

DESCRIPTION

CRYPTOGRAPHIC ASSET BLOCKCHAIN PROCESSING APPARATUS, PROCESSING METHOD, PROCESSING SYSTEM, AND PROCESSING PROGRAM

Technical Field

[0001]

The present invention relates to a system for collecting and analyzing cryptographic asset blockchain data for use in an audit corporation or the like. Specifically, the present technology relates to a system for analyzing various types of data regarding blocks, transactions, and the like included in cryptographic asset blockchain data and supporting audit of transaction information (balance and the like) of various virtual currencies (here, referred to as "cryptographic assets") such as Bitcoin and Ethereum.

Background Art

[0002]

There is a distributed ledger technology using a blockchain as a technology for sharing and managing records when an unspecified number of individuals or corporate entities perform business transactions through the Internet. In the distributed ledger technology using the blockchain, a plurality of implementation methods are

devised according to the applications, purposes, and the like, and data recording formats and methods according to each implementation method are defined.

[0003]

In general, transaction information of cryptographic assets such as Bitcoin can be acquired via the Internet using a block explorer (Non Patent Literature 1) such as BLOCKCHAIR. A conventional block explorer can specify specific addresses or blocks one by one to obtain desired transaction information. In addition, by accessing a blockchain in which transaction information of various cryptographic assets is recorded and acquiring the transaction information, it is also possible to audit the transaction content on the basis of the transaction information (Patent Literature 1).

Citation List

Patent Literature

[0004]

Patent Literature 1: JP 2018-525729 A

Non Patent Literature

[0005]

Non Patent Literature 1: BLOCKCHAIR, URL

<https://blockchair.com/> (Searched on August 27, 2020)

Summary of Invention

Technical Problem

[0006]

Sending a query for searching a blockchain using a conventional application programming interface (API) of a block explorer and receiving transaction information on the Internet may be watched (intercepted) by a third party. For example, in a case where a plurality of queries for searching a blockchain using a block explorer is transmitted from a certain computer in a certain period on the Internet for the purpose of audit, a relationship between an IP address of the computer and an owner of the address (cryptographic asset account) or a plurality of addresses and the like belonging to the same owner are specified, and a plurality of addresses associated with each other (clustered), a content of the query, transaction information obtained as a search result, and the like can be easily associated with each other and may be misused.

[0007]

Therefore, by designating a predetermined period and searching a blockchain published on the Internet and accumulating data (blocks, transactions, and the like) in a storage apparatus (database or the like) of a computer such as a server in a private network for each type of the cryptographic asset, it is possible to analyze the

accumulated blockchain data and perform audit or the like of the transaction information under a private environment in which a query for a specific transaction or transaction information is not intercepted by a third party.

[0008]

However, in interpreting a data record (blocks, transactions, and the like) in a blockchain of a certain cryptographic asset, it is usually necessary to use software (for example, an API of node software) provided by a developer of software that has devised an implementation method thereof, and since an input/output method of the software also differs depending on the implementation method, it is difficult to collect and analyze blockchain data according to a plurality of different implementation methods.

[0009]

In addition, depending on an implementation method, information regarding a transaction quantity when a transaction is performed and a unit price used for the transaction are recorded in different data records, and in order to know how much amount of money of the cryptographic asset has moved for a certain transaction, it is necessary to acquire each of the unit price data and the transaction quantity data and then perform calculation in combination (transaction amount = unit price of time when transaction

is performed $\times$ transaction quantity).

[0010]

Further, depending on the implementation method, only the latest time point information is stored as the balance of the cryptographic asset of the participant of the transaction, and the balance information at the specific time point sought in the past cannot be acquired.

[0011]

Therefore, the present invention provides a cryptographic asset blockchain processing apparatus, a processing method, a processing system, and a processing program (hereinafter, referred to as a cryptographic asset blockchain processing apparatus or the like) that improve convenience of analysis of a large amount of data for an accounting audit or the like by collecting blockchain data generated by a plurality of different implementation methods, converting the data into data that can be analyzed, and processing transaction content such as a quantity, a unit price, and a partner of a transaction cryptographic asset into a standardized format.

Solution to Problem

[0012]

As one embodiment of the cryptographic asset blockchain processing apparatus according to the present

invention, the cryptographic asset blockchain processing apparatus includes at least:

- a data collection unit; and

- a data conversion unit, wherein

- the data collection unit accesses a cryptographic asset blockchain designated by a user and collects blockchain data from the cryptographic asset blockchain based on a request range predetermined,

- the data conversion unit converts the blockchain data into analyzable transaction data, and

- the blockchain data and the analyzable transaction data are stored in a data storage apparatus connected to the cryptographic asset blockchain processing apparatus.

[0013]

As a preferred embodiment of the cryptographic asset blockchain processing apparatus according to the present invention, the data storage apparatus is a cloud storage accessible by the cryptographic asset blockchain processing apparatus via a network.

[0014]

As a preferred embodiment of the cryptographic asset blockchain processing apparatus according to the present invention, the data collection unit operates in a static mode,

- the data collection unit operating in the static

mode designates the number of transaction data for each data batch and sets an end point of the request range, and sets identification information of last transaction data of data collected last time as a start point of the request range.

[0015]

As a preferred embodiment of the cryptographic asset blockchain processing apparatus according to the present invention, the data collection unit operates in a dynamic mode,

the data collection unit operating in the dynamic mode designates a data size for each data batch and sets an end point of the request range, and

sets identification information of last transaction data of data collected last time as a start point of the request range.

[0016]

As a preferred embodiment of the cryptographic asset blockchain processing apparatus according to the present invention, the data collection unit operates in an automatic collection mode,

the data collection unit operating in the automatic collection mode acquires identification information of latest data on the cryptographic asset blockchain and sets the identification information as an end point of the

request range, and

sets identification information of last transaction data of data collected last time by the data collection unit as a start point of the request range.

[0017]

As a preferred embodiment of the cryptographic asset blockchain processing apparatus according to the present invention, when a previous collection mode is a static mode in which the number of transaction data for each data batch is designated or a dynamic mode in which a data size for each data batch is designated, the data collection unit recalculates identification information of last transaction data of data collected last time based on the number of transaction data or the data size of the previous collection mode and sets the identification information as a start point of the request range.

[0018]

As a preferred embodiment of the cryptographic asset blockchain processing apparatus according to the present invention, the blockchain data includes transaction data to which an identifiable block number is assigned,

the transaction data includes at least one or more pieces of unit price transaction data for unit price setting and one or more pieces of quantity transaction data for quantity designation, and

the data conversion unit searches, for each of the one or more pieces of quantity transaction data, unit price transaction data to which a block number closest to a block number assigned to the one or more pieces of quantity transaction data is assigned, and calculates an amount of money related to a transaction by multiplying a value of a unit price of the unit price transaction data searched by a quantity of the one or more pieces of quantity transaction data.

[0019]

As a preferred embodiment of the cryptographic asset blockchain processing apparatus according to the present invention, the data storage apparatus includes a blockchain data storage apparatus and a transaction data storage apparatus,

the blockchain data collected by the data collection unit is stored in the blockchain data storage apparatus, and

transaction data including the amount of money calculated by the data conversion unit is stored in the transaction data storage apparatus.

[0020]

As a preferred embodiment of the cryptographic asset blockchain processing apparatus according to the present invention, the cryptographic asset blockchain processing

apparatus further includes a data analysis unit, and

the data analysis unit acquires the transaction data matching a block number from a first block number to a block number at a specific time point from the transaction data storage apparatus, and

calculates a balance by adding an amount of money of the transaction data acquired for each address that is a recording unit corresponding to a bank account number in the cryptographic asset blockchain.

[0021]

As a preferred embodiment of the cryptographic asset blockchain processing apparatus according to the present invention, the blockchain data includes at least block data and transaction data,

the data conversion unit adds an attribute of year/month/date related to a transaction date and time to each of the block data and the transaction data to convert the block data and the transaction data into transaction data distinguishable by year/month/date, and

the transaction data is classified by year/month/date and stored in the data storage apparatus.

[0022]

As a preferred embodiment of the cryptographic asset blockchain processing apparatus according to the present invention, the data storage apparatus includes a blockchain

data storage apparatus and a transaction data storage apparatus,

the blockchain data collected by the data collection unit is stored in the blockchain data storage apparatus, and

the transaction data to which the attribute of the year/month/date is added by the data conversion unit and which can be distinguished by the year/month/date is stored in the transaction data storage apparatus.

[0023]

As a preferred embodiment of the cryptographic asset blockchain processing apparatus according to the present invention, the cryptographic asset blockchain processing apparatus further includes a data analysis unit,

the data conversion unit divides the transaction data into transaction input data and transaction output data, and

the data analysis unit calculates total revenue and total expenditure in a range of a specific block number based on the transaction input data and the transaction output data for each address that is a recording unit corresponding to a bank account number in the cryptographic asset blockchain.

[0024]

As a preferred embodiment of the cryptographic asset

blockchain processing apparatus according to the present invention, the cryptographic asset blockchain processing apparatus further includes a data analysis unit, and

the data analysis unit calculates a balance for each address based on the transaction data and a result of a smart contract for each address that is a recording unit corresponding to a bank account number in the cryptographic asset blockchain.

[0025]

As a preferred embodiment of the cryptographic asset blockchain processing apparatus according to the present invention, the cryptographic asset blockchain processing apparatus further includes a consistency verification unit,

the transaction data includes block data to which a sequence number is assigned in a generation order,

the consistency verification unit checks whether the sequence number is duplicated or missing by sequentially collating the sequence number of the block data, and

in a case where there is a duplication or missing in the sequence number, notification of inconsistency of the block data corresponding to the sequence number is provided.

[0026]

As a preferred embodiment of the cryptographic asset blockchain processing apparatus according to the present

invention, the consistency verification unit counts the number of transaction data for each sequence number with respect to transaction data having a sequence number of a belonging block, and compares the number counted of transaction data with the number of transactions recorded in block data to which the sequence number is assigned, and provides notification of an inconsistency of the block data in a case where there is a difference.

[0027]

As a preferred embodiment of the cryptographic asset blockchain processing apparatus according to the present invention, the cryptographic asset blockchain processing apparatus further includes a consistency verification unit,

the consistency verification unit calculates a verification balance of an address designated by a user using a block explorer managed by a third party,

acquires a balance at the address designated from a balance calculated for each address by the data analysis unit, and compares the balance calculated by the data analysis unit with the verification balance, and

provides notification that there is an inconsistency in data of the address designated in a case where there is a difference.

[0028]

As a preferred embodiment of the cryptographic asset

blockchain processing apparatus according to the present invention, the consistency verification unit accesses a site that manages a version of node software of a cryptographic asset, checks a latest version of node software of a cryptographic asset desired, compares the latest version with a version of node software of the cryptographic asset stored in the data storage apparatus, and provides notification that there is an inconsistency in the version of the node software of the cryptographic asset in a case where there is a difference in the version.

[0029]

As one embodiment of the cryptographic asset blockchain processing method according to the present invention, the cryptographic asset blockchain processing method includes:

- a step of accessing a cryptographic asset blockchain designated by a user;

- a step of collecting blockchain data from the cryptographic asset blockchain based on a request range predetermined; and

- a step of converting the blockchain data into analyzable transaction data, wherein

- the blockchain data and the analyzable transaction data are stored in a data storage apparatus connected to the cryptographic asset blockchain processing apparatus.

[0030]

As one embodiment of the cryptographic asset blockchain processing system according to the present invention, the system further includes:

an information processing terminal; and

a cloud storage, wherein

the cryptographic asset blockchain processing apparatus, the information processing apparatus, and the cloud storage are connected via a network.

[0031]

As one embodiment of the cryptographic asset blockchain processing program according to the present invention, the program is executed by a computer to cause the computer to function as each unit of the cryptographic asset blockchain processing apparatus.

[0032]

As another embodiment of the cryptographic asset blockchain processing program according to the present invention, the program is executed by a computer to cause the computer to execute each step of the cryptographic asset blockchain processing method.

Advantageous Effects of Invention

[0033]

The cryptographic asset blockchain processing

apparatus or the like according to the present invention collects blockchain data (blocks, transactions, and the like) of a cryptographic asset on the Internet, accumulates the blockchain data for each type of the cryptographic asset in a storage apparatus (database or the like) of a computer such as a server under a private environment in which a query or transaction information for a specific transaction is not intercepted by a third party, and converts the blockchain data into a data format suitable for analysis, so that it is possible not only to safely analyze the blockchain data and calculate a balance or the like for each address for audit but also to collect and analyze the blockchain data according to a plurality of different implementation methods of the cryptographic assets.

[0034]

In addition, the cryptographic asset blockchain processing apparatus or the like generates virtual transaction data in which a transaction amount (= the unit price of the time when the transaction is performed × the transaction quantity) calculated from the unit price data and the transaction quantity data is recorded, in a case where information regarding the transaction quantity at the time when the transaction is performed and the unit price used for the transaction are recorded in different data

records, depending on the implementation methods of the cryptographic assets, and thus, can comprehensively aggregate the transaction data up to a certain time point without being affected by the implementation methods of the cryptographic assets, and can easily calculate the balance of the cryptographic assets of the participants in the transaction at a specific time point sought in the past.

[0035]

Furthermore, by verifying duplication or missing of the collected blockchain data, a difference in the version of the node software of the cryptographic asset, and the like, it is possible to ensure consistency of the transaction data to be analyzed.

Brief Description of Drawings

[0036]

Fig. 1 is a diagram illustrating a configuration of a cryptographic asset blockchain processing system according to an embodiment of the present invention.

Fig. 2 is a block diagram illustrating an example of a hardware configuration of a cryptographic asset blockchain processing apparatus according to an embodiment of the present invention.

Fig. 3 is a block diagram illustrating a configuration of a cryptographic asset blockchain

processing apparatus according to an embodiment of the present invention.

Fig. 4 is a flowchart illustrating a flow of processing of collecting blockchain data.

Fig. 5 is a flowchart illustrating a flow of processing of converting collected blockchain data (level 1 data) into transaction data (level 2 data) that can be analyzed.

Fig. 6 is a diagram illustrating an overview of a processing flow of collecting and analyzing data of a blockchain of Bitcoin.

Fig. 7 is a diagram illustrating an example of a display screen of a block explorer that displays one piece of block information in a blockchain.

Fig. 8 is a diagram illustrating an example of collected block information.

Fig. 9 is a diagram illustrating an example of a display screen of a block explorer that displays one piece of transaction information in a blockchain.

Fig. 10 is a diagram illustrating an example of collected transaction information.

Fig. 11 is a diagram illustrating an example in which the block information and the transaction information (level 1 data) illustrated in Figs. 8 and 10 are stored in a folder as information (level 2 data) distinguishable by

year/month/date.

Fig. 12 is a diagram illustrating an example of block information stored in one folder illustrated in Fig. 11.

Fig. 13 is a diagram illustrating an example of a configuration of level 1 data of Bitcoin and a configuration of level 2 data corresponding to the level 1 data.

Fig. 14 is a diagram illustrating an example of a configuration of level 1 data of Bitcoin and a configuration of level 2 data corresponding to the level 1 data.

Fig. 15 is a diagram illustrating an overview of a processing flow of collecting and analyzing data of a blockchain of Ethereum.

Fig. 16 is a diagram illustrating an example of a configuration of level 1 data of Ethereum and a configuration of level 2 data corresponding to the level 1 data.

Fig. 17 is a diagram illustrating an example of a configuration of level 1 data of Ethereum and a configuration of level 2 data corresponding to the level 1 data.

Fig. 18 is a diagram illustrating an example of a configuration of level 1 data of Ethereum and a

configuration of level 2 data corresponding to the level 1 data.

Fig. 19 is a diagram illustrating an example of a configuration of level 1 data of Ethereum and a configuration of level 2 data corresponding to the level 1 data.

Fig. 20 is a diagram illustrating an example of a configuration of level 1 data of Ethereum.

Fig. 21 is a flowchart illustrating a flow of processing of an amount calculation method for data in which a unit price and an amount of money are separately recorded in a transaction.

Fig. 22 is a diagram illustrating an example of transaction data that can be acquired by an API of node software.

Fig. 23 is a diagram illustrating an example of virtual transaction data obtained by performing the processing illustrated in Fig. 22 on the transaction data illustrated in Fig. 22.

Fig. 24 is a flowchart illustrating a flow of processing of detecting duplication/missing of converted data (transaction data).

Fig. 25 is a diagram illustrating an example of missing of block data.

Fig. 26 is a diagram illustrating an example of

duplication of transaction data.

Fig. 27 is a schematic diagram illustrating a balance confirmation mechanism implemented by the cryptographic asset blockchain processing apparatus according to an embodiment of the present invention.

Fig. 28 is a diagram illustrating an example of a report that is automatically generated by comparing version updates of cryptographic assets on a blockchain as needed.

Description of Embodiments

[0037]

Hereinafter, embodiments of the present invention will be described with reference to the drawings. In all the drawings for describing the embodiments, the same reference numerals are assigned to the same elements in principle, and repeated description thereof will be omitted. The individual embodiments of the present invention are not independent, and can be appropriately implemented in combination.

[0038]

Fig. 1 illustrates a configuration of a cryptographic asset blockchain processing system according to an embodiment of the present invention. The cryptographic asset blockchain processing system illustratively includes a cryptographic asset blockchain

processing apparatus 10, an information processing terminal 20, and a cloud storage (online storage) 30. The cryptographic asset blockchain processing apparatus 10 is, for example, a computer connectable to a network N such as a server. Furthermore, the information processing terminal 20 is a terminal connectable to the network N, for example, a personal computer, a notebook computer, a smartphone, a mobile phone, or the like.

[0039]

The network N may be, for example, an open network such as the Internet, an intranet connected by a dedicated line, or a closed network. The network N is not limited thereto, and a closed network and an open network can be appropriately used in combination according to a required level of security or the like.

[0040]

As one embodiment, the cryptographic asset blockchain processing system includes at least the cryptographic asset blockchain processing apparatus 10 and the information processing terminal 20 connected to the cryptographic asset blockchain processing apparatus 10 via the network N. By directly operating the cryptographic asset blockchain processing apparatus 10 or operating via the information processing terminal 20, the user can access a blockchain related to a cryptographic asset (hereinafter,

referred to as a cryptographic asset blockchain) disclosed on the Internet and accumulate data recorded in the blockchain (hereinafter, referred to as blockchain data) in the storage apparatus of the cryptographic asset blockchain processing apparatus 10. As another embodiment, the cryptographic asset blockchain processing system may accumulate blockchain data collected from the cryptographic asset blockchain in the cloud storage 30 instead of the storage apparatus of the cryptographic asset blockchain processing apparatus 10.

[0041]

By operating the storage apparatus of the cryptographic asset blockchain processing apparatus 10 and the cloud storage 30 under a closed environment (private environment) in which external access is blocked, it is possible to prevent a third party from intercepting a query or transaction information for a specific transaction.

[0042]

Fig. 2 is a block diagram illustrating an example of a hardware configuration of the cryptographic asset blockchain processing apparatus according to an embodiment of the present invention. Note that, in the figure, reference numerals corresponding to the hardware of the cryptographic asset blockchain processing apparatus 10 are described without parentheses, and reference numerals

corresponding to the hardware of the information processing terminal 20 are described with parentheses.

[0043]

The cryptographic asset blockchain processing apparatus 10 is, for example, a server (computer), and illustratively includes a central processing unit (CPU) 11, a memory 12 including a read only memory (ROM), a random access memory (RAM), and the like, a bus 13, an input/output interface 14, an input unit 15, an output unit 16, a storage unit 17, and a communication unit 18.

[0044]

The CPU 11 executes various processes in accordance with programs recorded in the memory 12 or programs loaded from the storage unit 17 into the memory 12. The CPU 11 can execute, for example, a program for causing a server (computer) to function as the cryptographic asset blockchain processing apparatus of the present invention. In addition, at least some functions of the cryptographic asset blockchain processing apparatus can be implemented in hardware by an application specific integrated circuit (ASIC) or the like.

[0045]

The memory 12 appropriately stores data and the like necessary for the CPU 11 to execute various processes. The CPU 11 and the memory 12 are connected to each other via

the bus 13. The input/output interface 14 is also connected to the bus 13. The input unit 15, the output unit 16, the storage unit 17, and the communication unit 18 are connected to the input/output interface 14.

[0046]

The input unit 15 includes various buttons, a touch panel, a microphone, or the like, and inputs various types of information according to an instruction operation of the user or the like of the cryptographic asset blockchain processing apparatus 10. Note that the input unit 15 may be implemented by an input device such as a keyboard or a mouse independent of a main body that accommodates other units of the cryptographic asset blockchain processing apparatus 10.

[0047]

The output unit 16 includes a display, a speaker, or the like, and outputs image data or audio data such as a still image or a moving image. Image data and music data output by the output unit 16 are output from a display, a speaker, or the like as an image or music so as to be recognizable by the user.

[0048]

The storage unit 17 includes a semiconductor memory such as a dynamic random access memory (DRAM) or a storage apparatus such as a solid state drive (SSD) or a hard disk,

and can store various data.

[0049]

The communication unit 18 implements communication with other devices. For example, the communication unit 18 can communicate with the information processing terminal 20 and the cloud storage 30 via the network N.

[0050]

Note that a drive (not illustrated) is appropriately provided in the cryptographic asset blockchain processing apparatus 10 as necessary. For example, a removable medium including a magnetic disk, an optical disk, a magneto-optical disk, a semiconductor memory, or the like is appropriately mounted on the drive. The removable medium stores a program for accessing the cryptographic asset blockchain to collect blockchain data, and various data such as text data and image data. Programs and various data read from the removable medium by the drive are installed in the storage unit 17 as necessary.

[0051]

Next, a hardware configuration of the information processing terminal 20 will be described. As illustrated in Fig. 2, the information processing terminal 20 includes, for example, a CPU 21, a memory 22, a bus 23, an input/output interface 24, an input unit 25, an output unit 26, a storage unit 27, and a communication unit 28. Each

of these units has a function equivalent to that of each unit having the same name different only in the reference numeral included in the above-described cryptographic asset blockchain processing apparatus 10. Therefore, redundant description will be omitted. Note that, in a case where the information processing terminal 20 is configured as a portable device, each piece of hardware included in the information processing terminal 20 and a display or a speaker may be implemented as an integrated device.

[0052]

A functional configuration of the cryptographic asset blockchain processing apparatus 10 included in the cryptographic asset blockchain processing system will be described with reference to Fig. 3. Fig. 3 is a block diagram illustrating a configuration of the cryptographic asset blockchain processing apparatus according to an embodiment of the present invention. For example, in a case where a program for performing processing such as collection, conversion, analysis, and consistency verification of blockchain data is executed by a server (computer), the server functions as, for example, the cryptographic asset blockchain processing apparatus 10, and a data collection unit 111, a data conversion unit 112, a data analysis unit 113, and a consistency verification unit 114 function in hardware resources such as the memory 12 in

addition to the CPU 11.

[0053]

In addition, the storage unit 17 can function as the blockchain data storage apparatus 171 and the transaction data storage apparatus 172 by using a part of the storage area of the storage unit 17. As another embodiment, the blockchain data storage apparatus 171 and the transaction data storage apparatus 172 may be configured as an external storage apparatus separate from the cryptographic asset blockchain processing apparatus 10, or for example, the cloud storage 30 may be used as the external storage apparatus. In these embodiments, the blockchain data storage apparatus 171 and the transaction data storage apparatus 172 are divided, but may be one data storage apparatus without being divided. Details of the information stored in the blockchain data storage apparatus 171 and the transaction data storage apparatus 172 will be described later.

[0054]

The cryptographic asset blockchain processing apparatus 10 requests data recorded in the blockchain regarding the cryptographic asset disclosed on the Internet using the API provided by the conventional node software, and stores the downloaded blockchain data (here, also referred to as level 1 data) in the blockchain data storage

apparatus 171 which is a data storage apparatus. This processing can be performed by batch processing. In order to download blockchain data (level 1 data) from the cryptographic asset blockchain, it is necessary to develop nodes corresponding to different implementation methods of the cryptographic asset, and a plurality of the cryptographic asset blockchain processing apparatuses 10 can be provided to function as nodes corresponding to different implementation methods of the cryptographic asset. The blockchain data (level 1 data) is converted into transaction data (level 2 data) in the cryptographic asset blockchain processing apparatus 10 (node), and can be transferred to the cloud storage 30 via the node and stored.

[0055]

In the cryptographic asset blockchain processing system, for example, it is possible to handle types of cryptographic assets such as UTXO type cryptographic assets such as Bitcoin and Bitcoin Cash derived therefrom, and account type cryptographic assets such as Ethereum and Nem.

[0056]

The cryptographic asset blockchain processing apparatus 10 designates a range of requested data to collect blockchain data from the cryptographic asset blockchain published on the network. The cryptographic

asset blockchain processing apparatus 10 includes three types of modes for designating a range of data, and can execute collection of blockchain data by setting one of the modes.

[0057]

The three modes include a static mode, a dynamic mode, and an automatic collection mode. In the static mode and the dynamic mode, blockchain data is collected by batch processing.

[0058]

In the static mode, the number of data per batch (the number of data in which a transaction is recorded) is designated, and the cryptographic asset blockchain processing apparatus 10 can collect blockchain data according to the designated number of data. For example, in a case where the number of data for each batch is designated as 1000, 1000 pieces of blockchain data (that is, data in which a transaction is recorded) are collected, and the data can be stored in the blockchain data storage apparatus 171 by being divided for each folder.

[0059]

In the dynamic mode, a data size for each batch is designated, and the cryptographic asset blockchain processing apparatus 10 can collect blockchain data according to the designated data size. For example, in a

case where the data size for each batch is designated as 250 MB, 250 MB blockchain data (data in which a transaction is recorded) can be collected. Note that, since the number of data in which the transaction is recorded is not constant for each block in the cryptographic asset blockchain, in a case where the data size is designated, the number of blocks may be different even for blockchain data having the same data size.

[0060]

In the automatic collection mode, a blockchain request range or the like is automatically set in the cryptographic asset blockchain processing apparatus 10. A flow of processing in the automatic collection mode is illustrated in Fig. 4. Fig. 4 is a flowchart illustrating a flow of processing of collecting blockchain data. The user activates the cryptographic asset blockchain processing apparatus 10 (node) corresponding to the designated cryptographic asset blockchain using the information processing terminal 20 or the like (step S101). The cryptographic asset blockchain processing apparatus 10 accesses the cryptographic asset blockchain designated by the user.

[0061]

The cryptographic asset blockchain processing apparatus 10 is synchronized with the cryptographic asset

blockchain designated by the user (step S102). For example, the recording ledger held by the cryptographic asset blockchain processing apparatus 10 is synchronized with a recording ledger held by another node on the same blockchain network. Through synchronization, uncollected blockchain data can be identified in the cryptographic asset blockchain.

[0062]

The cryptographic asset blockchain processing apparatus 10 calculates data recording the latest transaction in the cryptographic asset blockchain. For example, an identification number (identification information) assigned to each block is acquired from a block header included in the blockchain data, and data in which the latest transaction is recorded is specified (step S103). Then, the cryptographic asset blockchain processing apparatus 10 sets the end point of the data request range on the basis of the block header of the data (step S104).

[0063]

The cryptographic asset blockchain processing apparatus 10 calculates a block header of data in which the last transaction is recorded in data collected in the previous execution of data collection on the basis of data stored in the data storage apparatus (for example, transaction data storage apparatus 172). For example, an

identification number (identification information) assigned to each block is acquired from a block header included in the blockchain data, and data in which the last transaction is recorded is specified (step S105). In addition, the cryptographic asset blockchain processing apparatus 10 recalculates a block header of data in which the last transaction is recorded in data collected in the previous execution of data collection on the basis of the mode (static or dynamic) as necessary (step S106). It is possible to accurately specify the block header of the data in which the last transaction as the start point is recorded in the current data collection by designating whether the request range is set according to the number of data designated in the static mode or the request range is set according to the data size designated in the dynamic mode in the data collection executed last time.

[0064]

The cryptographic asset blockchain processing apparatus 10 sets the start point of the data request range on the basis of the block header of the data in which the last transaction is recorded in the data collected in the previous execution of data collection (step S107). Note that, in a case where data collection is executed for the first time, the cryptographic asset blockchain processing apparatus 10 sets the first block (genesis block) of the

blockchain as the start point of the data request range, and the processes in steps S105 and S106 can be omitted.

[0065]

After setting the request range of the blockchain data, the cryptographic asset blockchain processing apparatus 10 waits until the cryptographic asset blockchain is synchronized with the end point of the request range (step S108), and after synchronization, starts data collection on the basis of the request range of the blockchain data (step S109). The cryptographic asset blockchain processing apparatus 10 stores the collected blockchain data (level 1 data) in the blockchain data storage apparatus.

[0066]

Fig. 5 is a flowchart illustrating a flow of processing of converting collected blockchain data (level 1 data) into transaction data (level 2 data) that can be analyzed. The cryptographic asset blockchain processing apparatus 10 reads the blockchain data (level 1 data) accumulated in the blockchain data storage apparatus 171 (step S121), converts the blockchain data (level 1 data) into transaction data (level 2 data) in an analyzable data format, that is, a data format capable of calculating the balance or the like of the cryptographic asset for each address (account) (step S122), and stores the converted

data in the transaction data storage apparatus 172 (step S123). Then, if necessary, the cryptographic asset blockchain processing apparatus 10 randomly extracts an address, which is a recording unit corresponding to a bank account number in the cryptographic asset blockchain, and verifies the consistency of the converted data (step S124). Details of the verification of the consistency will be described later (see Figs. 21 to 26 and description thereof). Fig. 6 illustrates an example of Bitcoin and Fig. 15 illustrates an example of Ethereum as a processing flow for converting the level 1 data of the cryptographic asset into the level 2 data.

[0067]

Fig. 6 illustrates an overview of a processing flow of collecting and analyzing data of the blockchain of Bitcoin. The user activates the cryptographic asset blockchain processing apparatus (node 10a in Fig. 6) corresponding to the implementation method of Bitcoin using the information processing terminal 20 and synchronizes with another node (corresponding to steps S101 to S102 in Fig. 4). After the synchronization, the node 10a collects blockchain data (level 1 data) (corresponding to steps S103 to S110 in Fig. 4).

[0068]

The level 1 data is blockchain data collected

directly from the blockchain via the node 10a. The level 1 data is divided into block data (blocks in Fig. 6) and transaction data (transactions in Fig. 6). A block in the blockchain is like a box that stores tens to hundreds of transactions (payments), and as a general blockchain structure, approval work of a transaction record (transaction) on the blockchain is performed at a block level.

[0069]

The block data collected by the node 10a originates from the first recorded block (genesis block), and includes all blocks up to the block of the latest transaction or a designated past block, and block information (a hash value (Hash) calculated by hashing the content of the block by a one-way function, a block ID, the number of bits (Bit), a timestamp (Timestamp) in which the block is recorded, and the like) of each block.

[0070]

Fig. 7 illustrates an example of each block information of the blockchain data of Bitcoin. Fig. 7 is an example of a display screen of a block explorer (for example, BLOCKCHAIR) that displays one piece of block information in the blockchain. The block "80234" in Fig. 7 is between the previously approved "80233" and the later approved "80235". Data of the block information (hash

value and timestamp (Mined on)) of 80234 is collected from the node 10a in the format of Fig. 8. Fig. 8 illustrates an example of block information collected by the node 10a. For example, the block information of the block "80234" is described below in a JSON format.

```
{"hash":  
"00000000002862a0885ec35cd86b8d95b1e1c0ba182845198b2a5b904d  
1dfb3e", "size": 473, "stripped_size": 473, "weight": 1864,  
"number": 80234, "version": 1, "merkle_root":  
729dff922569517e33b6f0e72ea567e53155df30736ef8625e25cf5123c  
0af68", "timestamp": 1284707604, "nonce": "122e0a2",  
"bits": "1b5bede6", "coinbase_param": "04e6ed5b1b021c01",  
"transaction_count": 2}  
[0071]
```

Further, an example of the transaction included in the block information of the block "80234" is as illustrated in Fig. 9. Fig. 9 illustrates an example of a display screen of a block explorer (BLOCKCHAIR) displaying one piece of transaction information in the blockchain. In the example illustrated in Fig. 9, the transaction includes senders and recipients of Bitcoin. When these pieces of data are collected, they are collected in a format (JSON) illustrated in Fig. 10.

[0072]

Fig. 10 illustrates an example of the collected

transaction information by the node 10a, and Fig. 11 illustrates an example in which the block information and the transaction information (level 1 data) illustrated in Figs. 8 and 10 are stored in a folder as information (level 2 data) distinguishable by year, month, and day. The level 2 data is converted into data searchable by year/month/date by adding an attribute of year/month/date to all the level 1 data on the basis of information such as a timestamp. The level 2 data is stored in the folder for each year/month/date.

[0073]

Fig. 12 illustrates an example of block information stored in one folder illustrated in Fig. 11. In the example illustrated in Fig. 12, the folder of the block information on December 18, 2009 includes information on blocks recorded on that day. Similarly, the transaction data is also divided into year, month, and day. The transaction data is also divided into a transaction input and a transaction output. Note that, according to a Bitcoin-specific unspent transaction output (UTXO) method, it is necessary to calculate the total expenditure and the total revenue for each account in a certain block range of the balance for each account.

[0074]

Figs. 13 and 14 illustrate an example of a

configuration of level 1 data of Bitcoin and a configuration of level 2 data corresponding to the level 1 data. Basically, in the item of the level 2 data of the block data (block) of Bitcoin, an item of year/month/date (year, month, day) is added to the item of the level 1 data. The item (hash, size, stripped_size, and the like) related to the Bitcoin block that can be acquired using the API of a conventional block explorer is described in the center column of the table of the block illustrated in Fig. 13, and the data type (string, bigint, and the like) of each item is described in the right column of the table. The same notation is applied to the table of the transaction (transactions, transaction_input, transaction_output) illustrated in Fig. 14.

[0075]

The transaction data (transactions) of Bitcoin is divided into transaction input data and transaction output data as level 2 data, and an item of year/month/date (year, month, day) is added to each of the transaction input data and the transaction output data.

[0076]

As another example of a cryptographic asset, collecting blockchain data from nodes of Ethereum is also described below. Fig. 15 illustrates an overview of a processing flow for collecting and analyzing data of the

blockchain of Ethereum. Using the information processing terminal 20, the user activates the cryptographic asset blockchain processing apparatus (the node 10b in Fig. 15) corresponding to the implementation method of Ethereum and synchronizes with another node (corresponding to steps S101 to S102 in Fig. 4). After the synchronization, the node 10b collects blockchain data (level 1 data) (corresponding to steps S103 to S110 in Fig. 4). The synchronization, collection, and analysis processing by the cryptographic asset blockchain processing apparatus for Ethereum basically has substantially the same flow as the processing for Bitcoin.

[0077]

Since the level 1 data of Ethereum is different from the level 1 data of Bitcoin, conversion for Ethereum is required for the conversion processing. For example, since Ethereum is not a Bitcoin UTXO method, it is necessary to convert processing results of transactions and smart contracts based on the Ethereum method so that the processing results can be used for calculation. As illustrated in Fig. 15, the Ethereum level 1 data includes not only block data (blocks) in CSV format but also data such as token_transfers, contracts, tokens traces, receipts, logs, and transactions in CSV format.

[0078]

Figs. 16 to 19 illustrate an example of a configuration of level 1 data of Ethereum and a configuration of level 2 data corresponding to the level 1 data, and Fig. 20 illustrates an example of a configuration of level 1 data of Ethereum. Similarly to the configuration of the data of Bitcoin illustrated in Figs. 13 and 14, in each table, an item of data is described in a center column and a type of data is described in a right column. Basically, in the item of level 2 data of the block data (blocks) of Ethereum, an item of year/month/date (year, month, day) is added to the item of the level 1 data (see Fig. 16).

[0079]

In token_transfers of the level 2 data of Ethereum, token_transfers and token included in the level 1 data are merged, unnecessary items are deleted at the time of merging, and items of year/month/date (year, month, day) are added (see Fig. 17). Further, in internal_transactions of the level 2 data of Ethereum, items of status, timestamp, and year/month/date (year, month, day) are added to traces included in the level 1 data (see Fig. 18).

[0080]

Further, in transactions of the level 2 data of Ethereum, transactions and receipts included in the level 1 data are merged, unnecessary items are deleted at the time

of merging, and items of timestamp and year/month/date (year, month, day) are added (see Fig. 19). Contracts and logs included in the level 1 data illustrated in Fig. 20 are not particularly converted into the level 2 data.

[0081]

In the cryptographic asset blockchain processing system of the present invention, as in the example of Bitcoin (Figs. 6 to 14) and the example of Ethereum (Figs. 15 to 20), it is possible to collect the blockchain data of the desired cryptographic asset by providing the cryptographic asset blockchain processing apparatus (node) corresponding to the implementation method and accessing the node corresponding to the cryptographic asset designated by the user, even for other cryptographic assets.

[0082]

Each of the cryptographic asset blockchain processing apparatuses 10 (10a, 10b, and the like) corresponding to implementation methods of various cryptographic assets collects blockchain data (level 1 data) in synchronization with other nodes on the P2P network of the blockchain, converts the blockchain data into analyzable transaction data (level 2 data) that is calculation of a balance or the like, and periodically executes a processing command to analyze the transaction

data (performs batch processing). For example, the cryptographic asset blockchain processing apparatus 10 can acquire data regarding the setting of the unit price of the transaction target by periodically executing these commands, create a data table that enables reference to the unit price at an arbitrary time point by combining the data regarding the unit price at the specific time point and the data regarding the time point at which the unit price is set, and store the data table in a data storage apparatus (for example, the blockchain data storage apparatus 171). In addition, the cryptographic asset blockchain processing apparatus 10 may acquire data regarding a time point and a quantity of transactions and store the data in the blockchain data storage apparatus 171.

[0083]

Fig. 21 is a flowchart illustrating a flow of processing of an amount calculation method for data in which a unit price and an amount of money are separately recorded in a transaction. Furthermore, Fig. 22 illustrates an example of transaction data that can be acquired by the API of the node software, and Fig. 23 illustrates an example of virtual transaction data obtained by performing the processing illustrated in Fig. 21 on the transaction data illustrated in Fig. 22.

[0084]

In a case where data in which the unit price and the amount of money are recorded separately is set as an analysis target, the cryptographic asset blockchain processing apparatus 10 calculates the amount of money from the data, generates a virtual transaction in which the unit price, the quantity, and the amount of money are recorded, and stores the updated content recorded in the original data in the transaction data storage apparatus 172, for example, in the flow of processing as illustrated in Fig. 21. In this manner, the blockchain data stored in the blockchain data storage apparatus 171 can be converted into transaction data in an analyzable data format, that is, a data format in which a balance or the like for each address can be calculated, and the transaction data can be stored in the transaction data storage apparatus 172.

[0085]

The flow of processing illustrated in Fig. 21 will be described with reference to an example of transaction data illustrated in Figs. 22 and 23. First, the cryptographic asset blockchain processing apparatus 10 acquires transaction data for unit price setting (referred to as unit price transaction data) from the blockchain data storage apparatus 171 (step S131), and acquires transaction data for quantity designation (referred to as quantity transaction data) from the blockchain data storage

apparatus 171 (step S132). In the example illustrated in Fig. 22, for example, the unit price transaction data is transactions with block heights of 500, 520, 540, and 541, which are block identification numbers, and the quantity transaction data is transactions with block heights of 510, 530, and 550.

[0086]

After acquiring each piece of data, the cryptographic asset blockchain processing apparatus 10 searches unit price transaction data having the most recent block number for each piece of quantity transaction data (step S133), and adds the value of the unit price of the searched unit price transaction data to the quantity transaction data (step S134). For example, for a transaction having a block height of 510, when unit price transaction data having the most recent block height (number) is searched, a transaction having a block height of 500 is found (see Fig. 22), and the unit price (50) of the transaction is added to the transaction having a block height of 510 (see Fig. 23). Similarly, a unit price (100) of a transaction having a block height of 520 is added to a transaction having a block height of 530, and a unit price (110) of a transaction having a block height of 541 is added to a transaction having a block height of 550.

[0087]

After adding the unit price recorded in the unit price transaction data to the quantity transaction data, the cryptographic asset blockchain processing apparatus 10 calculates an amount of money related to the transaction by multiplying the value of the quantity by the value of the unit price for each quantity transaction data (transactions with block heights of 510, 530, and 550 in Fig. 23) to which the unit price has been added, adds the amount of money to the transaction, and stores the amount of money in the transaction data storage apparatus (step S135). Similarly, the unit price transaction (transactions with block heights of 500, 520, 540, and 541 in Fig. 23) is also stored in the transaction data storage apparatus (step S136).

[0088]

The user of the cryptographic asset blockchain processing system according to the present invention executes a command of data collection, data conversion (data processing), or the like by the cryptographic asset blockchain processing apparatus 10 at an arbitrary timing, so that the cryptographic asset blockchain processing apparatus 10 can comprehensively aggregate transaction data up to a certain time point, calculate the balance of the cryptographic asset of the participant in the transaction at the timing, create balance data (TSV format, CSV format,

and the like) for each address (recording unit corresponding to the bank account number in the blockchain), and save the balance data in the transaction data storage apparatus 172.

[0089]

As a method of calculating the balance for each address at a specific time point, for example, the cryptographic asset blockchain processing apparatus 10 can acquire all transaction data matching from the genesis block to a specific block height from the transaction data storage apparatus 172, add the amounts of money of the acquired transaction data for each address, and store the transaction data in the transaction data storage apparatus 172. By using the transaction data stored in the transaction data storage apparatus 172, the cryptographic asset blockchain processing apparatus 10 can analyze the balance of the cryptographic asset or the like for each address for audit, for example. The user of the cryptographic asset blockchain processing system can arbitrarily extract the created transaction data and balance data, and can display the transaction data and balance data on a monitor or the like of the information processing terminal 20 to confirm the contents. In addition, the created transaction data and balance data can be further stored in another data storage apparatus or the

like, and can be compared with a book record or the like obtained from a device other than the blockchain.

[0090]

The cryptographic asset blockchain processing apparatus 10 can verify that blockchain data on the Internet is recorded without duplication or missing by using management information of transaction data periodically stored in the transaction data storage apparatus 172, and when an inconsistency occurs, an alert is generated and a user of the cryptographic asset blockchain processing system can be notified. For example, in a case where the inconsistency is detected, the cryptographic asset blockchain processing apparatus 10 can notify the information processing terminal 20 connected via the network N of an alert to notify the user of the alert.

[0091]

Fig. 24 is a flowchart illustrating a flow of processing of detecting duplication/missing of converted data (that is, transaction data in a data format capable of calculating the balance or the like of the cryptographic asset). Fig. 25 illustrates an example of missing block data, and Fig. 26 illustrates an example of duplication of transaction data. The cryptographic asset blockchain processing apparatus 10 reads transaction data including block data, transaction data, and the like from a data

storage apparatus (for example, transaction data storage apparatus 172) (step S141). Block data included in the transaction data is assigned with a serial number (sequence number) starting from 0 or 1 (genesis block number) in order of generation. The cryptographic asset blockchain processing apparatus 10 sequentially verifies whether there is no duplication or missing in the block number (sequence number) of the block data (step S142), and when there is duplication or missing (No in step S142), the cryptographic asset blockchain processing apparatus notifies the user of a consistency error (for example, via the information processing terminal 20,) providing notification that there is inconsistency in the blocks included in the transaction data (step S145).

[0092]

For example, as illustrated in Fig. 25, the block data loss is a state in which block data with a block number of 3 is not stored in the data storage apparatus (for example, transaction data storage apparatus 172) when sequentially viewed from a block A to a block C with a block number (block height, height) 1.

[0093]

When sequentially confirming the block A to the block C based on the block number, the cryptographic asset blockchain processing apparatus 10 can detect that the

block data having the block number of 3 is missing.

[0094]

In a case where there is no duplication or loss in the block data (Yes in step S142), the cryptographic asset blockchain processing apparatus 10 counts the number of transactions related to the block data for each sequence number by using the sequence number of the associated block in each of the transaction data (step S143), compares the counted result (the number of transactions) with the number of transactions recorded in the block data ("tra_cnt" in Fig. 26) (step S144), and in a case where there is a difference (in a case where there is no match) (No in step S144), notifies the user (for example, via the information processing terminal 20,) of a consistency error providing notification that there is an inconsistency in the transactions included in the transaction data (step S145).

[0095]

For example, as illustrated in Fig. 26, the mismatch of the number of transactions is a state in which the number of transactions included in the block data with the block number (block height) of 2 (height: 2) is 2 (tra_cnt: 2), whereas the result of counting the number of transactions A, B, and C (the number of hashes of transactions (tra_hash)) related to the block data with the block number of 2 is 3.

[0096]

Since the cryptographic asset blockchain processing apparatus 10 counts the transactions A, B, and C related to the block data (height: 2) for each block number and compares the counted result (in the example of Fig. 26, 3) with the number of transactions (tra_cnt) (in the example of Fig. 26, 2) recorded in the block data to obtain "number of transactions in block (tra_cnt) 2 < number of hashes of transactions 3" as illustrated in Fig. 26, the cryptographic asset blockchain processing apparatus 10 can detect that the number of transactions (tra_cnt) recorded in the block data does not match the actual count result, that is, that there is duplication of the transaction data.

[0097]

When the counted number of transactions matches the number of transactions (tra_cnt) recorded in the block data (Yes in step S144), the process of consistency verification of the transaction data is normally ended.

[0098]

In addition to the process of inconsistency verification illustrated in Fig. 24, inconsistency can be detected on the basis of a balance of an address that is a recording unit corresponding to a bank account number in the cryptographic asset blockchain. For example, the cryptographic asset blockchain processing apparatus 10

calculates the balance of the designated address (for example, address randomly extracted in the automatic collection mode (step S124 in Fig. 5)) using a block explorer managed and operated by a third party with high reliability.

[0099]

Next, the balance obtained from the block explorer of the third party is compared with the balance of the same address calculated by the cryptographic asset blockchain processing apparatus 10, and in a case where the balances do not match, it is possible to notify the user that there is an inconsistency and store a message or the like indicating which address has been inconsistent in a specific folder. The message stored in the folder is, for example, as follows.

address, data_bricks balance, external_explorer balance,
difference

1DFuBFLwJjXQapEBE36h3MmuHXMvjBUnA,701,600,101

1DPkMBvGTjUFJ621z1RkXjDBgloJykniYL,117125,117124,1

The message indicates that the balance (data_bricks balance) calculated by the cryptographic asset blockchain processing apparatus 10 and the balance (external_explorer) calculated using the block explorer of the third party do not match (difference) for the designated address (address).

[0100]

The balance confirmation mechanism via the block explorer of the third party can further improve reliability and objectivity of the calculation result provided by the cryptographic asset blockchain processing apparatus 10. Fig. 27 is a schematic diagram illustrating a balance confirmation mechanism implemented by the cryptographic asset blockchain processing apparatus according to an embodiment of the present invention.

[0101]

The cryptographic asset blockchain processing apparatus 10 functions as a blockchain node to acquire blockchain data itself, and processes the blockchain data as described above to calculate a balance for each address. Meanwhile, the cryptographic asset blockchain processing apparatus 10 communicates with a host 40 of a block explorer managed and operated by a trusted third party. The cryptographic asset blockchain processing apparatus 10 requests the block explorer (host 40) for a balance of a randomly selected address. The block explorer transmits the requested balance to the cryptographic asset blockchain processing apparatus 10. The cryptographic asset blockchain processing apparatus 10 compares the balance obtained from the block explorer of the third party with the balance of the same address calculated by the

cryptographic asset blockchain processing apparatus 10, and checks the consistency between them. This check may be performed periodically or in response to a request of the user.

[0102]

The cryptographic asset blockchain processing apparatus 10 and the transaction data storage apparatus 172 can be operated, for example, in a cloud (for example, an in-house cloud) operating in a closed environment of a certain audit corporation. By operating in such a cloud, verification of transaction data and an address balance are processed in an environment isolated from the public Internet, and protection of confidential information of a client can be reliably ensured (on the other hand, when an API of a block explorer or the like is used, an address or transaction information needs to be queried on the Internet, and the query information is not protected).

[0103]

In addition, by using the cloud technology, for example, the cryptographic asset blockchain processing apparatus 10 can be accessed from domestic or foreign firms (other audit corporations or the like) of the same group via a closed network of the audit corporation group. Since transactions of cryptographic assets are not affected by national borders, it is essential for fraudulent detection

of transactions and the like to be able to access the same data by farms (audit corporations or the like) in each country belonging to the same group.

[0104]

In general, implementation methods of various cryptographic assets are different, and implementation versions are frequently updated. For example, in a case where the implementation of the cryptographic asset is updated, it is necessary to change the processing content such as data collection according to the update content of the implementation method of the cryptocurrency for the cryptographic asset blockchain processing apparatus (node) corresponding to the implementation method of the cryptographic asset, and in order to ensure consistency of the blockchain data, it is necessary to make the node always compatible with the latest version.

[0105]

However, the user is not necessarily notified of the update of the version of the node software of the cryptographic asset. This is because there is no management company that manages and maintains the cryptographic asset such as Bitcoin although this is a feature of the distributed blockchain in which the blockchain data is distributed in P2P and managed in each node. Instead, in practice, the version of the node

software of the cryptographic asset is managed and maintained jointly by programmers who use the cryptographic asset (for example, a group of Bitcoin Core, or the like).

[0106]

Generally, when and for what reason the version of the node software of the cryptographic asset is updated is often known from a chat or news. Acquiring update information of the version of the node software of the desired cryptographic asset individually from the chat or the news has a risk that the information is incomplete or the update itself is overlooked, and thus, the cryptographic asset blockchain processing system according to the present invention provides a cryptographic asset fork checker.

[0107]

The cryptographic asset fork checker of the present invention is a mechanism that compares the version of the node software installed in the cryptographic asset blockchain processing apparatus 10 with the latest version of the node software managed by a site (Git Hub, Docker Hub, and the like) that manages the version of the node software, automatically creates a report, and issues an alert when there is a difference. Note that the fork refers to version update on the blockchain.

[0108]

The cryptographic asset fork checker in the cryptographic asset blockchain processing system according to the present invention can automatically generate a report as illustrated in Fig. 28. Fig. 28 illustrates an example of a report automatically generated by comparing the version of the node software installed in the cryptographic asset blockchain processing apparatus 10 with the latest version of the node software managed by a third-party management site (Git Hub, Docker Hub, and the like). For each cryptographic asset, the cryptographic asset fork checker can compare a version of the node software of the cryptographic asset in the cryptographic asset blockchain processing system with a latest version of the node software recorded at a third-party management site (for example, GitHub, Docker Hub, and the like), and automatically generate a report describing a result of the comparison. Note that the version of the node software of the cryptographic asset recorded in GitHub, Docker Hub, or the like is always the latest.

[0109]

As a result of the comparison, in a case where there is a difference between the version of the node software of the cryptographic asset in the cryptographic asset blockchain processing system and the version of the node software of the cryptographic asset recorded in the

management site (GitHub, Docker Hub, and the like), for example, the cryptographic asset blockchain processing apparatus 10 can notify the information processing terminal 20 of an alert (inconsistency) to notify the user.

[0110]

The items of the report illustrated in Fig. 28 are as follows.

[Table 1]

Currency name	Name of cryptographic asset (virtual currency)
Current version (in CAPP2)	Version of node software of cryptographic asset currently supported by cryptographic asset blockchain processing system according to present invention
Current version date (in CAPP2)	Date when version of node software of cryptographic asset currently supported by cryptographic asset blockchain processing system according to present invention began to be used publicly
Latest version (in Github)	Version recorded on GitHub, which is one of sites that manages versions of node software

Latest version date (in Github)	Date when version on GitHub, which is one of sites that manages versions of node software, began to be used publicly
Need to Update?	Whether it needs to be updated
Reference	Reference data
Remarks	Comments

[0111]

In the example of the report illustrated in Fig. 28, in the node software of Bitcoin, Bitcoin Cash, and Ethereum/Ethereum Classic, the field of "Need to Update?" is "True", so that it is possible to notify the user that update is necessary via the information processing terminal 20 or the like.

[0112]

As described above, the cryptographic asset blockchain processing apparatus or the like according to the present invention collects blockchain data (including blocks, transactions, and the like) of a cryptographic asset on an open network such as the Internet, accumulates the blockchain data for each type of the cryptographic asset in a computer (node) such as a server and a data storage apparatus under a private network environment in which a query or transaction information for a specific transaction is not intercepted by a third party, and

converts the blockchain data into a data format suitable for analysis, so that it is possible not only to safely analyze the blockchain data and calculate a balance or the like for each address for audit but also to collect and analyze the blockchain data according to a plurality of different implementation methods of the cryptographic assets.

[0113]

In addition, the cryptographic asset blockchain processing apparatus or the like according to the present invention generates virtual transaction data in which a transaction amount (= the unit price of the time when the transaction is performed × the transaction quantity) calculated from the unit price data and the transaction quantity data is recorded, in a case where information regarding the transaction quantity at the time when the transaction is performed and the unit price used for the transaction are recorded in different data records, depending on the implementation methods of the cryptographic assets, and thus, can comprehensively aggregate the transaction data up to a certain time point without being affected by the implementation methods of the cryptographic assets, and can easily calculate the balance of the cryptographic assets of the participants in the transaction at a specific time point sought in the past.

[0114]

Furthermore, the cryptographic asset blockchain processing apparatus or the like according to the present invention can ensure consistency of transaction data to be analyzed by verifying duplication or missing of collected blockchain data, a difference in version of node software of the cryptographic asset, or the like.

Industrial Applicability

[0115]

The cryptographic asset blockchain processing apparatus or the like according to the present invention can be used, for example, in an audit corporation to calculate a balance of the cryptographic asset for each address to be audited and support the audit.

Reference Signs List

[0116]

- 10 Cryptographic asset blockchain processing apparatus (node)
- 10a Node
- 10b Node
- 11 CPU
- 12 Memory
- 13 Bus

14	Input/output interface
15	Input unit
16	Output unit
17	Storage unit
18	Communication unit
20	Information processing terminal
21	CPU
22	Memory
23	Bus
24	Input/output interface
25	Input unit
26	Output unit
27	Storage unit
28	Communication unit
30	Cloud storage
40	Host
111	Data collection unit
112	Data conversion unit
113	Data analysis unit
114	Consistency verification unit
171	Blockchain data storage apparatus
172	Transaction data storage apparatus
N	Network

CLAIMS

1. A cryptographic asset blockchain processing apparatus, comprising at least:
 - a data collection unit; and
 - a data conversion unit, whereinthe data collection unit accesses a cryptographic asset blockchain designated by a user and collects blockchain data from the cryptographic asset blockchain based on a request range predetermined,
 - the data conversion unit converts the blockchain data into analyzable transaction data, and
 - the blockchain data and the analyzable transaction data are stored in a data storage apparatus connected to the cryptographic asset blockchain processing apparatus.
2. The cryptographic asset blockchain processing apparatus according to claim 1, wherein
 - the data storage apparatus is a cloud storage accessible by the cryptographic asset blockchain processing apparatus via a network.
3. The cryptographic asset blockchain processing apparatus according to claim 1 or 2, wherein
 - the data collection unit operates in a static mode,
 - the data collection unit operating in the static mode designates the number of transaction data for each data batch and sets an end point of the request range, and

sets identification information of last transaction data of data collected last time as a start point of the request range.

4. The cryptographic asset blockchain processing apparatus according to claim 1 or 2, wherein

the data collection unit operates in a dynamic mode, the data collection unit operating in the dynamic mode designates a data size for each data batch and sets an end point of the request range, and

sets identification information of last transaction data of data collected last time as a start point of the request range.

5. The cryptographic asset blockchain processing apparatus according to claim 1 or 2, wherein

the data collection unit operates in an automatic collection mode,

the data collection unit operating in the automatic collection mode acquires identification information of latest data on the cryptographic asset blockchain and sets the identification information as an end point of the request range, and

sets identification information of last transaction data of data collected last time by the data collection unit as a start point of the request range.

6. The cryptographic asset blockchain processing

apparatus according to claim 5, wherein

when a previous collection mode is a static mode in which the number of transaction data for each data batch is designated or a dynamic mode in which a data size for each data batch is designated, the data collection unit recalculates identification information of last transaction data of data collected last time based on the number of transaction data or the data size of the previous collection mode and sets the identification information as a start point of the request range.

7. The cryptographic asset blockchain processing apparatus according to any one of claims 1 to 6, wherein

the blockchain data includes transaction data to which an identifiable block number is assigned,

the transaction data includes at least one or more pieces of unit price transaction data for unit price setting and one or more pieces of quantity transaction data for quantity designation, and

the data conversion unit searches, for each of the one or more pieces of quantity transaction data, unit price transaction data to which a block number closest to a block number assigned to the one or more pieces of quantity transaction data is assigned, and calculates an amount of money related to a transaction by multiplying a value of a unit price of the unit price transaction data searched by a

quantity of the one or more pieces of quantity transaction data.

8. The cryptographic asset blockchain processing apparatus according to claim 7, wherein

the data storage apparatus includes a blockchain data storage apparatus and a transaction data storage apparatus,

the blockchain data collected by the data collection unit is stored in the blockchain data storage apparatus, and

transaction data including the amount of money calculated by the data conversion unit is stored in the transaction data storage apparatus.

9. The cryptographic asset blockchain processing apparatus according to claim 8, further comprising

a data analysis unit, wherein

the data analysis unit acquires the transaction data matching a block number from a first block number to a block number at a specific time point from the transaction data storage apparatus, and

calculates a balance by adding an amount of money of the transaction data acquired for each address that is a recording unit corresponding to a bank account number in the cryptographic asset blockchain.

10. The cryptographic asset blockchain processing

apparatus according to any one of claims 1 to 6, wherein

the blockchain data includes at least block data and transaction data,

the data conversion unit adds an attribute of year/month/date related to a transaction date and time to each of the block data and the transaction data to convert the block data and the transaction data into transaction data distinguishable by year/month/date, and

the transaction data is classified by year/month/date and stored in the data storage apparatus.

11. The cryptographic asset blockchain processing apparatus according to claim 10, wherein

the data storage apparatus includes a blockchain data storage apparatus and a transaction data storage apparatus,

the blockchain data collected by the data collection unit is stored in the blockchain data storage apparatus, and

the transaction data to which the attribute of the year/month/date is added by the data conversion unit and which can be distinguished by the year/month/date is stored in the transaction data storage apparatus.

12. The cryptographic asset blockchain processing apparatus according to any one of claims 7 to 11, wherein

the cryptographic asset blockchain processing

apparatus further includes a data analysis unit,

the data conversion unit divides the transaction data into transaction input data and transaction output data, and

the data analysis unit calculates total revenue and total expenditure in a range of a specific block number based on the transaction input data and the transaction output data for each address that is a recording unit corresponding to a bank account number in the cryptographic asset blockchain.

13. The cryptographic asset blockchain processing apparatus according to any one of claims 7 to 11, wherein

the cryptographic asset blockchain processing apparatus further includes a data analysis unit, and

the data analysis unit calculates a balance for each address based on the transaction data and a result of a smart contract for each address that is a recording unit corresponding to a bank account number in the cryptographic asset blockchain.

14. The cryptographic asset blockchain processing apparatus according to any one of claims 1 to 6, wherein

the cryptographic asset blockchain processing apparatus further includes a consistency verification unit,

the transaction data includes block data to which a sequence number is assigned in a generation order,

the consistency verification unit checks whether the sequence number is duplicated or missing by sequentially collating the sequence number of the block data, and

in a case where there is a duplication or missing in the sequence number, notification of inconsistency of the block data corresponding to the sequence number is provided.

15. The cryptographic asset blockchain processing apparatus according to claim 14, wherein

the consistency verification unit counts the number of transaction data for each sequence number with respect to transaction data having a sequence number of a belonging block, and compares the number counted of transaction data with the number of transactions recorded in block data to which the sequence number is assigned, and

provides notification of an inconsistency of the block data in a case where there is a difference.

16. The cryptographic asset blockchain processing apparatus according to claim 9 or 13, wherein

the cryptographic asset blockchain processing apparatus further includes a consistency verification unit,

the consistency verification unit calculates a verification balance of an address designated by a user using a block explorer managed by a third party,

acquires a balance at the address designated from a

balance calculated for each address by the data analysis unit, and compares the balance calculated by the data analysis unit with the verification balance, and

provides notification that there is an inconsistency in data of the address designated in a case where there is a difference.

17. The cryptographic asset blockchain processing apparatus according to any one of claims 14 to 16, wherein

the consistency verification unit accesses a site that manages a version of node software of a cryptographic asset, checks a latest version of node software of a cryptographic asset desired, compares the latest version with a version of node software of the cryptographic asset stored in the data storage apparatus, and provides notification that there is an inconsistency in the version of the node software of the cryptographic asset in a case where there is a difference in the version.

18. A cryptographic asset blockchain processing method comprising:

a step of accessing a cryptographic asset blockchain designated by a user;

a step of collecting blockchain data from the cryptographic asset blockchain based on a request range predetermined; and

a step of converting the blockchain data into

analyzable transaction data, wherein

the blockchain data and the analyzable transaction data are stored in a data storage apparatus connected to the cryptographic asset blockchain processing apparatus.

19. The cryptographic asset blockchain processing method according to claim 18, wherein

the data storage apparatus is a cloud storage accessible by the cryptographic asset blockchain processing apparatus via a network.

20. The cryptographic asset blockchain processing method according to claim 18 or 19, further comprising a step of designating the number of transaction data for each data batch and setting an end point of the request range, and setting identification information of last transaction data of data collected last time as a start point of the request range, according to a static mode designated by a user.

21. The cryptographic asset blockchain processing method according to claim 18 or 19, further comprising a step of designating a data size for each data batch and setting an end point of the request range, and setting identification information of last transaction data of data collected last time as a start point of the request range, according to a static mode designated by a user.

22. The cryptographic asset blockchain processing method according to claim 18 or 19, further comprising:

a step of acquiring identification information of latest data on the cryptographic asset blockchain, and setting the identification information as an end point of the request range, according to an automatic collection mode designated by a user; and

a step of setting identification information of last transaction data of data collected last time by the data collection unit as a start point of the request range.

23. The cryptographic asset blockchain processing method according to claim 22, further comprising a step of, when a previous collection mode is a static mode in which the number of transaction data for each data batch is designated or a dynamic mode in which a data size for each data batch is designated, recalculating identification information of last transaction data of data collected last time based on the number of transaction data or the data size of the previous collection mode and sets the identification information as a start point of the request range.

24. The cryptographic asset blockchain processing method according to any one of claims 18 to 23, wherein

the blockchain data includes transaction data to which an identifiable block number is assigned, and

the transaction data includes at least one or more pieces of unit price transaction data for unit price

setting and one or more pieces of quantity transaction data for quantity designation,

the cryptographic asset blockchain processing method further comprising:

a step of searching, for each of the one or more pieces of quantity transaction data, transaction data for unit price setting to which a block number closest to a block number assigned to the one or more pieces of quantity transaction data is assigned; and

a step of calculating an amount of money related to a transaction by multiplying a value of a unit price of the unit price transaction data searched by a quantity of the one or more pieces of quantity transaction data.

25. The cryptographic asset blockchain processing method according to claim 24, wherein

the data storage apparatus includes a blockchain data storage apparatus and a transaction data storage apparatus, and

the step of collecting the blockchain data includes storing the blockchain data collected in the blockchain data storage apparatus,

the cryptographic asset blockchain processing method further comprising

a step of storing transaction data including the amount of money calculated in the transaction data storage

apparatus.

26. The cryptographic asset blockchain processing method according to claim 25, further comprising:

a step of acquiring the transaction data matching a block number from a first block number to a block number at a specific time point from the transaction data storage apparatus; and

a step of calculating a balance by adding an amount of money of the transaction data acquired for each address that is a recording unit corresponding to a bank account number in the cryptographic asset blockchain.

27. The cryptographic asset blockchain processing method according to any one of claims 18 to 23, wherein

the blockchain data includes at least block data and transaction data,

the cryptographic asset blockchain processing method further comprising:

a step of adding an attribute of year/month/date related to a transaction date and time to each of the block data and the transaction data to convert the block data and the transaction data into transaction data distinguishable by year/month/date; and

a step of classifying the transaction data for each year/month/date and storing the transaction data classified in the data storage apparatus.

28. The cryptographic asset blockchain processing method according to claim 27, wherein

the data storage apparatus includes a blockchain data storage apparatus and a transaction data storage apparatus, and

the step of collecting the blockchain data includes storing the blockchain data collected in the blockchain data storage apparatus,

the cryptographic asset blockchain processing method further comprising

a step of storing the transaction data to which the attribute of the year/month/date is added by the data conversion unit and which can be distinguished by the year/month/date in the transaction data storage apparatus.

29. The cryptographic asset blockchain processing method according to any one of claims 24 to 28, further comprising:

a step of dividing the transaction data into transaction input data and transaction output data; and

a step of calculating total revenue and total expenditure in a range of a specific block number based on the transaction input data and the transaction output data for each address that is a recording unit corresponding to a bank account number in the cryptographic asset blockchain.

30. The cryptographic asset blockchain processing method according to any one of claims 24 to 28, further comprising a step of calculating a balance for each address based on the transaction data and a result of a smart contract for each address that is a recording unit corresponding to a bank account number in the cryptographic asset blockchain.

31. The cryptographic asset blockchain processing method according to any one of claims 18 to 23, wherein

the transaction data includes block data to which a sequence number is assigned in a generation order,

the cryptographic asset blockchain processing method further comprising:

a step of checking whether the sequence number is duplicated or missing by sequentially collating the sequence number of the block data; and

a step of, in a case where there is a duplication or missing in the sequence number, providing notification of inconsistency of the block data corresponding to the sequence number.

32. The cryptographic asset blockchain processing method according to claim 31, further comprising:

a step of counting the number of transaction data for each sequence number with respect to transaction data having a sequence number of a belonging block, and compares the number counted of transaction data with the number of

transactions recorded in block data to which the sequence number is assigned; and

a step of providing notification of an inconsistency of the block data in a case where there is a difference.

33. The cryptographic asset blockchain processing method according to claim 26 or 30, further comprising:

a step of calculating a verification balance of an address designated by a user using a block explorer managed by a third party;

a step of acquiring a balance at the address designated from a balance calculated for each address by the data analysis unit, and comparing the balance calculated by the data analysis unit with the verification balance; and

a step of providing notification that there is an inconsistency in data of the address designated in a case where there is a difference.

34. The cryptographic asset blockchain processing method according to any one of claims 31 to 33, further comprising:

a step of accessing a site that manages a version of node software of a cryptographic asset;

a step of checking a latest version of node software of a cryptographic asset desired;

a step of comparing the latest version with a

version of node software of the cryptographic asset stored in the data storage apparatus; and

a step of providing notification that there is an inconsistency in the version of the node software of the cryptographic asset in a case where there is a difference in the version.

35. A cryptographic asset blockchain processing system comprising:

the cryptographic asset blockchain processing apparatus according to any one of claims 1 to 17;

an information processing terminal; and

a cloud storage, wherein

the cryptographic asset blockchain processing apparatus, the information processing apparatus, and the cloud storage are connected via a network.

36. A cryptographic asset blockchain processing program that is executed by a computer to cause the computer to function as each unit of the cryptographic asset blockchain processing apparatus according to any one of claims 1 to 17.

37. A cryptographic asset blockchain processing program that is executed by a computer to cause the computer to execute each step of the cryptographic asset blockchain processing method according to any one of claims 18 to 34.