A user device for performing an exchange of an electronic value with another user device is provided. The user device includes an agreement unit configured to acquire offer information corresponding to at least a first random number, from another user device, generate a second random number, generate session information, generate agreement object information, generate an electronic signature, and output agreement information including at least the agreement object information, the session information, and the electronic signature. The user device further includes a second confirmation unit and an abort request unit. The second confirmation unit is configured to acquire from another user device, first confirmation information, perform a verification on a predetermined verification item, and output second confirmation information. The abort request unit is configured to generate an electronic signature and output abort request information.
Fig. 2

USER DEVICE

10

START DEVICE

11

FIRST CONFIRMATION DEVICE

12

END DEVICE

13

COMMITMENT REQUEST DEVICE

14

ABORT PERFORMANCE DEVICE

15

COMMITMENT PERFORMANCE DEVICE

16

STORAGE DEVICE

101

ELECTRONIC VALUE
Fig. 4

THIRD-PARTY DEVICE

31  ABORT DETERMINATION DEVICE

33  ABORT PERMISSION DEVICE

32  COMMITMENT DETERMINATION DEVICE

34  COMMITMENT PERMISSION DEVICE
Fig. 5

START DEVICE 11 OF USER DEVICE 1

S101
GENERATE FIRST RANDOM NUMBER n1
S102
GENERATE FIRST SESSION INFORMATION s1 = n1
S103
DEFINE FIRST SESSION STATE AS "START"
S104
REFERENCE ELECTRONIC VALUE (V1)
S105
OUTPUT (O,V1)

AGREEMENT DEVICE 21 OF USER DEVICE 2

S106
ACQUIRE (O,V1)
S107
REFERENCE ELECTRONIC VALUE V2
S108
GENERATE SECOND RANDOM NUMBER n2
S109
GENERATE SECOND SESSION INFORMATION s2 = H(n2)
S110
DEFINE SECOND SESSION STATE AS "VALID"
S111
GENERATE AGREEMENT OBJECT INFORMATION
Ao = H(V1 | V2 | s1)
S112
GENERATE Sa = SigP2(Ao | s2)
S113
DELETE V2 FROM STORAGE DEVICE 20 AND OUTPUT A = (Ao, s2, Sa), V2, AND CertP2

FIRST CONFIRMATION DEVICE 12 OF USER DEVICE 1

S114
ACQUIRE A AND CertP2
S115
VERIFICATION
S116
DEFINE FIRST SESSION STATE AS "VALID"
S117
GENERATE Se = SigP1(s2)
S118
DELETE V1 FROM STORAGE DEVICE
S119
OUTPUT E1 = (s2, Se) AND CertP1

EXECUTE "ABORT REQUEST PROCESS" WHEN USER DEVICE 2 DETECTS ABNORMALITY
Fig. 6

SECOND CONFIRMATION DEVICE 22
OF USER DEVICE 2

S121
ACQUIRE E1 AND CertP1

S122
ABORT REQUEST PROCESS

S123
IS VERIFICATION SUCCESSFULLY DONE?

S124
NO

S125
YES

ERASE SECOND SESSION STATE

STORE V1 INTO STORAGE

OUTPUT E2 = n2

EXECUTE "COMMITMENT REQUEST PROCESS"
WHEN USER DEVICE 1 DETECTS ABNORMALITY

END DEVICE 13 OF USER DEVICE 1

S126
ACQUIRE E2

S127
IS VERIFICATION SUCCESSFULLY DONE?

S128
NO

S129
YES

COMMITMENT REQUEST PROCESS

ERASE FIRST SESSION STATE

STORE V2 INTO STORAGE
**Fig. 7**

**ABORT REQUEST DEVICE 23**
**OF USER DEVICE 2**

1. **DEFINE SECOND SESSION STATE AS "HOLD"**
   - S201

2. **GENERATE Sab = SigP2(Mab| s2)**
   - S202

3. **OUTPUT Rab = (Mab, s2, Sab) AND CertP2**
   - S203

**ABORT DETERMINATION DEVICE 31**
**OF THIRD-PARTY DEVICE 3**

4. **ACQUIRE Rab AND CertP2**
   - S204

5. **VERIFICATION**
   - S205

- **THIRD SESSION STATE = COMPLETE?**
  - YES ➔ **COMMITMENT PERMISSION PROCESS**
  - NO ➔ **MAKE THIRD SESSION STATE CORRESPONDING TO SECOND SESSION INFORMATION s2 TO DEFINE IT AS "ABORT"**

**ABORT PERMISSION PROCESS**

- S206
- S207
Fig. 8

**COMMITMENT REQUEST DEVICE 14**
**OF USER DEVICE 1**

- GENERATE $Sco = \text{SigP1}(Mco \mid s2)$
- OUTPUT $Rco = (Mco, s2, Sco) \text{ AND CertP1}$

**COMMITMENT DETERMINATION DEVICE 32**
**OF THIRD-PARTY DEVICE 3**

- ACQUIRE $Rco$ AND $\text{CertP1}$

**VERIFICATION**

- THIRD SESSION STATE = ABORT?
  - YES: ABORT PERMISSION PROCESS
  - NO: MAKE THIRD SESSION STATE CORRESPONDING TO SECOND SESSION INFORMATION $s2$ TO DEFINE IT AS "COMPLETE"

**COMMITMENT PERMISSION PROCESS**
Fig. 9

Abort Permission Device 33 of Third-Party Device 3

Abort Request Process

Abort Request Process

Abort Performance Device 24 of User Device 2

Abort Performance Device 15 of User Device 1

Commit Request Process

ACQUIRE AT AND CertP3

VERIFICATION

ERASE SECOND SESSION STATE

STORE V2 INTO STORAGE

ACQUIRE AT AND CertP3

VERIFICATION

ERASE FIRST SESSION STATE

STORE V1 INTO STORAGE
**Fig. 11**

<table>
<thead>
<tr>
<th>THIRD SESSION STATE</th>
<th>SECOND SESSION INFORMATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABORT</td>
<td>S2-1</td>
</tr>
<tr>
<td>COMPLETE</td>
<td>S2-2</td>
</tr>
<tr>
<td>COMPLETE</td>
<td>S2-3</td>
</tr>
</tbody>
</table>
This application is a divisional application of U.S. application Ser. No. 11/371,106, filed on Mar. 9, 2006, which claims benefit of priority from the prior Japanese Application No. 2005-071690 filed Mar. 14, 2005; the entire contents of which are incorporated herein by reference.

BACKGROUND OF THE INVENTION

Field of the Invention

The present invention relates to an electronic value exchange method for implementing fair exchange of electronic values (e.g., electronic money, electronic tickets, etc.) being information electronically representing values, and relates to a user device and a third-party device for such electronic value exchange.

There is the conventionally known technology concerning the electronic value exchange for safely exchanging electronic values (e.g., electronic money, electronic tickets, etc.) being information electronically representing values, and Japanese Patent Application Laid-Open No. 2004-341643 suggests the technology of implementing a fair trade in the electronic value exchange through the use of a third-party device. The “fair trade” stated herein means mutual exchange of electronic values meeting the condition that neither of two parties involved in the trade loses an electronic value of a trading object of its own, without gaining an electronic value as a consideration or without obtaining a guarantee for acquisition thereof.

SUMMARY OF THE INVENTION

In the technology of implementing the fair trade in the electronic value exchange through the use of the third-party device as described above, however, various pieces of control information are exchanged multiple times between the parties involved in the trade, and on such occasions information containing essentially unnecessary control information is sometimes transmitted and received, so as to lead possibly to an increase in volume of data transmitted and received. In addition, the third-party device has to manage states while no proposal on technology of appropriately managing states of multiple electronic value exchanges. As described above, the technology for implementing the fair trade in the electronic value exchange is not mature yet, and there are desires for further promotion of efficiency of processing and improvement in processing.

The present invention has been accomplished in order to solve the above problem and an object of the present invention is to provide an electronic value exchange method, a user device, and a third-party device capable of achieving further promotion of efficiency of processing and improvement in processing for assuring fairness in electronic value exchange.

An electronic value exchange method according to the present invention is a method of exchanging a first electronic value stored in a first user device, for a second electronic value stored in a second user device, the method being an electronic value exchange method of: letting the first user device execute an offer step including: a step of generating a first random number; and a step of outputting offer information being information corresponding to at least the first random number; letting the second user device execute an agreement step including: a step of acquiring the offer information; a step of generating a second random number; a step of generating session information corresponding to the second random number; a step of generating agreement object information corresponding to information containing at least the session information; a step of generating an electronic signature Se corresponding to information containing the agreement object information and the session information; and a step of outputting agreement information being information containing at least the agreement object information, the session information, and the electronic signature Se; letting the first user device execute a first confirmation step including: a step of acquiring the agreement information; a step of performing a verification on a predetermined verification item; a step of generating an electronic signature Se for information containing the session information; and a step of outputting first confirmation information being information containing at least the session information and the electronic signature Se; letting the second user device execute a second confirmation step including: a step of acquiring the first confirmation information; a step of performing a verification on a predetermined verification item; a step of outputting second confirmation information being information containing the second random number; and letting the first user device execute an end step including: a step of acquiring the second confirmation information; a step of performing a verification on a predetermined verification item; wherein the second user device executes an abort request step including: a step of generating an electronic signature for information containing information indicating an abort request, and the session information; and a step of outputting abort request information being information containing the information indicating the abort request, the session information, and the electronic signature; and wherein a third-party device executes an abort determination step including: a step of acquiring the abort request information; a step of performing a verification on a predetermined verification item; and a step of determining whether a session state corresponding to the session information is defined as commit, and, if the session state is not defined as commit, making the session state corresponding to the session information as to define the session state as abort.

In the above electronic value exchange method, the second user device generates the electronic signature for the information containing the session information and the information indicating the abort request, using only the session information contained in the agreement information, instead of the agreement information, and outputs the abort request information being the information containing the session information, the information indicating the abort request, and the electronic signature; therefore, transmission/reception can be performed without essentially unnecessary control information, so as to avoid an increase in volume of data transmitted and received. In addition, the third-party device makes the session state corresponding to the session information so as to define the session state as abort, and is thus able to manage states while appropriately discriminating a plurality of concurrent electronic value exchanges. In this manner, the method achieves further promotion of efficiency of processing and improvement in processing for assuring fairness in the electronic value exchange.
The above electronic value exchange method is preferably configured as follows: when the session state is defined as abort, the third-party device executes an abort permission step including: a step of generating an electronic signature for information containing information indicating an abort permission, and the session information; and a step of outputting abort permission information being information containing the information indicating the abort permission, the session information, and the electronic signature; and the first user device further executes an abort performance step including: a step of acquiring the abort permission information; and a step of performing a verification on a predetermined verification item. In this manner, the third-party device generates the electronic signature for the information containing the session information and the information indicating the abort permission, using only the session information contained in the agreement information, instead of the agreement information, and outputs the abort permission information being information containing the information indicating the abort permission, the session information, and the electronic signature, to the first user device; therefore, the transmission/reception can be performed between the third-party device and the first user device, without essentially unnecessary control information, so as to avoid an increase in volume of transmitted and received data.

The above electronic value exchange method is preferably configured as follows: when the session state is defined as abort, the third-party device executes an abort permission step including: a step of generating an electronic signature for information containing information indicating an abort permission, and the session information; and a step of outputting abort permission information being information containing the information indicating the abort permission, the session information, and the electronic signature; and the first user device further executes an abort performance step including: a step of acquiring the abort permission information; and a step of performing a verification on a predetermined verification item. In this manner, the third-party device generates the electronic signature for the information containing the session information and the information indicating the abort permission, using only the session information contained in the agreement information, instead of the agreement information, and outputs the abort permission information being information containing the information indicating the abort permission, the session information, and the electronic signature, to the second user device; therefore, the transmission/reception can be performed between the third-party device and the second user device, without essentially unnecessary control information, so as to avoid an increase in volume of transmitted and received data.

Another electronic value exchange method according to the present invention is a method of exchanging a first electronic value stored in a first user device, for a second electronic value stored in a second user device, the method being an electronic value exchange method of: letting the first user device execute an offer step including: a step of generating a first random number; and a step of outputting offer information being information corresponding to at least the first random number; letting the second user device execute an agreement step including: a step of acquiring the offer information; a step of generating a second random number; a step of generating session information corresponding to the second random number; a step of generating agreement object information corresponding to information containing at least the session information; a step of generating an electronic signature Sa corresponding to information containing the agreement object information and the session information; and a step of outputting agreement information containing information at least the agreement object information, the session information, and the electronic signature Sa; and the first user device executes a first confirmation step including: a step of acquiring the agreement information; a step of performing a verification on a predetermined verification item; a step of generating an electronic signature Sa for information containing at least the session information; a step of outputting first confirmation information containing information at least the session information, and the electronic signature Sa; and a second user device executes a second confirmation step including: a step of acquiring the first confirmation information; a step of performing a verification on a predetermined verification item; and a step of outputting second confirmation information containing information at least the session information, and the electronic signature Sa; and the first user device executes an end step including: a step of acquiring the second confirmation information; and a step of performing a verification on a predetermined verification item; wherein the first user device executes a commitment request step including: a step of generating an electronic signature for information containing information indicating a commitment request, the session information, and the electronic signature; and wherein a third-party device executes a commitment determination step including: a step of acquiring the commitment request information; a step of performing a verification on a predetermined verification item; and a step of determining whether a session state corresponding to the session information is defined as abort, making the session state corresponding to the session information to define the session state as commit.
information being information containing the information indicating the commitment permission, the session information, and the electronic signature; and the first user device further executes a commitment performance step including: a step of acquiring the commitment permission information; and a step of performing a verification on a predetermined verification item. In this manner, the third-party device generates the electronic signature for the information containing the session information and the information indicating the commitment permission, using only the session information contained in the agreement information, instead of the agreement information, and outputs the commitment permission information being the information containing the session information, the information indicating the commitment permission, and the electronic signature, to the first user device; therefore, the transmission/reception can be performed between the third-party device and the first user device, without essentially unnecessary control information, so as to avoid an increase in volume of transmitted and received data.

[0013] The above electronic value exchange method is preferably configured as follows: when the session state is defined as commit, the third-party device executes a commitment permission step including: a step of generating an electronic signature for information containing information indicating a commitment permission, and the session information; and a step of outputting commitment permission information containing the information indicating the commitment permission, the session information, and the electronic signature; and the second user device further executes a commitment performance step including: a step of acquiring the commitment permission information; and a step of performing a verification on a predetermined verification item. In this manner, the third-party device generates the electronic signature for the information containing the session information and the information indicating the commitment permission, using only the session information contained in the agreement information, instead of the agreement information, and outputs the commitment permission information being the information containing the session information, the information indicating the commitment permission, and the electronic signature, to the second user device; therefore, the transmission/reception can be performed between the third-party device and the second user device, without essentially unnecessary control information, so as to avoid an increase in volume of transmitted and received data.

[0014] Incidentally, the present invention permits various processing steps to be applied as processing steps before arrival at the processing steps associated with the abort request and the commitment request.

[0015] For example, the aforementioned electronic value exchange method associated with the abort request can be described as stated below. “Second session information” in the description below corresponds to the “session information” in the aforementioned aspect of the present invention, and “start information” to the “offer information” in the aforementioned aspect of the invention.

[0016] Another electronic value exchange method according to the present invention is a method of exchanging a first electronic value stored in a first user device, for a second electronic value stored in a second user device, the method being an electronic value exchange method of: letting the first user device execute a start step including: a step of generating a first random number; a step of generating first session information corresponding to the first random number; and a step of outputting start information being information containing the first session information, and a first electronic value; letting the second user device execute an agreement step including: a step of acquiring the start information and the first electronic value; a step of generating a second random number; a step of generating second session information corresponding to the second random number; a step of generating agreement object information corresponding to the first electronic value, a second electronic value, and the first session information; a step of generating an electronic signature Sa for information containing the agreement object information and the second session information; and a step of deleting the second electronic value, and outputting agreement information being information containing the agreement object information, the second session information, and the electronic signature Sa, and the second electronic value; letting the first user device further execute a first confirmation step including: a step of acquiring the agreement information and the second electronic value; a first verification step of performing a verification on a predetermined verification item; a step of generating an electronic signature Se for information containing the second session information; a step of deleting the first electronic value; and a step of outputting first confirmation information being information containing the second session information and the electronic signature Se; letting the second user device further execute a second confirmation step including: a step of acquiring the first confirmation information; a second verification step of performing a verification on a predetermined verification item; a step of storing the first electronic value; and a step of outputting second confirmation information being information containing the second random number; and letting the first user device further execute an end step including: a step of acquiring the second confirmation information; a third verification step of performing a verification on a predetermined verification item; and a step of storing the second electronic value; wherein the second user device executes an abort request step including: a step of generating an electronic signature Sub for information containing information indicating an abort request, and the second session information; and a step of outputting abort request information being information containing the information indicating the abort request, the second session information, and the electronic signature Sub; and wherein a third-party device executes an abort determination step including: a step of acquiring the abort request information; a fourth verification step of performing a verification on a predetermined verification item; and a step of determining whether a session state corresponding to the second session information is defined as commit, and, if the session state is not defined as commit, making the session state corresponding to the second session information so as to define the session state as abort.

[0017] Similarly, the aforementioned electronic value exchange method associated with the commitment request can also be described as follows. Another electronic value exchange method according to the present invention is a method of exchanging a first electronic value stored in a first user device, for a second electronic value stored in a second user device, the method being an electronic value exchange method of: letting the first user device execute a start step including: a step of generating a first random number; a step of generating first session information corresponding to the first random number; and a step of outputting start information being information containing the first session information.
tion, and a first electronic value; letting the second user device execute an agreement step including: a step of acquiring the start information and the first electronic value; a step of generating a second random number; a step of generating second session information corresponding to the second random number; a step of generating agreement object information corresponding to the first electronic value, a second electronic value, and the first session information; a step of generating an electronic signature Sa for information containing the agreement object information and the second session information; and a step of deleting the second electronic value, and outputting agreement information being information containing the agreement object information, the second session information, and the electronic signature Sa, and the second electronic value; letting the first user device further execute a first confirmation step including: a step of acquiring the agreement information and the second electronic value; a first verification step of performing a verification on a predetermined verification item; a step of generating an electronic signature Se for information containing the second session information; a step of deleting the first electronic value; and a step of outputting first confirmation information being information containing the second session information and the electronic signature Se; letting the second user device further execute a second confirmation step including: a step of acquiring the first confirmation information; a second verification step of performing a verification on a predetermined verification item; a step of storing the first electronic value; and a step of outputting second confirmation information being information containing the second random number; and letting the first user device further execute an end step including: a step of acquiring the second confirmation information; a third verification step of performing a verification on a predetermined verification item; and a step of storing the second electronic value; wherein the first user device executes a commitment request step including: a step of generating an electronic signature Sco for information containing information indicating a commitment request, and the second session information; and a step of outputting commitment request information being information containing the information indicating the commitment request, the second session information, and the electronic signature Sco; and wherein a third-party device executes a commitment determination step including: a step of acquiring the commitment request information; a fifth verification step of performing a verification on a predetermined verification item; and a step of determining whether a session state corresponding to the second session information is defined as abort, and, if the session state is not defined as abort, making the session state corresponding to the second session information so as to define the session state as commit.

[0018] Incidentally, the present invention can also be described as follows, as an aspect of the invention associated with the second user device. A user device according to the present invention is a user device for performing an exchange with another user device to exchange a first electronic value stored in said another user device, for a second electronic value stored in the user device itself, the user device comprising: agreement means for acquiring offer information being information corresponding to at least a first random number, from said another user device, generating a second random number, generating session information corresponding to the second random number, generating agreement object information corresponding to information containing at least the session information, generating an electronic signature Sa for information containing the agreement object information and the session information, and outputting agreement information being information containing at least the agreement object information, the session information, and the electronic signature Sa; and second confirmation means for acquiring from said another user device, first confirmation information being information containing an electronic signature Se for information containing the session information, and said session information, performing a verification on a predetermined verification item, and outputting second confirmation information being information containing the second random number; the user device comprising abort request means for generating an electronic signature for information containing information indicating an abort request, and the session information, and for outputtingabort request information being information containing the information indicating the abort request, the session information, and the electronic signature.

[0019] The present invention can also be described as follows, as an aspect of the invention associated with the first user device. A user device according to the present invention is a user device for performing an exchange with another user device to exchange a second electronic value stored in said another user device, for a first electronic value stored in the user device itself, the user device comprising: offer means for generating a first random number, and outputting offer information being information corresponding to at least the first random number; first confirmation means for acquiring from said another user device, agreement information being information containing at least an electronic signature Sa for information containing agreement object information corresponding to information containing session information corresponding to a second random number, and the session information, the agreement object information, and the session information, performing a verification on a predetermined verification item, generating an electronic signature Se for information containing the session information, and outputting first confirmation information being information containing at least the session information and the electronic signature Se; and second confirmation means for acquiring from said another user device, electronic signature being information containing information indicating a commitment request, the session information, and for outputting commitment request information containing the information indicating the commitment request, the session information, and the electronic signature.

[0020] The present invention can also be described as follows, as an aspect of the invention associated with the third-party device for performing the abort determination. A third-party device according to the present invention is a third-party device used in a system for exchanging a first electronic value stored in a first user device, for a second electronic value stored in a second user device, said third-party device being used in the system configured as follows: the first user device executes an offer step of generating a first random number, and outputting offer information being information corresponding to at least the first random number; the second user device executes an agreement step of acquiring the offer information, generating a second random number, generating
session information corresponding to the second random number, generating agreement object information corresponding to information containing at least the session information, generating an electronic signature $S_a$ for information containing the agreement object information and the session information, and outputting agreement information being information containing at least the agreement object information, the session information, and the electronic signature $S_a$; the first user device executes a first confirmation step of acquiring the agreement information, performing a verification on a predetermined verification item, generating an electronic signature $S_e$ for information containing the session information, and outputting first confirmation information being information containing at least the session information and the electronic signature $S_e$; the second user device executes a second confirmation step of acquiring the first confirmation information, performing a verification on a predetermined verification item, and outputting second confirmation information being information containing the session information and the electronic signature $S_e$; the second user device executes a second confirmation step of acquiring the first confirmation information, performing a verification on a predetermined verification item, and outputting second confirmation information being information containing the second random number; and the first user device executes an end step of acquiring the second confirmation information, and performing a verification on a predetermined verification item; the third-party device comprising abort determination means configured so that when the second user device executes an abort request step of generating an electronic signature for information containing information indicating an abort request, and the session information, and outputting abort request information being information containing the information indicating the abort request, the session information, and the electronic signature, the abort determination means acquires the abort request information, performs a verification on a predetermined verification item, and determines whether a session state corresponding to the session information is defined as commit, and, if the session state is not defined as commit, the abort determination means makes the session state corresponding to the session information so as to define the session state as abort.

The third-party device according to the present invention is preferably configured as follows: it further comprises abort permission means configured so that when the session state is defined as abort, the abort permission means generates an electronic signature for information containing information indicating an abort permission, and the session information, and outputs abort permission information being information containing the information indicating the abort permission, the session information, and the electronic signature.

The present invention can also be described as follows, as an aspect of the invention associated with the third-party device for performing the commitment determination. A third-party device according to the present invention is a third-party device used in a system for exchanging a first electronic value stored in a first user device, for a second electronic value stored in a second user device, said third-party device being used in the system configured as follows: the first user device executes an offer step of generating a first random number, and outputting offer information being information corresponding to at least the first random number; the second user device executes an agreement step of acquiring the offer information, generating a second random number, generating session information corresponding to the second random number, generating agreement object information corresponding to information containing at least the session information, generating an electronic signature $S_a$ for information containing the agreement object information and the session information, and outputting agreement information being information containing at least the agreement object information, the session information, and the electronic signature $S_a$; the first user device executes a first confirmation step of acquiring the agreement information, performing a verification on a predetermined verification item, generating an electronic signature $S_e$ for information containing the session information, and outputting first confirmation information being information containing at least the session information and the electronic signature $S_e$; the second user device executes a second confirmation step of acquiring the first confirmation information, performing a verification on a predetermined verification item, and outputting second confirmation information being information containing the second random number; and the first user device executes an end step of acquiring the second confirmation information, and performing a verification on a predetermined verification item; the third-party device comprising abort determination means configured so that when the first user device executes a commitment request step of generating an electronic signature for information containing information indicating a commitment request, and the session information, and outputting commitment request information being information containing the information indicating the commitment request, the session information, and the electronic signature, the commitment determination means acquires the commitment request information, performs a verification on a predetermined verification item, and determines whether a session state corresponding to the session information is defined as abort, and, if the session state is not defined as abort, the commitment determination means makes the session state corresponding to the session information so as to define the session state as commit.

The third-party device according to the present invention is preferably configured as follows: it further comprises commitment permission means configured so that when the session state is defined as commit, the commitment permission means generates an electronic signature for information containing information indicating a commitment permission, and the session information, and outputs commitment permission information being information containing the information indicating the commitment permission, the session information, and the electronic signature.

The present invention successfully achieves further promotion of efficiency of processing and improvement in processing for assuring fairness in the electronic value exchange.

**BRIEF DESCRIPTION OF THE DRAWINGS**

A more complete appreciation of the invention and many of the attendant advantages thereof will be readily obtained as the same becomes better understood by reference to the following detailed description when considered in connection with the accompanying drawings, wherein:

**FIG. 1** is an illustration showing a configuration of an electronic value exchange system in an embodiment of the present invention.

**FIG. 2** is an illustration showing a configuration of user device 1.

**FIG. 3** is an illustration showing a configuration of user device 2.

**FIG. 4** is an illustration showing a configuration of third-party device 3.
FIG. 5 is an illustration showing a procedure in the first stage of main processing.

FIG. 6 is an illustration showing a procedure in the second stage of main processing.

FIG. 7 is an illustration showing a procedure of an abort request process.

FIG. 8 is an illustration showing a procedure of a commitment request process.

FIG. 9 is an illustration showing a procedure of an abort permission process.

FIG. 10 is an illustration showing a procedure of a commitment permission process.

FIG. 11 is an illustration showing an example of a management table of third session states.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Referring now to the drawings, wherein like reference numerals designate identical or corresponding parts throughout the several views.

Embodiments of the present invention will be described below with reference to the drawings.

FIG. 1 is an illustration showing an overall configuration of an electronic value exchange system according to the present invention. FIG. 1 shows a case where user device 1 is connected through communication means 4 to user device 2 and where an exchange transaction is performed so as to erase electronic value 101 stored in user device 1 and store it into user device 2 and further to erase electronic value 201 stored in user device 2 and store it into user device 1, through communication means 4. Each of the user devices 1, 2 is comprised of a portable terminal equipped with a tamper-resistant device (an IC card or the like) at a predetermined location (i.e., an aggregate of a tamper-resistant device and a portable terminal).

Furthermore, the system shown in FIG. 1 includes third-party device 3 connected through communication means 5 to the user devices 1 and 2. If the user device 1 and user device 2 find an abnormality in performance of the exchange transaction, e.g., detection of a blackout of communication means 4, the user device 1 or 2 finding the abnormality transmits information according to a point of occurrence of the abnormality, to the third-party device 3.

The third-party device 3 determines whether the exchange transaction is to be aborted or committed, according to the transmitted information, and returns information according to the determination result to the source user device. The user device, receiving the information returned from the third-party device, performs either an operation of aborting the exchange transaction according to the determination result or returning the electronic value to the original location, or an operation of deeming the exchange transaction as having been committed and storing the electronic value as an exchange object.

The communication means 4 herein is a temporary communication means, and does not have to establish a constant connection between the user devices 1 and 2. The communication means 5 is also a temporary communication means and does not have to establish a constant connection between the user devices and the third-party device. The communication means 4 and 5 may be provided by a single communication network.

Next, configurations and operations of the respective devices will be described in detail.

FIG. 2 is an illustration showing a configuration of user device 1 in an embodiment of the present invention. The user device 1 shown in the same figure has storage device 10, start device 11, first confirmation device 12, end device 13, commitment request device 14, abort performance device 15, and commitment performance device 16. As described previously, the user device 1 is comprised, for example, of a portable terminal equipped with a tamper-resistant device (an IC card or the like) at a predetermined location, and the storage device 10 is comprised of a memory of the tamper-resistant device. For this reason, data stored in the storage device 10 is prevented from being tampered.

FIG. 3 is an illustration showing a configuration of user device 2 in an embodiment of the present invention. The user device 2 shown in the same figure has storage device 20, agreement device 21, second confirmation device 22, abort request device 23, abort performance device 24, and commitment performance device 25. As described previously, the user device 2 is comprised, for example, of a portable terminal equipped with a tamper-resistant device (an IC card or the like) at a predetermined location, and the storage device 20 is comprised of a memory of the tamper-resistant device. For this reason, data stored in the storage device 20 is prevented from being tampered.

FIG. 4 is an illustration showing a configuration of third-party device 3 in an embodiment of the present invention. The third-party device 3 shown in the same figure has abort determination device 31, commitment determination device 32, abort permission device 33, and commitment permission device 34. Typically, the third-party device 3 herein is comprised of a server connected to a public network such as the Internet, and awaits a connection from a user device.

The communication means 4 in FIG. 1 can be two IC card reader/writers mutually connected through a communication medium such as an infrared communication line or the Internet. The communication means 5 can be an IC card reader/writer or the like connected through a communication medium such as the Internet to the third-party device 3.

For electronic value 101 stored in storage device 10, for electronic value 201 stored in storage device 20, using the devices of the configurations as described above.

It is assumed in the following description that the user device 1 preliminarily retains a public key certificate CertP1 containing a public key P1, the user device 2 a public key certificate CertP2 containing a public key P2, and the third-party device 3 a public key certificate CertP3 containing a public key P3. Here the public key certificates CertP1, CertP2 are issued by a user device certificate authority being a first certificate authority, and the public key certificate CertP3 is a public key certificate issued by a third-party device certificate authority being a second certificate authority.

An exchange of electronic values by this method is started by executing the main processing shown in FIGS. 5 and 6, as an example. If an abnormality is found in performance of the main processing, execution of the main processing is suspended to branch into an abort request process or into a commitment request process. After execution of the abort request process and the commitment request process, the execution branches into an abort performance process or into a commitment performance process according to a state of the third-party device. These branching conditions will be described in the following description of processing. It is,
however, noted that the main processing shown in FIGS. 5 and 6 is just an example and that the processing associated with recovery of fairness according to the present invention is also applicable to other modes of main processing.

[0051] [Main Processing]

[0052] The procedure of main processing will be described with reference to FIGS. 5 and 6.

[0053] First, the start device 11 of user device 1 executes a process below.

[0054] (step 101) It generates a first random number r1. It is noted that "s", e.g., in "sI01" described in FIGS. 5 to 10 means "step".

[0055] (step 102) It generates first session information s1 corresponding to the first random number r1. At this step, for example, the first session information s1 equal to the first random number r1 is generated.

[0056] (step 103) It defines a first session state as "start". For example, information indicating "start" is stored in correspondence to the "first session state".

[0057] (step 104) It references electronic value V1 from the storage device 10. In the description hereinafter, the electronic value V1 is assumed to be an electronic value V2.

[0058] (step 105) It outputs the start information O and the electronic value V1 equivalent to the first session information s1, i.e., (O,V1) to the communication means 4. The start information O corresponds to the "offer information" in the present invention.

[0059] The communication means 4 transfers (O,V1) from the user device 1 to the user device 2.

[0060] Subsequently, the agreement device 21 of the user device 2 executes a process below.

[0061] (step 106) It acquires the start information O and electronic value V1 from the communication means 4.

[0062] (step 107) It references the electronic value V2 from the storage device 20. In the description below, the electronic value V2 is assumed to be an electronic value V3.

[0063] (step 108) It generates a second random number r2.

[0064] (step 109) Using the one-way function H( ), it generates second session information s2=H(r2) corresponding to the second random number r2. The second session information s2 corresponds to the "session information" in the present invention.

[0065] (step 110) It defines a second session state as "start". For example, information indicating "start" is stored in correspondence to the "second session state".

[0066] (step 111) Using the one-way function H( ), it generates agreement object information Ao=H(V1||V2||s1) corresponding to the electronic values V1, V2 and the first session information s1. The notation "||" herein represents a concatenation.

[0067] (step 112) It generates an electronic signature Sa=SigP2(Ao||s2) for the information containing the agreement object information Ao and the second session information s2. Here SigP2( ) is a signature function to generate an electronic signature that can be verified by public key P2. Examples of this signature function to be applied include ESIGN, ECDSA, and so on.

[0068] (step 113) It deletes the electronic value V2 from the storage device 20, and outputs the agreement information A=(Ao,s2,sa), the electronic value V2, and the public key certificate CertP2 to the communication means 4. Here the agreement information A is information containing the agreement object information Ao, the second session information s2, and the electronic signature Sa.

[0069] Then the communication means 4 transfers the agreement information A, the electronic value V2, and the public key certificate CertP2, i.e., (A,V2,CertP2) from the user device 2 to the user device 1.

[0070] Subsequently, the first confirmation device 12 of the user device 1 executes a process below.

[0071] (step 114) It acquires the agreement information A and the public key certificate CertP2 from the communication means 4.

[0072] (step 115) It performs a verification on the items below and, if it results in a failure even about only one item, the subsequent processing is interrupted.

[0073] The first session state is "start".

[0074] The public key certificate CertP2 is a valid public key certificate issued by the user certificate authority.

[0075] The electronic signature Sa=SigP2(Ao||s2) is successfully verified by the public key P2.

[0076] The agreement object information Ao=H(V1||V2||s1) is approved.

[0077] (step 116) It defines the first session state as "valid".

[0078] (step 117) It generates an electronic signature Se=SigP1(s2) for the information containing the second session information s2. Here SigP1( ) is a signature function to generate an electronic signature that can be verified by the public key P1.

[0079] (step 118) It deletes the electronic value V1 from the storage device 10.

[0080] (step 119) It outputs first confirmation information E1=(s2,Se) being information containing the second session information s2 and the electronic signature Se, and the public key certificate CertP1 to the communication means 4.

[0081] Then the communication means 4 transfers the first confirmation information E1 and the public key certificate CertP1, i.e., (E1,CertP1) from the user device 1 to the user device 2. When this transfer is not carried out within a fixed time, to result in detection of an abnormality, e.g., a time-out, the user device 2 interrupts the subsequent processing and executes the "abort request process".

[0082] Subsequently, the second confirmation device 22 of the user device 2 executes a process below.

[0083] (step 121) It acquires the first confirmation information E1 and the public key certificate CertP1 from the communication means 4.

[0084] (step 122) It performs a verification on the following items and, if the verification results in a failure even about only one item, it interrupts the subsequent processing and executes the "abort request process".

[0085] The second session state is "valid".

[0086] The public key certificate CertP1 is a valid public key certificate issued by the user certificate authority.

[0087] The electronic signature Se=SigP1(s2) is successfully verified by the public key P1.

[0088] The second session information s2 contained in the first confirmation information E1 is the same as the second session information s2 contained in the agreement information A.

[0089] (step 123) It deletes the second session state.

[0090] (step 124) It stores the electronic value V1 into the storage device 20.

[0091] (step 125) It outputs second confirmation information being information containing the second random number, to the communication means 4. At this step, for example, it outputs the second confirmation information E2 equal to the second random number r2, to the communication means 4.
[0092] Then the communication means 4 transfers the second confirmation information E₂ from the user device 2 to the user device 1. If this transfer is not carried out within a fixed time, to result in detection of an abnormality, e.g., a time-out, the user device 1 interrupts the subsequent processing and executes the “commitment request process”.

[0093] Subsequently, the end device of the user device 1 executes a process below.

[0094] (step 126) It acquires the second confirmation information E₂ from the communication means 4.

[0095] (step 127) It performs a verification on the following items and, if the verification results in a failure even about only one item, it interrupts the subsequent processing and executes the “commitment request process”.

[0096] The third session state is “valid”.

[0097] The second session information s₂=H(n₂) is approved.

[0098] (step 128) It erases the first session state.

[0099] (step 129) It stores the electronic value V₂ into the storage device 10.

[0100] After the main processing consisting of the procedure from step 101 to step 129 described above has been executed to the end, the processing is terminated. At this point, the electronic value V₂ (i.e., electronic value 201) is stored in the storage device 10 of the user device 1, and the electronic value V₁ (i.e., electronic value 101) in the storage device 20 of the user device 2; therefore, the aforementioned electronic values are exchanged.

[0101] (Abort Request Process)

[0102] Next, the procedure of the “abort request process”, which is executed by the user device 2 when one of the predetermined cases is met in the main processing, will be described with reference to FIG. 7.

[0103] First, the abort request device 23 of the user device 2 executes a process below.

[0104] (step 201) It defines the second session state as “hold”.

[0105] (step 202) It generates an electronic signature Sab→Sigₚ₂(Mab|s₂) for information containing information Mab indicating an abort request, and the second session information s₂.

[0106] (step 203) It outputs the communication means 5, abort request information Rab→(Mab,s₂,Sab) being information containing the information Mab indicating the abort request, the second session information s₂, and the electronic signature Sab, and the public key certificate Certₚ₂.

[0107] The communication means 5 transfers the abort request information Rab and the public key certificate Certₚ₂ from the user device 2 to the third-party device 3. Then the abort determination device 31 of the third-party device 3 executes a process below.

[0108] (step 204) It acquires the abort request information Rab and the public key certificate Certₚ₂ from the communication means 5.

[0109] (step 205) It performs a verification on the following items and, if the verification results in a failure even about only one item, it interrupts the subsequent processing.

[0110] The public key certificate Certₚ₂ is a valid public key certificate issued by the user certificate authority.

[0111] The electronic signature Sab→Sigₚ₂(Mab|s₂) is successfully verified by the public key P₂.

[0112] (step 206) It references a third session state corresponding to the second session information s₂ and branches the processing according to the content thereof. The “third session state” corresponds to the “session state” according to the present invention.

[0113] If the third session state is defined as “commit”, the flow goes to the commitment permission process by the commitment permission device 34 in FIG. 10 which will be described later.

[0114] If the third session state is not defined as “commit”, step 207 below is executed.

[0115] (step 207) It makes the third session state corresponding to the second session information s₂ so as to define the third session state as “abort”. For example, as shown in FIG. 11, the third session state is made corresponding to the second session information s₂-1 to be defined as “abort”. After that, the flow goes to the abort permission process by the abort permission device 33 in FIG. 9 which will be described later.

[0116] After commitment of the processing according to the above procedure, the abort request process is terminated.

[0117] At the above steps 202, 203, the abort request device 23 generates the electronic signature Sab for the information containing the second session information s₂ and the information Mab indicating the abort request, using only the second session information s₂ contained in the agreement information A, instead of the agreement information A, and outputs the abort request information Rab being information containing the second session information s₂, the information Mab indicating the abort request, and the electronic signature Sab; therefore, the transmission/reception can be performed without essentially unnecessary control information, so as to avoid an increase in volume of transmitted and received data and achieve promotion of efficiency of the processing.

[0118] At step 207 the abort determination device 31 makes the third session state corresponding to the second session information s₂ so as to define the third session state as “abort”; therefore, the third-party device is able to manage states while appropriately distinguishing a plurality of concurrent electronic value exchanges as shown in FIG. 11.

[0119] [Commitment Request Process]

[0120] Next, the procedure of the “commitment request process”, which is executed by the user device 1 when one of the predetermined cases is met in the main processing, will be described with reference to FIG. 8. The commitment request process is executed according to the procedure below.

[0121] The commitment request device 14 of the user device 1 executes a process below.

[0122] (step 301) It generates an electronic signature Sco→Sigₚ₁(Mco|s₂) for information containing information Mco indicating a commitment request, and the second session information s₂.

[0123] (step 302) It outputs commitment request information Rco→(Mco,s₂,Sco) being information containing the information Mco indicating the commitment request, the second session information s₂, and the electronic signature Sco, and the public key certificate Certₚ₁ to the communication means 5.

[0124] The communication means 5 transfers the commitment request information Rco and the public key certificate Certₚ₁ from the user device 1 to the third-party device 3. Then the commitment determination device 32 of the third-party device 3 executes a process below.

[0125] (step 303) It acquires the commitment request information Rco and the public key certificate Certₚ₁ from the communication means 5.
It performs a verification on the following items and, if the verification results in a failure even about only one item, it interrupts the subsequent processing.

The public key certificate CertP1 is a valid public key certificate issued by the user certificate authority.

The electronic signature Sco=SigP1(Mc0||s2) is successfully verified by the public key P1.

It references the third session state corresponding to the second session information s2 and branches the processing according to the content thereof.

If the third session state is defined as "abort", the flow proceeds to the abort permission process by the abort permission device 33 in Fig. 9 which will be described later.

If the third session state is not defined as "abort", step 306 below is executed.

It makes the third session state corresponding to the second session information s2 so as to define the third session state as "commit". For example, as shown in Fig. 11, the third session state is made corresponding to the second session information s2 to be defined as "commit". After that, the flow goes to the commitment permission process by the commitment permission device 34 in Fig. 10 which will be described later.

After commitment of the processing according to the above procedure, the commitment request process is terminated.

In the above steps 301, 302, the commitment request device 14 generates the electronic signature Sco for the information containing the second session information s2 and the information Mc0 indicating the commitment request, using only the second session information s2 contained in the agreement information A, instead of the agreement information A, and outputs the commitment request information Sco containing the second session information s2, the information Mc0 indicating the commitment request, and the electronic signature Sco; therefore, the transmission/reception can be performed without essentially unnecessary control information, so as to avoid an increase in volume of transmitted and received data and achieve promotion of efficiency of processing.

At the step 306, the commitment determination device 32 makes the third session state corresponding to the second session information s2 so as to define the third session state as "commit"; therefore, the third-party device is able to manage states while appropriately distinguishing a plurality of concurrent electronic value exchanges as shown in Fig. 11.

[Abort Permission Process]

Next, the procedure of the abort permission process, which is executed when one of the predetermined cases is met in the commitment request process or in the abort request process, will be described with reference to Fig. 9.

The abort permission device 33 of the third-party device 3 executes a process below.

It generates an electronic signature Sabort=SigP3(abort||s2) for information containing information abort indicating an abort permission, and the second session information s2.

It outputs abort permission information AT=(abort,s2,Sabort) being information containing the information abort indicating the abort permission, the second session information s2, and the electronic signature Sabort, and the public key certificate CertP3 to the communication means 5.

The communication means 5 transfers the abort permission information AT and the public key certificate CertP3 from the third-party device 3 to the user device 1 or to the user device 2. To which the information is to be transferred is determined according to the following conditions.

If the preceding process is the commitment request process, the information is transferred to the user device 1.

If the preceding process is the abort request process, the information is transferred to the user device 2. When the user device 1 is the one receiving the abort permission information AT and the public key certificate CertP3, the abort performance device 15 of the user device 1 executes a process below.

It acquires the abort permission information AT and the public key certificate CertP3 from the communication means 5.

It performs a verification on the following items and, if the verification results in a failure even about only one item, it interrupts the subsequent processing.

The first session state is "valid".

The public key certificate CertP3 is a valid public key certificate issued by the third-party device certificate authority.

The electronic signature Sabort=SigP3(abort||s2) is successfully verified by the public key P3.

It erases the first session state or defines it as invalid.

It generates an electronic value corresponding to the electronic value V1 and stores it into the storage device 10.

On the other hand, when the user device 2 is the one receiving the abort permission information AT and the public key certificate CertP3, the abort performance device 24 of the user device 2 executes a process below.

It acquires the abort permission information AT and the public key certificate CertP3 from the communication means 5.

It performs a verification on the following items and, if the verification results in a failure even about only one item, it interrupts the subsequent processing.

The second session state is "hold" or "valid".

The public key certificate CertP3 is a valid public key certificate issued by the third-party device certificate authority.

The electronic signature Sabort=SigP3(abort||s2) is successfully verified by the public key P3.

It erases the second session state or defines it as invalid.

It generates an electronic value corresponding to the electronic value V2 and stores it into the storage device 20.

After commitment of the above processing, the abort permission process is terminated.

At the above steps 401, 402, the abort permission device 33 generates the electronic signature Sabort for the information containing the second session information s2 and the information abort indicating the abort permission, using only the second session information s2 contained in the agreement information A, instead of the agreement information A, and outputs the abort permission information AT being the information containing the second session information s2, the information abort indicating the abort permission, and the electronic signature Sabort; therefore, the transmission/re-
ception can be performed without essentially unnecessary control information, so as to avoid an increase in volume of transmitted and received data and achieve promotion of efficiency of processing.

Next, the commitment permission process, which is executed when one of the predetermined cases is met in the commitment request process or in the abort request process, will be described with reference to FIG. 10.

The commitment permission device 34 of the third-party device 3 executes a process below.

It generates an electronic signature Scommit $\rightarrow$ SigP3$\langle$commit$\rangle$2, for information containing the commitment information s2.

The second session information s2.

The output of commitment permission information CT$\rightarrow$commit$\langle$commit$\rangle$2, containing the information commit indicating the commitment permission, the second session information s2, and the electronic signature Scommit, and the public key certificate CertP3 to the communication means 5.

The communication means 5 transfers the commitment permission information CT and the public key certificate CertP3 from the third-party device 3 to the user device 1 or to the user device 2. To which the information is to be transferred is determined depending on the following conditions.

If the preceding process is the commitment request process, the information is transferred to the user device 1.

If the preceding process is the abort request process, the information is transferred to the user device 2.

When the user device 1 is the one receiving the commitment permission information CT and the public key certificate CertP3, the commitment performance device 16 of the user device 1 executes a process below.

It acquires the commitment permission information CT and the public key certificate CertP3 from the communication means 5.

It performs a verification on the following items and, if the verification results in a failure even about only one item, it interrupts the subsequent processing.

The first session state is "valid".

The public key certificate CertP3 is a valid public key certificate issued by the third-party device certificate authority.

The electronic signature Scommit $\rightarrow$ SigP3$\langle$commit$\rangle$2 is successfully verified by the public key P3.

It erases the first session state or defines it as invalid.

It generates an electronic value corresponding to the electronic value V2 and stores it into the storage device 10.

On the other hand, when the user device 2 is the one receiving the commitment permission information CT and the public key certificate CertP3, the commitment performance device 25 of the user device 2 executes a process below.

It acquires the commitment permission information CT and the public key certificate CertP3 from the communication means 5.

It performs a verification on the following items and, if the verification results in a failure even about only one item, it interrupts the subsequent processing.

The second session state is "hold" or "valid".

The public key certificate CertP3 is a valid public key certificate issued by the third-party device certificate authority.

The electronic signature Scommit $\rightarrow$ SigP3$\langle$commit$\rangle$2 is successfully verified by the public key P3.

It erases the second session state or defines it as invalid.

It generates an electronic value corresponding to the electronic value V1 and stores it into the storage device 20.

After commitment of the above processing, the commitment permission process is terminated.

At the above steps 501, 502, the commitment permission device 34 generates the electronic signature Scommit for the information containing the second session information.

After commitment of the above processing, the commitment permission process is terminated.

At the above steps 501, 502, the commitment permission device 34 generates the electronic signature Scommit for the information containing the second session information s2 and the information commit indicating the commitment permission, using only the second session information s2 contained in the agreement information A, instead of the agreement information A, and outputs the commitment permission information CT being the information containing the second session information s2, the information commit indicating the commitment permission, and the electronic signature Scommit; therefore, the transmission/reception can be performed without essentially unnecessary control information, so as to avoid an increase in volume of transmitted and received data and achieve promotion of efficiency of processing.

In the above embodiment, the electronic values 101, 201 can be electronic money indicating certain amounts of money. This substantiates an electronic currency exchange system. Furthermore, an electronic ticket sales system can be substantiated by a configuration wherein the electronic value 101 is one or more electronic tickets and wherein the electronic value 201 is electronic money representing a certain amount of money or by a configuration wherein the electronic value 201 represents one or more electronic tickets and the electronic value 101 electronic money representing a certain amount of money.

Programs to execute the processes of the present embodiment in the respective devices of the system in the present embodiment can be recorded, stored, or distributed in computer-readable recording media, e.g., P2 (flexible disk), MO, ROM, a memory card, CD-ROM, DVD, a removable disk, or the like. The programs can also be provided through a network, such as the Internet or e-mail.

It is noted that the present invention is not limited to the above embodiments and that a variety of changes and applications can be made within the scope of the claims.

Obviously, numerous modifications and variations of the present invention are possible in light of the above teachings. It is therefore to be understood that within the scope of the appended claims, the invention may be practiced otherwise than as specifically described herein.

1. A user device for performing an exchange with another user device to exchange a first electronic value stored in said another user device, for a second electronic value stored in the user device itself, the user device comprising:

an agreement unit configured to acquire offer information being information corresponding to at least a first ran-
the first user device executes an offer step of generating a first random number, and outputting offer information being information corresponding to at least the first random number;

the second user device executes an agreement step of acquiring the offer information, generating a second random number, generating session information corresponding to the second random number, generating agreement object information containing to information containing at least the session information, generating an electronic signature $S_e$ for information containing the agreement object information and the session information, and outputting agreement information being information containing at least the agreement object information, the session information, and the electronic signature $S_e$;

the first user device executes a first confirmation step of acquiring the agreement information, performing a verification on a predetermined verification item, generating an electronic signature $S_e$ for information containing the session information, and outputting first confirmation information being information containing at least the session information and the electronic signature $S_e$;

the second user device executes a second confirmation step of acquiring the first confirmation information, performing a verification on a predetermined verification item, and outputting second confirmation information being information containing the second random number;

the first user device executes an end step of acquiring the second confirmation information, and performing a verification on a predetermined verification item; and

the device comprising an abort determination unit configured so that when the second user device executes an abort request step of generating an electronic signature for information containing information indicating an abort request, and the session information, and outputting abort request information being information containing the information indicating the abort request, the session information, and the electronic signature, the abort determination unit acquires the abort request information, performs a verification on a predetermined verification item, and determines whether a session state corresponding to the session information is defined as commit, and, if the session state is not defined as commit, the abort determination unit makes the session state corresponding to the session information so as to define the session state as abort.

4. The device according to claim 3, further comprising:

an abort permission unit configured so that when the session state is defined as abort, the abort permission unit generates an electronic signature for information containing information indicating an abort permission, and the session information, and outputs abort permission information being information containing the information indicating the abort permission, the session information, and the electronic signature.

5. A device used in a system for exchanging a first electronic value stored in a first user device, for a second electronic value stored in a second user device, said device being used in the system configured as follows:

the first user device executes an offer step of generating a first random number, and outputting offer information being information corresponding to at least the first random number;

the second user device executes an agreement step of acquiring the offer information, generating a second random number, generating session information corresponding to the second random number, generating agreement object information containing to information containing at least the session information, generating an electronic signature $S_e$ for information containing the agreement object information and the session information, and outputting agreement information being information containing at least the agreement object information, the session information, and the electronic signature $S_e$;

the first user device executes a first confirmation step of acquiring the agreement information, performing a verification on a predetermined verification item, generating an electronic signature $S_e$ for information containing the session information, and outputting first confirmation information being information containing at least the session information and the electronic signature $S_e$;

the second user device executes a second confirmation step of acquiring the first confirmation information, performing a verification on a predetermined verification item, and outputting second confirmation information being information containing the second random number;

the first user device executes an end step of acquiring the second confirmation information, and performing a verification on a predetermined verification item; and

the device comprising an abort determination unit configured so that when the second user device executes an abort request step of generating an electronic signature for information containing information indicating an abort request, and the session information, and outputting abort request information being information containing the information indicating the abort request, the session information, and the electronic signature, the abort determination unit acquires the abort request information, performs a verification on a predetermined verification item, and determines whether a session state corresponding to the session information is defined as commit, and, if the session state is not defined as commit, the abort determination unit makes the session state corresponding to the session information so as to define the session state as abort.
the second user device executes an agreement step of acquiring the offer information, generating a second random number, generating session information corresponding to the second random number, generating agreement object information corresponding to information containing at least the session information, generating an electronic signature Sa for information containing the agreement object information and the session information, and outputting agreement information being information containing at least the agreement object information, the session information, and the electronic signature Sa;

the first user device executes a first confirmation step of acquiring the agreement information, performing a verification on a predetermined verification item, generating an electronic signature Se for information containing the session information, and outputting first confirmation information being information containing at least the session information and the electronic signature Se;

the second user device executes a second confirmation step of acquiring the first confirmation information, performing a verification on a predetermined verification item, and outputting second confirmation information being information containing the second random number;

the first user device executes an end step of acquiring the second confirmation information, and performing a verification on a predetermined verification item; and

the device comprising a commitment determination unit configured so that when the first user device executes a commitment request step of generating an electronic signature for information containing information indicating a commitment request, and the session information, and outputting commitment request information being information containing the information indicating the commitment request, the session information, and the electronic signature, the commitment determination unit acquires the commitment request information, performs a verification on a predetermined verification item, and determines whether a session state corresponding to the session information is defined as abort, and, if the session state is not defined as abort, the commitment determination unit makes the session state corresponding to the session information so as to define the session state as commit.

6. The device according to claim 5, further comprising a commitment permission unit configured so that when the session state is defined as commit, the commitment permission unit generates an electronic signature for information containing information indicating a commitment permission, and the session information, and outputs commitment permission information being information containing the information indicating the commitment permission, the session information, and the electronic signature.

* * * * *