Decision on Opposition

Opposition No. 2018-700665

Patentee	MUFG Bank, Ltd.
Patent Attorney	Takahashi Hayashi and Partner Patent Attorneys
Opponent	SHINOMORI, Shigeki

The case of opposition to the grant of a patent in Japanese Patent No. 6341491, entitled "SIGNAL PROCESSING METHOD AND SIGNAL PROCESSING PROGRAM", has resulted in the following decision.

Conclusion

The correction of the scope of claims of Japanese Patent No. 6341491 shall be approved as described in the corrected scope of claims attached to the written demand for correction, regarding Claims [1-4] and [5-8] after the correction.

The patent according to Claims 1, 2, 5 and 6 of Japanese Patent No. 6341491 is maintained.

The opposition to the grant of a patent regarding the patent according to Claims 3-4, 7-8 of Japanese Patent No. 6341491 shall be dismissed.

Reason

No. 1 History of the procedures

The application regarding the patent according to Claims 1 to 8 of Japanese Patent No. 6341491 was filed on February 21, 2017, the establishment of patent right was registered on May 25, 2018, and the gazette containing the patent was issued on June 13, 2018. Thereafter, an opposition to the granted patent was filed on August 9, 2018 by the opponent, Shigeki SHINOMORI. The body issued a notice of reasons for revocation dated on February 15, 2019. The patentee submitted a written opinion and a written demand for correction on April 22, 2019 in a designated period. A directive of amendment was made on the written demand for correction on May 8, 2019. A written amendment on the written demand for correction was submitted on May 29, 2019. The opponent, Shigeki SHINOMORI, submitted a written opinion against the demand for correction on August 16, 2019.

No. 2 Judgment on Propriety of Correction

1 Contents of correction

The contents of the correction by the present demand for correction are as described in the following (1) A to G and (2) A to G. (Corrected portions are underlined. The same applies hereinafter in this section.)

(1) Correction on a group of Claims 1 to 4

A Correction A

The term "multiple nodes" according to Claim 1 is corrected to "multiple communication terminals". The description before the correction, "a group composed of multiple nodes", is corrected to the description, "a group composed of communication terminals connected to each other over a network". The description before the correction, "receiving an approval signal from nodes corresponding to a certain ratio of the multiple nodes having received the approval request signal", is corrected to the description, "receiving an approval signal from communication terminals corresponding to a certain ratio of the multiple communication terminals having received the approval request signal".

B Correction B

Regarding the destination of the "approval request signal" according to Claim 1, the description before the correction, "transmitting an approval request signal for execution of a transaction to at least one of the multiple nodes", is corrected to the description, "transmitting an approval request signal for execution of a transaction to at least one of the multiple communication terminals".

C Correction C

Regarding the "procedure of executing the transaction" according to Claim 1, the description before the correction, "based on approval of the received approval signal", is corrected to the description, "after receiving the approval signal".

D Correction D

Regarding the "blockchain network" according to Claim 1, the description before the correction, "broadcasting the transaction and an electronic signature of the transaction to a blockchain network", is corrected to the description, "broadcasting the transaction and an electronic signature of the transaction to a blockchain network composed of multiple nodes and connected to the network".

E Correction E

Regarding the "signal processing method" according to Claim 1, the description

before the correction which includes "a procedure of transmitting", "a procedure of receiving", and "a procedure of executing the transaction", is corrected to the description, "at least one of the multiple communication terminals is connected to the blockchain network, and executes the broadcast".

F Correction F

Regarding "the approval signal" according to Claim 2, the description before the correction, "the approval signal is generated by adding an electronic signature in the node", is corrected to the description, "the approval signal is generated by adding an electronic signature to the transaction in the communication terminal having received the approval request signal".

G Correction G

Claims 3 and 4 before the correction are deleted.

(2) Correction on a group of Claims 5 to 8

A Correction H

The term "multiple nodes" according to Claim 5 is corrected to "multiple communication terminals". The description before the correction, "a group composed of multiple nodes", is corrected to the description,
"a group composed of communication terminals connected to each other over a network". The description before the correction, "receiving an approval signal from nodes corresponding to a certain ratio of the multiple nodes having received the approval request signal", is corrected to the description, "receiving an approval signal from communication terminals corresponding to a certain ratio of the multiple communication terminals having received the approval request signal".

B Correction I

Regarding the destination of the "approval request signal" according to Claim 5, the description before the correction, "transmitting an approval request signal for execution of a transaction to at least one of the multiple nodes", is corrected to the description, " transmitting an approval request signal for execution of a transaction from one of the multiple communication terminals to at least one of the multiple communication terminals".

C Correction J

Regarding the "procedure of executing the transaction" according to Claim 5, the description before the correction, "based on approval of the received approval signal", is corrected to the description, "after receiving the approval signal".

D Correction K

Regarding the "blockchain network" according to Claim 5, the description before the correction, "broadcasting the transaction and an electronic signature of the transaction to a blockchain network", is corrected to the description, "broadcasting the transaction and an electronic signature of the transaction to a blockchain network composed of multiple nodes and connected to the network".

E Correction L

Regarding the "signal processing method" according to Claim 5, the description before the correction which includes "configured to cause the plurality of nodes to execute" "a procedure of transmitting", "a procedure of receiving", and "a procedure of executing the transaction", is corrected to the description, "at least one of the multiple communication terminals is connected to the blockchain network, and executes the broadcast".

F Correction M

Regarding the "node" according to Claim 6, the description before the correction, "cause the multiple nodes to execute", is corrected to the description, "cause the multiple communication terminals to execute". Regarding an object to which an electronic signature is added, the description before the correction, "generating the approval signal by adding an electronic signature", is corrected to the description, "generating the approval signal by adding an electronic signature to the transaction".

G Correction N

Claims 7 and 8 before the correction are deleted.

2 Propriety of the purpose of correction, existence or absence of new matter, and enlargement or alternation of the scope of claims

(1) Regarding Correction A

Correction A includes a matter of correcting the "multiple nodes" before the correction to "multiple communication terminals".

The following descriptions are acknowledged in paragraphs 16 to 20 of the specification. (Underlines were added for explanation in this decision. The same applies hereinafter.)

"[0016]

Communication terminals 110, which are under the control of a user, are terminals having a communication function, e.g., a stationary (desk-top) computer and a mobile communication terminal, such as a notebook computer or cellphone (including a

tablet and smartphone). The communication terminals 110 can communicate with each other over a network 120. The network 120 may be an external network, such as the Internet, or an internal network, such as a LAN (Local Area Network). When an internal network is used as the network 120, at least one of the communication terminals 110 is connected to the external network. Some or all of the communication terminals 110 may be connected to each other over a telephone line (not shown in figures). The communication terminals 110 are also referred to as nodes.

[0017]

Data 100 are electronic data, such as text data, image data, or composite data thereof, e.g., documents, tables, images, pictures, or values. The data 100 do not need to be encrypted, protected by password in a user group, or subjected to access limitation. In this case, all members in the user group can freely access the data 100 through the communication terminals 110.

[0018]

The data 100 may be stored in a server 150 connected to the network 120. An administrator directly or indirectly managing the server 150 (hereinafter referred simply as administrator) provides various platforms for the data 100 in accordance with the contents of services of the administrator. For example, there is provided a platform for managing schedule data of a user group, a platform for displaying arbitrary input information of a user in time series, or a platform for displaying data relating to shared properties of a user group. A user selects an optimal platform for the data 100 treated, and treats the data 100 in accordance with an environment of the platform.

[0019]

A blockchain network 130 is also connected to the network 120. The blockchain network 130 is composed of multiple communication terminals 132_1 to 132_m (m is a natural number) connected to each other over the network 120. The communication terminals 132, which differ in performance specifications but have the same authority, can communicate with each other directly to form a so-called P2P (Peer-to-Peer) network. The communication terminals 132 are also referred to as nodes. In the following descriptions, the communication terminals 132 are referred to as nodes in order to distinguish them from the communication terminals 110. At least one of the communication terminals 110 is connected to at least one of the nodes 132 over the network 120. The communication terminal 110 can function as the node 132, while the node 132 can serve also as the communication terminal 110. In this case, at least only one of the communication terminals 110 is required to function as the node 132.

[0020]

The node 132 is a unit of information processing based on transmission or receiving processing of data, and may be a communication terminal to be managed by each of unspecified owners. In this case, the blockchain network 130 is also referred to as public blockchain network. The blockchain network 130 can be configured so that all or part of the nodes 132 may be managed by an administrator. For example, the blockchain network 130 is configured by multiple concerned parties in the same business field as the administrator. In this case, the blockchain network 130 is also referred to as a private blockchain network or a consortium blockchain network."

From the above descriptions (especially underlined portions), the following Technical Matter 1 is recognized.

"Communication terminals 110 are terminals having a communication function, which can communicate with each other over a network 120,

the communication terminals 110 are also referred to as nodes,

all members of a user group can freely access data 100 through the communication terminals 110,

a blockchain network 130 is also connected to the network 120,

the blockchain network 130 is composed of multiple communication terminals 132_1 to 132_m (m is a natural number) connected to each other over the network 120,

the communication terminals 132 are referred to as nodes in order to distinguish them from the communication terminals 110, at least one of the communication terminals 110 is connected to at least one of the nodes 132 over the network 120, and the communication terminal 110 can function as the node 132,

the node 132 can serve also as the communication terminal 110; in this case, at least only one of the communication terminals 110 is required to function as the node 132,

the node 132 is a unit of information processing based on transmission or receiving processing of data, and may be a communication terminal to be managed by each of unspecified owners."

According to Technical Matter 1, we recognize that the unit called "node" encompasses a "communication terminal 110" and that the "node" also encompasses a "communication terminal 132" as well as the "communication terminal 110". Thus, correcting the "multiple nodes" to the "multiple communication terminals" includes a

matter of limiting to one of multiple communication terminals constituting a node.

In addition, since "all members of a user group can freely access data 100 through the communication terminals 110" and "communication terminals 110 are terminals having a communication function, which can communicate with each other over a network 120", correcting the "group composed of multiple nodes" to the "group composed of communication terminals connected to each other over a network" includes a matter of limiting to one of multiple communication terminals constituting a node.

Furthermore, the following descriptions are included in paragraphs 26 to 28 of the specification.

"[0026]

2. 3 Approval request (S102)

After generating a transaction, the process proceeds to a step of approving the transaction. Specifically, as shown in FIG. 4, the first communication terminal 110_1 transmits an approval request signal to communication terminals 110 owned by other users in the user group (S120). The approval request signal includes an unencrypted (original) transaction TA and a first electronic signature ES1. In transmitting the approval request signal, or before or after transmitting the approval request signal, the first communication terminal 110_1 transmits a public key 112_1 to communication terminals 110 which are destinations of the approval request signal. Although FIG. 4 shows an example of transmitting an approval request signal to all of the communication terminals 110 excluding the first communication terminal 110_1, the approval request signal can be transmitted to some of the communication terminals 110 selectively as described later, or can be transmitted to the first communication terminal 110_1 itself.

[0027]

A user receiving the approval request signal decrypts the electronic signature ES1 using the public key 112_1 in the communication terminal 110, and collates the unencrypted transaction with a transaction generated by decrypting the electronic signature for verification. When they are coincident with each other a result of the collation, the transaction is not falsified or altered, thereby verifying validity of the transaction. On the other hand, when the original transaction is not coincident with the transaction generated by decrypting the electronic signature, falsification or alteration of the transaction is determined. When validity is not verified, the transaction is not approved and is discarded (not shown).

[0028]

2. 4 Approval (S104)

The users of the communication terminals 110 having received the transaction select an action to approve the transaction or an action not to approve the transaction (S104). When the transaction is approved, the transaction is encrypted with a private key 114_2 generated in the communication terminal (second communication terminal, for convenience) of a user who approves the transaction (second user, for convenience), to generate an electronic signature ES2 (FIG. 3 (B)). The second communication terminal 110_2 transmits an approval signal including the original transaction TA and the electronic signature ES1 included in the approval request signal transmitted from the first user and the electronic signature ES2 generated by the second communication terminal 110_2 (S122). In the same way as for the approval request signal, a public key 112_2 corresponding to the private key 114_2 is transmitted before or after transmitting the approval signal or simultaneously with the transmission. Although FIG. 4 shows an example of transmitting an approval signal to all of the communication terminals 110 excluding the second communication terminal 110_1, the approval signal can be transmitted to some of the communication terminals 110 selectively, or can be transmitted to the second communication terminal 110_2 itself. Through the above processes, two electronic signatures (ES1 and ES2) are generated for one transaction."

From the above descriptions (especially underlined portions), the following Technical Matter 2 is recognized.

"The first communication terminal 110_1 transmits an approval request signal to communication terminals 110 owned by other users in the user group,

the users of the communication terminals 110 having received the transaction select an action to approve the transaction or an action not to approve the transaction; when the transaction is approved, the transaction is encrypted with a private key 114_2 generated in the second communication terminal 110_2 of a user who approves the transaction, to generate an electronic signature ES2,

the second communication terminal 110_2 transmits an approval signal including the original transaction TA and the electronic signature ES1 included in the approval request signal transmitted from the first user and the electronic signature ES2 generated by the second communication terminal 110_2."

According to the Technical Matter 2, we recognize that when the "approval

request signal" is "transmitted to communication terminals 110 owned by users" of the "user group" from the "first communication terminal 110_1" and the "user of the communication terminal 110 having received the transaction" "selects" "approving the transaction", "an approval signal including an electronic signature ES2 generated by the second communication terminal 110_2 is transmitted". Thus, correcting the description, "receiving an approval signal from nodes corresponding to a certain ratio of the multiple nodes having received the approval request signal" to the description, "receiving an approval signal from communication terminals corresponding to a certain ratio of the multiple communication terminals having received the approval request signal", includes a matter of limiting a target to which the approval signal is transmitted.

Therefore, the Correction A is acknowledged as aiming at restriction of the scope of claims.

In light of the above Technical Matters 1 and 2, it is obvious that Correction A does not fall under addition of new matter and does not enlarge or alter the scope of claims substantially.

(2) Regarding Correction B

The point of correction regarding the destination of the "approval request signal" in Correction B, to the description, "transmitting at least one of the multiple communication terminals", is indicated in the description in Technical Matter 2 in (1), "the first communication terminal 110_1 transmits an approval request signal to communication terminals 110 owned by other users in the user group". As determined in (1), the correction from the "nodes" to the "communication terminals" includes a matter of limiting to one of multiple communication terminals constituting a node.

Therefore, Correction B is acknowledged as aiming at restriction of the scope of claims.

In light of the above Technical Matter 2, it is obvious that Correction B does not fall under addition of new matter and does not enlarge or alter the scope of claims substantially.

(3) Regarding Correction C

The correction, by Correction C, from the description before the correction, "based on approval of the received approval signal", to the description, "after receiving the approval signal" was made for dissolving the reasons for revocation that "what the description 'approval of the received approval signal' in Claim 1 indicates is unclear" in (1) of Reason 1 of the notice of reasons for revocation dated February 15, 2019 (Article

36(6)(ii) of the Patent Act), and the correction is acknowledged as aiming at clarification of an ambiguous statement.

The following descriptions are included in paragraphs 28 to 29 and 39 to 41 of the specification.

"[0028]

2. 4 Approval (S104)

The users of the communication terminals 110 having received the transaction select an action to approve the transaction or an action not to approve the transaction (S104). When the transaction is approved, the transaction is encrypted with a private key 114_2 generated in the communication terminal (second communication terminal, for convenience) of a user who approves the transaction (second user, for convenience), to generate an electronic signature ES2 (FIG. 3 (B)). The second communication terminal 110_2 transmits an approval signal including the original transaction TA and the electronic signature ES1 included in the approval request signal transmitted from the first user and the electronic signature ES2 generated by the second communication terminal 110_2 (S122). In the same way as for the approval request signal, a public key 112_2 corresponding to the private key 114_2 is transmitted before or after transmitting the approval signal or simultaneously with the transmission. Although FIG. 4 shows an example of transmitting an approval signal to all of the communication terminals 110 excluding the second communication terminal 110_1, the approval signal can be transmitted to some of the communication terminals 110 selectively, or can be transmitted to the second communication terminal 110_2. Through the above processes, two electronic signatures (ES1 and ES2) are generated for one transaction."

[0029]

The communication terminals 110 having received the approval signal decode the two electronic signatures by using corresponding public keys 112_1 and 112_2 to verify the transaction (see FIG. 3 (B)). Thus, the user who has approved can be identified."

"[0039]

2. 6 Broadcast (S110)

When the transaction is approved, execution of the transaction is started. Specifically, the transaction is first broadcast to the blockchain network 13 over the network 120 (S110).

[0040]

For example, the communication terminal 110_1 determines whether or not the number of electronic signatures included in the received approval signal satisfies approval condition. When the approval condition is satisfied, the transaction, the electronic signature ES1, and the received electronic signatures are broadcast to the blockchain network 130 (S128). The communication terminals 110 which perform broadcast are not limited to the first communication terminal 110_1, and can be arbitrarily set. For example, a communication terminal 110 determined in advance can be used for broadcast, or a communication terminal 110 which has generated the electronic signature required for satisfying the approval condition last is used for broadcast.

2. 7 Update of blockchain

[0041]

After broadcast, the transaction is verified. As shown in FIG. 5 (A), storage devices of the nodes 132 in the blockchain network 130 store blocks 140 formed by collecting past transactions broadcast. The blocks 140 are connected in the order of generation to form a time series. A new transaction is verified in the blockchain network 130. When validity of the transaction is verified, a new block 140 including the transaction is generated. The new block (block 140_3 in FIG. 5 (A)) is connected to blocks generated before (block 140_1, block 140_2) to update the blockchain, and the transaction is executed."

From the above descriptions (especially underlined portions), the following Technical Matter 3 is recognized.

"The users of the communication terminals 110 having received the transaction select an action to approve the transaction or an action not to approve the transaction; when the transaction is approved, the transaction is encrypted with a private key 114_2 generated in the communication terminal 110_2 of a user who approves the transaction to generate an electronic signature ES2,

the communication terminal 110_2 transmits an approval signal including the transaction TA, the electronic signature ES1, and the electronic signature ES2 generated by the communication terminal 110_2,

the communication terminals 110 having received the approval signal decode the two electronic signatures by using corresponding public keys 112_1 and 112_2 to verify the transaction,

when the transaction is approved, execution of the transaction is started,

the transaction is verified in the blockchain network 130; when validity of the transaction is verified, a new block 140 including the transaction is generated, the new block is connected to blocks generated before to update the blockchain, and the transaction is executed."

In light of the Technical Matter 3, we recognize that after the "approval signal" including the "transaction TA" is transmitted by the communication terminal 110_2, "the transaction is executed". Thus, it is obvious that Correction C does not fall under addition of new matter and does not enlarge or alter the scope of claims substantially.

(4) Regarding Correction D

The correction, regarding Correction D, from the description, "broadcasting the transaction and an electronic signature of the transaction to a blockchain network", to the description, "broadcasting the transaction and an electronic signature of the transaction to a blockchain network composed of multiple nodes and connected to the network" includes a matter of limiting the "blockchain network" to be "composed of multiple nodes" and "connected to the network".

The following descriptions are included regarding the "blockchain network" and "broadcast" relating to Correction D, in paragraphs 19 and 39 to 40 of the specification.

"[0019]

A blockchain network 130 is also connected to the network 120. The blockchain network 130 is composed of multiple communication terminals 132_1 to 132_m (m is a natural number) connected to each other over the network 120. The communication terminals 132, which differ in performance specifications but have the same authority, can communicate with each other to form a so-called P2P (Peer-to-Peer) communication network. The communication terminals 132 are also referred to as nodes. In the following descriptions, the communication terminals 132 are referred to as nodes in order to distinguish them from the communication terminals 110. At least one of the communication terminals 110 is connected to at least one of the nodes 132 over the network 120. The communication terminal 110 can function as the node 132, while the node 132 can serve also as the communication terminal 110. In this case, at least only one of the communication terminals 110 is required to function as the node 132."

"[0039]

2. 6 Broadcast (S110)

When the transaction is approved, execution of the transaction is started. Specifically, the transaction is first broadcast to the blockchain network 130 over the network 120 (S110).

[0040]

For example, the communication terminal 110_1 determines whether or not the number of electronic signatures included in the received approval signal satisfies the approval condition. When the approval condition is satisfied, the transaction, the electronic signature ES1, and the received electronic signatures are broadcast to the blockchain network 130 (S128). The communication terminals 110 which perform broadcast are not limited to the first communication terminal 110_1, and can be arbitrarily set. For example, a communication terminal 110 determined in advance can be used for broadcast, or a communication terminal 110 which has generated the electronic signature required for satisfying the approval condition last is used for broadcast."

From the above descriptions (especially underlined portions), the following Technical Matter 4 is recognized.

"A blockchain network 130 is connected to the network 120, the blockchain network 130 is composed of multiple communication terminals 132_1 to 132_m (m is a natural number) connected to each other over the network 120, the communication terminals 132 are also referred to as nodes,

the transaction is broadcast to the blockchain network 130 over the network 120,

the transaction, the electronic signature ES1, and the received electronic signatures are broadcast to the blockchain network 130."

In the Technical Matter 4, according to the descriptions, "a blockchain network 130 is connected to the network 120" and "the blockchain network 130 is composed of multiple communication terminals 132_1 to 132_m (m is a natural number) connected to each other over the network 120", we recognize that the "blockchain network" is "composed of multiple nodes". According to the description, "the transaction, the electronic signature ES1, and the received electronic signatures are broadcast to the blockchain network 130", we recognize that "the transaction and an electronic signature of the transaction are broadcast to a blockchain network composed of multiple nodes and connected to the network".

Therefore, Correction D is acknowledged as aiming at restriction of scope of claims. In light of Technical Matter 4, it is obvious that Correction D does not fall under addition of new matter and does not enlarge or alter the scope of claims substantially.

(5) Regarding Correction E

The matter described relating to Correction E, "at least one of the multiple communication terminals is connected to the blockchain network, and executes the broadcast", is acknowledged as further limiting the configuration of "broadcasting the transaction and an electronic signature of the transaction to a blockchain network " in the "procedure of executing the transaction by broadcasting the transaction and an electronic signature of the transaction to a blockchain network based on approval of the received approval signal and adding a block including information on the transaction to the blockchain" before the correction. Correction E is acknowledged as aiming at restriction of scope of claims.

According to Technical Matter 1 in (1), we recognize that "at least one of the communication terminals 110 is connected to at least one of the nodes 132 over the network 120, and can function as the node 132", and that "the node 132 can serve also as the communication terminal 110; in this case, at least one of the communication terminals 110 is required to function as the node 132" in the "blockchain network 130" which is "composed of multiple communication terminals 132_1 to 132_m (m is a natural number) connected to each other over the network 120". Thus, it is obvious that Correction E does not fall under addition of new matter and does not enlarge or alter the scope of claims substantially.

(6) Regarding Correction F

Correction F limits "the approval signal" in the description before the correction, "the approval signal is generated by adding an electronic signature in the node" so as to be generated "by adding an electronic signature to the transaction" in "the communication terminals having received the approval request signal". Correction F is acknowledged as aiming at restriction of scope of claims.

According to Technical Matter 2 in (1), we recognize that "the transaction is encrypted with a private key 114_2 generated in the second communication terminal 110_2 to generate an electronic signature ES2" and that "the second communication terminal 110_2" "transmits an approval signal including the transaction TA, the electronic signature ES1, and the electronic signature ES2 generated by the second

communication terminal 110_2". Thus, it is obvious that Correction F does not fall under addition of new matter and does not enlarge or alter the scope of claims substantially.

(7) Regarding Correction G

Correction G, which is to delete Claims 3 and 4 before the correction, is intended for restriction of the scope of claims.

It is obvious that Correction G does not fall under addition of new matter and does not enlarge or alter the scope of claims substantially.

(8) Regarding Correction H

Correction H, which includes the same matters of correction as Correction A, is acknowledged as aiming at restriction of the scope of claims, as indicated in (1).

According to Technical Matters 1 and 2, it is obvious that Correction H does not fall under addition of new matter and does not enlarge or alter the scope of claims substantially.

(9) Regarding Correction I

Correction I, which includes substantially the same matters of correction as Correction B, is acknowledged as aiming at restriction of the scope of claims, as indicated in (2).

According to Technical Matter 2, it is obvious that Correction I does not fall under addition of new matter and does not enlarge or alter the scope of claims substantially.

(10) Regarding Correction J

Correction J, which includes the same matters of correction as Correction C, is acknowledged as aiming at clarification of an ambiguous statement, as indicated in (3).

According to Technical Matter 3, it is obvious that Correction C does not fall under addition of new matter and does not enlarge or alter the scope of claims substantially.

(11) Regarding Correction K

Correction K, which includes the same matters of correction as Correction D, is acknowledged as aiming at restriction of the scope of claims, as indicated in (4). According to Technical Matter 4, it is obvious that Correction K does not fall under

addition of new matter and does not enlarge or alter the scope of claims substantially.

(12) Regarding Correction L

Correction L, which includes substantially the same matters of correction as Correction E, is acknowledged as aiming at restriction of the scope of claims, as indicated in (5).

According to Technical Matter 1, it is obvious that Correction L does not fall under addition of new matter and does not enlarge or alter the scope of claims substantially.

(13) Regarding Correction M

Correction M, which includes substantially the same matters of correction as Correction F, is acknowledged as aiming at restriction of the scope of claims, as indicated in (6).

According to Technical Matter 2, it is obvious that Correction M does not fall under addition of new matter and does not enlarge or alter the scope of claims substantially.

(14) Regarding Correction N

Correction N, which is to delete Claims 7 and 8 before the correction, is intended for restriction of the scope of claims.

It is obvious that Correction N does not fall under addition of new matter and does not enlarge or alter the scope of claims substantially.

3 Summary

As described above, the correction made by the demand for correction is intended for the matters stipulated in Article 120-5(2)(i) and (iii) of the Patent Act, and falls under the provisions of Article 126(5) and 126(6) of the Patent Act which are applied mutatis mutandis in the provisions of Article 126(9) of the Patent Act.

Therefore, the correction of the scope of claims shall be approved as described in the corrected scope of claims attached to the written demand for correction, regarding Claims [1-4] and [5-8] after the correction.

No. 3 The Invention after the correction

The inventions (hereinafter referred to as "Invention 1", "Invention 2", "Invention 5", and "Invention 6", respectively) according to Claims 1, 2, 5, and 6

corrected by the demand for correction are as specified by the following matters described in Claims 1, 2, 5, and 6 of the corrected scope of claims.

Invention 1:
"A signal processing method including: a procedure of transmitting an approval request signal for execution of a transaction on data to be shared in a group composed of multiple communication terminals connected to each other over a network, to at least one of the communication terminals;

a procedure of receiving an approval signal from communication terminals corresponding to a certain ratio of the multiple communication terminals having received the approval request signal; and

a procedure of executing the transaction by broadcasting the transaction and an electronic signature of the transaction to a blockchain network composed of multiple nodes and connected to the network, after receiving the approval signal, and adding a block including information on the transaction to a blockchain, wherein

at least one of the multiple communication terminals is connected to the blockchain network, and executes the broadcast."

Invention 2:
"The signal processing method described in Claim 1, wherein the approval signal is generated by adding an electronic signature to the transaction in the communication terminal having received the approval request signal."

Invention 5:
"A signal processing program which is configured to cause the multiple nodes to execute:
a procedure of transmitting an approval request signal for execution of a transaction on data to be shared in a group composed of multiple communication terminals connected to each other over a network, from one of the communication terminals to at least one of the communication terminals;

a procedure of receiving an approval signal from communication terminals corresponding to a certain ratio of the multiple communication terminals having received the approval request signal; and

a procedure of executing the transaction by broadcasting the transaction and an electronic signature of the transaction to a blockchain network composed of multiple nodes and connected to the network, after receiving the approval signal, and adding a

block including information on the transaction to a blockchain, wherein

at least one of the multiple communication terminals is connected to the blockchain network, and executes the broadcast."

Invention 6:
"The signal processing program described in Claim 5 configured to cause the multiple communication terminals to execute generating the approval signal by adding an electronic signature to the transaction."

No. 4 Reasons for revocation described in the notice of reasons for revocation
1 Outline of the reasons for revocation

The summary of the reasons for revocation notified by the body to the patentee on February 15, 2019, regarding the patent according to Claims 1 to 8 before the correction, is as follows.

A. The patent according to Claims 1 to 8, which has been granted for the patent application for which the description of the scope of claims does not satisfy the requirements stipulated in Article 36(6)(ii) of the Patent Act, should be cancelled.

B. The inventions according to Claims 1 to 8 could have been easily conceived by a person skilled in the art on the basis of the inventions described in Evidence A No. 1 and Evidence A No. 3, and the patent according to Claims 1 to 8, which violates the provisions of Article 29(2) of the Patent Act, should be cancelled.

2 Description of Evidence A
(1) Matters described in Evidence A No. 1 and Cited invention

Evidence A No. 1 ("Bitcoin and Blockchain, Technology for supporting cryptographic currencies", the first edition, Andreas M. Antonopoulos, Takaya IMAI, Junichiro HATOGAI, published by NTT Publishing on July 21, 2016, p. 1-p. 296) includes the following descriptions.

A "What is Bitcoin?

Bitcoin is a collection of concepts and technologies that form the basis of a digital money ecosystem. Units of currency called bitcoins are used to store and transmit value among participants in the bitcoin network. Bitcoin users communicate with each other using the bitcoin protocol primarily via the Internet, although other

transport networks can also be used. The bitcoin protocol stack, available as open source software, can be run on a wide range of computing devices, including laptops and smartphones, making the technology easily accessible. (p. 1 l.1-l.8)

B "

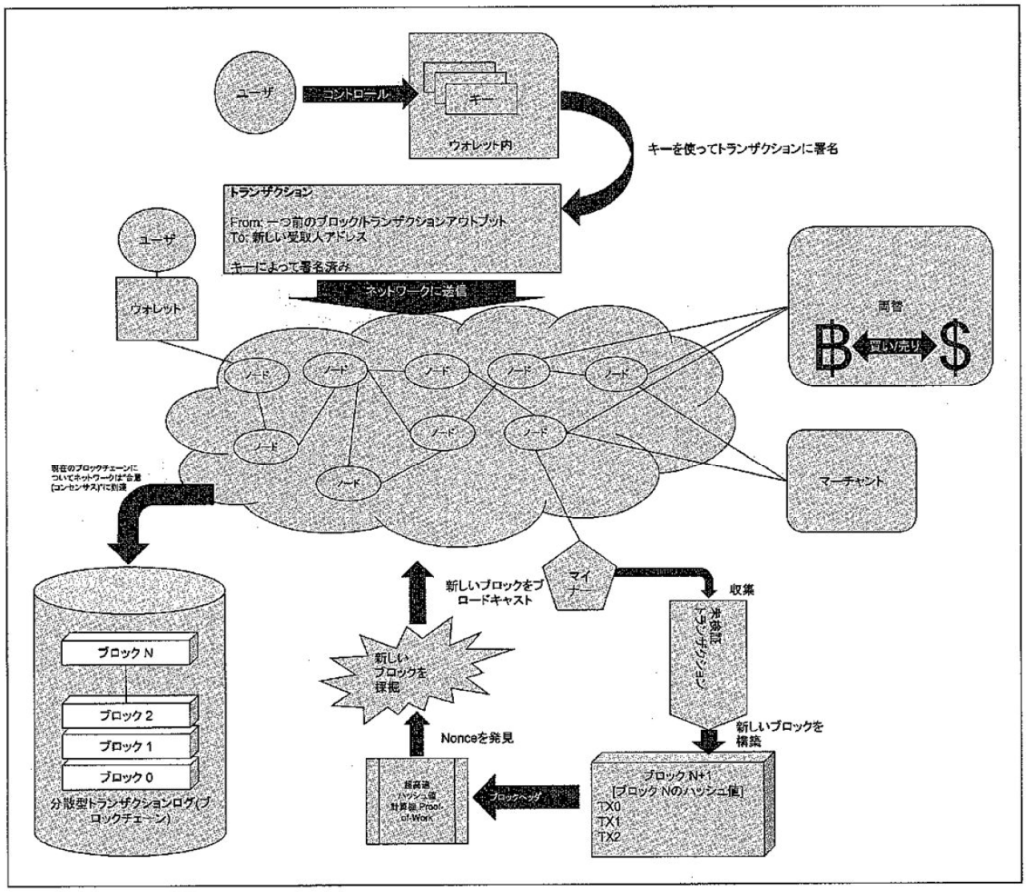

図2－1　ビットコイン概観

ユーザ	User
コントロール	Control
キー	Key
ウォレット内	in Wallet
キーを使ってトランザクションに署名	Sign the transaction with key
トランザクション	Transaction
Ｆｒｏｍ：一つ前のブロック／トランザクションアウトプット	From: Previous block/Transaction Output
Ｔｏ：新しい受取人アドレス	To: New Recipient Address
キーによって署名済み	Signed by key

ネットワークに送信　Transmission to network
ウォレット　Wallet
ノード　Node
現在のブロックチェーンについてネットワークは"合意（コンセンサス）"に到達　Network achieves "consensus" on current blockchain
両替　Exchange
買い／売り　Buy/Sell
マーチャント　Merchant
ブロック　Block
分散型トランザクションログ（ブロックチェーン）　Decentralized Transaction Log (Blockchain)
新しいブロックをブロードキャスト　New block broadcast
マイナー　Miner
収集　Collection
未検証トランザクション　Unverified Transaction
新しいブロックを構築　New block constructed
［ブロック　Ｎのハッシュ値］　[Hash of Block N]
ブロックヘッダ　Block Header
超高速ハッシュ値計算機　Ultra-high-speed hash value calculator
Ｎｏｎｃｅを発見　Finding Nonce
新しいブロックを採掘　New Block mined
図２－１　ビットコイン概観　FIG. 2-1 Bitcoin overview

FIG. 2-1" (p. 16)

C "In simple terms, a transaction tells the network that the owner of a number of bitcoins has authorized the transfer of some of those bitcoins to another owner. The new owner can now spend these bitcoins by creating another transaction that authorizes transfer to another owner.

... (Omitted) ...

The transaction also contains proof of ownership for each input, in the form of a digital signature, which can be independently validated by anyone. In bitcoin terms, 'spending' is signing a transaction." (p. 18 l. 18-l. 33)

D "Transactions move value from transaction inputs to transaction outputs. An input is where the coin value is coming from, usually a previous transaction's output. A transaction output assigns a new owner to the value by associating it with a key. The key is called an encumbrance. It imposes a requirement for a signature for the funds to be redeemed in future transactions. Outputs from one transaction can be used as inputs in a new transaction, thus creating a chain of ownership as the value is moved from address to address (see FIG. 2-4)." (p. 19 l. 1-l. 8)

E "

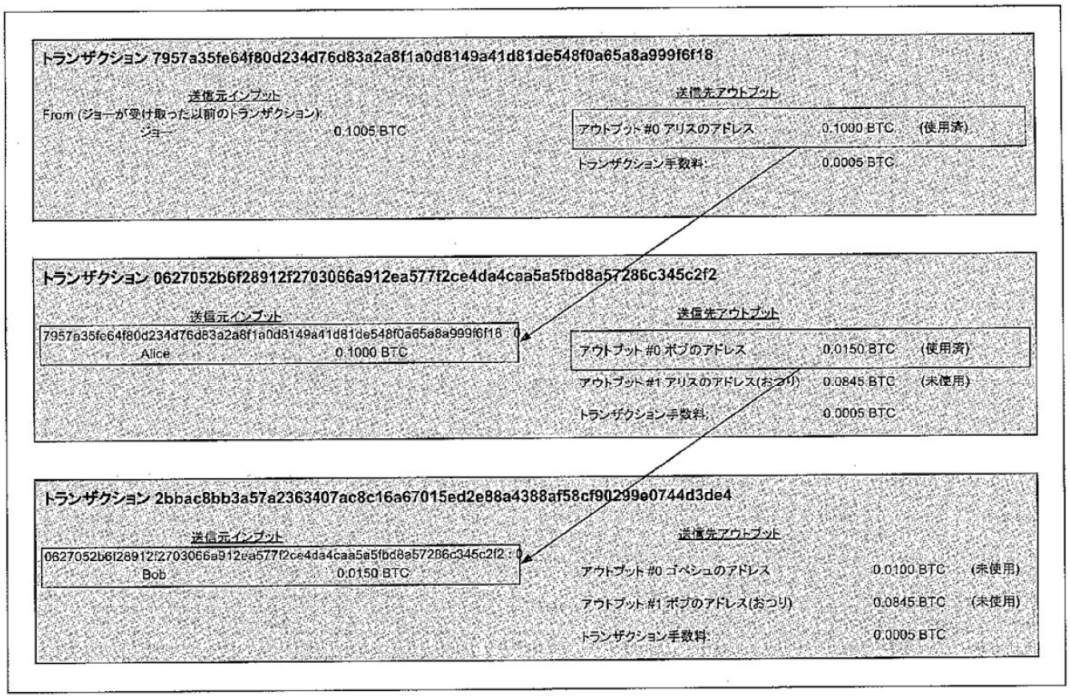

図2－4　トランザクションの連鎖。あるトランザクションのアウトプットは次のトランザクションのインプットになる。

トランザクション	Transaction
送信元インプット	INPUTS From
（ジョーが受け取った以前のトランザクション）	(previous transactions Joe has received)
ジョー	Joe
送信先アウトプット	OUTPUTS To
アウトプット	Output
アリスのアドレス	Alice's Address
（使用済）	(spent)

トランザクション手数料　　Transaction fees
ボブのアドレス　　Bob's Address
（おつり）　　(Change)
（未使用）　　(unspent)
ゴペシュのアドレス　　Gopesh's Address
図２－４　トランザクションの連鎖。あるトランザクションのアウトプットは次のトランザクションのインプットになる。　　FIG. 2-4 A chain of transactions, where the output of one transaction is the input of the next transaction

FIG. 2-4" (p. 20)

F "Alice's payment to Bob's Cafe uses a transaction from Joe to Alice as its input. In the previous chapter Alice received bitcoin from her friend Joe in return for cash. That transaction is locked with Alice's key. A new transaction from Alice to Bob references the transaction from Joe to Alice as an input and creates transaction outputs to pay for the cup of coffee and receive change. The transactions form a chain, where the inputs from the latest transaction correspond to outputs from previous transactions. Alice's key unlocks those previous transaction outputs, thereby proving to the bitcoin network that she owns the funds. Alice attaches the payment for coffee to Bob's address, thereby requiring Bob to produce a signature in order to spend that amount. This represents a transfer of value between Alice and Bob. This chain of transactions, from Joe to Alice to Bob, is illustrated in FIG. 2-4." (p. 20 l. 1-l. 14)

G "Creating the Outputs

A transaction output is created in the form of a script that creates an encumbrance to spend funds and can only be redeemed by the introduction of a solution to the script. In simpler terms, the script says something like, 'This output is payable to whoever can present a signature from the private key corresponding to Bob's public address.' Because only Bob has the wallet with the private keys corresponding to that address, only Bob's wallet can present such a signature to redeem this output. Alice will therefore encumber the output value with a demand for a signature from Bob." (p. 24 l.4-l. 11)

H "Because the transmission to be transmitted to the bitcoin network contains all the information necessary for inclusion to the blockchain, it does not matter how or where it is transmitted to the bitcoin network. The bitcoin network is a peer-to-peer network,

with each bitcoin client participating by connecting to several other bitcoin clients. The purpose of the bitcoin network is to propagate transactions and blocks to all participants." (p. 25 l. 10-l. 16)

I "A common misconception about bitcoin transactions is that they must be 'confirmed' by waiting 10 minutes for a new block, or up to 60 minutes for a full six confirmations. Although confirmations ensure that the transaction has been accepted by the whole network, such a delay is unnecessary for small-value items such as a cup of coffee. A merchant may accept a valid small-value transaction with no confirmations, with no more risk than a credit card payment made without an ID or a signature, as merchants routinely accept today." (p. 26 l. 19-l. 25)

J "Bitcoin mining

The transaction is now propagated on the bitcoin network. It does not become part of the shared ledger (the blockchain) until it is verified and included in a block by a process called mining. See Chapter 8 for a detailed explanation.

The bitcoin system of trust is based on computation. Transactions are bundled into blocks, which require an enormous amount of computation to prove, but only a small amount of computation to verify as proven. The mining process serves two purposes in bitcoin:

. Mining creates new bitcoins in each block, almost like a central bank printing new money. The amount of bitcoin created per block is fixed and diminishes with time.
. Mining creates trust by ensuring that 'transactions are only confirmed if enough computational power was devoted to the block that contains them'. More blocks mean more computation, which means more trust." (p. 26 l. 26-p. 27 l. 7)

K "Pay-to-Script Hash (P2SH) and Multi-signature address

As we know, traditional bitcoin addresses begin with the number '1', and are derived from a public key, which is derived from a private key. Although anyone can send bitcoin to '1' addresses, that bitcoin can only be spent by presenting the corresponding private key signature and public key hash.

Bitcoin addresses that begin with the number '3' are pay-to-script hash (P2SH) addresses, sometimes erroneously called multi-signature addresses or multi-sig addresses. They designate the beneficiary of a bitcoin transaction as the hash of a script, instead of the owner of a public key. This feature was introduced in 2012 with

Bitcoin Improvement Proposal 16 (see [bio0016]) and is being widely adopted because it provides the opportunity to add functionality to the address itself. Unlike transactions that 'send' funds to traditional '1' bitcoin addresses (also known as pay-to-public-key-hash [P2PKH]), funds sent to '3' bitcoin addresses require something more than the presentation of one public key hash and one private key signature as proof of ownership. The requirements are designated at the time the address is created, within the script, and all inputs to this address will be encumbered with the same requirements. A Pay-to-script hash address is created from a transaction script, which defines who can spend a transaction output. (See Chapter 5 'Pay-to-Script-Hash (P2SH)' for more details). Encoding a pay-to-script hash address involves using the same double-hash function as used during creation of a bitcoin address, only applied on the script instead of the public key.

... (Omitted) ...

Multi-signature address and P2SH

Currently, the most common implementation of the P2SH function is the multi-signature address script. As the name implies, the script requires one or more signatures to prove ownership and therefore spend funds. The bitcoin multi-signature feature is designed to require M signatures (also known as 'threshold') from a total of N keys, known as an M-of-N multi-sig, where M is equal to or less than N. For example, Bob the coffee shop owner from Chapter 1 could use a multi-signature address requiring 1-of-2 signatures from a key belonging to him and a key belonging to his spouse, ensuring that either of them could sign to spend a transaction output locked to this address. Gopesh (web designer paid by Bob to create a website) might have a 2-of-3 multi-signature address for his business that ensures that no funds can be spent unless at least the two of the business partners sign a transaction." (p. 105 the 5th line from the bottom to p. 107 l. 8)

L "Transaction lifecycle

A transaction's lifecycle starts with the transaction's creation, also known as origination. The transaction is then signed with signatures indicating the authorization to spend the funds referenced by the transaction. The signed transaction is then broadcast on the bitcoin network, where each network node (participant of the bitcoin network) validates and propagates the transaction until it reaches (almost) every node in the network. Finally, the transaction is verified by a mining node and included in a

block of transactions that is recorded on the blockchain." (p. 117 l. 11-l. 18)

M " Broadcasting transaction to the Bitcoin Network

First, a transaction needs to be delivered to the bitcoin network so that it can be recorded in the blockchain. A bitcoin transaction is 300 to 400 bytes of data and has to reach any one of tens of thousands of bitcoin nodes. The senders do not need to trust the bitcoin nodes, so long as they broadcast more than one bitcoin node. The nodes don't need to trust the sender or establish the sender's identity. Because the transaction is signed and contains no confidential information (private keys or credentials), it can be publicly broadcast using any open transfer means. Unlike credit card transactions, for example, which contain sensitive information and can only be transmitted on encrypted networks, a bitcoin transaction can be sent over any network. So long as the transaction can reach a bitcoin node, it doesn't matter how it is transported. Bitcoin transactions can therefore be transmitted over insecure networks such as WiFi, Bluetooth, NFC, Chirp, barcodes, or by copying and pasting a bitcoin address into a web form." (p. 118 l.18-l. 32)

N "Transaction Outputs and Inputs

The fundamental building block of a bitcoin transaction is an unspent transaction output (UTXO). UTXO are indivisible chunks of bitcoin currency locked to a specific owner, recorded on the blockchain, and recognized as currency units by the entire network. The bitcoin network tracks all available (unspent) UTXO, currently numbering in the millions. Whenever a user receives bitcoin, that amount is recorded within the blockchain as a UTXO. Thus, a user's bitcoin might be scattered as UTXO amongst hundreds of transactions and hundreds of blocks. In effect, there is no such thing as a stored balance of a bitcoin address or account. There are only scattered UTXO, locked to specific owners. The concept of a user's bitcoin balance is a derived construct created by the wallet. The wallet calculates the user's balance by scanning the blockchain and aggregating all UTXO belonging to that user." (p. 120 the 14th line from the bottom to the last line)

O "Multi-Signature

Multi-signature scripts set a condition where N public keys are recorded in the script and at least M of those must provide signatures to release the encumbrance. This is also known as an M-of-N scheme, where N is the total number of keys and M is the number of signatures required for validation. For example, a 2-of-3 multi-

signature is one where three public keys are listed as potential signers and at least two of those must be used to create signatures for a valid transaction to spend the funds. At this time, standard multi-signature scripts are limited to at most 15 listed public keys, meaning you can do anything from a 1-of-1 to a 15-of-15 multi-signature or any combination within that range. The limitation to 15 listed keys might be lifted by the time this book is published, so check the Standard() function to see what is currently accepted by the network." (p. 138 the 5th line from the bottom to p. 139 l. 6)

P "Pay-to-Script-Hash (P2SH)

Pay-to-script-hash (P2SH) was introduced in 2012 as a powerful new type of transaction that greatly simplifies the use of complex transaction scripts. To explain the need for P2SH, let's look at a practical example. In Chapter 1 we introduced Mohammed, an electronics importer based in Dubai. Mohammed's company uses bitcoin's multi-signature feature extensively for its corporate accounts. Multi-signature scripts are one of the most common uses of bitcoin's advanced scripting capabilities and are a very powerful feature. Mohammed's company uses a multi-signature script for all customer payments, known in accounting terms as 'accounts receivable,'. With the multi-signature scheme, any payments made by customers are locked in such a way that they require at least two signatures to be released, from Mohammed and one of his partners or from his attorney who has a backup key. A multi-signature scheme like that offers corporate governance controls and protects against theft, embezzlement, or loss.

... (Omitted) ...

Pay-to-script-hash (P2SH) was developed to resolve these practical difficulties and to make the use of complex scripts as easy as a payment to a bitcoin address. With P2SH payments, the complex locking script is replaced with a cryptographic hash. When a transaction attempting to spend the UTXO is presented later, it must contain the script that matches the hash, in addition to the unlocking script. In simple terms, P2SH means 'pay to a script matching this hash, a script that will be presented later when this output is spent.'" (p. 141 the 9th line from the bottom to p. 142 the 12th line from the bottom)

In light of the above, Evidence A No. 1 is acknowledged as disclosing the following invention (hereinafter referred to as "Cited invention").

"A signal processing method, wherein
bitcoin is a collection of concepts and technologies that form the basis of a digital money ecosystem, users communicate with each other using the bitcoin protocol primarily via the Internet, the application runs on a wide range of computing devices, including laptops and smartphones,

a transaction tells the network that the owner of bitcoins has authorized the transfer of some of those bitcoins to another owner, the transaction also contains proof of ownership for each input, in the form of a digital signature, which can be independently validated by anyone, transactions move value from transaction inputs to transaction outputs, a transaction output assigns a new owner to the value by associating it with a key, which is called an encumbrance,

Alice's payment to Bob's Cafe uses a transaction from Joe to Alice as its input, a new transaction from Alice to Bob references the transaction from Joe to Alice as an input and creates transaction outputs to pay for the cup of coffee and receive change,

the inputs from the latest transaction correspond to outputs from previous transactions, Alice's private key unlocks those previous transaction outputs, thereby proving to the bitcoin network that she owns the funds,

a transaction output is created in the form of a script that creates an encumbrance to spend funds, the script says something like, 'This output is payable to whoever can present a signature from the private key corresponding to Bob's public address,'

the bitcoin network is a peer-to-peer network, with each bitcoin client participating by connecting to several other bitcoin clients,

confirmations ensure the transaction has been accepted by the whole network,

the transaction is propagated on the bitcoin network, it does not become part of the shared ledger (the blockchain) until it is verified and included in a block by a process called mining,

bitcoin addresses that begin with the number '3' are pay-to-script hash (P2SH) addresses, sometimes erroneously called multi-signature addresses or multi-sig addresses, they designate the beneficiary of a bitcoin transaction as the hash of a script, instead of the owner of a public key,

funds sent to '3' addresses require something more than the presentation of one public key hash and one private key signature as proof of ownership, the requirements are designated at the time the address is created, within the script, and all inputs to this address will be encumbered with the same requirements, a Pay-to-script hash address is created from a transaction script, which defines who can spend a transaction output,

the script requires one or more signatures to prove ownership and therefore spend funds, the bitcoin multi-signature feature is designed to require M signatures (also known as 'threshold') from a total of N keys, known as an M-of-N multi-sig,

a multi-signature address requiring 1-of-2 signatures from a key belonging to him and a key belonging to his spouse can be used, ensuring either of them could sign to spend a transaction output locked to this address,

one might have a 2-of-3 multi-signature address that ensures that no funds can be spent unless at least the two of the business partners sign a transaction,

a transaction's lifecycle starts with the transaction's creation, also known as origination, the transaction is then signed with signatures indicating the authorization to spend the funds referenced by the transaction, the signed transaction is then broadcast on the bitcoin network, where each network node (participant of the bitcoin network) validates and propagates the transaction until it reaches (almost) every node in the network, finally, the transaction is verified by a mining node and included in a block of transactions that is recorded on the blockchain,

a transaction needs to be delivered to the bitcoin network so that it can be recorded in the blockchain,

because the transaction is signed and contains no confidential information (private keys or credentials), it can be publicly broadcast using any open transfer means,

the fundamental building block of a bitcoin transaction is an unspent transaction output (UTXO), UTXO are indivisible chunks of bitcoin currency locked to a specific owner, recorded on the blockchain,

multi-signature scripts set a condition where N public keys are recorded in the script and at least M of those must provide signatures to release the encumbrance, which is also known as an M-of-N scheme, where N is the total number of keys and M is the number of signatures required for validation, for example, a 2-of-3 multi-signature is one where three public keys are listed as potential signers and at least two of those must be used to create signatures for a valid transaction,

pay-to-script-hash (P2SH) is a new type of transaction that greatly simplifies the use of complex transaction scripts,

any payments, made by customers using a multi-signature script for all customer payments, known in accounting terms as 'accounts receivable', require at least two signatures to release, from Mohammed and one of his partners or from his attorney who has a backup key. which offers corporate governance controls and protects against theft, embezzlement, or loss,

P2SH means 'pay to a script matching this hash, a script that will be presented

later when this output is spent'."

(2) Matters described in Evidence A No. 3

Evidence A No. 3 ("Multisig related transaction", [online], January 12, 2017, GitHub, [searched on July 26, 2018], Internet < https://github.com/NEMJPManual/NEM_Technical_reference_JA/blob/eccf8b1a6b3914f2cdf1e13416b174c5e63a66f5/Transactions/4.3.md>) includes the following descriptions.

Q "At present, NEM natively supports m-of-n multisig (multisignature) accounts.

NEM multisig transactions have been designed with flexibility in mind. Any other transaction (as of now: importance transfer transaction, transfer transaction, multisig modification transaction) can be converted into a multisig transaction." (p. 1 "Multisig related transaction")

R "As mentioned earlier, any transaction can be wrapped in a multisig transaction.

To send XEM from a multisig account to another account, a transfer transaction must be wrapped.
The multisig wrapper transaction has a fee of 6 XEM extra.

The following example shows the steps that must be taken in more detail:
Assume that a multisig account $$(M)$$ as a balance of 1000 XEM and has cosignatories $$(A, B, C)$$ and 100 XEM needs to be transferred to another account $$X$$.

Any of the cosignatories can initiate the 100 XEM transfer. Assuming that B initiates the transfer and A and C cosign, the following steps must happen for the transaction to be accepted:
1. B creates a regular, a transfer transaction that has the multisig account as the 'signer' and the transfer amount as 100 XEM.
2. B wraps the unsigned transfer transaction in a multisig transaction.
3. B signs the multisig transaction and sends it to the NEM network.
4. A and C are notified of the pending multisig transaction.
5. A creates a multisig signature transaction by calculating and signing the hash value of

the unsigned transfer transaction and sends it to the network.
6. C does the same thing A does.
7. Once all cosignatories have signed the unsigned transfer transaction, the transaction is accepted by the network and 100 XEM is transferred from M to X.

If A and/or C do not send a multisig signature transaction corresponding to the multisig transfer transaction before the transaction deadline, the multisig transfer transaction will be rejected as invalid by the network and no XEM will be transferred from $$M$$ to $$X$$." (p. 1 the last line to p. 2 the last line "4.3.3 Multisig transactions")

In light of the above, Evidence A No. 3 is acknowledged as disclosing the following technical matter (A-3 Described matter).

"In NEM natively supporting m-of-n multisig (multisignature) accounts,
When B initiates the transfer and A and C cosign,
B creates a transfer transaction that has the transfer amount as 100 XEM,
B wraps the unsigned transfer transaction in a multisig transaction,
B signs the multisig transaction and sends it to the NEM network,
A creates a multisig signature transaction by calculating and signing the hash value of the unsigned transfer transaction and sends it to the network,
Once all cosignatories have signed the unsigned transfer transaction, the transaction is accepted by the network and 100 XEM is transferred from M to X,
If A and/or C do not send a multisig signature transaction corresponding to the multisig transfer transaction before the transaction deadline, the multisig transfer transaction will be rejected as invalid by the network,
and no XEM will be transferred from $$M$$ to $$X$$."

3 Judgment by the body
(1) Regarding Article 29(2) of the Patent Act (Reason 2)

A Regarding Invention 1
(A) Comparison
Invention 1 and the Cited Invention are compared below.

1) The "transaction", "peer-to-peer network", "bitcoin network", "network node (participant of the bitcoin network)", "broadcast", and "signal processing method" in the

Cited Invention correspond to the "transaction", "network", "blockchain network", "node", "broadcast", and "signal processing method" in Invention 1, respectively.

2) The Cited Invention is configured to allow "users to communicate with each other" "using the bitcoin protocol primarily via the Internet", for "bitcoin", which is "a collection of concepts and technologies that form the basis of a digital money ecosystem", and to allow the application to "run on a wide range of computing devices, including laptops and smartphones". "The bitcoin network is a peer-to-peer network, with each bitcoin client participating by connecting to several other bitcoin clients", and the "wide range of computing devices" such as "laptops" and "smartphones" constituting the "bitcoin client" are considered as "multiple communication terminals connected to each other over a network".

The "bitcoin", which is" a collection of concepts and technologies that form the basis of a digital money ecosystem", can be "data to be shared in a group composed of multiple "bitcoin clients".

In addition, since the "transaction" relating to the "bitcoin" is configured to "start with the transaction's creation, also known as origination, the transaction is then signed with signatures indicating the authorization to spend the funds referenced by the transaction, the signed transaction is then broadcast on the bitcoin network", it can be said that a signal for the "transaction" on the "bitcoin", or a signal "for execution of a transaction on data" is "transmitted from a predetermined 'bitcoin client' to at least one of multiple communication terminals".

In summary, the Cited Invention and the Invention 1 are different from each other in the following Different Feature 1, while they are identical in including a "procedure of transmitting a signal for execution of a transaction on data to be shared in a group composed of multiple communication terminals connected to each other over a network, to at least one of the communication terminals".

3) In the Cited Invention, since the "transaction" is configured to "start with the transaction's creation, also known as origination, the transaction is then signed with signatures", it is obvious that data corresponding to the "electronic signature of the transaction" in Invention 1 are generated. According to the description in the Cited Invention, "the signed transaction is then broadcast on the bitcoin network", based on the acknowledgment in 1), it is obvious that the transaction and an electronic signature of the transaction are "broadcast to the blockchain network".

The "bitcoin network" in the Cited Invention, which is configured so that the

"transaction" is "broadcast on the bitcoin network", where "each network node (participant of the bitcoin network) validates" and "propagates the transaction until it reaches (almost) every node in the network", can be the "blockchain network composed of multiple nodes and connected to the network" in Invention 1. Consequently, the Cited Invention and the Invention 1 are identical in "broadcasting "a transaction and an electronic signature of the transaction" to a blockchain network composed of multiple nodes and connected to a network".

4) The Cited Invention includes the description, "the transaction is then broadcast on the bitcoin network, where each network node (participant of the bitcoin network) validates and propagates the transaction until it reaches (almost) every node in the network, finally, the transaction is verified by a mining node and included in a block of transactions that is recorded on the blockchain". Accordingly, with the acknowledgment in 3), the Cited Invention and Invention 1 are identical in including a "procedure of executing the transaction by broadcasting the transaction and an electronic signature of the transaction to a blockchain network composed of multiple nodes and connected to the network, and adding a block including information on the transaction to a blockchain". (The Cited Invention includes the following description: "Bitcoin addresses that begin with the number '3' are pay-to-script hash (P2SH) addresses, sometimes erroneously called multi-signature addresses or multi-sig addresses. They designate the beneficiary of a bitcoin transaction as the hash of a script, instead of the owner of a public key.

Funds sent to '3' addresses require something more than the presentation of one public key hash and one private key signature as proof of ownership. The requirements are designated at the time the address is created, within the script, and all inputs to this address will be encumbered with the same requirements. A Pay-to-script hash address is created from a transaction script, which defines who can spend a transaction output.

The script requires one or more signatures to prove ownership and therefore spend funds. The bitcoin multi-signature feature is designed to require M signatures (also known as 'threshold') from a total of N keys, known as an M-of-N multi-sig", and configured to use "a multi-signature address requiring 1-of-2 signatures from a key belonging to him and a key belonging to his spouse" for "ensuring that either of them could sign to spend a transaction output locked to this address", or "configured to ensure that no funds locked to a 2-of-3 multi-signature address can be spent unless at least two of the business partners sign a transaction". The "signatures" do not directly relate to

"executing the transaction" by "adding a block including information on the transaction to a blockchain".)

5) The "bitcoin client" in the Cited Invention "participates by connecting to several other bitcoin clients", and "the transaction is broadcast on the bitcoin network". Thus, it is obvious that there are communication terminals, such as "a wide range of computing devices, including laptops and smartphones" which "broadcast" the "transaction" on the "bitcoin network". Accordingly, the Cited Invention and Invention 1 are identical in that "at least one of the multiple communication terminals is connected to the blockchain network, and executes the broadcast".

6) In light of the examinations in 1) to 5), Invention 1 and the Cited Invention have the following corresponding feature and different features.

<Corresponding Feature>

A signal processing method including: a procedure of transmitting a signal for execution of a transaction on data to be shared in a group composed of multiple communication terminals connected to each other over a network, to at least one of the multiple communication terminals; and

a procedure of executing the transaction by broadcasting the transaction and an electronic signature of the transaction to a blockchain network composed of multiple nodes and connected to the network, and adding a block including information on the transaction to a blockchain, wherein

at least one of the multiple communication terminals is connected to the blockchain network, and executes the broadcast".

<Different Feature 1>

Regarding a signal "for execution of a transaction on data to be shared in a group composed of multiple communication terminals connected to each other over a network", Invention 1 uses an "approval request signal", while the Cited Invention does not specify an "approval request signal" while specifying that "the transaction is broadcast on the bitcoin network, where each network node (participant of the bitcoin network) validates and propagates the transaction until it reaches (almost) every node in the network".

<Different Feature 2>

Invention 1 includes "a procedure of receiving an approval signal from communication terminals corresponding to a certain ratio of the multiple communication terminals having received the approval request signal", and specifies that the process of "executing the transaction" "after receiving the approval signal". Cited Invention does not specify including the "procedure of receiving an approval signal from communication terminals corresponding to a certain ratio of the multiple communication terminals".

(B) Judgment

Different Features 1 and 2 are examined together.

Regarding the "approval request signal" in Invention 1, according to paragraphs 24 to 26 of the specification, a first user creates a transaction including details of data processing and approval condition required for starting the data processing (paragraph 24), as for the transaction, a private key 114_1 is generated in a first communication terminal 110_1 for transmitting the transaction, and a first electronic signature (ES1) is generated by encrypting the transaction TA with the private key 114_1 (paragraph 25), and the "approval request signal" is a signal including unencrypted (original) transaction TA, which has not been encrypted by the first communication terminal 110_1, and first electronic signature ES1 (paragraph 26).

Regarding the "approval signal" in Invention 1, according to paragraph 28 of the specification, users of the communication terminals 110 having received the transaction select an action to approve the transaction or an action not to approve the transaction, when the transaction is approved, the transaction is encrypted with a private key 114_2 generated in a second communication terminal 110_2 of a second user who approves the transaction, to generate an electronic signature ES2, and the "approval signal" is a signal including the original transaction TA and the electronic signature ES1 included in the approval request signal transmitted by the second communication terminal 110_2 from the first user and the electronic signature ES2 generated by the second communication terminal 110_2.

In light of the above, the "approval signal" is considered as a signal which is generated after a selection is made as to whether or not to approve a transaction, in a communication terminal having received an "approval request signal" including an unencrypted (original) transaction TA and a first electronic signature ES1. Meanwhile, the Cited Invention describes that the "transaction" is "signed", "the signed transaction is then broadcast on the bitcoin network, where each network node (participant of the bitcoin network) validates and propagates the transaction until it reaches (almost) every

node in the network; finally, the transaction is verified by a mining node", "funds sent to '3' bitcoin addresses" "require something more than the presentation of one public key hash and one private key signature as proof of ownership, the requirements are designated at the time the address is created, within the script", "the script requires one or more signatures to prove ownership and therefore spend funds, the bitcoin multi-signature feature is designed to require M signatures (also known as 'threshold') from a total of N keys, known as an M-of-N multi-sig", and that "multi-signature scripts" "set a condition where N public keys are recorded in the script and at least M of those must provide signatures to release the encumbrance, which is also known as an M-of-N scheme, where N is the total number of keys and M is the number of signatures required for validation, for example, a 2-of-3 multi-signature is one where three public keys are listed as potential signers and at least two of those must be used to create signatures for a valid transaction to spend the funds". However, the Cited Invention does not include any description about the selection as to whether or not to approve the transaction by a user of a communication terminal having received an approval request signal and receiving an approval signal based on the selection as described above. There is no description about the matter in other than the portions of Evidence A No. 1 cited in No. 4 2 (1). The procedure of transmitting/receiving the "approval request signal" and the "approval signal" is not disclosed in the A-3 Described matter, and was not a matter of well-known art before the filing of the application. It cannot be said that Invention 1 could have been easily made by a person skilled in the art based on Evidence A No. 1 and Evidence A No. 3.

(C) Summary

As described above, it cannot be said that Invention 1 could have been easily made by a person skilled in the art based on the matters described in Evidence A No. 1 and Evidence A No. 3.

B Regarding Invention 2

It cannot be said that Invention 2, which depends on Invention 1, could have been easily made by a person skilled in the art based on the matters described in Evidence A No. 1 and Evidence A No. 3, for the same reason as for Invention 1.

C Regarding Invention 5

It cannot be said that Invention 5, which is different only in category expression from Invention 1 basically, could have been easily made by a person skilled in the art

based on the matters described in Evidence A No. 1 and Evidence A No. 3, for the same reason as for Invention 1.

D Regarding Invention 6

It cannot be said that Invention 6, which depends on Invention 5, could have been easily made by a person skilled in the art based on the matters described in Evidence A No. 1 and Evidence A No. 3, for the same reason as for Invention 5.

E Summary

As judged above, it cannot be said that Invention 1, Invention 2, Invention 5, and Invention 6 could have been easily made by a person skilled in the art based on the matters described in Evidence A No. 1 and Evidence A No. 3.

(2) Regarding Article 36(6)(ii) of the Patent Act (relating to the notice of reasons for revocation)

The ambiguity stated in the notice of reasons for revocation about the "description 'approval of the received approval signal' in Claim 1", was clarified by the correction made by Correction C indicated in No. 2 1 (1) C.

The ambiguity stated in the notice of reasons for revocation about "'the node' indicated by the 'multiple nodes' described in Claim 1 cited by Claim 2, regarding the matter in Claim 2, 'the approval signal is generated by adding an electronic signature in the node'", was clarified by the correction made by Corrections A, B, and F indicated in No. 2 1 (1) A, B, and F.

The ambiguity stated in the notice of reasons for revocation about "the matter in Claim 3, 'the approval signals received in the procedure of receiving the approval signal do not reach a certain ratio of the multiple nodes'" and "the matter in Claim 4, 'the approval is determined by the total number of electronic signatures included in the received approval signals'", was clarified by the correction made by Correction G indicated in No. 2 1 (1) G.

The ambiguity stated in the notice of reasons for refusal about Claims 5 to 8 before the correction was clarified by the correction made by Corrections H to J and M and N indicated in No. 2 1 (2).

Therefore, the description of the scope of claims is clear.

(3) Regarding the opinion of the opponent

The opponent, Shigeki SHINOMORI alleges that the specification does not

include the effect, "In a configuration where a transaction is approved between communication terminals not participating in a blockchain network, as described in Corrected Invention 1, a heavy load to be imposed on nodes ([0041]) or hash calculation for satisfying the condition defined by the blockchain network ([0045], etc.) is not required for the communication terminal. Thus, as described in [0010], convenience of multiple users sharing data is secured, and the shared data can be safely managed or used", which is alleged by the patentee in "(b) Examination on the different feature" on p. 4. l. 5 in "Written opinion submitted on the same day as the written demand for correction", at the time of correcting, with the demand for correction, the "multiple nodes" before the correction to "multiple communication terminals", and thus Corrections A and F are to "substantially enlarge or alter the technical significance of the Invention according to Claims 1 to 8 before the correction". (Written opinion submitted on August 16, 2019 (hereinafter simply referred to as "Opponent opinion") p. 1-p. 9)

However, the matter, "heavy load to be imposed on nodes ([0041]) or hash calculation for satisfying the condition defined by the blockchain network ([0045], etc.) is not required for the communication terminal" due to approval of transaction between communication terminals not participating in the blockchain network, is not described in the specification. The correction from the "multiple nodes" to the "multiple communication terminals" does not violate correction requirements as indicated in No. 2 2. Therefore, the above allegation cannot be accepted.

The opponent, Shigeki SHINOMORI, presents Evidence A No. 9 as a new evidence for "(Reason 2)" in the Opponent opinion, and alleges that Patents 1, 2, 5 and 6 should be revoked under the provisions of Article 29-2 of the Patent Act. However, the argument is an addition of new reason to the grounds for opposition in the written opposition, and it is not acceptable.

The opponent, Shigeki SHINOMORI, adds Evidence A No. 11 as "(Reason 3)" in the Opposition opinion, and alleges that the Patents 1, 2, 5, and 6 should be revoked under the provisions of Article 29(2) of the Patent Act. However, Evidence A No. 11 also does not disclose a configuration relating to Different Features 1 and 2 indicated in No. 4 3 (1) A (A). The argument in not acceptable.

(4) Summary

Thus, it cannot be said that Inventions 1, 2, 5, and 6 could have been easily conceived by a person skilled in the art from the inventions disclosed in Evidence A No. 1 and Evidence A No. 3.

No. 5 Regarding the reasons for the opposition to the patent which are not accepted in the notice of reasons for revocation

1 Regarding Article 29(1)(iii) of the Patent act (Reason 1)

The opponent, Shigeki SHINOMORI, alleges in the written opposition that the inventions according to Claims 1 to 8 of the scope of the claims before the correction are inventions described in Evidence A No. 1, and the patent for the inventions should be revoked under the provisions of Article 29(1)(iii) of the Patent Act.

However, as indicated in No. 4 3 (1), it cannot be said that Inventions 1, 2, 5, and 6 are inventions described in Evidence A No. 1. The allegation of the opponent, Shigeki SHINOMORI, cannot be accepted.

2 Regarding Article 36(6)(ii) of the Patent Act (Reason 3)

The opponent, Shigeki SHINOMORI, alleges in the written opposition that the inventions according to Claims 5 to 8 of the scope of the claims before the correction are unclear. However, the procedures in the methods described in Claims 1 and 2, which are specified as information processing methods, would be comprehended by a person skilled in the art with the details described as the "First embodiment" in paragraphs 14 to 52 in the specification, and programs for implementing the procedures would be understood by a person skilled in the art without concrete flowcharts or descriptions about association with hardware. Thus, Inventions 5 and 6 are clear, and the description of the scope of claims satisfies the requirements stipulated in Article 36(6)(ii) of the Patent Act.

Therefore, the allegation of the opponent, Shigeki SHINOMORI, cannot be accepted.

3 Regarding Article 36(4)(i) (Reason 4)

The opponent, Shigeki SHINOMORI, alleges in the written opposition that the description of the detailed description of the invention in the specification is not clear and sufficient as to enable a person skilled in the art to implement the invention according to Claims 5 to 8 of the scope of claims before the correction. However, as with the above 2, it can be said that Inventions 5 and 6 would be easily implemented by a person skilled in the art who encounters the description of paragraphs 14 to 52 of the specification. Thus, the description of the specification satisfies the requirements stipulated in Article 36(4)(i) of the Patent Act.

Therefore, the allegation of the opponent, Shigeki SHINOMORI, cannot be

accepted.

4 Regarding Article 17-2(3) of the Patent Act (Reason 5)

The opponent, Shigeki SHINOMORI, alleges in the written opponent that the description in Claim 5 of the scope of the claims before the correction, "executing the transaction by broadcasting the transaction and an electronic signature of the transaction to a blockchain network and adding a block including information on the transaction to the blockchain", is an addition of new technical matter in light of the description in the specification, scope of claims, and drawings originally attached to the application (hereinafter referred to as "the originally attached specification").

The gist of the allegation is based on no concrete program configuration being disclosed in paragraphs 39 to 51 and FIGS. 4 and 5 of the originally attached specification, which yields the correction. However, as indicated in 3 and 4, a person skilled in the art could have easily implemented the matters described in paragraphs 39 to 51 and FIGS. 4 and 5 of the originally attached specification with programs without presenting concrete programs or implementation modes, and the above description cannot be considered as addition of new technical matter to the originally attached specification, etc. just because there is no clear indication about details of program.

Therefore, the allegation of the opponent, Shigeki SHINOMORI, cannot be accepted.

No. 6 Closing

As described above, the patent according to Claims 1, 2, 5, and 6 cannot be revoked due to the reasons for revocation described in the notice of reasons for revocation and reasons for the opposition to the patent described in the written opposition.

No other reasons for revoking the patent according to Claims 1, 2, 5, and 6 are found.

The patent according to Claims 3 and 4 and Claims 7 and 8 was deleted by the correction, as described above. Therefore, the opposition to the patent according to Claims 3 and 4 and Claims 7 and 8 made by the opponent, Shigeki SHINOMORI, has no subjects, and the opposition shall be dismissed under the provisions of Article 135 of the Patent Act which is applied mutatis mutandis in the provisions of Article 120-8(1) of the Patent Act.

Therefore, the decision shall be made as described in the conclusion.

November 27, 2019

Chief administrative judge: NAKAMA, Akira
Administrative judge: YAMAZAKI, Shinichi
Administrative judge: MATSUHIRA, Hide