PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To: G.E. EHRLICH (1995) LTD.
11 MENACHEM BEGIN ROAD
5268104 RAMAT-GAN
ISRAEL

PCT

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing *(day/month/year)*	24 MAR 2020
Applicant's or agent's file reference 80249	**FOR FURTHER ACTION** See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/IL 19/51330	05 December 2019 (05.12.2019)	06 December 2018 (06.12.2018)

International Patent Classification (IPC) or both national classification and IPC

IPC - G06F 15/16 (2020.01)

CPC - H04L 29/08072, H04L 29/06, H04L 29/08135, H04L 29/08144, H04L 29/0809, H04L 29/08648, H04L 29/08981, H04L 9/08, H04L 63/0428, H04L 63/0442, H04L 9/00, H04N 7/1675

Applicant
GK8 LTD.

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step and industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☐ Box No. VII Certain defects in the international application
- ☐ Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1*bis*(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

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

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/IL 19/51330

Box No. I Basis of this opinion

1. With regard to the **language**, this opinion has been established on the basis of:

   ☒ the international application in the language in which it was filed.

   ☐ a translation of the international application into _____ which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43*bis*.1(b)).

3. ☐ With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of a sequence listing:

   a. ☐ forming part of the international application as filed:

      ☐ in the form of an Annex C/ST.25 text file.

      ☐ on paper or in the form of an image file.

   b. ☐ furnished together with the international application under PCT Rule 13*ter*.1(a) for the purposes of international search only in the form of an Annex C/ST.25 text file.

   c. ☐ furnished subsequent to the international filing date for the purposes of international search only:

      ☐ in the form of an Annex C/ST.25 text file (Rule 13*ter*.1(a)).

      ☐ on paper or in the form of an image file (Rule 13*ter*.1(b) and Administrative Instructions, Section 713).

4. ☐ In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that forming part of the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

5. Additional comments:

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/IL 19/51330

Box No. V **Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step and industrial applicability; citations and explanations supporting such statement**

1. Statement

Novelty (N)	Claims	NONE	YES
	Claims	1-41	NO
Inventive step (IS)	Claims	NONE	YES
	Claims	1-41	NO
Industrial applicability (IA)	Claims	1-41	YES
	Claims	NONE	NO

2. Citations and explanations:
Claims 1-41 lack novelty under PCT Article 33(2) as being anticipated by US 2017/0232300 A1 to Tran et al. (hereinafter "Tran").

Regarding claim 1, Tran discloses a method of validating a multi-party consensus over a limited connection (Verification of a transaction is based on mutual consensus among the nodes, para [0204]), comprising: using at least one processor of a validating device for: transmitting a query to a plurality of computing nodes via a unidirectional secure communication channel, the query having a finite number of possible valid answers (A website may be utilized to provide an interface with which a retailer and/or consumer may view the validation data obtained from the geolocation information, time reference data, or additional data as described above, para [0240]); receiving a limited length string computed based on an aggregated response aggregating a plurality of responses each computed for a multi-party consensus answer to the query by each of at least some of the plurality of computing nodes using a respective one of a plurality of secret components (In another embodiment, the data may be extracted from the database to be transformed, aggregated, and combined into standardized thin file records for each borrower, para [0885]); computing a plurality of locally computed strings each computed based on a respective one of the finite number of possible valid answers using an aggregated secret aggregating the plurality of secret components (The data queries and their associated information are crafted by the care provider and modified when new records are added. To enable patients to share records with others, a dictionary implementation (hash table) maps viewers' addresses to a list of additional query strings, para [0275]); validating the multi-party consensus answer by comparing the received limited length string to each of the plurality of locally computed strings (In FIG. 1A, the monitoring device used for a sport device 9 includes an interface with a radio transmitter for forwarding the result of the comparison to a remote device, para [0018], Fig. 1A); and initiating at least one operation according to an outcome of the validation (The characteristics may be specified by the user, or lender, that initiates a search for an exchange partner or by the lending system 108, para [0922], Fig. 2).

Regarding claim 2, Tran discloses wherein the at least one operation comprising outputting the outcome of the validation (The captured field of view image may be used to estimate a head pose of the user. The captured field-of-view image may be used to convert at least one physical object to a physically rendered virtual object, and to display the physically rendered virtual object to the user, para [1013]).

Regarding claim 3, Tran discloses wherein the validating device applies the validation of the multi-party consensus answer for checking blockchain transactions information relating to the validating device (Blockchain token ownership is immediately transferred to a new owner after authentication and verification, which are based on network ledgers within a peer-to-peer network, guaranteeing nearly instantaneous execution and settlement, para [0119]).

Regarding claim 4, Tran discloses wherein the validating device is a crypto-currency wallet and the validation of the multi-party consensus response is applied for checking a balance of the cryptocurrency wallet (Furthermore, every account has a balance in Ether (such as in "Wei") which can be modified by sending transactions that include Ether, para [0137]).

Regarding claim 5, Tran discloses wherein the at least one operation comprising transmitting at least one cryptocurrency transaction based on the multi-party consensus answer after validated (Typically, the shared transaction ledger (140) includes all these transactions as a chain of transaction records or receipts, commonly referred to as a "block chain" in at least one known cryptocurrency system, para [0148], Fig. 13E).

Regarding claim 6, Tran discloses wherein the unidirectional secure communication channel is physically tamper resistant thus supporting reliable and secure one-way communication from the validating device to each of the plurality of computing nodes (The microcontroller 155 wirelessly transmits tension information in the appropriate digital electronic format, which may be encoded or encrypted for secure communications, corresponding to the sensed traffic and/or crime indication through a wireless communication module or transceiver 160 and antenna 170, para [0049], Fig. 2A).

Regarding claim 7, Tran discloses wherein the validating device communicates with the plurality of computing nodes via at least one access node of the plurality of computing nodes which broadcasts messages received from the validating device to the plurality of computing nodes (A coordinator of the two-phase commitment is, in some embodiments, a trusted node, for example a node that both traders mutually agree to have act as coordinator (including each other), para [0201]).

---(continued in the Supplemental Boxes)---

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/IL 19/51330

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**
Continuation of:
Box V, item 2. Citations and explanations:

Regarding claim 8, Tran discloses wherein the secure unidirectional communication channel established with at least one of the plurality of computing nodes is secured by encrypting communication transmitted from the validating device to the at least one computing node using an encryption key of a respective encryption-decryption key pair uniquely associated with the at least one computing node, the respective encryption key is provided to the validating device as a respective limited length string (Each system user has an account that is associated with a unique number, for example, an Ed25519 public-key ("pubkey") pair, or other appropriate pubkey system, which allows the user to sign Issue and Transfer Records, para [0317]).

Regarding claim 9, Tran discloses the secure unidirectional communication channel established with at least one of the plurality of computing nodes is secured by encrypting communication transmitted from the validating device to the at least one computing node using an encryption key of an encryption-decryption key pair uniquely associated with the at least one computing node, the encryption key is provided to the validating device by at least one trusted controller adapted to distribute to the at least one computing node a decryption key of the encryption-decryption key pair uniquely associated with the at least one computing node, the encryption-decryption key pair is produced deterministically using a pseudorandom number generator initialized with a random seed shared in advance with the validating device, using the shared random seed the validating device generates the encryption key of the encryption-decryption key pair and uses it to establish the encrypt communication transmitted to the at least one computing node (Energy seller can first generate a private/public key pair before Energy buyer can create the first transaction. Bitcoin uses the Elliptic Curve Digital Signature Algorithm (ECDSA) with the secp256kl curve; secp256kl private keys are 256 bits of random data, para [0719]).

Regarding claim 10, Tran discloses wherein the at least one trusted controller is further adapted to periodically distribute a new encryption-decryption key pair to the at least one computing node every predefined period of time, the new encryption-decryption key is produced deterministically using the pseudorandom number generator initialized with the random seed shared with the validating device and a time identifier assigned to the new encryption-decryption key (External accounts that are controlled by public-private key pairs (i.e. humans) and contract accounts which are controlled by the code stored together with the account, para [0137]).

Regarding claim 11, Tran discloses wherein the at least one trusted controller is further adapted to distribute a respective encryption-decryption key pair to each of multiple computing nodes, the respective encryption-decryption key pair is produced deterministically using the pseudorandom number generator initialized with the random seed shared with the validating device and an index of the respective computing node (FIG. 13D shows another exemplary process executed by the smart contract system. In (20) Buyer requests to obtain the service or item from the service or item provider. In (24) Item provider utilizes the blockchain system described above and generates a cryptographic key pair and in (26) the service or item provider embeds the key data in the service or item, para [0145], Fig. 13D).

Regarding claim 12, Tran discloses wherein the at least one trusted controller communicates with the at least one computing node via a unidirectional secure communication channel similar to the unidirectional secure communication channel of the validating device (Moreover, a posture graph is used to depict the inter-relationships among all the model-states, defined as PG (ND, LK), where ND is a finite set of nodes and LK is a set of directional connections between every two nodes. The directional connection links are called posture links. Each node represents one model-state, and each link indicates a transition between two model-states. In the posture graph, each node may have posture links pointing to itself or the other nodes, para [1040]).

Regarding claim 13, Tran discloses the validating device signs the query transmitted to the plurality of computing nodes using a signing key (When an Blockchain token is first created (i.e., by an issuer) there are no previous owners from which to verify ownership in the ledgers. In one or more embodiments, the issuer can maintain the same private key for digitally signing each Blockchain token as it is issued and entered into in the ledgers, para [0203]).

Regarding claim 14, Tran discloses transmitting a plurality of queries simultaneously to the plurality of computing nodes such that a later query is transmitted before receiving response to an earlier transmitted query (The data queries and their associated information are crafted by the care provider and modified when new records are added, para [0275]).

Regarding claim 15, Tran discloses transmitting the query coupled with a unique identifier which is used by the at least some computing nodes to compute the plurality of responses is used by the validating device to verify that the limited length string corresponds to the query (In some embodiments, the unique identifier used for a physical asset may be a physical unclonable function, para [0317]).

Regarding claim 16, Tran discloses the unique identifier is a time stamp of the transmission of the query (Evidence of creatorship provided by blockchain can be done: if an original design document and details of the designer are uploaded to a blockchain, this creates a time-stamped record and good evidence to prove these matters, para [0324]).

Regarding claim 17, Tran discloses at least one of the plurality of computing nodes communicates with at least another one of the plurality of computing nodes to support computation of a respective one of the plurality of responses (The computing device 600 may represent any of the member device 104 or 116 shown in architecture 100, para [0910], Fig. 14H).

Regarding claim 18, Tran discloses wherein the plurality of secret components are transmitted by the validating device to the plurality of computing nodes (The computing device 600 may represent any of the member device 104 or 116 shown in architecture 100, para [0910], Fig. 14H).

Regarding claim 19, Tran discloses the validating device transmits the plurality of secret components to the plurality of computing nodes once during an initialization sequence (Next, in step 342, a timer is initialized to track the time taken to review the document displayed in step 341, para [0709], Fig. 14B).

---(continued on the next page)---

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/IL 19/51330

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**
Continuation of:
Box V, item 2. Citations and explanations:

Regarding claim 20, Tran discloses the validating device signs the plurality of secret components transmitted to the plurality of computing nodes using a signing key (When an Blockchain token is first created (i.e., by an issuer) there are no previous owners from which to verify ownership in the ledgers. In one or more embodiments, the issuer can maintain the same private key for digitally signing each Blockchain token as it is issued and entered into in the ledgers, para [0203]).

Regarding claim 21, Tran discloses wherein the validating device transmits the respective secret component to each of the computing nodes with the query (The computing device 600 may represent any of the member device 104 or 116 shown in architecture 100, para [0910], Fig. 14H).

Regarding claim 22, Tran discloses wherein the limited length string is provided to the validating device using at least one access computing node of the plurality which computes the limited length string based on the aggregated response (Pubkey hashes are almost always sent encoded as Bitcoin addresses, which are base58-encoded strings containing an address version number, the hash, and an error-detection checksum to catch typos, para [0720]).

Regarding claim 23, Tran discloses wherein the limited length string is received via a secure Human Machine Interface (HMI) operated by a user to input the limited length string (For example, the first, second, and third smart devices 240, 250, 260 may send information regarding human interactions with the first, second, and third smart devices 240, 250, 260, para [0061], Fig. 2A).

Regarding claim 24, Tran discloses increasing a length of the limited length string requested for computing the aggregated response received in response to at least one subsequent query in case the received multi-party consensus answer is invalid (A stock ID, in some embodiments, is determined (and invalidated) by an issuer, para [0197]).

Regarding claim 25, Tran discloses applying a two-stage query for a complex query having an extremely large number of possible valid answers as follows: in a first stage of the two-stage query, the validating device transmits the complex query to the plurality of computing nodes and receives in response a first limited length string computed based on a first multi-party answer computed by at least one of the at least some computing nodes for the multi-party consensus answer to the complex query using the respective secret component, wherein the validating device uses the aggregated secret to extract the first multi-party answer, and in a second stage of the two-stage query, the validating device transmits a second query requesting the at least some computing nodes to confirm the first multi-party answer received for the complex query, the second query having two possible valid answers, namely correct and incorrect (For SQL data queries, a provider references the patient's data with a SELECT query on the patient's address. For patients uses an interface that allows them to check off fields they wish to share through a graphical interface, para [0275]).

Regarding claim 26, Tran discloses wherein the plurality of secret components is a plurality of symmetric hash functions, each of the plurality of computing nodes uses a respective one of the plurality of symmetric hash functions to compute a respective one of a plurality of hash values based on the multi-party consensus answer to the query, the limited length string is an aggregated hash value computed by aggregating the plurality of hash values computed by the plurality of computing nodes, the validation is done by comparing the limited length string to each of a set of locally generated limited length strings each generated for a respective one of the finite number of possible valid answers using aggregation of the plurality of symmetric hash functions (The data encoded in the circuit can be cryptographically protected. For example, the data can be encrypted using a symmetric or asymmetric key using any suitable cryptographic protocol known in the art, para [0218]).

Regarding claim 27, Tran discloses publishing a plurality of hash values locally computed by the validating device for each of the finite number of possible valid answers in case, based on analysis of the received limited length string, the validating device determines that the multi-party consensus answer is invalid, each of the plurality of locally computed hash values is computed using a respective one of the plurality of symmetric hash functions, at least one of the plurality of computing nodes identifies at least one malicious computing node of the plurality of computing nodes by detecting incompliance between at least one hash value computed by at least one malicious computing node and a respective one of the plurality of locally computed hash values (The accepting or rejecting relationships is done only by the patients. To avoid notification spamming from malicious participants, only trusted providers can update the status variable. Other contract terms or rules can specify additional verifications to confirm proper actor behavior, para [0278]).

Regarding claim 28, Tran discloses using a plurality of deterministic signing functions instead of the plurality of symmetric hash functions, each of the plurality of deterministic signing functions has a respective one of a plurality of signing-verifying key pairs, each of the plurality of computing nodes applies a respective one of the plurality of deterministic signing functions to sign a respective one of the plurality of responses using a signing key of the respective signing-verifying key pair (In one or more embodiments, the issuer can maintain the same private key for digitally signing each Blockchain token as it is issued and entered into in the ledgers, para [0203]).

Regarding claim 29, Tran discloses at least one computing node having the verifying key of at least some of the plurality of signing-verifying key pairs determines, prior to computing the aggregated hash value, that at least one malicious computing node is present among the plurality of computing nodes in case of detection that at least one of the plurality of responses is incompliant with a majority of the plurality of responses, the at least one malicious computing node is identified according to the verifying key corresponding to the signing key used to sign the at least one incompliant response (The accepting or rejecting relationships is done only by the patients. To avoid notification spamming from malicious participants, only trusted providers can update the status variable. Other contract terms or rules can specify additional verifications to confirm proper actor behavior, para [0278]).

---(continued on the next page)---

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/IL 19/51330

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**
Continuation of:
Box V, item 2. Citations and explanations:

Regarding claim 30, Tran discloses wherein the plurality of secret components are a plurality of partial secret components created from a secret value generated for each of the finite number of possible valid answers using at least one secret sharing algorithm, the validating device generates a respective one of a plurality of random strings each generated for the respective possible valid answer and splits each of the plurality of random strings to a respective set of partial strings using the at least one secret sharing algorithm applied according to at least one configuration parameter, the query transmitted to each of the plurality of computing nodes comprises a respective partial string of each set of partial values, each of the at least some computing nodes transmits its respective partial string corresponding to the multi-party consensus answer, the limited length string is a hash value computed based on the aggregated response aggregating the partial strings received from a sufficient number of the plurality of computing nodes, the sufficient number is defined by the at least one configuration parameter, the validation is done by comparing the limited length string to each of a set of locally generated limited length strings each generated for a respective one of the finite number of possible valid answers using the secret value (The mathematical condition, as an example, might be that the hash contains a certain number of leading zeros and a hashing algorithm that requires more steps to find a hash containing a greater number of leading zeros, and fewer steps to find a hash containing a lesser number of leading zeros, para [0310]).

Regarding claim 31, Tran discloses publishing a plurality of commitment values to support detection of at least one malicious computing node of the sufficient number of computing nodes prior to providing the limited length string to the validating device, each of the plurality of commitment values is computed for a respective partial string of each set of partial strings using at least one commitment function, in addition to its respective partial string each of the plurality of sufficient number of computing nodes publishes a respective proof of commitment computed for its respective partial string using the at least one commitment function, at least one of the plurality of computing nodes uses a respective one of the plurality of commitment values published by the validating device in conjunction with the proof of commitment received from each of the sufficient number of computing nodes to verify each received partial string is compliant with the respective response received from the respective computing node of the sufficient number of computing nodes, in case at least one of the received partial strings is incompliant, the at least one computing node identifies the at least one malicious computing node which transmitted the at least one incompliant partial string (Energy seller provides the pubkey hash to Energy buyer. Pubkey hashes are almost always sent encoded as Bitcoin addresses, which are base58-encoded strings containing an address version number, the hash, and an error-detection checksum to catch typos, para [0720]).

Regarding claim 32, Tran discloses the at least one malicious computing node is discarded from the sufficient number of computing nodes and replaced with another computing node currently not part of the sufficient number of computing nodes (Each node represents one model-state, and each link indicates a transition between two model-states. In the posture graph, each node may have posture links pointing to itself or the other nodes, para [1040]).

Regarding claim 33, Tran discloses splitting the query to a plurality of sub-queries each corresponding to a respective one of a plurality of portions which aggregated together map each of the finite number of possible valid answers, for each of the plurality of portions a respective set of partial secret components is created from a secret value generated for each possible valid answers to the respective portion using at least one secret sharing algorithm, the validating device generates a respective one of a plurality of random strings each possible valid answer of each portion and splits each of the plurality of random strings to a respective set of partial strings using the at least one secret sharing algorithm applied according to at least one configuration parameter, each of the sub-queries transmitted to each of the plurality of computing nodes comprises a respective partial string of each set of partial values generated for the respective sub-query, each of the at least some computing nodes transmits its respective partial string corresponding to the multi-party consensus answer for the respective portion, the limited length string is a hash value computed based on a concatenation of the aggregated responses for each of the sub-queries aggregating the partial strings received from a sufficient number of the plurality of computing nodes (The blockchain address and public key may thus comprise different values or strings of characters that are uniquely associated with each other such that the private key remains unambiguously linked to the blockchain address, para [0187]).

Regarding claim 34, Tran discloses transmitting at least some of the plurality of subqueries simultaneously to the plurality of computing nodes such that a later sub-query is transmitted before receiving response to an earlier transmitted sub-query (The data queries and their associated information are crafted by the care provider and modified when new records are added, para [0275]).

Regarding claim 35, Tran discloses wherein the plurality of secret components are a plurality of decryption key components created by splitting a decryption key of an encryption- decryption key pair using at least one threshold decryption algorithm applied according to at least one configuration parameter, the query transmitted to the plurality of computing nodes comprises the query and a plurality of encrypt values encrypting a plurality of random strings each generated by the validation device for a respective one of the finite number of possible valid answers, the plurality of encrypt values are produced by encrypting the plurality of random strings using an encryption key of the encryption-decryption key pair, a sufficient number of the plurality of computing nodes engage in a Multi-Party Computation (MPC) and use their respective decryption key components to decrypt an encrypt value of the plurality of encrypt values corresponding to a certain one of the finite number of possible valid answers as expressed in the multi-party consensus answer, the limited length string is a hash value computed for the decrypted encrypt value, the sufficient number is defined by the at least one configuration parameter, the validation is done by comparing the limited length string to each of a set of locally generated limited length strings each generated for a respective one of the random strings generated for the finite number of possible valid answers (The private key is used to decrypt cipher text, to create a digital signature, and to secure Blockchain tokens, para [0202]).

---(continued on the next page)---

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/IL 19/51330

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**
Continuation of:
Box V, item 2. Citations and explanations:

Regarding claim 36, Tran discloses publishing the encryption key and the plurality of decryption key components to identify at least one malicious computing node of the sufficient number of computing nodes in case the at least one malicious computing node engaged in MPC in an improper manner, the at least one malicious computing node is identified according to its respective decryption key component (So each relying party can determine if the claim issuer is one they can trust. A community of relying parties (e.g., banks, insurance companies, universities, government agencies) can define a trust framework that will define the rules for verifying a claim or credential to a certain level of assurance (LOA), and then issuers operating under that trust framework can indicate the LOA that applies when they write a claim to the ledger, para [0273]).

Regarding claim 37, Tran discloses the at least one malicious computing node is discarded from the sufficient number of computing nodes and replaced with another computing node currently not part of the sufficient number of computing nodes (Each node represents one model-state, and each link indicates a transition between two model-states. In the posture graph, each node may have posture links pointing to itself or the other nodes, para [1040]).

Regarding claim 38, Tran discloses wherein the plurality of secret components are a plurality of signing key components created from a signing key of a signing-verifying key pair split using at least one threshold signature algorithm applied according to at least one configuration parameter, the at least one threshold signature algorithm is characterized by producing a deterministic output for a given input, the query transmitted to the plurality of computing nodes comprises the query and a plurality of strings each corresponding to a respective one of the finite number of possible valid answers, a sufficient number of computing nodes of the plurality of computing nodes engage in a Multi-Party Computation (MPC) and use their respective signing key components to produce a deterministic signature for one of the plurality of strings corresponding to an agreed one of the finite number of possible valid answers as expressed in the multi-party consensus answer, the limited length string is a hash value computed for the deterministic signature, the sufficient number is defined by the at least one configuration parameter, the validation is done by comparing the limited length string to each of a set of locally computed limited length strings each computed for respective deterministic signature generated for a respective one of the plurality of strings using the signing key (The mathematical condition, as an example, might be that the hash contains a certain number of leading zeros and a hashing algorithm that requires more steps to find a hash containing a greater number of leading zeros, and fewer steps to find a hash containing a lesser number of leading zeros, para [0310]).

Regarding claim 39, Tran discloses at least one of the sufficient number of computing nodes identifies at least one malicious computing node of the sufficient number of computing nodes in case the at least one malicious computing node engaged in MPC in an improper manner, identification of the at least one malicious computing node is inherent to the at least one threshold signature algorithm (Duress: Elements include one party (D) with improper threat and one party (P) with no reasonable alternative (in a vulnerable situation), and the 2 parties entered into an agreement, para [0456]).

Regarding claim 40, Tran discloses the at least one malicious computing node is discarded from the sufficient number of computing nodes and replaced with another computing node currently not part of the sufficient number of computing nodes (Each node represents one model-state, and each link indicates a transition between two model-states. In the posture graph, each node may have posture links pointing to itself or the other nodes, para [1040]).

Regarding claim 41, Tran discloses an apparatus for validating a multi-party consensus over a limited connection (Verification of a transaction is based on mutual consensus among the nodes, para [0204]), comprising: a first interface, adapted to transmit messages to a plurality of computing nodes over a unidirectional secure communication channel; a second interface adapted to receive limited length strings; and at least one processor coupled to the first and second interfaces, the at least one processor is adapted to execute a code, the code comprising: code instructions to transmit a query to the plurality of computing nodes, the query having a finite number of possible valid answers (A website may be utilized to provide an interface with which a retailer and/or consumer may view the validation data obtained from the geolocation information, time reference data, or additional data as described above, para [0240]), code instructions to receive a limited length string computed based on an aggregated response aggregating a plurality of responses each computed for a multi-party consensus answer to the query by each of at least some of the plurality of computing nodes using a respective one of a plurality of secret components (In another embodiment, the data may be extracted from the database to be transformed, aggregated, and combined into standardized thin file records for each borrower, para [0885]), code instructions to compute a plurality of locally computed strings each computed based on a respective one of the finite number of possible valid answers using an aggregated secret aggregating the plurality of secret components, code instructions to validate the multi-party consensus answer by comparing the received limited length string to each of the plurality of locally computed strings (In FIG. 1A, the monitoring device used for a sport device 9 includes an interface with a radio transmitter for forwarding the result of the comparison to a remote device, para [0018], Fig. 1A), and code instructions to initiate at least one operation according to an outcome of the validation (The characteristics may be specified by the user, or lender, that initiates a search for an exchange partner or by the lending system 108, para [0922], Fig. 2).

Claims 1-41 have industrial applicability as defined by PCT Article 33(4), because the subject matter can be made or used in industry.