

SYSTEMS, METHODS, AND DEVICES FOR CONDUCTING FIAT CURRENCY AND CRYPTOCURRENCY TRANSACTIONS

CROSS-REFERENCE TO RELATED APPLICATION

5

This application claims priority to United States Provisional Application No. 63/592,369, filed October 23, 2023, the contents of which are incorporated herein by reference in their entirety for all purposes.

BACKGROUND OF THE INVENTION

10

Payment cards (e.g. credit card, debit card, points card, etc.) are widely used to facilitate payments. For example, a consumer may make a payment using their payment card to purchase a product or service from a merchant. The customer can present their payment card at a point of sale (POS) terminal (e.g. the card is inserted or swiped through the POS terminal, required card information may be entered manually, or the POS terminal – which may include a mobile device operating with POS functionality, e.g. on Android or iOS -- accepts contactless transactions). Upon receipt of the requisite card information, the POS terminal transmits the same to the acquirer for approval of the transaction, along with other relevant information, such as merchant information and transaction information (e.g. amount and currency). The acquirer then communicates with the issuer (e.g. entity that issued the card to the consumer) for approval to authorize the transaction.

However, new payment or transaction systems have been introduced and have recently gained popularity. In one example, cryptocurrency is implemented across a network of computing devices that maintains a digital ledger in the form of a blockchain, directed acyclic graph, or hashgraph. Specifically, transactions using cryptocurrency may occur between a cryptocurrency wallet of a sender and a cryptocurrency wallet of a receiver; these cryptocurrency wallets may store private and public keys. In the field of cryptocurrency (such as Bitcoin, etc.), a private key (the unique, typically alphanumeric, code that allows the currency to be spent) is required to sign the transaction cryptocurrency for spending purposes. A public key, or hash of the public key, essentially identifies a destination for the currency. A transaction in cryptocurrency typically requires the sender and receiver to share their addresses that are the derivations of public keys with each other to complete the transaction, with the associated blockchain used to certify validity of the transaction and to confirm that the sender has the funds. For other types of authentication (e.g. FIDO or PGP), the sender and receiver share their actual public keys (or raw pubkeys in selected blockchains). Once the payment has been delivered to the address, the receiver needs the private

key to access the funds. An exemplary illustration of a derivation process from private key to public key to address can be found at <https://iancoleman.io/bip39/> & <https://learnmeabitcoin.com/technical/>, incorporated herein by reference.

Additionally, in the field of cryptocurrency, smart contracts are machine-readable instructions stored in a computer memory (i.e. written in code on a blockchain and stored on each server that constitutes a node in the p2p network) configured for causing a processor associated with the smart contract to execute actions when predetermined conditions have been met and verified. In so doing, certain actions, such as initiating a transfer of funds with appropriate parties to verify that the transfer took place, releasing funds to appropriate parties, and assigning to another party the right to transfer funds, are automated.

These new transaction systems typically require servers or systems for managing the transaction processes and databases, which are different from existing transaction systems. Thus, improvements are desired in providing transaction systems capable of accepting and/or facilitating multiple payment methods, such as fiat currencies (e.g. US dollars, Euro, etc.), and non-fiat currencies, such as cryptocurrencies (bitcoin, ether, etc.), to satisfy a transaction between two parties (e.g. a customer and a merchant).

SUMMARY OF THE INVENTION

One aspect of the invention relates to a transaction system configured for conducting a cryptocurrency transaction. The transaction system has a hardware storage device having an integrated circuit comprising at least one secure element. The secure element has a secure element processor, a secure element digital memory module comprising a cryptographic module, and at least one secure element near field communications (NFC) or contact interface. The secure element digital memory module embodies instructions readable by the secure element processor for causing the secure element to generate and store a private key in encrypted state in the digital memory, generate a public key using the private key, and to perform a signature operation. The transaction system includes a cryptocurrency transaction processing device having a user interface embodying a virtual wallet having a first cryptocurrency address associated therewith, a processing device NFC or contact interface, and a communication interface configured for connection to an exchange server of a cryptocurrency transaction network on a global communications network and for sending signed transaction information to the exchange server to initiate a cryptocurrency transaction. The transaction system also includes a fiat currency

transaction system for processing a fiat currency transaction. The fiat currency transaction system includes an application process interface (API) configured for processing the fiat currency transaction in accordance with a smart contract comprising machine-readable instructions stored in a computer memory accessible by the fiat
5 currency transaction system for causing a processor associated with the smart contract to interface with the cryptocurrency processing device to process a cryptocurrency transaction sufficient to convert a suitable amount of cryptocurrency associated with the virtual wallet into fiat currency for satisfying the fiat currency transaction.

Another aspect of the invention relates to a transaction system
10 configured for conducting a plurality of transactions. The transaction system includes a transaction card including a hardware storage device. The hardware storage device has an integrated circuit comprising at least one secure element, the secure element having a secure element processor, a secure element digital memory module comprising a cryptographic module, and at least one secure element NFC or contact interface. The
15 secure element digital memory module embodies instructions readable by the secure element processor for causing the secure element to store a private key in an encrypted state in the digital memory, generate a public key using the private key, and perform a signature operation. The transaction system also includes a cryptocurrency transaction processing device having a user interface embodying a virtual wallet, a
20 processing device NFC or contact interface, and a communication interface configured for connecting to an exchange server of a cryptocurrency transaction network on a global communications network and for sending signed transaction information to the exchange server to initiate a cryptocurrency transaction. The transaction system also has a fiat currency transaction system for processing a transaction using fiat currency
25 via a custodial account associated with the transaction card.

In some embodiments, the hardware storage device is configured to: (a) conduct cryptocurrency transactions by establishing a connection between the hardware storage device and the cryptocurrency transaction processing device using the secure element NFC or contact interface in communication with the processing
30 device NFC or contact interface, receiving information from the processing device, retrieving the private key from the digital memory, performing signature operations using the private key, checking a chain associated with the public key to confirm that the signature conforms to a public key signature that could only have been generated using the private key, signing the transaction, and sending signed transaction
35 information to the cryptocurrency transaction processing device; and (b) conduct fiat transactions by establishing a connection over NFC or via a contact interaction with a

card reader of the fiat currency transaction system, and authorizing a transaction processed using funds stored in the custodial account.

In some embodiments, performing step (a) converts an amount of cryptocurrency associated with the virtual wallet into fiat currency loaded into the custodial account prior to performing step (b). In still other embodiments, performing step (b) moves an amount of cryptocurrency associated with the transaction from a self-custody account of a card user to the custodial account, and step (b) includes a custodian of the custodial account converting an appropriate amount of the cryptocurrency to fiat currency and transmitting the converted fiat currency to a requesting recipient to complete the fiat currency transaction.

Another aspect of the invention relates to a hardware storage device having an integrated circuit comprising at least one secure element, the secure element having a secure element processor, a secure element digital memory module comprising a cryptographic module, and at least one secure element NFC or contact interface, the secure element digital memory module embodying instructions readable by the secure element processor for causing the secure element to store a private key in encrypted state in the digital memory, generate a public key using the private key, and to perform a signature operation.

In some embodiments, the secure element digital memory module embody instructions readable by the secure element processor for causing the secure element to, in response to receipt of information from a cryptocurrency transaction processing device linked via a connection with the at least one secure element via the NFC or contact interface, perform the steps of: (a) retrieving the private key from the digital memory, define a signature using the private key, checking a chain associated with the public key to confirm that the signature conforms to a public key signature that could only have been generated using the private key, signing the transaction, and sending signed transaction information to the cryptocurrency transaction processing device; and step (b) conducting fiat transactions by establishing a connection over NFC or via a contact interaction with a card reader of a fiat currency transaction system including an API and authorizing the cryptocurrency transaction processed via the API in accordance with a smart contract comprising machine-readable instructions stored in a computer memory accessible by the fiat currency transaction system for causing a processor associated with the smart contract to interface with the cryptocurrency processing device to process a cryptocurrency transaction sufficient to convert a suitable amount of cryptocurrency associated with the virtual wallet into fiat currency for satisfying the fiat currency transaction.

In other embodiments, step (a) includes causing the at least one secure element to perform a signature operation associated with assigning to an assignee having a second cryptocurrency address associated therewith a right to transfer a designated amount of cryptocurrency in accordance with the smart contract, and step
5 (b) includes the API approving the fiat transaction upon confirmation of sufficient funds allocated under the execution of the smart contract to complete the fiat transaction, and the assignee upon receipt of approval from the API, optionally converting the funds corresponding to the fiat transaction from cryptocurrency to fiat currency, and transmitting the appropriate amount of funds (e.g. of the converted fiat currency or of
10 unconverted cryptocurrency) to a requesting recipient to complete the fiat currency transaction.

Yet another aspect of the invention relates to a transaction card including a hardware storage device having an integrated circuit comprising at least one secure element, the at least one secure element having a secure element processor, a secure
15 element digital memory module comprising a cryptographic module, and at least one secure element near field communications (NFC) or contact interface, the secure element digital memory module embodying instructions readable by the secure element processor for causing the secure element to store a private key in an encrypted state in the digital memory, generate a public key using the private key, and perform a
20 signature operation.

In some embodiments, the secure element digital memory module embodies instructions readable by the secure element processor for causing the secure element to, in response to receipt of information from a cryptocurrency transaction processing device linked via a connection with the at least one secure element via the
25 NFC or contact interface, perform the steps of: (a) retrieving the private key from the digital memory, performing signature operations using the private key, checking a chain associated with the public key to confirm that the signature conforms to a public key signature that could only have been generated using the private key, signing the transaction, and sending signed transaction information to the cryptocurrency
30 transaction processing device; and step (b) conducting fiat transactions by establishing a connection over NFC or via a contact interaction with a card reader of the fiat currency transaction system, and authorizing a transaction processed using funds stored in a custodial account associated with the transaction card.

In still other embodiments, performing step (a) converts an amount of
35 cryptocurrency associated with the virtual wallet into fiat currency loaded into the custodial account prior to performing step (b). In some embodiments, performing step

(b) moves an amount of cryptocurrency associated with the transaction from a self-custody account of a card user to the custodial account, and step (b) includes a custodian of the custodial account converting an appropriate amount of the cryptocurrency to fiat currency and transmitting the converted fiat currency to a requesting recipient to complete the fiat currency transaction.

Yet another aspect includes a transaction system configured for conducting a cryptocurrency transaction, the transaction system comprising a cryptocurrency transaction processing system configured for sending instructions to an exchange server of a cryptocurrency transaction network to initiate a cryptocurrency transaction; and a fiat currency transaction system for processing a fiat currency transaction. The fiat currency transaction system includes an application process interface (API) configured for processing the fiat currency transaction in accordance with a smart contract comprising machine-readable instructions stored in a computer memory accessible by the cryptocurrency transaction network for causing an issuer associated with the smart contract to process a cryptocurrency transaction sufficient to satisfy the fiat currency transaction. In embodiments, the cryptocurrency transaction processing system further comprises a cryptocurrency transaction processing device having a user interface embodying a virtual wallet having a first cryptocurrency address associated therewith, a processing device NFC or contact interface, and a communication interface configured for connection to the exchange server of the cryptocurrency transaction network via a global communications network and for sending signed transaction information to the exchange server to initiate the cryptocurrency transaction. Embodiments further include a hardware storage device configured to perform a signature operation and to transmit the signed transaction information to the virtual wallet via a communication protocol other than via the global communications network.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 depicts an exemplary system for conducting a cryptocurrency transaction in accordance with aspects of the invention.

FIG. 2 is a flowchart depicting exemplary process steps in accordance with aspects of the invention.

FIG. 3 is a flowchart depicting additional steps of FIG. 2 for a method associated with a smart contract.

FIG. 4 is a flowchart depicting exemplary process steps in accordance with a method for conducting a cryptocurrency transaction in accordance with aspects of the invention associated with a custodial account.

Fig. 5A depicts elements of an exemplary user interface or portion thereof associated with an aspect of the invention.

Fig. 5B depicts elements of another exemplary user interface or portion thereof associated with an aspect of the invention.

FIG. 6 depicts an exemplary generalized flow diagram depicting an exemplary Decentralized Finance (DeFi) payment solution in accordance with aspects of the invention.

DETAILED DESCRIPTION OF THE INVENTION

An exemplary transaction system 100 for conducting cryptocurrency transactions in accordance with aspects of the invention is depicted in FIG. 1. In general, the transaction system 100 includes a hardware storage device 110, a cryptocurrency transaction processing device 120, and a fiat currency transaction system.

In an exemplary embodiment, the hardware storage device 110 is in the form of a transaction card (as depicted in FIG. 1), such as a luxury card comprising metal, ceramic, glass, or a combination thereof, having standard dimensions of a transaction card in conformance with ISO / IEC 7810:2003 ID-1, namely a length and width of 85.6 x 53.98 mm (3.4 x 2.1 inches) and a thickness of 0.76 millimeters ($\frac{1}{32}$ in). Like a standard debit card or credit card, the card 110 may have a magnetic stripe (and/or printed barcode) and physical contacts associated with transaction cards configured for interacting with a card reader or a POS terminal. In these embodiments, hardware storage device 110 is configured to conduct routine credit card or debit card transactions, and may be thus configured with all of the typical trappings of a payment card, such as a credit card, including a payment module 10, magnetic stripe (not shown but well understood in the art), and the like. In some embodiments, user-identifying information, such as a card number, a user name (not shown but well understood in the art), user photo (not shown but well understood in the art), and user signature block (not shown but well understood in the art), (e.g. comprising a fingerprint or thumbprint reader for controlling access to the hardware storage device) may be included. In some embodiments, there may be advantages to configuring the card 110 or other form factor (fob, etc.) for payment plus authentication (e.g. using

FIDO). It should be understood that in some embodiments, the card 110 / other form factor may feature any combination of crypto, FIDO, access control/loyalty, and/or payment, depending on the combination of software.

Although depicted as a transaction-card-sized device, which offers the advantage of neatly fitting in a holder's physical wallet alongside standard transaction cards, the invention is not limited to any particular size or shape. Any form factor configured for NFC or contact communications with a mobile device, as described herein, may be suitable. For example, the hardware storage device 110 may comprise a key fob, a coin, or any type of physical token. Although a construction of metal, ceramic, glass, or a combination thereof, is preferred for durability, the materials of construction are not limited.

The hardware storage device 110 has an integrated circuit (e.g. residing within module 10) comprising at least one secure element 112. The at least one secure element 112 includes a secure element processor 114, a secure element digital memory module 116 comprising a cryptographic module, and at least one secure element near field communications (NFC) or contact interface 118. The secure element 112 digital memory 116 includes a cryptographic module embodying instructions readable by the at least one secure element processor 114 for causing the secure element 112 to store a private key in encrypted state in the digital memory 116, generate a public key using the private key, and to perform a signature operation.

In NFC interface embodiments, NFC interface 118 may include one or more antennas, including in some embodiments (including embodiments in which the card comprises plastic, metal, ceramic, wood, or any other material of construction) a first antenna integrated within an integrated circuit (IC) chip that contains the secure element, and a second (booster) antenna comprising a layer of the card. In some embodiments, a metal layer of the card itself may be configured as the antenna. Configurations of metal cards with operable NFC interfaces are described, for example but not limited thereto, in U.S. Patent No. 10,318,859, titled DUAL INTERFACE METAL SMART CARD WITH BOOSTER ANTENNA, and U.S. Patent No. 10,762,412, titled DI CAPACITIVE EMBEDDED METAL CARD, both of which are incorporated herein by reference. Although described in the foregoing in the context of payment modules comprising secure elements for communicating with card readers, the NFC interfaces as described therein are comparable to those used between the cards and processing devices discussed herein. Likewise, although not disclosed in detail herein, contact chip interfaces for credit / debit cards are well known, and such designs may be used in embodiments of the invention as described herein instead of or in addition to NFC

interfaces. It should be understood that although embodiments may be described or depicted with only one or the other of an NFC or contact interface, the other or both types of interfaces may instead or also be present.

In an exemplary embodiment, the transaction system 100 includes the
5 cryptocurrency transaction processing device 120, such as a mobile device, a smart phone, a tablet, a desktop NFC or contact reader, or other type of computer (e.g. an IoT-enabled object that utilizes local or edge computing, such as the on-board computer of a vehicle), also known hereinafter as Processing Device (PD). In some
10 embodiments, the PD may comprise a wallet on a desktop computer with an NFC or contact card reader, wherein the card acts as key storage. The cryptocurrency transaction processing device 120 includes a user interface 126, which embodies a virtual wallet 129 having a first cryptocurrency address associate therewith. The
15 cryptocurrency transaction processing device 120 has a processing device NFC or contact interface 124 and a communication interface 128 configured for connection to an exchange server of a cryptocurrency transaction network on a global
communications network 130. Additionally, or optionally, communication interface 128 is configured for sending signed transaction information to the exchange server to
20 initiate a cryptocurrency transaction. Notably, although NFC is a preferred wireless communication protocol, the invention is not limited only to the use of NFC, and other (preferably secure) wireless protocols (e.g. Bluetooth®, UWB, and the like) may be
used for communication of signals between the card and the PD. Likewise, although
chips with physical contacts for use in credit cards, and associated readers configured to connect manually (or wirelessly) to a mobile device, are well known, the invention is
not limited to any particular contact protocol, and any combination of contact readers
25 and (e.g. serial) adapters for transmitting a signal read from a card using any type of technology to the mobile device may be used.

In some embodiments, the cryptocurrency transaction processing device
120 has a digital memory 122 programmed with instructions readable by processing
30 device NFC or contact interface 124 for causing the cryptocurrency transaction processing device 120 to establish a secure connection with the secure element NFC or contact interface 118 using the NFC or contact communication interface 128 on the
cryptocurrency transaction processing device 120, and to send information to the
secure element 112 for processing by the secure element 112. The cryptocurrency or
virtual wallet 129 is operable for accessing a cryptocurrency network 150 via the global
35 communications network 130. Access to the cryptocurrency network may be direct or indirect (i.e. the virtual wallet 129 may directly interact with a second layer

cryptocurrency network, such via the Lightning Network or via Decentralized Finance (DeFi) protocols (e.g. Compound or Uniswap) over their respective chains, as non-limiting examples.

The instructions readable by the hardware storage device processor 114 and the mobile device processor 124, when read by the respective processors from the memory connected thereto, are capable of causing the system 100 to perform step (a) to process a cryptocurrency transaction and step (b) to process a fiat transaction. In embodiments, the virtual wallet is essentially a self-custody wallet. In a typical process 200, summarized in the flowchart depicted in FIG. 2, step (a) includes a cryptocurrency transaction initiated by a user via the hardware storage device 110 and user interface 126 of the cryptocurrency transaction processing device (e.g. mobile device 120). In step 210, a connection is established between the hardware storage device (e.g. transaction card 110) and the cryptocurrency transaction processing device (e.g. mobile device 120) using the secure element NFC or contact interface 118 in communication with the processing device NFC interface 128. The connection comprises a communications link, such as a secure communications link (e.g. encrypted), between the secure element (SE) 112 and the processing device 120. Using this connection, in step 220, the processing device 120 sends high-level information to the secure element 112 for processing in communication 132, and in step 230, the secure element processor 114, retrieves the private key from digital memory 116, define a signature using the private key, decrypts the private key using the public key stored in memory 116 (i.e. checks the chain associated with public key to confirm that the signature conforms to the public key signature that could only have been generated using the specific private key), signs the transaction, and sends signed transaction information back to the mobile device 120, such as via an NFC or contact communication 136. This communication may or may not be encrypted. The mobile device 120 then establishes a communication session over the global communications network 130 with a cryptocurrency exchange server 152 of the cryptocurrency network 150 and sends the signed transaction information to the cryptocurrency exchange, which initiates a transaction operative to send the currency value or token to the exchange server.

In an exemplary embodiment, the transaction system 100 performs step (b) to process a fiat transaction. To achieve this, the transaction system 100 includes the fiat currency transaction system for processing a fiat currency transaction. The fiat currency transaction system includes a payment terminal (e.g. card reader) 140 and an application process interface (API) 142 configured for processing the fiat currency

transaction (e.g. in accordance with a smart contract, an example of which is described below and depicted in connection with FIG. 5). As described above, the smart contract includes machine-readable instructions stored in a computer memory accessible by the fiat currency transaction system for causing a processor associated with the smart

5 contract to interface with the cryptocurrency processing device 120. In one non-limiting example, the smart contract includes instructions for causing the processor associated with the smart contract to process a cryptocurrency transaction sufficient to convert a suitable amount of cryptocurrency associated with the virtual wallet 129 into fiat currency for satisfying the fiat currency transaction. In another non-limiting example,

10 the smart contract includes instructions for causing the processor associated with the smart contract to process a cryptocurrency transaction sufficient to move a suitable amount of cryptocurrency associated with the virtual wallet 129 into a custodial account or a recipient account for satisfying the fiat currency transaction, without conversion of the cryptocurrency to fiat currency.

15 In step 250, a fiat transaction is initiated by a user via the hardware storage device 110 and the card reader 140 of the fiat currency transaction system. For example, a connection is established over NFC or via a contact interaction between the card 110 and the card reader 140. In an exemplary embodiment, the connection prompts a standard credit or debit card transaction that is communicated to the

20 transaction processing network for authorization and satisfaction of the transaction. Typically asynchronously, prior to conducting the fiat transaction, or attendant to a step performed immediately prior to and in the same workflow as the fiat transaction, a cryptocurrency transaction is processed via the API (e.g. as authorized by mobile device 120) in accordance with the governing terms of the smart contract to ensure

25 that the funds are available for the fiat transaction. Conversion from crypto to fiat is optionally performed (for recipients who require payment in fiat currency) by a conversion operation by a third party provider in the value chain. The fiat transaction itself is indistinguishable from a routine fiat credit card transaction. To facilitate this fiat transaction, secure element 112 comprises a payment module 10 configured to

30 exchange payment information with a card reader for conducting a purchase transaction. The payment module 10 is connected to the portion of the secure element configured for processing cryptocurrency transactions, such that the cold storage device 110 establishes the connection with the mobile device 120, and therefore prompt the initiation of the transaction, and the remaining portions of the transaction

35 may occur as described above.

In some embodiments, as shown in the flow chart of FIG. 3 showing substeps of steps 240 and 250, step 240a of conducting a cryptocurrency transaction comprises the hardware storage device 110 assigning to an assignee a right to transfer a designated amount of cryptocurrency associated with the first hardware storage 110 device as a proxy. Additionally, step 250a comprises the API 142 approving the fiat transaction upon confirmation of sufficient funds allocated under the proxy assignment to complete the fiat transaction. Optionally, step 250b includes the assignee, upon receipt of approval from the API 142, converting the funds corresponding to the fiat transaction from cryptocurrency to fiat currency and transmitting the appropriate amount of the converted fiat currency to a requesting recipient (e.g. a merchant) to complete the fiat currency transaction. In some embodiments, however, the entire payment may be made in crypto, in which case 250b includes the assignee, upon receipt of approval from the API 142, transmitting the appropriate amount of the crypto to the requesting recipient to complete the transaction.

System 100 may be further configured to receive a cryptocurrency deposit. A method for facilitating such a deposit may include the mobile device 120 displaying on display 125 a cryptocurrency address associated with the cryptocurrency wallet 129 in an encoded form for providing to a payor. For example, the address may be in the form of a bar code or QR code that the payor can capture with the payor's mobile device 120. The system may also read an address from an NFC or other wireless signal, or a contact-communicated signal. The system may further be configured to conduct any type of cryptocurrency transaction, such as purchasing cryptocurrency (i.e. using fiat currency) or swapping cryptocurrencies (i.e. trading an amount of one cryptocurrency for an equivalent amount of another cryptocurrency).

Another embodiment of system 100, such as system 300, is disclosed. System 300 is similar to system 100. For example, the transaction system 300 is configured for conducting a plurality of transactions, and generally includes a transaction card, a cryptocurrency transaction processing device, and a fiat currency transaction system, the details of each of which generally correspond to those of hardware storage device 110, cryptocurrency transaction processing device 120, and the fiat currency transaction system of system 100, respectively.

However, system 300 is different from system 100 in some respects. For example, the fiat currency transaction system of system 300 is configured to process a transaction using fiat currency via a custodial account associated with the transaction card 110. As is known in the art, a "custodial account" is typically associated with a centralized exchange (e.g. Coinbase®) or financial institution platform (e.g. PayPal®).

The transaction card 110 comprises a hardware storage device configured to perform step (a) of conducting cryptocurrency transaction and step (b) of conducting fiat transactions. As with system 100, the instructions readable by the hardware storage device processor 114 and the mobile device processor 124, when read by the
5 respective processors from the memory connected thereto, are capable of causing the system 100 to perform a plurality of transactions, including step (a) to process a cryptocurrency transaction and step (b) to process a fiat transaction. In a typical process 300, summarized in the flowcharts depicted in FIG. 4, steps (a) and (b) of system 300 are generally similar to those of system 100, respectively, but they differ in
10 some respects.

For example, step 350 or step (b) is different at least in that the hardware storage device conducts fiat transactions by authorizing a transaction processed using funds stored in the custodial account. In some embodiments, step 340 or step (a) converts an amount of cryptocurrency associated with the virtual wallet 129
15 into fiat currency loaded into the custodial account prior to performing step 350. The custodial account, for example, may be an account associated with a known credit card provider (e.g. VISA, AMERICAN EXPRESS, MASTERCARD, etc.) or a bank issuer of the card. Additionally, or optionally, in step 350, the hardware storage device moves an amount of cryptocurrency associated with the transaction from a self-custody account
20 of a card user to the custodial account, and a custodian of the custodial account converts an appropriate amount of the cryptocurrency to fiat currency and transmits the converted fiat currency to a requesting recipient (e.g. a merchant or merchant processor) to complete the fiat currency transaction. In the example discussed with respect to FIG. 3, step 250b, the custodial account holds the funds in cryptocurrency
25 and does not exchange the funds to fiat currency until the request for the transaction is made, but the crypto changes hands from user self-custody to the custodial account prior to any fiat transaction being specified. In embodiments, the software that implements the process may include functionality that provides "pop-up" windows or other notifications (e.g. on a mobile device) when the funds in the custodial account
30 need to be replenished, or the user may invoke a setting that replenishes by a predetermined amount whenever the balance is less than another predetermined amount. In the example discussed with respect to FIG. 3, step 250a, the custodial account holds the funds in fiat currency that is converted prior to the details of the transaction (i.e. time, amount, payee) being specified.

35 By contrast, in the example discussed with respect to FIG. 2, the user retains self-custody of the cryptocurrency, but has provided via smart contract a pre-

authorization to move crypto from the self-custody location to a location where the crypto is either accepted in the form of crypto, or converted to fiat currency, depending upon the terms implemented by the transaction processor. As used herein the term "smart contract" may refer to a public smart contract or a permissioned smart contract (e.g. via the ARCULUS® platform), which may contain platform-specific terms. For example, the smart contract may specify terms for spending the crypto assets, such as amount of crypto that can be converted and a date range during which the transaction can take place. This enables the fiat processing system to query and confirm sufficient funds are available under the contract (and in the designated account), similar to checking whether a user's fiat account has sufficient funds or credit balance can support the transaction, before initiating the transaction. This provides a similar level of assurance to the retailer as is provided by having custody of the crypto (or a set amount of fiat currency converted from crypto). From the user's perspective, it keeps the crypto in the form of crypto and in the custody and control of the user until the transaction is actually initiated.

FIGS. 5A and 5B depict aspects of an exemplary user interface 500, 502 such as may be used in connection with the method as described in this example. A first aspect of the user interface 500, for specifying the terms of the contract, displays and facilitates user entry of the amount of allowance 520 (to be moved from self-custody to a different location), the user name 530, and includes radio buttons 540 selectable to enable spending, 542 to disable spending, and 544 to set a time range (for the spending), along with an interface portion 546 for setting the time range during which the spend is permitted. Although depicted in the form of blocks for entry of a number of days, hours, and minutes from the time of setting the range, the time range setting in other embodiments may facilitate setting beginning and end dates/times or time (stated in days, hours, etc.) permitted from a start date in the future. Although not shown, the smart contract may specify other types of information limiting the permissible transactions (e.g. recipients who are eligible to receive the funds relating to the transaction, or the type(s) of cryptocurrency in the subject account eligible for use), without limitation. The user interface may also depict one or more virtual cards 510, each of which may display the card number, username, and allowance. For example, a user may have multiple virtual cards, each with different permissions. The on-chain crypto account address 515 (typically a long alphanumeric string) associated with the card may also be shown on the user interface screen. Specification of the contract may be initiated by clicking icon 535, which may trigger additional screens (e.g. to permit the user to select the account associated with the

crypto to be "loaded" onto the card, to indicate final approval of the transaction, or the like). The features of the user interface are not limited to those shown, and may include fewer or more functions and associated icons or fields. As shown, the interface also includes an exit icon 574 for exiting the interface aspect 500.

- 5 A second aspect of the user interface 502 is configured to conduct on-chain transactions. This aspect may also depict a copy of the virtual card 510 with relevant information and the crypto account address 515. This aspect of the user interface may provide a data entry field 550 for listing the on-chain address of the recipient of the funds. The on-chain address may be manually entered, or may be
- 10 populated from predetermined or preferred information (e.g. by selecting an icon 572 associated with a particular recipient, such as a coffee shop or other type of retailer). The on-chain address may also be entered via an image capture (i.e. via a web camera or mobile device camera) of a code such as a QR or bar code, prompted by user selection of icon 555. The user may enter the amount of the transaction in field 560.
- 15 Clicking icon 570 may initiate the on-chain transaction, which initiation may prompt the pop-up of one or more additional screens (e.g. to solicit user approval), not shown.

- It should be noted that the virtual card as depicted may or may not resemble the user's physical card, which physical card is then also enabled to perform the transactions permitted under the contract. To initiate a transaction with the
- 20 physical card, the user may submit the physical card to an on-chain POS terminal, which initiates population of the appropriate fields in the user interface associated with the user's digital wallet, from which the user can then approve the transaction. In instances where a user wishes to use a POS terminal is not on-chain, the card may be dual provisioned to permit traditional debit or credit transactions associated with a
- 25 standard debit or credit account, as described above.

- Most of the sequence relating to the cryptocurrency transactions is well known, such as defined by the Bitcoin protocol or BIP32/39, "Bitcoin Improvement Protocol" updates. In one embodiment, the steps are implemented inside a Java applet running on the secure element. Keys are generated inside the secure element, which
- 30 may be, for example, an SLC37 security microcontroller from Infineon Technologies, and are stored in encrypted form in a secure keystone. The keys do not leave the card and are known outside by their logical indexes, but not real values. All sign and hash operations are done using the secure element. In essence, the software embedded in the card manages all cryptocurrency cryptographic primitives. A mobile applet on the
- 35 mobile device (e.g. running on an Android/iOS operating system) sends the relevant, high-level information to the card for processing. Then, once the mobile applet

receives the signed transaction from the card, it establishes communication session with a crypto exchange and sends this data to initiate a transaction.

Further, in a typical process 600, summarized in the flow diagram depicted in FIG. 6, a transaction, corresponding to a transfer of currency having a value (e.g. \$40), between a user 610 and a merchant 620 is initiated by the user 610, in step 1. One skilled in the art would understand from the description herein that the sequential numbering of steps in the typical process 600 is not intended to be limiting, and a combination of steps or sub-steps thereof may be performed simultaneously or in an asynchronous manner.

In step 1, a fiat transaction is initiated by user 610 via the hardware storage device 110 and the card reader 140 of the fiat currency transaction system. For example, a connection is established over NFC or via a contact interaction between the card 110 and the card reader 140. Additionally, a cryptocurrency transaction is initiated by user 610 via the hardware storage device 110 and user interface 126 of the cryptocurrency transaction processing device (e.g. mobile device 120), as described herein above. As described above, crypto transactions are not synchronous with fiat transactions, and may occur less frequently than fiat transactions. In an exemplary embodiment, the connection between card reader and card prompts a standard credit or debit card transaction that is communicated to the mobile device 120 for authorization and satisfaction of the transaction. Separately, (as will be discussed in steps 2-7 below), the mobile device 120 authorizes cryptocurrency to be moved from a user's self-custody account to a location accessible by the transaction processor via the API, in accordance with a smart contract or funds may already be accessible in a custodial account associated with the transaction card. To facilitate this fiat transaction, secure element 112 comprises a payment module 10 configured to exchange payment information with a card reader for conducting a purchase transaction. The payment module 10 is connected to the portion of the secure element configured for processing cryptocurrency transactions, such that the cold storage device 110 establishes the connection with the mobile device 120, and therefore prompts the initiation of the transaction approval (e.g. a one-time – or otherwise not occurring each time a transaction is processed -- contract approval call that occurs before the transaction, which authorizes moving the crypto in accordance with the contract from self-custody to a location accessible by the transaction processor), and the remaining portions of the transaction (fiat or otherwise) may occur as described below.

In step 2, information concerning the fiat transaction initiated by user 610 is captured and parsed by an acquirer/processor 630, which in turn submits an

authorization request to a transaction network administrator 640 (e.g. VISA). This step performed by the acquirer/processor 630 incurs one or more fees totaling to X for merchant 620. In step 3, the transaction network administrator 640 routes the authorization request to an issuer processor 650. In step 4, an issuer processor 650
5 initiates a cooperative authorization. Notably, the issuer processor 650 may be a different entity, or the same entity, as the issuer. In one example, the issuer may be a card manufacturer (e.g. Arculus Holdings LLC), and the issuer processor may be a service provider contracted by the issuer.

In response, the issuer processor 650 inquires with the issuer 651, the
10 issuer confirms sufficient funds for approving the fiat transaction (step 5), and upon receipt of confirmation of sufficient funds allocated to complete the fiat transaction, the issuer processor 650 transmits to the transaction network administrator 640 a communication of approval of the fiat transaction (step 5). Optionally, confirmation of sufficient funds allocated to complete the fiat transaction includes initiating a transfer of
15 funds or releasing funds to a wallet issuer 660 (e.g. moving funds to a settlement wallet owned by the transaction network administrator that is managed by the issuer processor), and assigning to another party the right to transfer funds in accordance with a smart contract or via a custodial account associated with the transaction card (as described above). These step(s) performed by the issuer processor 650 incurs one
20 or more fees totaling to Y for merchant 620. In turn, in step 6, the transaction network administrator 640 transmits to the acquirer processor 630 a communication conveying approval/authorization. These step(s) performed by the transaction network administrator 640 incurs one or more fees totaling to Z for merchant 620. In step 7, the acquirer processor 630 notifies merchant 620 of the approval decision, such that
25 merchant is notified receipt of an amount of $\$40 - (X+Y+Z)$ and in step 8, merchant 620 displays or conveys to user 610 completion or success of the fiat transaction.

Although the invention is illustrated and described herein with reference to specific embodiments, the invention is not intended to be limited to the details shown. Rather, various modifications may be made in the details within the scope and
30 range of equivalents of the claims and without departing from the invention.

In particular, the systems, storage device, and processing devices as discussed herein may be used in connection with conducting any type of transaction (not limited to financial transactions), and may include any type of public key/private key authentication known in the art. For example, the storage device as described
35 herein may be paired with a transaction application on a mobile device to conduct any type of transaction, including authentications using the FIDO® standard. The initiation

of the transaction may take any form, such as a push from a first device connected to a network that prompts a second device connected to the network, provision of a code (e.g. a QR code) displayed by a first device (or embodied in a physical manifestation such as a printed document) read by a second device, or may be initiated by the user
5 using the transaction application user interface on the device, or by the user using the storage device placed in an activation proximity to the mobile device capable of exchanging information with the storage device. The initiated is not limited to any particular method. In some embodiments, the card may also or instead be used as an authentication token for hot wallets or other online accounts using the same or similar
10 cryptographic primitives as described above. In such embodiments, the secure element in the card may exchange encryption credentials through the mobile device hosting the online account. This exchange may occur during initial setup. For example, a PGP key exchange between the two devices may be performed via an applet. A simple recognition token may then be verified via an encrypted channel during
15 subsequent transactions that matches the token during initial registration. A card so configured may function as an independent factor of authentication, but does not sign any cryptocurrency transaction as it does not maintain the keys. Keys may be federated across multiple platforms with further software interactions.

What is Claimed:

1. A transaction system configured for conducting a cryptocurrency transaction, the transaction system comprising:

5 a hardware storage device having an integrated circuit comprising at least one secure element, the at least one secure element having a secure element processor, a secure element digital memory module comprising a cryptographic module, and at least one secure element wireless or contact interface, the at least one secure element digital memory module embodying instructions readable by the at least one secure element processor for causing the at least one secure element to store a
10 private key in encrypted state in the digital memory, generate a public key using the private key, and to perform a signature operation;

a cryptocurrency transaction processing device having a user interface embodying a virtual wallet having a first cryptocurrency address associated therewith, a processing device wireless or contact interface, and a communication interface
15 configured for connection to an exchange server of a cryptocurrency transaction network on a global communications network and for sending signed transaction information to the exchange server to initiate a cryptocurrency transaction; and

a fiat currency transaction system for processing a fiat currency transaction, the fiat currency transaction system including at least one payment
20 terminal and an application process interface (API) configured for processing the fiat currency transaction in accordance with a smart contract comprising machine-readable instructions stored in a computer memory accessible by the cryptocurrency transaction network for causing an issuer associated with the smart contract to process a cryptocurrency transaction sufficient to satisfy the fiat currency transaction upon
25 receipt of instructions from the cryptocurrency transaction network prompted by the fiat currency transaction initiated at the at least one payment terminal.

2. The transaction system of claim 1, wherein the hardware storage device comprises a transaction card and the payment terminal comprises a card reader, and the instructions embodied in the at least one secure element digital memory
30 module include instructions for performing the steps of:

a) conducting cryptocurrency transactions by establishing a connection between the hardware storage device and the cryptocurrency transaction processing device using the secure element wireless or contact interface in communication with the processing device wireless or contact interface, receiving
35 information from the processing device, retrieving the private key from the digital

- memory, defining a signature using the private key, checking a chain associated with the public key to confirm that the signature conforms to a public key signature that could only have been generated using the private key, signing the transaction, and sending signed transaction information to the cryptocurrency transaction processing device; and
- 5 b) conducting fiat transactions by establishing a connection over wireless or via a contact interaction with the card reader and authorizing the cryptocurrency transaction processed via the API in accordance with the smart contract.
- 10 3. The transaction system of claim 2, wherein step (a) comprises the hardware storage device causing the at least one secure element to perform a signature operation associated with assigning to an assignee having a second cryptocurrency address associated therewith a right to transfer a designated amount of cryptocurrency in accordance with the smart contract, and step (b) comprises the API
- 15 approving the fiat transaction upon confirmation of sufficient funds allocated under execution of the smart contract to complete the fiat transaction, and the assignee upon receipt of approval from the API, transmitting an appropriate amount to a requesting recipient to complete the fiat currency transaction.
- 20 4. The system of claims 1-3, wherein the at least one secure element also comprises one or more of a payment module, a magnetic stripe, and a code configured to be read by the card reader for conducting the fiat currency transaction.
- 25 5. The system of claims 1-3, wherein the cryptocurrency transaction processing device comprises a mobile device.
- 30 6. The system of claim 5, wherein the mobile device comprises one of a smartphone, a tablet, or a laptop computer.
7. The transaction system of claim 1, wherein the machine-readable instructions include instructions for converting a suitable amount of cryptocurrency associated with the virtual wallet into fiat currency for satisfying the fiat currency transaction.
8. A transaction system configured for conducting a plurality of transactions, the transaction system comprising:
- a transaction card including a hardware storage device having an integrated circuit comprising at least one secure element, the at least one secure

element having a secure element processor, a secure element digital memory module comprising a cryptographic module, and at least one secure element wireless or contact interface, the at least one secure element digital memory module embodying instructions readable by the at least one secure element processor for causing the at
5 least one secure element to store a private key in an encrypted state in the digital memory, generate a public key using the private key, and perform a signature operation;

a cryptocurrency transaction processing device having a user interface embodying a virtual wallet, a processing device wireless or contact interface, and a
10 communication interface configured for connecting to an exchange server of a cryptocurrency transaction network on a global communications network and for sending signed transaction information to the exchange server to initiate a cryptocurrency transaction;

a fiat currency transaction system for processing a transaction using fiat
15 currency via a custodial account associated with the transaction card;

the instructions embodied on the hardware storage device including instructions for performing the steps of:

(a) conducting cryptocurrency transactions by establishing a connection between the hardware storage device and the cryptocurrency transaction
20 processing device using the secure element wireless or contact interface in communication with the processing device wireless or contact interface, receiving information from the processing device, retrieving the private key from the digital memory, performing signature operations using the private key, checking a chain associated with the public key to confirm that the signature conforms to a public key
25 signature that could only have been generated using the private key, signing the transaction, and sending signed transaction information to the cryptocurrency transaction processing device; and

(b) conducting fiat transactions by establishing a connection over wireless or via a contact interaction with a card reader of the fiat currency transaction
30 system, and authorizing a transaction processed using funds stored in the custodial account;

wherein:

i) performing step (a) causes conversion of an amount of cryptocurrency associated with the virtual wallet into fiat currency and loading the converted fiat currency into the custodial account; or

ii) performing step (b) causes a transfer amount of cryptocurrency associated with the transaction to be moved from a self-custody account of a card user to the custodial account, and step (b) includes a custodian of the custodial account (A) providing a transaction amount of the cryptocurrency to the requesting recipient or (B) converting the transaction amount of the cryptocurrency to fiat currency and transmitting the converted fiat currency to a requesting recipient to complete the fiat currency transaction.

9. The system of claim 8, wherein the at least one secure element also comprises one or more of a payment module, a magnetic stripe, or a code configured to be read by the card reader for conducting the fiat currency transaction.

10. The system of claims 8-9, wherein the cryptocurrency transaction processing device comprises a mobile device running application software.

11. The system of claim 10, wherein the mobile device comprises one of a smartphone, a tablet, or a laptop computer.

12. The system of claims 8-11, wherein: performing step (a) causes conversion of an amount of cryptocurrency associated with the virtual wallet into fiat currency and loading the converted fiat currency into the custodial account prior to or at a same time as performing step (b).

13. The system of claim 8-11, wherein performing step (b) causes an amount of cryptocurrency associated with the transaction to be moved from a self-custody account of a card user to the custodial account in accordance with a smart contract comprising machine-readable instructions stored in a computer memory accessible by the cryptocurrency transaction network, and step (b) includes a custodian of the custodial account transmitting the transaction amount of the cryptocurrency or the transaction amount of cryptocurrency converted fiat currency to a requesting recipient to complete the fiat currency transaction.

14. A hardware storage device having an integrated circuit comprising at least one secure element, the at least one secure element having a secure element processor, a secure element digital memory module comprising a cryptographic module, and at least one secure element wireless interface, the at least one secure element digital memory module embodying instructions readable by the at least one

secure element processor for causing the at least one secure element to store a private key in encrypted state in the digital memory, generate a public key using the private key, and to perform a signature operation.

15. The hardware storage device of claim 14, wherein the at least one
5 secure element digital memory module embodies instructions readable by the at least one secure element processor for causing the at least one secure element to, in response to receipt of information from a cryptocurrency transaction processing device linked via a connection with the at least one secure element via the wireless or contact interface, perform the steps of: (a) retrieving the private key from the digital memory,
10 define a signature using the private key, checking a chain associated with the public key to confirm that the signature conforms to a public key signature that could only have been generated using the private key, signing the transaction, and sending signed transaction information to the cryptocurrency transaction processing device; and (b)
15 conducting fiat transactions by establishing a wireless connection or a contact interaction with a card reader of a fiat currency transaction system including an application process interface (API) and authorizing the cryptocurrency transaction processed via the API in accordance with a smart contract comprising machine-readable instructions stored in a computer memory accessible by the cryptocurrency transaction network for causing an issuer associated with the smart contract to process
20 a cryptocurrency transaction sufficient to satisfy the fiat currency transaction.

16. The hardware storage device of claim 15, wherein step (a)
comprises causing the at least one secure element to perform a signature operation associated with assigning to an assignee having a second cryptocurrency address a right to transfer a designated amount of cryptocurrency associated with the smart
25 contract, and step (b) comprises the API approving the fiat transaction upon confirmation of sufficient funds allocated under the execution of the smart contract to complete the fiat transaction, and the API sending an approval to the assignee configured to cause the assignee to transmit funds corresponding to the fiat transaction in the form of cryptocurrency or cryptocurrency converted to fiat currency to a
30 requesting recipient to complete the fiat currency transaction.

17. The hardware storage device of claims 14-16, wherein the hardware storage device comprises one or more of a payment module, a magnetic stripe, or a code configured to be read by the card reader for conducting the fiat currency transaction.

18. The hardware storage device of claims 14-17, wherein the cryptocurrency transaction processing device comprises a mobile device running application software.

19. The hardware storage device of claim 18, wherein the mobile
5 device comprises one of a smartphone, a tablet, or a laptop computer.

20. A transaction card including a hardware storage device having an integrated circuit comprising at least one secure element, the at least one secure element having a secure element processor, a secure element digital memory module comprising a cryptographic module, and at least one secure element wireless or contact
10 interface, the at least one secure element digital memory module embodying instructions readable by the at least one secure element processor for causing the at least one secure element to store a private key in an encrypted state in the digital memory, generate a public key using the private key, and perform a signature operation.

21. The transaction card of claim 20, wherein the at least one secure
15 element digital memory module embodies instructions readable by the at least one secure element processor for causing the at least one secure element to, in response to receipt of information from a cryptocurrency transaction processing device linked via a connection with the at least one secure element via the wireless or contact interface,
20 perform the steps of: (a) retrieving the private key from the digital memory, performing signature operations using the private key, checking a chain associated with the public key to confirm that the signature conforms to a public key signature that could only have been generated using the private key, signing the transaction, and sending signed transaction information to the cryptocurrency transaction processing
25 device; and step (b) conducting fiat transactions by establishing a wireless connection or a contact interaction with a card reader of the fiat currency transaction system, and authorizing a transaction processed using funds stored in a custodial account associated with the transaction card.

22. The transaction card of claim 21, wherein performing step (a)
30 converts an amount of cryptocurrency associated with the virtual wallet into fiat currency loaded into the custodial account prior to performing step (b); or performing step (b) moves an amount of cryptocurrency associated with the transaction from a self-custody account of a card user to the custodial account, and step (b) includes a custodian of the custodial account transmitting an appropriate amount of the
35 cryptocurrency, or converting the appropriate amount of cryptocurrency to fiat currency

and transmitting the converted fiat currency, to a requesting recipient to complete the fiat currency transaction.

23. The transaction card of claims 20-22, wherein the hardware storage device comprises one or more of a payment module, a magnetic stripe, or a code configured to be read by the card reader for conducting the fiat currency transaction.

24. The transaction card of claims 20-23, wherein the cryptocurrency transaction processing device comprises a mobile device running application software.

25. The transaction card of claim 24, wherein the mobile device comprises one of a smartphone, a tablet, or a laptop computer.

26. A transaction system configured for conducting a cryptocurrency transaction in satisfaction of a fiat transaction, the transaction system comprising:

a cryptocurrency transaction processing system configured for sending instructions to a node of a cryptocurrency transaction network to initiate a cryptocurrency transaction; and

a fiat currency transaction system for processing a fiat currency transaction, the fiat currency transaction system including an application process interface (API) configured for processing the fiat currency transaction in accordance with a smart contract comprising machine-readable instructions stored in a computer memory accessible by the cryptocurrency transaction network for causing an issuer associated with the smart contract to process a cryptocurrency transaction sufficient to satisfy the fiat currency transaction.

27. The transaction system of claim 26, wherein the cryptocurrency transaction processing system further comprises:

a cryptocurrency transaction processing device having a user interface embodying a virtual wallet having a first cryptocurrency address associated therewith, a processing device NFC or contact interface, and a communication interface configured for connection to an exchange server of the cryptocurrency transaction network on a global communications network and for sending signed transaction information to the exchange server to initiate the cryptocurrency transaction.

28. The transaction system of claim 27, wherein the cryptocurrency transaction processing system further comprises:

a hardware storage device configured to perform a signature operation and to transmit the signed transaction information to the virtual wallet via communication protocol other than via the global communications network.

29. The transaction system of claim 28, wherein the hardware storage
5 device comprises at least one secure element, the at least one secure element having a secure element processor, a secure element digital memory module comprising a cryptographic module, and at least one secure element wireless or contact interface, the at least one secure element digital memory module embodying instructions
10 readable by the at least one secure element processor for causing the at least one secure element to store a private key in encrypted state in the digital memory, generate a public key using the private key, and to perform the signature operation.

30. The transaction system of claim 29, wherein the hardware storage device comprises a transaction card configured to perform the steps of:

a) conducting cryptocurrency transactions by establishing a
15 connection between the hardware storage device and the cryptocurrency transaction processing device using the secure element wireless or contact interface in communication with the processing device NFC or contact interface, receiving information from the processing device, retrieving the private key from the digital memory, defining a signature using the private key, checking a chain associated with
20 the public key to confirm that the signature conforms to a public key signature that could only have been generated using the private key, signing the transaction, and sending signed transaction information to the cryptocurrency transaction processing device; and

b) conducting fiat transactions by establishing a wireless connection
25 or a contact interaction with a card reader of the fiat currency transaction system and authorizing the cryptocurrency transaction processed via the API in accordance with the smart contract.

31. The transaction system of claim 30, wherein step (a) comprises the hardware storage device causing the at least one secure element to perform a
30 signature operation associated with assigning to an assignee having a second cryptocurrency address associated therewith a right to transfer a designated amount of cryptocurrency in accordance with the smart contract, and step (b) comprises the API approving the fiat transaction upon confirmation of sufficient funds allocated under execution of the smart contract to complete the fiat transaction, and the assignee upon
35 receipt of approval from the API, converting the funds corresponding to the fiat

transaction from cryptocurrency to fiat currency and transmitting the appropriate amount of the converted fiat currency to a requesting recipient to complete the fiat currency transaction.

32. A computer implemented method for conducting a cryptocurrency transaction in satisfaction of a fiat transaction, the method comprising:

5 sending instructions via a computer to a node of a cryptocurrency transaction network to initiate a cryptocurrency transaction from a first cryptocurrency address associated with a self-custody account of a user to a second cryptocurrency address in accordance with a smart contract that assigns to an assignee a right to transfer a designated amount of cryptocurrency in accordance with the smart contract;
10 and

processing a fiat currency transaction via a computer running an application process interface (API) configured for processing the fiat currency transaction by approving the fiat transaction upon confirmation of sufficient funds allocated under execution of the smart contract to complete the fiat transaction, and
15 the assignee upon receipt of approval from the API, transmitting an appropriate amount of funds corresponding to the fiat transaction as cryptocurrency, or converting the appropriate amount of funds to cryptocurrency and transmitting the converted cryptocurrency to a requesting recipient to complete the fiat currency transaction.

20 33. A method for conducting a cryptocurrency transaction, the method comprising:

a) providing a transaction system comprising:

25 a hardware storage device having an integrated circuit comprising at least one secure element, the at least one secure element having a secure element processor, a secure element digital memory module comprising a cryptographic module, and at least one secure element wireless or contact interface, the secure element digital memory module further comprising a private key stored in an encrypted state therein;

30 a cryptocurrency transaction processing device having a user interface embodying a virtual wallet having a first cryptocurrency address associated therewith, a processing device wireless or contact interface, and a communication interface;

- a fiat currency transaction system for processing a fiat currency transaction, the fiat currency transaction system including at least one payment terminal and an application process interface (API) configured for processing the fiat currency transaction in accordance with a smart contract comprising machine-readable instructions stored in a computer memory accessible by the cryptocurrency transaction network;
- b) processing an authorization cryptocurrency transaction via the API in accordance with authorization of the smart contract, the authorization cryptocurrency transaction comprising the steps of:
- i) establishing a connection between the wireless or contact interface of the hardware storage device and the wireless or contact interface of the cryptocurrency transaction processing device;
- ii) the hardware storage device secure element processor receiving information from the processing device, retrieving the private key from the digital memory, defining a signature using the private key, checking a chain associated with the public key to confirm that the signature conforms to a public key signature that could only have been generated using the private key, signing the transaction, and sending signed transaction information to the cryptocurrency transaction processing device; and
- iii) the cryptocurrency transaction processing device connecting via the communication interface to an exchange server of a cryptocurrency transaction network on a global communications network and sending the signed transaction information to the exchange server to initiate the authorization cryptocurrency transaction, the authorization cryptocurrency transaction comprising assigning to an assignee having a second cryptocurrency address associated therewith a right to transfer a designated amount of cryptocurrency from the first cryptocurrency address in accordance with the smart contract;
- c) initiating the fiat currency transaction at the at least one payment terminal and
- d) an issuer associated with the smart contract processing a transfer authorized by the smart contract, including the API approving the fiat transaction upon confirmation of sufficient funds allocated under execution of the smart contract to complete the fiat transaction, and the assignee upon receipt of approval from the API, transfer an appropriate amount from the first cryptocurrency address to the requesting recipient to complete the fiat currency transaction.

34. The method of claim 33, wherein the method includes converting the appropriate amount of cryptocurrency transferred from the first cryptocurrency address to fiat currency before transferring it to the requesting recipient.

35. The method of claim 33, wherein the appropriate amount is
5 transferred from the first cryptocurrency address to the requesting recipient as cryptocurrency.

36. The method of claim 33, wherein step b is performed asynchronously with steps c and d.

37. The method of claim 33, wherein step b is performed as part of a
10 same workflow as performing steps c and d.

38. A method for conducting a cryptocurrency transactions, the method comprising:

a) providing a transaction system comprising:

15 a transaction card including a hardware storage device having an integrated circuit comprising at least one secure element, the at least one secure element having a secure element processor, a secure element digital memory module comprising a cryptographic module, and at least one secure element wireless or contact interface, the at least one secure element digital
20 memory module embodying instructions readable by the at least one secure element processor for causing the at least one secure element to store a private key in an encrypted state in the digital memory, generate a public key using the private key, and perform a signature operation;

25 a cryptocurrency transaction processing device having a user interface embodying a virtual wallet, a processing device wireless or contact interface, and a communication interface configured for connecting to an exchange server of a cryptocurrency transaction network on a global communications network and for sending signed transaction information to the exchange server to initiate a cryptocurrency transaction;

30 a fiat currency transaction system for processing a transaction using fiat currency via a custodial account associated with the transaction card;

(b) conducting a cryptocurrency transaction by establishing a connection between the hardware storage device and the cryptocurrency transaction processing device using the secure element wireless or contact interface in communication with the processing device wireless or contact interface, receiving

information from the processing device, retrieving the private key from the digital memory, performing signature operations using the private key, checking a chain associated with the public key to confirm that the signature conforms to a public key signature that could only have been generated using the private key, signing the transaction, and sending signed transaction information to the cryptocurrency transaction processing device; and

(c) conducting a fiat transaction by establishing a connection over wireless or via a contact interaction with a card reader of the fiat currency transaction system, and authorizing a transaction processed using funds stored in the custodial account;

wherein:

- i) performing step (b) causes conversion of an amount of cryptocurrency associated with the virtual wallet into fiat currency and loading the converted fiat currency into the custodial account; or
- ii) performing step (c) causes a transfer amount of cryptocurrency associated with the transaction to be moved from a self-custody account of a card user to the custodial account, and step (c) includes a custodian of the custodial account (A) providing a transaction amount of the cryptocurrency to the requesting recipient or (B)_converting the transaction amount of the cryptocurrency to fiat currency and transmitting the converted fiat currency to a requesting recipient to complete the fiat currency transaction.