



(51) International Patent Classification:

G06F 17/40 (2006.01) G07D 11/32 (2019.01)
G07D 11/12 (2019.01) G07D 11/125 (2019.01)
G07F 19/00 (2006.01) G06Q 20/20 (2012.01)
G07D 11/24 (2019.01) G06Q 20/18 (2012.01)

(21) International Application Number:

PCT/AU2019/050284

(22) International Filing Date:

29 March 2019 (29.03.2019)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

2018901897 29 May 2018 (29.05.2018) AU

(71) Applicant: **TILL PAYMENTS PTY LTD** [AU/AU]; c/-
Davies Collison Cave Pty Ltd, Level 10, 301 Coronation
Drive, Milton, Queensland 4064 (AU).

(72) Inventors: **HADDAD, Shadi**; Suite 6, 2-4 Giffnock Av-
enue, Macquarie Park, New South Wales 2113 (AU).
LANE, Richard Benjamin; Suite 6, 2-4 Giffnock Avenue,
Macquarie Park, New South Wales 2113 (AU).

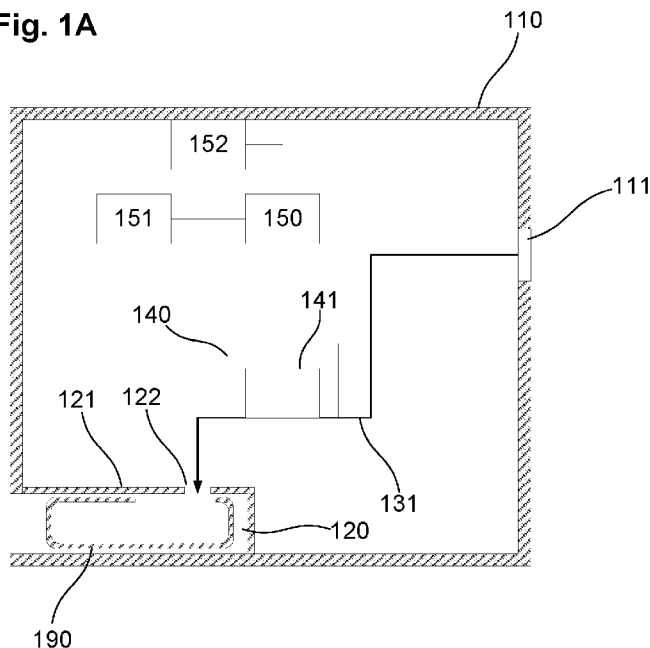
(74) Agent: **DAVIES COLLISON CAVE PTY LTD**; Level
10, 301 Coronation Drive, Milton, Queensland 4064 (AU).

(81) Designated States (unless otherwise indicated, for every
kind of national protection available): AE, AG, AL, AM,
AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ,
CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO,
DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN,
HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP,
KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME,
MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ,
OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA,
SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN,
TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every
kind of regional protection available): ARIPO (BW, GH,

(54) Title: PAYMENT PROCESSING SYSTEM AND METHOD

Fig. 1A



(57) Abstract: A system for processing a payment for a transaction, the system including a payment terminal including a housing including a container cavity that in use receives a currency container, a currency input and a currency transport system that transports currency from the currency input to an opening in the container cavity to allow currency to be dispensed into the currency container. The system also includes one or more payment modules including at least one currency module having a currency sensor that senses currency transported by the transport system and determines a currency value, a terminal memory, a terminal communications interface and one or more terminal processing devices. The terminal processing devices determine a transaction amount and a received payment amount, and cause at least some of the currency to be dispensed into the currency container. Payment data indicative of the transaction is also stored.



GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ,
UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ,
TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK,
EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV,
MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM,
TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW,
KM, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

PAYMENT PROCESSING SYSTEM AND METHOD

Background of the Invention

[0001] The present invention relates to a method and system for processing a payment for a transaction, and in one particular example, to a method and system for processing a cash payment.

Description of the Prior Art

[0002] The reference in this specification to any prior publication (or information derived from it), or to any matter which is known, is not, and should not be taken as an acknowledgment or admission or any form of suggestion that the prior publication (or information derived from it) or known matter forms part of the common general knowledge in the field of endeavour to which this specification relates.

[0003] Transactions in commercial environments, such as within shops, entertainment venues or the like are often conducted utilising a point of sales (POS) terminal. The POS terminal typically includes a mechanism that allows a cashier or other individual to enter details of goods and/or services being purchased. The POS terminal calculates a total transaction amount based on a purchase price of each item and generates a receipt which can be printed via a printer connected to the POS terminal.

[0004] Payments can be collected utilising a variety of mechanisms depending on the circumstances. For example, the POS terminal can be connected to a credit/debit card machine which is able to perform a credit/debit card transaction, or similar. Alternatively, in some scenarios, particularly when a cashier is involved in the transaction, a cash drawer may be provided to allow payments to be performed utilising cash. In this instance, the cashier is responsible for receiving the currency, checking the currency is valid and placing this in the cash drawer.

[0005] Performing a cash transaction in this manner leads to a number of disadvantages. In particular, this places a burden on the cashier to ensure the cash is valid and that a correct amount is provided. Particularly in busy venues, such as bars and clubs, there is significant

time pressure on the cashier making this job difficult. As a result, it is easy to miss fraudulent currency and/or incorrectly count money provided or change given, leading to an incorrect payment amount being collected. Additionally, many venues such as supermarkets are moving towards a self-service checkout system. Currently, no mechanisms are provided that allow this to occur using cash payments and these are therefore limited to credit/debit card payments which is inconvenient for some customers. This is exacerbated in situations where debit/credit payments fail, for example, in the event of a banking systems failure, or failure of a communications network. In this instance, it is typically necessary to revert to cash payments but this is not feasible in cases where suitable facilities such as cash drawers do not exist.

[0006] Additionally, there are a wide range of types of compliance associated with commercial transactions, such as requirement for compliance with taxation or money laundering rules. For example, compliance with tax rules typically relies on entities, such as merchants or other parties, collating and providing evidence of transactions to an overseeing authority, such as a government tax department. Tax departments will typically perform audits of such records to ensure their accuracy, and in turn to ensure taxes are correctly applied and paid. However, for many entities, particularly those involved in large volumes of transactions, the burden in recording transaction details is undue, particularly in the case of cash transactions, for which there is often little record, leading to compliance with tax requirements being a time consuming and expensive process. Additionally, it can be easy for entities to modify transaction details, and hence fraudulently avoid tax payments. Accordingly, an improved process for transaction compliance monitoring is required.

Summary of the Present Invention

[0007] In one broad form an aspect of the present invention seeks to provide a system for processing a payment for a transaction, the system including a payment terminal including: a housing including: a container cavity that in use receives a currency container; a currency input; and, a currency transport system that transports currency from the currency input to an opening in the container cavity to allow currency to be dispensed into the currency container; one or more payment modules including at least one currency module having a currency

sensor that senses currency transported by the transport system and determines a currency value; a terminal memory; a terminal communications interface; and, one or more terminal processing devices that: determine a transaction amount; determine a received payment amount indicative of an amount of a received currency; cause at least some of the currency to be dispensed into the currency container; and cause payment data to be stored, the payment data being indicative of at least one of: the transaction amount; the payment amount; an amount of currency dispensed into the currency container; and, a container identifier indicative of an identity of the currency container.

[0008] In one embodiment the one or more terminal processing devices: determine a currency container identifier; and, store the currency container identifier in the terminal memory.

[0009] In one embodiment the payment terminal includes a display that displays at least one of: a transaction amount; transaction details; and, a received payment amount.

[0010] In one embodiment the payment terminal includes first and second displays that in use display information to a merchant and customer respectively.

[0011] In one embodiment the payment terminal includes a user input that receives user input commands.

[0012] In one embodiment the payment terminal includes a lock that secures the currency container within the container cavity.

[0013] In one embodiment the lock includes a solenoid lock that engages at least one of: the currency container; and, a door to the container cavity.

[0014] In one embodiment the system includes a currency container including: a container housing including a container cavity; a lid for selectively closing the container cavity; a securing mechanism to secure the lid; a container communications interface; a container memory; and, one or more container processing devices that communicate with the one or more terminal processing devices via the communications interface.

[0015] In one embodiment the one or more container processing devices: retrieve the container identifier from the container memory; and, provide the container identifier to the terminal processing device.

[0016] In one embodiment the one or more container processing devices: receive currency data indicative of dispensed currency from the one or more terminal processing devices; and store the currency data in the container memory.

[0017] In one embodiment the one or more container processing devices: receive a currency data request from a processing system; in response to the request, retrieve the currency data from the container memory; and provide the currency data to the processing system via the container communications interface.

[0018] In one embodiment the one or more container processing devices: receive requests via the container communications interface; and, control the securing mechanism in accordance with requests to thereby selectively open or close the lid to provide access to the container cavity.

[0019] In one embodiment the currency container includes a reader that determines a user identity and wherein the one or more container processing devices at least one of: store the user identity in the memory; authenticate the user at least in part using the user identity; and, selectively perform actions based on permissions associated with the user identity.

[0020] In one embodiment the one or more container processing devices: determine a container status; and, at least one of: record an indication of the container status in the container memory; and, periodically broadcast an indication of the container status to a remote processing system via the container communications interface.

[0021] In one embodiment the currency container includes a location tracking module that tracks a location of the currency container and wherein the container status includes an indication of the container status.

[0022] In one embodiment the currency container includes at least one container tamper sensor, and wherein the one or more container processing devices: monitor changes in signals from the container tamper sensors to detect tamper events; and, at least one of: determine a container status in accordance with tamper events; and, cause an alert notification to be generated in the event that tampering is detected.

[0023] In one embodiment the sensors include at least one of: an accelerometer; a position sensor; a temperature sensor; an air pressure sensor; a light sensor; and, a humidity sensor.

[0024] In one embodiment the securing mechanism is a drive and wherein the one or more container processing devices selectively activate the drive to thereby open or close the container lid.

[0025] In one embodiment the one or more container processing devices store in container memory an indication of at least one of: a container identifier; a container status; tamper events; received requests; actions performed; a request identifier associated with received requests; and, a payment terminal identifier.

[0026] In one embodiment currency container includes an inductively charged battery.

[0027] In one embodiment: the payment terminal includes an inductive power transmitter positioned adjacent the container cavity; and, the currency container includes an inductive power receiver to thereby inductively power the currency container.

[0028] In one embodiment the payment terminal and currency containers include: a first interface used to exchange communications information; and, a second interface used to provide a secure communication channel between the payment terminal and the currency container using the communications information.

[0029] In one embodiment the communications information includes at least one of: an identifier associated with the second communications interface; and, an encryption key.

[0030] In one embodiment the one or more terminal processing devices: determine user input commands indicative of a container release request; generate a close container request;

transfer the close container request to the currency container, the one or more container processing devices being responsive to the close container message to activate the securing mechanism to secure the lid; determine the lid is closed; and, activate the lock to thereby release the currency container.

[0031] In one embodiment the one or more terminal processing devices determine the lid is closed using at least one of: a lid closed response received from the currency container; and, signals from a lid sensor.

[0032] In one embodiment the one or more terminal processing devices: detect the presence of a currency container using the first communications interface; selectively activate the lock to thereby secure the currency container; generate an open container request; transfer the open container request to the currency container, the one or more container processing devices being responsive to the open container request to activate the securing mechanism to open the lid; determine the lid is open; and, activate the currency payment module.

[0033] In one embodiment the one or more terminal processing devices determine the lid is closed using at least one of: a lid open response received from the currency container; and, signals from a lid sensor.

[0034] In one embodiment the one or more payment modules include: a coin currency module including a coin sensor that senses coins; a note currency module including a note sensor that senses notes; and, a card module including a card reader that reads payment cards.

[0035] In one embodiment the system includes a plurality of payment modules, and wherein the one or more terminal processing devices: cause a display to display a number of payment options; determine a selected payment option in accordance with user input commands; and, selectively activate one or more of the payment modules in accordance with the user input commands.

[0036] In one embodiment the payment module uses signals from the currency sensor to validate the received currency.

[0037] In one embodiment at least one payment module includes: a currency input; a currency validator to validate received currency; and, a currency outlet.

[0038] In one embodiment at least one payment module is removably mounted within the housing.

[0039] In one embodiment at least one payment module includes a currency store that stores currency.

[0040] In one embodiment the currency store includes a plurality of cartridges, each cartridge being configured to store a respective denomination of currency.

[0041] In one embodiment each cartridge is removably mounted to a chassis and wherein the housing includes a door to allow cartridges to be removed from the housing.

[0042] In one embodiment the system includes a cartridge removal tool, including a body having downwardly facing wings that engage a catch on the chassis to detach the cartridges from the chassis.

[0043] In one embodiment the transport system includes at least one of: an outlet path that transfers to a currency outlet at least one of: change; and, invalid currency; a float path that selectively transfers validated currency to or from a float storage; and, a float dump path that selectively transfers currency from the float storage to the currency container.

[0044] In one embodiment the one or more terminal processing devices control the transport system in accordance with at least one of: user input commands; signals from the payment module; and, instructions stored in memory.

[0045] In one embodiment the one or more terminal processing devices: retrieve a current float balance and a target float level from memory; determine a float deficit; and, control the transport system to transfer currency having a value equal to the float deficit to the float storage.

[0046] In one embodiment the one or more terminal processing devices: determine a float dump request; and, control the transport system to cause at least some currency in the float storage to be dispensed into the currency container.

[0047] In one embodiment the transport system includes a feeder outlet that dispenses currency through the opening in the container cavity to thereby dispense currency into the currency container.

[0048] In one embodiment the feeder outlet is movably mounted within the housing to allow the feeder outlet to move between a dispensing position, in which the feeder outlet projects through the opening in the container cavity and a retracted position in which the feeder outlet is retracted from the opening in the container cavity.

[0049] In one embodiment the system includes an outlet actuator that moves the feeder outlet between the dispensing and retracted position.

[0050] In one embodiment the one or more terminal processing devices: determine a user request in accordance with user input commands; determine a user identity of the user making the request; use the user identity to at least one of: authenticate the user; and; determine permissions associated with the user; selectively perform an operation depending at least one of: results of authentication of the user; and, a user permissions associated with the user.

[0051] In one embodiment the payment terminal includes a reader that determines the user identity.

[0052] In one embodiment the payment processing device: obtains transaction data indicative of a transaction performed using a transaction terminal; and, determines the transaction amount using the transaction data.

[0053] In one embodiment the payment terminal intercepts transaction data on a communications network, the transaction data being intercepted as the transaction data is transferred from the transaction terminal to a network enabled device.

[0054] In one embodiment the payment terminal: receives network traffic directed to the network enabled device; determines transaction details if the network traffic includes transaction data; and, forwards the network traffic to the network enabled device.

[0055] In one embodiment the payment terminal is configured in accordance with network addresses of each network enabled device.

[0056] In one embodiment the network enabled device is a printer.

[0057] In one embodiment the transaction data includes print data indicative of a transaction to be printed, and the one or more terminal processing devices determine the transaction amount from the print data.

[0058] In one embodiment the one or more terminal processing devices scrape the print data to determine the transaction amount.

[0059] In one embodiment the one or more terminal processing devices determine the transaction amount using at least one of: optical character recognition techniques; and, templates defining the location of transaction details within the transaction data.

[0060] In one embodiment the payment terminal is updated with templates based on a format of the transaction data associated with the transaction terminals.

[0061] In one embodiment the payment terminal causes transaction details to be stored to allow the transaction details to be used in monitoring transaction compliance.

[0062] In one embodiment at least one of payment data and transaction details are stored as part of a blockchain.

[0063] In one embodiment a processing system: determines transaction details for at least one transaction; compares the transaction details to one or more transaction rules; and, at least one of: determines if one or more transaction rules are breached based on results of the comparison; and, causes an indication of results of the comparison to be displayed.

[0064] In one embodiment the transaction rules are used to identify at least one of: taxation payable; and, suspicious activities.

[0065] In one embodiment the transaction amount includes a taxation amount, the transaction rules include taxation rules and the system is used in monitoring compliance with taxation payments.

[0066] In one embodiment a processing system: determines transaction details for a number of transactions associated with an entity; and, determines an amount of tax payable by the entity in accordance with the transaction details.

[0067] In one embodiment the one or more terminal processing devices: periodically transmit a status notification to a processing system, the processing system being responsive to the status notification to generate a status response; and, use the status notification and status response to at least one of: control payment terminal communication; cause the payment terminal to cache transaction details; and, generate an alert.

[0068] In one embodiment the payment terminal includes at least one terminal tamper sensor, and wherein the one or more terminal processing devices: monitor changes in signals from the terminal tamper sensors to detect tampering with the payment terminal; and, cause an alert notification to be generated in the event that tampering is detected.

[0069] In one embodiment the tamper sensors include at least one of: an accelerometer; a position sensor; a temperature sensor; an air pressure sensor; a light sensor; and, a humidity sensor.

[0070] In one broad form an aspect of the present invention seeks to provide a system for processing a payment for a transaction, the system including one or more terminal processing devices that: determine a transaction amount; determine a received payment amount indicative of an amount of a received currency; cause at least some of the currency to be dispensed into the currency container; and cause payment data to be stored, the payment data being indicative of at least one of: the transaction amount; the payment amount; an amount of

currency dispensed into the currency container; and, a container identifier indicative of an identity of the currency container.

[0071] In one broad form an aspect of the present invention seeks to provide a method for processing a payment for a transaction, the method including, in one or more terminal processing devices: determining a transaction amount; determining a received payment amount indicative of an amount of a received currency from one of a number of payment modules, at least one of the modules including a currency module having: a currency input; a currency container that stores the received currency; and, a currency counting device that: receives currency from the currency input; validates the currency; and, evaluates the currency; and, dispenses currency into the currency container; causing at least some of the currency to be dispensed into the currency container; and causing payment data to be stored, the payment data being indicative of at least one of: the transaction amount; the payment amount; an amount of currency dispensed into the currency container; and, a container identifier indicative of an identity of the currency container.

[0072] In one broad form an aspect of the present invention seeks to provide a container for receiving security documents, wherein the container includes: a container housing including a container cavity; a lid for selectively closing the container cavity; a securing mechanism to secure the lid; a container communications interface; a container memory; and, one or more container processing devices that communicate with one or more terminal processing devices via the communications interface to control the securing mechanism in accordance with requests received via the container communications interface to selectively open or close the lid to provide access to the container cavity.

[0073] In one embodiment the one or more container processing devices: retrieve the container identifier from the container memory; and, provide the container identifier to a terminal processing device.

[0074] In one embodiment the one or more container processing devices: receive currency data indicative of dispensed currency from the one or more terminal processing devices; and store the currency data in the container memory.

[0075] In one embodiment the document container includes a reader that determines a user identity and wherein the one or more container processing devices at least one of: store the user identity in the memory; and, authenticate the user at least in part using the user identity; and, selectively perform actions based on permissions associated with the user identifier.

[0076] In one embodiment the one or more container processing devices: determine a container status; and, at least one of: recording an indication of the container status in the container memory; and, periodically broadcast an indication of the container status to a remote processing system via the container communications interface.

[0077] In one embodiment the currency container includes a location tracking module that tracks a location of the currency container and wherein the container status includes an indication of the container status.

[0078] In one embodiment the currency container includes at least one container tamper sensor, and wherein the one or more container processing devices: monitor changes in signals from the container sensors to detect tamper events; and, at least one of: determine the container status in accordance with tamper events; and, cause an alert notification to be generated in the event that tampering is detected.

[0079] In one embodiment the sensors include at least one of: an accelerometer; a position sensor; a temperature sensor; an air pressure sensor; a light sensor; and, a humidity sensor.

[0080] In one embodiment the document container includes an inductively charged battery.

[0081] In one embodiment the document container includes: a first interface used to exchange communications information; and, a second interface used to provide a secure communication channel with the one or more terminal processing devices.

[0082] In one embodiment the communications information includes at least one of: an identifier associated with the second communications interface; and, an encryption key.

[0083] In one embodiment the securing mechanism is a drive and wherein the one or more terminal processing devices selectively activate the drive to thereby open or close the container lid.

[0084] In one embodiment the one or more container processing devices store in memory an indication of at least one of: a container identifier; a container status; tamper events; received requests; actions performed; a request identifier associated with received requests; and, a payment terminal identifier.

[0085] In one broad form, an aspect of the present invention seeks to provide a cartridge removal tool for removing cartridges from a payment module, the cartridge removal tool including a tool body having downwardly facing wings that engage a catch on a chassis of the payment module to detach a cartridge from the chassis.

[0086] In one embodiment the tool body includes a flat front underside and an upwardly sloping rear underside.

[0087] In one embodiment the downwardly extending wings are provided proximate a front of the tool body but laterally spaced therefrom.

[0088] In one embodiment the tool body includes lateral tabs extending outwardly from sides of the body to support the downwardly extending wings.

[0089] In one embodiment the tabs support L-shaped guides extending downwardly and outwardly from the tabs, rearwardly and outwardly of the wings.

[0090] In one broad form, an aspect of the present invention seeks to provide a method of using a cartridge removal tool to remove cartridges from a payment module, the cartridge removal tool including a body having downwardly facing wings that engage a catch on a chassis of the payment module to detach a cartridge from the chassis and the method including positioning the cartridge removal tool on an upper surface of a cartridge, and urging the wings into engagement with a catch to thereby release the cartridge.

- 14 -

[0091] In one embodiment the tool body is positioned on a top surface of a cartridge, with a sloped rear underside flush against the top of the cartridge, with the tool body being pushed forwardly until the wings are in position to release the catch.

[0092] In one embodiment the tool body is pushed forwardly until tabs engage or are aligned with side walls of the payment module.

[0093] In one embodiment the tool body is rotated so that a flat underside of the tool body lies flat against an upper surface of the cartridge so that the wings engage a catch and release the cartridge.

[0094] In one embodiment the tool is urged rearwardly so that the wings engage a mounting pin of the cartridge allowing the mounting pin to be lifted from within a channel thereby releasing the cartridge.

[0095] It will be appreciated that the broad forms of the invention and their respective features can be used in conjunction and/or independently, and reference to separate broad forms is not intended to be limiting. Furthermore, it will be appreciated that features of the method can be performed using the system or apparatus and that features of the system or apparatus can be implemented using the method.

Brief Description of the Drawings

[0096] Various examples and embodiments of the present invention will now be described with reference to the accompanying drawings, in which: -

[0097] Figure 1A is a schematic diagram of an example of a payment terminal;

[0098] Figure 1B is a schematic diagram of an example of a currency container;

[0099] Figure 2 is a flow chart of an example of a payment process;

[0100] Figure 3 is a schematic diagram of an example of a payment system architecture;

[0101] Figure 4A is a schematic front left perspective view of a first example of a payment terminal;

[0102] Figure 4B is a schematic front right perspective view of the payment terminal of Figure 4A;

[0103] Figure 4C is a schematic rear left perspective view of the payment terminal of Figure 4A;

[0104] Figure 4D is a schematic rear left perspective view of the payment terminal of Figure 4A with a currency container partially removed;

[0105] Figure 5A is a schematic front view of a second example of a payment terminal;

[0106] Figure 5B is a schematic front left perspective view of the payment terminal of Figure 5A;

[0107] Figure 5C is a schematic front left top perspective view of the payment terminal of Figure 5A with a currency container partially removed;

[0108] Figure 6A is a schematic front view of an example of a currency container;

[0109] Figure 6B is a schematic top side perspective view of the currency container of Figure 6A;

[0110] Figure 6C is a schematic underside perspective view of the currency container of Figure 6A;

[0111] Figure 7 is a schematic diagram of components of a currency container;

[0112] Figure 8 is a schematic diagram of an example of components of a payment terminal;

[0113] Figure 9 is a schematic diagram of an example of a POS terminal;

[0114] Figure 10 is a schematic diagram of an example of a processing system;

[0115] Figure 11 is a schematic diagram of an example of a client device;

[0116] Figures 12A to 12C are a flow chart of an example of a payment process;

[0117] Figure 13 is a flow chart of an example of a process of inserting a currency container into a payment terminal; and,

[0118] Figures 14A and 14B are a flow chart of an example of process of ejecting and transporting a currency container;

[0119] Figure 15 is a flowchart of a tamper detection process;

[0120] Figure 16 is a flowchart of an example of an operational status monitoring process;

[0121] Figure 17A is a schematic cross sectional side view of a first example of a currency container and feeder outlet with the feeder outlet in a retracted position;

[0122] Figure 17B is a schematic cross sectional side view of the currency container and feeder outlet of Figure 17A with the feeder outlet in a dispensing position;

[0123] Figure 17C is a schematic plan view of the currency container and feeder outlet of Figure 17A with the feeder outlet in a retracted position;

[0124] Figure 17D is a schematic plan view of the currency container and feeder outlet of Figure 17A with the feeder outlet in a dispensing position;

[0125] Figure 17E is a schematic cross sectional side view of a second example of a currency container and feeder outlet with the feeder outlet in a retracted position;

[0126] Figure 17F is a schematic cross sectional side view of the currency container and feeder outlet of Figure 17E with the feeder outlet in a dispensing position;

[0127] Figure 18A is a schematic side view of an example of a payment module;

[0128] Figure 18B is a schematic plan view of the payment module of Figure 18A;

[0129] Figure 18C is a schematic end view of the payment module of Figure 18A;

[0130] Figure 19A is a schematic plan view of an example of a cartridge removal tool;

[0131] Figure 19B is a schematic end view of the cartridge removal tool of Figure 19A;

[0132] Figure 19C is a schematic side view of the cartridge removal tool of Figure 19A;

[0133] Figures 20A and 20B are schematic side views showing operation of the cartridge removal tool of Figure 19A; and,

[0134] Figures 20C and 20D are schematic end views showing operation of the cartridge removal tool of Figure 19A.

Detailed Description of the Preferred Embodiments

[0135] An example of a system for processing a payment for a transaction will now be described with reference to Figures 1A and 1B, which show a payment terminal and a currency container, respectively.

[0136] For the purpose of the following explanation, the term "currency" will be understood to refer primarily to cash in the form of notes and/or coins, as well as other forms of currency such as crypto-currencies, or similar. However, it will be appreciated that the techniques described herein could be applied more broadly to other security documents, including but not limited to tokens, gambling chips, cheques, vouchers, or the like.

[0137] Additionally, whilst reference is made to a currency container, in practice the currency container could be used to contain and optionally transport any form of security documents. Thus, when used in conjunction with the payment terminal, the document container is typically used to transport currency and is referred to as a "currency container", but it will be appreciated, that the terms "currency container" and "document container" should be considered as largely interchangeable, and that the features of a document container and currency container would be substantially identical.

[0138] In this instance, the payment terminal shown in Figure 1A includes a housing 110 including a container cavity 120 that, in use, receives a currency container 190. The container cavity 120 is defined by an internal wall 121 having an opening 122 to allow currency to be dispensed into the container cavity.

[0139] The housing 110 includes a currency input 111 which may be in the form of an aperture, slot, opening, draw, or other suitable receptacle, which can receive currency, either in the form of notes and/or coins, depending upon the preferred implementation.

[0140] The payment terminal includes a currency transport system 131 that transports currency from the currency input 111 to an opening 121 in the container cavity 120 that allows currency to be dispensed into the currency container 190. It will be appreciated that the nature of the currency transport system will vary depending upon the nature of the currency and the preferred implementation. For example, in the case of coins, the currency transport system could simply include a chute, or similar, which allows coins to slide from the currency input 111 to the opening 121. In the case of notes, the note transport system is typically a driven system including rollers extending along a transport path, which urge the notes from the currency input 111 to the opening 121. It will be appreciated however, that other suitable arrangements could be used, and as such currency transport systems are well known these will not be described in further detail.

[0141] The payment terminal further includes one or more payment modules, with a variety of different payment modules optionally being provided. The nature of the modules will vary depending on the preferred implementation and the nature of payments to be processed. For example, the modules could include modules that are able to process credit/debit card payments, detect and process vouchers or cheques, processing crypto currency payments, or the like.

[0142] Typically, the system will include at least one currency module 140 having a currency sensor 141 that senses currency transported by the transport system 131 and operates to determine a currency value, such as a denomination of individual notes or coins. The nature of the currency sensor 141 will vary depending upon the nature of the currency and the

preferred implementation. For example, in the case that the currency includes notes, the currency sensor could include a note reader, which operates to scan the note and detect physical characteristics of the note including a note size, shape, colouration, presence or absence of security features, or the like. In the case of coins, the sensor could include an imaging device, which images the coin to detect the size, shape and surface markings on the coins, and/or could include a weight measuring device that measures a weight of the coins. Suitable currency modules and their associated sensors are well known, and indeed in one example, the currency module may be formed from commercially available currency modules, and the operation of these will not therefore be described in any detail.

[0143] It will also be noted that the payment module could be integrated into, or could form part of, the transport system. Thus, the payment module may include an input that receives the currency and is aligned with the currency input 111 allowing currency to be detected as it is inserted into the payment terminal, with an output of the payment module 140 cooperating with the transport mechanism 131 to transport to the currency to the container cavity 120.

[0144] The payment terminal also includes one or more electronic terminal processing devices 150. The electronic processing devices may be in the forms of microprocessors, or the like. The terminal processing devices 150 could be any electronic processing device such as a microprocessor, microchip processor, logic gate configuration, firmware optionally associated with implementing logic such as an FPGA (Field Programmable Gate Array), or any other electronic device, system or arrangement. The terminal processing devices 150 execute instructions to control operation of the payment terminal and optionally communicate with currency container. For ease of illustration the remaining description will make reference to a processing device, but it will be appreciated that multiple processing devices could be used, with processing distributed between the devices as needed, and that reference to the singular encompasses the plural arrangement. It will also be appreciated that the functionality of the terminal processing devices could be implemented using hardware, software, firmware, or a combination of the above, and the particular form is not intended to be limiting.

[0145] The payment terminal also typically includes one or more terminal memories 151, which could include volatile and/or non-volatile memories, and which may be used for storing control instructions in the form of applications software, firmware, or the like, as well as storing data relating to operation of the payment terminal, such as records of payments processed. The payment terminal includes a terminal communications interface 152, which can be used to allow for wired and/or wireless communications either directly with another device or via an intervening communications network. Although a single communications module is shown, this is for the purpose of example only, and in practice multiple interfaces using various methods (eg. Ethernet, serial, USB, wireless, 3G, 4G, 5G, cellular communications, or the like) may be provided.

[0146] An example of a currency container for receiving currency and/or other security documents will now be described with reference to Figure 1B.

[0147] In this instance, the container 190 includes a container housing 190.1 defining a container internal cavity 190.2. The container includes a lid 190.3 which can be selectively opened or closed to provide access to or seal the container cavity. The lid can be hingeably or slideably mounted to the container housing 190 and it will be appreciated that other various arrangements could be used.

[0148] A securing mechanism 196 is provided that allows the lid to be secured in at least the closed position. The nature of the securing mechanism will vary depending upon the preferred implementation and this could include a locking mechanism and/or an actuator, which allows the lid to move between open and closed positions solely through operation of the actuator.

[0149] The container 190 includes one or more container electronic processing devices 191. The electronic processing devices may be in the forms of microprocessors, or the like. The container processing devices 191 could be any electronic processing device such as a microprocessor, microchip processor, logic gate configuration, firmware optionally associated with implementing logic such as an FPGA (Field Programmable Gate Array), or any other electronic device, system or arrangement. The processing devices 191 execute

instructions to control operation of the currency container, for example to operate the securing mechanism, and optionally communicate with payment terminal to determine an amount of currency or other documents stored therein. For ease of illustration the remaining description will make reference to a processing device, but it will be appreciated that multiple processing devices could be used, with processing distributed between the devices as needed, and that reference to the singular encompasses the plural arrangement. It will also be appreciated that the functionality of the container processing devices could be implemented using hardware, software, firmware, or a combination of the above, and the particular form is not intended to be limiting.

[0150] The container 190 also typically includes one or more container memories 192, which could include volatile and/or non-volatile memories, and which may be used for storing a range of different data. In one example, this is used to store a container identifier, which can be used to identify the particular container into which currency is dispensed, or other documents stored. Additionally and/or alternatively, the container memory 192 could be used to store data indicative of currency or other documents stored in the container. The container memories 192 can also be used to store instructions in the form of applications software, firmware, or the like, as well as storing data relating to operation of the payment terminal, such as records of payments processed.

[0151] The currency container 190 also includes a container communications interface 193, which can be used to allow for wired and/or wireless communications either directly with another device, such as the payment terminal, or another processing system, such as a computer system, via an intervening communications network. Although a single communications module is shown, this is for the purpose of example only, and in practice multiple interfaces using various methods (eg. Ethernet, serial, USB, wireless, 3G, 4G, 5G, cellular communications, or the like) may be provided.

[0152] It will be appreciated that the pre-fixes "terminal" and "container" with reference to the memory, communications module and processing device are used to distinguish between the memory, communications module and processing device in the container and payment terminal respectively and these are not otherwise intended to be limiting.

[0153] Operation of the payment terminal and currency container will now be described with reference to Figure 2.

[0154] At step 200 a transaction amount is determined. This can be achieved in any suitable manner, depending on the preferred implementation. In one example, the one or more terminal processing devices 150 obtain transaction data indicative of a transaction performed using a transaction terminal, and use this to determine the transaction amount. Alternatively, however details of the transaction, and in particular a transaction amount, could be entered manually by a user, such as a merchant, cashier, or customer.

[0155] At step 210, the one or more terminal processing devices determine a payment amount received from the payment module 140. In particular, the payment module 140 receives currency and detects denominations of individual notes or coins using the currency sensor 141, using this to determine a total amount of currency received. As the currency is provided, at step 220 the terminal processing device(s) 150 cause the currency to be dispensed into the currency container via the transport mechanism 131. Whilst in most cases all currency will be dispensed into the currency container, in some instances some of the currency may be diverted to a float for use in providing change or cash back, although this is not necessarily required, as will be described in more detail below.

[0156] At step 230, the terminal processing devices 150 cause payment data to be stored. The payment data typically includes an indication of the transaction amount, payment amount, an amount of currency dispensed into the currency container and/or a container identifier indicative of an identity of the currency container. This allows details of the transaction and/or payment to be subsequently reviewed, for example for the purpose of tracking the container and associated currency, transaction monitoring, monitoring compliance with transaction rules, or the like.

[0157] The payment data could be stored in any suitable data store, such as a memory, database, or the like. In a preferred example the payment data are stored remotely, for example as part of a cloud based, or other remote storage facility, allowing the records to be accessed as required, using a computer system, client device, or the like. In one particular

example, the payment data can be stored in an unmodifiable manner, allowing this to act as an absolute record of the currency stored in the container, hence ensuring currency is not fraudulently removed from the currency container. In one example, the payment data is stored as part of a blockchain, although it will be appreciated that other data stores could be used.

[0158] It will also be appreciated that whilst the above described process stores payment data, the system is not so limited, and could additionally store further information. In one example, this could include any data relating to the transaction process, and could include transaction details, payment details, including details of currency scanned and the time and date on which this occurred, or the like. Such information can be used for logging transactions and payments, allowing these to be subsequently reviewed, for example for auditing, compliance monitoring, analysing business operation, or the like.

[0159] Accordingly, the above-described system operates to receive currency and uses a payment module including a sensor, such as a note reader, coin detector, or the like, in order to determine an amount of currency that has been received. The currency is dispensed into a container provided within the payment terminal, whilst an indication of the amount of currency dispensed into the container is stored so that this can be subsequently used for a variety of purposes, such as tracking currency and/or monitoring payments. In one example, the container further includes a lid that can be secured in a closed position, to thereby secure the currency within the container, allowing this to be used to transport the currency, although it will be appreciated that other forms of currency container could be used in conjunction with the payment terminal.

[0160] In any event, this provides a mechanism for cash payments to be collected, with the cash payment being dispensed directly into an optionally secure currency container for storage. Payment data is stored allowing this to act as a record of the transaction performed, the payment received and/or the currency stored in the currency container, allowing this to be utilised for tracking of the currency.

[0161] In one example, this allows the currency container to be removed from the payment terminal and transported directly to a financial institution, such as a banking facility, or the like, to allow the currency to be deposited into a relevant financial account. In particular, the financial institution can use the payment data to identify the currency stored within the currency container. This can be used to verify the contents of the container and ensure that the contents of the container have not been tampered with, for example to prevent unauthorised removal of currency from the container.

[0162] In one particular example, remote access to the payment data can be provided, for example by allowing this to be uploaded to a remote computer system, such as a server, enabling funds to be deposited into a bank account. This can be performed without requiring access to the container and could be performed based on other factors, such as a location of the container. In this instance, when the container is received by a banking facility or similar, funds can be credited to an account of the merchant without requiring that the currency is actually removed from the container, which can then be done at a later time depending on the availability of processing capabilities or personnel.

[0163] Accordingly, the above described system provides a mechanism for securely collecting currency, and in particular cash in the form of notes or coins, to allow for payment to be made in respect of a transaction. The device can be used with existing transaction terminals, such as point of sales terminals, and can be used to allow an alternative payment mechanism to be implemented or allow the burden on existing cashiers to be reduced, thereby making cash payments easier to perform.

[0164] Additionally, the payment terminal can be used in transaction monitoring, and in one particular example for compliance monitoring, for example to ensure compliance with one or more transaction rules. In this regard, the payment data can be retrieved and then compared to transaction rules, allowing breaches in rules to be identified, as well as allowing the payment data to be analysed, for example to monitor patterns in transactions, business performance or the like.

[0165] Whilst the payment data could be stored in any suitable data store, in a preferred example the payment data are stored as part of a remote data store, such as a database, blockchain, or the like. For example, the distributed and encoded nature of the blockchain can be used to prevent transaction details that have been added to the blockchain from being subsequently altered. This, in turn, allows these to act as an absolute record of the transaction, enabling these to provide immutable evidence of the transaction, hence ensuring compliance monitoring can be performed accurately.

[0166] It will also be appreciated that there are a number of different blockchain implementations, each of which is implemented in a different manner. For example, blockchains can be public or private, or hybrids, and may include one node or multiple nodes, depending on the preferred implementation. In one example, the preferred blockchain implementation may be a private blockchain and may hash the contents of a single transaction, a block or a series of blocks. In a further example, the particular implementation is based on the Hyperledger blockchain, and in one particular example, Hyperledger Fabric blockchain. However, it will be appreciated that this is not intended to be limiting and any suitable implementation might be used.

[0167] Furthermore, whilst blockchain is a particular preferred example that can be used for storing the transaction details, it will be appreciated that any technique could be used which provides immutability to the content to allow this to be used for auditing or other purposes. Accordingly, it will be appreciated that other storage techniques could be used, such as more general distributed and/or encrypted storage.

[0168] Additionally, the transaction details could be stored in any suitable format. In one example, the transaction details are stored in the form of details extracted from the transaction data. However, this is not essential, and the transaction details could additionally and/or alternatively be stored by storing the transaction data. In one example, this could include storing print data generated by the transaction terminal, which can help provide further evidence of the transaction that was performed, and in particular, prove that the transaction details accurately reflect the transaction that was performed. It will also be

appreciated that transaction details could be stored in multiple formats, including in raw and/or altered formats.

[0169] In a further example, the transaction details could be stored in different data stores. For example, a blockchain is not ideal for storing large volumes of data, but is ideally suited for storing data in an immutable form. Accordingly, in one example, transaction details, optionally including the transaction data, can be stored in a remote data store such as a database. Verification data, such as a hash or digital signature derived from the transaction details are then stored in a blockchain or similar immutable data store. In this instance, the verification data can then be retrieved from the blockchain and compared to the transaction data to later verify that the transaction data is legitimate and has not been altered.

[0170] In any event, in one example, the above described arrangement provides a mechanism for transaction monitoring which operates by automatically collecting payment and/or transaction details and storing these in a blockchain or other suitable remote data store to ensure that the payment or transaction details accurately represent the payments or transactions that have been performed and cannot be subsequently altered. This removes the burden on entities involved in the transaction from having to collect and store transaction details themselves, facilitating the collection process, whilst ensuring that collected details cannot be subsequently altered.

[0171] Furthermore, this can be achieved through the use of a payment terminal, which can intercept transaction data being transmitted via a communications network, enabling this to be implemented by attaching the payment terminal to the network and performing some minor installation steps, such as configuring the payment terminal to act as a proxy for network enabled devices, such as printers. This avoids the need for modification of existing transaction terminals, and allows transaction terminals to operate in a substantially existing manner whilst enabling the transaction data to be easily collected. Accordingly, this allows the compliance monitoring process can be easily implemented at a wide range of different facilities.

[0172] It will therefore be appreciated that the above described arrangement can also enable transaction details to be automatically captured and stored in an unmodifiable manner, making this ideal for use in monitoring compliance with transaction rules, such as taxation rules, or the like.

[0173] A number of further features will now be described.

[0174] In one example, the payment terminal determines a container identifier that is indicative of an identity of the currency container. In this regard, it is useful to be able to track the currency container into which currency is dispensed, so each currency container has a unique identifier, which could be defined in any one of a number of ways depending on the preferred implementation. In one example, the container identifier is stored in container memory 192, with the one or more terminal processing devices 150 obtaining the container identifier by communicating with the container processing devices 192, which retrieves the container identifier from the container memory 192. Alternatively, the container identifier could be encoded on the container as machine readable coded data, allowing the payment terminal to sense the container identifier using a suitable sensor, such as an RFID (Radio-frequency Identification) sensor, barcode reader, or the like. As a further alternative, the container identifier could be presented visually, allowing this to be entered manually by a user, such as a merchant, cashier, or customer, via a user interface.

[0175] This process is typically performed at least when the currency container 190 is initially inserted into the payment terminal, allowing the location of and interactions with the currency container to be constantly monitored. However, this is not essential and could be performed later, on a daily or periodic basis, when the payment terminal is activated, prior to ejection of the currency container, or the like. Irrespective of how this is performed, the container identifier can be associated with details of the currency stored in the currency container to assist in tracking of currency.

[0176] In one example, the payment terminal includes a display that displays at least one of a transaction amount, transaction details and/or a received payment amount. This allows a user to check the amount that is due to be paid for the transaction, and also see how much has

been received, thereby facilitating the transaction process. It will be appreciated that in some circumstances the payment machine may also be adapted to return change based on a difference between a payment amount and a transaction amount, in which case a change amount may also be displayed. Further information that could be displayed, which includes, but is not limited to, information regarding an identity of a user, a merchant and/or a cashier, available options, such as selecting between payment mechanisms, or the like.

[0177] Whilst a single display may be provided, in other examples, the payment terminal includes first and second displays that in use display information to a merchant and customer respectively, although this is not essential.

[0178] The payment terminal typically includes a user input that receives user input commands. In one example, the user input is in the form of a touchscreen display but it will be appreciated that this is not essential and any other suitable form of user input, such as input buttons, could be provided.

[0179] In one example, the payment terminal includes a lock that secures the currency container within the container cavity. This prevents the currency container being removed from the payment terminal without authorisation. The manner in which this is achieved will vary depending upon the preferred implementation. In one example, the lock includes a solenoid lock which can be adapted to engage either the currency container directly and/or a door to the container cavity. It will be appreciated, however, that other suitable arrangements could be used and this is not intended to be limiting.

[0180] In one example, the one or more container processing devices receive currency data from the one or more terminal processing devices and store the currency data in the container memory. This can be used to provide a further mechanism for storing data relating to dispensed currency, separate to storing as part of the payment data. This can be useful for independent verification, or to act as a fall back in case there are issues with the payment data. It will also be appreciated that in a similar manner payment data can additionally and/or alternatively be stored in the container memory.

[0181] In one example, the container processing devices 191 can be adapted to receive a currency data request from a processing system, such as a remote computer system, and in response to the request, retrieve currency data, and optionally a currency container identifier, from the container memory 192 and then provide the currency data to the processing system. The processing system can be a remote computer system, such as a remote server, and/or could be provided locally to the currency container. For example, the computer system could form part of a banking network infrastructure which operates to retrieve currency data from the container memory when the currency container is delivered to a banking facility or similar. It will also be appreciated that the computer system could form part of the payment terminal itself allowing the payment terminal to retrieve currency data from the currency container, for example for auditing purposes.

[0182] In one example, the container processing device 191 receive requests via the container communications interface 193 and then control the securing mechanism 196 in accordance with the request, to thereby selectively open or close the lid to provide access to the container internal cavity 190.2. The requests can be received from the terminal processing device, with this being used to control opening or closing of the lid upon insertion of, or removal of, the container 190 from the container cavity 120. It will be appreciated, however, that the request could also be received from other remote computer systems, such as processing systems provided at a banking facility, to thereby provide access to the container cavity to allow the currency to be removed therefrom when the container reaches an intended destination.

[0183] In one example, the currency container includes a reader that is used to determine a user identity, with this then being used by the container processing devices 191 to either store the user identifier in the memory 192, authenticate the user at least in part utilising the user identity, or selectively perform actions based on permissions associated with the user identity. The nature of the reader and the user identifier can vary depending on the preferred implementation. In one example, the user identifier is associated with an identification device, such as an RFID tag, which may be provided as part of a wearable device, such as a bracelet or watch, or could be provided in a swipe card, or similar. Alternatively however,

the reader could be a biometric reader that determines a user identity based on biometric information. In a further example two-factor authentication could be used. For example this could involve entering a PIN into a smartcard, such as a smartcard similar to that described in US20140330726, the contents of which are incorporated herein by cross reference. The card validates the PIN, which this then being detected by a reader on the payment terminal, which reads the card to confirm the PIN has been validated, thereby authenticating the user. Thus, in this instance the user is authenticated both through the presence of the smartcard, and also knowledge of the PIN, which is required to unlock the smart card. It will be appreciated that that other two factor techniques could be used, and this example is for the purpose of illustration only. Irrespective of how this is performed, this allows an individual interacting with the currency container to be uniquely identified, with this information being stored in the memory to track individuals that interact with the container. Such interactions can include transporting a container and/or opening the container to remove currency. As part of this process, the user may undergo authentication and/or may have their identity checked against permissions, in order to validate that the user has permission to perform the necessary interaction. For example, if a user wishes to open the currency container, a request can be submitted via a processing system, with the user's identity being validated to ensure that the user has permission to open the currency container before this occurs.

[0184] In one example, the one or more container processing devices 191 can determine a container status and then either record an indication of the container status in the container memory 192 and/or periodically broadcast an indication of the container status, optionally together with other information, such as a currency container identifier, to a remote computer or processing system via the container communications interface 193. The nature of the container status can vary depending on the preferred implementation and this could include information such as details of a last known location, details of a current user with whom the currency container is currently associated, details of attempted tamper events or the like. This information can be broadcast periodically so that an up-to-date indication of the container can be determined remotely to enable this to be used in tracking of the container and hence the container contents.

[0185] Accordingly, in one example, the currency container includes a location tracking module, such as GPS module, that tracks the location of the currency container, with the container status including an indication of the location.

[0186] Similarly, the currency container can include at least one container tamper sensor, with the one or more container processing devices operating to monitor changes in signals from the container tamper sensors to detect tamper events. Details of the tamper events can be incorporated into the container status and/or could be used to cause an alert notification to be generated. This could include activating a siren or transferring an alert to a remote computer system or similar. The nature of the tamper sensors and the changes identified will vary depending upon the preferred implementation. For example, the tamper sensors could include accelerometer and/or position sensors which are used to detect attempts to move and/or damage the currency container through the application of external force. Additionally, the sensors could include any one or more of a temperature sensor, an air pressure sensor, a light sensor or humidity sensor, which can be used to detect changes in the container cavity environment, which are in turn indicative of attempts to open the housing. For example, a light sensor can be used to detect increase in ambient illumination within the container cavity whilst the temperature, pressure and humidity sensors can detect changes in temperature, air pressure and humidity respectively.

[0187] It will be appreciated that in the event attempts are detected to tamper with the container, status updates may be performed more frequently, for example by increasing frequency of communication with a remote processing system to thereby facilitate tracking of the container.

[0188] Whilst any form of securing mechanism, such as a lock, could be used, in one example the securing mechanism is in the form of an actuator including a drive, such as a worm drive. In this example, the container processing device 191 can selectively activate the container drive to thereby open or close the lid, allowing the lid to be opened by communicating with the container processing device 191. This can be used to open or close the container lid when the container is positioned within the payment terminal, which in turn

reduces the opportunity for individuals to access the contents of the container when the container is removed from the payment terminal.

[0189] As previously mentioned, the container processing device 191 can store information in container memory 192, such as currency data. The container memory 192 can also be used to store additional information such as a container status, tamper events, received requests, details of actions performed, a processing device identifier associated with a payment terminal, user identities of detected users, or the like. This can be used to track events for auditing purposes, including details of users interactions with the currency container, which in turn helps ensure security is maintained.

[0190] The currency container typically includes an inductively charged battery in order to power internal electronics. In this example, the payment terminal can include an inductive power transmitter positioned adjacent the container cavity 120, allowing the currency container to include an inductive power receiver so that the battery can be inductively charged when the currency container is contained within the payment terminal. This ensures that the currency container is fully charged prior to the currency container being removed from the payment terminal, enabling this to be used in tracking the container as it is transported to an off-site location such as a banking facility, or similar. This can also be used to inductively power the container electronics directly when the container is inserted into a payment terminal.

[0191] It will also be appreciated that charging could be performed at other locations. For example, a banking facility may include a storage arrangement, such as a vault or other repository, which is configured to receive and store containers. In one example, this can be used to receive containers when these are being returned, for example for depositing cash, with the vault storing the containers until the containers can be opened and the contents removed. In this instance, the vault can include individual receptacles for containers, with these optionally being similar in form to, and incorporating some or all of the functionality of the payment terminal cavity. In this instance, this allows containers to be charged as well as allowing the vault to communicate with the containers, for example to determine a container identifier, and hence confirm receipt of the respective container, and retrieve corresponding

payment data. Thus, this enables receipt of the container contents to be confirmed in advance of the container being opened.

[0192] The payment terminal and currency containers can include first and second interfaces to allow for more secure communication. In one particular example, a first interface is used to exchange communications information, with the second interface being used to provide a secure communication channel between the payment terminal and the currency converter using the communications information. The communications information could be of any appropriate form and could include an identifier associated with the second communications interface, a password, an encryption key, or the like. In one particular example, the first interface is a Near-Field Communication (NFC) interface, although other short range communications interfaces, such as Bluetooth or the like, could be used. The first interface is utilised to both detect the presence of the currency container 190 within the container cavity 120, and also to exchange a Wi-Fi network identifier and password so that this can be used to establish Wi-Fi communication between the currency container 190 and the payment terminal 120 using the second communications interface, to thereby allow currency data and other data, such as the container identifier, to be exchanged. Again, it will be appreciated that other communications interfaces could be used for the second interface.

[0193] In one example, the payment terminal can be used to activate release of the currency container. In this instance, the terminal processing device 150 typically determine the currency containers to be released in accordance with user input commands indicative of a container release request, which could be achieved selecting an appropriate option presented via a touch screen, or the like. The terminal processing device 150 then typically generates a close container request, which is transferred to the currency container, so that the container processing device 191 can activate the securing mechanism 196 to thereby secure the lid 190.3. The terminal processing device 150 then generates a lid closed response, which is transferred to the payment terminal, so that the terminal processing device 150 can confirm the lid 190.3 has been closed. Once this has been done, the payment terminal can activate the lock and thereby release the currency container. The payment terminal can additionally and/or alternatively confirm the lid 190.3 is closed using an inbuilt lid sensor, positioned

adjacent the container cavity 120. It is also possible to detect lid opening and closing, as well as jams or other fault issues based on operation of the lid drive motor. For example, if the current drawn by the motor increases, this corresponds to an increase in motor power, which in turn can indicate a blockage or other issues.

[0194] A similar process can be performed in order to open the container lid 190.3 upon insertion of the currency container 190 into the container cavity 120. In this instance, the terminal processing device 150 detects the presence of a currency container using the first communications interface, selectively activates a lock to thereby secure the currency container 190 within the cavity 120, and generates an open container request, which is transferred to the currency container. The container processing device 191 is responsive to the open container request to activate a securing mechanism to thereby open the lid 190.3. Following this, one or more processing devices can determine the lid has been opened, using either a lid open response received from the currency container or signals from a lid sensor, and then activate the currency payment module 140, allowing payments to be received.

[0195] During insertion of the container, the payment terminal may also operate to determine a currency container identifier from the one or more container processing devices and then store the currency container identifier in the terminal memory. This can be used to maintain a history of currency containers that have received currency from the payment terminal, which can in turn help with tracking currency, for example in the event that currency is mislaid, paid into an incorrect bank account, or the like.

[0196] As previously mentioned, the payment modules could include a coin currency module including a coin sensor that senses coins or a note currency module including a note sensor that senses notes. However, it will be appreciated that other modules could be provided, such as a card module including a card reader that reads payment cards, a cheque processing module, a voucher reading module, a crypto-currency processing module, or the like.

[0197] In one particular example, the payment terminal includes a plurality of payment modules, with the terminal processing device 150 causing a display to display a number of payment options, determine a selected payment option in accordance with user input

commands and selectively activate one or more of the payment modules in accordance with the user input commands.

[0198] The payment module 140 can use signals from the currency sensors 141 to authenticate/validate the received currency, for example by checking characteristics of the currency against a database of known characteristics. This can include checking features of shape, colour, pattern, security features, or the like, which can be used to identify counterfeit currency, which can then be rejected.

[0199] In one example, the payment module(s) can include a currency input, a currency validator to validate received currency and a currency outlet. In this regard, the payment modules can be self-contained modules, and may be supplied by an external supplier. For example, a payment module to process note or paper based currency could include a Suzohapp SBB-120 Bill-to-Bill Currency Management System, although it will be appreciated that other suitable payment modules could be used.

[0200] In one embodiment, one or more of the payment modules can be removably mounted within the housing. This allows the payment modules to be removed and replaced if required. As many payment modules include currency stores that can operate as float storage, this also allows the payment module to be removed from the payment terminal, allowing float to be removed from the terminal, for example if the terminal is stored unsupervised outside of business hours. As some payment modules are quite heavy, however, removal of the entire module can be undesirable as this can be inconvenient, and could lead to the potential for injury to users. However, in many cases, the currency store includes a plurality of cartridges, with each cartridge being configured to store a respective denomination of currency. In this example, the cartridges are typically removably mounted to a chassis, in which case, the payment terminal housing can include a door to allow cartridges to be removed from the housing. In some instances, a cartridge removal tool can be provided, which includes a body having downwardly facing wings that engage a catch on the chassis to detach the cartridges from the chassis, and thereby facilitate removal of the cartridges and hence float.

[0201] In this regard, the transport system 131 typically includes an outlet path that transfers currency to an outlet, for example to return invalid currency (which may alternatively be returned via the inlet) and/or provide change. This can also be used to provide cash-out for credit/debit card transactions. A float path is also provided that transfers currency to or from a float storage, allowing float to be used to deliver change via the outlet. In this instance, a float dump path can be provided that selectively transfers currency from the float storage to the currency container. Thus it will be appreciated that currency can not only be transferred from the currency input to the currency container, but can also be diverted to an outlet in the event that the currency is deemed invalid or counterfeit, or could be diverted to a float. The float can be used to store a predetermined amount of currency, optionally of different denominations, within the payment terminal, which can then be used in order to allow change to be issued.

[0202] The transport system 131 is typically controlled by the terminal processing device 150, with this performed in accordance with user input commands, signals from the payment module and/or instructions stored in memory. Thus, for example, instructions stored in memory could define a predetermined amount of float that is to be maintained in other float storage. In this instance, when a payment is received, the processing devices can retrieve a current float balance and a target float level from memory. A float deficit can then be determined, which could be a deficit of an amount or a particular denomination, with the transport system then being controlled based on the float deficit, to replenish the float as needed. Any currency not required to replenish the float can then be transferred to the currency container in the normal way. The float level could be pre-set, but more typically can be set and/or adjusted by a user, such as a merchant or cashier, to ensure there is sufficient float to meet the requirements of the business.

[0203] Additionally, the terminal processing device 150 can be used trigger dumping of some or all of the float into the currency container. This may be performed for example at the end of the day, or periodically during the day, when it is desired to remove currency containers and return these to a banking facility or similar. In this instance, the one or more processing devices can determine a float dump request in accordance with user input

commands and then control the transport system to cause float to be dispensed in to the currency container.

[0204] It will be appreciated that operation of the float, and in particular, the target float level, can be performed automatically and/or could be set or adjusted in accordance with user input commands. Similarly, a float dump request could be automated, for example occurring at a pre-set time each day.

[0205] In one example, the transport system includes a feeder outlet that dispenses currency through the opening in the container cavity to thereby dispense currency, such as notes, into the currency container. The feeder outlet can be of any appropriate form depending on the nature of the currency being dispensed, and could include a ramp for dispensing coins, or could include a note feeder for dispensing notes, or similar.

[0206] In one example, the feeder outlet is movably mounted within the housing to allow the feeder outlet to move between a dispensing position, in which the feeder outlet projects through the opening in the container cavity and a retracted position in which the feeder outlet is retracted from the opening in the container cavity. This is typically facilitated by an outlet actuator that moves the feeder outlet between the dispensing and retracted position. This ensures that notes and/or coins are accurately dispensed into the container, and can also facilitate directing currency into the container, for example, ensuring notes do not bundle up and block the opening.

[0207] In one example, the terminal processing device 150 determines a user request in accordance with user input commands, determines a user identity of the user making the request, uses the user identity to either authenticate the user or determine permissions associated with the user and then selectively performs an operation depending on the results of the authentication and/or user permissions. In this regard, certain actions such as removing the currency container may only be allowed in the event that the user has permission to do so. The user identity could be determined in any one of a number of ways and could include having the user enter identity information, such as a username and/or password via a user interface, or could include using a reader such as biometric reader or

identifier reader to determine the user identity either from biometric information or from an identification device such as an RFID enabled device, such as a bracelet or watch, smartcard, or the like. In a further example two-factor authentication could be used, for example requiring the user to enter a PIN to unlock a smart card, with this being provided to the terminal processing device as part of an authentication process.

[0208] As previously mentioned, a transaction amount may be input manually by a user. In other examples however, the payment terminal obtains transaction data indicative of a transaction performed from a transaction terminal and determines the transaction amount from the transaction data. The manner in which this is achieved will vary depending upon the preferred implementation and the format of the transaction data. For example, the transaction data may be in a structured file format, such as a mark-up language, or XML file and may include tags or headers identifying particular transaction details, such as payment amounts, VAT, GST, or the like. In this case, the relevant transaction details and, in particular the payment amount, can be easily extracted from the transaction data. More typically, however, the transaction data is print data in which case the payment terminal may need to examine the print data and extract transaction details therefrom using scraping or other similar techniques, as will be described in more detail below.

[0209] In one particular example, transaction data is obtained by intercepting transaction data on a communications network, with the transaction data being intercepted as the transaction data is transferred from the transaction terminal to a network enabled device. This arrangement is particularly advantageous as many POS terminals are configured to automatically print receipts to network enable devices, such as printers. In this instance, the payment terminal can intercept such transmissions and thereby automatically determine transaction data without requiring modification of existing payment infrastructure. This allows the payment terminal to be readily integrated into existing POS environments, without requiring complex integration processes.

[0210] In this instance, the transaction terminal could intercept communications via Bluetooth, Wi-Fi, USB, or other forms of connectivity depending upon the preferred implementation. In one preferred example, the payment terminal can receive network traffic

directed to the network enabled device, determine transaction details if the network traffic includes transaction data and then forward the network traffic to the network enabled device. This enables the network enabled device to continue to function normally. However, this is not essential, and alternatively, the payment terminal may generate modified transaction data, for example to add details of the payment received, with this being transferred to the network enabled device for actioning.

[0211] In one example, the payment terminal can be configured in accordance with network addresses of each of the network enabled devices. Thus, the payment terminal can act as a proxy for the network enabled device and receive traffic directed to a network enabled device and then forward this on as required. Alternatively however, POS terminals could be configured to print receipts directly to the payment terminal, with the payment terminal then being configured to on-print receipts to a network printer. It will be appreciated from this that a wide variety of configurations are achievable depending upon the preferred implementation and the ability to control operation of the POS terminal.

[0212] As previously mentioned, in one example the network enabled device can include a printer. In this case, the transaction data typically includes print data indicative of the transaction to be printed, such as a receipt, with the payment terminal operating to determine the transaction amount and/or any other transaction details from the print data. The manner in which this is performed will vary depending on the preferred implementation. Typically, this includes scraping the print data to determine the transaction amount and may involve the use of optical character recognition techniques and/or templates defining the location of transaction details within the transaction data. In this regard, different transaction terminals will typically generate transaction receipts in a particular format. This will often include presenting transaction amounts at certain locations within the receipt, and/or the use of particular identifier codes or formatting to identify a transaction amount. For example, this may include certain formatting elements, such as delineations, within the receipt that can be identified in order to allow the location of the transaction amount to be correctly identified. This avoids payment devices mistakenly identifying subtotals for individual item values for a total transaction amount. In one particular example, the transaction details are determined by

scraping the print job in an ESC/POS format, but it will be appreciated that other techniques could be used, such as obtaining transaction details from transaction data in an XML, EPOS, OPOS format or the like and that other forms of text or binary output can be provided by the POS hardware, software or OS print driver. It will be appreciated that OCR techniques could be implemented on the payment terminal, but this is not essential, and alternatively, OCR could be performed by other systems, such as by a blockchain node, a smart contract on the blockchain, or offchain by a remote processing system, such as a server, or the like. Different OCR techniques might be required to process different transaction data from different POS terminals, and that OCR might be utilised in conjunction with machine learning techniques, in order to more accurately process transaction data. It will also be appreciated that OCR techniques might not be required depending on the format in which the transaction data is generated.

[0213] It will be appreciated that as transaction terminal operators update their systems, they may periodically update the format in which receipts are printed, in which case the payment terminal may need to be updated with templates based on a current format of the transaction data as generated by the transaction terminals. This ensures that the payment terminal is able to accurately identify transaction amounts within the transaction data.

[0214] As previously mentioned, in addition to storing payment data, other transaction details, including payment amounts and optional taxation amounts, can be stored by the payment terminal, and optionally uploaded to a remote data store for storage. The process typically involves storing an indication of the transaction amount, and optionally other transaction details, as well as a device identifier associated with the payment terminal. In this regard, each payment terminal typically has a unique identifier, which could be identified during an initial configuration phase or could include an inherent identifier, such as a MAC (media access control) identifier or similar. The device identifier could additionally and/or alternatively be hardcoded into the payment terminal, or could be encoded on a separate identification device that communicates with the payment terminal. For example, this might include the use of a USB storage device, or smart card, which store the device ID in an encoded format, and which can be plugged into the payment terminal to allow the device to

determine the device ID. It will be appreciated that other suitable techniques could be used, and that this is not intended to be limiting.

[0215] The device identifier is typically uniquely associated with an entity involved in performing the transactions, such as the merchant owning the transaction terminals. By storing the device identifier, for example within the blockchain, this allows the entity associated with the transaction to be easily identified. Thus, the device identifier can be uniquely associated with the payee or payor and in one particular example is uniquely associated with a tax identifier of an entity such as merchant. Thus in one example the payment terminal can be issued by a taxation authority with the authority maintaining a record of to which the payment terminal has been issued by uniquely associating the device identifier of the payment terminal with the tax identifier, such as a tax file number, of the entity.

[0216] It will also be appreciated that other information may be stored as part of the record, with examples including, an IP address of the payment terminal, a location at which the transaction was performed, a time and date of the transaction, any other information presented on the receipt, such as details of products/services purchased, or the like. This information can be used in conjunction with the transaction amount, to further help identify transactions breaching transaction rules.

[0217] As previously mentioned, the transaction details are preferably immutably stored. A variety of different storage mechanisms can be used, either alone or in conjunction, and examples include, but are not limited to storage in a distributed data store, an encrypted data store and/or a blockchain. Such immutable storage can be achieved either by immutably storing the transaction details themselves, or by storing verification data, such as a hash or digital signature derived from the transaction details, which can be used to subsequently verify that stored transaction details have not been altered.

[0218] In this latter case, the process typically includes storing verification data derived from the transaction details, for example as part of a blockchain, and separately storing the transaction details, for example in a database. The verification data can then be retrieved and

used to validate the transaction details, for example by generating new verification data from the transaction details, such as the transaction data, and comparing this to the stored verification data.

[0219] In one example, the storage processes are performed by respective processing systems. For example, a first processing system can receive transaction details, such as the raw transaction data, or data derived therefrom, from the compliance monitoring device and store the verification data, optionally by generate the verification data, or by receiving the verification data from the compliance monitoring device. A second processing system can then receive transaction details from the first processing system and store the transaction details.

[0220] In a further development to the process, the first processing system provides a verification confirmation message to the compliance monitoring device once the verification data is stored, allowing the compliance monitoring device to register that the transaction details have been successfully stored. In this example, the compliance monitoring device can be configured to store, and optionally repeatedly transmit, transaction details until the verification confirmation message is received.

[0221] In a further example, the second processing system can be configured to store the transaction details and provide a details confirmation message to the first processing system after the storing is completed, so that the first processing system only stores the verification data and/or issues the verification confirmation, when the details confirmation message is received.

[0222] In these examples, the transaction details can be stored on the compliance monitoring device until the transaction details and/or verification data are successfully stored, thereby ensuring that transaction details are not lost during the transmission and storage processes.

[0223] The transaction details can include any one or more of the transaction data, verification data derived from the transaction details, a hash derived from content of the transaction data, a digital signature derived from content of the transaction data, the transaction amount, an entity associated with the transaction, a transaction time, a transaction

location, a transaction date or a device identifier associated with the compliance monitoring device. The transaction details could also be transmitted in any appropriate form, for example as part of suitably configured data packets. In this regard, it will be appreciated that the transaction details could be transmitted in different formats between the compliance monitoring device and the first and second processing systems. Similarly, the transaction details transmitted may vary, for example only transmitting or storing some of the transaction details. For example, the transaction details transmitted by the compliance monitoring device could include raw transaction data, but the transaction details stored may include only select information derived therefrom, such as a transaction amount, time, date or the like. Reference to transaction details is therefore understood to encompass any information include or derived from the transaction data, and need not be identical at each stage in the transmission and/or storage process.

[0224] In addition to storing payment data and/or transaction details within the blockchain, the system can be used to allow the payment data and/or transaction details to be retrieved. Thus, in one example, the method can include retrieving payment data or transaction details from a blockchain node or other data store, and then displaying an indication of the transaction details and/or dispensed currency, using a client device. The client device could be of any appropriate form and could include a computer system, mobile device, smart phone, tablet, or the like.

[0225] In one example, retrieval of payment data or other transaction details is achieved by receiving a request from a client device, with the request being indicative of a user identity associated with a user making the request and an indication of one or more transactions. This can be achieved by specifying a particular transaction, or alternatively by identifying a group of transactions, for example based on a device identifier of a payment terminal, or a tax identifier of an entity, together with other filters, such as defined time periods. This can also be performed by specifying a container identifier to allow details of currency dispensed into a particular container to be retrieved.

[0226] Upon receipt of a request, it is determined if the user is authorised to view the one or more transactions or payment data using the user identity. In this regard, as payment data

and/or other transaction details include private information, it may be necessary to limit access to the transaction details, so that only certain users have access to transactions associated with certain entities. Thus, for example, a user may be able to access their own transactions, a financial officer, or other individual might wish to review payments or transactions associated with their business, whilst an accountant may be able to access details of transactions performed by their own clients. Similarly, individuals working for the Taxation Office may be able to access any of the transaction details. Accordingly, the user identity can be used to check permissions associated with different device identifiers, so that transaction details are selectively provided depending upon whether or not the user is so authorised.

[0227] In one example, the method includes determining transaction details for at least one transaction, comparing the transaction details to one or more transaction rules and then determining if rules have been breached based on the results of the comparison. Additionally and/or alternatively, this could involve causing an indication of the results of the comparison to be displayed. Thus, this can be used to automatically identify breaches in compliance, for example by comparing the transaction details to compliance rules.

[0228] The transaction rules can be defined in a variety of manners depending on the preferred implementation and the nature of the transaction rules. For example, if the transaction rules are taxation rules used to ensure compliance with a countries taxation regime, then in this instance the taxation rules would typically be defined by a taxation authority, such as a government agency, or similar.

[0229] This is not however so limited and indeed the technique can be used to analyse transactions more broadly to identify other suspicious activities. Thus, whilst the process could involve simply comparing an amount of taxation paid to a predicted amount of taxation, the system can also look for other suspicious activities, such as transactions performed out of business hours, unexpected peaks or troughs in transactions, unexpected transaction amounts, or the like. All of these can be used to identify forms of activity which are precluded, including potential money laundering, taxation avoidance or the like. For example, the transaction rules could be business rules defined by a business operator and

used to oversee operation of their business. An example of this is that of a franchise, in which a franchisor wishes to oversee operation of franchisees. In this instance, the franchisor can define transaction rules, such as a number or value of transactions performed in a given time period, with this being used to identify breaches, which can in turn be indicative of performance issues associated with a particular franchisee.

[0230] Accordingly, it will be appreciated that the above described system provides a mechanism for easily monitoring transactions and ensuring compliance with various transaction rules. Whilst the above described techniques have focussed on a payment terminal intercepting transaction data provided from a transaction terminal to a network enabled device, the process could be applied more broadly in other situations.

[0231] For example, the process could be implemented simply by obtaining transaction data in other manners, such as by having the transaction terminal generate a log of transactions, which are stored and then subsequently retrieved by the payment terminal.

[0232] Similarly, whilst the above described example focuses on storing of transaction details in a blockchain, it will be appreciated that the process could be applied more broadly to allow transaction details to be stored in another remote data store. For example, a taxation authority may maintain a tax database and store the transaction details centrally within that database. The transaction details can also be securely stored in other suitable repositories. For example, this could include storage in databases of a service provided, such as an entity overseeing the compliance monitoring process, databases of a third party service provider or the like.

[0233] Accordingly, in one example the method includes using a payment terminal having one or more electronic processing devices that obtain transaction data indicative of a transaction performed using a transaction terminal, determine from the transaction data transaction details indicative of a transaction amount and cause transaction details to be stored in a remote data store to allow the transaction details to be used in monitoring transaction compliance.

[0234] In addition to storing transaction details, additional information can be stored, such as a currency container identifier, status information provided by the currency container, or the like enabling these to provide evidence of the transaction. This allows the blockchain or other data stored to provide a complete audit trail of where currency was received and transported. This can be used to assist in tracking currency received as part of a payment process, and can also be used by financial institutions to assist in processing contents of currency containers upon receipt. This can also be used to allow analysis of transactions for example as part of a business analytics process.

[0235] In one example, the payment terminal is also configured to prevent tampering with the payment terminal and to ensure the payment terminal is functioning correctly. In this example, the one or more processing devices can periodically transmit a status notification to a computer system, which is responsive to the status notification to generate a status response. The status notification and status response are used to control payment terminal communication, cause the payment terminal to cache transaction details or generate an alert. Thus, this can be used to identify attempts to take the payment terminal offline and hence avoid transactions being logged or otherwise recorded. In one example, the payment terminal can include a terminal tamper sensor, with the terminal processing devices monitoring changes in signals from the terminal tamper sensors to detect attempts to tamper with the payment terminal. This can cause an alert to be generated, for example to sound a siren or transmit a notification to a remote computer system, allowing that tampering to be detected. As in the case of the container, the tamper sensors can include an accelerometer, position sensor, temperature sensor and air pressure sensor, a light sensor and/or a humidity sensor.

[0236] In another broad form, a cartridge removal tool can be provided for removing cartridges from a payment module. In this instance, as mentioned above, this can avoid the need to remove an entire payment module in order to store float outside of the payment terminal.

[0237] In one example, the cartridge removal tool includes a tool body having downwardly facing wings that engage a catch on a chassis of the payment module to detach a cartridge

from the chassis. Specifically, this can be achieved by positioning the cartridge removal tool on an upper surface of a cartridge, and urging the wings into engagement with a catch to thereby release the cartridge. This allows the cartridge to be easily removed from the payment module, which is not otherwise feasible, thereby reducing the burden of removing float from the payment terminal.

[0238] In one example, the tool body includes a flat front underside and an upwardly sloping rear underside. This allows the tool body to be positioned on a top surface of a cartridge, with a sloped rear underside flush against the top of the cartridge, with the tool body being pushed forwardly until the wings are in position. The body can then be rotated so that the flat underside of the tool body lies flat against an upper surface of the cartridge so that the wings engage a catch and release the cartridge.

[0239] The downwardly extending wings are typically provided proximate a front of the tool body but laterally spaced therefrom. This allows the wings to pass between the cartridge and side walls of the payment module, to allow the wings to engage the catch, whilst also allowing the wings to clear the mounting pin as the tool is pushed forwards.

[0240] In one embodiment the tool body includes lateral tabs extending outwardly from sides of the body to support the downwardly extending wings, with the tabs supporting L-shaped guides extending downwardly and outwardly from the tabs, rearwardly and outwardly of the wings. In this instance, removal tool can be pushed forward until the tabs engage or are aligned with side walls of the payment module, at which point the wings are in position to release the catch.

[0241] In one embodiment, once the catch is released the tool is urged rearwardly so that the wings engage a mounting pin of the cartridge allowing the mounting pin to be lifted from within a channel thereby releasing the cartridge.

[0242] An example of a payment system architecture will now be described with reference to Figure 3.

[0243] In this example, a payment terminal 310 is provided interconnected to one or more transaction terminals 320 and one or more network enabled devices, such as printers 330, via a communications network 340. The communications network 340 is typically a LAN provided within one or more facilities of an entity, such as a merchant, or similar. However, it will be appreciated that the term communications network should be interpreted broadly and can refer to any appropriate technique for communications technique, including but not limited to connections via Bluetooth, Wi-Fi, USB, or other forms of connectability.

[0244] The LAN 340 may be coupled to one or more other communications networks, such as the Internet 350, with the payment terminal 310 also optionally being coupled directly to the communications network 350, for example to provide a redundant communications link.

[0245] The communications network 350 is also typically coupled to one or more processing devices 360 and one or more client devices 370. In use this configuration allows the payment terminal 310 to provide transaction details via the communications network 350, so that this can be used by the processing systems 360 or client devices 370 in order to allow the transaction details to be stored as well as allowing additional functionality to be implemented, such as allowing transaction details to be retrieved and reviewed. In one example, the processing systems 360 and/or client devices 370 form part of a cloud or other remote system to allow for independent storage of payment data, allowing the payment data to be retrieved and reviewed by the client devices 370 as required.

[0246] It will be appreciated that the configuration of the networks are for the purpose of example only, and in practice the payment terminal 310, transaction terminals 320, printers 330, processing systems 360 and client devices 370 can communicate via any appropriate mechanism, such as via wired or wireless connections, including, but not limited to mobile networks, private networks, such as an 802.11 networks, the Internet, LANs, WANs, or the like, as well as via direct or point-to-point connections, such as Bluetooth, or the like.

[0247] An example of the physical construction of a payment terminal will now be described with reference to Figures 4A to 4D.

[0248] In this example, the payment terminal includes a housing of 410 having a generally cuboid configuration. The housing 410 has front and rear panels 410.1, 410.2, which in use are designed to face the customer and merchant respectively. Each of the front and rear panels 410.1, 410.2, includes a respective display 461, 462, which is in the form of a touch screen, which can be used to display information to and detect input commands from the customer and merchant respectively.

[0249] The front panel 410.1 further includes currency inlets 411.1, 411.2, which are adapted to receive notes and coins respectively and currency outlets 412.1, 412.2, which can be used to dispense reject currency and/or change. In this regard, typically reject notes will be returned via the currency inlet 411.1, with note change being dispensed via the outlet 411.2, whilst reject coins are change are provided via the outlet 412.2. The currency outlets 412.1, 412.2 can also be used to withdraw cash, for example as part of a cash-out transaction during a credit/debit card purchase, or to allow the payment terminal to function as an ATM (Automated Teller Machine).

[0250] The housing 410 further includes a door 423 provided near a base of the rear panel 410.2, which provides access to the container cavity to allow the currency container to be removed as shown in Figure 4D. A reader, such as a biometric or RFID reader, can be provided in the rear panel of the housing, which can be used to determine an identity of a user, such as a merchant or cashier. A power button 453 can also be provided in the rear panel, which is used to activate the payment terminal.

[0251] In use, the system allows users, and in particular customers to view details of the transaction, including a required payment amount, and select payment options via the front display 461, provide currency via the inlets at 411.1, 411.2, and receive change via the outlets 412.1, 412.2. In one example, reject notes are returned via the inlet 411.1. Additionally, the merchant is able to interact via the rear touch screen 462, for example to monitor details of the transaction and payment process. Additionally, this allows the merchant to perform administrator functions, such as ejecting the currency container 490, adjusting a float amount, dumping float, or the like.

[0252] An alternative arrangement is shown in Figures 5A to 5C.

[0253] In this arrangement, the payment terminal again includes a generally upright cuboid configuration having front and rear panels 510.1, 510.2. In this instance the housing includes a slideable outer cover 510.3, which can be moved forwardly to open the container cavity 520, which in this example is mounted vertically adjacent the rear panel 510.2, allowing a currency container 590 to be removed as shown in Figure 5C.

[0254] In this instance the payment terminal includes a single touch screen 561 which can be used by both the customer and the merchant. An RFID reader and power button would also typically be provided in a front panel 510.1, so that interaction is via the front panel for both the customer and merchant, or other users.

[0255] The configuration of Figures 5A to 5C also includes a currency inlet 511.1, which is configured to receive notes and return rejected notes, a currency inlet 511.2 for receiving coins, and a coin outlet 512.2 for returning rejected coins.

[0256] This configuration provides a smaller light-weight device which can be used in portable scenarios, such as incorporating the payment terminal into vehicles or the like. This is particularly useful in scenarios where quantities of cash are to be collected and minimal change provided, allowing a merchant or other operative to maintain a separate float supply for the purposes of providing change, whilst allowing large high denomination notes and/or coins, to be collected in a secure manner.

[0257] An example of a document container will now be described with reference to Figures 6A to 6C.

[0258] In this example, the currency container 690 includes a housing shaped similar to a small briefcase or other elongate flat cuboid. The housing includes first and second handles 690.4, 690.5 which are mounted on a side and end of the housing respectively. The side handle 690.4 can be used to allow the currency container to be carried in a manner similar to a briefcase, while the end handle 690.5 can be used to facilitate removal of the currency

container from a container cavity. Additionally, the currency container includes a lid 690.3 which is slideably mounted to the housing to allow the lid to be opened and closed.

[0259] An example of the internal structure of the currency container is shown in Figure 7.

[0260] As shown in this example, the currency container 790 includes a container processor 791 coupled to a container memory 792 and first and second container communication interfaces 793, 794. As previously described, the container processor 791 and container memory 792 could be of any appropriate form, and may include multiple processors or memories, depending on the preferred implementation. The communications interfaces are typically in the form of NFC and Wi-Fi modules, although other suitable arrangements could be used.

[0261] The container processor 791 is further connected to a number of container anti-tamper sensors 795 typically including one or more of light, temperature, humidity, pressure or other sensors, whilst a container location sensor 798, such as GPS module can be provided for determining a location of the currency container. A container identity reader 799 can be used for reading an identity of a user, and this could include a biometric reader, such as a fingerprint reader or the like, or alternatively could be adapted to read an identification device such as an RFID chip which could be provided in a wearable device, card, tag or the like.

[0262] The container processor 791 is also connected to a lid actuator, which in this example includes a motor 796.1 and worm gear 796.2, which engages a nut mounted in a tab 790.11 projecting from an underside of the lid 790.1, thereby allowing the lid to be driven between open and closed positions.

[0263] The currency container 790 further includes an inductive power receiver 797.1 which is connected to a battery 797.2 allowing the battery to be inductively charged to thereby power the internal components.

[0264] An example of the internal configuration of a payment terminal will now be described with reference to Figure 8.

[0265] In this example, a payment terminal includes an outer housing 810 including container cavity 820 in a rear panel 810.2 of the housing 810, which is formed from internal walls 821 within the housing 810. The internal walls 821 include an opening 822, which in use aligns with the lid of the currency container 790, so that currency can be dispensed into the currency container when the lid is open. A door 823 is hingeably mounted in the rear panel 810.2 of the housing to close the container cavity 820, opening as shown in dotted lines to provide access to the container cavity, and allow currency containers to be inserted into or removed from the container cavity 820. The door can also include a door tab 823.1 projecting inwardly from a rear face, which acts as a keep to receive a latch of a locking mechanism.

[0266] As described in the example with respect to Figures 4A to 4D, the housing can include currency inlets 811.1, 811.2, which receive notes and coins respectively, as well as currency outlets 812.1, 812.2, which are used for dispensing reject currency or change as the form of notes or coins, respectively. The inlets 811.1, 811.2 and outlets 812.1, 812.2 form part of a currency transport mechanism represented by the bold lines 831. The transport mechanism transports currency received via the currency inlets 811.1, 811.2 to a respective currency sensor 841.1, 841.2, in note and coin payment modules 840.1, 840.2. The currency sensors 841.1, 841.2 sense the notes and coins, operating to authenticate the currency, for example to ensure this is not counterfeit, and to count the denomination of the currency. The notes and coins are then transported to a redirect mechanism 842.1, 842.2, which operate to direct currency either to the respective outlets 812.1, 812.2, a float store 870 or the opening 821, depending on the outcome of the sensing process, and the current payment situation.

[0267] The payment terminal further includes a terminal processor 850 which is connected to a terminal memory 851 and a communications interface 852, such as a LAN or Wi-Fi network connection. Again multiple processors, memories or interfaces could be used depending on the preferred implementation.

[0268] In this example, the terminal processor 850 is connected to a control board 880, which is used to generate control signals to control various componentry of the payments terminal and also receive signals from on-board sensors, routing these and optionally partially processing the signals as required.

[0269] The control board 880 is in communication with a lid sensor 881, which is an optical sensor mounted in the opening 821 of the container cavity 820 that can be used to detect whether the lid 790.1 of the currency container 790 is open or closed. The control 880 is further coupled to first and second terminal communications interfaces 883, 884 which are provided in proximity with the current container cavity 820, to allow for communication with the first and second container communications interfaces 793, 794 of the currency container.

[0270] The payment terminal further includes one or more terminal anti-tamper sensors 885, such as pressure, temperature, light, humidity sensors or the like and front and rear displays 861 and 862. A terminal reader 889 can also be provided for determining an identity of a user, and this could include a biometric reader, such as a fingerprint reader or the like, or alternatively could be adapted to read an identification device such as an RFID chip which could be provided in a wearable device, card, tag, or the like.

[0271] Front and rear displays 861, 862, in the form of touch screens are provided, allowing these to be used to display information to a merchant and/or consumer, and for allowing user input commands to be received.

[0272] Finally, an inductive power transmitter 887 is provided for inductively charging the currency container battery 797.2. The control 880 is further coupled to a door lock mechanism in the form of a solenoid 882.1, which controls a latch 882.2 that engages the keep in the door tab 883.1, to thereby lock the door.

[0273] An example of a transaction terminal will now be described with reference to Figure 9.

[0274] In this example, the transaction terminal 320 includes at least one microprocessor 900, a memory 901, an input/output device 902, such as a keyboard and/or display, an external interface 903, and optionally a card reader 904, interconnected via a bus 905 as shown. In this example the external interface 903 can be utilised for connecting the transaction terminal 320 to peripheral devices, such as the communications networks 230 databases, other storage devices, or the like. Although a single external interface 903 is shown, this is for the purpose of example only, and in practice multiple interfaces using

various methods (eg. Ethernet, serial, USB, wireless or the like) may be provided. The card reader 904 can be of any suitable form and could include a magnetic card reader, or contactless reader for reading smartcards, or the like.

[0275] In use, the microprocessor 900 executes instructions in the form of applications software stored in the memory 901, to allow the transaction terminal to perform transactions and generate receipts. The applications software may include one or more software modules, and may be executed in a suitable execution environment, such as an operating system environment, or the like.

[0276] Accordingly, it will be appreciated that the transaction terminals 320 may be formed from any suitable transaction terminal, and could include suitably programmed PCs, Internet terminal, lap-top, or hand-held PC, POS terminals, ATMs or the like, as well as a tablet, or smart phone, optionally with integrated or connected card reading capabilities. However, it will also be understood that the transaction terminals 320 can be any electronic processing device such as a microprocessor, microchip processor, logic gate configuration, firmware optionally associated with implementing logic such as an FPGA (Field Programmable Gate Array), or any other electronic device, system or arrangement.

[0277] An example of a suitable processing system 360 is shown in Figure 10.

[0278] In this example, the processing system 360 includes at least one microprocessor 1000, a memory 1001, an optional input/output device 1002, such as a keyboard and/or display, and an external interface 1003, interconnected via a bus 1004 as shown. In this example the external interface 1003 can be utilised for connecting the processing system 360 to peripheral devices, such as the communications networks, databases, other storage devices, or the like. Although a single external interface 1003 is shown, this is for the purpose of example only, and in practice multiple interfaces using various methods (eg. Ethernet, serial, USB, wireless or the like) may be provided.

[0279] In use, the microprocessor 1000 executes instructions in the form of applications software stored in the memory 1001 to allow the required processes to be performed. The

applications software may include one or more software modules, and may be executed in a suitable execution environment, such as an operating system environment, or the like.

[0280] Accordingly, it will be appreciated that the processing system 360 may be formed from any suitable processing system, such as a suitably programmed client device, PC, web server, network server, or the like. In one particular example, the processing system 360 is a standard processing system such as an Intel Architecture based processing system, which executes software applications stored on non-volatile (e.g., hard disk) storage, although this is not essential. However, it will also be understood that the processing system could be any electronic processing device such as a microprocessor, microchip processor, logic gate configuration, firmware optionally associated with implementing logic such as an FPGA (Field Programmable Gate Array), or any other electronic device, system or arrangement.

[0281] An example of a client device 370 will now be described with reference to Figure 11.

[0282] In this example, the client device 370 includes at least one microprocessor 1100, a memory 1101, an input/output device 1102, such as a keyboard and/or display, and an external interface 1103, interconnected via a bus 1104 as shown. In this example the external interface 1103 can be utilised for connecting the client device 370 to peripheral devices, such as the communications networks, databases, other storage devices, or the like. Although a single external interface 1103 is shown, this is for the purpose of example only, and in practice multiple interfaces using various methods (eg. Ethernet, serial, USB, wireless or the like) may be provided.

[0283] In use, the microprocessor 1100 executes instructions in the form of applications software stored in the memory 1101 to allow communication with the processing systems 360, for example to view details of transactions performed, currency contained within respective currency containers, or the like. The applications software may include one or more software modules, and may be executed in a suitable execution environment, such as an operating system environment, or the like.

[0284] Accordingly, it will be appreciated that the client devices 370 may be formed from any suitable processing system, such as a suitably programmed PC, Internet terminal, lap-top,

or hand-held PC, and in one preferred example is either a tablet, or smart phone, or the like. However, it will also be understood that the client devices 370 can be any electronic processing device such as a microprocessor, microchip processor, logic gate configuration, firmware optionally associated with implementing logic such as an FPGA (Field Programmable Gate Array), or any other electronic device, system or arrangement.

[0285] Examples of the processes for processing payments will now be described in further detail. For the purpose of these examples it is assumed that the transaction terminals 320 are used to perform transactions, with operation of the terminal being controlled by the processor 900 executing applications software for performing transactions and generating receipts that are transferred to the printers 330 as print data.

[0286] The payment terminal 310 executes applications software for intercepting print data from the transaction terminal 320, and forwarding this to the printers 330 for printing. The payment terminal 310 also stores currency in the currency containers 790, provides currency data to the currency containers 790, and provides payment details to the processing systems 360 for monitoring and tracking purposes. Actions performed by the payment terminal 310 are performed by the terminal processor 850 in accordance with instructions stored as applications software in the terminal memory 851.

[0287] The currency containers 790 receive currency and currency data, storing the currency data in the memory 792. Actions performed by the currency container are performed by the container processor 791 in accordance with instructions stored as applications software in the container memory 792.

[0288] The processing systems 360 typically execute applications software for receiving transaction details and optionally storing these for logging and/or auditing purposes. Actions performed by the processing system 360 are performed by the processor 1000 in accordance with instructions stored as applications software in the memory 1001 and/or input commands received from a user via the I/O device 1002, or commands received from the client device 370.

[0289] It will also be assumed that the user interacts with the processing system 360 via a GUI (Graphical User Interface), or the like presented on the client device 370, and in one particular example via a browser application that displays webpages hosted by the processing system 360, or an App that displays data supplied by the processing system 360. Actions performed by the client device 370 are performed by the processor 1100 in accordance with instructions stored as applications software in the memory 1101 and/or input commands received from a user via the I/O device 1102.

[0290] However, it will be appreciated that the above described configuration assumed for the purpose of the following examples is not essential, and numerous other configurations may be used. It will also be appreciated that the partitioning of functionality between the client devices 370, and the processing systems 360 and the payment terminals 310 may vary, depending on the particular implementation.

[0291] It will also be appreciated that additional processes can optionally performed not otherwise described herein in detail. For example, an administrator or installer might be able to connect to the payment terminal via SSH (Secure Socket Shell) or directly or remotely to perform maintenance or servicing.

[0292] Operation of the payment terminal will now be described with reference to Figures 12A to 12C.

[0293] In this example, at step 1200 a POS terminal 320 performs a transaction by determining the value of particular goods or services, and generating a total transaction amount. This information can be entered manually or could be determined by scanning product barcodes or the like, in the normal way. At the end of the transaction, the POS terminal transmits a receipt, in the form of print data, to a printer 330 at step 1205. At step 1210 the payment device 310 intercepts the receipt print data, for example, by acting as a proxy for the printer 330 and then scrapes the receipt at step 1215 using a template format. In this regard, the POS terminal will typically generate a receipt having a predetermined format and so by using a template format associated with the respective POS terminal 320, this allows the payment terminal 310 to readily identify the potential location of transaction

details within the receipt print data. This can be performed utilising optical character recognition or the like which can be used to discern alpha numeric characters, with these being interpreted based on the template, allowing the transaction details such as a transaction amount to be determined at step 1220.

[0294] At step 1225, the payment terminal 310 displays a transaction amount and payment options on the front display 861, allowing these to be viewed by a customer, with these also optionally being displayed on the rear display 862, for example to allow the merchant to check the transaction amount and ensure this is correct. The customer can proceed with selecting a payment option at 1230, for example by selecting an option presented on the touch screen. It will be appreciated that alternatively this step could be performed by the merchant via the merchant screen 862, although generally this is not preferred as the intention is that the payment terminal will reduce the burden on the merchant. As a further alternative, a merchant and/or consumer could select an option to cancel a transaction.

[0295] At step 1235 assuming a currency payment option has been selected, the terminal processor 850 activates the currency modules 840.1, 840.2. It will be appreciated that if card or other payment options are selected, these will be handled in a corresponding manner, adapted for the selected technique, and this will not therefore be described in further detail.

[0296] At step 1240, the terminal processor 850 causes a current balance to be displayed on the front display 861, allowing the user to determine how much currency remains owing. The user then commences providing currency via a respective currency inlet 811.1, 811.2, with the currency being transferred to the respective currency sensor 841.1, 841.2 allowing the currency module 840.1, 840.2, to authenticate the currency and determinate the denomination of the currency at steps 1250 and 1255. As this process is performed, an indication of the value of the supplied currency is provided to the terminal processor 850, which updates the displayed balance at step 1240, allowing further currency to be provided as required.

[0297] Simultaneously, the terminal processor 850 will retrieve a float target amount and current float amount from the memory 851, at step 1260, using this to determine if there is a float deficit at step 1265. During these processes at step 1270 the terminal processor 850 will

instruct the control board 880 to generate control signals which are transferred to the currency redirect mechanisms 842.1, 842.1 allowing currency to be diverted to the float 870 or the container 790 as required. In particular, this is performed to replenish the float in the event that the float is below the float target, or to direct currency to the currency container 790 for storage.

[0298] As part of this process, if currency is rejected, for example in the event that it is counterfeit, or damaged to a point where it cannot be authenticated or identified, the payment module 840.1, 84.2, will cause the respective redirect mechanism 842.1, 842.2 to divert the currency to the outlet 812.1, 812.2.

[0299] At step 1275, the terminal processor 850 calculates an amount of currency which is dispensed into the currency container 790, recording this as currency data in the memory 851, and then optionally uploading the currency data to the container, allowing the container processor 791 to store the currency data in the container memory 792. Additionally, payment data, including the currency data, an indication of the container identifier and other transaction details, such as a transaction or payment amount, can be uploaded to a processing system 360.

[0300] Uploading the payment data to the processing system 360 allows the payment data to be stored, and subsequently retrieved and reviewed as needed. For example, the payment data could be retrieved by a financial institution upon receipt to ascertain the amount of currency present in a container received at their premises. In this example, upon receipt of the container, the container identifier can be determined and used to retrieve the payment data associated with the respective container, so that the financial institution can determine the container content without having to open the container. This can also be retrieved and used for other purposes. For example, the payment data could be used to retrieve details of transactions associated with a respective merchant, allowing this to be used for compliance monitoring, and/or performing business analytics. Furthermore, this can be used by the processing system 360 to allow currency containers and their contents to be tracked, as well as to allow transactions and payment to be monitored.

[0301] In one example, a first processing system 360 receives transaction details, including raw transaction data, and uses these to generate verification data. In one preferred example, the verification data includes a digital signature and/or hash value derived from the raw transaction data. Other information, such as the raw transaction data, or transaction details derived therefrom, could also be stored as part of the blockchain, although in general, the preference is to minimise the amount of data stored, and hence the raw transaction data is not typically stored.

[0302] Transaction details, and more typically the transaction details including the raw transaction data, are forwarded to a second processing system 360, allowing the second processing system 360 to store the transaction details, and preferably the raw transaction data, in a secure and optionally distributed database. The second processing system 360 then provides a details confirmation message, to the first processing system 360 to confirm the details have been stored. The first processing system 360 then stores the verification data in the blockchain, before providing a verification confirmation to the payment terminal, so that the payment terminal knows the transaction details are stored. In one example, this allows the payment terminal to clear the transaction details from internal memory, although this is not essential and will depend on factors such as the available storage capacity. In any event, having the payment terminal retain the transaction details until confirmation is received that the details have been stored, allows the transaction details to be retransmitted if required, thereby ensuring the details are stored

[0303] Additionally, and/or alternatively, the transaction details, or information derived therefrom, such as verification data, could be incorporated into a block and added to a locally stored copy of the blockchain by the payment terminal itself with the block then being transmitted to other blockchain nodes for storage.

[0304] Once the transaction details have been stored, transaction details can be subsequently retrieved as required. This may be performed on a case-by-case basis, periodically, or in the event that a user wishes to analyse transaction details. This process may also involve verifying transaction details, by retrieving the verification data from the blockchain, allowing a processing system to verify the retrieved transaction details are correct and have not been

subsequently altered. For example, this can involve generating verification data, such as a signature or hash from the stored transaction details or data, and then comparing this to the stored verification data to ensure there is a match.

[0305] Following this, the terminal processor 850 causes confirmation of payment to be displayed at step 1285, typically via both touch screens 861, 862, so that the merchant and customer know that correct payment has been provided. The terminal processor 850 can also generate modified print data corresponding to a modified receipt showing the payment received, with this being transferred to the printer 330 for printing at step 1290.

[0306] An example of the process for inserting currency at container 790 into the payment terminal 310 will now be described with reference to Figure 13.

[0307] At step 1300 the merchant selects an insert container option via the touch screen 862. The terminal processor 850 instructs the control board 880 to activate the solenoid 882.1, to disengage the lock, allowing the door 823 to open so that the currency container 790 can be inserted into the currency cavity 820 at step 1310.

[0308] At step 1320 the payment terminal detects the container. In particular, this will be achieved by the terminal NFC module 883, which typically repeatedly generates broadcast packets. The packets are detected by the container NFC module 793, which generates a response that is received by the terminal NFC module 883 allowing the terminal processor 850 to detect that a currency container 790 has been provided in the container cavity 820.

[0309] At step 1330, the payment terminal and currency container establish communication, by having the terminal and container NFC modules 793, 883 exchange communication information, such as a Wi-Fi network SSID and password, and/or encryption key, allowing communication to be established via the terminal and container Wi-Fi modules 794, 884.

[0310] Having established Wi-Fi communication, payment terminal and currency container identifiers can be exchanged at step 1340. The identifiers are stored against any currency data or transaction records, to thereby create a log of usage of the payment terminals and currency containers. This allows the currency container 790 to maintain a record of the payment

terminals from which currency has been received and similarly allows payment terminals to maintain a record of currency containers into which currency has been dispensed. This can be used for cross checking, which can in turn be used to detect attempts to fraudulently alter records stored in either the payment terminal and/or currency container. This can also be useful for auditing purposes to ensure that funds are correctly allocated to a particular bank account. In this regard, a financial institution can maintain a register of payment terminals associated with a merchant account, so that when a currency container is received, the financial institution can automatically determine the bank account into which the currency should be provided.

[0311] The terminal and container identifiers are recorded in the respective container and terminal memories 792, 851, before the solenoid is activated at step 1350, to lock the door 823, and thereby secure the currency container 790 in the container cavity 820.

[0312] Once this is completed, at step 1370 the container lid 790.1 is opened. This is achieved by having the terminal processor 850 transmit a lid open request to the container processor 791. The container processor 791 actuates the motor 796.1 and opens the lid 790.3. A lid open confirmation response can be provided to the terminal processor 850. Alternatively, the terminal processor 850 can confirm the lid 790.3 is open using the lid sensor 881. Assuming that these steps have been completed successfully, the terminal processor 850 can then activate the currency payment modules 841.1, 841.2 at step 1370, allowing payments to be provided.

[0313] An example of the process for ejecting and subsequently tracking the container to a financial institution will now be described with reference to Figure 14.

[0314] In this example, at step 1400 a user selects an eject container option presented on the display 862. Prior to ejecting the container, the user is required to undergo authentication at step 1410. The user can be authenticated in any appropriate manner and this could include scanning a user identifier, such as biometric information or information contained in an identification device using the reader 889, entering a username and password, or the like. Assuming the user is successfully authenticated by the terminal processor 850, the terminal

processor 850 proceeds to check permissions associated with the user to ensure the user is permitted to eject the currency container.

[0315] In the event the user is not authenticated, or does not have necessary permissions, the process will be halted and the currency container will remain locked in the payment terminal. Additionally, a notification may be optionally generated and transferred to a processing system 360 and/or client device 370, notifying an operative, such as a merchant or financial institution that attempts have been made to remove the container.

[0316] Assuming however that the user is authenticated and has necessary permissions, the election process proceeds. Accordingly, at step 1415, the terminal processor 850 optionally dumps the float, by activating the transport system 831. This can be performed automatically, based on float dump rules stored in the terminal memory 851, or manually based on confirmation from a user. Following this, at step 1420, the terminal processor 850 communicates with the container processor 791 to confirm the stored currency data is correct.

[0317] Following this, at step 1425 the terminal processor 850 can upload the payment data, including an indication of the container identifier and dispensed currency, and details of the transaction and payment amounts to a processing system 360 for tracking purposes. In one example, this allows the payment data to be uploaded to or retrieved by a financial institution to allow the financial institution to check the funds received are correct when the container is received. However, the recorded payment data can also be used for other reasons, such as to track operation of the business. For example, the payment data can include information regarding the time and date on which transactions are performed, and the payment provided. This can allow a business owner to perform an analysis to understand what currency is used at what times during the day, and hence what levels of float might be required. It will be appreciated that a wide range of other analytics could be performed and that this is merely one example for illustrative purposes.

[0318] Once these processes have been completed at step 1430 the container lid 790.3 is closed by having the terminal processor 850 transfer a lid close request to the container processor 791, causing the container processor 791 to activate the motor 796.1 and close the

lid. The terminal processor 850 confirms the lid is closed, using either the lid sensor 881 or a lid closed response from the container processor 791, and then activates the solenoid 882.1 at step 1435 to release the lock and allow the door 823 to be opened and the currency container 823 removed.

[0319] Once removed, the container will undergo a continuous monitoring process as it is transferred to a financial institution. In this process, anti-tamper sensors 795 are monitored by the container processor 791 at step 1440 and a location determined at step 1445 with a status update being periodically transmitted to a processing system 360, allowing transfer of the currency container to be tracked. This will typically be continued until a predetermined location, such as the location of the financial institution, is reached. This allows the financial institution to track the transfer of the container, and detect any attempts to tamper with the container and access the container contents.

[0320] When the financial institution detects the container has been received, they can use the processing system 360 to query the currency container and retrieve the currency data. This can be compared to the currency data received from the payment terminal to check these are in agreement, in which case the funds can be allocated to an account of the merchant, with this optionally being performed even before the container is opened.

[0321] At some point, the container can be opened. This is typically achieved by providing instructions to the container processor 850 from a processing system 360, or another suitable device. As part of this process, the container processor 792 can determine an identity of a user attempting to open the container, using the reader 799. In the event that the user is successfully authenticated, permissions can be checked in a manner similar to that described above with respect to the process performed by the terminal processor 850 in steps 1405 and 1410. This allows the container processor 791 to confirm the user has permission to open the lid, before the lid is opened to provide access to the currency contained therein. Additionally, other rules can be applied, such as only allow the container to be opened at defined locations, or the like.

[0322] Accordingly, the above described system allows cash payments to be collected using a payment terminal that can interface with existing POS terminals to allow cash payments to be added as an additional options as part of an existing transaction infrastructure. As the cash is collected it is counted and then directly transferred to a currency container and/or used to replenish a float. The currency container can be secured and removed from the payment terminal, allowing this to be transported to a financial institution or other facility for banking. Throughout this process, the currency container can be tracked, with currency data also being recorded and made available for auditing purposes.

[0323] Additionally, as transaction data is recorded in the above described process, this can be used in a transaction monitoring process, in particular in order to monitor compliance with transaction rules.

[0324] In this regard, once transaction details have been stored, the processing system 360 can subsequently retrieve transaction details either on a case-by-case basis, periodically, or in the event that a user wishes to analyse transaction details.

[0325] Having retrieved transaction details, the processing system 360 can analyse the transaction details and perform one or more types of analysis or action. For example, the processing system 360 can determine an amount of tax payable and then optionally compare this to an amount of tax that has been paid, allowing one or more breaches to be determined.

[0326] Additionally and/or alternatively, the transaction can be compared to transaction rules with the results of this comparison being displayed, allowing suspicious behaviours to be identified, such as unexpected transactions, transactions not fitting typical profiles, or the like.

[0327]

[0328] In this example, at step 1500 the payment terminal monitors tamper sensors 885 and detects changes in signals from the sensors at step 1510. The changes are then compared to tamper rules at step 1520 which identify changes in signals indicative of tampering behaviours. For example, the tamper rules might define that if the ambient light within the

housing of the payment terminal exceeds a set threshold, then this is indicative of the housing being fraudulently opened, thereby indicating that tampering is being performed.

[0329] Other detection modalities could include identifying changes in temperature, humidity or pressure, again associated with opening of the housing. Additionally, detection could be achieved by detecting impacts or other accelerations, indicative of a person attempting to force the housing open. Finally, position sensing could be used to identify movement of the payment terminal outside a defined area, such as the geographical extent of the facility within which the payment terminal is located, thereby detecting attempts to remove the payment terminal from within the facility. Typically tamper detection will be performed using a combination of different modalities in parallel, although this is not essential and any suitable detection mechanism could be used.

[0330] In the event that tampering is detected, at step 1530 a tamper notification is typically generated with this being transferred to a processing system 360 at step 1540 for actioning. For example, this could be used to transfer the notification on to an authorised person, allowing this to be actioned, for example to allow a site visit to be performed to inspect the payment terminal. Alternatively, this could be used to flag transaction details as suspicious, allowing these to be investigated further.

[0331] It will be appreciated that the currency container processor 791 can perform a broadly similar set of steps when performing tamper detection at step 1440.

[0332] In addition to utilising on-board sensors to detect tampering, the system can also monitor a network configuration at step 1550 and detect changes in the configuration at step 1560. For example, this may identify if a user attempts to alter IP addresses of the printer to thereby circumvent the payment terminal, again thereby allowing attempts to subvert the payment terminal to be detected.

[0333] The system also operates to monitor communication between the payment terminal 310 and a processing system 360 in order to ensure that communication is maintained and hence that the payment terminal has not been disabled or otherwise removed from network access. An example of this will now be described with reference to Figure 16.

[0334] In order to achieve this, at step 1600 the payment terminal 310 transmits a status notification to a processing system 360. This process is typically performed periodically, so that transmissions are repeated with a set time interval between subsequent transmissions. At step 1605 the processing system 360 monitors for receipt of such notifications and determines if a notification has been received. If no notification is received in the set time limit, an indication of the operational status of the payment terminal is updated at step 1610. If a notification is received, a status response is transmitted at step 1615.

[0335] Having sent a status notification to the processing system 360 at step 1600 the payment terminal 310 will wait for a response to be received at step 1620. If a response is received, this confirms that communication is established and is working correctly and the process can simply return to step 1600, allowing a further status notification to be transmitted after a certain time period.

[0336] However, in the event that no response is received, the payment terminal 310 will revert to a secondary communications link and transmit a further status notification to the processing system 360 at step 1620. In the event that the processing system 360 did not receive a first notification, the processing system will monitor for a second notification at step 1625. If this is not received, the processing system 360 will update an operational status at step 1630 and further generate an alert at step 1635 indicating that no status notification is being received by either the primary or secondary communications channels, and hence that the payment terminal is offline. This can be used to allow further investigation to be performed, for example to allow a site visit to be performed, or the like.

[0337] Assuming a notification is received, a status response will be transmitted at step 1640 with the payment terminal 310 monitoring for receipt of the response at step 1645. In the event that a response is not received, the payment terminal will determine it is offline and commence caching data. The payment terminal will wait for communication to be re-established with the processing system 360. Otherwise the process returns to step 1600, allowing a further status notification to be transmitted after a certain time period.

[0338] Accordingly, by following the above described process this enables the payment terminal 310 and processing system 360 to communicate and ensure communication is established via either the primary, or in the event of failure of the primary, the secondary communication channel. In the event that communication fails, transaction data is cached and stored for subsequent transmission whilst a notification is generated to alert authorities that the payment terminal is offline. In the event that the payment terminal is offline and unable to communicate, then currency data can be stored locally in the memory 851, allowing container data to be uploaded at a later time, for example when communication is re-established. It will again be appreciated that a similar process can be performed in respect of the currency container, allowing the currency container to use two communications interfaces to communicate with a processing system 360, with communication being monitored in order to identify a communications and hence tracking failure.

[0339] Accordingly, the above described system and process can also operate to perform monitoring of transactions, allowing payment data and transaction details to be captured and stored in a remote store, such as a blockchain, allowing this to be used for tracking compliance with transaction rules, and in one preferred example, taxation rules, as well as tracking payments and transaction more broadly, for example for business analytics processes, and tracking of cash during transfer to a processing facility.

[0340] Examples of a currency container and currency feeder will now be described in more detail with reference to Figures 17A to 17F.

[0341] In this instance, the container includes a container housing 1790.1 defining an internal container internal cavity 1790.2. The container includes a lid 1790.3 which can be selectively opened or closed to provide access to or seal the container cavity. In this example, the lid 1790.3 is connected to a lid actuator, which in this example includes a motor 1796.1 and worm gear 1796.2, which engages a nut mounted in a tab 1790.11 projecting from an underside of the lid 1790.1, thereby allowing the lid to be driven between open and closed positions shown in Figure 17A and 17B respectively. Thus, it will be appreciated that in contrast to previous examples, the lid opens outwardly.

[0342] The container 1790 includes electronics, similar to that described in previous examples, which is contained in an electronics housing 1790.13, positioned within the container cavity. A coin box 1790.12 can also be provided to receive coins.

[0343] In this example, a currency feeder is provided in the form of a note feeder, including a feeder housing 1731.1, containing feed rollers 1731.2, arranged in pairs to define nips through which notes pass. Some of the feed rollers 1731.2 can be driven, allowing notes received via the transport system 131 to be driven through and ejected from the feeder housing 1731.1.

[0344] In this example, an actuator is provided, which can be used to move the currency feeder from the retracted position shown in Figures 17A and 17C to the dispensing position shown in Figures 17B and 17D, in which the feeder housing 1731.1 extends through the container lid opening and into the container cavity. In this example, the actuator is in the form of drive rollers 1731.3, which engage the feeder housing 1731.1, allowing the feeder housing 1731.1 to be moved as required. However, it will be appreciated that other forms of actuator could be used, such as linear actuators, or similar.

[0345] In this instance, when a container is inserted into the container cavity, this can be detected using a suitable sensor, and the lid actuator 1796.1 activated, causing the lid 1790.3 to open. Opening of the lid can be detected by the terminal processor 850, for example, using an optical sensor to detect the lid 1790.1, with the actuator then being activated to move the feeder housing 1731.1 into the dispensing position. By ensuring the feeder housing is inserted into the container internal cavity 1790.2, this ensures currency is dispensed into the container, and does not for example become caught in the opening, or similar. This also allows the notes to be ejected with sufficient force to prevent notes blocking an exit to the feeder housing 1731.1.

[0346] In the example shown in Figures 17A to 17D, the container is horizontally orientated. However, as shown in Figures 17E and 17F, a similar arrangement can also be used if the container is vertically orientated. In this example, the container can be supported in the container cavity 1720 between an inner wall 1721 and the housing 1710, with the container

- 70 -

being supported above a recess 1724 that can receive the lid 1790.3 of the container, as shown in Figure 17F. Otherwise operation is substantially as described above and will not therefore be described in any further detail.

[0347] An example of a payment module will now be described with reference to Figures Figure 18A to 18C.

[0348] In this example, the payment module includes a chassis including a base 1871.1 and side walls 1871.2. The payment module includes an currency inlet 1811.1 and currency sensor 1841.1, in the form of a note validator. The note validator is attached to a transport system 1872, which is in turn connected to a number of cartridges 1873, which are configured to store currency. In this example, one of the cartridges 1873 also includes a currency outlet 1812.1, although this is not essential and other arrangements can be used An internal outlet may be provided for dispensing currency into the transport system 131 of the payment terminal. The payment module will also include processing electronics for validating currency, determining a currency denomination and feeding notes into and out of the cartridges are required.

[0349] In use the transport system 1872 is supported between the side walls 1871.2, with the cartridges 1873 being removably mounted to the side walls 1871.2, so that when attached thereto, the cartridges 1873 abut the transport system, allowing currency to be fed into and retrieved from the cartridges 1873 by the transport system 1872. To achieve this, the cartridge includes front and rear sections 1873.1, 1873.2, with the rear section being narrower, allowing this to slide between the side walls 1871.2, which the front section engages the side walls 1871.2 to position the cartridge. The side walls 1871.2 include open channels 1871.3, which in use receive mounting pins 1873.1 extending laterally from the rear section 1873.2 of the cartridges 1873. A catch 1871.4 is pivotally mounted to an inside of the side wall, so that once the cartridge pin is inserted into the channel 1871.3, the cartridge cannot be removed until the catch is released. Other guide channels (not shown) may also be provided to help support the cartridge 1872.

[0350] In one example, the payment module is a Suzohapp SBB-120 Bill-to-Bill Currency Management System, although this is not intended to be limiting and other arrangements could be used.

[0351] The payment module is mounted within the payment terminal housing 1810, above the container cavity 1820, and with the currency inlet and outlet 1811.1, 1812.1 projecting through a front of the housing, allowing notes to be inserted into and ejected from the payment terminal.

[0352] The payment module is removably mounted, allowing this to be removed if needed, which might be desirable for example to remove float from the payment terminal. However, the payment module is typically heavy (in excess of 20kg) and so removal of the entire module is not desirable.

[0353] In one example, a cartridge removal tool is provided, which can allow cartridges to be decoupled from the chassis, allowing these to be removed from the payment terminal separately, and an example of this will now be described with reference to Figures 19A to 19C.

[0354] In this example, the cartridge removal tool 1975 includes a tool body having a flat front underside 1975.1 and an upwardly sloping rear underside 1975.2. Lateral tabs extending outwardly from sides of the tool body support downwardly extending wings 1975.4 provided proximate a front of the tool body but laterally spaced therefrom. The tabs also support L-shaped guides 1975.5, extending downwardly and outwardly from the tabs, rearwardly and outwardly of the wings 1975.4.

[0355] In use, as shown in Figures 20A to 20D, the tool body is initially positioned on a top surface of a cartridge 1873, with the sloped rear underside 1975.2 flush against the top of the cartridge. In this configuration, the wings 1975.4 are elevated enough to clear the mounting pins 1873.3 allowing the removal tool 1975 to be pushed towards the side walls 1871.2. The guides 1975.5 engage or align with the side walls (depending on whether an upper or lower cartridge is removed), with the wing 1975.4 extending beyond the pin 1873.3. The removal tool 1975 can then be rotated so that the flat underside 1975.1 lies flat against an

- 72 -

upper surface of the cartridge 1873. The wing 1975.4 passes between the side wall 1871.2 and the rear part 1873.2 of the cartridge 1873, engaging and releasing the catch 1871.4. The removal tool can then be urged rearwardly, thereby engaging the mounting pin 1873.3 allowing this to be lifted from within the channel 1871.3, thereby releasing the cartridge 1873.

[0356] It will therefore be appreciated that this allows individual cartridges to be released from the payment module, without requiring the entire payment module to be removed from the housing 1810. This in turn makes it feasible to remove float from the payment terminal, without requiring the payment module to be removed, thereby easing the float removal process, and making the removed float easier to store.

[0357] Throughout this specification and claims which follow, unless the context requires otherwise, the word “comprise”, and variations such as “comprises” or “comprising”, will be understood to imply the inclusion of a stated integer or group of integers or steps but not the exclusion of any other integer or group of integers. As used herein and unless otherwise stated, the term "approximately" means $\pm 20\%$.

[0358] Persons skilled in the art will appreciate that numerous variations and modifications will become apparent. All such variations and modifications which become apparent to persons skilled in the art, should be considered to fall within the spirit and scope that the invention broadly appearing before described.

THE CLAIMS DEFINING THE INVENTION ARE AS FOLLOWS:

- 1) A system for processing a payment for a transaction, the system including a payment terminal including:
 - a) a housing including:
 - i) a container cavity that in use receives a currency container;
 - ii) a currency input; and,
 - iii) a currency transport system that transports currency from the currency input to an opening in the container cavity to allow currency to be dispensed into the currency container;
 - b) one or more payment modules including at least one currency module having a currency sensor that senses currency transported by the transport system and determines a currency value;
 - c) a terminal memory;
 - d) a terminal communications interface; and,
 - e) one or more terminal processing devices that:
 - i) determine a transaction amount;
 - ii) determine a received payment amount indicative of an amount of a received currency;
 - iii) cause at least some of the currency to be dispensed into the currency container; and
 - iv) cause payment data to be stored, the payment data being indicative of at least one of:
 - (1) the transaction amount;
 - (2) the payment amount;
 - (3) an amount of currency dispensed into the currency container; and,
 - (4) a container identifier indicative of an identity of the currency container.
- 2) A system according to claim 1, wherein the one or more terminal processing devices:
 - a) determine a currency container identifier; and,
 - b) store the currency container identifier in the terminal memory.

- 74 -

- 3) A system according to claim 1 or claim 2, wherein the payment terminal includes a display that displays at least one of:
 - a) a transaction amount;
 - b) transaction details; and,
 - c) a received payment amount.
- 4) A system according to claim 3, wherein the payment terminal includes first and second displays that in use display information to a merchant and customer respectively.
- 5) A system according to any one of the claims 1 to 4, wherein the payment terminal includes a user input that receives user input commands.
- 6) A system according to any one of the claims 1 to 5, wherein the payment terminal includes a lock that secures the currency container within the container cavity.
- 7) A system according to any one of the claims 1 to 6, wherein the lock includes a solenoid lock that engages at least one of:
 - a) the currency container; and,
 - b) a door to the container cavity.
- 8) A system according to any one of the claims 1 to 7, wherein the system includes a currency container including:
 - a) a container housing including a container cavity;
 - b) a lid for selectively closing the container cavity;
 - c) a securing mechanism to secure the lid;
 - d) a container communications interface;
 - e) a container memory; and,
 - f) one or more container processing devices that communicate with the one or more terminal processing devices via the communications interface.
- 9) A system according to claim 8, wherein the one or more container processing devices:
 - a) retrieve the container identifier from the container memory; and,
 - b) provide the container identifier to the terminal processing device.
- 10) A system according to claim 8 or claim 9, wherein the one or more container processing devices:
 - a) receive currency data indicative of dispensed currency from the one or more terminal processing devices; and

- b) store the currency data in the container memory.
- 11) A system according to any one of the claims 8 to 10, wherein the one or more container processing devices:
- a) receive a currency data request from a processing system;
 - b) in response to the request, retrieve the currency data from the container memory; and
 - c) provide the currency data to the processing system via the container communications interface.
- 12) A system according to any one of the claims 8 to 11, wherein the one or more container processing devices:
- a) receive requests via the container communications interface; and,
 - b) control the securing mechanism in accordance with requests to thereby selectively open or close the lid to provide access to the container cavity.
- 13) A system according to any one of the claims 8 to 12, wherein the currency container includes a reader that determines a user identity and wherein the one or more container processing devices at least one of:
- a) store the user identity in the memory;
 - b) authenticate the user at least in part using the user identity; and,
 - c) selectively perform actions based on permissions associated with the user identity.
- 14) A system according to any one of the claims 8 to 13, wherein the one or more container processing devices:
- a) determine a container status; and,
 - b) at least one of:
 - i) record an indication of the container status in the container memory; and,
 - ii) periodically broadcast an indication of the container status to a remote processing system via the container communications interface.
- 15) A system according to claim 14, wherein the currency container includes a location tracking module that tracks a location of the currency container and wherein the container status includes an indication of the container status.
- 16) A system according to any one of the claims 8 to 15, wherein the currency container includes at least one container tamper sensor, and wherein the one or more container processing devices:

- 76 -

- a) monitor changes in signals from the container tamper sensors to detect tamper events; and,
 - b) at least one of:
 - i) determine a container status in accordance with tamper events; and,
 - ii) cause an alert notification to be generated in the event that tampering is detected.
- 17) A system according to claim 16, wherein the sensors include at least one of:
- a) an accelerometer;
 - b) a position sensor;
 - c) a temperature sensor;
 - d) an air pressure sensor;
 - e) a light sensor; and,
 - f) a humidity sensor.
- 18) A system according to any one of the claims 8 to 17, wherein the securing mechanism is a drive and wherein the one or more container processing devices selectively activate the drive to thereby open or close the container lid.
- 19) A system according to any one of the claims 8 to 18, wherein the one or more container processing devices store in container memory an indication of at least one of:
- a) a container identifier;
 - b) a container status;
 - c) tamper events;
 - d) received requests;
 - e) actions performed;
 - f) a request identifier associated with received requests; and,
 - g) a payment terminal identifier.
- 20) A system according to any one of the claims 8 to 19, wherein the currency container includes an inductively charged battery.
- 21) A system according to claim 20, wherein:
- a) the payment terminal includes an inductive power transmitter positioned adjacent the container cavity; and,
 - b) the currency container includes an inductive power receiver to thereby inductively power the currency container.

- 22) A system according to any one of the claims 1 to 21, wherein the payment terminal and currency containers include:
- a) a first interface used to exchange communications information; and,
 - b) a second interface used to provide a secure communication channel between the payment terminal and the currency container using the communications information.
- 23) A system according to claim 22, wherein the communications information includes at least one of:
- a) an identifier associated with the second communications interface; and,
 - b) an encryption key.
- 24) A system according to any one of the claims 8 to 23, wherein the one or more terminal processing devices:
- a) determine user input commands indicative of a container release request;
 - b) generate a close container request;
 - c) transfer the close container request to the currency container, the one or more container processing devices being responsive to the close container message to activate the securing mechanism to secure the lid;
 - d) determine the lid is closed; and,
 - e) activate the lock to thereby release the currency container.
- 25) A system according to claim 24, wherein the one or more terminal processing devices determine the lid is closed using at least one of:
- a) a lid closed response received from the currency container; and,
 - b) signals from a lid sensor.
- 26) A system according to any one of the claims 8 to 25, wherein the one or more terminal processing devices:
- a) detect the presence of a currency container using the first communications interface;
 - b) selectively activate the lock to thereby secure the currency container;
 - c) generate an open container request;
 - d) transfer the open container request to the currency container, the one or more container processing devices being responsive to the open container request to activate the securing mechanism to open the lid;
 - e) determine the lid is open; and,

- 78 -

- f) activate the currency payment module.
- 27) A system according to claim 26, wherein the one or more terminal processing devices determine the lid is closed using at least one of:
- a) a lid open response received from the currency container; and,
 - b) signals from a lid sensor.
- 28) A system according to any one of the claims 1 to 27, wherein the one or more payment modules include:
- a) a coin currency module including a coin sensor that senses coins;
 - b) a note currency module including a note sensor that senses notes; and,
 - c) a card module including a card reader that reads payment cards.
- 29) A system according to any one of the claims 1 to 28, wherein the system includes a plurality of payment modules, and wherein the one or more terminal processing devices:
- a) cause a display to display a number of payment options;
 - b) determine a selected payment option in accordance with user input commands; and,
 - c) selectively activate one or more of the payment modules in accordance with the user input commands.
- 30) A system according to any one of the claims 1 to 29, wherein the payment module uses signals from the currency sensor to validate the received currency.
- 31) A system according to any one of the claims 1 to 30, wherein at least one payment module includes:
- a) a currency input;
 - b) a currency validator to validate received currency; and,
 - c) a currency outlet.
- 32) A system according to any one of the claims 1 to 31, wherein at least one payment module is removably mounted within the housing.
- 33) A system according to any one of the claims 1 to 32, wherein at least one payment module includes a currency store that stores currency.
- 34) A system according to claim 33, wherein the currency store includes a plurality of cartridges, each cartridge being configured to store a respective denomination of currency.

- 35) A system according to claim 34, wherein each cartridge is removably mounted to a chassis and wherein the housing includes a door to allow cartridges to be removed from the housing.
- 36) A system according to claim 35, wherein the system includes a cartridge removal tool, including a tool body having downwardly facing wings that engage a catch on the chassis to detach the cartridges from the chassis.
- 37) A system according to any one of the claims 1 to 36, wherein the transport system includes at least one of:
- a) an outlet path that transfers to a currency outlet at least one of:
 - i) change; and,
 - ii) invalid currency;
 - b) a float path that selectively transfers validated currency to or from a float storage; and,
 - c) a float dump path that selectively transfers currency from the float storage to the currency container.
- 38) A system according to claim 37, wherein the one or more terminal processing devices control the transport system in accordance with at least one of:
- a) user input commands;
 - b) signals from the payment module; and,
 - c) instructions stored in memory.
- 39) A system according to claim 37 or claim 38, wherein the one or more terminal processing devices:
- a) retrieve a current float balance and a target float level from memory;
 - b) determine a float deficit; and,
 - c) control the transport system to transfer currency having a value equal to the float deficit to the float storage.
- 40) A system according to any one of the claims 37 to 39, wherein the one or more terminal processing devices:
- a) determine a float dump request; and,
 - b) control the transport system to cause at least some currency in the float storage to be dispensed into the currency container.

- 41) A system according to any one of the claims 1 to 40, wherein the transport system includes a feeder outlet that dispenses currency through the opening in the container cavity to thereby dispense currency into the currency container.
- 42) A system according claim 41, wherein the feeder outlet is movably mounted within the housing to allow the feeder outlet to move between a dispensing position, in which the feeder outlet projects through the opening in the container cavity and a retracted position in which the feeder outlet is retracted from the opening in the container cavity.
- 43) A system according to claim 42, wherein the system includes an outlet actuator that moves the feeder outlet between the dispensing and retracted position.
- 44) A system according to any one of the claims 1 to 43, wherein the one or more terminal processing devices:
- a) determine a user request in accordance with user input commands;
 - b) determine a user identity of the user making the request;
 - c) use the user identity to at least one of:
 - i) authenticate the user; and;
 - ii) determine permissions associated with the user;
 - d) selectively perform an operation depending at least one of:
 - i) results of authentication of the user; and,
 - ii) a user permissions associated with the user.
- 45) A system according to claim 44, wherein the payment terminal includes a reader that determine the user identity.
- 46) A system according to any one of the claims 1 to 45, wherein the payment processing device:
- a) obtains transaction data indicative of a transaction performed using a transaction terminal; and,
 - b) determines the transaction amount using the transaction data.
- 47) A system according to claim 46, wherein the payment terminal intercepts transaction data on a communications network, the transaction data being intercepted as the transaction data is transferred from the transaction terminal to a network enabled device.
- 48) A system according to claim 47, wherein the payment terminal:
- a) receives network traffic directed to the network enabled device;

- b) determines transaction details if the network traffic includes transaction data; and,
 - c) forwards the network traffic to the network enabled device.
- 49) A system according to claim 47 or claim 48, wherein the payment terminal is configured in accordance with network addresses of each network enabled device.
- 50) A system according to any one of the claims 47 to 49, wherein the network enabled device is a printer.
- 51) A system according to any one of the claims 46 to 50, wherein the transaction data includes print data indicative of a transaction to be printed, and the one or more terminal processing devices determine the transaction amount from the print data.
- 52) A system according to claim 51, wherein the one or more terminal processing devices scrape the print data to determine the transaction amount.
- 53) A system according to claim 51 or claim 52, wherein the one or more terminal processing devices determine the transaction amount using at least one of:
- a) optical character recognition techniques; and,
 - b) templates defining the location of transaction details within the transaction data.
- 54) A system according to any one of the claims 51 to 53, wherein the payment terminal is updated with templates based on a format of the transaction data associated with the transaction terminals.
- 55) A system according to any one of the claims 1 to 54, wherein the payment terminal causes transaction details to be stored to allow the transaction details to be used in monitoring transaction compliance.
- 56) A system according to any one of the claims 1 to 55, wherein at least one of payment data and transaction details are stored as part of at least one of:
- a) a blockchain; and,
 - b) a remote data store.
- 57) A system according to any one of the claims 1 to 56, wherein a processing system:
- a) determines transaction details for at least one transaction;
 - b) compares the transaction details to one or more transaction rules; and,
 - c) at least one of:
 - i) determines if one or more transaction rules are breached based on results of the comparison; and,

- 82 -

- ii) causes an indication of results of the comparison to be displayed.
- 58) A system according to claim 57, wherein the transaction rules are used to identify at least one of:
- a) taxation payable; and,
 - b) suspicious activities.
- 59) A system according to claim 57 or claim 58, wherein the transaction amount includes a taxation amount, the transaction rules include taxation rules and the system is used in monitoring compliance with taxation payments.
- 60) A system according to any one of the claims 55 to 59, wherein a processing system:
- a) determines transaction details for a number of transactions associated with an entity; and,
 - b) determines an amount of tax payable by the entity in accordance with the transaction details.
- 61) A system according to any one of the claims 1 to 60, wherein the one or more terminal processing devices:
- a) periodically transmit a status notification to a processing system, the processing system being responsive to the status notification to generate a status response; and,
 - b) use the status notification and status response to at least one of:
 - i) control payment terminal communication;
 - ii) cause the payment terminal to cache transaction details; and,
 - iii) generate an alert.
- 62) A system according to any one of the claims 1 to 61, wherein the payment terminal includes at least one terminal tamper sensor, and wherein the one or more terminal processing devices:
- a) monitor changes in signals from the terminal tamper sensors to detect tampering with the payment terminal; and,
 - b) cause an alert notification to be generated in the event that tampering is detected.
- 63) A system according to claim 62, wherein the tamper sensors include at least one of:
- a) an accelerometer;
 - b) a position sensor;
 - c) a temperature sensor;

- d) an air pressure sensor;
 - e) a light sensor; and,
 - f) a humidity sensor.
- 64) A system for processing a payment for a transaction, the system including one or more terminal processing devices that:
- a) determine a transaction amount;
 - b) determine a received payment amount indicative of an amount of a received currency;
 - c) cause at least some of the currency to be dispensed into the currency container; and
 - d) cause payment data to be stored, the payment data being indicative of at least one of:
 - i) the transaction amount;
 - ii) the payment amount;
 - iii) an amount of currency dispensed into the currency container; and,
 - iv) a container identifier indicative of an identity of the currency container.
- 65) A method for processing a payment for a transaction, the method including, in one or more terminal processing devices:
- a) determining a transaction amount;
 - b) determining a received payment amount indicative of an amount of a received currency from one of a number of payment modules, at least one of the modules including a currency module having:
 - i) a currency input;
 - ii) a currency container that stores the received currency; and,
 - iii) a currency counting device that:
 - (1) receives currency from the currency input;
 - (2) validates the currency; and,
 - (3) evaluates the currency; and,
 - (4) dispenses currency into the currency container;
 - c) causing at least some of the currency to be dispensed into the currency container; and
 - d) causing payment data to be stored, the payment data being indicative of at least one of:
 - i) the transaction amount;
 - ii) the payment amount;

- 84 -

- iii) an amount of currency dispensed into the currency container; and,
 - iv) a container identifier indicative of an identity of the currency container.
- 66) A container for receiving security documents, wherein the container includes:
- a) a container housing including a container cavity;
 - b) a lid for selectively closing the container cavity;
 - c) a securing mechanism to secure the lid;
 - d) a container communications interface;
 - e) a container memory; and,
 - f) one or more container processing devices that communicate with one or more terminal processing devices via the communications interface to control the securing mechanism in accordance with requests received via the container communications interface to selectively open or close the lid to provide access to the container cavity.
- 67) A container according to claim 66, wherein the one or more container processing devices:
- a) retrieve the container identifier from the container memory; and,
 - b) provide the container identifier to a terminal processing device.
- 68) A system according to claim 66 or claim 67, wherein the one or more container processing devices:
- a) receive currency data indicative of dispensed currency from the one or more terminal processing devices; and
 - b) store the currency data in the container memory.
- 69) A container according to any one of the claims 66 to 68, wherein the document container includes a reader that determines a user identity and wherein the one or more container processing devices at least one of:
- a) store the user identity in the memory; and,
 - b) authenticate the user at least in part using the user identity; and,
 - c) selectively perform actions based on permissions associated with the user identifier.
- 70) A container according to any one of the claims 66 to 69, wherein the one or more container processing devices:
- a) determine a container status; and,
 - b) at least one of:
 - i) recording an indication of the container status in the container memory; and,

- ii) periodically broadcast an indication of the container status to a remote processing system via the container communications interface.
- 71) A container according to any one of the claims 66 to 70, wherein the currency container includes a location tracking module that tracks a location of the currency container and wherein the container status includes an indication of the container status.
- 72) A container according to any one of the claims 66 to 71, wherein the currency container includes at least one container tamper sensor, and wherein the one or more container processing devices:
- a) monitor changes in signals from the container sensors to detect tamper events; and,
 - b) at least one of:
 - i) determine the container status in accordance with tamper events; and,
 - ii) cause an alert notification to be generated in the event that tampering is detected.
- 73) A container according to claim 72, wherein the sensors include at least one of:
- a) an accelerometer;
 - b) a position sensor;
 - c) a temperature sensor;
 - d) an air pressure sensor;
 - e) a light sensor; and,
 - f) a humidity sensor.
- 74) A container according to any one of the claims 66 to 73, wherein the document container includes an inductively charged battery.
- 75) A container according to any one of the claims 66 to 74, wherein the document container includes:
- a) a first interface used to exchange communications information; and,
 - b) a second interface used to provide a secure communication channel with the one or more terminal processing devices.
- 76) A container according to claim 75, wherein the communications information includes at least one of:
- a) an identifier associated with the second communications interface; and,
 - b) an encryption key.

- 77) A container according to any one of the claims 66 to 76, wherein the securing mechanism is a drive and wherein the one or more terminal processing devices selectively activate the drive to thereby open or close the container lid.
- 78) A container according to any one of the claims 66 to 77, wherein the one or more container processing devices store in memory an indication of at least one of:
- a) a container identifier;
 - b) a container status;
 - c) tamper events;
 - d) received requests;
 - e) actions performed;
 - f) a request identifier associated with received requests; and,
 - g) a payment terminal identifier.
- 79) A cartridge removal tool for removing cartridges from a payment module, the cartridge removal tool including a tool body having downwardly facing wings that engage a catch on a chassis of the payment module to detach a cartridge from the chassis.
- 80) A cartridge removal tool according to claim 79, wherein the tool body includes a flat front underside and an upwardly sloping rear underside.
- 81) A cartridge removal tool according to claim 79 or claim 80, wherein the downwardly extending wings are provided proximate a front of the tool body but laterally spaced therefrom.
- 82) A cartridge removal tool according to any one of the claims 79 to 81, wherein the tool body includes lateral tabs extending outwardly from sides of the body to support the downwardly extending wings.
- 83) A cartridge removal tool according to claim 82, wherein the tabs support L-shaped guides extending downwardly and outwardly from the tabs, rearwardly and outwardly of the wings.
- 84) A method of using a cartridge removal tool to remove cartridges from a payment module, the cartridge removal tool including a body having downwardly facing wings that engage a catch on a chassis of the payment module to detach a cartridge from the chassis and the method including positioning the cartridge removal tool on an upper surface of a

cartridge, and urging the wings into engagement with a catch to thereby release the cartridge.

- 85) A method according to claim 84, wherein the tool body is positioned on a top surface of a cartridge, with a sloped rear underside flush against the top of the cartridge, with the tool body being pushed forwardly until the wings are in position to release the catch.
- 86) A method according to claim 85, wherein the tool body is pushed forwardly until tabs engage or are aligned with side walls of the payment module.
- 87) A method according to claim 85 or claim 86, wherein the tool body is rotated so that a flat underside of the tool body lies flat against an upper surface of the cartridge so that the wings engage a catch and release the cartridge.
- 88) A method according to claim 88, wherein the tool is urged rearwardly so that the wings engage a mounting pin of the cartridge allowing the mounting pin to be lifted from within a channel thereby releasing the cartridge.

1/28

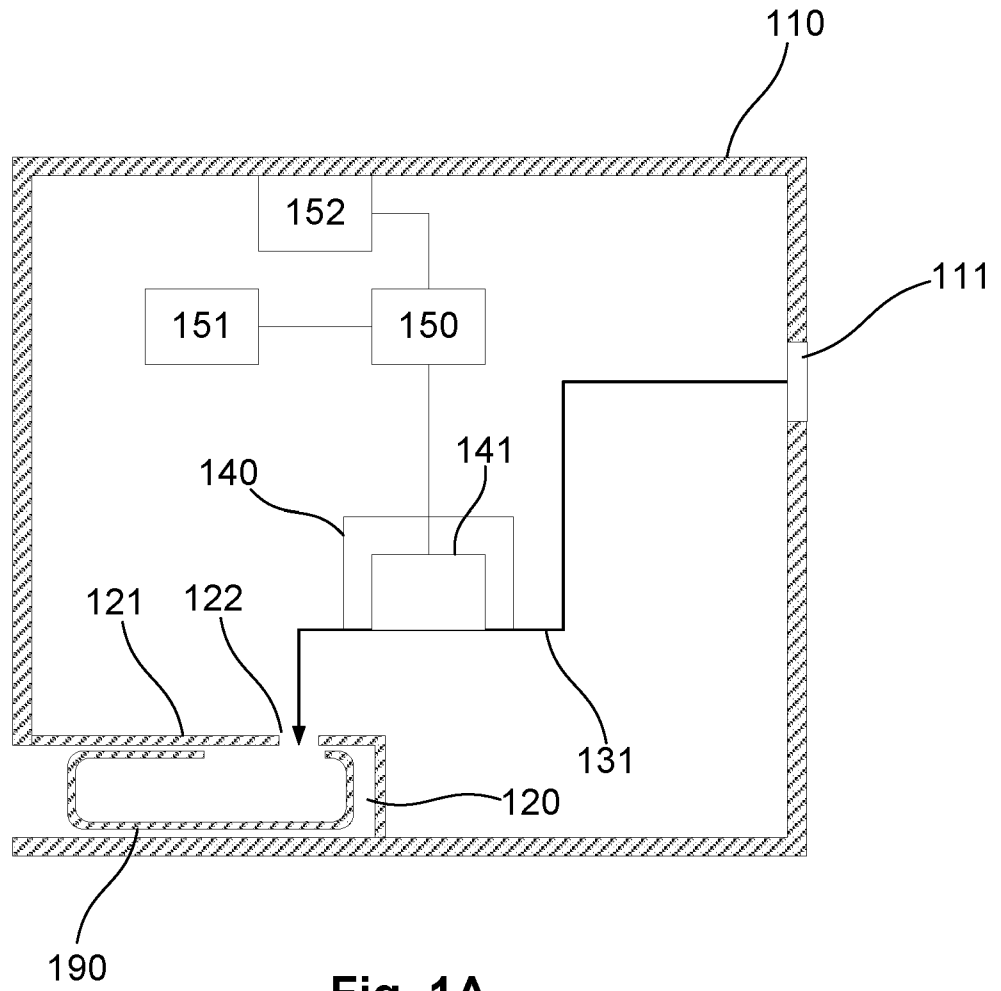


Fig. 1A

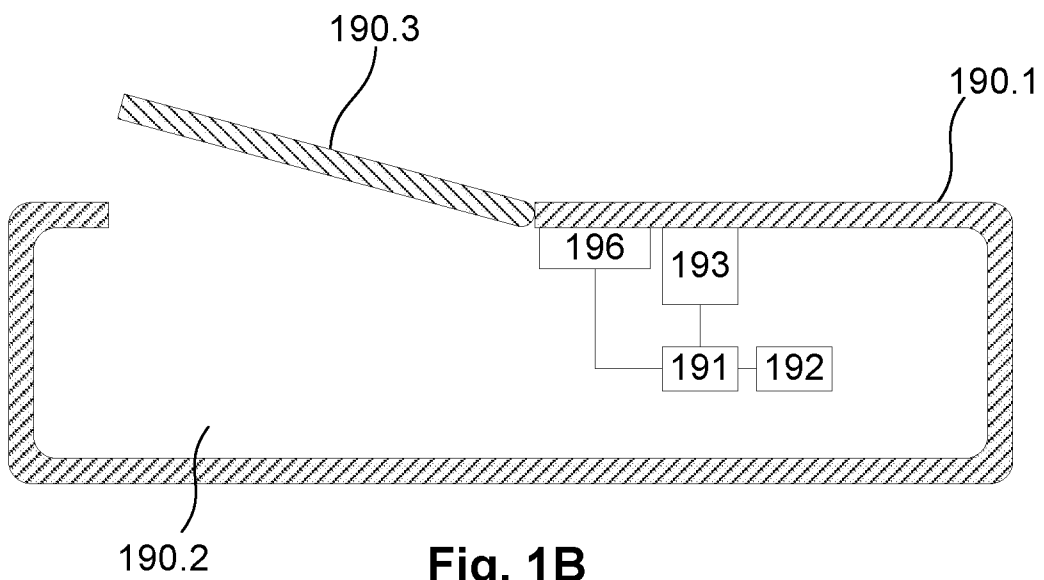


Fig. 1B

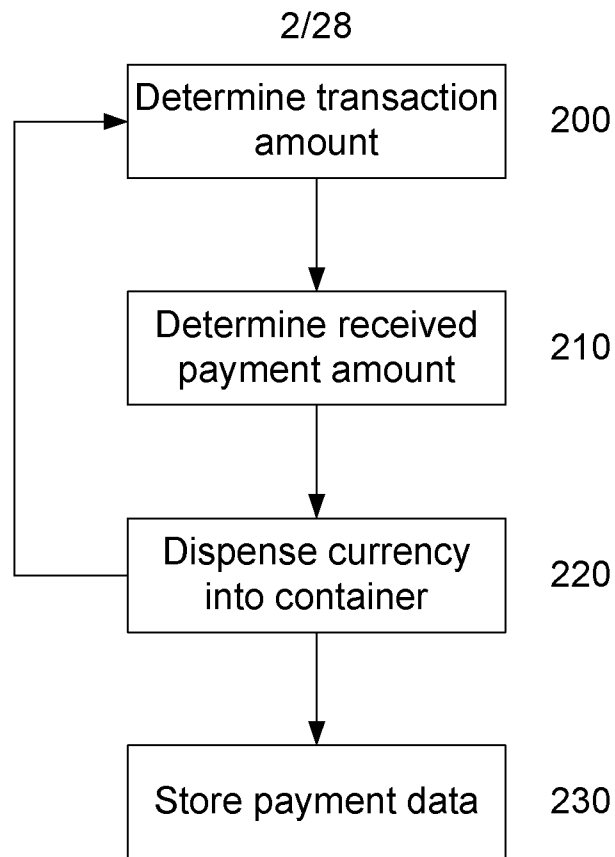


Fig. 2

3/28

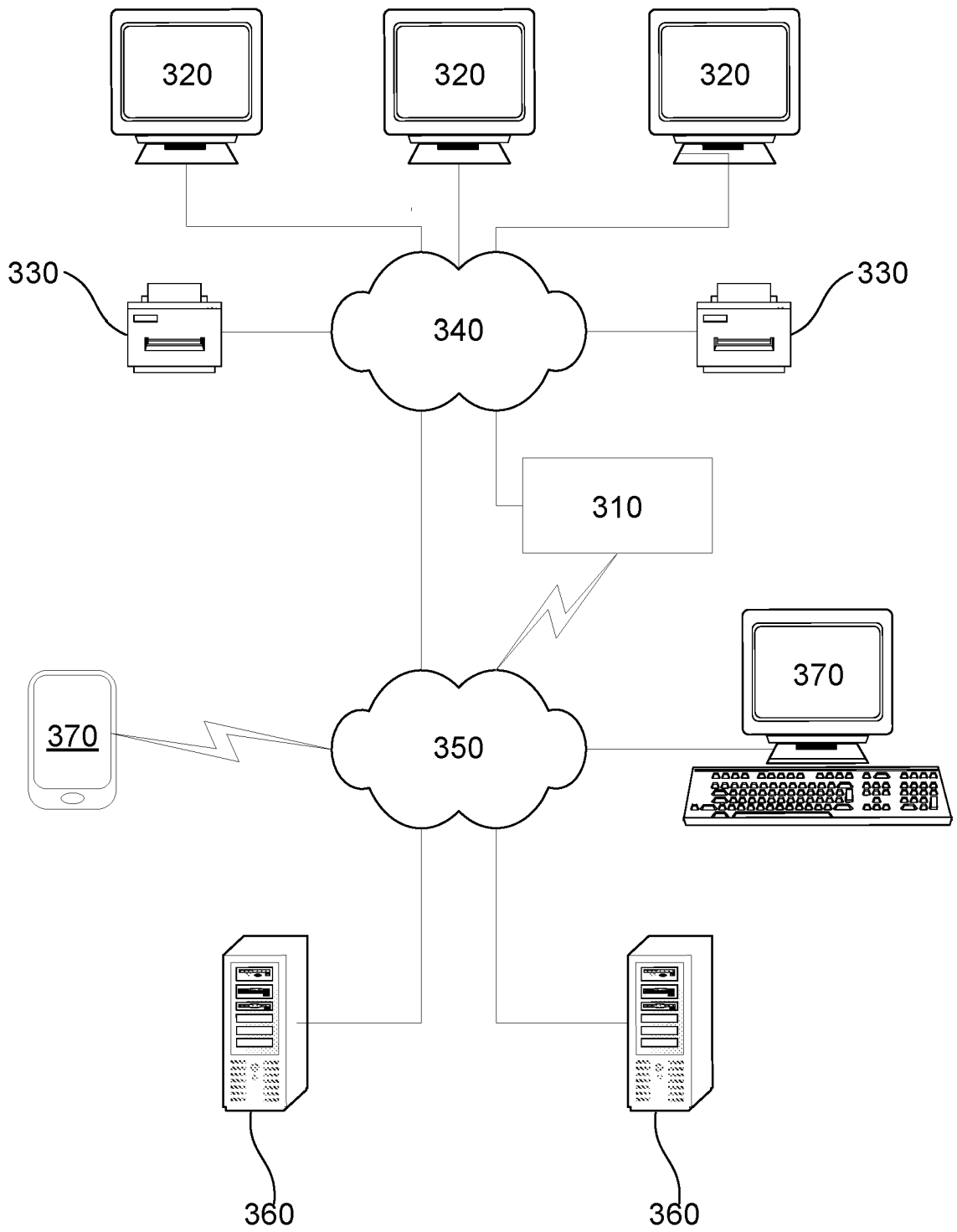


Fig. 3

4/28

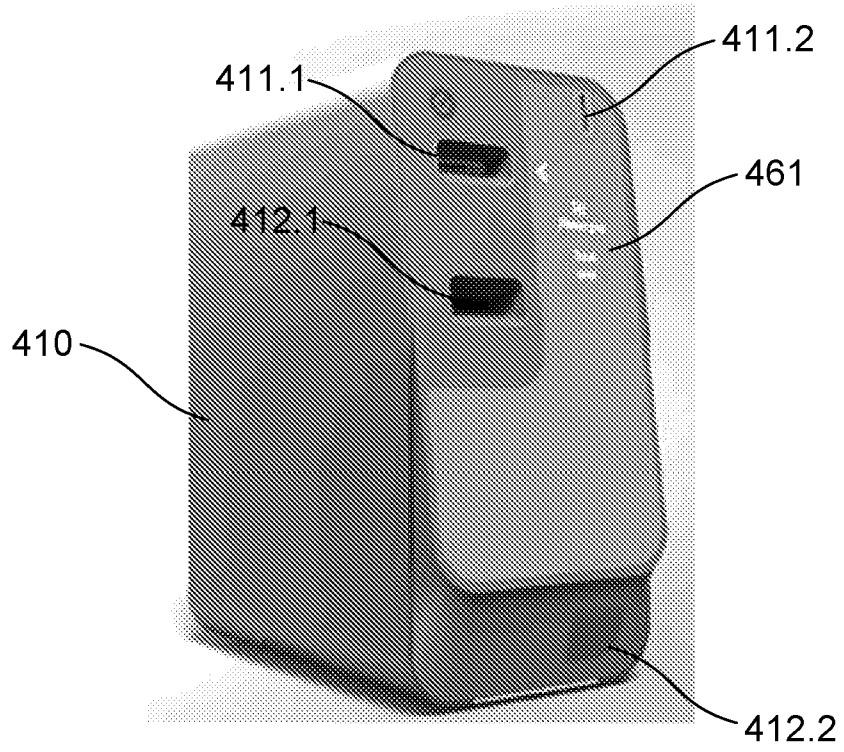


Fig. 4A

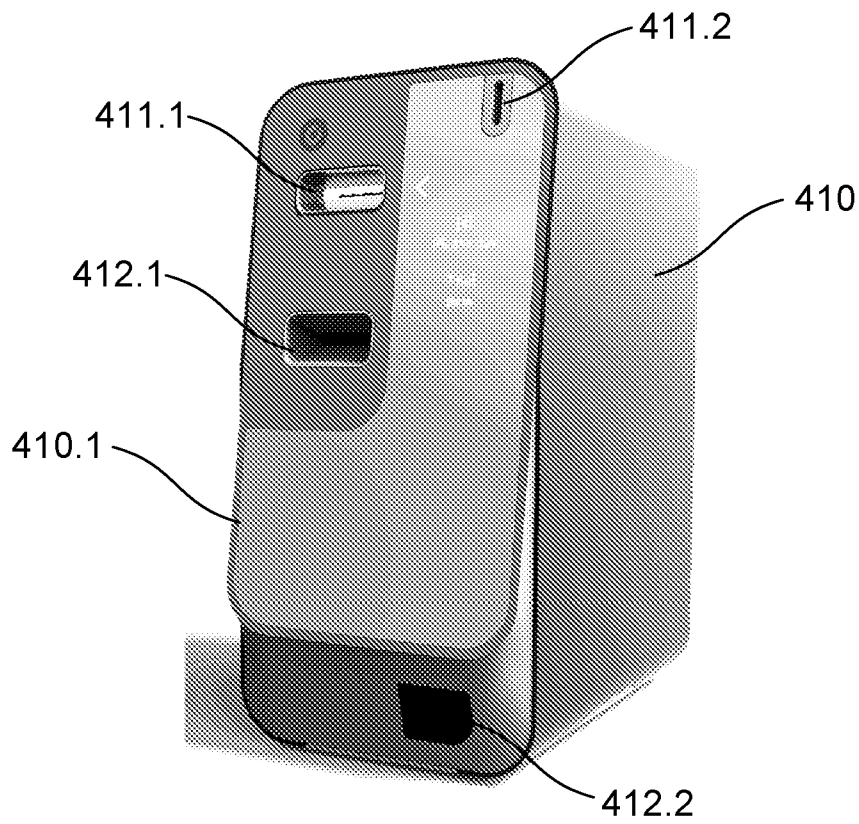


Fig. 4B

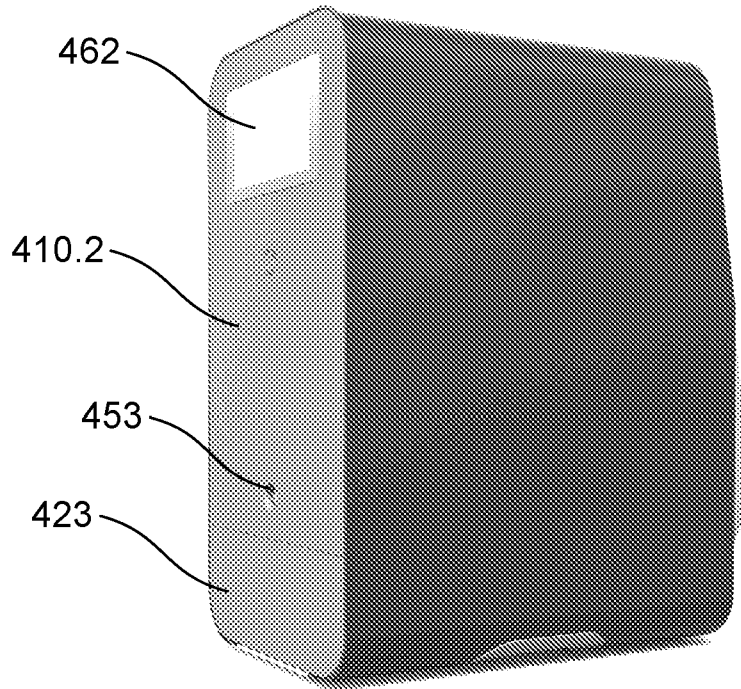


Fig. 4C

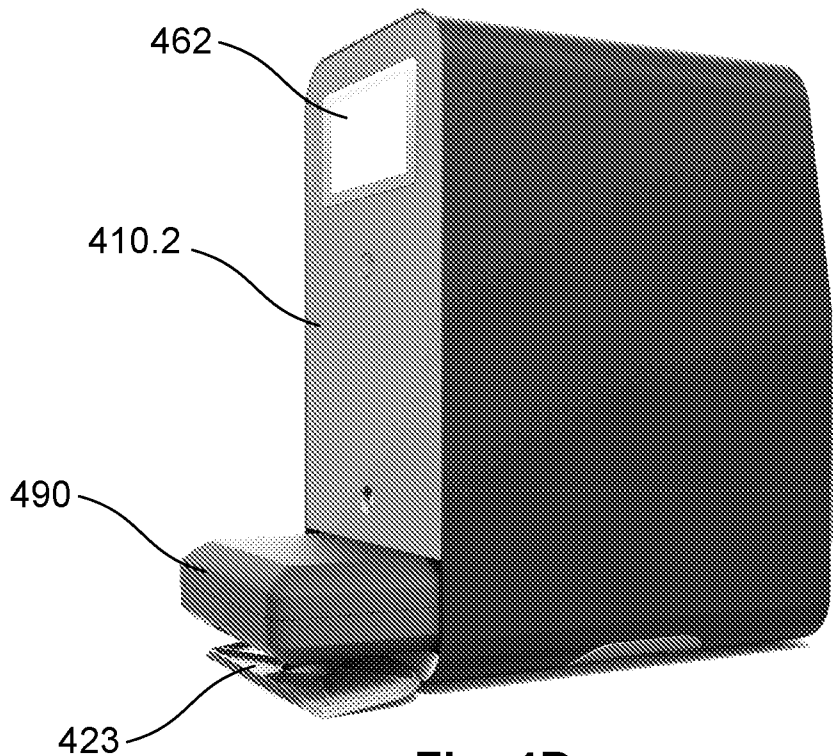


Fig. 4D

6/28

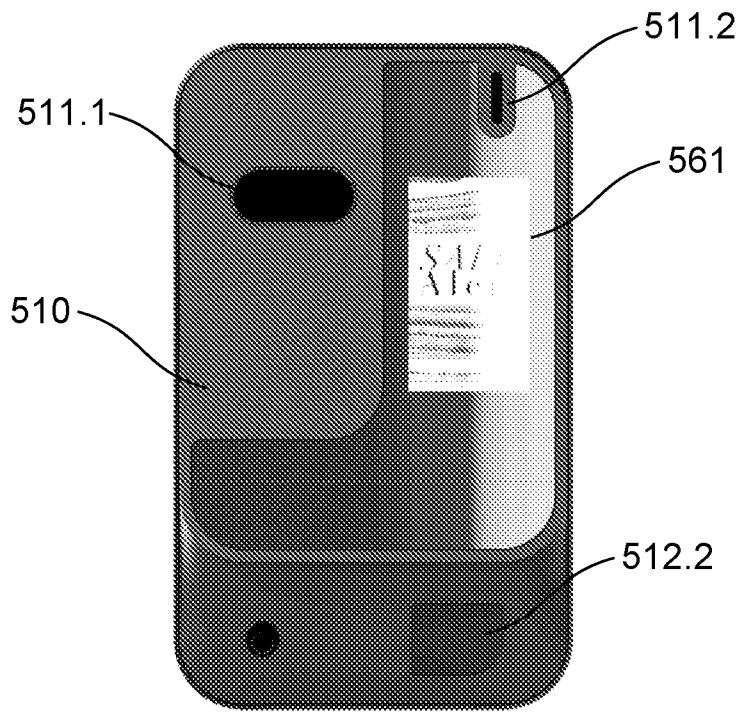


Fig. 5A

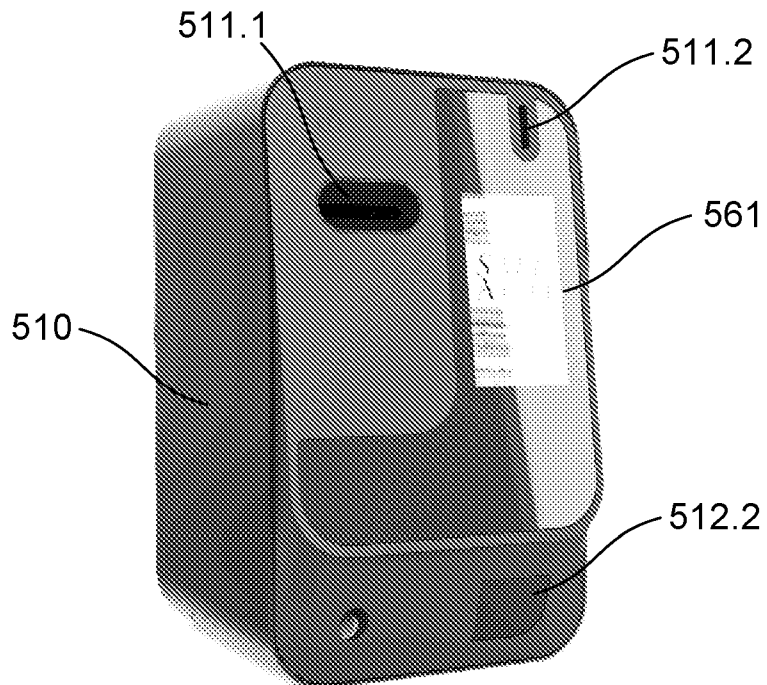


Fig. 5B

7/28

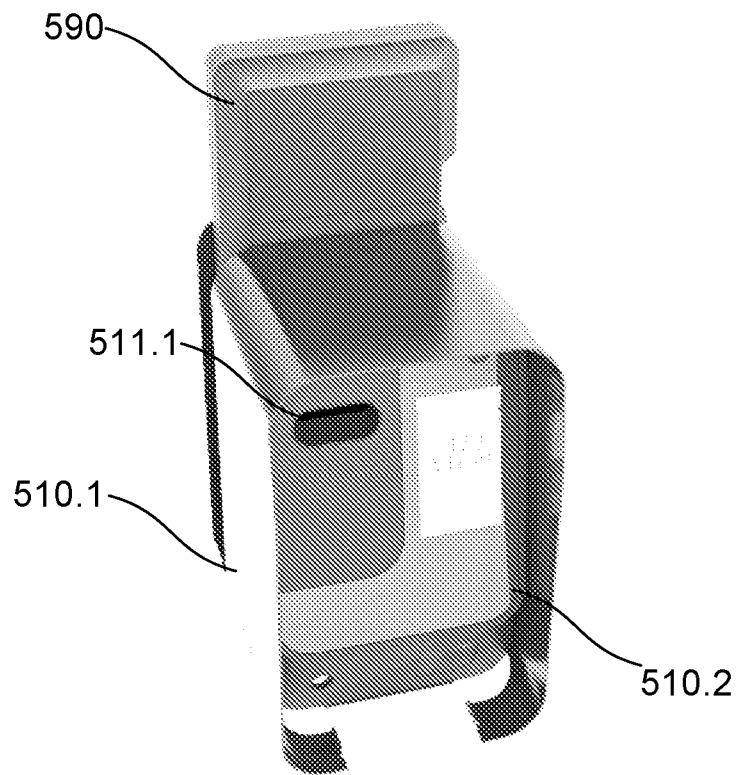


Fig. 5C

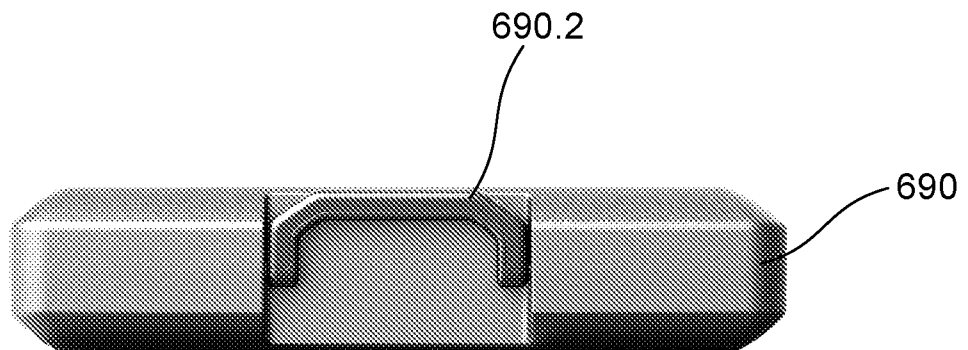


Fig. 6A

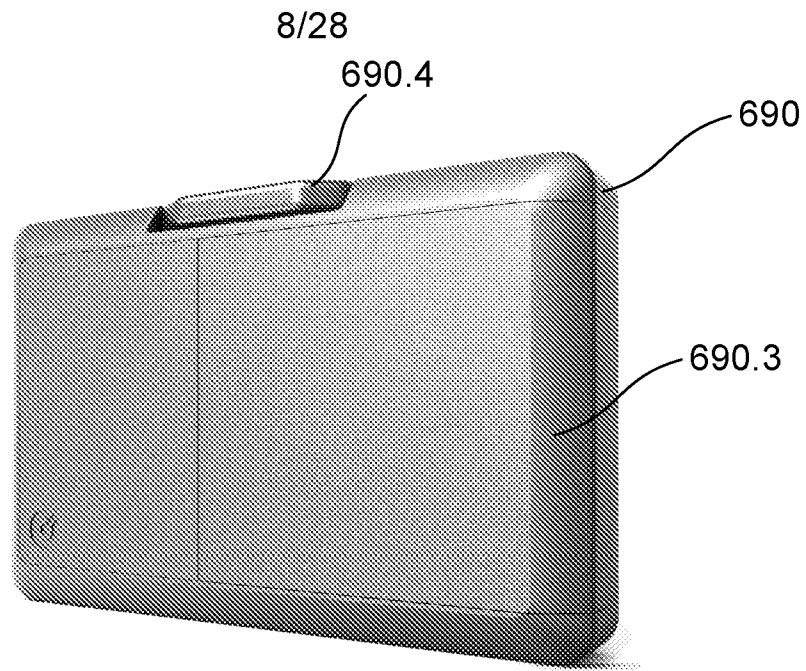


Fig. 6B

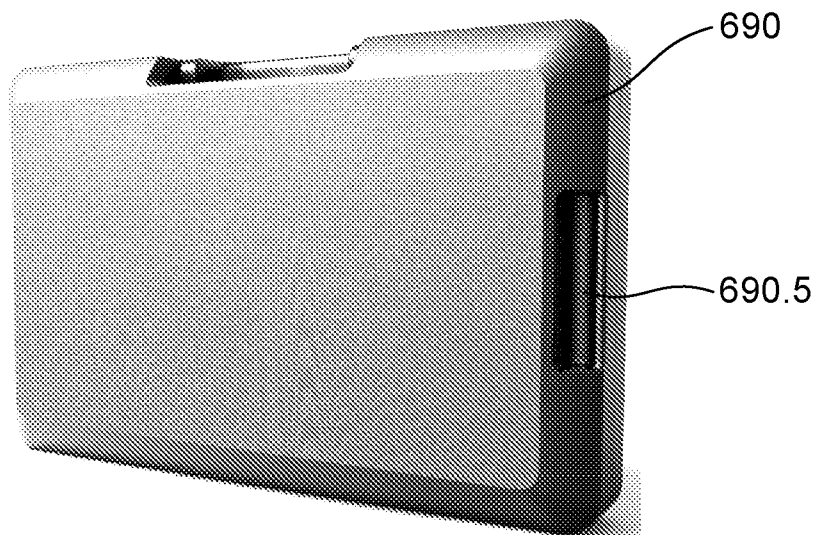


Fig. 6C

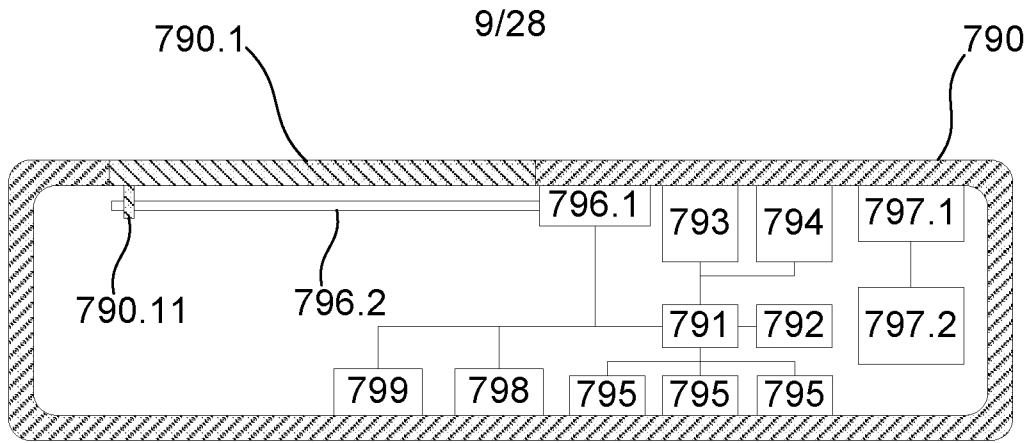


Fig. 7

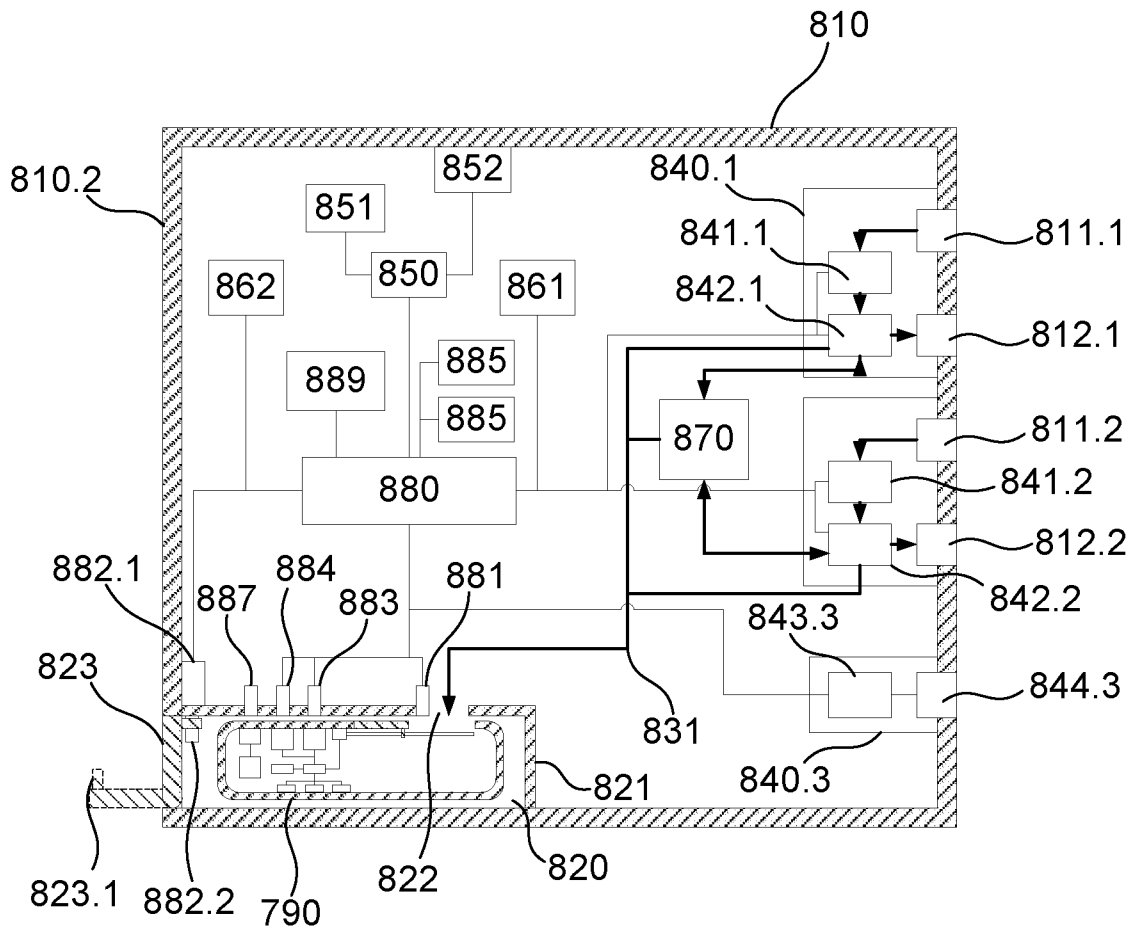


Fig. 8

10/28

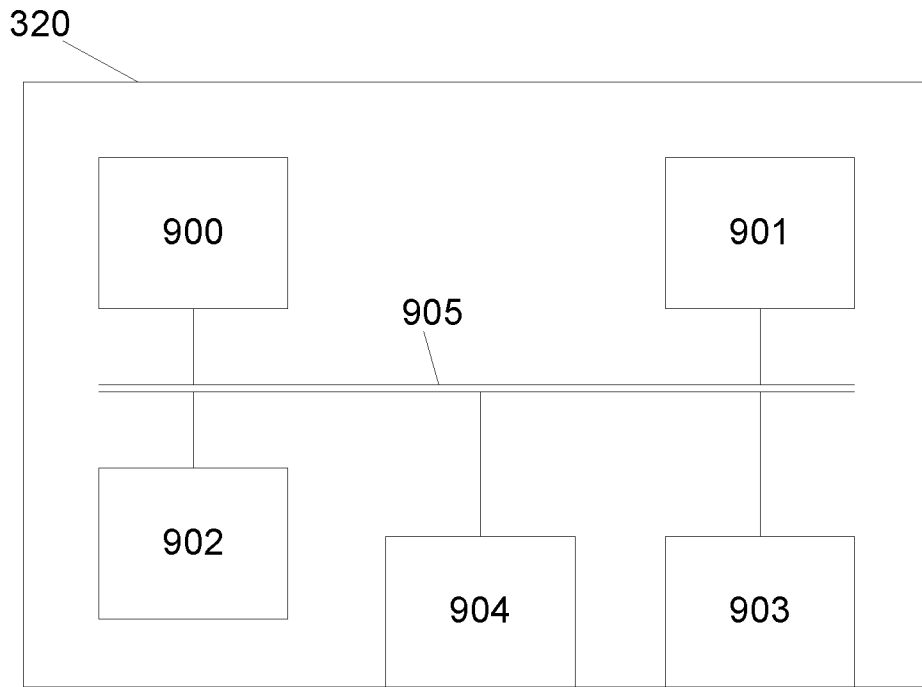


Fig. 9

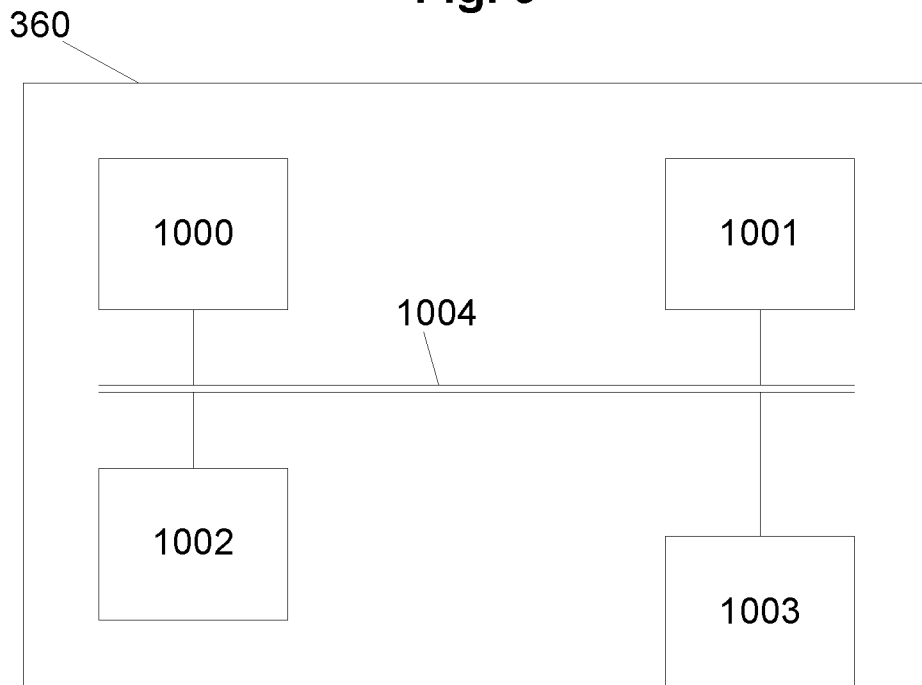


Fig. 10

11/28

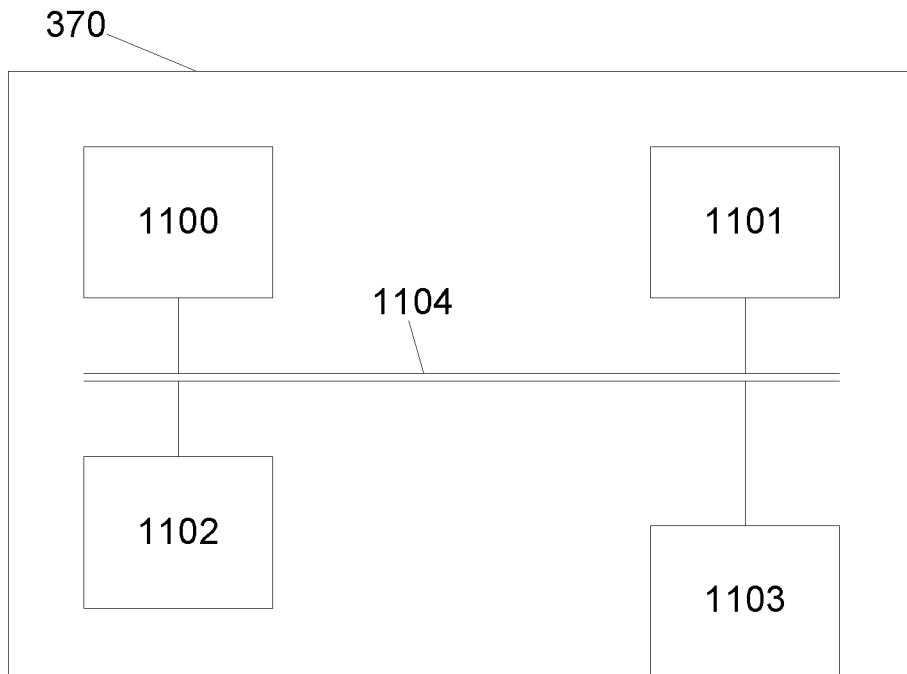


Fig. 11

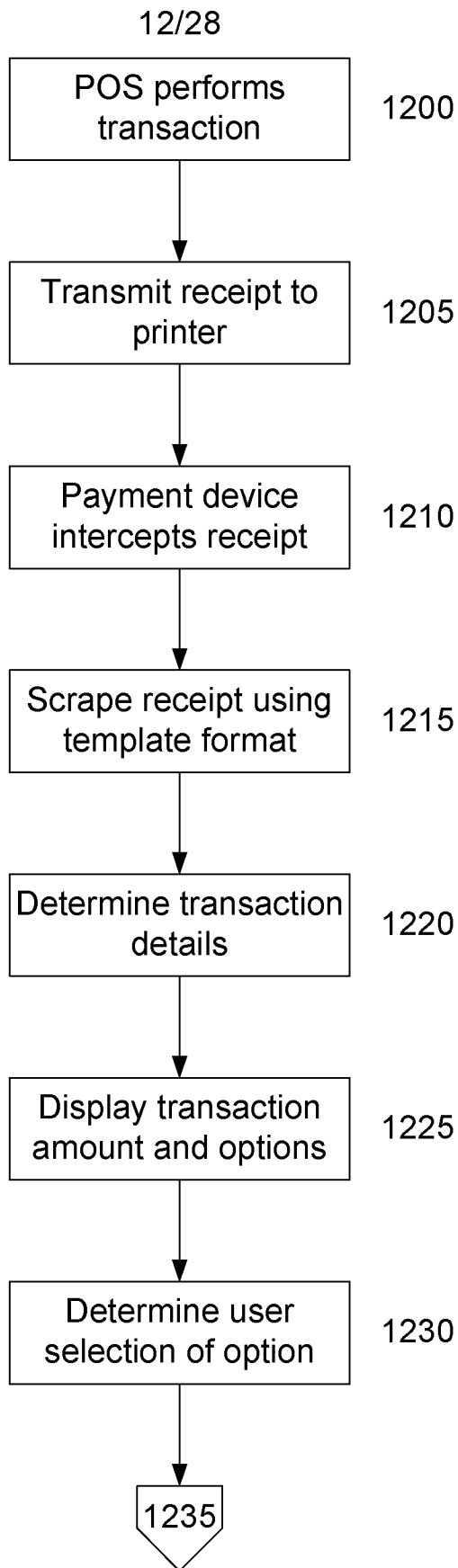


Fig. 12A

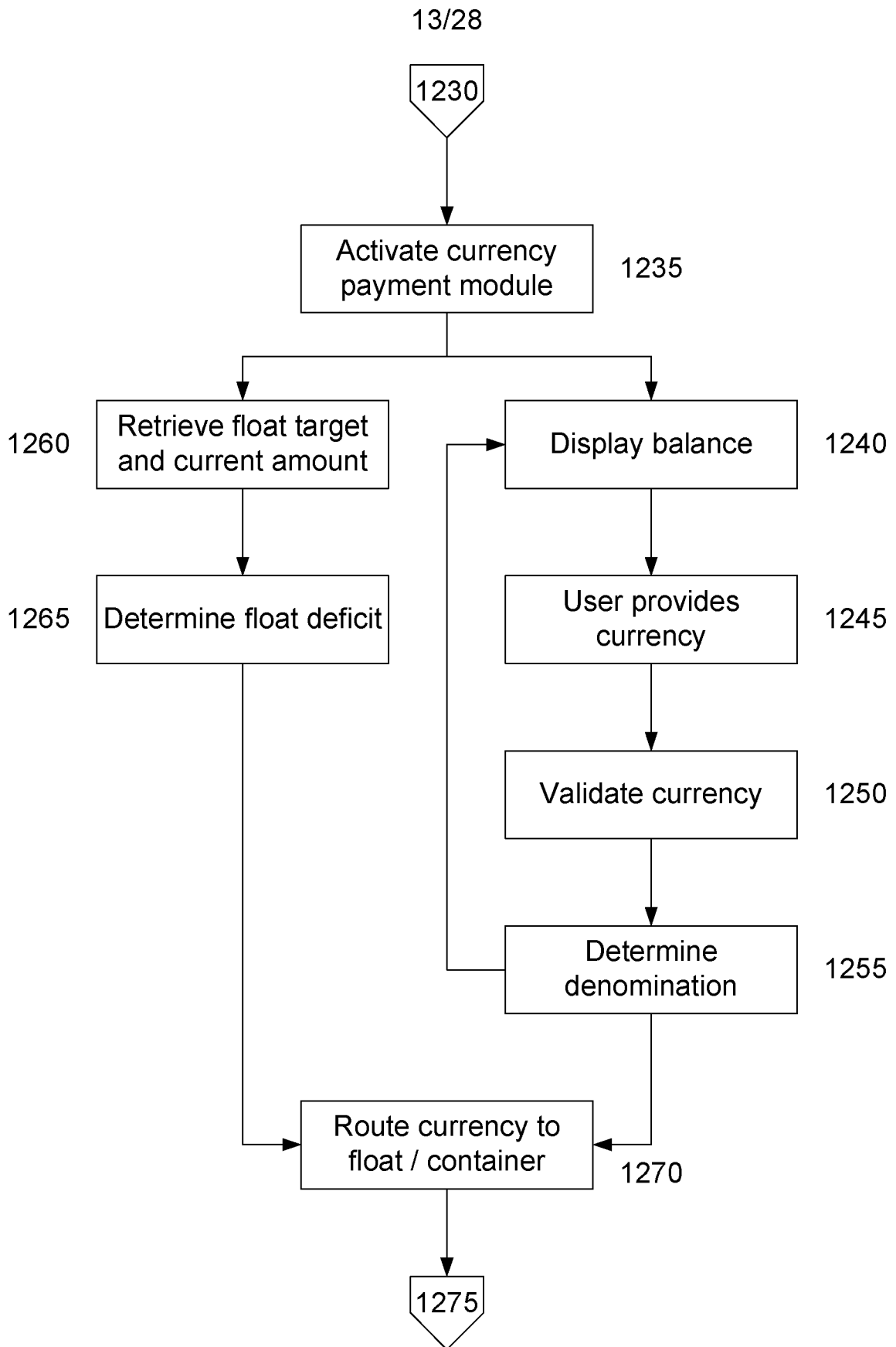


Fig. 12B

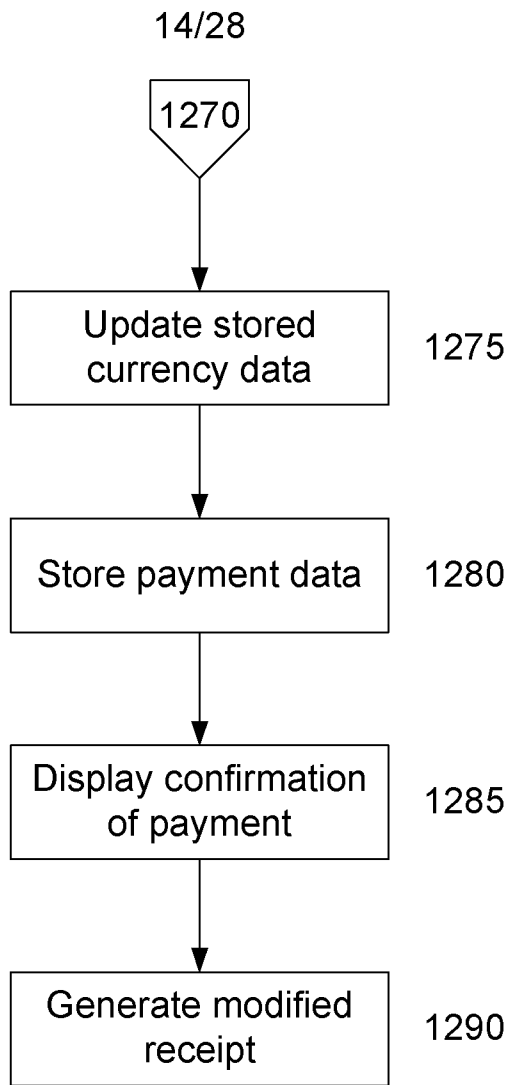


Fig. 12C

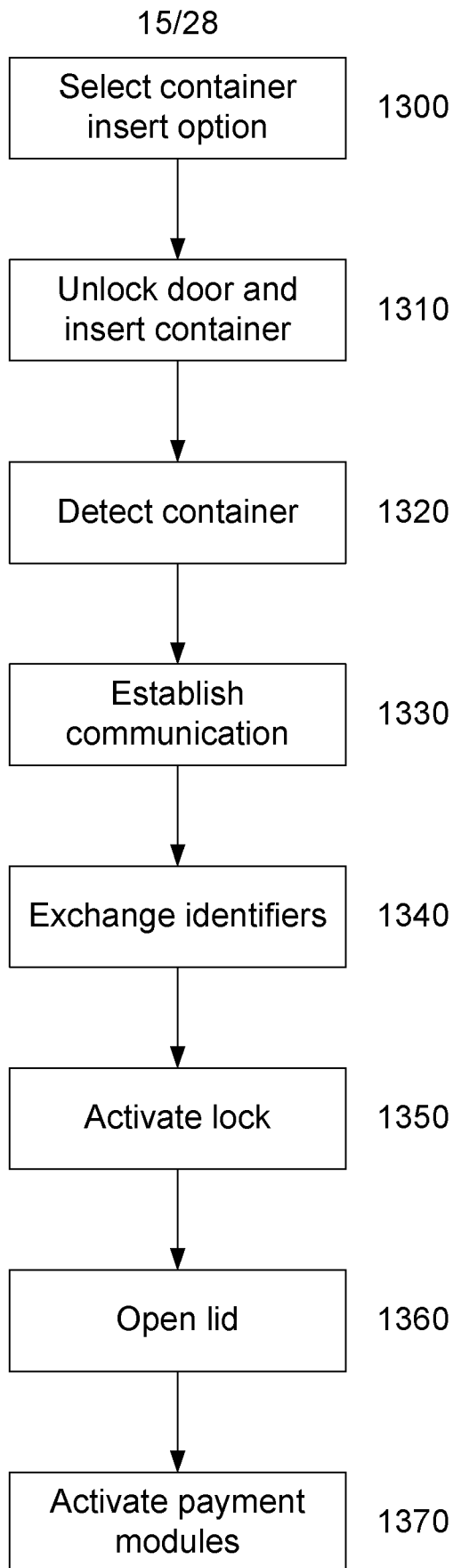


Fig. 13

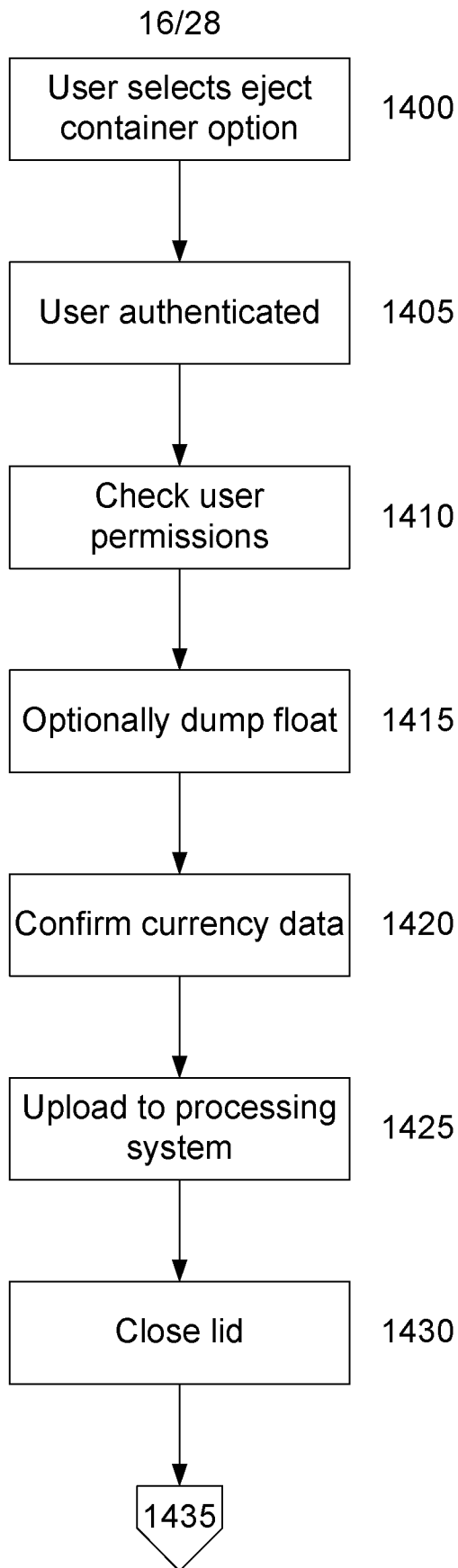


Fig. 14A

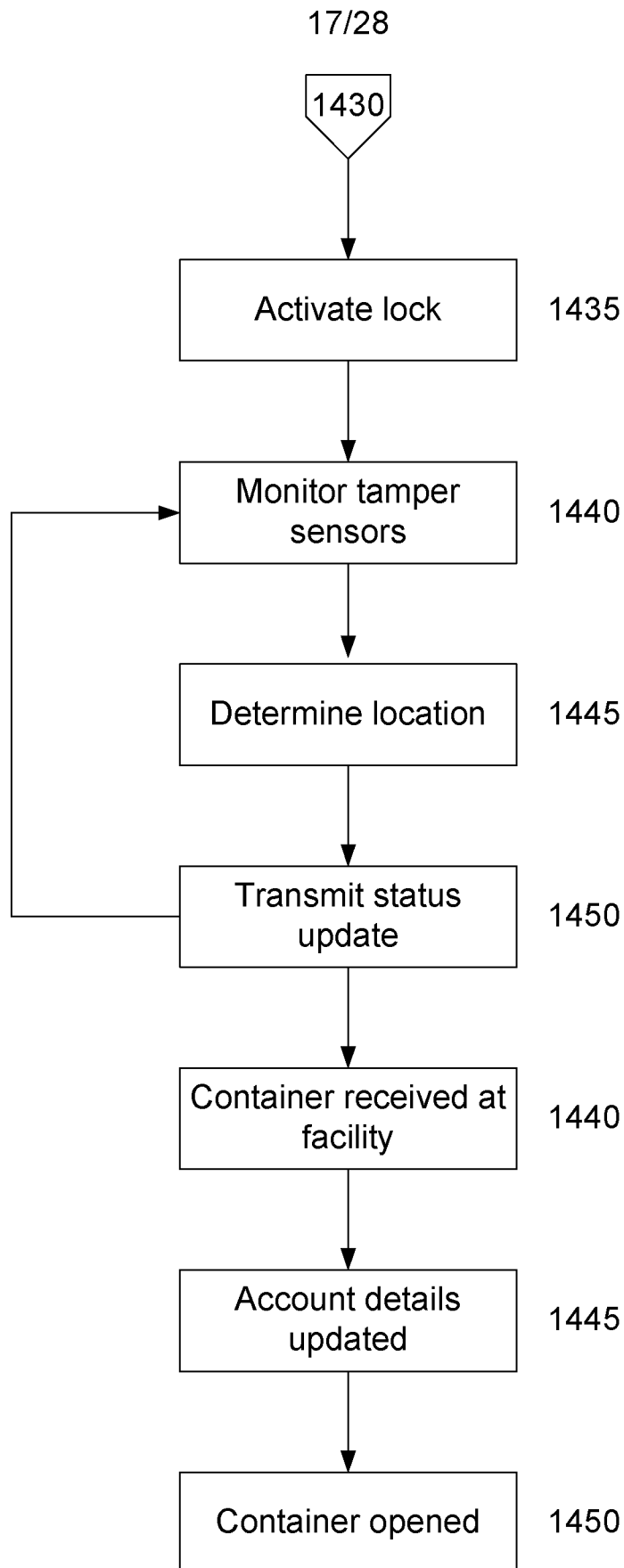


Fig. 14B

18/28

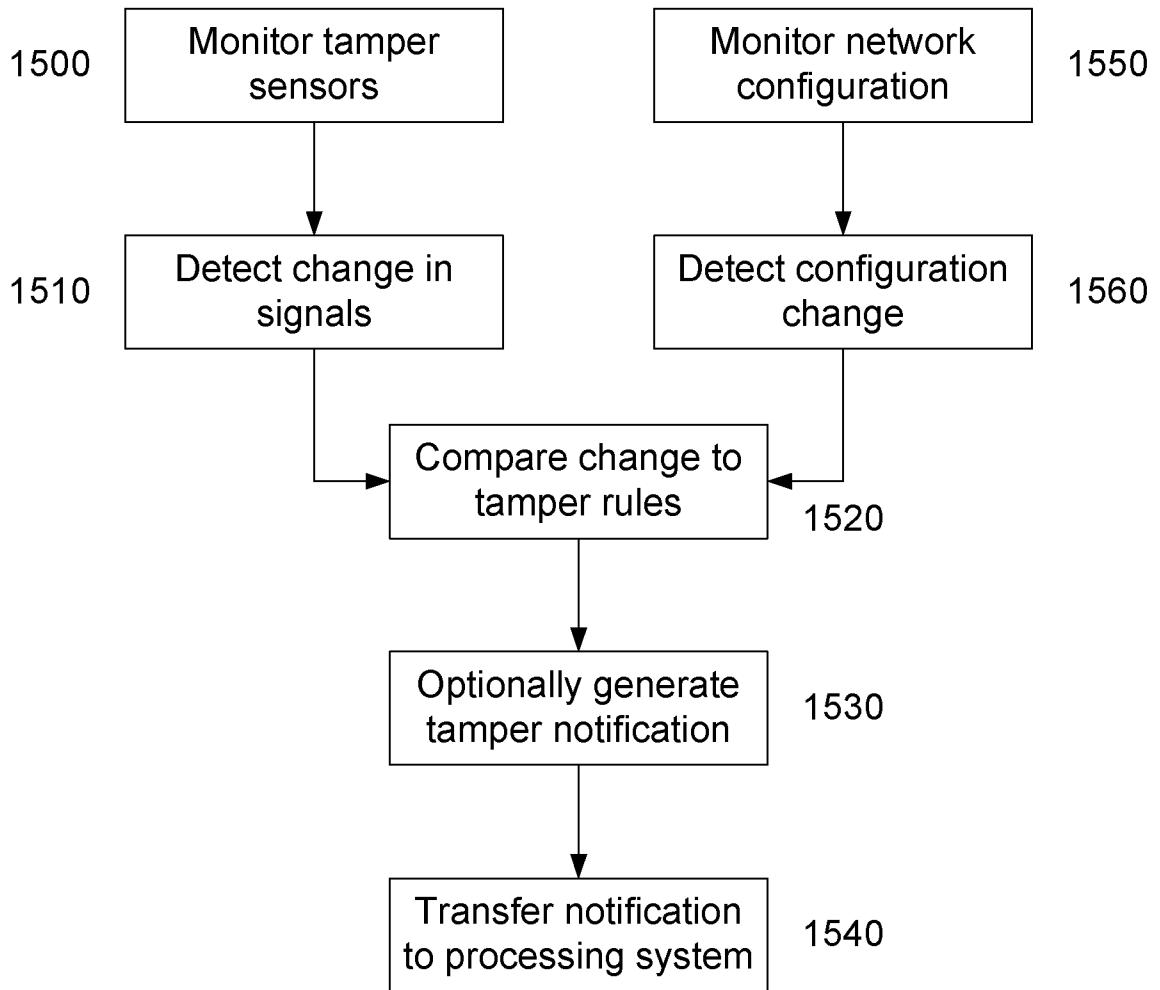


Fig. 15

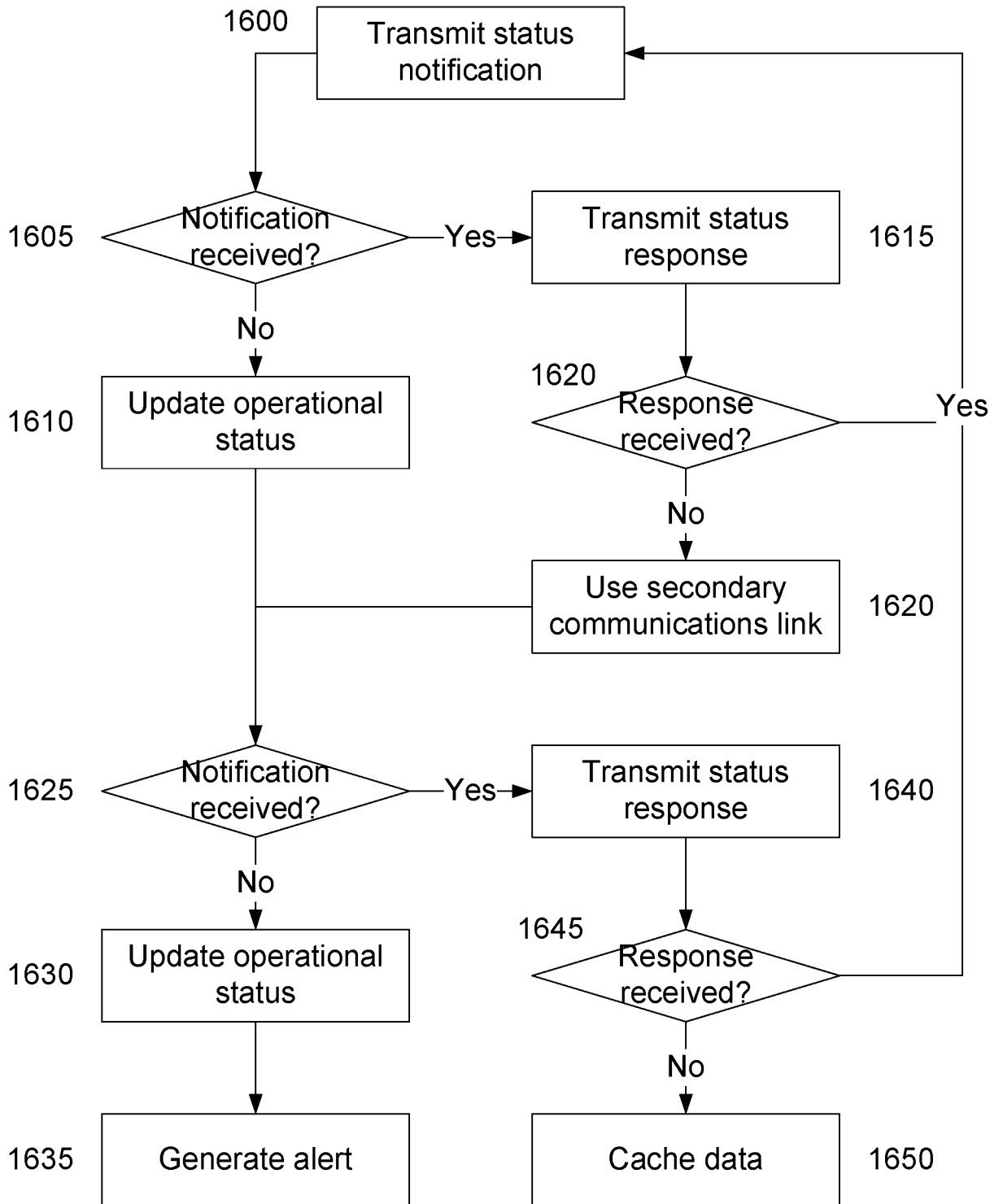


Fig. 16

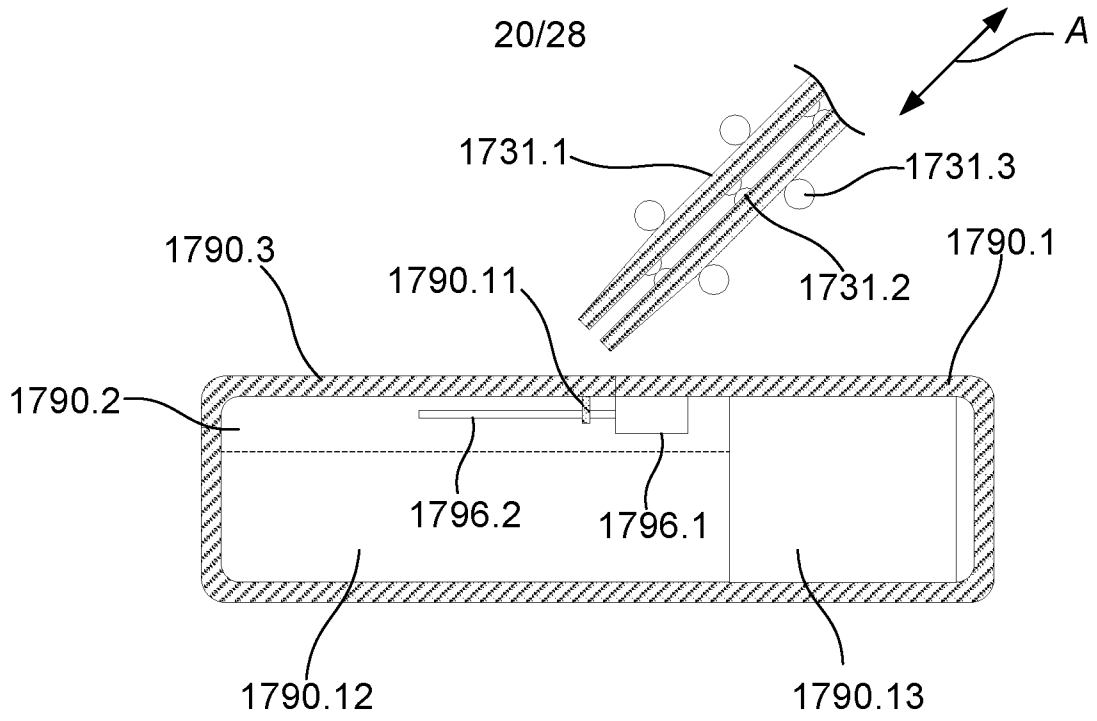


Fig. 17A

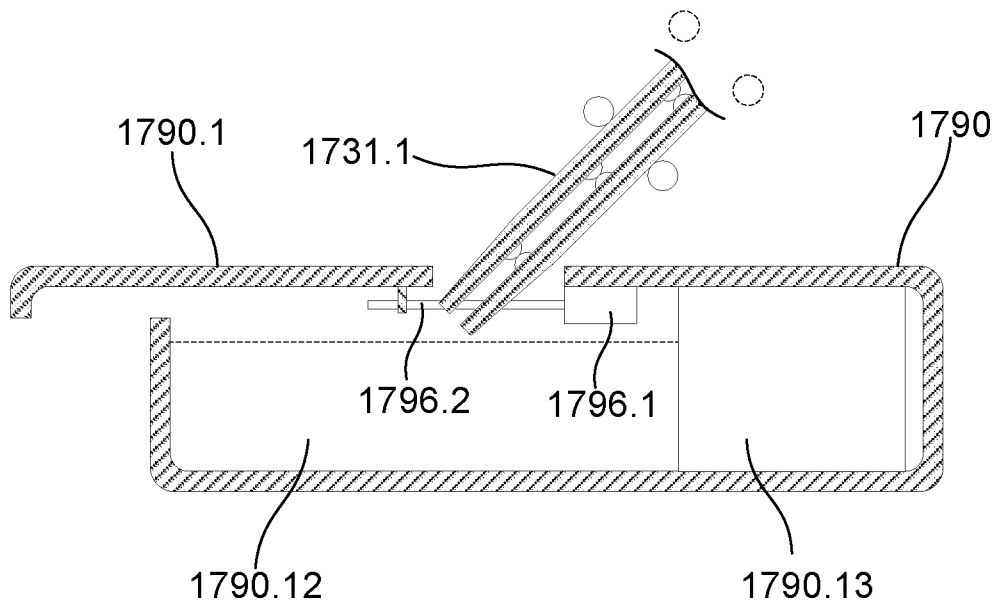


Fig. 17B

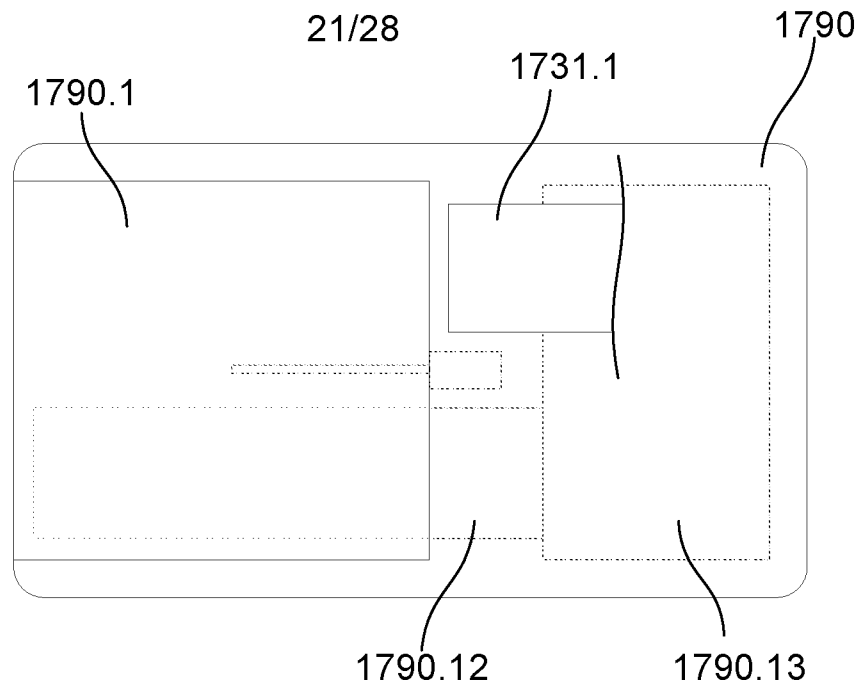


Fig. 17C

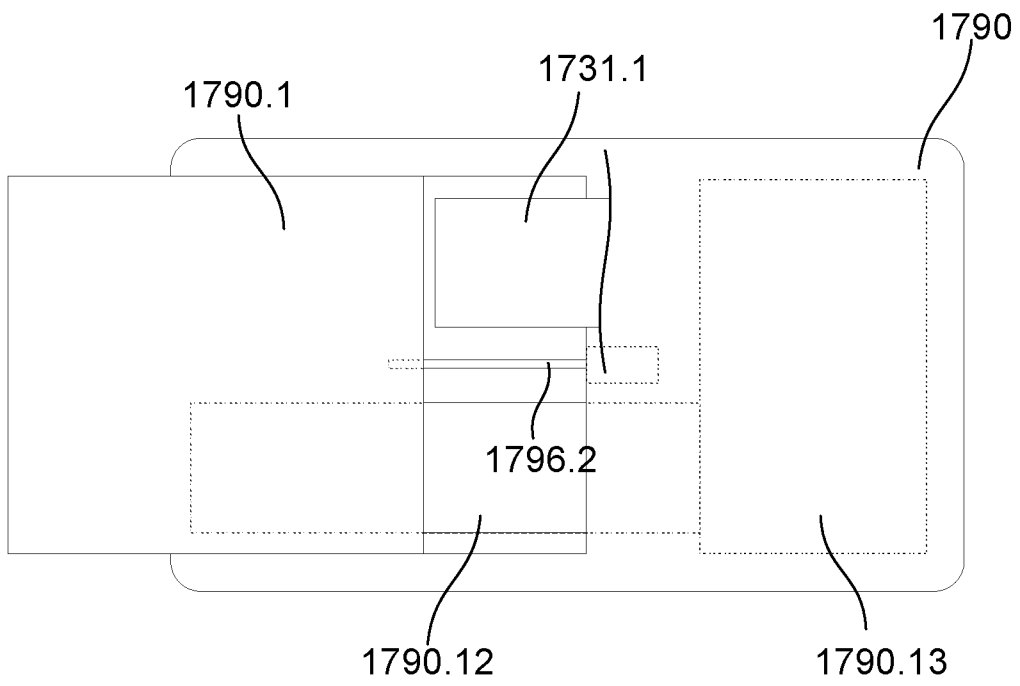


Fig. 17D

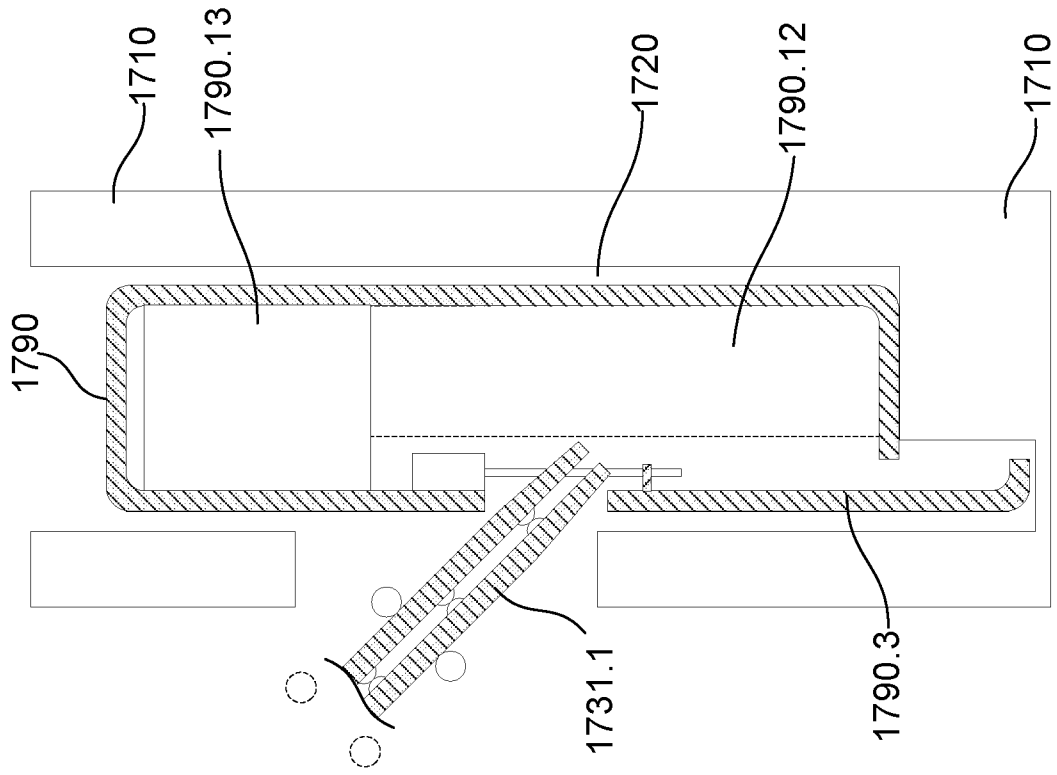


Fig. 17F

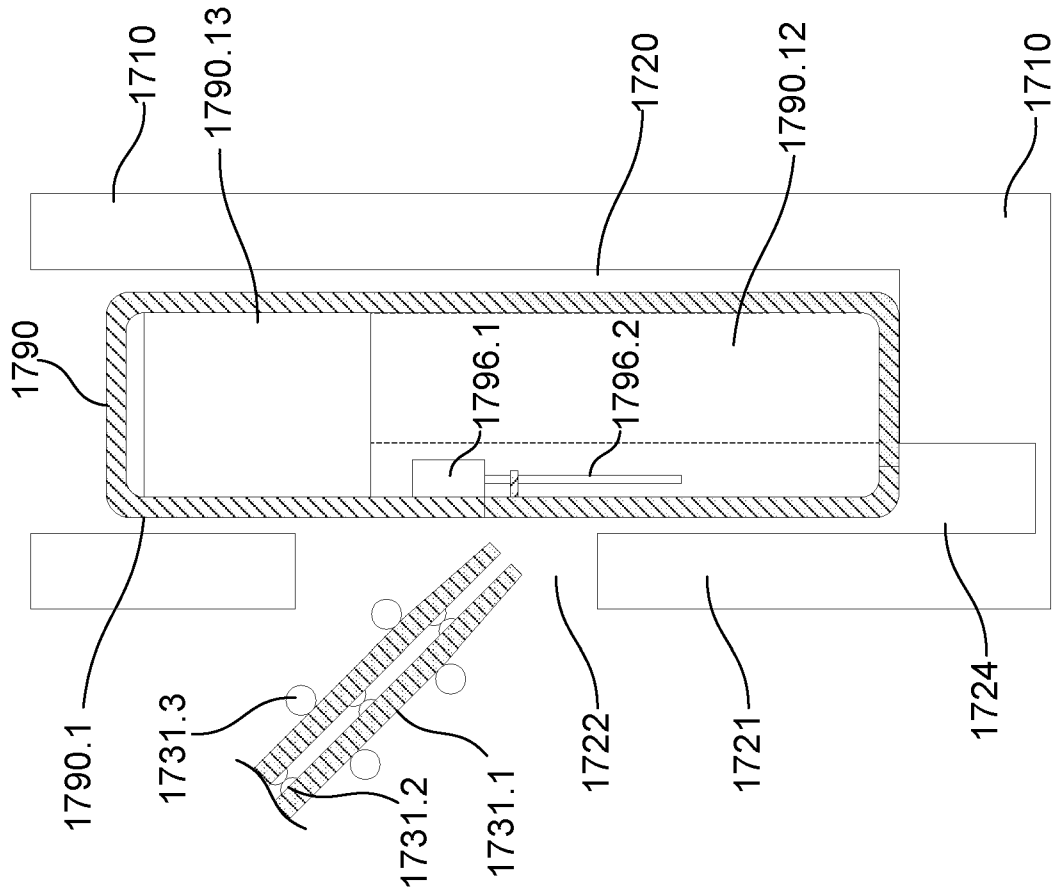


Fig. 17E

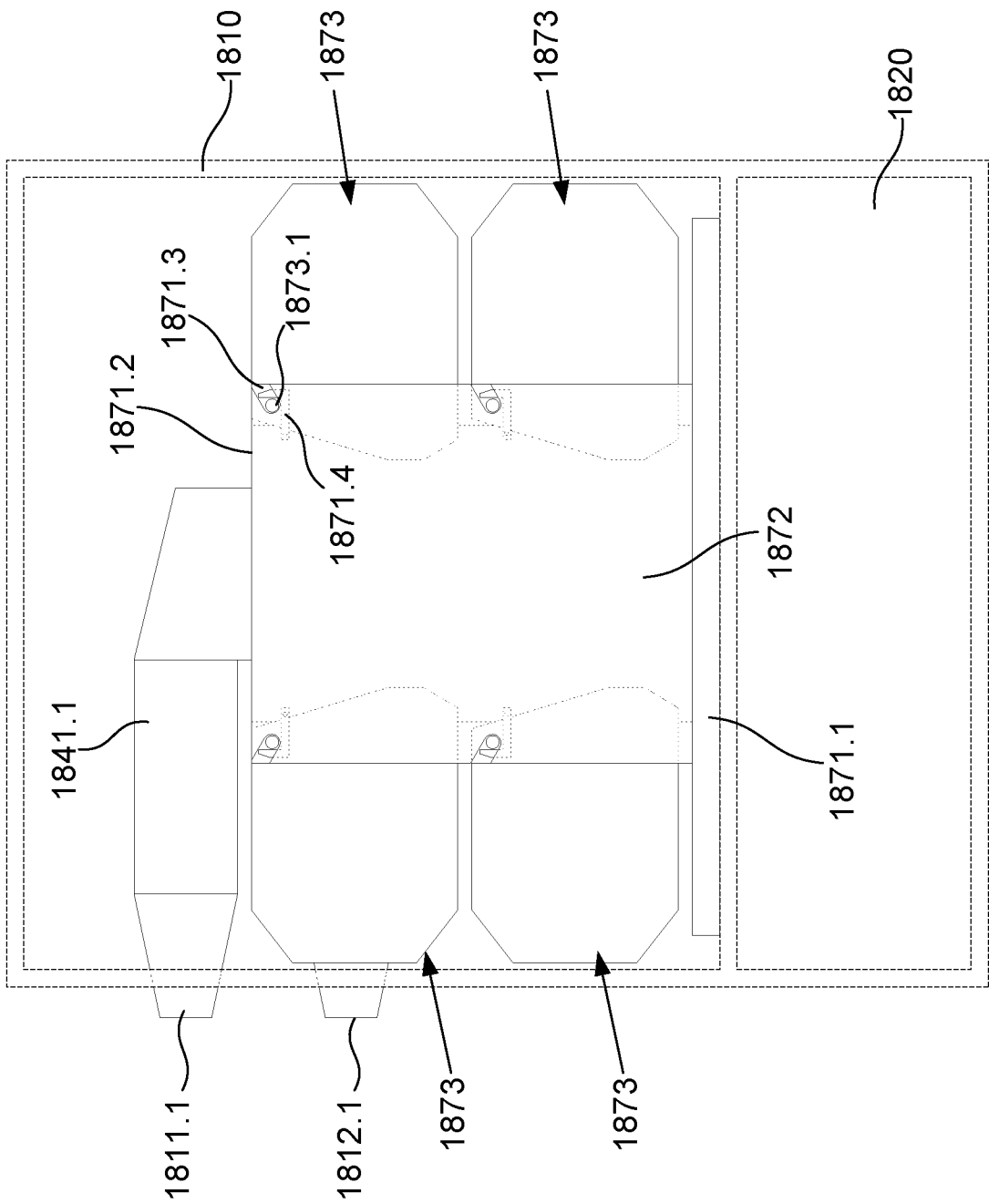


Fig. 18A

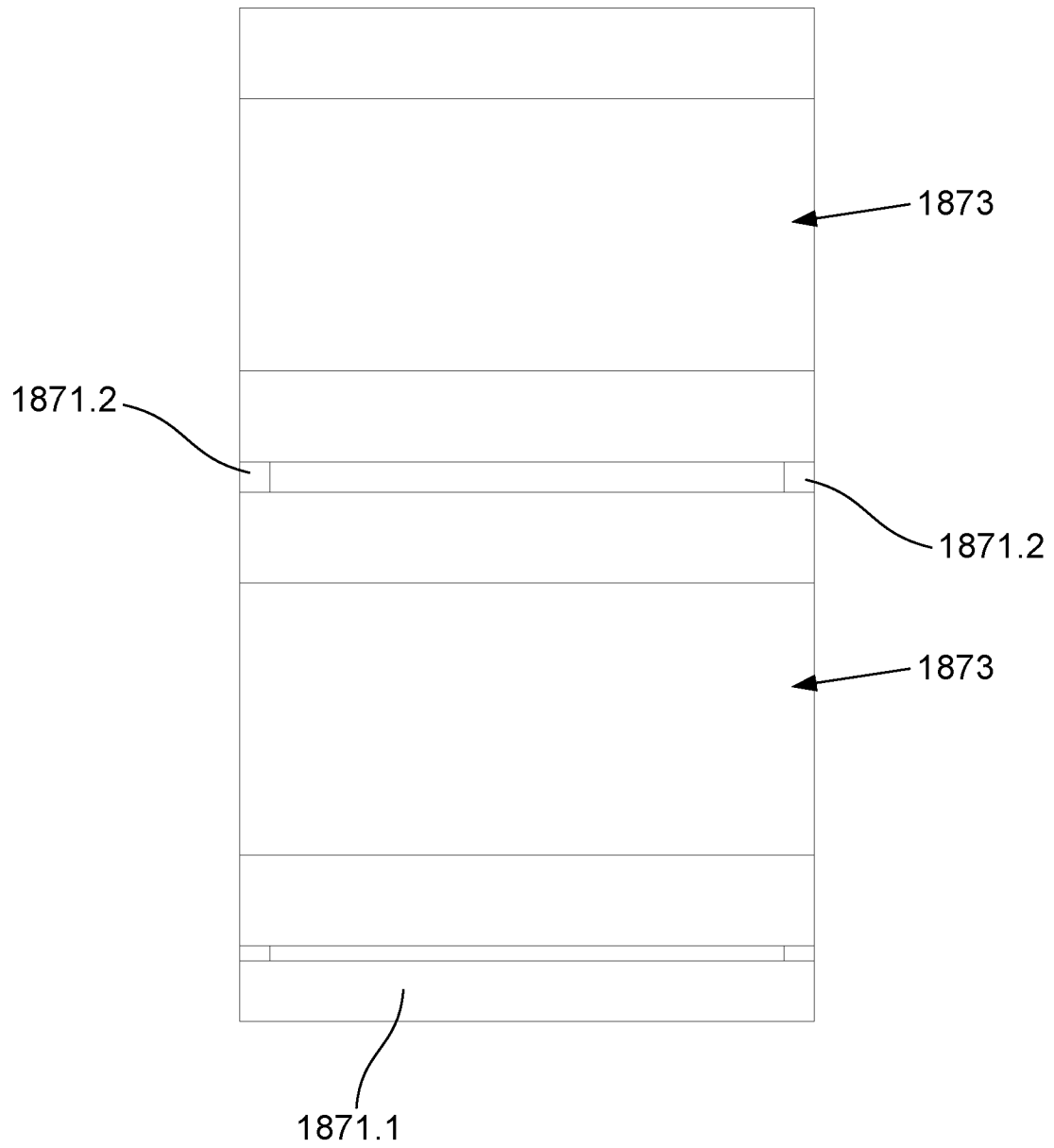
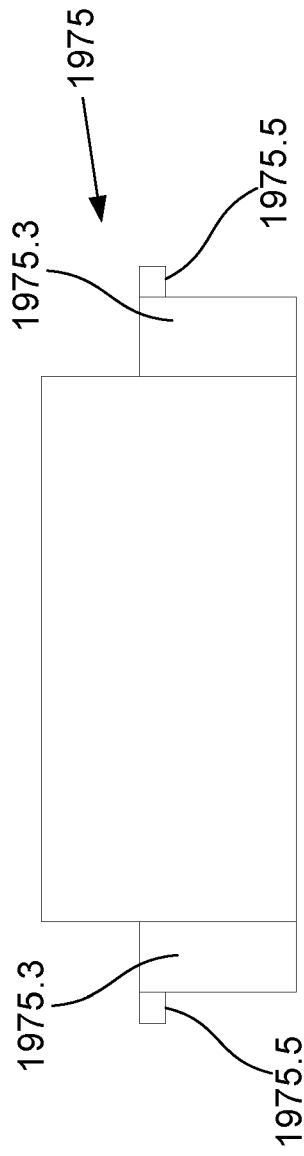


Fig. 18C

Fig. 19A



26/28

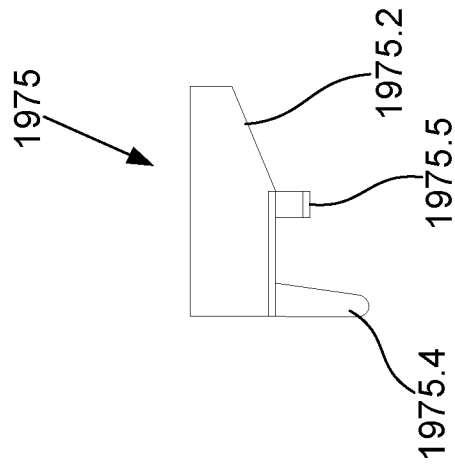


Fig. 19B

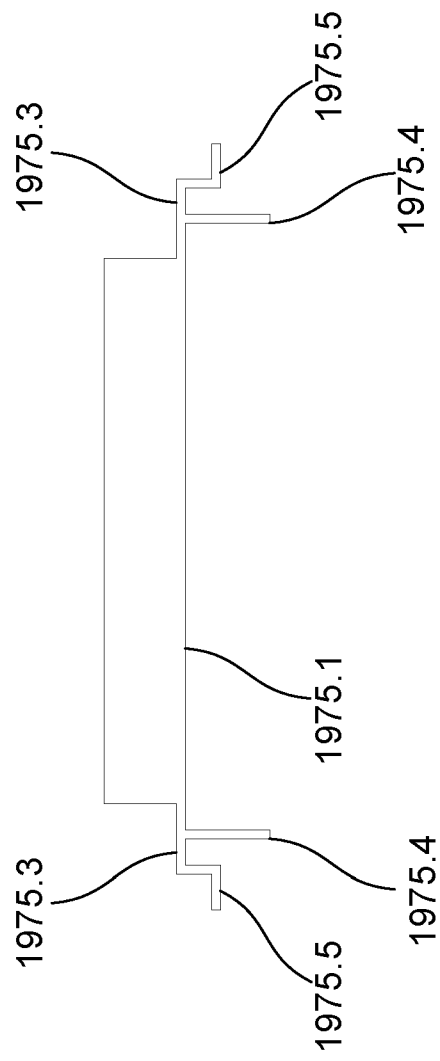


Fig. 19C

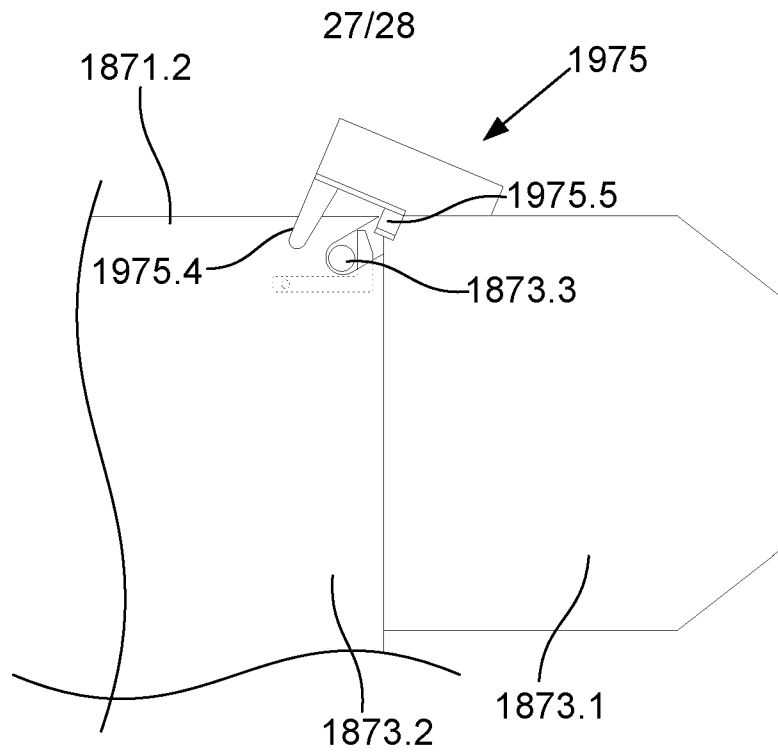


Fig. 20A

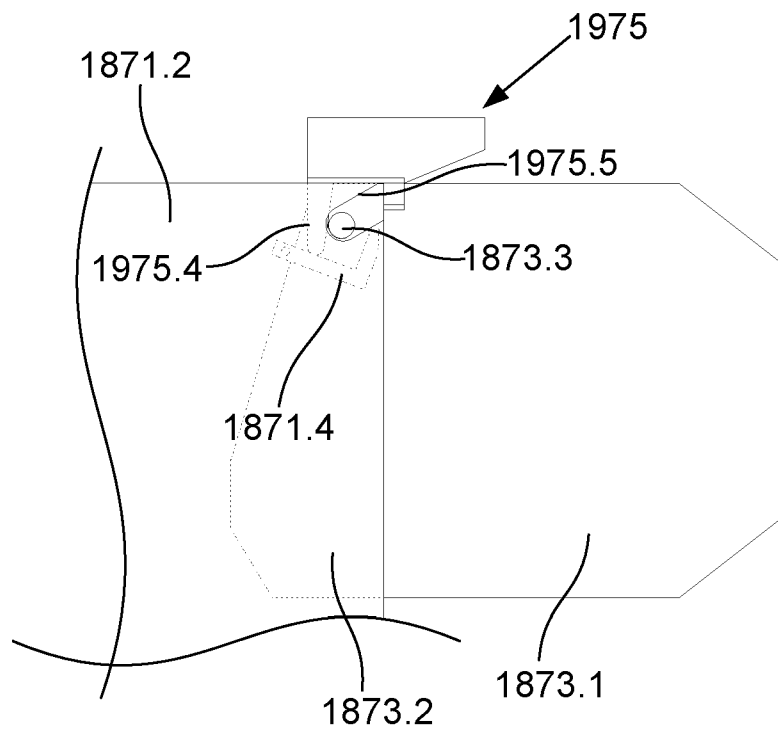


Fig. 20B

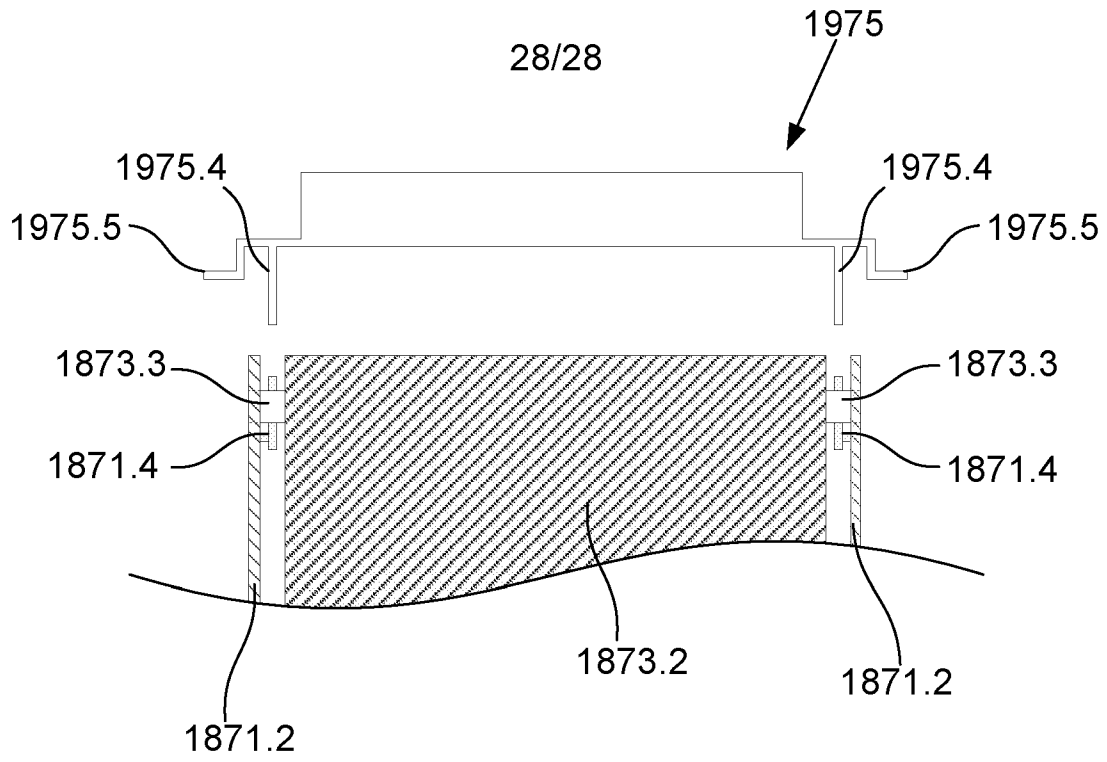


Fig. 20C

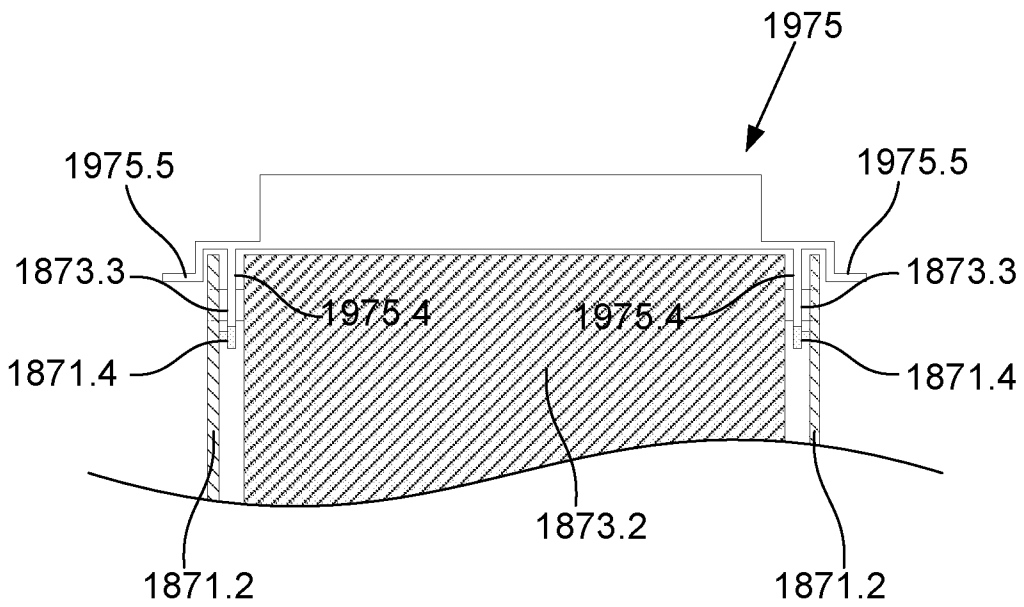


Fig. 20D

INTERNATIONAL SEARCH REPORT

International application No.

PCT/AU2019/050284

A. CLASSIFICATION OF SUBJECT MATTER		
G06F 17/40 (2006.01) G07D 11/12 (2019.01) G07F 19/00 (2006.01) G07D 11/24 (2019.01) G07D 11/32 (2019.01) G07D 11/125 (2019.01) G06Q 20/20 (2012.01) G06Q 20/18 (2012.01)		
According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED		
Minimum documentation searched (classification system followed by classification symbols)		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)		
Google patents: CPC G07,E05G7/001, keywords (cash, cassette, acceptor, memory, identifier, lock, cavity, deposit, atm, foreign currency," scanning, remove, hopper, removal, tool, detach, drawer ejector, intercept printer data) & similar terms; Espacenet: CPC G07D11/12 G07G1/14 g06q20 G07D11/30 G07D11/24 Keywords (scan barcode) & like terms; IP Australia internal databases: inventor, applicant		
Epoque Internal: CPC & IPC E05G1/005, E05G5/006, G07F19/205, G07D2211/00, G07D11/12, E05G, G07F, G07D, B25B27, G07F19, G07F7, G07D11, G07D7, G07G1, E05G1, G06Q20, E05G5 Keywords (REMOVE CARTRIDGE MONEY TOOL DEVICE IMPLEMENT HAND HELD UNLOCK SHEET DEPOSIT TRANSACTION FOREIGN INTERFACE ACCEPTOR ID LATCH EJECT WING WEDGE SLOPE) & like terms;		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	Documents are listed in the continuation of Box C	
<input checked="" type="checkbox"/> Further documents are listed in the continuation of Box C <input checked="" type="checkbox"/> See patent family annex		
* "A"	Special categories of cited documents: document defining the general state of the art which is not considered to be of particular relevance	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"E"	earlier application or patent but published on or after the international filing date	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"O"	document referring to an oral disclosure, use, exhibition or other means	"&" document member of the same patent family
"P"	document published prior to the international filing date but later than the priority date claimed	
Date of the actual completion of the international search 11 June 2019	Date of mailing of the international search report 11 June 2019	
Name and mailing address of the ISA/AU AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA Email address: pct@ipaustrialia.gov.au	Authorised officer Peter Garay AUSTRALIAN PATENT OFFICE (ISO 9001 Quality Certified Service) Telephone No. +61262832451	

INTERNATIONAL SEARCH REPORT		International application No.
C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		PCT/AU2019/050284
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2017/122768 A1 (GLORY KOGYO KK) 20 July 2017 & US 2019/0026970 A1 The whole document, especially figs 2-4 paragraphs 0016, 0035, 0038, 0043, 0056-0059, 0063, 0065, 0075	1, 29-35, 37-43, 46, 61, 64, 65
Y	The whole document, especially figs 1-4 paragraphs 0016, 0035, 0038, 0040, 0043, 0056-0059, 0063, 0065, 0075	2-28, 36, 44, 45, 47-60, 62, 63
X	US 2017/020035 A1 (DIEBOLD NIXDORF INCORPORATED) 13 July 2017 The whole document, especially figs 1, 4, 5, paragraphs 0007, 0042, 0044, 0046, 0049-0051, 0055, 0065	66-78
Y	The whole document, especially figs 1, 4, 5, paragraphs 0004, 0005, 0007, 0030, 0042-0044, 0046, 0049-0053, 0055, 0056, 0065	2-28, 44, 45, 47-60, 62, 63
X	EP 0166041 A1 (BURROUGHS CORPORATION) 02 January 1986 The whole document, especially Fig 5	79-88
Y	The whole document, especially Fig 5	36
Y	US 6384931 B1 (BROWN et al.) 07 May 2002 The whole document, especially abstract	47-54
A	EP 2800070 A1 (GLORY LTD) 05 November 2014 abstract	57-60

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:
the subject matter listed in Rule 39 on which, under Article 17(2)(a)(i), an international search is not required to be carried out, including
2. Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:
3. Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a)

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

See Supplemental Box for Details

1. As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.
3. As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:
4. No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

- The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.
- The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.
- No protest accompanied the payment of additional search fees.

Supplemental Box**Continuation of: Box III**

This International Application does not comply with the requirements of unity of invention because it does not relate to one invention or to a group of inventions so linked as to form a single general inventive concept.

This Authority has found that there are different inventions based on the following features that separate the claims into distinct groups:

- Claims 1-65 are directed to a system and method for processing a payment for a transaction, the system including a payment terminal. The feature of determine a transaction amount; determine a received payment amount indicative of an amount of a received currency; cause at least some of the currency to be dispensed into the currency container; and cause payment data to be stored is specific to this group of claims.
- Claims 66-78 are directed to a container for receiving security documents. The feature of a container housing including a container cavity; a lid for selectively closing the container cavity; a securing mechanism to secure the lid; a container communications interface; a container memory; and, one or more container processing devices that communicate with one or more terminal processing devices is specific to this group of claims.
- Claims 79-88 are directed to a cartridge removal tool and methods to use a cartridge removal tool. The feature of the cartridge removal tool including a tool body having downwardly facing wings that engage a catch on a chassis of the payment module to detach a cartridge from the chassis is specific to this group of claims.

PCT Rule 13.2, first sentence, states that unity of invention is only fulfilled when there is a technical relationship among the claimed inventions involving one or more of the same or corresponding special technical features. PCT Rule 13.2, second sentence, defines a special technical feature as a feature which makes a contribution over the prior art.

When there is no special technical feature common to all the claimed inventions there is no unity of invention.

While the currency container is a feature that is common to all claims, there is no technical relationship between tracking the content, securing the content, and the removal mechanism of the container as each of these inventions can be implemented separately.

In the above groups of claims, the identified features may have the potential to make a contribution over the prior art but are not common to all the claimed inventions and therefore cannot provide the required technical relationship. Therefore there is no special technical feature common to all the claimed inventions and the requirements for unity of invention are consequently not satisfied *a priori*.

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/AU2019/050284

This Annex lists known patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document/s Cited in Search Report		Patent Family Member/s	
Publication Number	Publication Date	Publication Number	Publication Date
WO 2017/122768 A1	20 July 2017	WO 2017122768 A1	20 Jul 2017
		EP 3404628 A1	21 Nov 2018
		JP 2017126275 A	20 Jul 2017
		US 2019026970 A1	24 Jan 2019
US 2017/020035 A1	13 July 2017	US 2017020035 A1	19 Jan 2017
		US 10021817 B2	10 Jul 2018
		CN 104053347 A	17 Sep 2014
		CN 104053347 B	01 Jun 2018
		KR 20150129793 A	20 Nov 2015
		KR 101814265 B1	02 Jan 2018
		US 2014262473 A1	18 Sep 2014
		US 9462732 B2	04 Oct 2016
		WO 2014143308 A1	18 Sep 2014
EP 0166041 A1	02 January 1986	EP 0166041 A1	02 Jan 1986
		EP 0166041 B1	24 Aug 1988
		GB 2136498 A	19 Sep 1984
		GB 2136498 B	09 Jul 1986
		US 4580422 A	08 Apr 1986
US 6384931 B1	07 May 2002	US 6384931 B1	07 May 2002
		EP 0974914 A2	26 Jan 2000
EP 2800070 A1	05 November 2014	EP 2800070 A1	05 Nov 2014
		JP 2013134568 A	08 Jul 2013
		JP 2013134569 A	08 Jul 2013
		WO 2013099795 A1	04 Jul 2013

End of Annex

Due to data integration issues this family listing may not include 10 digit Australian applications filed since May 2001.

Form PCT/ISA/210 (Family Annex)(revised January 2019)