(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
04 June 2020 (04.06.2020)

WIPO | PCT

(10) International Publication Number
WO 2020/110079 A1

(51) International Patent Classification:
G06F 11/30 (2006.01)

(21) International Application Number:
PCT/IB2019/060321

(22) International Filing Date:
29 November 2019 (29.11.2019)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
62/772,996 29 November 2018 (29.11.2018) US

(71) Applicant: **CEEVO BLOCKCHAIN VENTURE LTD.** [LI/LI]; c/o TTA Trevis-Trehaud-Anstalt, Landstrasse 14, FL-9490 Vaduz (LI).

(72) Inventor; and

(71) Applicant *(for VC only)*: **KOURIE, Keith Derrick** [ZA/ZA]; 4th Floor President Place, cnr Jan Smuts Avenue and Bolton Road, Rosebank, 2196 Johannesburg (ZA).

(72) Inventors: **HAKANS, Erik**; Unit 2801 Wu Chung House, 213 Queen's Road East, Wan Chai, 100020, Hong Kong (CN). **TELFER, Chris**; Unit 2801 Wu Chung House, 213 Queen's Road East, Wan Chai, 100020, Hong Kong (CN).

(74) Agent: **FIANDEIRO, João Achada**; Adams & Adams (Johannesburg), 2nd Floor, 34 Fredman Drive, cnr 5th Street, Sandton, 2193 Johannesburg (ZA).

(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, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ,

(54) Title: SECURE CRYPTOCURRENCY STORAGE SYSTEM AND METHOD

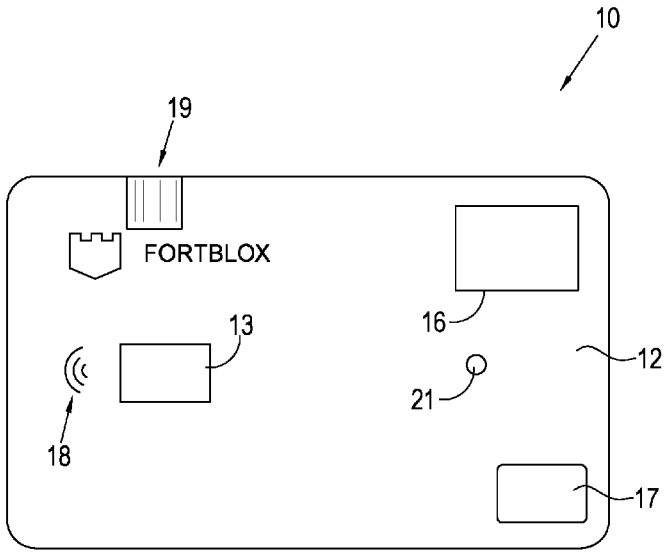

Fig. 1

(57) Abstract: At a high level, the present invention provides a cryptocurrency token storage product to create an ultra-secure corporate storage product, for corporate entities and private individuals, to enable the storage of cryptocurrency tokens securely. According to a first aspect of the invention there is provided a cryptocurrency token storage product comprising a smart card having a controller; an embedded screen with sufficient size to display the full and/or a truncated signature payment hash and/or any other information; and a fingerprint scanner connected (typically integrated directly) to the controller, for user authentication.

WO 2020/110079 A1

[Continued on next page]

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).

Declarations under Rule 4.17:

— *of inventorship (Rule 4.17(iv))*

Published:

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

SECURE CRYPTOCURRENCY STORAGE SYSTEM AND METHOD

FIELD OF INVENTION

THIS invention relates to a secure cryptocurrency storage system and method, for both corporate entities and individuals.

BACKGROUND OF INVENTION

A cryptocurrency is a digital asset designed to work as a medium of exchange that uses strong cryptography to secure financial transactions, control the creation of additional units, and verify the transfer of assets. Cryptocurrencies use decentralization as opposed to centralized digital currency and central banking systems.

The decentralized control of each cryptocurrency works through distributed ledger technology, typically a blockchain, that serves as a public financial transaction database.

Bitcoin

Bitcoin, first released as open-source software in 2009 by pseudonymous developer Satoshi Nakamoto, is generally considered the first decentralized cryptocurrency. The creators' original motivation behind bitcoin was to develop a cash-like payment system that permitted electronic transactions but that also included many of the advantageous characteristics of physical cash. Bitcoin is a virtual, digital monetary unit and therefore has no physical representation.

Since the release of bitcoin, many other altcoins (alternative variants of bitcoin, or other cryptocurrencies) have been created, and continue to be created.

Bitcoin uses SHA-256, a cryptographic hash function, as its proof-of-work scheme. Other cryptocurrencies use other cryptographic schemes, with LiteCoin, for example, being the first successful cryptocurrency to use scrypt as its hash function instead of SHA-256.

As of May 2018, over 1,800 cryptocurrency specifications existed. Within a cryptocurrency system, the safety, integrity and balance of the ledger is maintained by a community of parties referred to as miners, who use their computers to help validate and timestamp transactions, adding them to the ledger in accordance with a particular consensus scheme.

Blockchain

The validity of each cryptocurrency's coins is provided by a blockchain. A blockchain is a continuously growing list of records, called blocks, which are linked and secured using cryptography. Each block typically contains a cryptographic hash function pointer as a link to a previous block, a timestamp and transaction data. By design, blockchains are inherently resistant to modification of the data. It is an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way.

For use as a distributed ledger, a blockchain is typically managed by a peer-to-peer network, collectively adhering to a protocol for validating new blocks.

The bitcoin blockchain is thus a data file that carries the records of all past bitcoin transactions, including the creation of new bitcoin units. It is often referred to as the ledger of the bitcoin system. There is a total of 21 million bitcoins that can be mined of which almost 18 million were in circulation as of October 2019. There are a little over 3 million bitcoins left that are not in circulation yet.

Cryptocurrency Wallet

A cryptocurrency wallet stores the public and private keys or "addresses" which are used to “receive” and “spend” a cryptocurrency. With the private key, it is possible to write in the public ledger, effectively spending the associated cryptocurrency. With the public key, it is possible for others to send currency. A wallet can contain multiple

public and private key pairs. As described above, the cryptocurrency is decentrally stored and maintained in a publicly available ledger called the blockchain. Every piece of cryptocurrency has a private key. With the private key, it is possible to digitally sign a transaction and write it in the public ledger, effectively spending the associated cryptocurrency.

A backup of a cryptocurrency wallet can come in different forms, as follows:

1. An encrypted file, like wallet.dat or wallet.bin, which contains all the private keys.
2. A mnemonic sentence from which the root key can be generated, from which all the private keys can be recreated. Preferably these words could be remembered or written down and stored in other physical locations.
3. A private key itself, such as: KxSRZnttMtVhe17SX5FhPqWpKAEgMT9T3R6Eferj3sx5frM6obqA.

Significantly, when the private keys and the backup are lost, then that cryptocurrency is lost forever.

A cryptocurrency wallet can itself come in different forms, as follows:

1. A software wallet, in which, in one version, an application is installed locally on a computer, telephone or tablet. In another version, namely a web wallet, the private keys are managed by a trusted third party. In yet another version, cryptocurrency exchanges link the user's wallet to their centrally managed wallet/s.
2. A hardware wallet, which is more the focus of the present invention, and which are generally considered secure, because the private keys never leave the physical wallet i.e. the private keys are born (created), live (transaction signing) and die (deleted) inside the hardware wallet. The private keys remain safe inside the hardware wallet, and without the private key, a signed transaction cannot be altered successfully. However, hardware wallets typically use a mnemonic list of words to enable the root key to be generated, from which all the private keys can be recreated; this in turn requires users to write down these words and store them in a separate physical location. This is cumbersome, impractical and insecure for most people.

3. A watch-only wallet, to enable someone to keep track of all transactions. Only the address (public key) is needed, and thus the private key can be kept safe in another location.
4. A multisignature wallet, in which multiple users have to sign (with each of their private keys) for a transaction out of that wallet (public key address).

Terms also used in the context of cryptocurrency wallets are hot and cold wallets. Hot wallets are connected to the internet while cold wallets are not. With a hot wallet cryptocurrency can be spent at any time. A cold wallet has to be 'connected' to the internet first. These concepts will be explored further within the context of the present invention.

Altcoins

As indicated above, after bitcoin several more cryptocurrencies were created. Today there are in total about 1770 different cryptocurrency currencies listed on Coinmarketcap, with an estimated market cap of Circa USD230 billion. The 10 most popular cryptocurrencies in circulation today are:

1. Bitcoin, as described above, although critics suggest that its volatility, slow speeds, energy usage and higher transaction fees will put a limit on its growth.
2. Bitcoin cash, which is based on the original bitcoin, but which has already soared to become one of the most traded cryptocurrencies. There is now approximately the same amount of bitcoin cash in circulation as bitcoin. Nevertheless, there are key differences – most notably, bitcoin cash has an 8MB block size compared with 1MB of the original bitcoin.
3. Litecoin, which is referred to as “bitcoin’s little brother”, and resembles its older sibling in that it is a peer-to-peer cryptocurrency but has faster transaction speeds as well as a substantially higher token limit of 84 million. However, its mining process is more memory-intensive and its market cap is around 1/20th of the size of bitcoin.
4. Ethereum, which has been labelled a “decentralised app” provider. Originally developed as a “world computer” super network, it is aimed to get rid of the need for third-party companies such as Apple in the creation

of apps. The apps developed on Ethereum are on a distributed public platform where miners can earn "ether" to fuel the network.

5. NEO, which was the first open-source public blockchain in China. NEO was initially launched in 2014 as Antshares and enables the development of smart contracts and assets on its platform. The group follows the Ethereum model, but aims to be the platform of choice for the new smart economy.
6. Ripple XRP, which has been designed as a centralised transaction network to be used by banks for money transfers in much the same way as, say, SWIFT. It uses the XRP currency, to enable money (FIAT) to be converted to the XRP token, which can then be sent via the Ripple network and then converted back to money (FIAT) when it is withdrawn. It is designed to be faster, more reliable and less volatile than other cryptocurrencies.
7. Stellar (XLM), which was launched by Ripple co-founder Jed McCaleb in 2014 and, like Ripple, it is a transaction network for fast and efficient cross-border money transfers.
8. Cardano (ADA) is another platform used to send and receive digital currencies, including its own cryptocurrency, ADA, and is the first peer-blockchain powered by scientists and academics. The Cardano network also aims to run decentralised apps on the blockchain.
9. Dash is an open source peer-to-peer cryptocurrency and decentralized autonomous organization. It features instant transactions, private transactions and a self-funded, self-governed organizational structure.
10. Monero is an open-source cryptocurrency created in April 2014 that focuses on fungibility and decentralization.

Security Risk

As cryptocurrencies continue to become more popular, there is an increasing need for security measures designed to help keep cryptocurrency wallets and investment portfolios safe. This has become very important in the wake of targeted attacks at specific cryptocurrency exchanges, wallet providers and holders. The onus also lies on users and investors to keep their cryptocurrency investments safe and secure. Unfortunately, individuals themselves are often the weakest link in cryptocurrency

security, with it being relatively easy to hack a cryptocurrency user's and/or investor's wallet and move their assets if they are careless. The reality is that once a cryptocurrency wallet is left open and vulnerable, "crypto thieves" can compromise the cryptocurrency assets, and the funds can never be recovered.

As already indicated above, cryptocurrency, unlike most traditional currencies, is a digital currency. Thus, the approach to this kind of currency is completely different, particularly when it comes to acquiring and storing it. Since cryptocurrencies do not exist in any physical shape or form, they cannot technically be stored anywhere. Instead, a so-called private key is used to access a public cryptocurrency address and sign for transactions, and thus it is the private key that needs to be securely stored. It is thus a combination of the recipient's public key and a private key that makes a cryptocurrency transaction possible.

There have been several cases of bitcoin theft, typically involving the obtaining or accessing of the private key to a victim's bitcoin address. If the private key is stolen, all the bitcoins from the compromised address can be transferred. In that case, the network does not have any provisions to identify the thief, block further transactions of those stolen bitcoins, or return them to the legitimate owner.

Current Solutions

Most professional cryptocurrency investors use custom designed hardware wallets, of the type described above, to store their cryptocurrency assets. Using a specific method designed by the manufacturer, a secure private key is generated when the hardware wallet is first enabled/set up by the user. During the setup process, the user has the option to create a backup of the device to allow the recreation of the private key, should the user lose the device, or should the device get destroyed. This is done by the device creating 12 to 24 random words (known as seeds) that the user needs to write down in the order displayed on the device, as described above. Should the user need to set up a new device, it uses the random words in the correct sequence to re-create the private key. The user then again has access to his/her cryptocurrency assets as the original private key has been restored and can be used to again sign cryptocurrency transactions.

However, there are three significant risks with hardware wallets on the market today, as follows:

1. If an investor loses the hardware wallet itself and loses the recovery seeds to their hardware wallet private key, they lose their cryptocurrency assets forever.
2. The investor is solely responsible for the safe and secure storage of the recovery seeds as anyone who has access to them can recreate the investor's private key and hence transfer their assets as if they were the investor him/herself.
3. Man-in-the-middle attacks, with a number of consumer-grade hardware wallets on the market having been shown to be vulnerable to such attacks. A man-in-the-middle attack occurs when malware on an end-user's computer changes the destination wallet address when sending or receiving funds, thereby stealing cryptocurrency assets by having them diverted to a different wallet address than that which was intended by the user.

Some cryptocurrency traders opt to store their hardware wallets at a cryptocurrency friendly bank, in a safety deposit box environment, with the random words to recreate the private key in separate safety deposit boxes. This is commonly referred to as cold storage, but since cold storage is offline, it can take hours if not days to retrieve the storage device should the person wish to conduct a cryptocurrency transaction.

Problem Statement

The current landscape surrounding cryptocurrency storage, as described above, has several problems and/or shortcomings. These will be separated below into corporate cryptocurrency storage (i.e. custodian services) and personal cryptocurrency storage.

- **Corporate Cryptocurrency Storage/Custodian Services**

One of the main obstacles to institutional investors entering the cryptocurrency market is the lack of custodian services. High-profile hacks and the fact that losing the private key means losing the related cryptocurrency assets, has made these investors reluctant to participate in the cryptocurrency market. In terms of existing corporate cryptocurrency storage solutions, Coinbase Vault can receive funds like a normal

wallet, and can also prevent stored funds from being immediately withdrawn by adding optional security steps. Users can, for example, choose to split ownership between multiple users and email accounts, requiring these users to approve a transaction before it can be completed. Beyond hardware, there are also cold storage "crypto vault" companies, as described above.

In addition, institutions do not take custody of cryptocurrency assets, they take custody of private keys. This means that it is critical to be able to hand back the original private key once custody ends; existing solutions do not support this, but instead transfer cryptocurrency assets to another wallet address.

Finally, all existing solutions are centralised, which are generally considered to be riskier, as their centralised nature make them a target for attack.

- **Personal Cryptocurrency Storage**

One segment of the cryptocurrency financial industry that has all too often been neglected, has been cryptocurrency token storage and security. The way private and public keys are stored has remained largely unchanged since the very first hardware wallets were assembled, and the complexities of today's wallets mean that small mistakes made by non-technically minded users can spell vulnerability for funds. Cryptocurrency storage and payment solutions ought to be just as efficient and user-friendly as asset management solutions in the fiat-based economy.

Over the last few years, a number of hardware wallet brands have come to dominate the market. While these may have been adequate devices for an early adopter economy, recent trends towards the mainstreaming of blockchain mean that hardware wallets must begin to meet the needs of regular, often not very technically-minded users.

At the moment, setting up a hardware wallet is far from intuitive. New users may be surprised to learn that the most important part of the legacy hardware wallet package is not the device itself, but rather a little piece of paper, dubbed “a recovery sheet”. Having spent USD100 plus (plus shipment) on a hardware wallet device, the user learns that the entire security of their funds depends on properly copying down

(writing) and storing of a 12 to 24-word recovery phrase on a piece of paper, as described above.

This recovery phrase, or "private seed" represents a major vulnerability for hardware wallet users. Even if the hardware walled device itself is not stolen, anyone with this recovery phrase can gain access to the user's private key, by just recreating the private key using the "private seed" on another device. Once the private key has been recreated, the cryptocurrency assets can be transferred to another wallet and the assets are lost forever.

Experienced users are happy to store this recovery sheet in a place like a home safe or a safe deposit box. New entrants into the cryptocurrency economy see taking such responsibility over one's funds as an unnecessary hassle. In addition, for new users, the learning curve required to invest in the cryptocurrency markets is steep, presenting a significant barrier to entry. Thus, being able to address issues regarding eliminating the need to learn how to setup a trading account, how to fund an account, how to trade, how to transfer their assets, how to secure their assets, how to use hardware wallets, etc. will make the cryptocurrency markets accessible to the man-on-the-street, thereby creating an entirely new customer base and market.

Consumers need a simple way to acquiring cryptocurrency assets, using payment methods they are familiar with – such as credit/debit cards – via an easy to use, online platform. Of course, consumers need assurance that their investments are safe.

It is therefore the aim of the present invention to provide a new breed of secure cryptocurrency token storage products for corporate (i.e. to enable custodian services) and personal use, which address the issues described above.

SUMMARY OF INVENTION

At a high level, the present invention provides a cryptocurrency token storage product, based on an HSM (Hardware Security Module), to create an ultra-secure corporate

storage product, for corporate entities and private individuals, to enable the storage of cryptocurrency tokens securely. A HSM is a physical computing device that safeguards and manages digital keys for strong authentication and provides cryptoprocessing. These modules traditionally come in the form of a plug-in card or an external device that attaches directly to a computer or network server. Within the context of the present invention, the HSM generates private keys that cannot be viewed by anyone else.

According to a first aspect of the invention there is provided a cryptocurrency token storage product comprising a smart card having:

a controller;

an embedded screen with sufficient size to display the full and/or a truncated signature payment hash and/or any other information; and

a fingerprint scanner connected (typically integrated directly) to the controller, for user authentication.

In an embodiment, the smart card comprises a standard PVC core coloured 85.60 mm x 53.98 mm card, with rounded corners, and the screen may comprise an LCD or eInk screen (and related circuitry). In one version, the smart card further comprises a battery, primarily to power the screen.

In an embodiment, the controller comprises an HSM chip module and a processing chip (and a related memory device containing instructions for the processing chip).

In an embodiment, the controller comprises an embedded latest generation CCEAL6+ EMV certified chip module (and related circuitry).

In an embodiment, the smart card further comprises an RFID antenna and a USB connector socket (and related circuitry).

In an embodiment, the smart card further comprises an LED status indicator.

The smart card is thus biometrically enabled for user authentication, to ensure that a user is uniquely identified for deposits and/or withdrawals of cryptocurrency tokens, ensuring that the deposits and/or withdrawals are indeed done by the correct person.

Conveniently, the smart card is the same format as a bank card, with the same format chip reader, so that it can fit into normal modern-day banking devices like ATM's and POS machines to enable the future upgrade to banking scheme payment options. The card's USB connector allows connection to PC's and smartphones, and is RFID enabled for contactless payments options.

In one version, a consumer package comprises two of the smart cards defined above, one of which is fitted with a removable sticker, and a connector cable to connect to the USB connector. In one version, the consumer package may include a secure chip reader to read the smart card.

In another version, a consumer package comprises a single smart card defined above and a related USB connector cable.

The cryptocurrency token storage product works in conjunction with a bespoke software application, either in the form of a website or a mobile 'app', with the user being prompted to download the app onto the user's preferred computing hardware device, via a related app store. After opening the software application, a screen prompts the user to connect one of the smart cards to the computing hardware device using the connector cable or holding the card near the device for RFID communications.

The controller includes an enrolment module to manage an enrolment procedure. The software application prompts the user to register each fingerprint on multiple occasions, using the fingerprint scanner on the smart card itself, until sufficient templates have been established.

In the version in which the consumer package comprises two smart cards, the user is prompted to connect the second smart card for backup purposes. The necessary

information is then transferred to the second smart card, in an encrypted session. The user is then prompted to verify that the second backup smartcard is working by validating their fingers. Upon completion of the enrolment process, a dashboard appears in the software application for displaying the user's wallets, balances, graphics around the portfolio, spending history and commonly used functions. The user then also has the option of adding an additional security PIN, linked to the smart cards.

In use, when the user wishes to make a payment from a wallet, the user opens the bespoke software application on his/her computing hardware device and connects the smart card to his/her device with the connector cable (and/or the chip reader, if provided).

The controller includes an authentication module to manage the authentication procedure. The authentication module prompts the user to authenticate him/herself directly on the smart card itself, using the fingerprint scanner.

The controller includes a transaction module to manage the transacting procedure. Proximate the conclusion of a transaction, a payment hash is generated and displayed on the software application and the transaction module generates and displays the payment hash and/or relevant information on the screen of the smart card itself. The software application and/or the transaction module prompts the user to check that the payment hash and/or relevant information are both the same, and if so, the software application and/or the transaction module prompts the user to approve the transaction using one or more of his/her fingers for authentication as above.

In one version, a SaaS model is provided as an optional feature, termed Crypto As A Service (CaaS). The main purposes of the CaaS option are as follows:

1. To provide cloud backup of the user's card, thus addressing the need to worry about safe storage of the smart cards (the private keys, in particular) in the user's possession. The controller includes a cloud backup module to manage the backing up of the relevant data in the cloud. The cloud backup module is arranged to link the smart card hardware in the user's possession to the user's online cloud account, with the cloud backup module setting up a secure session

between the cloud storage service and the user's controller to enable the backing up of the relevant data in the cloud.

2. To provide a safe and convenient way for a user to purchase and/or sell cryptocurrency for their smart card wallet. In particular, the CaaS enables users to purchase and sell cryptocurrency (typically using a credit/debit card) directly via the provided platform, with the platform accordingly facilitating this for users via third parties, with the relevant exchange rate at the time and related fees.
3. To provide a safe and convenient way for a user to "swap" one cryptocurrency for another cryptocurrency of a similar value to the original cryptocurrency. In particular, the CaaS enables users to perform cryptocurrency swaps, with the relevant exchange rate at the time and related fees.

In one application, the cryptocurrency token storage product may be deployed within a decentralised, distributed HSM network comprising nodes run and maintained by external entities, with all actions of the network posted to a private blockchain.

In use, in one version, private keys are generated by the cryptocurrency token storage product, upon enrolment (as described above), with the cryptocurrency token storage product interfacing with, and temporarily sharing the private key, with a primary HSM at a custodian.

In another version, the primary HSM may generate the private key itself without the card.

In both cases, the primary HSM never stores the private key; it just repackages and distributes it. The primary HSM does not have a repository, with all of this taking place within a controlled, secured environment. After enrolment, in the first version mentioned above, the cryptocurrency token storage product is placed into a box with tamper-proof seal and stored in the custodian's vault (for the duration of the custodianship). This feature is of course thus optional in the case of the second version mentioned above.

The primary HSM at the custodian repackages the private key for each node and then distributes it via HSM middleware to a distributed network of nodes, run and

maintained by the external entities. Each node comprises a secondary HSM and a database, which encrypts the received component for itself before storing it in the database. The secondary decentralised HSM's do not have any mechanism or way of recreating the private key from the component from the primary HSM. When the custodian signs a transaction, middleware on the primary HSM requests components from the distributed network of nodes and combines these to temporarily generate the private key for transaction signing. All actions performed by the nodes are recorded on a private blockchain for auditing.

At the end of the custody, each node deletes their respective components and writes this to the private blockchain. All nodes independently confirm this action. The customer then receives the smart card and confirmation that components have been deleted, making it impossible for the private key to be recovered.

In one version of the invention, the invention is implemented as an HSM storage system. The main tasks of this system include secure storage for private keys, signing of cryptographic transactions on the various protocols, address generation and management. The HSM storage system includes HSM's, which may either be hosted and operated locally, or on site where the client operates the services on their own premises.

The HSM storage system also includes servers for the private keys and a biometric database. Regarding the latter, the HSM storage system uses biometric authentication smart cards together with the enrolment procedures for biometric registration of various role players in the system, such as administrators, operators, security officers etc. The HSM's communicate with these smartcards for authentication verification to set up and to approve payments, with user keys.

The biometric database is provided to store the private keys, cryptocurrency wallets and the user keys. Biometric templates of each enrolled role player may be validated. This validation includes at least an original validation process on hardware level performed by the controller on the smart card only. An optional secondary validation may be done against the biometric database where the secure templates are stored.

The system will create a set of encryption keys via the HSM. These keys are encrypted via the HSM's master key. All wallets (private keys) are encrypted under the HSM's master key. The HSM's master key will be automatically changed periodically.

The HSM storage system also includes API and middleware VM servers. The middleware may be separated into system administration and management, such as key management, reporting etc. but with no ability to perform any transactions, and client administration, where clients can manage their customer's keys and payments on behalf of their clients etc.

The middleware also provides a GUI for administering cryptocurrency assets via a payment feeder API that interacts with the role players. The middleware also manages disaster recovery sites, secure backups and auditing records. The middleware thus takes care of the application side of the system via API's facing the client.

The middleware provides a feeder API where the client can send all the payout requests produced by their exchange software application. It will also be capable of handling requests for new wallets on demand to the exchange with the public key securely provided to them. The communication is end to end encrypted, validating that the sender is client facing, with updated security keys periodically.

The HSM's can be arranged to offer two types of basic wallets for clients, namely an open session "hot wallet" and a cold storage wallet. The open session wallet requires that the client has multiple operator cards active and connected to a software wallet and that the session has been authenticated by authorised staff members through biometric validation. The hot wallet allows the clients middleware to hardcode the access keys in order to provide automated payout services. The hot wallet is designed to have a very limited amount of assets available for redemption and limits the exposure for the client while not compromising the speed of delivery for everyday services.

The cold storage wallet caters for long term large storage of the main assets of the client. Each transaction has to be biometrically signed by the assigned staff. This

wallet will naturally have a lower transaction frequency. Additional security features such as payouts to only approved addresses and similar security can be added for client safety.

According to a second aspect of the invention there is provided a method of managing a cryptocurrency token storage product comprising a smart card having an controller, an embedded screen with sufficient size to display the full and/or a truncated signature payment hash and/or any other information, and a fingerprint scanner connected to the controller on the card, for user authentication.

The method includes providing a software application, either in the form of a website or a mobile 'app', with the user being prompted to download the app onto the user's preferred computing hardware device, via a related app store. After opening the software application, the method comprises prompting the user to connect one of the two provided smart cards to the device, either using RFID (via the RFID antenna), a chip reader (if provided), or a connector cable (via the USB connector).

The method includes running an enrolment procedure, which includes the step of prompting the user to register each fingerprint on multiple occasions, using the fingerprint scanner on the smart card itself, until sufficient templates have been established.

In the version in which the consumer package comprises two smart cards, the method then prompts the user to connect the second smart card for backup purposes, with the method then transferring the necessary data to the second smart card, in an encrypted session. The method then prompts the user to verify that the second backup smartcard is working by validating their fingers. Upon completion of the enrolment process, the method displays a dashboard in the software application for displaying the user's wallets, balances, graphics around the portfolio, spending history and commonly used functions.

The controller includes a transaction module to manage the transacting procedure. Proximate the conclusion of a transaction, the method comprises generating and displaying a payment hash on the software application and on the screen of the smart

card itself. The method then prompts the user to check that the payment hash on both is the same, and if so, the method prompts the user to approve the transaction using one of his/her fingers for authentication, as above.

In one application, the method includes deploying the cryptocurrency token storage product within a decentralised, distributed HSM network comprising nodes run and maintained by external entities, with all actions of the network posted to a private blockchain. In use, the method includes generating private keys by the cryptocurrency token storage product, upon enrolment (as described above), with the cryptocurrency token storage product interfacing with, and temporarily sharing the private key, with a primary HSM at a custodian.

At the end of the custody, the method includes deleting their respective components and writing them to the private blockchain. All nodes independently confirm this action. The customer then receives the smart card and confirmation that components have been deleted, making it impossible for the private key to be recovered.

BRIEF DESCRIPTION OF DRAWINGS

The objects of this invention and the manner of obtaining them, will become more apparent, and the invention itself will be better understood, by reference to the following description of embodiments of the invention taken in conjunction with the accompanying diagrammatic drawings, wherein:

Figure 1 shows a schematic top view of a cryptocurrency token storage product, in the form of a smart card, according to the invention;

Figure 2 shows a functional block diagram of the key modules of the token storage product of the invention;

Figure 3 shows a schematic block diagram of a HSM distributed network, according to a further aspect of the invention; and

Figure 4 shows a schematic block diagram of a HSM storage solution, according to yet another aspect of the invention.

DETAILED DESCRIPTION OF EXAMPLE EMBODIMENTS

The following description of the invention is provided as an enabling teaching of the invention. Those skilled in the relevant art will recognise that many changes can be made to the embodiment described, while still attaining the beneficial results of the present invention. It will also be apparent that some of the desired benefits of the present invention can be attained by selecting some of the features of the present invention without utilising other features. Accordingly, those skilled in the art will recognise that modifications and adaptations to the present invention are possible and can even be desirable in certain circumstances, and are a part of the present invention. Thus, the following description is provided as illustrative of the principles of the present invention and not a limitation thereof.

At a high level, with reference to Figures 1 and 2, the present invention provides a cryptocurrency token storage product 10, based on an HSM (Hardware Security Module), to create an ultra-secure corporate storage product 10, for corporate entities and private individuals, to enable the storage of cryptocurrency tokens securely.

A HSM is a physical computing device that safeguards and manages digital keys for strong authentication and provides cryptoprocessing. These modules traditionally come in the form of a plug-in card or an external device that attaches directly to a computer or network server. Within the context of the present invention, the HSM generates private keys that cannot be viewed by anyone else.

To ensure competitive advantage in the market for secure private key storage, the present invention adheres to the following basic design principles:

- Storage hardware will never give up the private key and sign the relevant cryptocurrencies transactions on a hardware level.
- All solutions will not utilize traditional seed management, of the type described above.

- All hardware developed will have a competitive cost point compared to existing solutions.
- Consumer product will be compatible with current card infrastructure as far as possible.

The cryptocurrency token storage product 10 comprises a smart card 12 having a controller 13 comprising an HSM chip module 14 and processing chip 20, an embedded screen 16 with sufficient size to display the full and/or a truncated signature payment hash and/or any other information, and a touch fingerprint scanner 17 integrated directly to the controller 13 on the card 12, for user authentication.

In one version, the smart card 12 further comprises a battery (not shown), primarily to power the screen 16.

In an embodiment, the smart card 12 comprises a standard PVC core coloured 85.60 mm x 53.98 mm card 12, with rounded corners. The screen 16 may comprise an LCD or eInk screen.

The controller 13 comprises an embedded latest generation CCEAL6+ EMV certified chip module. The controller 13 of the smart card 12 provides an ultra-secure mini controller 13 to create an ultra-secure portable cryptocurrency token storage device, for personal use.

In an embodiment, the smart card 12 further comprises an RFID antenna 18 and a USB connector 19 (and related circuitry).

In an embodiment, the smart card 12 further comprises an LED status indicator 21.

The smart card 12 is thus biometrically enabled for user authentication, to ensure that a user is uniquely identified for deposits and/or withdrawals of cryptocurrency tokens, ensuring that the deposits and/or withdrawals are indeed done by the correct person.

In an embodiment, the controller 13 includes a processor 20 and related memory 22 to allow:

- end to end encrypted environment using 256-bit (or higher) cryptography;
- storage of cryptocurrency private keys on card level;
- signing of cryptocurrency transactions on multiple block chains;
- wallet and address generation;
- random number generation hardware support;
- tampering safeguards;
- diagnostics of hardware during operational life cycle;
- middleware for management of blockchain messages;
- biometric storage and management, authentication and verification;
- secondary PIN block validation.

The controller 13 may define a stand-alone operating system off a slave device managing all cryptographic operations required under the card life cycle. All cards 12 will have an expiry date clearly labelled on the card 12 well within hardware parameters to reduce risk of lost assets due to hardware failure. This solution generates a security grade level where trust in the software used for managing the device 10 is severely reduced and becomes agnostic to vulnerabilities arising from malware, viruses, key loggers and similar threats.

Conveniently, as best shown in Figure 1, the smart card 12 is the same format as a bank card, with the same format chip reader, so that it can fit into normal modern-day banking devices like ATM's and POS machines to enable the future upgrade to banking scheme payment options. The card's USB connector allows connection to PC's and smartphones, and is RFID enabled for contactless payments options.

In one version, a consumer package comprises two of the smart cards 12 defined above, one of which is fitted with a removable sticker, and a connector cable to connect to the USB connector. In one version, the consumer package may include a secure chip reader. In another version, the consumer package comprises a single smart card defined above and a related USB connector cable.

In this consumer package version, with no SaaS services attached, the consumer journey commences once the user has purchased the cryptocurrency token storage product 10, either in a retail environment or online. The product 10 is then shipped to

the user, the user opens the package after checking the security seals of the package with reference to a provided security note. Once opened, the user reviews a small instruction booklet, which sets out the steps to activate the product.

The cryptocurrency token storage product 10 works in conjunction with a bespoke software application, either in the form of a website or a mobile 'app', with the user being prompted to download the app onto the user's preferred computing hardware device (Android, Apple, Windows and Linux etc.), via a related app store. After opening the software application, a screen prompts the user to connect one of the smart cards 12 to the computing hardware device using the connector cable. Alternatively, the user may hold the card near the device for RFID communications.

After a connection has been established, the software will recognize this as a new card and prompt the enrolment procedure. The controller 13 accordingly includes an enrolment module 24 to manage the enrolment procedure. The app prompts the user to register each fingerprint on multiple occasions, using the fingerprint scanner 17 on the smart card 12 itself, until sufficient template data has been established (for multiple 10 fingers, typically).

After registration, a validation loop is executed to ensure that all fingers are working as intended.

In the version in which the consumer package comprises two smart cards, the user is prompted to connect the second smart card 12 for backup purposes. The necessary information is then transferred to the second smart card 12, in an encrypted session. The user is then prompted to verify that the second backup smartcard is working by validating their fingers. Upon completion of the enrolment process, a dashboard appears in software application for displaying the user's wallets, balances, graphics around the portfolio, spending history and commonly used functions. The user then also has the option of adding an additional security PIN, linked to the smart cards 12.

When the user wishes to make a payment from a digital wallet, the user opens the software application on his/her computing hardware device and connects the smart card 12 to his/her device with the connector cable. The controller 13 accordingly

includes an authentication module 26 to manage the authentication procedure. The authentication module 26 prompts the user to authenticate him/herself directly on the smart card 12 itself, using the fingerprint scanner.

The controller 13 includes a transaction module 28 to manage the transacting procedure. The transaction module 28 prompts the user to choose the relevant currency and the option to make a payment. The receiving address is then entered into the sender form, plus the amount and related information in respect of the desire payment and an indication of the fee. The app verifies that the address is compatible with the currency chosen.

After pressing 'Pay' on the app, proximate the conclusion of a transaction, a payment hash is generated and, optionally displayed on the app. The transaction module 28 may optionally also generate and display the payment hash and/or relevant information on the screen 16 of the smart card 12 itself. The app and/or the transaction module 28 optionally prompts the user to check that the payment hash and/or relevant information on both is the same, and if so, the app and/or the transaction module 28 prompts the user to approve the transaction using one of his/her fingers for authentication as above. The payment is then completed, with an updated status, as well as a link to enable the user to look it up on the blockchain.

In an embodiment, the invention includes a card upgrade migration feature. Thus, when a new card 12 that supports new currencies or new hardware becomes available, the migration feature requires the user to re-register his/her fingerprints for authorisation. Alternatively, the invention allows the user to simply transfer his/her assets from one account to another account.

In one version, a SaaS model is provided as an optional feature, termed Crypto As A Service (CaaS). One of the main purposes of the CaaS option is to provide cloud backup of the user's card 12, thus addressing the need to worry about safe storage of the smart cards 12 (the private keys, in particular) in the user's possession. The controller 13 accordingly includes a cloud backup module 30 to manage the backing up of the relevant data in the cloud. Thus, after completing the user setup process described above, the user has the option of activating cloud storage services. After

choosing this service (with applicable payment option and service duration), accepting applicable terms and conditions and registering the user's credit card, the user is prompted to personalise his/her online cloud account (including entering the user's personal details plus an address).

The CaaS model cloud backup module 30 is arranged to link the smart card 12 hardware in the user's possession to the user's online cloud account. When payment is complete, the cloud backup module 30 sets up a secure session between the cloud storage service and the user's controller 13 to enable the backing up of the relevant data to the cloud. This backing up process cannot be spoofed as keys authenticating the cryptocurrency token storage product 10 against the controller 13 are required and only known by the controller 13 and the related cloud storage service. Any other attempt to spoof a session in this manner would fail.

Another purpose of the CaaS option is to provide a safe and convenient way for a user to purchase and/or sell cryptocurrency for their smart card wallet. In particular, the CaaS enables users to purchase and sell cryptocurrency (typically using a credit/debit card) directly via the provided platform, with the platform accordingly facilitating this for users via third parties, with the relevant exchange rate at the time and related fees. The CaaS model thus provides a simple means of allowing a user to sell their cryptocurrency assets, liquidating them at the click of a button within their online account. This removes the need for an exchange entirely, as users would be selling to the market via the provider service.

Yet a further purpose of the CaaS option is to provide a safe and convenient way for a user to "swap" one cryptocurrency for another cryptocurrency of a similar value to the original cryptocurrency. In particular, the CaaS enables users to perform cryptocurrency swaps, with the relevant exchange rate at the time and related fees.

Additional envisaged services of the CaaS model include cloud backup (including private key back-up/recovery) services, next-of-kin recovery services in the event of a user's death, express card replacement services with tracking, automatically sending generation cards to the user without having to reorder them, discounted accessories,

call centre access and access to affiliate programs (i.e. referrals for consumer and enterprise).

In one application, with reference now to Figure 3, the cryptocurrency token storage product 10 may be deployed within a decentralised, distributed HSM network 40, comprising nodes 42 run and maintained by external entities (such as auditors acting as escrow agents), with all actions of the network 40 posted to a private blockchain 44.

In use, in one version, private keys are generated by the cryptocurrency token storage product 10, upon enrolment (as described above), with the cryptocurrency token storage product 10 interfacing with, and temporarily sharing the private key, with a primary HSM 46 at a custodian (such as a bank).

In another version, the primary HSM 46 may generate the private key itself without the card 10.

Significantly, in both cases, the primary HSM 46 never stores the private key, it just repackages and distributes it. The primary HSM 46 does not have a repository, with all of this taking place within a controlled, secured environment.

After enrolment, in the first version mentioned above, the cryptocurrency token storage product 10 is placed into a box with tamper-proof seal and stored in the custodian's vault (for the duration of the custodianship). This feature is of course thus optional in the case of the second version mentioned above.

The primary HSM 46 at the custodian repackages the private key for each node 42 and then distributes it via HSM middleware to a distributed network of nodes 42, run and maintained by the external entities (i.e. escrow agents). Each node 42 comprises a secondary HSM 48 and a database 50, which encrypts the received components for itself before storing it in the database 50. The secondary decentralised HSM's 48 do not have any mechanism or way of recreating the private key from the component from the primary HSM 46.

When the custodian signs a transaction, middleware on the primary HSM 46 requests components from the distributed network of nodes 42 and combines these to temporarily generate the private key for transaction signing. All actions performed by the nodes 42 are recorded on the private blockchain 44 for auditing.

At the end of the custody, each node 42 deletes their respective components and writes this to the private blockchain 44. All nodes 42 independently confirm this action. The bank customer then receives the smart card 12 and confirmation that components have been deleted, making it impossible for the private key to be recovered.

Turning now to Figure 4, in one version of the invention, the invention is implemented as an HSM storage system 60. The envisaged primary user of this storage system 60 would be any organisation that manages or wants to manage client's cryptocurrency assets, including corporate clients, exchanges, miners, hedge funds, investment houses etc.

The main tasks of this system 60 are secure storage for private keys, signing of cryptographic transactions on the various protocols, address generation and management.

The HSM storage system 60, as best shown in Figure 4, includes HSM's 62, which may either be hosted and operated locally, or on site where the organisation operates the services on their own premises.

The HSM storage system 60 also includes servers 64 for the private keys and a biometric database 66. Regarding the latter, the HSM storage system 60 uses biometric authentication smart cards together with the enrolment procedures for biometric registration of various role players in the system, such as administrators, operators, security officers etc. The HSM's 62 communicate with these smartcards for authentication verification to set up and to approve payments, with user keys.

The biometric database 66 is provided to store the private keys, cryptocurrency wallets and the user keys. Biometric templates of each enrolled role player may be validated. This includes at least an original validation on hardware level performed by the

controller 13 on the smart card only. An optional secondary validation may be done against the biometric database 66 where the secure templates are stored.

The system will create a set of encryption keys via the HSM 62. These keys are encrypted via the HSM's master key. All wallets (private keys) are encrypted under the HSM's master key. The HSM's master key will be automatically changed periodically.

The HSM storage system 60 also includes API and middleware VM servers 68. The middleware may be separated into:

- system administration and management, such as key management, reporting etc. but with no ability to perform any transactions; and
- client administration, where clients can manage their customer's keys and payments on behalf of their clients etc.

The middleware also provides a GUI for administering cryptocurrency assets via a payment feeder API that interacts with the role players. The middleware also manages disaster recovery sites, secure backups and auditing records. The middleware thus takes care of the application side of the solution via API's facing the client.

The middleware provides a feeder API where the client can send all the payout requests produced by their exchange software application. It will also be capable of handling requests for new wallets on demand to the exchange with the public key securely provided to them. The communication is end to end encrypted, validating that the sender is client facing, with updated security keys periodically.

The system 60 is housed within a secure zone 70, with a firewall 72 connecting the system 60 to blockchain nodes VM servers 74 (for bitcoin, Ethereum, Litecoin etc.), various external services 76 and general database VM servers 78 for reporting and other administrative services. The system 60 further includes application services VM servers 80 to manage user interaction between with users 82, 84, and web services VM servers 86 to manage website interaction with users 88.

The HSM's 62 are arranged to offer two types of basic wallets for clients, namely an open session "hot wallet" and a cold storage wallet. The open session wallet requires that the client has multiple operator cards active and connected to the software wallet and that the session has been authenticated by authorised staff members through biometric validation. The hot wallet allows the client's middleware module to hardcode the access keys in order to provide automated payout services. The hot wallet is designed to have a very limited amount of assets available for redemption and limits the exposure for the client while not compromising the speed of delivery for everyday services.

The cold storage wallet caters for long term large storage of the main assets of the client. Each transaction has to be biometrically signed by the assigned staff. This wallet will naturally have a lower transaction frequency. Additional security features such as payouts to only approved addresses and similar security can be added for client safety.

The HSM storage system 60 will reside in at least two security locations providing high availability in the case if one system goes offline. Database backups are performed and securely stored offline, with the database backup being encrypted. In the case that both HSM units 62 are destroyed, a new HSM unit 62 may be setup using a minimum of 3 components given to individual security officers.

Regarding user authentication, in one version, there are four basic categories of operators on the platform, as follows:

Operator – Approval of payments
Operator – Setting up payments
Operator – Enrolment
Operator – Approval of enrolment
Optional – End Client withdrawal request

Every approved operator is enrolled with their fingerprints. Each operator is provided with a card holding the biometric information on the individual chip. Each time an operator performs a function, biometrics are stored for security logs with optional photo logs. The client can routinely go through the security logs to ensure everything is

operated as per their internal procedures. As an operator cannot hold more than one function, it becomes a prohibitive exercise to abuse the access of the funds. The security flow of each authenticated transaction is shown below.

Clients also have the option of enabling a "withdrawal request card" to the end customer. This establishes that any withdrawal request coming into the organisation is legitimate and biometrically verified as an added security layer.

During operator validation, the operator places their fingerprint on the reader to extract the fingerprint templates. The fingerprint templates are validated and the operator card (chip) will produce a one-time use biometric hash (bio-block). Together, the bio-block, a photo of the operator, and transactional data are sent to the HSM unit 62 which will further validate the bio-block. With a positive match, the operation is performed. The smart card will work with any standard smart card reader, RFID reader or USB cable connected to the administration terminal.

To support multiple HSMs, the HSM unit 62 itself needs to be stateless. When setting up the authorised operators, first the enrolment operator and the approval of enrolment operator need to be setup. Thereafter they can use the principle of dual control to add the setup payment operators and approval of payment operators. A command to the HSM unit 62 is required to update the key token and the returned key token must then be saved in the database so that it can be passed in the next request to the any one of the configured HSMs 62. If an operator's smart card is stolen/lost, then that smart card can be revoked from the HSM unit 62 by the enrolment and approval of enrolment operators. The loss of one smart card is not catastrophic because multiple smart cards 12 are required to allow the use of the secret key.

Additional services of the present invention include the following:

Smart contract Node

This enables near instant transactions as well as a peer to peer infrastructure. A fundamental option is to enable a proprietary protocol for instant transfers using fingerprints. The development opens up for peer to peer, open retail protocols plus decentralised services.

Succession Functionality

This feature allows a second person to register their fingerprints on the smart card 12 for a disaster recovery option (losing fingerprints). This would be added to the registration part of the card setup on first use or alternatively done at a later stage as an option to the client. Alternatively, the user may sign up details of a next of kin or trusted person. Upon connecting the device and if a person is registered, a PIN and/or Password would be needed to open the functionality to open "activate unlocking" for trusted persons. Alternatively, if the account is registered, it can be activated on account level with procedures around death certificates and appropriate legal due process.

Retail payments

This enables activating dedicated spending wallets through quick finger print and RFID access for instant transactions in a retail environment. This functionality is suitable for small size transactions as well as peer to peer transactions on the product suites.

Duress functionality

During the registration process or alternatively at a later stage as an option, the client has an option to choose at least one finger to be "duress". This opens up the wallet in a "low value mode" that will only show a small amount available for spending and not allow any transfers above these amounts regardless of what the true value of portfolio is. With subscription services, (CaaS) a notification can go to the call centre identifying the duress and contact the local authorities where applicable.

The advantages of the secure cryptocurrency storage system and method are numerous, and will be separated below into corporate cryptocurrency storage (i.e. custodian services) and personal cryptocurrency storage.

Corporate cryptocurrency storage

Private keys are generated by an HSM and cannot be seen by anybody, and thus the present invention provides effective, secure backups. The private keys are stored in

an encrypted format in a financial-grade PCI (Peripheral Component Interconnect) facility.

The security protocols of this facility will regularly be audited by trusted third parties.

The present invention provides easy, safe, and quick wallet recovery. Thus, if a user loses or damages their smart cards, a new setup package may be promptly shipped to their home or office address.

The present invention also provides an affordable solution; for example, even the cheapest cold storage solutions cost thousands of dollars a year, and do not provide 24/7 access to funds.

All hardware is built in house and is tamper-proof. In house development and complete control of the supply chain ensure that no third party could tamper with the hardware wallet, the storage facility, or any other hardware or firmware components.

With this solution, the solution provider of the invention, the Bank, and/or external auditors (escrow agents) never hold a customer's private key. The solution represents a simpler commercial model, typically comprising a fee per private key, per month, plus fee per transaction, as opposed to a percentage of assets held.

Personal cryptocurrency Storage product

The present invention provides an extremely affordable solution, when compared to traditional hardware wallets.

The invention essentially removes the client's responsibility to manage their recovery seed or private key, since recovery sheets are not part of the present invention.

The product may be registered at home: clients will order the cards in the mail, then activate them through an app and/or website.

Biometrics are built in: Payments can only be approved with the correct biometric match.

Tamper-proof: All hardware is developed and built in house.

Payment standards card type and interfaces for later integration into regular payment schemes.

Thus, viewed holistically, the invention provides an end-to-end cryptocurrency solution (asset purchase, secure storage, and asset sale (conversion to fiat)), giving novice retail investors access to the cryptocurrency markets with greater ease, and peace of mind, than is possible today.

Consumers will now be able to access a simple way to acquiring cryptocurrency assets, using payment methods they are familiar with, such as credit/debit cards, via an easy to use, online platform.

No cryptocurrency assets would be held, thereby mitigating currency risk. Instead, assets would be acquired from the market via API instantly. In this regard, a key feature of the present invention is open API support, thus allowing the hardware module to be used with existing software solutions currently in the market.

CLAIMS

1. A cryptocurrency token storage product comprising a smart card having:

a controller;

an embedded screen with sufficient size to display the full and/or a truncated signature payment hash and/or any other information; and

a fingerprint scanner connected to the controller, for user authentication.

2. The cryptocurrency token storage product of claim 1, wherein the controller comprises an HSM chip module and a processing chip.

3. The cryptocurrency token storage product of claim 1, wherein the smart card further comprises an RFID antenna and a USB connector to enable the smart card to communicate and/or connect with a device.

4. The cryptocurrency token storage product of claim 1, wherein the smart card comprises an LED status indicator.

5. The cryptocurrency token storage product of claim 1, wherein the smart card comprises a battery.

6. The cryptocurrency token storage product of claim 1, wherein the smart card is biometrically enabled for user authentication, to ensure that a user is uniquely identified for deposits and/or withdrawals of cryptocurrency tokens, ensuring that the deposits and/or withdrawals are done by the correct person.

7. The cryptocurrency token storage product of claim 3, wherein a consumer package comprises two of the smart cards, one of which is fitted with a removable sticker, and a connector cable to connect to the USB connector.

8. The cryptocurrency token storage product of claim 7, wherein the consumer package comprises a secure chip reader to read the smart card.

9. The cryptocurrency token storage product of claim 1, wherein the cryptocurrency token storage product works in conjunction with a bespoke software application.

10. The cryptocurrency token storage product of claim 9, wherein the controller includes an enrolment module to manage an enrolment procedure, wherein the software application prompts the user to register a plurality of fingerprints on multiple occasions, using the fingerprint scanner on the smart card, until sufficient templates have been established.

11. The cryptocurrency token storage product of claim 9, wherein the controller includes an authentication module to manage the authentication procedure, the authentication module prompting the user to authenticate him/herself directly on the smart card itself, using the fingerprint scanner.

12. The cryptocurrency token storage product of claim 9, wherein the controller includes a transaction module to manage transactions, so that proximate the conclusion of a transaction, a payment hash is generated and displayed on the software application and the transaction module generates and displays the payment hash and/or relevant information on the screen of the smart card itself.

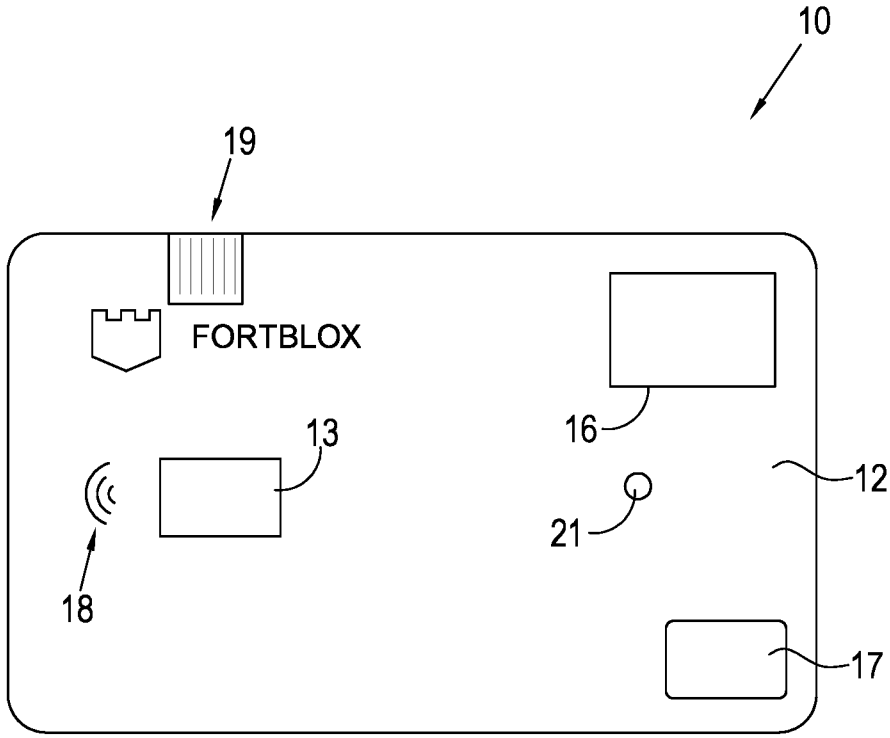
10
19
FORTBLOX
16
13
12
21
18
17

Fig. 1

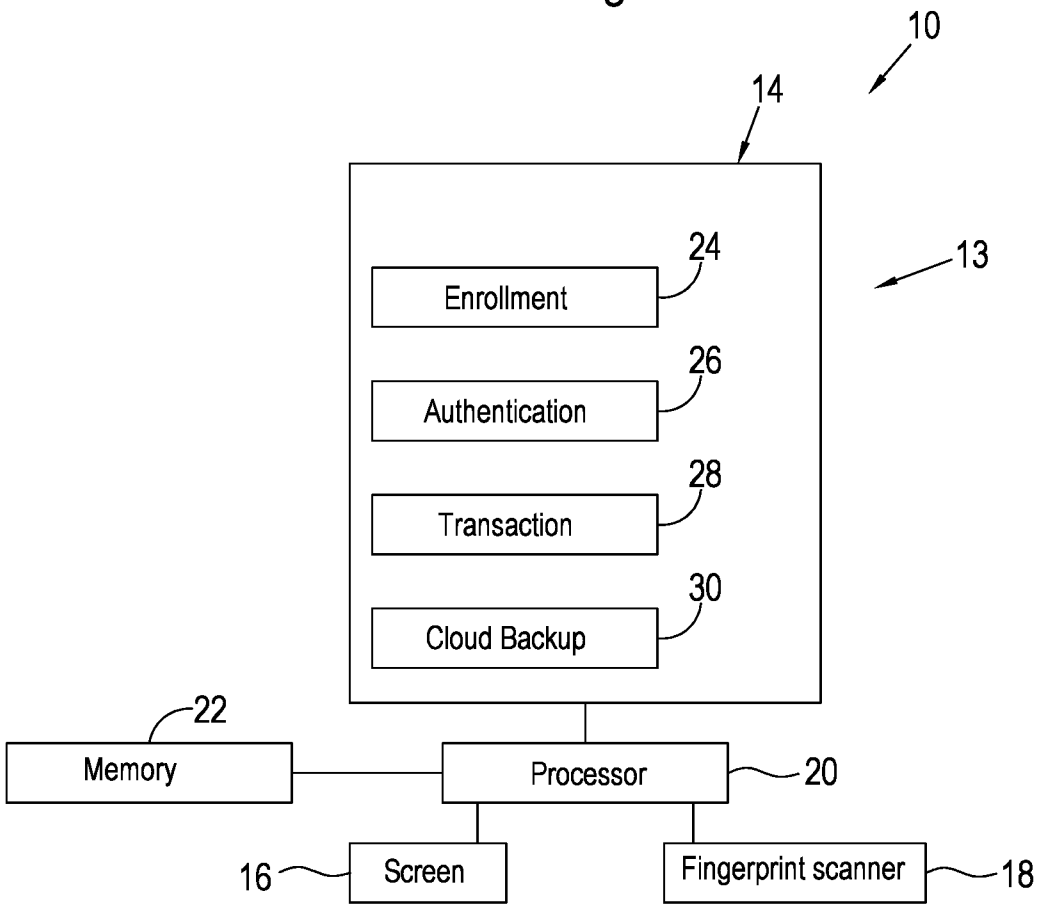
10
14
13
24
Enrollment
26
Authentication
28
Transaction
30
Cloud Backup
22
Memory
Processor
20
16
Screen
Fingerprint scanner
18

Fig. 2

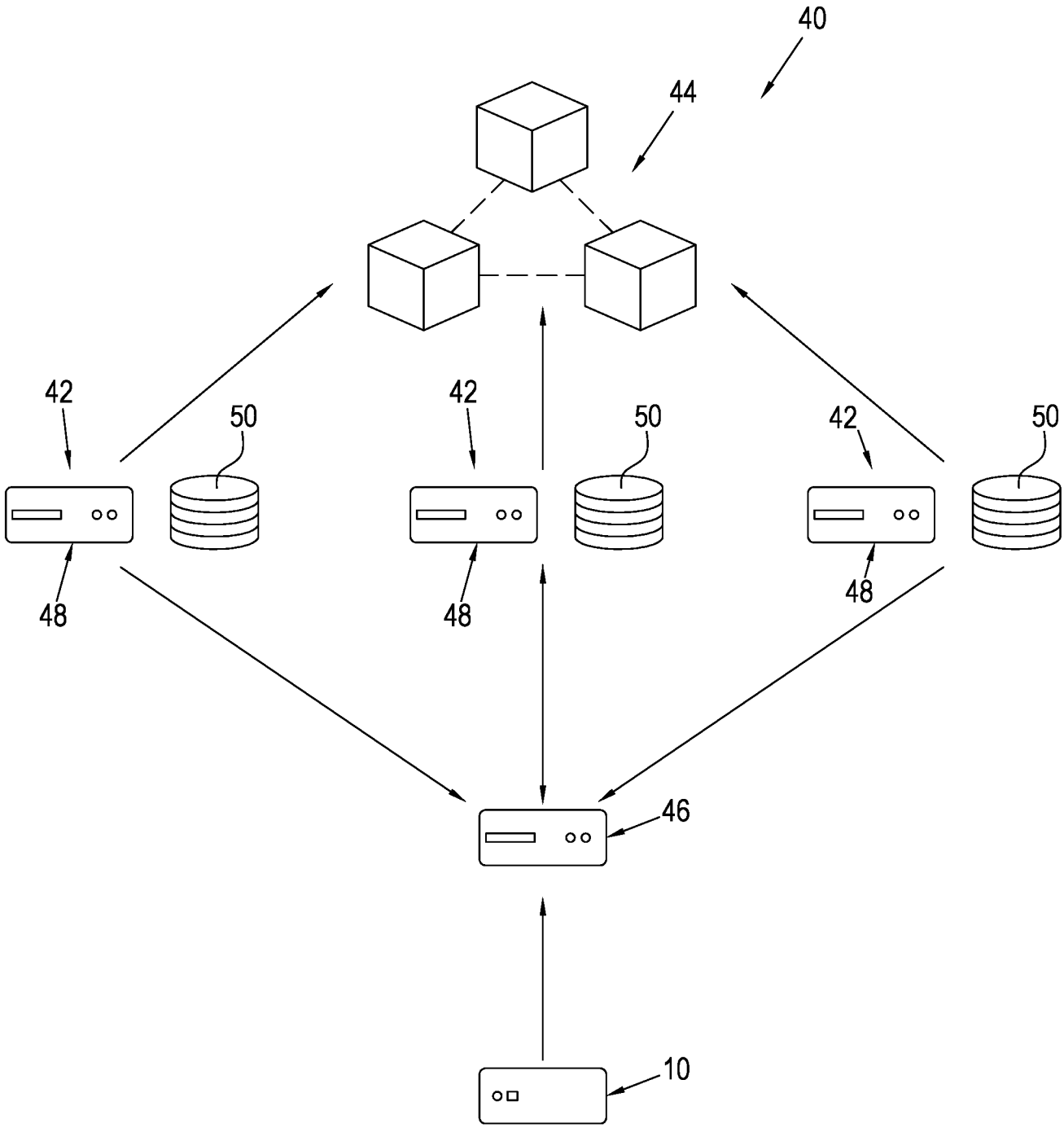

Fig. 3

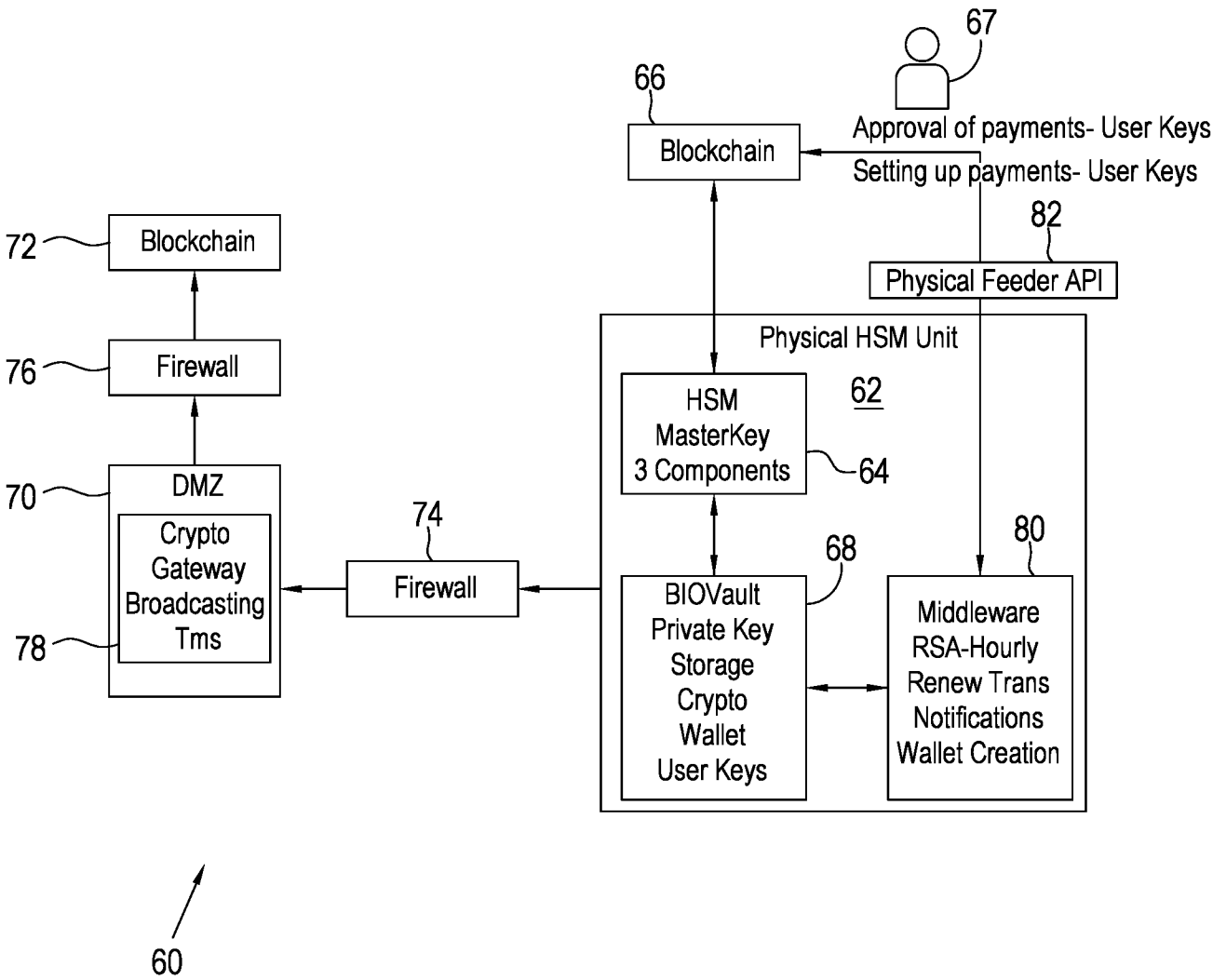
67
66
Blockchain
Approval of payments- User Keys
Setting up payments- User Keys
82
Physical Feeder API
72
Blockchain
Physical HSM Unit
76
Firewall
HSM
MasterKey
3 Components
62
64
70
DMZ
74
Crypto
Gateway
Broadcasting
Tms
Firewall
68
80
78
BIOVault
Private Key
Storage
Crypto
Wallet
User Keys
Middleware
RSA-Hourly
Renew Trans
Notifications
Wallet Creation
60

Fig. 4

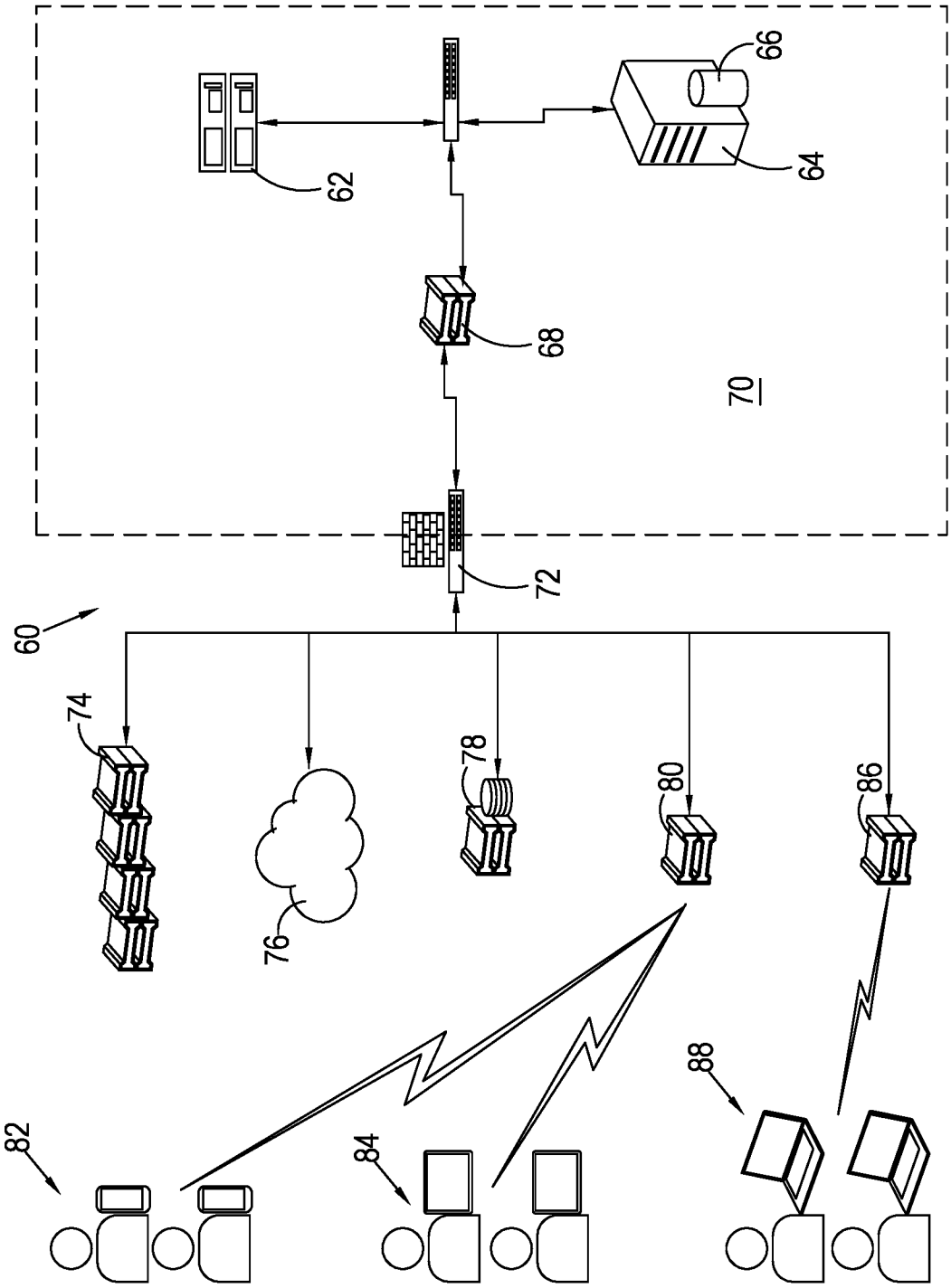

Fig. 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IB 19/60321

A. CLASSIFICATION OF SUBJECT MATTER

IPC - G06F 11/30 (2020.01)

CPC - G06F 21/86, G06F 21/10, G06F 21/72, G06F 2221/2107, G06F 2221/2143, G06F 21/10, G11B 20/00086, G11B 20/0021, G06F 2221/2107, H04L 9/08, H04L 9/08, H04L 63/0428

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)
See Search History document

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
See Search History document

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
See Search History document

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X -- Y	US 2018/0300489 A1 (Amazon Technologies, Inc.) 18 October 2018 (18.10.2018), entire document, especially Fig. 2a; paras [0015, [0018], [0029]-[0030], [0032]-[0033], [0041], [0048], [0059].	1-2, 4, 6, 9 and 11 ---------- 3, 5, 7-8, 10 and 12
Y	US 2007/0042767 A1 (Stepanian) 22 February 2007 (22.02.2007), entire document, especially Abstract, paras [0006], [0022], [0029], [0028], [0126], [0145], [0167], [00224], [0246]; claim 25.	3, 5, 7-8, 10 and 12
A	US 2018/0189527 A1 (Kang et al.) 05 July 2018 (05.07.2018), entire document.	1-12
A	US 2004/0255127 A1 (Arnouse) 16 December 2004 (16.12.2004), entire document.	1-12
A	US 2018/0129831 A1 (Semiconductor Energy Laboratory Co. Ltd.) 10 May 2018 (10.05.2018), entire document.	1-12
A	US 2013/0314208 A1 (Arkami, Inc.) 28 November 2013 (28.11.2013), entire document.	1-12
A	US 2004/0019790 A1 (Aono et al.) 29 January 2004 (29.01.2004), entire document.	1-12

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"D" document cited by the applicant in the international application
"E" earlier application or patent but published on or after the international filing date
"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)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"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
"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
"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
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
19 February 2020	27 FEB 2020
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-8300	Authorized officer Lee Young Telephone No. PCT Helpdesk: 571-272-4300