV (dynamic card verification value), an expiration date, etc. An authorization request message may also comprise "transaction information," such as any information associated with a current transaction, such as the transaction amount, merchant identifier, merchant location, etc., as well as any other information that may be utilized in determining whether to identify and/or authorize a transaction.

[0035] As used herein, the term "authorization response message" may be an electronic message reply to an authorization request message generated by an issuing financial institution or a payment processing network. The authorization response message may include, by way of example only, one or more of the following status indicators: Approval -- transaction was approved; Decline -- transaction was not approved; or Call Center -- response pending more information, merchant must call the toll-free authorization phone number. The authorization response message may also include an authorization code, which may be a code that a credit card issuing bank returns in response to an authorization request message in an electronic message (either directly or through the payment processing network) to the merchant's access device (e.g., POS equipment) that indicates approval of the transaction. The code may serve as proof of authorization. As noted above, in some embodiments, a payment processing network may generate or forward the authorization response message to the merchant.

[0036] As used herein, the term "blockchain" can be a distributed database that maintains a continuously-growing list of records secured from tampering and revision. A blockchain may include a number of blocks of interaction records. Each block in the blockchain can contain also include a timestamp and a link to a previous block. Stated differently, interaction records in a blockchain may be stored as a series of "blocks," or permanent files that include a record of a number of interactions occurring over a given period of time. Blocks may be appended to a blockchain by an appropriate node after it completes the block and the block is validated. Each block can be associated with a block header. In embodiments of the invention, a blockchain may be distributed, and a copy of the blockchain may be maintained at each full node in a verification network. Any node within the verification network may subsequently use the blockchain to verify interactions.

[0037] As used herein, the term “node” may be a point at which lines or pathways intersect or branch or can be a central or connecting point. A node can also be a “computer node,” which can be any computer or device that connects to the verification network. A node that can fully verify each block and interaction in the blockchain can be a full node. A “full node” can store the full blockchain (i.e., each block and each interaction). In some embodiments, a “user device” may be a computer node in the verification network.

[0038] As used herein, the term “block header” can be a header including information regarding a block. A block header can be used to identify a particular block of a blockchain. A block header can comprise any suitable information, such as a previous hash, a Merkle root, a timestamp, and a nonce. In some embodiments, a block header can also include a difficulty value.

[0039] As used herein, the term “nonce” can include an arbitrary number. In some embodiments, a nonce can be a value that can be adjusted by a full node while performing a proof-of-work process. A nonce can be input into a hash function along with block data to determine the output hash value. A correct nonce (also referred to as a golden nonce) yields an output hash value that satisfies a predetermined criteria, such as being less than a difficulty value. A nonce can be of any suitable length (e.g., 32-bits).

[0040] It will be apparent that systems and/or methods, described herein, can be implemented in different forms of hardware, software, or a combination of hardware and software. The actual specialized control hardware or software code used to implement these systems and/or methods is not limiting of the implementations. Thus, the operation and behavior of the systems and/or methods are described herein without reference to specific software code, it being understood that software and hardware can be designed to implement the systems and/or methods based on the description herein.

[0041] Some non-limiting embodiments or aspects are described herein in connection with thresholds. As used herein, satisfying a threshold may refer to a value being greater than the threshold, more than the threshold, higher than the threshold, greater than or equal to the threshold, less than the threshold, fewer than the threshold, lower than the threshold, less than or equal to the threshold, equal to the threshold, etc.

[0042] The CBDC system is a two-tier model, which comprises of an infrastructure tier and a payment tier. The infrastructure tier includes a central bank and intermediate Central Authorities (CA) which may issue and distribute the CBDC. Also, the infrastructure tier certifies some of the financial institutions of banks for issuing the CBDCs. The payment tier includes one or more banks, or the financial institutions and the users associated with the financial institutions. In some embodiments, payment network such as Visa may be part of both the payment tier and the infrastructure tier. In the payment tier, the CBDCs are transferred between user wallets as a medium of exchange by the financial institutions or the banks.

[0043] The CBDC payments may be performed using online mode of payments or offline mode of payments. Online payments are the most common type of payments. These payments require either or both ends of the payment to communicate with one or more payment providers at the time of payment to verify the availability of funds and to ensure the compliance of the transaction with policies and regulations. In cryptocurrency payments, the users needs to communicate with Distributed Ledger Technology (or DLT) to issue and validate payment transactions.

[0044] Offline payments, on the other hand, may happen without any communication with the payment providers or DLT, and for that reason, are sometimes called point-to-point payments. This is a unique feature of physical cash transactions that can happen under any condition between two parties. When the offline device comes online, it syncs with the server to make the offline balance available online. For that reason, offline payments complement online payments. Unlike cash payments, offline payments traditionally expose the payee to settlement risks, as it is not possible to independently verify that the payer has sufficient funds to honor the payment. To address this challenge, an Offline Payment System (or OPS) is proposed in the present disclosure which relies on secure hardware to remove settlement risks. This resembles for instance to a tamper-resistance property of physical cash that protects against double spending of money in absence of payment providers.

[0045] The CBDC offline payments may be performed using point-to-point (P2P) payments, cash like features. The offline payment system relies on secure hardware and has less settlement risks and there is no risk of double spending. Similarly, the CBDC online payments may be executed through the payment providers (e.g., PayPal, Paytm, Razorpay, Visa and the like) or a distributed ledger technology (DLT) (e.g., Blockchain).

[0046]

[0047] Before any offline payment can occur, sender needs to provision secure wallet by obtaining a certificate and a special piece of code, known as the OPS Trusted Application (or OPS TA), from senders bank as shown in the **FIG.4**. The certificate is essentially a set of digital signatures attesting that the secure hardware is authentic, and the issuing bank as well as all intermediate CAs on the path to the central bank are also certified. The OPS TA consists of a set of instructions deployed on the secure hardware within the enclave and executes the core functionalities of OPS such as updating the user's offline balance. Wallet provisioning is a one-time setup that is performed after the user installs the OPS wallet app on user device such as smartphone, tablet phone, laptop and the like. The CBDC offline payments may be performed between the users directly. Consider a scenario where user 1 (also referred to as sender) should initiate CBDC payment to user 2 (also referred to as receiver). Further, consider user 1 and user 2 may have an account in different banks. For example, consider user 1 directly interacts with Bank B to register for the CBDC payments using his mobile device and upon successful registration, a

wallet is created for an application installed in the mobile device associated with the user 1. Similarly, user 2 directly interacts with Bank C for registration and creation of wallet in an application installed in the mobile device associated with user 2 to make the CBDC payments, in the offline payment system. Upon registration and creation of wallet, the user 1 may make a payment to user 2 securely without either user communicating with their bank at the time of payment. OPS may require the sender phone to have a secure hardware which is already available on mobile device. A secure hardware provides an isolated execution environment inside the mobile device that can store data and execute code securely. Such environment is designed such that it is difficult to tamper with the code and data stored in it. This means that funds can be stored on the secure hardware and issue payments that are digitally signed with the secure hardware's secret key. User 2 may then verify the authenticity of the payment completely offline using the secure hardware's certificate. Also, OPS does not require User 2 to have a secure hardware unless user 2 is also willing to send money offline. Therefore, secure hardware is only needed on sender phones.

[0048] In some embodiments of the present disclosure, the online CBDC payments may be performed between the sender and the receiver. The sender device and the receiver device are associated with a secure hardware for performing the secure transaction. For online CBDC payment, the sender and the receiver may register using an application and a wallet for sender and receiver is created in the application installed in user devices such as smartphones, laptops, tablet phones etc., of the sender and receiver respectively. Once the wallet is provisioned, the user may deposit funds into his/her wallet when he/she is online. For depositing the funds, the user requests the bank to deposit an amount of "x" money from his/her online balance stored at the bank into his/her offline balance stored in the secure hardware. The bank may then respond with a signature indicating that "x" amount was deducted from the user's online balance. The Offline Payment System (OPS) inside the secure hardware verifies the signature with the bank's public verification key and adds x to the offline balance stored in Trusted Application (TA). When the sender initiates CBDC payment to the receiver, verification of sufficient funds in sender's account to make the CBDC payments is performed. In some embodiments, when both sender and receiver are offline, sender may initiate an offline payment by requesting receiver's address which is essentially his public key. Thereafter, sender triggers his/her secure hardware by calling the OPS TA to securely deduct the payment amount from his/her balance and create a signed payment message containing

the payment amount (CBDC amount), the sender's certificate, the receiver's address, and a replay protection counter referred to as Index. Thereafter, sender sends the payment message to receiver who verifies the sender's signature and his/her certificate and checks that the payment contains his address as the recipient. If all checks pass, receiver accepts the payment and stores it on his/her computing device such as a mobile phone. By deducting the payment amount (CBDC amount) from the sender's offline balance, the secure hardware is essentially preventing double spending of that amount. When the receiver wants to add the CBDC amount of the payment that he/she received offline from the sender to his online balance stored at bank associated with the receiver (also referred as receiver's bank), then receiver may claim it from the bank whenever he/she goes online as shown in the **FIG.5**. The bank verifies the validity of payment by checking the signature and whether or not it was previously marked as spent using a payment log that the bank stores. If all checks pass, the bank adds the CBDC amount of the payment to the receiver's online balance, for example in the form of Fiat Currency, and adds the payment to the log.

[0049] In some embodiments, as shown in **Fig. 6**, the receiver may also have a secure hardware that is set up in a similar fashion to the sender. If receiver wishes to make offline payments using funds he previously received offline from sender without going online, then receiver can invoke a special functionality of the OPS TA, known as Collect, to add the payment amount into his/her offline balance. This allows receiver to spend the funds offline in exactly the same way as sender made the first offline payment. Also, to ensure that payments meet the bank's policies and regulations, the OPS users periodically sync with their banks. For example, the bank might want to limit how much money the user can spend offline during each epoch or even blacklist one's wallet after suspecting fraud activities. The frequency of online syncs and all the conditions set by it can be set by the bank after every online sync.

[0050] In some embodiments, as shown in **Fig. 7** when a user with secure hardware wishes to move funds from his/her offline wallet to his/her online wallet stored at the bank, the present disclosure enables such an action to be performed via a protocol called "Withdraw" which invokes OPS TA withdraw function to deduct funds from the secure hardware and return a message signed with the secure hardware's signing key. The user thereafter forwards the signed withdraw message

to the bank who adds the fund to the user's online balance after verifying the signature and certificates.

[0051] In some embodiments, to protect against replay attacks by malicious intermediaries such as a corrupt wallet application on the user's phone, both the secure hardware and the bank maintain monotonically increasing counters that are incremented after every round of communication between the two parties such as a sender and a receiver. Both parties include the latest value of these counters in their signed messages so that the receiver can verify the uniqueness and ordering of all messages according to their local counter which is synchronized after every exchange.

[0052] For example, consider during the protocol flow, two measures in OPS protect users against offline double spending attacks: Secure hardware and Payment logs. In some embodiments, a malicious wallet app may try to send copies of the same payment object to the same user to spend the same money twice. In fact, the payment log maintained by receiver can detect this attempt and drop the second object. In some embodiments, the malicious app may attempts to send the same payment object to two different users, which in fact, is not allowed as each payment message is signed by the sender's secure hardware and the message includes the address of the actual recipient.

[0053] As discussed above, the present disclosure relates to a CBDC payment module for facilitating CBDC payments. The CBDC payment module is also referred to as interaction module hereinafter. The interaction module conceptualizes blockchain middleware for Central banks and financial institutions to easily manage the core operations of CBDC with a payment module as an on-ramp to existing payment network. To perform the CBDC payments, the user may use their card such as debit card, credit card and the like which is linked to the CBDC wallet associated with the user. For example, card of the user may be provided by the financial institutions partnered with institutions such as Visa. The interaction module applies double spend protection to authorize payment and triggers CBDC payment processing using the existing infrastructure. Also, the CBDC infrastructure enables a two-tier CBDC system for Central banks to issue and distribute CBDC. The interaction module confirms and settles the CBDC transaction, after which the interaction

module converts CBDC to bank money. Finally, the transaction with the merchant is settled as per established standards and processes.

[0054] **FIG. 1** discloses a schematic diagram of a system for facilitating CBDC payments using an interaction module, in accordance with some embodiments of the present disclosure.

[0055] In **FIG. 1**, a schematic diagram of a system **100** shows a user **101**, an issuer bank (also referred to as authorizing entity) **103**, a merchant **105** (also referred to as resource provider hereinafter), an acquirer bank **107**, an interaction module **109**, blockchain network **111** and a central bank (also referred to as central entity) **113**. The interaction module **109** further comprises a bank or a financial institution sub-module **115**, a user wallet management sub-module **117**, a payment authorization module **119** and a payment settlement sub-module **121**.

[0056] Initially, the bank or financial institution sub-module **115** of the interaction module **109** performs an onboarding process of the authorization entity **103**. The onboarding process of the authorization entity **103** is performed by steps 1 – 6 of FIG. 1. An authorizing entity **103** (shown as Issuer Bank in FIG. 1) may communicate with the interaction module **109** to perform the onboarding process (e.g., via an issuer computer). The interaction module **109** may communicate with a central entity **113** (shown as Central Bank in FIG. 1) via a Blockchain Network **111** to complete the onboarding process.

[0057] In step 1, the authorizing entity **103** may communicate with the interaction module **109** to begin onboarding. After the onboarding is complete, the authorizing entity **103** may access payment processing, key custodians, etc., from the interaction module **109**.

[0058] In step 2, after receiving the onboarding request, the interaction module **109** may transmit a request to the Blockchain Network **111** to generate tenants for the authorizing entity **103**.

[0059] In step 3, after receiving the request to generate tenants, the Blockchain Network **111** may generate a wallet identifier and a private key, which will be assigned to the authorizing entity **103**. The Blockchain Network **111** may then transmit the wallet identifier and the private key to the bank or financial institution sub-module **115** of the interaction module **109**.

[0060] In step 4, after receiving the wallet identifier and the private key from the Blockchain Network **111**, the interaction module **109** may store the wallet identifier and the private key in a secure vault. In some embodiments, the interaction module **109** may communicate with a Custodian Computer that manages the private key for the authorizing entity **103**.

[0061] In step 5, after storing the wallet identifier and the private key, the interaction module **109** may notify the authorizing entity **103** that onboarding is complete. The interaction module **109** may manage an account for the authorizing entity **103** that is accessed using the wallet identifier and/or the private key. The interaction module **109** may update a local ledger which stores the amount of CBDC held by various accounts. For example, the local ledger may store information such as <wallet ID, card ID, customer ID, balance> for each account of each user associated with the authorizing entity **103**. The authorizing entity may then request to add an amount (e.g., an amount of CBDC) to the authorizing entity's account with the Blockchain Network **111**. For example, the authorizing entity **103** may provide an indication of an amount of CBDC to be added to their account.

[0062] In step 6, after receiving a request to add CBDC to the authorizing entity account, the interaction module **109** may communicate with the Blockchain Network **111** to obtain the requested CBDC amount. For example, the interaction module **109** may purchase the CBDC amount from the Central Bank **113** via the Blockchain Network **111**.

[0063] In step 7, after receiving a request to purchase the CBDC amount from the interaction module, the Central Bank may issue and burn the CBDC amount. The interaction module may then associate the CBDC amount with the authorizing entity account. The interaction module may update the local ledger to include the CBDC amount. The update to the local ledger may additionally comprise a timestamp, which indicates when the CBDC amount was added to the account.

[0064] The user wallet management sub-module **117** performs a user wallet onboarding process. The user wallet onboarding process is performed in steps 7 – 13 of FIG. 1. A user **101** operating a user device comprising a digital wallet application (shown as Banking App/Fintech App in FIG. 1) may communicate with the interaction module **109** to perform the onboarding process.

[0065] In step 7, the user **101** may use the digital wallet application to transmit a request to create a CBDC account to the interaction module **109** via the authorizing entity **103**.

[0066] In step 8, after receiving the request to create a CBDC account from the User **101**, the authorizing entity **103** may transmit a request to create a new wallet under the authorizing entity **103** to the interaction module **109**.

[0067] In step 9, after receiving the request to create a new wallet from the authorizing entity **103**, the interaction module **109** may request the Blockchain Network **111** to generate a wallet identifier and private key for the User account. The interaction module **109** may additionally generate a user entity within the authorizing entity account (e.g., the user's account will be associated with the authorizing entity). The Blockchain Network **111** may generate the wallet identifier and private key and transmit it back to the interaction module **109**.

[0068] In step 10, after receiving the User's wallet identifier and private key from the Blockchain Network **111**, the interaction module **109** may store the wallet identifier in a secure vault. In some embodiments, the interaction module **109** may communicate with a Custodian Computer that manages the user's account.

[0069] In step 11, after the user's account is established, the interaction module **109** may issue a CBDC card (e.g., a debit card) linked to the user's account. For example, the CBDC card may comprise a card identifier which is linked to the wallet identifier.

[0070] In step 12, after issuing the CBDC card, the interaction module may transmit the user's wallet identifier and the card details (e.g., the card identifier) to the authorizing entity. After that, the authorizing entity may transmit the user's wallet identifier and the card details to the digital wallet application. The authorizing entity may then respond to the interaction module by transmitting a user bank identifier, which the authorizing entity uses to uniquely identify the User.

[0071] In step 13, the interaction module **109** may store the mapping between the user's wallet identifier and the user bank identifier.

[0072] In some embodiments, the user wallet onboarding and user key management may be handled by the authorizing entity **103**.

[0073] In some embodiments, the payment authorization sub-module may perform an authorization process. The authorization process is completed by steps 14 – 22 of FIG. 1. The user **101** may wish to purchase goods and/or services from the resource provider **105** (shown as Merchant in FIG. 1). The resource provider **105** may be associated with an Acquirer Bank **107**, which can communicate with the interaction module **109** in order to authorize payments in CBDC.

[0074] In step 14, the User **101** may present the CBDC card to an access device operated by the resource provider **105** (e.g., a POS location). The CBDC card and the access device interact such that access data from the CBDC card (e.g., the card identifier, etc.) is received by the access device.

[0075] In step 15, after receiving access data, the resource provider **105** may transmit an authorization request message that includes the information received from the CBDC card along with additional transaction information (e.g., a transaction amount, merchant specific information, etc.) using a resource provider computer (not shown) or the access device and electronically transmits this information to a transport computer (not shown) operated by the Acquirer Bank **107**.

[0076] In step 16, after receiving the authorization request message from the resource provider **105**, the Acquirer Bank **107** may then receive, process, and forward the authorization request message to a processing network (shown as VisaNet in FIG. 1) for authorization.

[0077] In step 17, after receiving the authorization request message from the Acquirer Bank **107**, the processing network may identify that the card identifier in the authorization request message corresponds to a CBDC card. After identifying the CBDC card, the processing network may transmit the authorization request message to the interaction module **109** for authorization.

[0078] In step 18, the interaction module **109** may retrieve the user wallet identifier associated with the card identifier from the secure vault.

[0079] In step 19, after retrieving the user wallet identifier, the interaction module **109** may check the balance of the user's account. In some embodiments, if the Blockchain Network **111** allows for balance checking in real time, the interaction module **109** may communicate with the Blockchain Network **111** to check the balance of the user's account and determine if it is sufficient to complete the payment. This may be an example of determining if a first amount (e.g., the transaction amount) is less than or equal to a second amount (e.g., the balance of the user's account).

[0080] In step 20, the interaction module **109** may check the local ledger to determine if the balance of CBDC in the user's account (e.g., the account associated with at least the following <wallet ID, card ID, customer ID, balance>) is sufficient to complete the payment.

[0081] In step 21, after determining the user's balance is sufficient, the interaction module **109** may transmit an instruction message to the Blockchain Network **111** for completing a transfer of CBDC funds between the user's account identified by the wallet identifier and the authorizing entity's account **103**. The interaction module **109** may then wait for a notification from the Blockchain Network **111** that the transfer has been settled.

[0082] In step 22, after transmitting the instruction message to the Blockchain Network **111**, the interaction module **109** may transmit the transaction authorization status to the processing network and the authorizing entity **103**.

[0083] In some embodiments, the payment settlement sub-module **121** may perform a settlement process. The settlement process is completed by steps 23 – 26 of FIG. 1. The settlement process may move funds used to complete the payment described above from the issuing bank **103** to the acquiring bank **107**.

[0084] In step 23, after step 21, the interaction module **109** may receive notification that the transfer has been settled.

[0085] In step 24, after some time period (e.g., a day), the interaction module **109** may generate a settlement message for the authorizing entity **103**. The settlement message may comprise settlements to be performed for all CBDC transactions made during the time period. The interaction module **109** may then transmit the settlement message to the authorizing entity **103**.

[0086] In step 25, after receiving the settlement message from the interaction module **109**, the authorizing entity **103** may request that the interaction module **109** to burn (i.e., exchange) CBDC for USDC or USD (fiat currency) (e.g., burning a first type of amount for a second type of amount). In some embodiments, the authorizing entity **103** may request this for each time period (e.g., to obtain USDC or USD for the settlements to be processed). In other embodiments, the authorizing entity **103** may request only when the CBDC liquidity exceeds the USDC or USD backed limit.

[0087] In step 26, after the interaction module **109** burns CBDC to obtain INR for the authorizing entity **103**, the authorizing entity **103** may perform a normal fiat currency settlement between the authorizing entity **103**, and the acquirer bank **107** using INR from the liquidity pool.

[0088] FIG.2 discloses an architecture of Delegated Certificate Authority (CA) for wallet providers.

[0089] In **FIG. 2**, payment network such as Visa may act as the delegated certificate authority (CA) **203** that assess digital wallet partners **205a, 205b and 205c** and monitors the approved wallets on an ongoing basis. Also, the CA **203** supervises and manages CBDC network access on behalf of the central bank **201** using entirely the digital infrastructure available inside the CBDC environment.

[0090] FIG.3 discloses a process flow between the wallet providers and the central bank using the delegated CA.

[0091] In step 1: The central bank **309** is a Root Authority (RA) which may specify the one or more rules and policies of the CBDC environment. The central bank **309** may define the tiers of access to the CBDC network, define the standards and requirements for each tier, define the level of interaction with the CBDC network permitted under each tier, grant verifiable authority to its delegated CAs using cryptographic techniques and the like.

[0092] In step 2: A payment network such as Visa may act as a delegated certificate authority (CA) **307** on behalf of the central bank to provision access to the CBDC network. The CA may evaluate the digital wallet providers using the policy rules set out by the central bank **309**. Further the delegated CA **307** may provide approved digital wallets access to the CBDC network and assigns the corresponding tier.

[0093] In step 3: The delegated CA **307** may provide credentials of the network provider to all the approved digital wallets so that the CBDC can be spent at any merchant that accepts Visa and the CBDC directly.

[0094] In step 4: The digital wallet providers **301** may purchase and redeem CBDC from central bank **309** via a blockchain network **305** using delegated CA **307**.

[0095] In step 5: The central bank **309** issues and burns CBDC to retail bank as requested by the digital wallet providers **301**

[0096] In the present disclosure, the on-chain access to the wallets are restricted. Any wallet transactions outside the knowledge of the interaction module will result in out of sync balance between the off-chain and the on-chain ledger. The off-chain ledger that is the blockchain network protects against the double spend. The payment transaction authorization workflow blocks amount in the off-chain ledger before its reflected on-chain. Once the transaction is settled, the blocked amount is removed and equivalent amount is reduced from the off-chain ledger balance. Also, in the present disclosure the settlement for a CBDC transaction is transfer of assets from consumer wallet to an authorizing entity wallet and from the authorizing entity wallet assets are transferred to the merchant wallet.

[0097] Finally, the language used in the specification has been principally selected for readability and instructional purposes, and it may not have been selected to delineate or circumscribe the inventive subject matter. Accordingly, the disclosure of the embodiments of the disclosure is intended to be illustrative, but not limiting, of the scope of the disclosure.

[0098] With respect to the use of substantially any plural and/or singular terms herein, those having skill in the art can translate from the plural to the singular and/or from the singular to the plural as is appropriate to the context and/or application. The various singular/plural permutations may be expressly set forth herein for sake of clarity.

[0099] Although the invention has been described in detail for the purpose of illustration based on what is currently considered to be the most practical and preferred embodiments, it is to be understood that such detail is solely for that purpose and that the invention is not limited to the disclosed embodiments, but, on the contrary, is intended to cover modifications and equivalent arrangements that are within the spirit and scope of the appended claims. For example, it is to be understood that the present invention contemplates that, to the extent possible, one or more features of any embodiment can be combined with one or more features of any other embodiment.

DEVICE AND METHOD FOR ACCEPTING CENTRAL BANK DIGITAL CURRENCY(CBDC) IN PAYMENT NETWORKS

ABSTRACT

The present disclosure relates to a device and method for accepting CBDC in payment networks. Initially an authorizing entity communicates with an interaction module to complete onboarding process. Further, the user also communicates with interaction module via the authorizing entity to perform the onboarding process. The interaction module transmits the onboard request to the blockchain network. Further the blockchain network provides a wallet identifier and the private key for the authorizing entity and the user. The interaction module stores the wallet identifier and the private key of the authoring entity and the user in a secure vault. Upon the onboarding, the interaction module performs an authorization process when the user performs a transaction with the resource provider. Finally, the interaction module performs a settlement process, where the authorizing entity settles the transaction amount from the CBDC to fiat currency to the resource provider.

FIG. 1

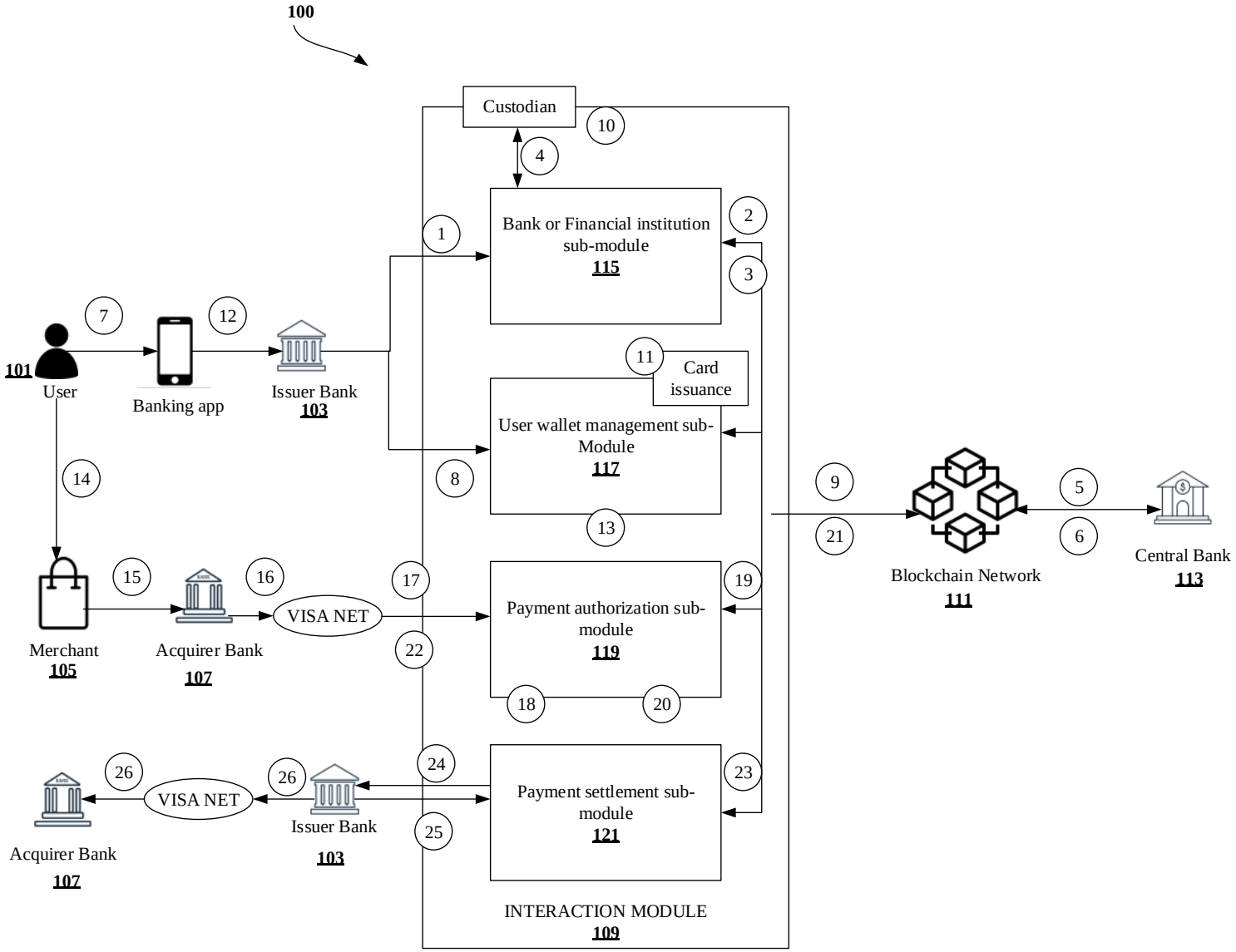
100
Custodian
10
4
Bank or Financial institution sub-module
115
2
3
1
7
12
101
User
Banking app
Issuer Bank
103
11
Card issuance
User wallet management sub-Module
117
13
8
14
9
21
Blockchain Network
111
5
6
Central Bank
113
15
16
17
19
Merchant
105
Acquirer Bank
107
VISA NET
Payment authorization sub-module
119
22
18
20
24
26
26
23
Payment settlement sub-module
121
VISA NET
Issuer Bank
103
Acquirer Bank
107
25
INTERACTION MODULE
109

FIG.1

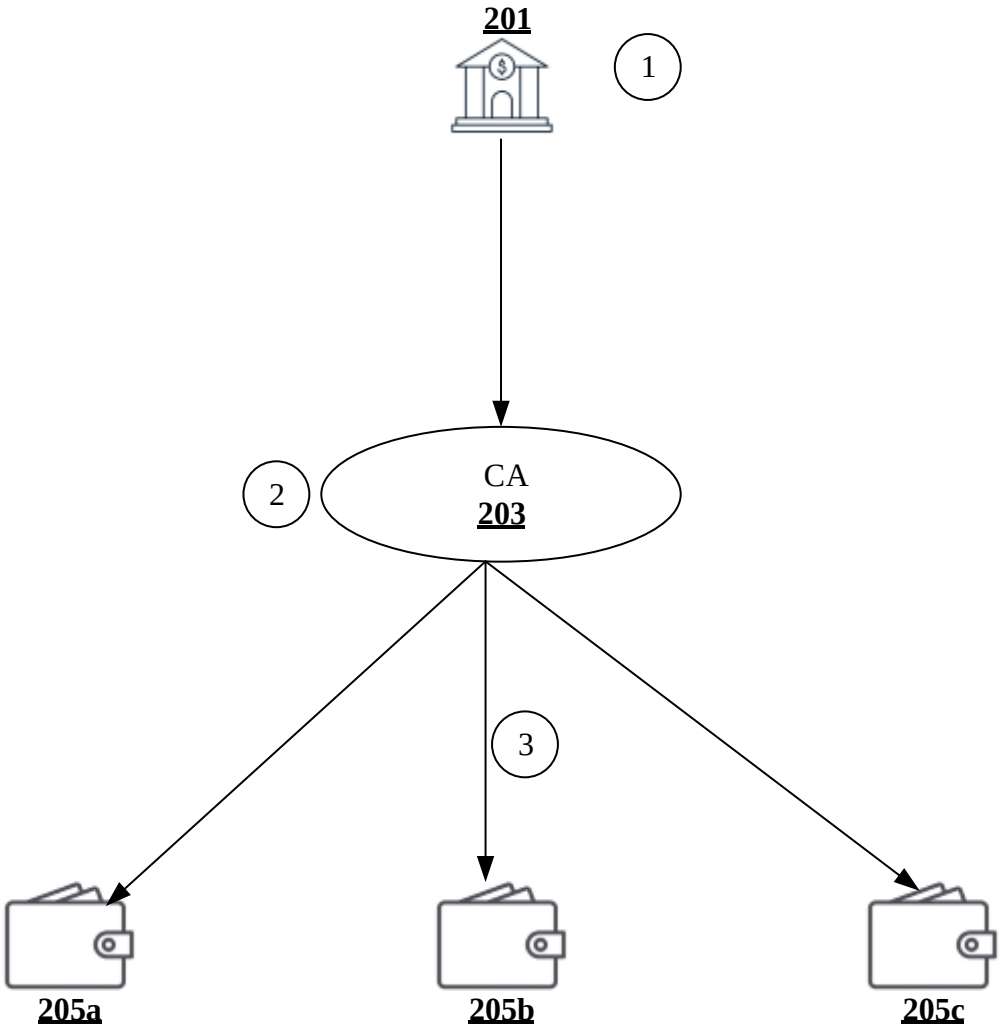

FIG. 2

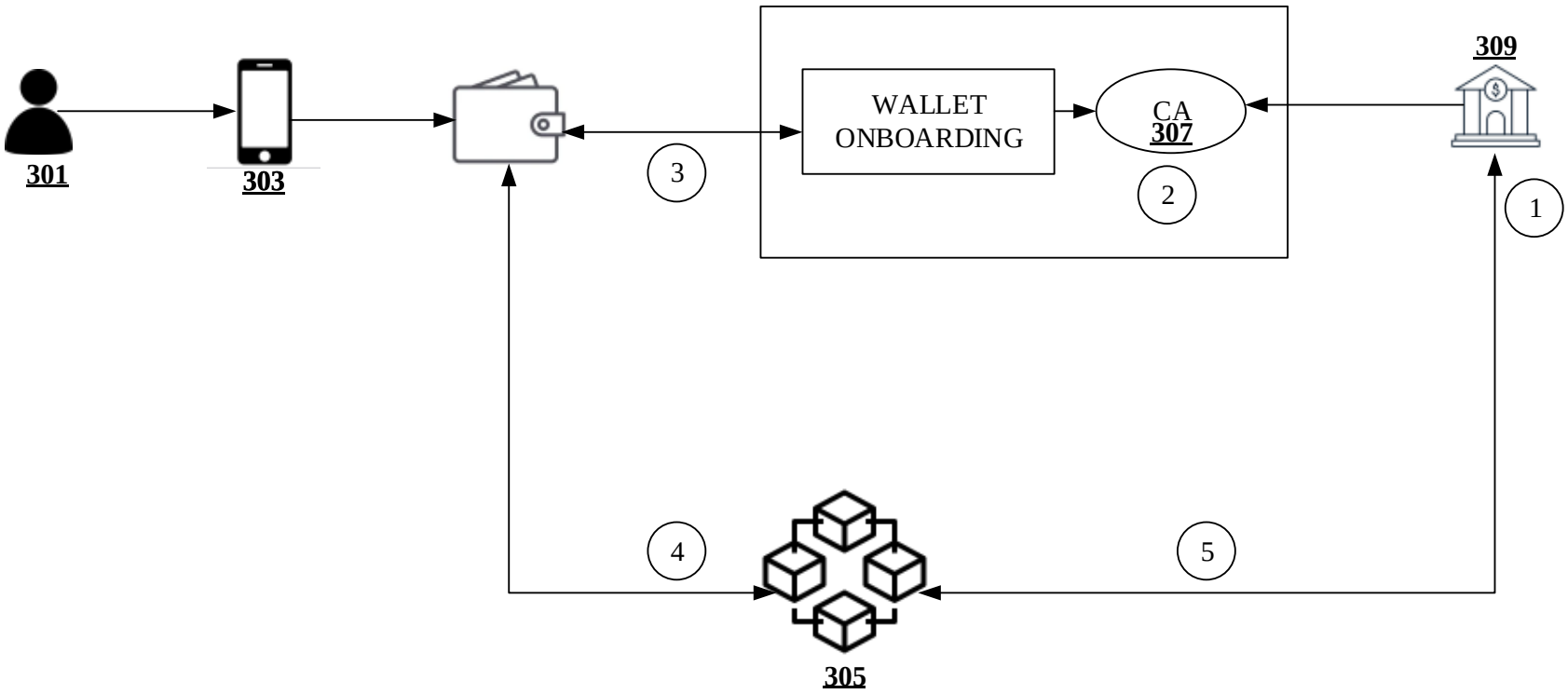

FIG. 3

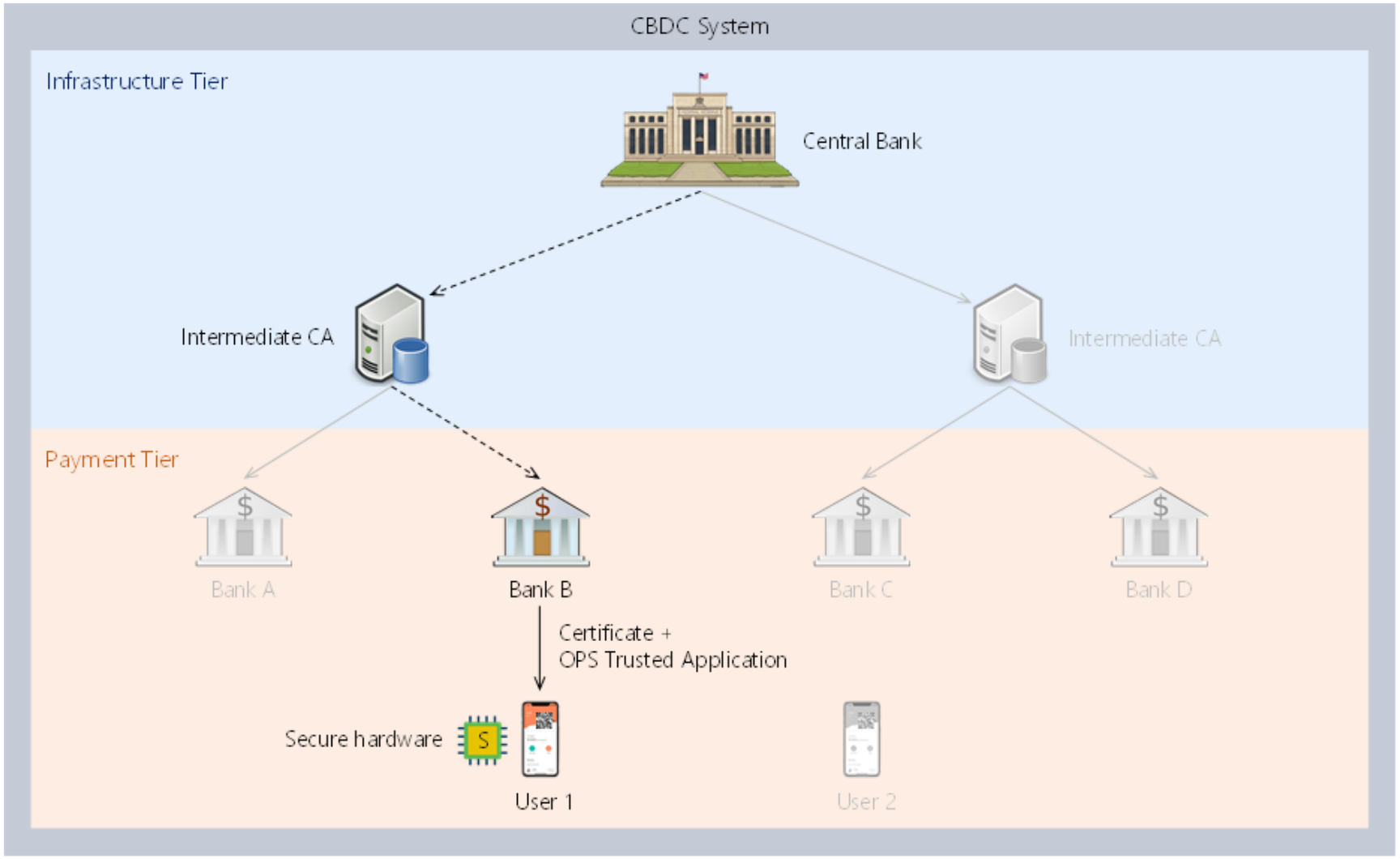
CBDC System
Infrastructure Tier
Central Bank
Intermediate CA
Intermediate CA
Payment Tier
Bank A
Bank B
Bank C
Bank D
Certificate +
OPS Trusted Application
Secure hardware
User 1
User 2

FIG. 4

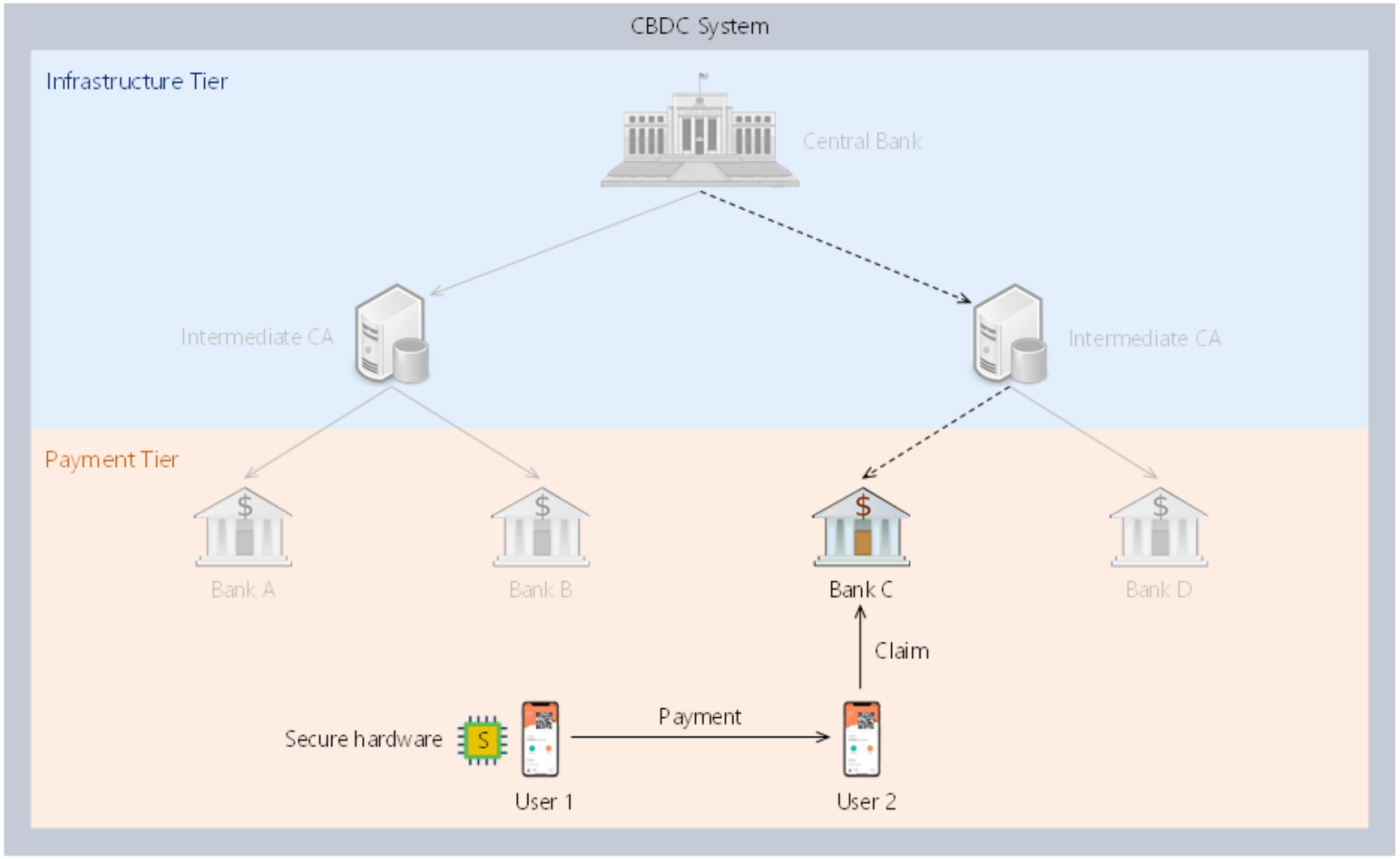
CBDC System
Infrastructure Tier
Central Bank
Intermediate CA
Intermediate CA
Payment Tier
Bank A
Bank B
Bank C
Bank D
Claim
Secure hardware
S
Payment
User 1
User 2

FIG. 5

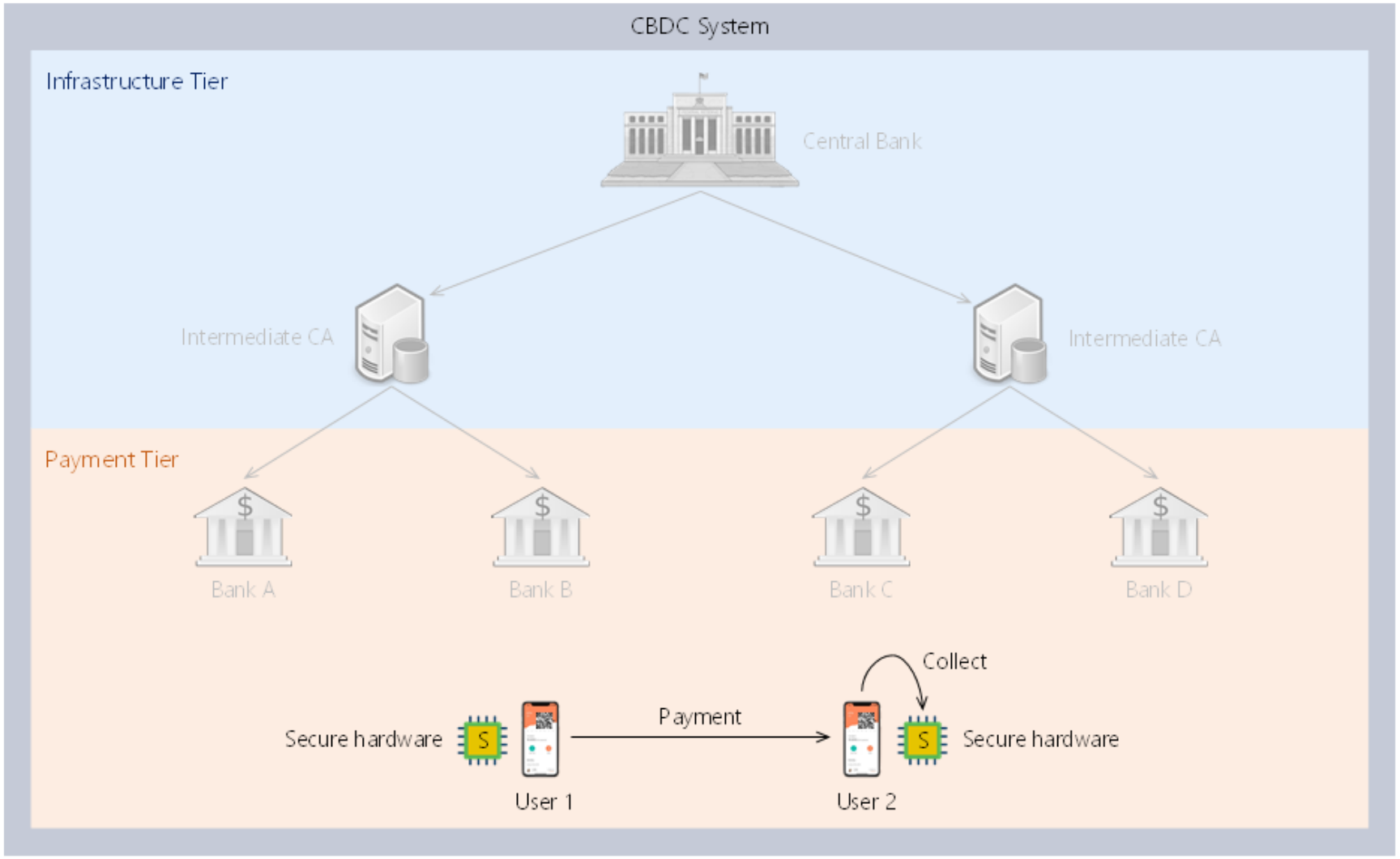
CBDC System
Infrastructure Tier
Central Bank
Intermediate CA
Intermediate CA
Payment Tier
Bank A
Bank B
Bank C
Bank D
Collect
Secure hardware
Payment
Secure hardware
User 1
User 2

FIG.6

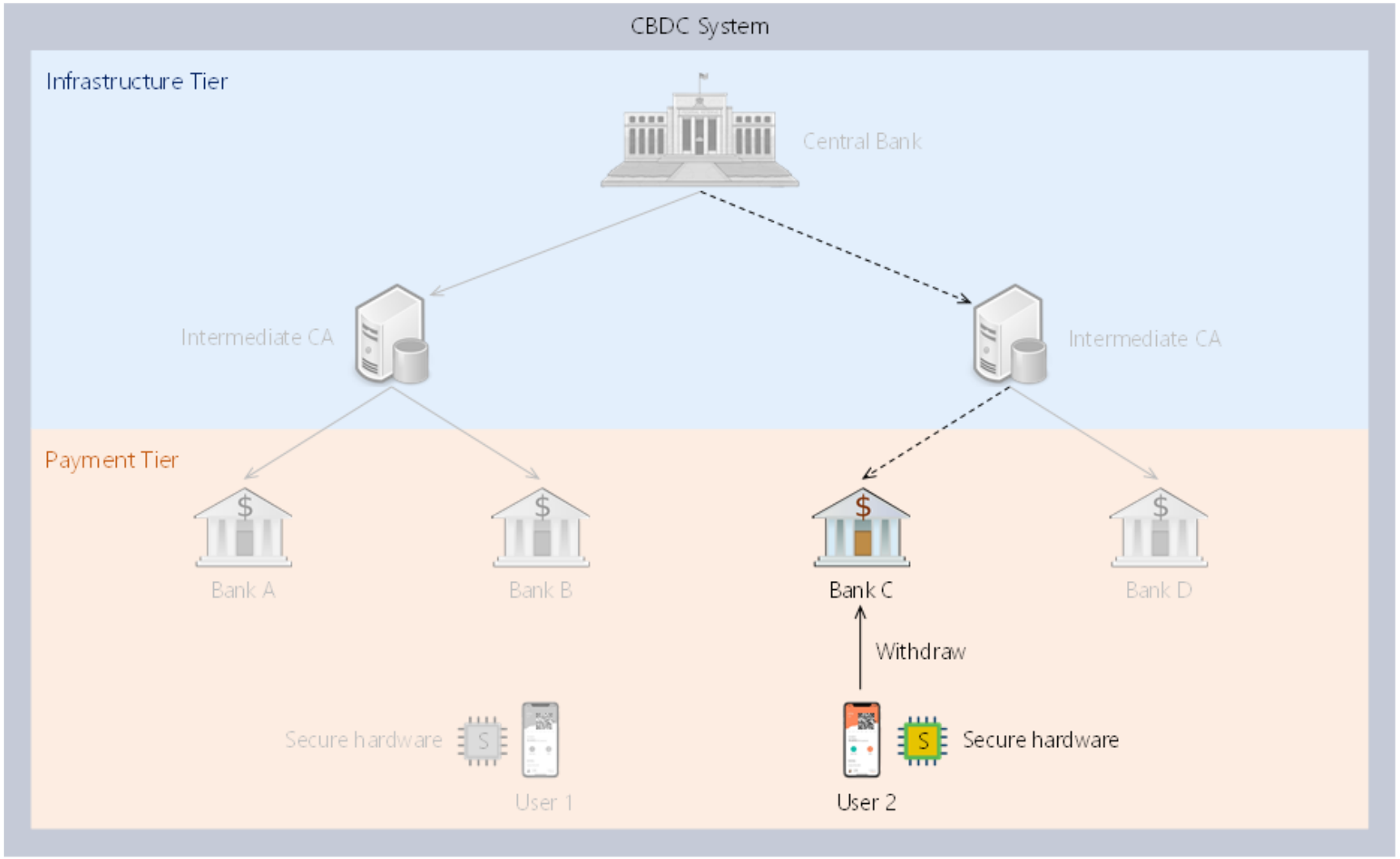
CBDC System
Infrastructure Tier
Central Bank
Intermediate CA
Intermediate CA
Payment Tier
Bank A
Bank B
Bank C
Bank D
Withdraw
Secure hardware
User 1
Secure hardware
User 2

FIG. 7