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

(19) **World Intellectual Property Organization**
International Bureau

(43) **International Publication Date**
28 November 2019 (28.11.2019)

WIPO | PCT

(10) **International Publication Number**
WO 2019/224826 A1

(51) **International Patent Classification:**
H04L 29/06 (2006.01)

(21) **International Application Number:**
PCT/IL20 19/050586

(22) **International Filing Date:**
23 May 2019 (23.05.2019)

(25) **Filing Language:** English

(26) **Publication Language:** English

(30) **Priority Data:**
259568 23 May 2018 (23.05.2018) IL

(71) **Applicant: ESSENCE SECURITY INTERNATIONAL (E.S.I.) LTD.** [IL/IL]; Ackerstein Buildings, Building D, 7th Floor, 12 Abba Eben Boulevard, 4672530 Herzlia Pituach (IL).

(72) **Inventors: KAUFMAN, Yehuda;** 7 HaShita Street, 6092000 Kadima (IL). **BENAILY, Gabriel;** 27/2 Hartsit Street, 7171581 Modiin-Maccabim-Reut (IL). **AMAR, Shalom;** 108/34 Ben Tzvi Street, 4242299 Netanya (IL). **SANDLER, Guy;** 9 HaRimon Street, 6099100 Bnei-Atarot (IL). **YASSO, Eran;** 12b ReUt Street, 4529614 Hod-HaSharon (IL). **SCHNAPP, Jonathan;** 101/1 1 Shlomo Hamelech Street, 645 1234 Tel Aviv (IL).

(74) **Agent: EHRLICH, Gal** et al.; G. E. EHRLICH (1995) LTD., 11MenachemBeginRoad, 5268 104 Ramat Gan (IL).

(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, 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, Cl, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

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

(54) **Title:** GUARDING A DEVICE AGAINST A CYBER THREAT

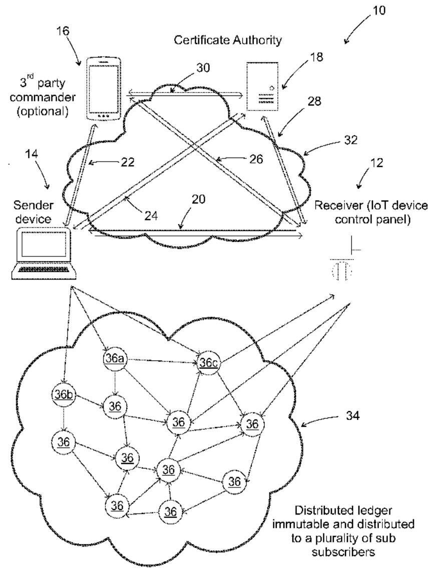
10
16
Certificate Authority
18
30
3rd party commander (optional)
28
32
14
22
26
12
Sender device
24
20
Receiver (IoT device/ control panel)
36a
36c
36b
36
34
Distributed ledger immutable and distributed to a plurality of sub subscribers

FIG. 1

(57) **Abstract:** Disclosed herein is a method for guarding a first device (12) against a cyber threat. A transaction record (52) is received on a ledger (50) distributed amongst a plurality of nodes (12, 14, 36) including the first device (12); receiving at least one message (105, 308, 2 13), via a secure communica¬ tion channel (20), from an authenticated second device (14). The message may include an identifier (Hash(Tx1)) for the first transaction (Tx1). The identifier may be used to read the record (52). The record may include a first validation tool. Validity of first data received in the record and/or the message may be verified using the first validation tool and/or a second validation tool; and in an event that a predefined condition is met, an operation of the first device may be executed based on the first data, the predefined condition requiring at least that the validity is verified.

WO 2019/224826 A1

GUARDING A DEVICE AGAINST A CYBER THREAT

RELATED APPLICATION

This application claims the benefit of priority from Israel Patent Application No. 259568 filed on 23 May 2018, the contents of which are incorporated herein by reference in their entirety.

TECHNICAL FIELD

The present invention relates to a method for guarding a device against a cyber threat, and is particularly, but not exclusively, suited to facilitating operation of Internet-of-Things (IoT) devices while protecting them from cyberattacks. The invention also relates to the device and a computer readable medium for configuring the device.

BACKGROUND

With the growth of Internet of Things (IoT) devices and networks there is need for new and/or improved cybersecurity for such devices and systems. For example, there are challenges in securely transferring information to IoT devices connected a network, while preventing unauthorized persons from accessing the device, e.g. by gaining control of such devices or accessing their data. Information requiring secure transfer may for example be a command or other data used in operation of the device, e.g. reading data from the device, or commanding the device to interact with its surrounding environment. The interaction with the environment may for example be sensing/capturing a condition of the environment, e.g. by taking a photo or recording audio, detecting motion etc.

In some networks, IoT devices are controlled by a central server, which if successfully hacked may provide the hacker with access to all devices controlled by the server.

This weakness may be combated by decentralizing control through use of a distributed ledger on a peer-to-peer network, for example as used by cryptocurrency technology such as Bitcoin.

Such technology uses an immutable ledger that is distributed amongst many network devices, whereby each of the devices receives an identical copy of the ledger. The validity of transactions of cryptocurrency coins may be verified by checking that there is consensus among the devices that the transaction occurred and was proper. Thus, there is no, or at least only minor, involvement of a central server. Nonetheless distributed ledgers are not impervious to cyberattacks.

Further transactions on such ledgers may be anonymous so the device receiving cryptocurrency coins via a transaction does not know the device that caused the transaction, so it may be unknown whether the transaction was executed by a legitimate source.

Further challenges lie in how to use such distributed ledgers to convey data to the device, for use of the data by the device, in such a manner that guards against influence by from an unauthorized device.

The present invention is intended to solve or at least ameliorate one or more of the above or other weaknesses of the prior art.

Reference to any prior art in this specification is not an acknowledgement or suggestion that this prior art forms part of the common general knowledge in any jurisdiction, or globally, or that this prior art could reasonably be expected to be understood, regarded as relevant/or combined with other pieces of prior art by a person skilled in the art.

SUMMARY OF THE INVENTION

In a first aspect of the present invention there is provided a method for guarding a first device against a cyber threat, the method comprising:

receiving a record of a first transaction for a ledger distributed amongst a plurality of nodes of a peer-to-peer network, the plurality of nodes including the first device;

receiving at least one message, via a secure communication channel, from an authenticated second device, the at least one message including an identifier for identifying the first transaction; and

using the identifier to read the record of the transaction.

Without limiting the scope of the invention, the present invention may advantageously enable a transaction-receiving device to identify a source of a transaction on a ledger. Transactions, in isolation, are themselves anonymous, but in the present invention the transaction may be identified by an identifier that is received from an authenticated device, over a secure communication protocol. This enables inference of an authenticated identification of the source of the transaction by virtue of receiving an identification of the transaction over a secure communication protocol, since the secure communication protocol does involve authentication.

The record of the first transaction may include a first validation tool.

In some embodiments, the method further comprises:

verifying validity of first data received in at least one of: the record of the first transaction and the at least one message, wherein the validity is verified using at least one of the first validation tool and a second validation tool, and in an event that a predefined condition is met, executing an operation of the first device based on said first data, the predefined condition requiring at least that said validity is verified.

Advantageously, a record of that transaction includes a first validation tool that is used verify validity of certain data (the first data) so that the first data can confidently be used in an execution of an operation on the device. Since the record is on a distributed ledger it is difficult to tamper with the validation tool.

However, to boost security in some embodiments, the first data is received over the secure communication protocol and the first validation tool comprises a signed version of timing data (e.g. a timestamp) so that the first data will not be accepted if it is associated with a time that too different from the timing data. To boost security in other embodiments, the first validation tool comprises a signed version of the first data. In either case the signing, enables the transaction receiving device to determine that at least a relevant part of the transaction (which is somehow tied to the first data) has not been tampered with. The second validation tool may be used by the transaction-receiving device to confirm the integrity of the signed data (i.e. it has not been changed). The second validation tool may for example be a public key corresponding to a private key used to sign the data. In some implementations, the second validation tool is received over a secure communication channel.

A further potential advantage of the present invention is that there are multiple layers/factors of security for a device to execute an operation based on received data. One of the layers is that a second device trying to transmit data to the first device must be authenticated, thereby providing confidence that at least one message is from a known source, for example an authorized device. However, should a potential hacker manage to fake a secured communication this does grant them an ability to cause the device to use certain transmitted data and thereby provide access to the device. This is because of another layer of security, whereby the secure communication must be tied to a transaction on a distributed ledger of a peer-to-peer network. A further layer of security is that there is a verification step that is based on a validation tool included in at least the ledger.

In a second aspect of the present invention there is provided a method for guarding a first device against a cyber threat, the method comprising:

receiving a record of a first transaction for a ledger distributed amongst a plurality of nodes of a peer-to-peer network, the plurality of nodes including the first device;

receiving at least one message, via a secure communication channel, from an authenticated second device, the at least one message including:

first data for executing an operation of the first device based on the first data;

verifying validity of the first data based on a correlation between the at least one message and the first transaction; and

in an event that a predefined condition is met, executing the operation of the first device based on said first data, the predefined condition requiring at least that said validity is verified.

In some embodiments, the correlation comprises a timing relationship that correlates a first event associated with the at least one message with a second event associated with the first transaction. The first event may for example be receipt of the first data. The second event may for example be a time defined in the record (e.g. a time at which the first transaction was executed), or in another embodiment a time at which validity of the first transaction is determined to reach consensus according to a rule of the peer-to-peer network.

In some embodiments the method comprises determining that the timing relationship correlates the first event with the second event, if any one of (or in some embodiments both of):

the first event is determined to have occurred within a predefined time window in relation to the second event; and

the second event is determined to have occurred within a predefined time window in relation to the first event.

For example, the timing relationship may be determined to correlate the first event with the second event in an event that a difference in time between occurrence of the first event and the second event is less than a predefined maximum.

In some embodiments, the method comprises: receiving, via the at least one message, an identifier for identifying the first transaction; and using the identifier to read the record of the transaction to determine whether there is said correlation between the at least one message and the first transaction.

In some embodiments the record of the first transaction includes a first validation wherein said predefined condition further requires a verification that the first validation tool is valid. Verification that the first validation tool is valid may involve use of a second validation tool received via the secure communication channel.

Each of the following embodiments applies to all of the above aspects of the invention and all of the above embodiments of those aspects of the invention.

In some embodiments, the method comprises receiving the second validation tool via a secure communication channel, more preferably said secure communication channel. The second tool is preferably verified as being derived from an authenticated second device. In some embodiments, the verification that the second tool is derived from the authenticated second device is by virtue of the second tool being received over a secure communication channel with the second device. In other words, since the authenticity of the second device is known by virtue of the secure communication channel, the second tool is known, by the first device, to have come from the second device.

The record of the first transaction is received in a separate communication to receiving said at least one message. For example, the record of the first transaction may be received via a different communication channel to said communication channel.

In some embodiments the first validation tool comprises a first message and a first digital signature, the first digital signature being a digitally signed version of the first message. In such embodiments the second validation tool may be a first public key of the second device, wherein the validity is verified by using the first public key of the second device to check that the first digital signature was derived from the first message. Thus, the verification of validity may be based on public key cryptography.

In other public key cryptography based embodiments, other distributions of the first message, the first digital signature, and the first public key of the second device may be employed. For example, the first validation tool may a first public key of the second device, and the second validation tool may be a first message and a signed version of the first message.

By being a secure communication channel, the communication channel is resistant to overhearing (i.e. it is a confidential channel) and tampering. It preferably provides a private communication between the first device and the second device.

In some embodiments the communication channel is secured by cryptography, e.g. public key cryptography, that encrypts the at least one message; and

In some embodiments, the secured communication channel is also secured by requiring verification of an integrity check of the at least one message from the communication.

In some embodiments, the communication channel is secured by a cryptographic protocol, for example, Transport Layer Security (TLS) or Secure Sockets Layer (SSL), but in some embodiments is more specifically TLS.

In some embodiments the first message comprises said first data. In other embodiments, the first data is distinct from said first message. For example, the first message may be included on the transaction record and the first data may be a separate entity either in the transaction record or in one or more of said at least one messages received the said communication channel.

In some embodiments, first cryptographic keys used for security of the communication channel are different to second cryptographic keys used for security of the first data on the record of the first transaction. For example, the method may comprise using different public keys of the second device to respectively: authenticate the at least one message; and verify validity of the first data.

In some embodiments, the first data is encrypted, wherein the method comprises decrypting the first data using a first private key of the first device. In such embodiments, the method may comprise, before receiving said first data, instructing transmission a first public key of the first device to said second device, wherein the first public key of the first device corresponds to the first private key of the first device. As will be appreciated, the encryption of the first data in such cases may be performed by the second device using the first public key of the first device.

In some embodiments, the identifier of the record of the first transaction is a hash of the record of the first transaction for uniquely identifying the transaction.

In some embodiments, the method further comprises verifying authenticity of the second device.

For example, in some embodiments, the method comprises:

receiving, in a handshake with the second device, a digital certificate for authenticating the second device to establish the secure communication channel; and

wherein the authenticity of the second device is verified based on the received digital certificate.

For example, verification of the authenticity may involve checking, either at the first device or at a trusted authentication device, e.g. as a Certification Authority, that said received digital certificate matches a digital certificate at the trusted authentication device.

In embodiments in which the at least one message comprises a plurality of messages, the identification of the transaction need only be included in one of the messages, provided each of the messages can be determined to be associated with each other, for example by a common identifier included in each message.

In some embodiments, the method further comprises instructing transmission of a first address of the first device for receiving (i.e. having assigned thereto) an amount (e.g. one coin, a part of one coin, or more than one coin) of a cryptocurrency by way of said first transaction. An “address” as used herein is an address in the ledger. Each device that is a member of the peer-to-peer network has a unique seed from which addresses may generated, wherein each seed produces different addresses to other each other seed.

In some embodiments the distributed ledger comprises a Directed Acyclic Graph (DAG). Preferably, a framework, operated on each of the nodes of the peer-to-peer to implement the ledger on the node, requires each transaction to validate a preceding transaction, preferably more than one preceding transaction. This contrasts with blockchain technology (used to administer Bitcoin transactions) for example, in which there are blocks of transactions, and the transactions are ordered according to a chain but there is no rule by which each block of transactions validates a preceding block of transactions.

This facilitates parallel processing of transactions onto the ledger by different nodes. Blockchain technology by contrast requires consensus of a previous block of transactions before new transactions may be processed.

The record of the first transaction may include one or more identifiers identifying at least one other transaction, and more preferably respective identities at least two other transactions, validated to execute the first transaction. In some embodiments, in the DAG, a transaction that has validated another transaction points to the other transaction.

In some embodiments, the method comprises instructing transmission of a request for a transaction. The request for a transaction may comprise instructing transmission of the first address of the first device.

In some embodiments, the method further comprises determining an amount of the cryptocurrency assigned to the first address of the first device, wherein the predefined condition also requires that the assigned amount is consistent with a predetermined required amount (e.g. that the amount is greater than a predefined threshold). For example, it requires a coin and it is assigned the coin.

The method may further comprise storing the record of the first transaction on the ledger, and determining whether there is consensus in respect of the first transaction. There may be determined to be consensus in respect of the first transaction in an event that: (a) a predetermined measure (e.g. percentage) of nodes in the network collectively agree, based on their respective manifestations of the ledger, that the first transaction is confirmed as valid, or (b) that there is at least a predetermined measure (e.g. percentage) of instances of preliminary validations related to the first transaction and recorded in the ledger in the first device.

In the case of (a), in some embodiments consensus is reached once some defined amount (e.g. a number or percentage) of nodes actually agree (as is the case in Blockchain).

In the case of (b), in other embodiments, consensus is reached if more than some predefined measure, e.g. in some embodiments more than 50%, or more than 90%, of un-validated transactions (called edges or leaves) in a DAG has either: preliminarily validated (and so directly points to) the first transaction or indirectly points or provided a preliminary validation of a transaction in a chain of preliminarily validated transactions that leads back to the first transaction. For example, as is the case in IOTA.

In some embodiments, said predefined condition further requires that said consensus has been reached. In some embodiments, said predefined condition further requires that said consensus has been reached within a predefined amount of time since any one or both of: (a) the record of the transaction was received; or b) a time corresponding to a timestamp in the transaction, the timestamp defining, for example, when the transaction was executed by the second device. In some embodiments, in an event that said consensus is not reached within a predefined amount of time (e.g. said predefined amount of time), the method further comprises any one more of: instructing transmission of an alert notification; instructing transmission of a request for a second transaction.

In any case, the method may comprise instructing transmission of information for executing a second transaction.

In some embodiments, the information for executing a second transaction comprises a second address of the first device for receiving an amount of a cryptocurrency by way of said second transaction.

In other embodiments, a request for a second transaction comprises instructing re-transmission of the first address of the first device.

In some embodiments, the method comprises instructing transmission of:

a second address of the first device for receiving an amount of a cryptocurrency by way of a second transaction; and

a second public key of the first device to be used for encryption in a record of the second transaction that is to be received onto the ledger.

In some embodiments, the method comprises receiving a first address of the second device for assigning thereto a second amount of a cryptocurrency by way of a return transaction onto the ledger. For example, in some embodiments, the second amount is the same as said amount to balance the amount received by the first device with an amount returned by the first device.

In some embodiments the method comprises, in an event the predefined condition is met, instructing transmission of an acknowledgement message via a communication channel, e.g. via said communication channel. For example, the acknowledgment message may be used to inform the second device that the first device has executed said operation based on said first data.

In some embodiments, said data on which an operation of the first device is based is included the record of the first transaction. Thus, for such embodiments there is therefore synchronous receipt at said first device of: (a) said data and (b) the record of the transaction.

In other embodiments, said data on which an operation of the first device based is included in the at least one message, e.g. in a first one of such a message or spread amongst a first set of such messages. Thus, for such embodiments there is asynchronous receipt of said data and said record of the transaction. For such embodiments, the first data is preferably encrypted using the first public key of the first device, wherein method preferably includes decrypting the first data using the first private key of the first device.

In some embodiments, a method includes:

determining a time corresponding to (e.g. a time of execution of) the first transaction;

determining a time corresponding to (e.g. a time of receiving) the first data; and

wherein the predefined condition for using the first data further requires that a difference between the time of the receiving the first data and the time corresponding to the transaction is less than a predefined maximum time difference.

The use of such a maximum time difference in this manner may advantageously guard against reply attacks after the maximum time has elapsed.

In some embodiments time corresponding to the first transaction is a time of execution of the first transaction based on a time-stamp included in the record of the first transaction.

In some embodiments, the time-stamp is encrypted (e.g. using the first public key of the first device) and the method comprises decrypting the time-stamp (e.g. using the first private key of the first device).

In some embodiments, the time-stamp is signed by a first private key of the second device encrypted and the method comprises verifying the signature of the timestamp using the first public key of the second device, the first public key of the second device corresponding to the first private key of the second device.

In some embodiments, the method further comprises:

receiving second data in the at least one message, the second data being included in a different message to the first data, wherein first data is preferably encrypted (e.g. using the first public key of the first device); and

decrypting the first data (e.g. using the first private key of the first device); and in an event that a second predefined condition is met, executing an operation of the first device based on said second data, the second predefined condition requiring at least that said validity is verified.

In some embodiments, the method further comprises determining an amount of the cryptocurrency assigned to the first address of the first device, wherein the second predefined condition also requires that the assigned amount is consistent with a predetermined required amount (e.g. that the amount is greater than a predefined threshold).

Thus, advantageously one transaction may be used to enable multiple receptions of commands or other data. In embodiments where consensus on a transaction is required before an operation can be performed based on such received data, using a single transaction for multiple receptions of data may reduce or avoid any latency arising from needing to wait for consensus before received data may be acted upon.

In some embodiments, the method includes:

determining a time corresponding to (e.g. a time of execution of) the first transaction;

determining a time corresponding to (e.g. a time of receiving) the second data; and

determining a difference between the time corresponding to the second data and the time corresponding to the transaction,

wherein the predefined condition also requires that said difference is less than a predefined maximum time difference.

In some embodiments, the method includes:

receiving a record of a second transaction for the ledger, the record of the second transaction including a third validation tool;

receiving at least one message via a secure communication channel, from an authenticated device, the at least one message and including a second identifier for identifying the second transaction;

using the second identifier to read the record of the second transaction;

verifying validity of further data received in at least one of: the record of the second transaction and said at least one message that includes the second identifier, wherein the validity is verified based at least one of the third validation tool and a fourth validation tool, and

in an event that a predefined condition is met, executing an operation of the first device based on said further data, the predefined condition requiring at least that said validity is verified based at least on the third validation tool and the fourth validation tool.

The authenticated device is in some embodiments the second device, and in other embodiments an additional or alternative authenticated device includes another sender device (not shown). Thus, in such embodiments, the device may be operated based on data received from different devices (e.g. the second device and the other sender device), each of the different devices identifying a different transaction.

In any case, the third validation tool may for example be a further message and a further digital signature, and the fourth validation tool may for example be a second public key of the second device. Thus advantageously, the validation tools may be specific to each transaction, thereby providing increased security against reply attacks.

In some embodiments, the second public key of the second device and the first public key of the second device are derived from a common seed.

In some embodiments, the method comprises receiving a trigger to wake up the first device from a power-saving mode, e.g. a sleep mode, wherein upon receiving the trigger the first device enters an operating mode for communicating with the second device.

In some embodiments, the secure communication channel is with a third device, rather than the second device.

In some embodiments, the first device is an IoT device. In some embodiments, the first device is a control panel of a monitoring system, for example a security system, wherein said device controls operation of one or more peripheral devices. Said operation of the first device may in such cases be a communication with a peripheral device to instruct the peripheral device to interact with the environment. The interaction with the environment may, for example, be one or more of taking a photo; sensing infrared light using a passive infrared sensor to detect motion; recording and/or forwarding an incident audio signal; sensing a vibration; instructing transmission of and/or reception of a radar signal; generating a light-based output, such as illumination of one or more lights, light emitting diodes, and/or screens; and the like. In other embodiments the first device, by way of the operation, performs an interaction with the environment, such as one or more of the interactions described above. In any case, the operation is in some embodiments an operation of a monitoring system, for example a security system or other threat detection and/or threat verification system.

In a third aspect of the present invention there is provided a device for use as a first device in a peer-to-peer network, the device configured to:

receive a record of a first transaction for a ledger distributed amongst a plurality of nodes of a peer-to-peer network, the plurality of nodes including the first device, the record of the first transaction including a first validation tool;

receive at least one message, via a secure communication channel, from an authenticated second device, the at least one message including an identifier for identifying the first transaction;

use the identifier to read the record of the transaction;

verify validity of first data received in at least one of: the record of the first transaction and the at least one message, wherein the validity is verified using at least one of the first validation tool and a second validation tool, and

in an event that a predefined condition is met, execute an operation of the first device based on said first data, the predefined condition requiring at least that said validity is verified.

In a fourth aspect of the present invention there is provided a device configured to perform the method of the any one of (and in some embodiments both of) the first aspect and/or second aspect of the present invention.

In a fifth aspect of the present invention there is provided a non-transient computer readable medium storing instructions for executing on a first device in a peer-to-peer network, wherein executing the instructions by the first device configures the first device to:

receive a record of a first transaction for a ledger distributed amongst a plurality of nodes of a peer-to-peer network, the plurality of nodes including the first device, the record of the first transaction including a first validation tool;

receive at least one message, via a secure communication channel, from an authenticated second device, the at least one message including an identifier for identifying the first transaction;

use the identifier to read the record of the transaction;

verify validity of first data received in at least one of: the record of the first transaction and the at least one message, wherein the validity is verified using at least one of the first validation tool and a second validation tool, and

in an event that a predefined condition is met, execute an operation of the first device based on said first data, the predefined condition requiring at least that said validity is verified.

In a sixth aspect of the present invention there is provided a non-transient computer readable medium storing instructions for executing on a first device in a peer-to-peer network, wherein executing the instructions by the first device configures the first device to perform the method of the any one of (and in some embodiments both of) the first aspect and/or second aspect of the present invention.

In a seventh aspect of the present invention there is provided a method for facilitating guarding of a first device against a cyber threat, the method comprising, at a second device:

instructing transmission of an authentication tool (e.g. a digital certificate) to a receiving device for authenticating the second device;

executing a first transaction for a ledger distributed amongst a plurality of nodes of a peer-to-peer network, the plurality of nodes including the first device;

instructing transmission of at least one message, via a secure communication channel, to the receiving device;

instructing transmission of a record of the first transaction,

wherein the at least one message and the transaction are correlated so that the first device is able to determine verify, based on the at least one message and the transaction, validity of first data included in at least one of the at least one message and the record of the transaction, to execute an operation of the first device based on said first data.

In some embodiments, the at least one message includes an identifier for identifying the first transaction to at least in part correlate the at least one message with the first transaction.

In some embodiments, the record of the first transaction includes a first validation tool to, additionally or alternatively, at least in part correlate the at least one message with the first transaction based on a verification that uses the first validation tool in combination with a second validation tool received over the secure communication channel.

In some embodiments the correlation is additionally or alternatively, at least in part, based on a timing relationship between the at one message and the first transaction.

Thus, this aspect of the invention has an advantage of using a distributed ledger as part of processes that provides data to execute an operation of the device, while correlating a securely transmitted message(s) with the transaction.

In some embodiments, the receiving device and the first device are the same device, the authentication tool is transmitted to the first device, and the secure communication channel used to transmit to the receiving device is therefore the same as the secure communication channel used to transmit to the first device. Thus, the first device is able to verify the authenticity of the second device, which executed the transaction on the ledger. In other embodiments, the receiving device is a different device to the first device and acts as a commander that determines the first data transmitted to the first device. The authentication tool may be transmitted to the first device directly or via the commander so that the first device can verify the authenticity of the second device, which may be used to verify that the second device had authority to execute the transaction.

In some embodiments, the receiving device, being the commander, may use secure (and therefore authenticated) communication with the first device to instruction transmission of the first data and, therewith, the identifier or a reference to the identifier.

In some embodiments the method comprises:

receiving a first address of the first device and a first public key of the first device; and

instructing transmission of the second tool to the first device.

In some embodiments the first transaction comprises assigning an amount of a cryptocurrency to the first address of the first device, wherein one or more of the first tool and second tool have been encrypted using the first public key of the first device.

In some embodiments subsequent transactions use the first public key of the first device for the encryption, while in other embodiment a next transaction uses a second public key of the first device for the encryption.

The above elements of the seventh aspect of the present invention may match the elements of the first and/or second aspects of the present invention. For example, the first public key of the seventh aspect of the invention may be the first public key of the first aspect of the present invention, wherein the first and second devices of the seventh aspect of invention respectively correspond to the first and second devices of the first aspect of the invention, etc.

In some embodiments, executing the first transaction comprises preliminarily validating at least one other transaction, and more preferably at least two other transactions (advantageously, for convergence of consensus), wherein preliminarily validating a transaction comprises determining that a From address in the record of the transaction has enough of a cryptocurrency to transfer an amount of the cryptocurrency specified by the transaction. The method may further comprise instructing transmission of a copy of the record of the first transaction, wherein the record of the copy of the first transaction identifies said at least one transaction preliminarily validated by the first transaction.

In some embodiments, the method comprises including said first data in the record of the first transaction.

In other embodiments, said first data is included in said at least one message transmitted to the first device. Thus, in such embodiments the transaction and the at least one message are asynchronous.

For such asynchronous embodiments, the first device may be configured to require the first data to be received within a predefined time-period since the transaction was executed. In some embodiments, the method further comprises, at the second device, including a timestamp in the record of the first transaction, the timestamp being digitally signed by the second device (e.g. using a first private key that corresponds to the first public key of the second device). The time stamp may also be encrypted (e.g. at the second device), and in some embodiments the encryption uses the first public key of the first device.

Further, in some embodiments the second device is configured, in the event of another predefined condition being satisfied, to execute a second transaction on the distributed ledger and instructing transmission of an identifier identifying the second transaction. Satisfaction of the other predefined condition may include a requirement that a time elapsed since a reference time is less than a predefined maximum. The reference time may, for example, a time corresponding to a time-stamp included in the record of the first transaction. As another example, the reference time may be a time of receiving an acknowledgment of a notification from the first device. As another example, the reference may be a time of day (e.g. whereby transactions are executed at predetermined times of a day).

In addition to or as an alternative to executing a second transaction based on a time, the second device may be configured to execute a second transaction in an event of any one of:

receiving a request from the first device to make a second transaction; or

not receiving a request from the first device to refrain from making a second transaction.

Maintaining the presence of an active transaction at the first device may avoid a period in which it is unable to use data received over the secure command asynchronously with a transaction, such a period otherwise arising if an amount of cryptocurrency transmitted to the first device to enable use of data is returned to the second device, or a maximum period of time has elapsed since the most recent transaction, for example.

In an eighth aspect of the present invention there is provided a second device for facilitating guarding of a first device against a cyber threat, the second device being configured to perform the method the seventh aspect of the present invention.

In a ninth aspect of the present invention there is provided a non-transient computer readable medium storing instructions for executing on a second device in a peer-to-peer network to facilitate guarding of a first device against a cyber threat, wherein executing the instructions by the second device configures the second device to perform the method of the seventh aspect of the present invention.

In a tenth aspect of the present invention there is provided a method for a first device, the method comprising:

receiving at least one message, via a secure communication channel, from an authenticated second device, the at least one message including an identifier for identifying a first transaction, for a ledger distributed amongst a plurality of nodes of a peer-to-peer network, the plurality of nodes including the first device;

using the identifier to call for the record of the transaction from a copy of the ledger on the first device; and

in an event that the call for the record fails to return the record, instructing transmission of a request, to another device in the peer-to-peer network, for a copy of the record of transaction.

The request for a copy of the record of transaction may comprise said identifier, which in some embodiments is a hash of the record of the transaction.

The record of the first transaction may include a first validation tool.

In some embodiments, the method further comprises:

receiving a copy of the record from the other device;

using the identifier to read the record of the transaction from the copy of the ledger on the first device;

verifying validity of first data received in at least one of: the record of the first transaction and the at least one message, wherein the validity is verified using at least one of the first validation tool and a second validation tool, and

in an event that a predefined condition is met, executing an operation of the first device based on said first data, the predefined condition requiring at least that said validity is verified.

In an eleventh aspect of the present invention there is provided a first device configured to perform the method the tenth aspect of the present invention.

In a twelfth aspect of the present invention there is provided a non-transient computer readable medium storing instructions for executing on a first device, wherein executing the instructions by the first device configures the first device to perform the method of tenth aspect of the present invention.

As used herein, except where the context requires otherwise, the terms “comprises”, “includes”, “has”, and grammatical variants of these terms, are not intended to be exhaustive. They are intended to allow for the possibility of further additives, components, integers or steps.

Various embodiments of the invention are set out in the claims at the end of this specification. Further aspects of the present invention and further embodiments of the aspects described in the preceding paragraphs will become apparent from the following figures and description, given by way of non-limiting example only. As will be appreciated, other embodiments are also possible and are within the scope of the claims.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is an exemplary topology of system which is operated in part with a peer-to-peer network in accordance with one or more aspects of the present invention;

FIG. 2 is conceptual diagram showing part of the system of FIG. 1, and showing parameters transferred in a first communication method in accordance with some embodiments of the present invention, in which data for an operation of a device is communicated via a transaction on a distributed ledger;

FIG. 3 is a swim lane diagram of a first embodiment of the first communication method;

FIG. 4 is swim lane diagram conceptual diagram of a second embodiment of the first communication method;

FIG. 5 is conceptual diagram showing part of the system of FIG. 1, and showing parameters transferred in a second communication method in accordance with some embodiments of the present invention, in which data for an operation of a device is communicated via a secure communication protocol, wherein the data is linked to a transaction on a distributed ledger by a timing relationship; and

FIG. 6 is swim lane diagram conceptual diagram of an embodiment of the second communication method.

DETAIFED DESCRIPTION OF THE EMBODIMENTS

An exemplary system topology 10 in which one or more aspects of the present invention may be implemented is illustrated in FIG. 1. The topology includes a first device 12 that acts as a receiver of data from a second device 14, which acts as a sender. The receiver 12 is in some embodiments an IoT device which may be, for example, an internet enabled camera, passive infrared (PIR) sensor, motion detector, microphone, speaker, or any other IoT device, or a device having a combination of such internet enabled functions, or may be an internet enabled control device that in turn controls such devices (not shown) via a secure private network (not shown). The control device may for example be a control panel that controls a plurality of sensing devices and/or output devices, which may collectively form a threat detection and/or verification system, such as a monitoring system.

The data sent by sender device 14 to the receiver device 12 is used for execution of an operation on the receiver device 12. For example, in embodiments where the receiver device is a camera, the operation may be to take a photo, or to read a photo stored in a memory or the device, or to enable configuration data to be written to the device (e.g. to update software on the device). Additionally, or alternatively, the data may data included in previously commanded operation, e.g. the data some or all of a set of data that makes up new, or an update to, software for the device. In embodiments where the receiver device is a control panel the operation may similarly be to read data from or write data to memory on the receiver device, and/or the operation may be to transmit data such as a command and/or read/write data to one or more peripheral devices such as cameras or other sensors accessed via the private network between the control panel and the peripheral device(s). The sender device 14 may, for example, be a device at a central monitoring station (CMS) where personnel monitor data sensed by or via the receiver device 12.

Optionally, the transmission of the information from the sender to the receiver may be commanded by a third device 16, for example a smart phone or other portable computing device, which is may be carried by an owner, or relative of a resident, of a premises being monitored with the receiver device 12.

Each of these devices 12, 14 and 16, in this example, communicates with a Certificate Authority (CA) device 18 to enable authentication of their identity to one or more of the other devices 12, 14, 16 if and when such authentication is requested by the other device. Authentication techniques for establishing a secure communication channel are well known in the art. Authentication may for example be achieved by checking that a digital certificate received from a device is checked against a digital certificate received from the CA 18. Such authentication techniques are integral to various secure communication protocols such as Secure Sockets Layer (SSL) and its more recent counterpart Transport Layer Security (TLS), which are used in the exemplary embodiment described herein if and when any one of the devices 12, 14 or 16 communicates with another one of the devices 12, 14 or 16. The authentication process is part of a handshake procedure used to establish a secure communication channel 20, 22, 24, 26, 28, 30 according to these protocols, via a network 32, e.g. a wide area network such as the Internet. Though authentication may be in both directions, in the exemplary embodiments communications to the device 12 involve authentication of at least the device(s) that transmits information to it. After authentication, information communicated between the devices using the secure communication channel is signed and encrypted to guard against tampering and overhearing. Such encryption may for example be by asymmetric cryptography, as is the case in TLS, for example.

In at least some communications between the sender device 14 and the receiver device 12 communication over the secure communication channel is intertwined with communication using a distributed ledger via a peer-to-peer network 34 that comprises the receiver device 12, the sender device 14 and a plurality of other device nodes 36. In some embodiments the devices in network 34 may be part of the network 32, but in some embodiments the devices in network 34 may be part of a private network within the broader network 32. The private network within the broader network 32 may in some architectures include one or a plurality (including potentially, all) of the abovementioned peripheral device(s), in embodiments in which the receiver device 32 is used to control the peripheral device(s).

The ledger stores a record of each transaction executed using the distributed ledger framework of the peer-to-peer network 34. The ledger has a history that is immutable (a record cannot be deleted once added), and is replicated on all of the device 35, 12 and 14 in the peer-to-peer network 34. When a device (e.g. sender device 14) in the network 34 executes a transaction, it stores a record of the transaction on its copy of the ledger and then forwards a copy of the record of the transaction to one or more other devices, in this case three other devices 36a, 36b, 36c, which in turn forward a copy of the record to others of the devices 36, and so on. A plurality of devices ends up with a copy of the record of the transaction. Ideally all of the devices 36, including receiver device 12, ends up with a copy of the record of the transaction. However, in an event that the receiver device 12 receives an identification of a transaction as described herein but has not received a copy of the record of transaction, the receiver device may transmit a request to another device 36 in the network 34 to forward to it a copy of the record. If the other device 36 does not have a copy it may ask yet another device for a copy, and so on.

In any case, each device of the network 34 forwards a copy of the record of the transaction to another one or more devices in the peer-to-peer network, but in other embodiments to at least two other devices, and ultimately the receiver device 12 receives a copy of the record and integrates it into its ledger.

A transaction on the distributed ledger involves a transfer of cryptocurrency, and the transaction may be defined as being either to or from the address of the first device. However, for a given device of the network 34 to execute a transaction it must preliminarily validate each of a certain minimum number (e.g. two) of un-validated transactions on its ledger.

The ledger is a directed acyclic graph (DAG) of the transactions, each transaction being represented by a record that is identifiable by an identifier that is an output of a hash function that uses the record as an input. The DAG depicts which transactions have been preliminarily validated by which other transactions. Frameworks for implementing a DAG are known in the art, so will not be further described here. For example, the framework may be IOTA or Hashgraph framework.

In the case of IOTA, the DAG may be referred to as a Tangle, and the cryptocurrency may be measured in MIOTA coins. To receive an assignment of the cryptocurrency, a given device distributes an address to which the amount of the cryptocurrency in a given transaction is to be assigned. The address is generated from a seed that is a secret on the given device. The seed is also used to generate cryptographic keys. For example, a pair of private and public keys (for public key cryptography) may be generated from the seed. In some embodiments for increased security, different cryptographic keys are generated for different transactions to the given device. Also for increased security, from the seed different addresses are generated for different transactions to the given device. Further, the public and private keys used for respectively encryption and signing in transactions onto the distributed ledger framework, are in the described embodiments distinct from keys used to communicate over the secure network connection.

Each device of the network 34, by way of the distributed ledger, receives information about all of the transactions that have occurred, but unless it looks into the record of every transaction, does not know which transaction record is addressed to it. The device can however, readily check whether it has cryptocurrency in its address, and how much of the cryptocurrency is present. However, neither the address nor the presence of cryptocurrency in the address informs the device of identity of the device that the assigned the cryptocurrency to the address. Thus, the transactions on the ledger are effectively anonymous. However, in the examples described herein a device that executes a transaction transmits a hash of the transaction record to the device that is the recipient of the transaction. The hash uniquely identifies the transaction to the recipient, and is transmitted to the recipient via the secure communication channel. The recipient may then use the hash to identify and read the record of the transaction, optionally, in a single hop (i.e. step). Data for operation of the device is transmitted in either the transaction record, or in a message transmitted over the secure communication protocol. Further, because a secure communication protocol is used to transfer the hash, the recipient of the hash is able to authenticate the identity of the device (e.g. using its digital signature and corresponding digital certificate, for example) that transmitted the hash and by inference the device that executed the transaction corresponding to the hash. In this manner the recipient of the transaction can determine whether the transaction was made from an authorized device.

For added security the recipient verifies the validity of the received data by using a first validation tool that is included in the transaction record. The validation step also utilizes a second validation tool which is received separately from the transaction record. For example, validation may be based on public key cryptography, whereby a public key of the device that executed the transaction is used to check that a received signed version a message was derived from the same message. For example, the first validation tool may be the message along with the signed version of the message, the signed version being signed using a private key of the sender device 14. The second validation tool may in such a case be the public key of the sender device 14 that corresponds to that private key. Thus, as will be appreciated the validation step may thereby be verifying that the message was correctly digitally signed with the private key of the sender device 14.

In some embodiments, that public key is received by the receiver device 12 from the sender device 14 over a secure communication channel. Since the sender device 14 is authenticated by virtue of the secure communication channel, it is inferred that the received public key is also authentic because that public key was itself digitally signed and verified as being authentic using an authenticated key of the secure communication channel.

In other embodiments that public key is received by a different means and independently verified with CA18, as being authentic. However, the public key of the sender device 14 may advantageously be different to the key (public or otherwise) used to verify data received over the secure communication channel 20.

As will be appreciated other validation tools may alternatively be used, for example symmetric cryptographic techniques.

Although the sender and recipient are described herein as being the controlling device 14 and the IoT device 12, when data is transmitted from the IoT device 12 to the controlling device 14, the IoT device 12 may act as the sender with the controlling device 14 acting as the recipient. However, for ease of explanation, the examples included herein treat device 12 as the recipient and device 14 as the sender, unless otherwise stated.

Examples:

FIGS. 2 and 3 illustrate an embodiment in which the data transmitted to the receiver device 12 is included in the record of the transaction and is therefore synchronous with the transaction. FIG.2 is a conceptual diagram of a “synchronous” embodiment 49, listing various parameters communicated between the sender device 14 and the receiver device 12 in order to transfer data to the receiver device 12 to execute an operation of the receiver device 12.

Using secure communication channel 20, the sender device 14 transmits, in relation to a first transaction Txl, the hash (Hash (Txl)) of a record of the first transaction Txl, and a first address of the sender device 14 (Device2Addressl) for the receiver device 12 to use when acknowledging Txl.

The receiver device 12 uses the secure communication channel 20 to transmit the first public key of the receiver device 12, and a first address of the receiver device 12 to which the sender 14 is to direct the transaction Txl.

FIG. 2 also depicts a part of the ledger 50 on the sender device 14 immediately after executing two transactions Txl and Tx3. In the depicted part of the ledger 50 each of transactions Txl, Tx2 and Tx3 point to two other transactions that they have preliminarily validated, the validation being preliminary because consensus has not yet been reached. Transactions TxX, TxY and TxZ point to other transactions (not shown).

As each of transactions Txl and Tx3 are executed by the sender device 14, the sender device 14 transmits copies of respective records 52 and 56 of the transactions to the peer-to-peer network 34 to be dispersed to each of the nodes in the network 34, including the receiver device 12. As each node receives the records 52 and 56, the node incorporates the records into its own version of the ledger. As will be explain herein Tx2 is intermediate transaction from the receiver device 12 to the sender device 14. A record 52 of the transaction first transaction Txl includes the following parameters:

- The address (Device2Address) of the sender device 14 from which an amount cryptocurrency (e.g. 1 coin) is being assigned by the transaction,
- The address (Device1Address1) of the receiver device 14 to which the amount cryptocurrency is being assigned by the transaction.
- The data and a signed version of the data (signed with a first private key of the sender device 14), the data and the signed version of the data being, in some embodiments, encrypted using the first public key of the receiver device 12.
- The amount of cryptocurrency being assigned by the transaction (in some embodiments the amount is zero, however, or this parameter may be excluded).

Once receiver device 12 receives a copy of the record 52 and confirms that consensus has been reached in respect of the transaction Txl, the receiver device 12 using its first private key to decrypt the data and signed data and uses the first public key of the sender device 14 to check that the data was correctly signed (i.e. it was signed using the corresponding private key of the second device 14). If consensus is not reached and/or if the data was not correctly signed, the receiver device 12 notifies the sender device 14 (e.g. via the secure communication channel 20) that the transaction failed, or alternatively the device 12 may execute other appropriate actions, e.g. alert some other device (e.g. a monitoring station, which may be a network operations center) that an unsuccessful transaction occurred. However, in an event that consensus is reached and the data was found to be correctly signed, the sender device uses the data. For example, it may read or write to memory or execute some other action, e.g. take a photo, depending on what is defined by the data.

Once the data has been validated for use, the receiver device 12 executes a transaction Tx2, having a corresponding record 54, to return the amount of cryptocurrency assigned to it by transaction Txl. Thus the respective balances of cryptocurrency at the sender device 14 and receiver device 12 before Txl is maintained.

When the sender device 14 next needs to transfer a command or other relevant data to the receiver device 12, a new transaction Tx3, having a record 56, is executed by the sender device 14. The new transaction Tx3 may have the same parameters as the previous transaction Txl, but with at least one different value so that it produces a different hash for its identification.

However, in some embodiments, the new transaction Tx3 is based on different addresses and/or different keys. Thus any addresses and/or keys that may become known to an authorized person cannot be used by that person to perform a “replay” attack, by reusing the addresses and/or keys.

The depicted portion of the ledger 50 in FIG. 2 illustrates, using arrows, that the execution of each transaction Txl, Tx2 and Tx3 involves a preliminary validation of two other previously un-validated transactions. As will be appreciated, in FIG. 2 Tx3 is a leaf/edge transaction as it is yet to be preliminarily validated. For clarity, the term validation in referring to the validation of the transaction (as dictated by the framework of the distributed ledger, such as the IOTA or framework, for example). This is distinct from the validation of the received data using the first and second validation tools.

A swim lane timing diagram showing an exemplary data transfer method 100 using Txl and Tx2 discussed in FIG. 2 in shown more detail in FIG. 3. The method begins upon wakeup of the receiver device 12. The wakeup may be triggered, for example, by an environmental event sensed by the receiver device 12. For example, the event may be a detected movement of a person, sensed by a motion sensor included in the receiver device 12 or in a device with which the receiver device is in communication. Alternatively, the trigger may be based on a request to wake, received from the sender device 14. Alternatively, the trigger may result from powering on the receiver device 12.

Upon waking, the receiver device 12 enters a communication mode. Prior to waking the receiver device may have been in an idle state in which no active communication session to a sender device 14 is in use. In other embodiments, prior to being in the awake state, the receiver device 12 may be in a power-saving state, especially but not necessarily only, in embodiments in which the receiver device 12 is battery powered, and power usage may be highly regulated.

At step 101, upon entering communication mode, the receiver device 12 requests a secure communication channel with the sender device 14. In the illustrated examples herein the secure communication channel is exemplified by a TLS communication channel. The establishment of the TLS in this example involves authentication of the identity of at least the sender device 14, using a digital certificate from CA 18, as is standard for TLS, and which was described herein in reference to FIG. 1. It also involves an exchange of TLS public keys for sender and the receiver for signing and encrypting TLS all information communicated over the TLS channel.

Once the secure communication protocol has been established, at step 102, the receiver device 12 transmits its first address and first public key (distinct from its TLS public key) to the sender device 14. The sender device 14 then, at step 103, supplies its first address and first public key (distinct from its TLS public key) to the receiver device 12.

At step 104 the sender device 104 executes transaction Txl referred to in FIG. 2 by transferring/assigning, via the ledger 50, a designated amount (e.g. 1 coin) of the cryptocurrency to the first address of the receiver device 12. A record 52 of the transaction Txl is written to the ledger 50 by the sender device 14, and includes the data intended for an operation of the receiver device 12. A signed version of the data is also included, being signed using a first private key of the sender device 14, the first private key of the sender device 14 corresponding to the first public key of the sender device 14. The data and the signed data are together encrypted using the public key of the receiver device 12.

The record may also include a timestamp (not shown in FIG. 2) or some other parameter such that a hash of the record is unique. The record of Txl also includes identifiers (not shown) such as hashes identifying respective transactions that were preliminarily validated to execute the Txl.

At step 105, the sender device 14 transmits over the secure communication channel the hash of the record of the transaction.

At step 106 the receiver device 12 uses the received hash to identify and read the record 52 from its own manifestation of ledger 50. The receiver device 12 then uses its first private key, which corresponds to its first public key, to decrypt the data and the signed data and uses the public key of the sender device 14 to verify that the signed data was derived from the data. If the signature is successfully verified, the receiver device 12 then uses the data for its intended purpose, which depends on what is encoded in the data. In some embodiments, for added security, the receiver device 12 only uses the data if and when consensus is reached on the transaction.

Upon successful verification and use of the data, at step 107, the sender device 12 executes transaction Tx2 to return the received amount of cryptocurrency from its first address to the first address of the sender device 14.

The receiver device 12 also transmits, at step 108, an acknowledgement to the sender device 14, over the secure communication channel. The acknowledgement identifies the corresponding identification, by referencing the hash of the record of Txl in the acknowledgement. Additionally, the receiver device 12 transmits over the secure communication channel a second address and a second public key of the receiver device 12 to be used for the next transaction Tx3 by the sender device 14. Alternatively, the second address and second public key may be sent earlier, e.g. before executing Tx2 and/or before completing verification of Txl, so that the next transaction Tx3 by the sender device 14 need not wait until receiving acknowledgement of the first transaction Txl.

In the embodiment of FIG. 3 the receiver device 12 may for example be an IP (internet protocol) enabled camera, and the sender device 14 may for example be an application server. The server may be any authorized device that is part of the peer to peer network 34. In some embodiments the server may, for example, be a smart watch. The relevant data transmitted in the record 52 for use in operating the IP camera may for example be a command to take a photo or video. The acknowledgement may inform the server that the photo was actually taken. Subsequently the IP camera may act and the sender and the server may act as the receiver, and the method 100 may be repeated accordingly. The relevant data may then be for example the relevant photo or video to be forwarded or stored by the application server. As will be appreciated the relevant data may be a portion photo or video, whereby transmission of the whole photo/video is spread over multiple iterations of the method 100, with different transaction records comprising different portions of the photo/video file.

In some embodiments, the data for the operation of the receiver device 12 originates from a device other than the sender device 14. For example, the data may originate from the third device 16 referred to in FIG. 1. The third device 16 may for example be a smart phone that is not part of the peer-to-peer network. Since the third device 16 is outside the peer-to-peer network, the sender device 14, being part of the network 34, acts to execute the transaction onto the distributed ledger on behalf of the third device 16. The sender device 12 may be any random and ready device in the peer-to-peer 34.

Using a secure connection, such as TLS between the third device 16 and the sender device 14, the data for operating the receiver device 12 may be communicated from the third device 16 to the sender device and the sender device 14 then forwards the data using a secure communication with the receiver device 12 and a transaction on the ledger 50, in accordance with method 100. When the sender device 14 receives the acknowledgement from the receiver device 12 the sender device 14 then transmits an acknowledgement to the third device 16.

Another exemplary method 300 in which the data originates from a third device 16 is illustrated as a swim lane diagram in FIG. 4. For simplicity of explanation the FIG. 3 shows only a single transfer of command data, but as will be appreciated, subsequent transfers of data may be executed using new sets of keys and/or addresses, for example as discussed in relation to FIG. 2. In this exemplary embodiment, the interaction between the sender device 14 and the receiver device 12 is the same as in FIG. 3, except that rather than the data being signed by the private key of the sender device 14 and verified by the receiver device 12 using the corresponding public key of the sender device 14, the data is signed by the third device 16 using a private key of the third device 16, and is encrypted (using the public key of the receiver device 12) by the third device 16 rather than the sender device 14. The sender device 12 is in this example not involved in encryption or signing. However, the source of the data is still authenticated because the because the public key of the third device 16 is received by the receiver device 12 over a secure and therefore authenticated communication channel with the third device 16.

More specifically, in method 300, the receiver device 12 communicates with both the sender device 14 and the third device 16 using respective secure communication channels (e.g. TLS or its predecessor SSL), and the transaction Txl on the ledger 50 is made by the sender device. By virtue of the secure communication channel both the sender device 14 and the third device are authenticated by the receiver 12 during the handshake procedure establishing the respective secure communication channels. Additionally, there is a secure communication channel between the sender device 14 and third device 16, with each of these devices being authenticated to each other during the handshake establishing that secure communication channel.

In contrast with method 100 in which the receiver device 12 wakes up and initiates a communication with device 14, in method 300, at step 301, there is a public key exchange between the third device 16 and the sender 14 and the receiver device is woken by a third device 16. Additionally, the third device informs the receiver device 12, over a secure communication protocol, of the identify of a sender device 14 that will execute the transaction onto the ledger. This may be achieved for example by supplying the receiver device 12 with the public key of the sender device 14.

At step 302 the receiver device 12 transmits its address for Txl to the sender device 14. Using the secure communication channel between the receiver device 12 and third device 16, in step 303 the receiver device 12 receives the public key of the third device 16 and in step 304 sends the receiver device 12 sends its own public key to the third device 16. In step 306 the third device 16 transmits, to the sender device 14, the data for executing an operation on the receiver device 12. A signed version of the data is included in the transmission, the signing using the private key of the third device 16, and the data and the signed data are collectively encrypted at the third device 16, using the public key of the receiver device 12. As will be appreciated, this signed and encrypted data is itself signed and encrypted as part of the TLS communication to the sender device 14 using the TLS signing and encryption keys.

Upon receipt of the signed and encrypted data at the sender device 14, and decrypting the TLS layer encryption and checking the TLS layer signature, at step 307 the sender device 14 executes transaction Txl transferring a coin to from the sender device 14 to the receiver device 12, and includes the signed and encrypted data (as signed using the private key of the third device 16 and encrypted using the public key of the receiver device 12), received from the third device 16, in the record of the transaction Txl.

At step 308 the sender device 14 transmits, via its secure communication channel with the receiver device 12, the hash of the record of transaction Txl. At step 309 the receiver device 12 uses the received hash of the record of Txl to read the signed and encrypted data from the record of Txl, decrypts the data using its private key, and uses the public key of the third device 16 to verify the validity of the data by verifying the signature. Additionally, in some embodiments the receiver device 12 also checks to ensure consensus on the transaction Txl. Assuming the required conditions for use are met (verification/validation of the data and consensus of the transaction) the receiver device 12 sends an acknowledgement to the sender device 14 at step 310, and executes transaction Tx2 returning the coin to the sender device 14 at step 311. At step 312, the sender device then transmits an acknowledgment of success to the third device 16 in respect of the data (e.g. command) that transmitted at step 306. The acknowledgement is signed and encrypted by virtue of being over a secure communication channel 22 (FIG. 1). However, it is additionally signed using the sender device’s private key that may change with each transaction onto the distributed ledger. The corresponding public key to verify the signature for that transaction was transferred to the third device 16 at step 301.

In a subsequent transaction the roles of the sender and the receiver may be reversed. For example, the third device may instruct the device 12 to act as a sender to device 14 which acts as the receiver.

As alternative to including the data for operation of the receiver device 12 in a record of transaction, in other embodiments the data is asynchronous with the transaction by being included in the secure communication channel. This is depicted conceptually in an exemplary embodiment of such a “asynchronous” communication 60 in FIG. 5. The communicated parameters in the depicted asynchronous embodiment 60 are the same as in the synchronous embodiment 49, except that in the asynchronous case, the record 62 of the transaction Txl includes a timestamp that is at least signed and in some embodiments encrypted, and the record 62 excludes the signed and encrypted data, which is instead communicated over the secure communication channel 20. The receiver device 12 may associate the hash of the record 62 of transaction Txl with the data received in the same secure communication session to determine that the data is intended to be linked to that transaction Txl. The timestamp in the record of the transaction Txl is used to provide one means of limiting the amount of time available for data sent over the communication channel to be associated with the transaction Txl. An additional or alternative means of limiting the amount of time the data may be associated with the transaction is for the receiver device 12 to, after some defined time, return the amount of the cryptocurrency received in the transaction Txl, and only using the data received over the secure communication protocol if the amount of the deposited cryptocurrency for the associated transaction is still present in the relevant address of the receiver device 12 (i.e. the coin has not yet been returned).

A swim lane timing diagram 200 illustrating an example of such an asynchronous embodiment is illustrated in FIG. 6. For ease of explanation the description below assumes that the amount of cryptocurrency transferred in any given transaction is one coin, but of course other quantities may be used. In this example twice the amount (i,e. two coins) of a single transaction is juggled in the method 200 in order to facilitate there always being at least one in-consensus transaction in place to which data over the secure communication channel may be associated, when the receiver device 12 is in the communication mode. Therefore, for ease of explanation the description below refers to a first coin and a second coin that are alternatively used for successive transactions. It will be appreciated however, that the coins themselves are not independently identifiable or distinguishable. They are conceptually distinguishable for the purpose of the description of the present example however by the respective addresses to which they are assigned.

In the method 200, upon waking the receiver device 12, a secure (and therefore authenticated) communication channel is established with the sender device 14, as in step 101 of method 100. Then at step 201 the receiver 12 transmits to the sender device 14 a public key (ReceiverPublicKeyl) and address (ReceiverAddressl) of the receiver device, for receiving coinl. The receiver device 12 already has another coin (coin2) assigned to another address (ReceiverAddres sO).

At step 202 the sender device 14 executes a transaction Txl assigning coinl to ReceiverAddressl and includes in the record 62 of the corresponding transaction a timestamp defining a time at which the transaction was executed. The timestamp is signed using a first private key of the sender device 14 and, in some embodiments, encrypted, using ReceiverPublicKeyl. The signed and unsigned versions of the timestamp may collectively act as the first validation tool, the second validation tool being the public key of the sender device (SenderPublicKeyl) corresponding to the sender's first private key.

At step 203 the sender device 14 transmits, over the secure communication channel, SenderPublicKeyl and a first address (SenderAddressl) for returning coin2. The transmission also includes the hash of the record 62 of the transaction Txl.

At step 204 the receiver device 12 checks for consensus on the transaction Txl, the transaction Txl being identified by the received hash. The receiver device 12 also checks that coinl is present at RecieverAddressl (i.e. it has not yet been assigned back to the sender device 14). Additionally, the receiver device 12 uses the first validation tool in combination with the second validation tool as part of the verification of the validity of data that will be asynchronously received (or may already have been received) over secure communication channel 20. For example, the receiver device 12 may use SenderPublicKeyl as the second validation tool with the signed timestamp and unsigned timestamp (collectively the first validation tool) to determine whether the timestamp was validly signed, and determining the data received over the secure communication protocol to be valid if it was received within some predefined time window in relation to the time in the time stamp. Since the data is received asynchronously it may in some cases be received before the record of the transaction. Thus, in some embodiments, at least part of the time window may comprise a portion of time before the time defined in the timestamp.

Within some predefined time-window that commenced upon identifying consensus on the transaction Txl or, in some embodiments, commences at the time designated in the timestamp, the receiver device at step 205 executes transaction Tx2, retuning coin2 from ReceiverAddres sO to SenderAddressl.

Asynchronously with the steps 202 and optionally independently of step 203, the receiver device receives one or more messages such as message 213, over the secure communication channel 20, each of the messages includes a hash of the record of the transaction to which the message is intended to be associated and data (e.g. a command) for operation of the receiver device 12. Along with the given data there is included a version of the data that has been signed by a private key of the sender device 14. The data and the signed data are in some embodiments also encrypted, for example using a public key of the receiver device 12. The keys of a given device are different for different ledger transactions from that device. For example, the receiver device 12 requires for Txl that corresponding data received over the secure communication channel 20 will be encrypted using the ReceiverPublicKeyl and will have that its correct signing can be verified by use of SenderPublicKeyl.

Thus, when a message 213 is received over the secure communication channel 20, the receiver device 12 at step 214 uses the sender public key that corresponds to the transaction (as identified by the received hash) to verify that at least part of the message, that includes the data intended for an operation of the receiver device 12, was correctly signed. Verification that the data is valid also requires that the coin assigned to the address of the receiver device 12 for the associated transaction is still present at that address. Further, verification that the data is valid also requires that the data (i.e. command data or example) received over the secure communication is received within a predefined maximum amount of time since the time corresponding to the timestamp in the associated transaction. As will be appreciated these security techniques guard against a “replay” attack by a potential hacker. If the data is verified, at step 214, as being valid then at step 215 the receiver device 12 transmits an acknowledgement to the sender device 14, referencing the hash of the record of the transaction. In some embodiments where multiple messages may be received for a single transaction, the reference to the relevant message may also be included in the acknowledge. Different messages for the same transaction may, for example, be distinguished by timestamp information included in the message.

At step 206, the sender device 14 checks SenderAddressl to verify that it has received back a coin (corresponding to coin2) and verifies consensus has been reached in respect of the transaction. Receipt of the coin may be verified by periodically checking SenderAddressl for a balance of cryptocurrency. Consensus may be verified by reading the record of each transaction to identify a transaction that assigned the coin the SenderAddressl, and checking for consensus on that transaction. However, in some embodiments there may be more than one transaction to a given address, and in any case reading every record is computationally expensive. Therefore, more preferably in parallel with executing Tx2 step 205, the receiver device 12 transmits (not shown) a hash of the record of Tx2 to the sender device 14. If the expected cryptocurrency has not been returned and/or consensus has not been reached on the transaction that returned the coin, the sender device 14 may optional issue an alter or undergo an action on an inference that the receiver device 12 may have had its security/integrity compromised, may be offline, or it may have lost SenderAddressl.

At step 207 the receiver device 12 transmits ReceiverAdress2 and ReceiverPublicKey2, for the sender to use on its next transaction to the receiver device 12. That next transaction Tx3 is executed at step 208, assigning a coin (e.g. coin2) to ReceiverAdress2 with a timestamp signed with SenderPivateKey2 and encrypted with ReceiverPublicKey2. At step 209, the sender device 14 transmits to the receiver device 12 a hash of the record of Tx3; and SenderAddress2 and SenderPublicKey2 for the receiver device 12 to use eventually return a coin (e.g. coinl) in step 211. However, before returning the coin the receiver at step 210 verifies the relevant validation tool (e.g. by checking that the relevant timestamp was correctly signed) and that consensus is obtained on Tx3, in the same manner as done at step 204 for transaction Txl. Any further data/commands for the receiver device 12 received over the secure communication channel will therefore at this stage need to include a signature verifiable by SenderPublicKey2, be decryptable using SenderPrivateKey2 and be associated with an identifier of Tx3 (e.g. the hash of the record of the Tx3). Additionally, as will be appreciated the message must be received within a predefined time window with respect to time defined by the relevant time stamp of Tx3 and while the relevant coin is still assigned to ReceiverAddressl.

As in the synchronous case, synonymous with method 300, asynchronous embodiments may alternatively use a third device to determine what data/commands are to be communicated to the receiver device 12 for executing an operation on the receiver device 12.

In some embodiments, the sender device 14 may communicate by a secure communication channel to the third device to inform the third device 16 of a currently active transaction, providing to the third device 16 the hash of the record of the relevant transaction so that the third device can supply commands over a secure communication channel to the receiver device 12. The sender device 14 knows the relevant key and address of device 12 to by a prior exchange over the secure communication protocol. The sender device 14 may also supply the third device, with any other information if desired, for example, a copy of the timestamp so that the third device 16 knows how long the transaction will remain valid for. Such embodiments, may optionally be simplified by omitting the requirement that the commands may be signed by the same device that executed the transaction, but optionally include an alternate means (e.g.

through an appropriate public key exchange) to identify the third device 16 as being related to the sender device 14 that issued the relevant transaction.

The device of any of the aspects of present invention is in some embodiments a chip. Various steps of the invention involving instructing of a transmission. In embodiments in which the device is a chip the device may instruct a transmission component or module, which may comprise an antenna, do the transmission. In other embodiments, the device may itself do the transmission. For example, the device may include one or more components, e.g. one or more antennas, which performs the transmission. In some embodiments, where the device is not solely a chip, the device may include one or more processors configured to perform the steps of the present invention. For example, this is case for embodiments in which the device is an IoT device and/or a control panel, or monitoring station, or a general purpose computing device (e.g. a smartphone, laptop, desktop, tablet or the like).

Further in some embodiments executed on a plurality of processors, the processors may be distributed and geographically separated from each other. In some embodiments, the or each processor may communicate with a non-transient memory to configure the processor to be able to perform a method of the invention. In executing the method, the/each processor may use non-transient memory that is external to the chip. Alternatively, the/each processor may include a one or onboard more memory which may include at least part of the non-transient memory and/or at least part of the transient memory. The/each processor may for example be an ASIC chip, micro-controller, FPGA or microprocessor, and suchlike. The non-transient memory may include for example any one or more of a ROM (e.g. for a Bios), Flash memory or other EEPROM device, or any other non-transient memory. The transient memory may for example be a random access memory such as one or more DRAM modules. Where a given item is referenced herein with the preposition “a” or “an”, it is not intended to exclude the possibility of additional instances of such an item, unless context requires otherwise.

Where the specification defines a range, the stated outer extremities of the range are part of the range, unless context requires exclusion of the outer extremities from the range. From example, a range defined in terms of being between X and Y or from X to Y, should be interpreted as including X and Y.

The invention disclosed and defined herein extends to all plausible combinations of two or more of the individual features mentioned or evident from the text or drawings. All of these different combinations constitute various alternative aspects of the invention.

WHAT IS CLAIMED IS:

1. A method for guarding a first device against a cyber threat, the method comprising:

receiving a record of a first transaction for a ledger distributed amongst a plurality of nodes of a peer-to-peer network, the plurality of nodes including the first device;

receiving at least one message, via a secure communication channel, from an authenticated second device, the at least one message including an identifier for identifying the first transaction; and

using the identifier to read the record of the transaction.

2. The method of claim 1 wherein the method further comprises:

verifying validity of first data received in at least one of: the record of the first transaction and the at least one message, wherein the record of the first transaction includes a first validation tool and the validity is verified using at least one of a first validation tool and a second validation tool, and

in an event that a predefined condition is met, executing an operation of the first device based on said first data, the predefined condition requiring at least that said validity is verified.

3. The method according to claim 2, wherein the first data is received over the secure communication protocol and the first validation tool comprises a signed version of timing data, whereby the first data is not accepted by the first device if the first data is associated with a time that is different from the timing data by more than a threshold.

4. The method according to claim 2, wherein the first validation tool comprises a signed version of the first data.

5. The method according to any one of claims 3 to 4, wherein the second validation tool is used by the first device to confirm the integrity of the signed data.

6. The method according to any one of claims 2 to 5, wherein the second validation tool is a public key corresponding to a private key used to sign the data.

7. The method according to any one of claims 2 to 6, wherein the second validation tool is received over the secure communication channel.

8. A method for guarding a first device against a cyber threat, the method comprising:

receiving a record of a first transaction for a ledger distributed amongst a plurality of nodes of a peer-to-peer network, the plurality of nodes including the first device;

receiving at least one message, via a secure communication channel, from an authenticated second device, the at least one message including:

first data for executing an operation of the first device based on the first data;

verifying validity of the first data based on a correlation between the at least one message and the first transaction; and

in an event that a predefined condition is met, executing the operation of the first device based on said first data, the predefined condition requiring at least that said validity is verified.

9. The method according to claim 8, wherein the correlation comprises a timing relationship that correlates a first event associated with the at least one message with a second event associated with the first transaction.

10. The method according to claim 9, wherein the first event is receipt of the first data.

11. The method according to claim 9 or 10, wherein the second event is any of: a time defined in the record; and a time at which validity of the first transaction is determined to reach consensus according to a rule of the peer-to-peer network.

12. The method according to any one of claims 9 to 11 wherein the method comprises determining that the timing relationship correlates the first event with the second event, if any one of, or both of:

the first event is determined to have occurred within a predefined time window in relation to the second event; and

the second event is determined to have occurred within a predefined time window in relation to the first event.

13. The method according to any one of claims 8 to 12, wherein the method comprises: receiving, via the at least one message, an identifier for identifying the first transaction; and using the identifier to read the record of the transaction to determine whether there is said correlation between the at least one message and the first transaction.

14. The method according to any one of claims 8 to 12, wherein the record of the first transaction includes a first validation wherein said predefined condition further requires a verification that the first validation tool is valid.

15. The method according to claim 14, wherein verification that the first validation tool is valid involves use of a second validation tool received via the secure communication channel.

16. The method according to any one of claims 2 to 15, wherein the record of the first transaction is received in a separate communication to receiving said at least one message.

17. The method according to any one of claims 2 to 7 and 15 to 16, wherein the first validation tool comprises a first message and a first digital signature, the first digital signature being a digitally signed version of the first message.

18. The method according to claim 17, wherein the second validation tool is a first public key of the second device, wherein the validity is verified by using the first public key of the second device to check that the first digital signature was derived from the first message.

19. The method according to any one of claims 2 to 7 and 14 to 16, wherein the first validation tool is a first public key of the second device, and the second validation tool is a first message and a signed version of the first message.

20. The method of any one of the preceding claims wherein the communication channel is secured Transport Layer Security (TLS).

21. The method of any one of the preceding claims wherein first cryptographic keys used for security of the communication channel are different to second cryptographic keys used for security of the first data on the record of the first transaction.

22. The method of any one of the preceding claims wherein the first data is encrypted, wherein the method comprises decrypting the first data using a first private key of the first device.

23. The method of any one of the preceding claims wherein the identifier of the record of the first transaction is a hash of the record of the first transaction for uniquely identifying the transaction.

24. The method of any one of the preceding claims wherein the distributed ledger comprises a Directed Acyclic Graph (DAG).

25. The method of any one of the preceding claims wherein a framework, operated on each of the nodes of the peer-to-peer to implement the ledger on the node, requires each transaction to validate one or more preceding transactions.

26. The method of any one of the preceding claims wherein the method further comprises storing the record of the first transaction on the ledger, and determining whether there is consensus in respect of the first transaction and said predefined condition further requires that said consensus has been reached.

27. The method of claim 26 wherein said predefined condition further requires that said consensus has been reached within a predefined amount of time since any one or both of: (a) the record of the transaction was received; or b) a time corresponding to a timestamp in the transaction.

28. The method of claim 27 wherein in an event that said consensus is not reached within a predefined amount of time, the method further comprises any one more of: instructing transmission of an alert notification; instructing transmission of a request for a second transaction.

29. The method of any one of the preceding claims wherein the method further comprises instructing transmission of a first address of the first device for receiving an amount of a cryptocurrency by way of said first transaction.

30. The method of claim 29 wherein the method further comprises determining an amount of the cryptocurrency assigned to the first address of the first device, wherein the predefined condition also requires that the assigned amount is consistent with a predetermined required amount.

31. The method of claim 29 or 30, wherein the method comprises instructing transmission of information for executing a second transaction, wherein the information for executing a second transaction comprises a second address of the first device for receiving an amount of a cryptocurrency by way of said second transaction.

32. The method of any one of claims 26 to 31, wherein the method comprises, before receiving said first data, instructing transmission a first public key of the first device to said second device, wherein the first public key of the first device corresponds to a first private key of the first device, and the method comprises instructing transmission of:

a second address of the first device for receiving an amount of a cryptocurrency by way of a second transaction; and

a second public key of the first device to be used for encryption in a record of the second transaction that is to be received onto the ledger.

33. The method according to any one of claims 29 to 32, wherein the method comprises receiving a first address of the second device for assigning thereto a second amount of a cryptocurrency by way of a return transaction onto the ledger.

34. The method according to any one of the preceding claims, wherein the method comprises, in an event the predefined condition is met, instructing transmission of an acknowledgement message via a communication channel.

35. The method according to any one of the preceding claims, wherein said data on which an operation of the first device is based is included the record of the first transaction.

36. The method according to any one of the preceding claims, wherein said data on which an operation of the first device based is included in the at least one message and the first data is encrypted using the first public key of the first device, wherein method preferably includes decrypting the first data using the first private key of the first device.

37. The method according to any one of the preceding claims wherein the method includes:

determining a time corresponding to the first transaction;

determining a time corresponding to the first data; and

wherein the predefined condition for using the first data further requires that a difference between the time of the receiving the first data and the time corresponding to the transaction is less than a predefined maximum time difference.

38. The method according to claim 37, wherein the time-stamp is signed by a first private key of the second device and encrypted with a public of the first device, and the method comprises verifying the signature of the timestamp using the first public key of the second device, the first public key of the second device corresponding to the first private key of the second device.

39. The method according to any one of the preceding claims, wherein the method further comprises:

receiving second data in the at least one message, the second data being included in a different message to the first data, wherein first data is encrypted; and

decrypting the first data; and

in an event that a second predefined condition is met, executing an operation of the first device based on said second data, the second predefined condition requiring at least that said validity is verified.

40. The method according to claim 39, wherein the method further comprises determining an amount of the cryptocurrency assigned to a first address of the first device, wherein the second predefined condition also requires that the assigned amount is consistent with a predetermined required amount.

41. The method according to claim 39 or 40, wherein the method includes:

determining a time corresponding to the first transaction;

determining a time corresponding to the second data; and

determining a difference between the time corresponding to the second data and the time corresponding to the transaction, wherein the predefined condition also requires that said difference is less than a predefined maximum time difference.

42. The method according to any one of the preceding claims, wherein the method includes:

receiving a record of a second transaction for the ledger, the record of the second transaction including a third validation tool;

receiving at least one message via a secure communication channel, from an authenticated device, the at least one message and including a second identifier for identifying the second transaction;

using the second identifier to read the record of the second transaction;

verifying validity of further data received in at least one of: the record of the second transaction and said at least one message that includes the second identifier, wherein the validity is verified based at least on the third validation tool and a fourth validation tool, and

in an event that a predefined condition is met, executing an operation of the first device based on said further data, the predefined condition requiring at least that said validity is verified based at least one of the third validation tool and the fourth validation tool.

43. The method according to claim 42 wherein, the validation tools are specific to each transaction.

44. The method according to any one of the preceding claims, wherein the method comprises receiving a trigger to wake up the first device from a power-saving mode, wherein upon receiving the trigger the first device enters an operating mode for communicating with the second device.

45. The method according to any one of the preceding claims, wherein the secure communication channel is with a third device, rather than the second device.

46. The method according to any one of the preceding claims, wherein the first device is a control panel of a monitoring system, wherein said device controls operation of one or more peripheral devices, and said operation of the first device is a communication with a peripheral device to instruct the peripheral device to interact with the environment.

47. A device for use as a first device in a peer-to-peer network, the device configured to:

receive a record of a first transaction for a ledger distributed amongst a plurality of nodes of a peer-to-peer network, the plurality of nodes including the first device, the record of the first transaction including a first validation tool;

receive at least one message, via a secure communication channel, from an authenticated second device, the at least one message including an identifier for identifying the first transaction;

use the identifier to read the record of the transaction;

verify validity of first data received in at least one of: the record of the first transaction and the at least one message, wherein the validity is verified using at least one of the first validation tool and a second validation tool, and

in an event that a predefined condition is met, execute an operation of the first device based on said first data, the predefined condition requiring at least that said validity is verified.

48. A device configured to perform the method of any one of claims 1 to 46.

49. A non-transient computer readable medium storing instructions for executing on a first device in a peer-to-peer network, wherein executing the instructions by the first device configures the first device to:

receive a record of a first transaction for a ledger distributed amongst a plurality of nodes of a peer-to-peer network, the plurality of nodes including the first device, the record of the first transaction including a first validation tool;

receive at least one message, via a secure communication channel, from an authenticated second device, the at least one message including an identifier for identifying the first transaction;

use the identifier to read the record of the transaction;

verify validity of first data received in at least one of: the record of the first transaction and the at least one message, wherein the validity is verified using at least one of the first validation tool and a second validation tool, and

in an event that a predefined condition is met, execute an operation of the first device based on said first data, the predefined condition requiring at least that said validity is verified.

50. A non-transient computer readable medium storing instructions for executing on a first device in a peer-to-peer network, wherein executing the instructions by the first device configures the first device to perform the method of any one of claims 1 to 46.

51. A method for facilitating guarding of a first device against a cyber threat, the method comprising, at a second device:

instructing transmission of an authentication tool to a receiving device for authenticating the second device;

executing a first transaction for a ledger distributed amongst a plurality of nodes of a peer-to-peer network, the plurality of nodes including the first device;

instructing transmission of at least one message, via a secure communication channel, to the receiving device;

instructing transmission of a record of the first transaction,

wherein the at least one message and the transaction are correlated so that the first device is able to determine verify, based on the at least one message and the transaction, validity of first data included in at least one of the at least one message and the record of the transaction, to execute an operation of the first device based on said first data.

52. The method according to claim 51, wherein the at least one message includes an identifier for identifying the first transaction to at least in part correlate the at least one message with the first transaction.

53. The method according to claim 51 or 52 wherein the record of the first transaction includes a first validation tool to at least in part correlate the at least one message with the first transaction based on a verification that uses the first validation tool in combination with a second validation tool received over the secure communication channel.

54. The method according to claim 52 or 53 wherein the correlation is, at least in part, based on a timing relationship between the at one message and the first transaction.

55. The method according to any one of claims 51 to 54, wherein the receiving device and the first device are the same device, the authentication tool is transmitted to the first device, and the secure communication channel used to transmit to the receiving device is therefore the same as the secure communication channel used to transmit to the first device.

56. The method according to any one of claims 51 to 55, wherein the receiving device is a different device to the first device and acts as a commander that determines the first data transmitted to the first device.

57. The method according to claim 56, wherein the receiving device, being the commander, uses secure communication with the first device to instruction transmission of the first data and, therewith, the identifier or a reference to the identifier.

58. The method according to any one of claims 51 to 57 wherein the method comprises:

receiving a first address of the first device and a first public key of the first device; and

instructing transmission of the second tool to the first device.

59. The method according to claim 58, wherein the first transaction comprises assigning an amount of a cryptocurrency to the first address of the first device, wherein one or more of the first tool and second tool have been encrypted using the first public key of the first device.

60. The method according to claim 58 or 59 wherein subsequent transactions use the first public key of the first device for the encryption.

61. The method according to claim 58 or 59 wherein a next transaction uses a second public key of the first device for the encryption.

62. The method of any one of claims 51 to 61 wherein the first public key is the first public key of the claim 32, wherein the first and second devices of the correspond to the first and second devices of claim 32.

63. The method of any one of claims 51 to 62, wherein executing the first transaction comprises preliminarily validating at least one other transaction, wherein preliminarily validating a transaction comprises determining that a From address in the record of the transaction has enough of a cryptocurrency to transfer an amount of the cryptocurrency specified by the transaction.

64. The method of any one of claims 51 to 63, wherein the method further comprises instructing transmission of a copy of the record of the first transaction, wherein the record of the copy of the first transaction identifies said at least one transaction preliminarily validated by the first transaction.

65. The method of any one of claims 51 to 64, wherein the method comprises including said first data in the record of the first transaction.

66. The method of any one of claims 51 to 64, wherein said first data is included in said at least one message transmitted to the first device.

67. The method of any one of claims 51 to 66, wherein the method further comprises, at the second device, including a time-stamp in the record of the first transaction, the timestamp being digitally signed by the second device.

68. The method of any one of claims 51 to 67, wherein the second device is configured, in the event of another predefined condition being satisfied, to execute a second transaction on the distributed ledger and instructing transmission of an identifier identifying the second transaction.

69. The method of claim 68 wherein satisfaction of the other predefined condition includes a requirement that a time elapsed since a reference time is less than a predefined maximum.

70. The method of claim 69 wherein the reference time is: a time corresponding to a time-stamp included in the record of the first transaction; a time of receiving an acknowledgment of a notification from the first device; or a time of day.

71. The method of claim 60 or 70 wherein the second device is configured to execute a second transaction in an event of any one of:

receiving a request from the first device to make a second transaction; or

not receiving a request from the first device to refrain from making a second transaction.

72. A second device for facilitating guarding of a first device against a cyber threat, the second device being configured to perform the method of any one of claims 51 to 71.

73. A non-transient computer readable medium storing instructions for executing on a second device in a peer-to-peer network to facilitate guarding of a first device against a cyber threat, wherein executing the instructions by the second device configures the second device to perform the method of any one of claims 51 to 71.

74. A method for a first device, the method comprising:

receiving at least one message, via a secure communication channel, from an authenticated second device, the at least one message including an identifier for identifying a first transaction, for a ledger distributed amongst a plurality of nodes of a peer-to-peer network, the plurality of nodes including the first device;

using the identifier to call for the record of the transaction from a copy of the ledger on the first device; and

in an event that the call for the record fails to return the record, instructing transmission of a request, to another device in the peer-to-peer network, for a copy of the record of transaction.

75. The method according to claim 74 wherein the request for a copy of the record of transaction comprises said identifier.

76. The method according to claim 75 wherein the identifier is a hash of the record of the transaction.

77. The method according to claim 76 wherein the record of the first transaction includes a first validation tool.

78. The method according to any one of claims 74 to 77 wherein the method further comprises:

receiving a copy of the record from the other device;

using the identifier to read the record of the transaction from the copy of the ledger on the first device;

verifying validity of first data received in at least one of: the record of the first transaction and the at least one message, wherein the validity is verified using at least one of the first validation tool and a second validation tool, and

in an event that a predefined condition is met, executing an operation of the first device based on said first data, the predefined condition requiring at least that said validity is verified.

79. A first device configured to perform the method of any one of claims 74 to 78.

80. A non-transient computer readable medium storing instructions for executing on a first device, wherein executing the instructions by the first device configures the first device to perform the method of any one of claims 74 to 78.

81. A system having a first device and second device, wherein the first device is a device according to claim 48 or 79, and the second device is a device according to claim 72.

82. A system according to claim 81 wherein the system includes the peer-to-peer network.

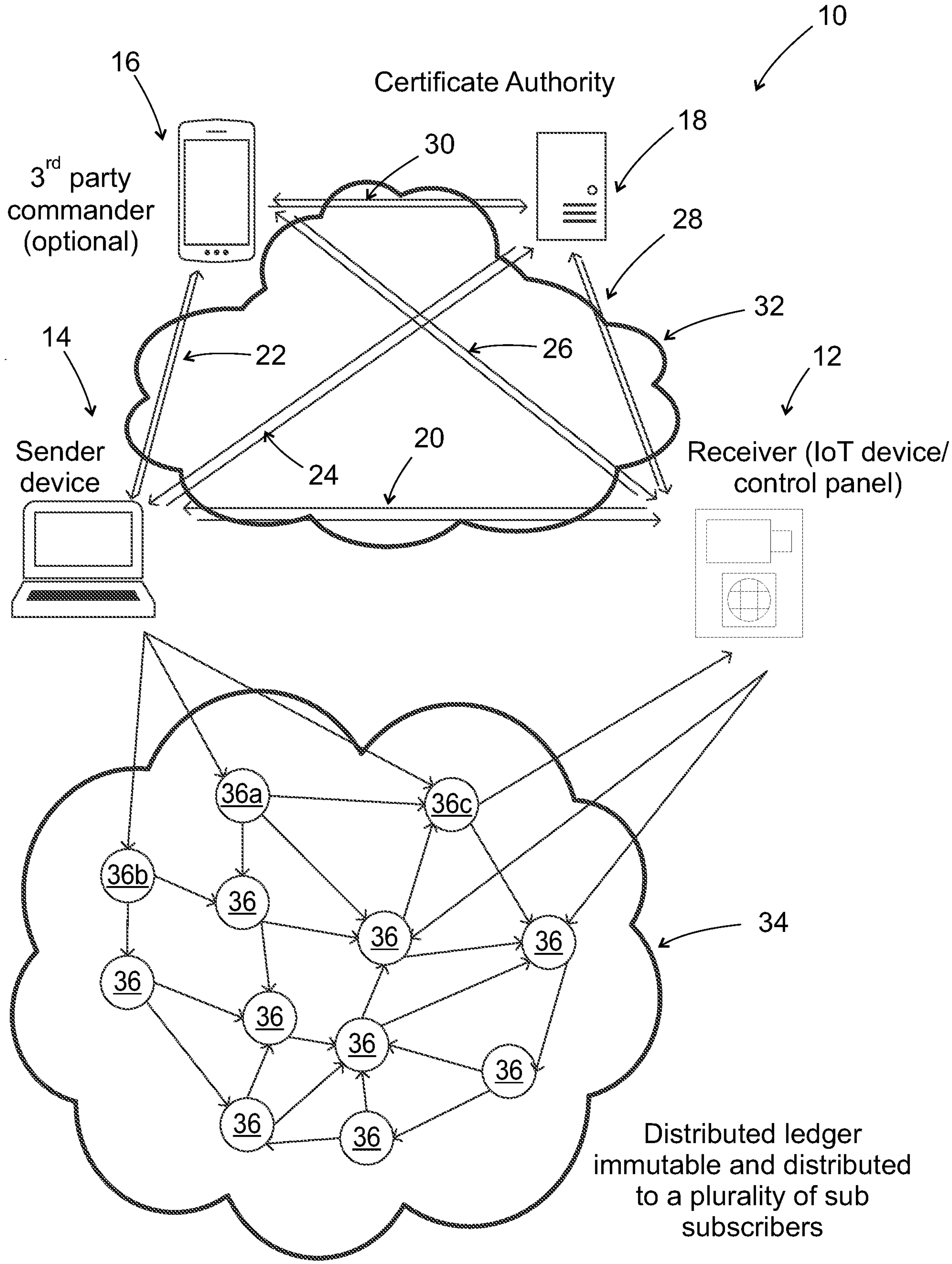
10
16
Certificate Authority
18
30
3rd party
commander
(optional)
28
32
14
22
26
12
20
Sender
device
24
Receiver (IoT device/
control panel)
36a
36c
36b
36
36
36
36
36
36
36
36
36
36
34
Distributed ledger
immutable and distributed
to a plurality of sub
subscribers

FIG. 1

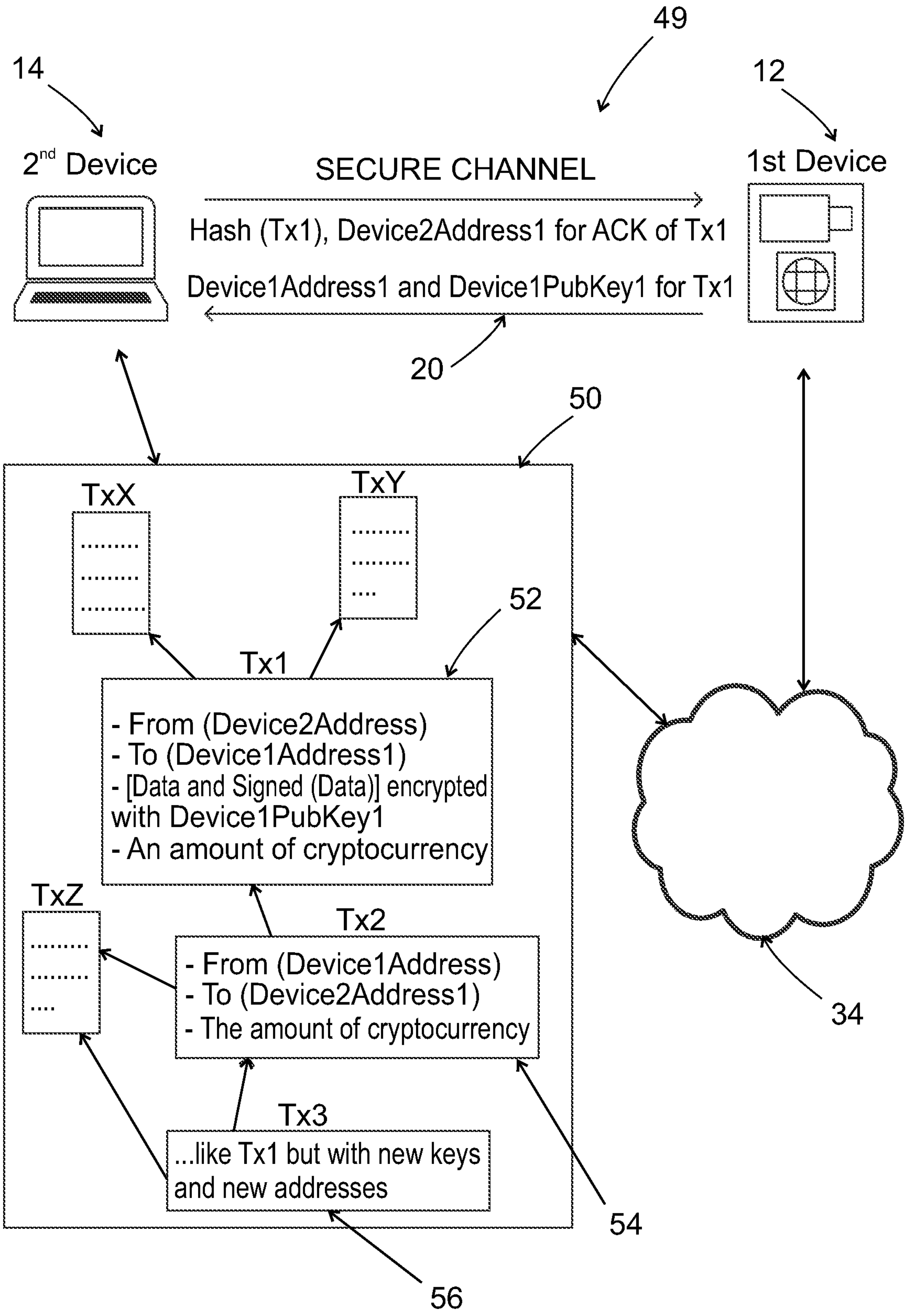
49
14
12
2nd Device
SECURE CHANNEL
1st Device
Hash (Tx1), Device2Address1 for ACK of Tx1
Device1Address1 and Device1PubKey1 for Tx1
20
50
TxX
TxY
52
Tx1
- From (Device2Address)
- To (Device1Address1)
- [Data and Signed (Data)] encrypted with Device1PubKey1
- An amount of cryptocurrency
TxZ
Tx2
- From (Device1Address)
- To (Device2Address1)
- The amount of cryptocurrency
Tx3
...like Tx1 but with new keys and new addresses
34
54
56

FIG. 2

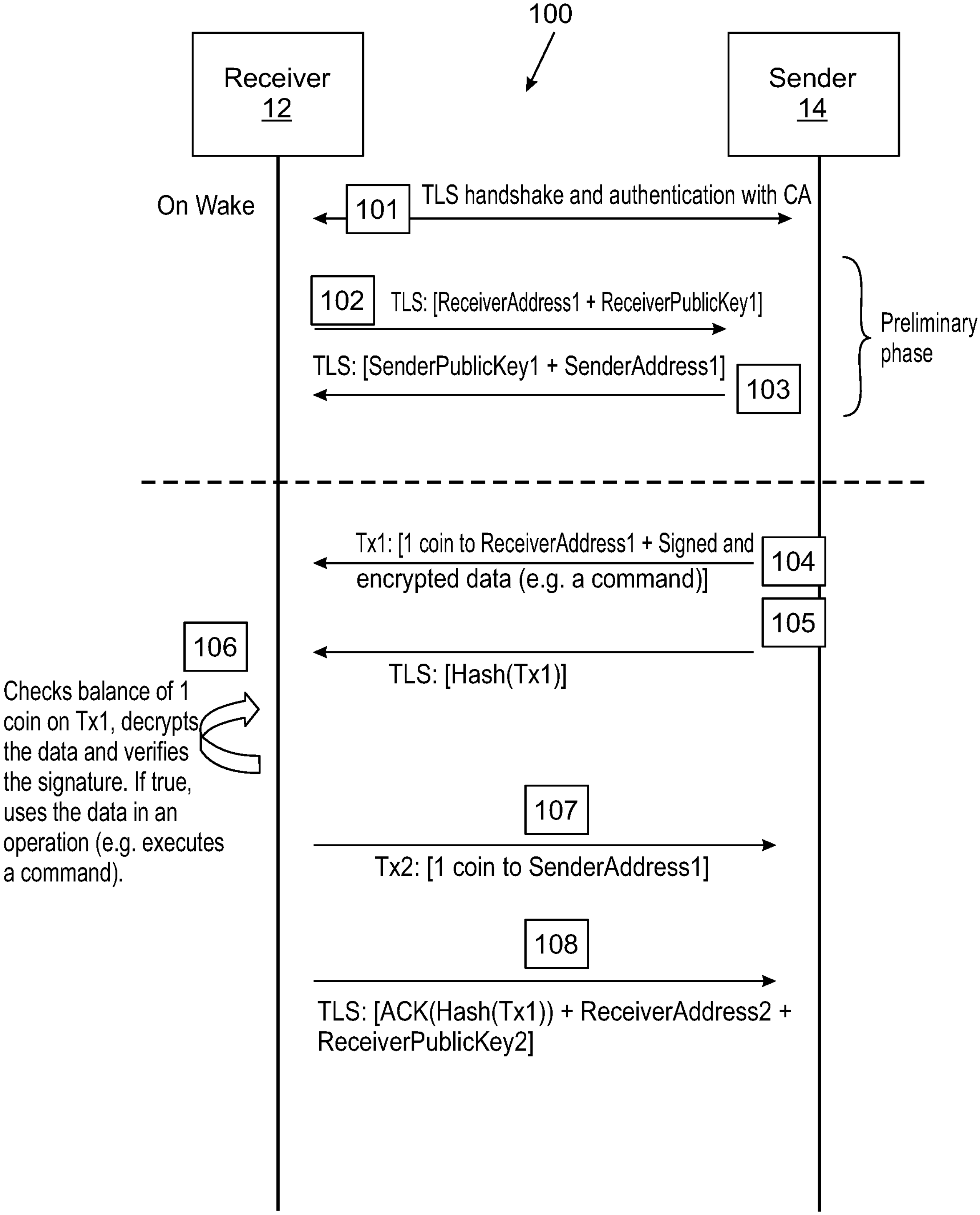
100
Receiver
12
Sender
14
On Wake
101
TLS handshake and authentication with CA
102
TLS: [ReceiverAddress1 + ReceiverPublicKey1]
TLS: [SenderPublicKey1 + SenderAddress1]
103
Preliminary phase
Tx1: [1 coin to ReceiverAddress1 + Signed and encrypted data (e.g. a command)]
104
105
106
TLS: [Hash(Tx1)]
Checks balance of 1 coin on Tx1, decrypts the data and verifies the signature. If true, uses the data in an operation (e.g. executes a command).
107
Tx2: [1 coin to SenderAddress1]
108
TLS: [ACK(Hash(Tx1)) + ReceiverAddress2 + ReceiverPublicKey2]

FIG. 3

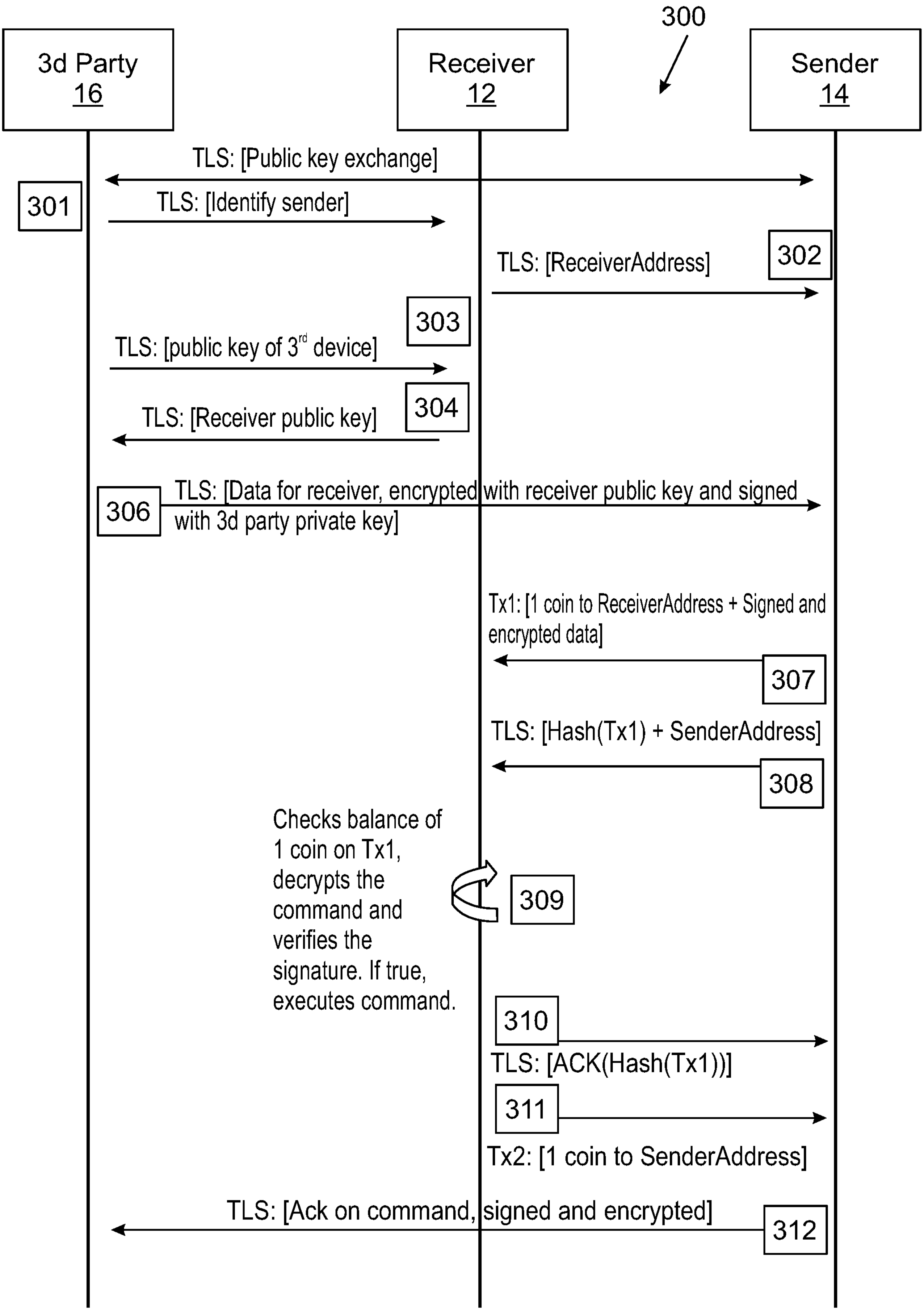
300
3d Party
16
Receiver
12
Sender
14
TLS: [Public key exchange]
301
TLS: [Identify sender]
TLS: [ReceiverAddress]
302
303
TLS: [public key of 3rd device]
304
TLS: [Receiver public key]
306
TLS: [Data for receiver, encrypted with receiver public key and signed with 3d party private key]
Tx1: [1 coin to ReceiverAddress + Signed and encrypted data]
307
TLS: [Hash(Tx1) + SenderAddress]
308
Checks balance of 1 coin on Tx1, decrypts the command and verifies the signature. If true, executes command.
309
310
TLS: [ACK(Hash(Tx1))]
311
Tx2: [1 coin to SenderAddress]
TLS: [Ack on command, signed and encrypted]
312

FIG. 4

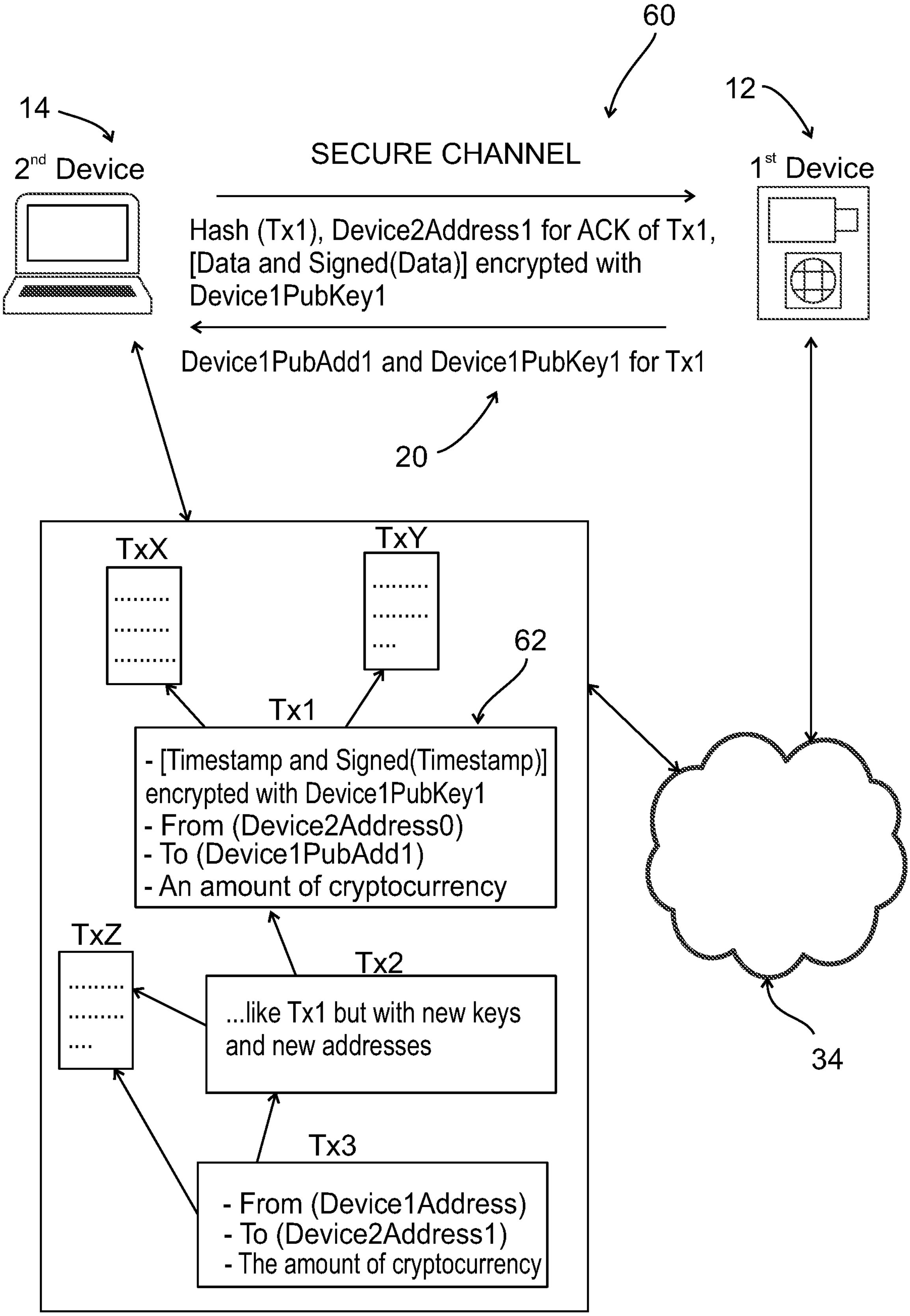
60
14
12
2nd Device
SECURE CHANNEL
1st Device
Hash (Tx1), Device2Address1 for ACK of Tx1, [Data and Signed(Data)] encrypted with Device1PubKey1
Device1PubAdd1 and Device1PubKey1 for Tx1
20
TxX
TxY
62
Tx1
- [Timestamp and Signed(Timestamp)] encrypted with Device1PubKey1
- From (Device2Address0)
- To (Device1PubAdd1)
- An amount of cryptocurrency
TxZ
Tx2
...like Tx1 but with new keys and new addresses
34
Tx3
- From (Device1Address)
- To (Device2Address1)
- The amount of cryptocurrency

FIG. 5

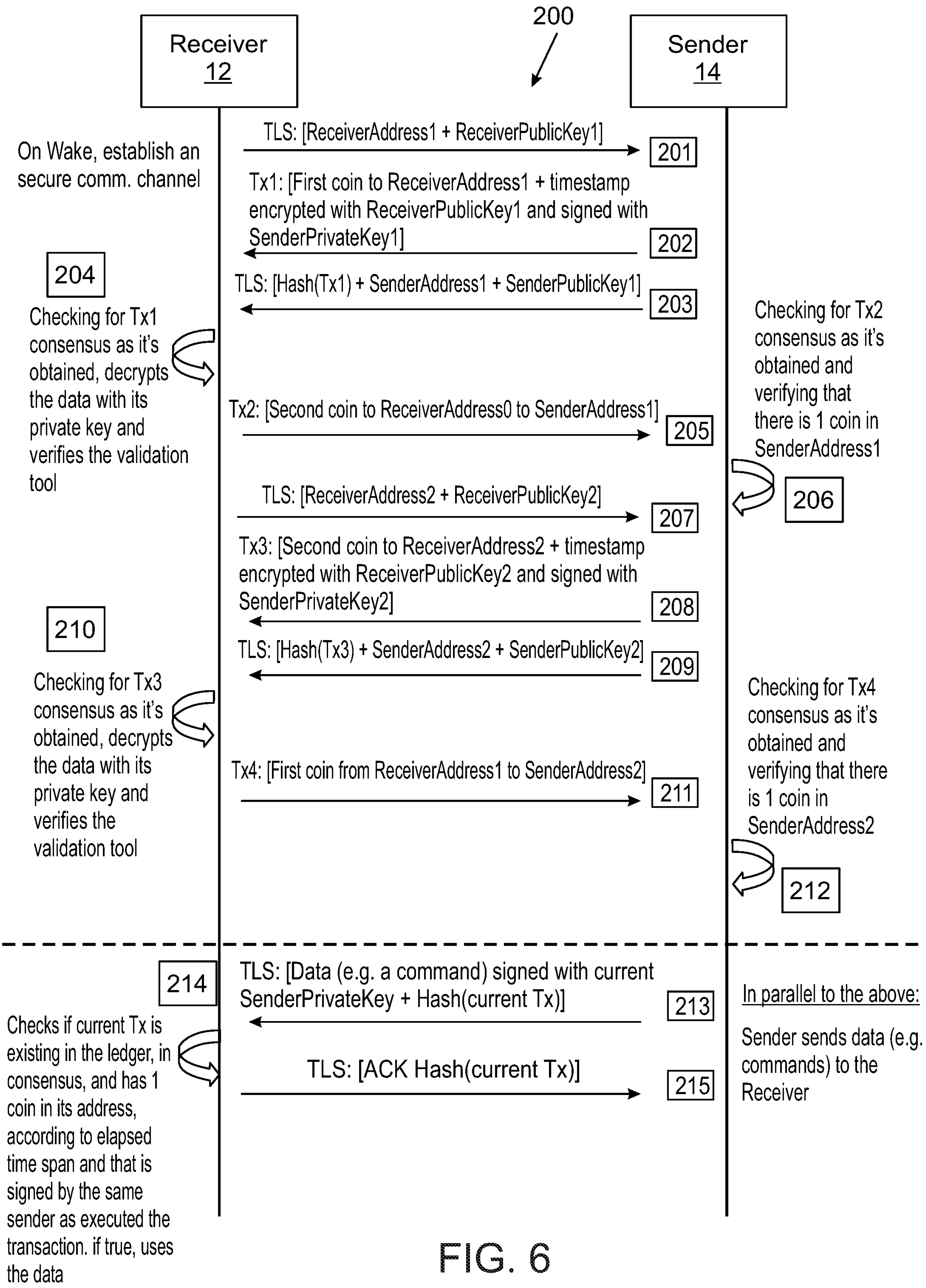
200
Receiver
12
Sender
14
On Wake, establish an secure comm. channel
TLS: [ReceiverAddress1 + ReceiverPublicKey1]
201
Tx1: [First coin to ReceiverAddress1 + timestamp encrypted with ReceiverPublicKey1 and signed with SenderPrivateKey1]
202
204
TLS: [Hash(Tx1) + SenderAddress1 + SenderPublicKey1]
203
Checking for Tx1 consensus as it's obtained, decrypts the data with its private key and verifies the validation tool
Checking for Tx2 consensus as it's obtained and verifying that there is 1 coin in SenderAddress1
Tx2: [Second coin to ReceiverAddress0 to SenderAddress1]
205
206
TLS: [ReceiverAddress2 + ReceiverPublicKey2]
207
Tx3: [Second coin to ReceiverAddress2 + timestamp encrypted with ReceiverPublicKey2 and signed with SenderPrivateKey2]
208
210
TLS: [Hash(Tx3) + SenderAddress2 + SenderPublicKey2]
209
Checking for Tx3 consensus as it's obtained, decrypts the data with its private key and verifies the validation tool
Checking for Tx4 consensus as it's obtained and verifying that there is 1 coin in SenderAddress2
Tx4: [First coin from ReceiverAddress1 to SenderAddress2]
211
212
214
TLS: [Data (e.g. a command) signed with current SenderPrivateKey + Hash(current Tx)]
213
In parallel to the above:
Sender sends data (e.g. commands) to the Receiver
Checks if current Tx is existing in the ledger, in consensus, and has 1 coin in its address, according to elapsed time span and that is signed by the same sender as executed the transaction. if true, uses the data
TLS: [ACK Hash(current Tx)]
215

FIG. 6

INTERNATIONAL SEARCH REPORT

International application No

PCT/I L2019/050586

A. CLASSIFICATION OF SUBJECT MATTER

INV. H04L29/06

ADD.

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)

H04L

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)

EPO-Internal , COMPENDEX, INSPEC, IBM-TDB, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2017/177898 A1 (DILLENBERGER DONNA N [US]) 22 June 2017 (2017-06-22) abstract paragraphs [0037] - [0045]; figures 3, 4 -----	1-82
A	LIANG XUEPING ET AL: "Towards data assurance and resilience in IoT using blockchain", MILCOM 2017 - 2017 IEEE MILITARY COMMUNICATIONS CONFERENCE (MILCOM), IEEE, 23 October 2017 (2017-10-23), pages 261-266, XP033265107, DOI: 10.1109/MILCOM.2017.8170858 [retrieved on 2017-12-07] * section I, third paragraph, section II.B and D, section III.B and C * ----- -/--	1-82

☒ 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

'E " earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) orwhich 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 2 July 2019	Date of mailing of the international search report 09/07/2019
Name and mailing address of the ISA/ European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Authorized officer Agudo Cortada, E

International application No

PCT/ I L20 19/050586

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	YUANYU ZHANG ET AL: "Smart Contract-Based Access Control for the Internet of Things", IEEE INTERNET OF THINGS JOURNAL, vol. 6, no. 2, 13 February 2018 (2018-02-13), pages 1594-1605, XP055591509, DOI: 10.1109/JIOT.2018.2847705 * sections II and III * -----	1-82
A	LUNARDI ROBEN CASTAGNA ET AL: "Distributed access control on IoT ledger-based architecture", NOMS 2018 - 2018 IEEE/IFIP NETWORK OPERATIONS AND MANAGEMENT SYMPOSIUM, IEEE, 23 April 2018 (2018-04-23), pages 1-7, XP033371605, DOI: 10.1109/NOMS.2018.8406154 [retrieved on 2018-07-06] * section III * -----	1-82

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/I L2019/050586

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2017177898 A1	22-06-2017	US 2017177898 A1	22-06-2017
		US 2018268162 A1	20-09-2018
