

TITLE OF INVENTION: UNSPENT TRANSACTION OUTPUT FINANCIAL TAGGING SYSTEM

Technical Field

The present invention relates to a server and a method for operating a financial system using transaction tags based on unspent transaction outputs (UTXOs).

Background Art

Financial systems utilizing blockchain technology are actively being researched. When a transaction that alters a wallet balance occurs, the transaction record may be stored on a distributed ledger, and such records can serve as the basis for operating a decentralized financial system. However, the transaction records disclosed through the distributed ledger contain only limited information, which presents a challenge in providing meaningful insights to potential trading parties based solely on publicly available data.

Summary of the Invention

One of the objectives of the present invention is to provide a financial system that supplements the limited information available from a blockchain distributed ledger by publicly disclosing various types of transaction-related information in the form of tags.

According to certain embodiments of the present invention, a server for operating a blockchain financial system comprises:

a memory configured to store instructions; and

a processor configured to execute the instructions to:

- set a transaction input of a target transaction based on a first unspent transaction output (UTXO) list of a withdrawal wallet;
- update the first UTXO list to a second UTXO list of the withdrawal wallet based on a transaction output of the target transaction for a deposit wallet and the transaction input;
- generate transaction tags for the target transaction based on balance information of the withdrawal wallet according to the second UTXO list and transaction information of the target transaction; and
- record the transaction tags on a blockchain distributed ledger together with the target transaction.

According to certain embodiments, each of the transaction tags includes a keyword of the target transaction, a value length, and a value describing the target transaction.

According to certain embodiments, the transaction information includes payee information, payer information, transaction type, and transaction name of the target transaction, and the balance information includes the sum of UTXO balances contained in the second UTXO list.

According to certain embodiments, the processor is further configured to serialize the transaction input and transaction output, tag the transaction tags thereto to generate a deduplication key, and record the target transaction on the blockchain distributed ledger based on the deduplication key.

According to certain embodiments, the processor is configured to use a sorting

algorithm to check, based on the deduplication key, whether the target transaction is redundantly recorded on the blockchain distributed ledger, and to perform deduplication for the redundantly recorded transaction.

According to certain embodiments, the processor is configured to encrypt the transaction tags for information hiding and generate encrypted tags, and to decrypt the encrypted tags each time they are retrieved from the blockchain distributed ledger.

According to certain embodiments, the processor is configured to provide transaction statistical data and trend data for the transaction information of the target transaction based on the transaction tags recorded on the blockchain distributed ledger.

According to certain embodiments, the transaction tags include transaction policy information of a buyer associated with the withdrawal wallet or a seller associated with the deposit wallet, and the transaction policy information is publicly disclosed through the blockchain distributed ledger.

According to certain embodiments, the transaction policy information includes transaction conditions, transaction availability, and fund usage.

According to certain embodiments, the number of transaction tags recorded with the target transaction on the blockchain distributed ledger is determined based on a tag fee policy of the buyer associated with the withdrawal wallet or the seller associated with the deposit wallet.

According to certain embodiments, a method for operating a blockchain financial

system, performed by a processor executing instructions stored in a memory, comprises: setting a transaction input of a target transaction based on a first unspent transaction output (UTXO) list of a withdrawal wallet; updating the first UTXO list to a second UTXO list of the withdrawal wallet based on a transaction output of the target transaction for a deposit wallet and the transaction input; generating transaction tags for the target transaction based on balance information of the withdrawal wallet according to the second UTXO list and transaction information of the target transaction; and recording the transaction tags on a blockchain distributed ledger together with the target transaction.

According to embodiments of the present invention, a financial system may be provided that supplements the limited information available from a blockchain distributed ledger by appending various types of transaction-related information in the form of tags and publicly recording them on the distributed ledger.

Brief Description of the Drawings

- FIG. 1 illustrates components of a blockchain financial system according to certain embodiments.
- FIG. 2 illustrates components of a server for operating a blockchain financial system according to certain embodiments.
- FIG. 3 illustrates an example of a transaction tag according to certain embodiments.

- FIGS. 4 to 7 illustrate pseudocode examples for implementing operations of the blockchain financial system according to certain embodiments.
- FIG. 8 illustrates steps of a method for operating a blockchain financial system according to certain embodiments.

Detailed Description

The embodiments of the present invention will now be described in detail with reference to the accompanying drawings. The following description is provided merely to illustrate specific examples of embodiments, and is not intended to limit the scope of the invention. Those skilled in the art to which the invention pertains will appreciate that modifications, equivalents, and alternatives that can be readily derived from the detailed description and drawings also fall within the scope of the invention. Well-known components and techniques may be omitted from the description when they are deemed unnecessary to facilitate understanding of the invention.

The terminology used in this specification is to be interpreted based on the general meaning in the relevant technical field, unless otherwise defined. It should be noted that the meanings of certain terms may vary depending on the intention of the inventors, advances in technology, examination guidelines, or judicial decisions. Some terms may have been defined arbitrarily by the applicant, in which case their meanings will be clearly described herein. Accordingly, the terminology should be interpreted in light of the overall context of the specification and not solely based on dictionary definitions.

FIG. 1 illustrates components of a blockchain financial system according to certain embodiments.

Referring to FIG. 1, a blockchain financial system 100 may include a seller device 110, a buyer device 120, an exchange 130, a server 140 for operating the blockchain financial system, and a distributed ledger 150.

The blockchain financial system 100 may refer to a system that supports financial transactions between users using blockchain-based cryptocurrencies or virtual assets. A seller may receive cryptocurrency or virtual assets in exchange for providing goods or services, and a buyer may purchase goods or services using cryptocurrency or virtual assets. Alternatively, a seller may sell fiat currency (such as KRW or USD) to receive cryptocurrency or virtual assets, and a buyer may provide cryptocurrency or virtual assets to purchase fiat currency.

The seller and the buyer may conduct transactions through the exchange 130 using their respective devices 110 and 120. One of the seller device 110 or the buyer device 120 may submit an offer to sell or purchase via the exchange 130, and the other party may accept the offer, thereby forming a transaction through the exchange 130. For example, the exchange 130 may be a cryptocurrency exchange that facilitates trading between fiat and virtual currencies, or an open marketplace that supports cryptocurrency-based payments for goods or services.

The server 140 operates the blockchain financial system 100 by executing computer programs, mobile applications, or other software implementations. The server 140 may manage blockchain-related operations necessary to facilitate transactions between sellers and buyers. The server 140 may record transaction processes and outcomes to the distributed ledger 150. The distributed ledger 150 may publicly record the circulation history of cryptocurrencies or virtual assets in a decentralized manner based on blockchain technology.

FIG. 2 illustrates components of a server for operating a blockchain financial system according to certain embodiments.

Referring to FIG. 2, a server 140 for operating the blockchain financial system may include a memory 141 and a processor 142. However, the server 140 is not limited thereto, and certain components may be omitted or additional general-purpose components may be included. For example, the server 140 may further include a communication module for communicating with a seller device 110, a buyer device 120, and an exchange 130.

The memory 141 may be configured to store various instructions, computer programs, software, mobile applications, or data processed by the server 140. For example, the memory may be implemented as non-volatile memory such as ROM, PROM, EPROM, EEPROM, flash memory, PRAM, MRAM, RRAM, or FRAM; or volatile memory such as DRAM, SRAM, SDRAM, PRAM, RRAM, or FeRAM. It may also be implemented in the form of HDDs, SSDs, SD or Micro-SD cards, or combinations thereof.

The processor 142 may be configured to perform processing required for the operation of the server 140. The processor 142 may be implemented as an array of logic gates or a general-purpose microprocessor for handling various computations, and may comprise a single processor or a plurality of processors. For example, the processor 142 may be implemented as a microprocessor, CPU, GPU, AP, or any combination thereof.

The processor 142 may be configured to set a transaction input of a target transaction based on a first unspent transaction output (UTXO) list of a withdrawal wallet. A transaction may refer to a unit of operation that changes the state of a distributed ledger 150 or a wallet. When a transaction is performed, a balance corresponding to the difference between the input and output amounts may occur, and such a balance that has not been spent by subsequent transactions may be referred to as a UTXO. The withdrawal wallet of a buyer in the blockchain financial system 100 may already include UTXOs, which constitute the first UTXO list. The buyer performs a payment transaction using UTXOs from the withdrawal wallet, and at least some of the UTXOs may be set as transaction inputs of the target transaction. For example, the first UTXO list may include two UTXOs of 1 BTC and 5 BTC. A 5 BTC UTXO may be selected as the transaction input to purchase 3 BTC worth of goods, services, or fiat currency. The processor 142 may be configured to update the first UTXO list to a second UTXO list of the withdrawal wallet based on a transaction output of the target

transaction for a deposit wallet and the transaction input. For example, if 3 BTC is used for a purchase from a 5 BTC UTXO, the remaining 2 BTC may be returned as a new UTXO. The 5 BTC UTXO is thus replaced with a 2 BTC UTXO, and the first UTXO list is updated accordingly to the second UTXO list. This update process may be recorded on the distributed ledger 150.

The processor 142 may be configured to generate transaction tags for the target transaction based on balance information of the withdrawal wallet according to the second UTXO list and transaction information of the target transaction. The transaction tags may be publicly disclosed to unspecified users and represent information related to the target transaction, such as the buyer, seller, resulting balance (UTXO), transaction type, transaction category, contract format, and transaction progress stages. For example, the transaction tags may function similarly to transfer memos in banking, but unlike memos shared only between parties, the tags are publicly accessible to third parties.

The processor 142 may be configured to record the transaction tags on the blockchain distributed ledger together with the target transaction. Since the transaction tags can be accessed by unspecified users on the distributed ledger 150, transaction trends and statistics may be analyzed based on the tags. For example, one may analyze how frequently certain types or forms of transactions are occurring.

In some embodiments, each transaction tag may include a keyword, a value length,

and a value describing the target transaction. For example, as illustrated in FIG. 3, each tag may include a keyword (KEY), length (LENGTH), and value (VALUE). The tag may follow a KEY-LENGTH-VALUE structure, which enables efficient data structuring and delivery of transaction-related information.

In some embodiments, the transaction information may include payee information, payer information, transaction type, and transaction name, while the balance information may include the sum of UTXO balances in the second UTXO list. By publicly disclosing this minimum information, transaction types and frequencies may be analyzed, which can support transaction planning and promote transaction volume. For example, the transaction type may include spot, futures, conditional, scheduled, collateralized, periodic, or renewable transactions.

The processor 142 may be further configured to serialize the transaction input and transaction output, tag the transaction tags thereto, and generate a deduplication key. Based on the deduplication key, the target transaction may be recorded on the blockchain distributed ledger. The serialization of the input and output may simplify the data structure, while the transaction tags may remain un-serialized. This combined data can function as the deduplication key and prevent duplicate records on the ledger 150.

The processor 142 may be configured to use a sorting algorithm to check whether the target transaction has already been recorded based on the deduplication key and remove duplicates. Various sorting algorithms may be used, including bubble

sorting or other algorithms.

The processor 142 may also be configured to encrypt the transaction tags for information hiding and generate encrypted tags. The encrypted tags may be decrypted each time they are retrieved from the blockchain distributed ledger. While transaction tags are by default intended for public disclosure, in exceptional cases, private information may be included and encrypted. In such cases, when authorized parties access the tags on the distributed ledger 150, decryption may be performed upon each access.

The processor 142 may further be configured to provide transaction statistical data and trend data based on the transaction tags recorded on the blockchain distributed ledger. Since the ledger 150 records a large number of transactions along with their tags, statistical and trend analysis can be performed. For example, it may be possible to retrieve how transaction volumes for specific types have changed over a month, a week, or other timeframes. Statistics may also be provided for transactions involving particular cryptocurrencies. The statistical data may include transaction frequency, transaction count, total transaction value, average transaction amount, and user asset distribution.

The transaction tags may include transaction policy information of the buyer associated with the withdrawal wallet or the seller associated with the deposit wallet, which may be publicly disclosed via the blockchain distributed ledger. For example, during analysis of trends, those interested in transacting with

specific buyers or sellers may view their transaction policy information via the ledger 150. This information may include contractual constraints, minimum transaction amounts, available transaction timeframes, and eligibility criteria for private transactions.

The transaction policy information may include transaction conditions, availability, and fund usage. For example, transaction conditions may be specified in contracts and include monetary, temporal, frequency, eligibility, currency, or usage conditions. Availability may vary by user and be determined by factors such as time, amount, credit, and usage, and may be disclosed via transaction tags. Fund usage information may indicate where a cryptocurrency purchased with fiat (e.g., KRW or USD) can be used.

The number of transaction tags recorded together with the target transaction may be determined based on a tag fee policy of the buyer or seller. A user may wish to disclose as much information as possible via the blockchain financial system 100. According to system policy, a certain number of tags may be provided free of charge, while additional tags may incur fees.

FIG. 3 illustrates a transaction tag according to certain embodiments.

Referring to FIG. 3, a table 310 and a data structure 320 are shown to exemplify the structure of a transaction tag.

As illustrated in the table 310, a transaction tag may include a keyword (KEY), a data length (LENGTH), and a data value (VALUE). The KEY may represent attributes such as expiration time of balance, payee information, payer information, transaction type, or transaction name. The LENGTH may indicate the size or length of the subsequent VALUE, and the VALUE may contain a description corresponding to the KEY. For example, as shown in the data structure 320, the KEY and LENGTH may each be configured as 1 byte, and the VALUE may be configured as 4 bytes.

A transaction tag may represent a keyword of a transaction, and may be combined with a serialized ID (e.g., UHS, UTXO hash set) to form a single key, which may be used for deduplication. The transaction tag may follow a KEY-LENGTH-VALUE (KLV) format. The KEY may be 1 byte in size and support up to 254 different keys. The LENGTH may also be 1 byte and indicate the length of the VALUE, while the VALUE may store unsigned data according to the length specified in the LENGTH.

There may be no inherent limit on the number of transaction tags included in a transaction. However, the number of tags may be limited according to a fee policy.

Regarding security, the transaction tags may not undergo a separate encryption process by default. This is because the system may prioritize the benefits of public disclosure over data confidentiality. Accordingly, the transaction tags may not store data containing sensitive information.

With respect to encryption for information hiding, an encrypted tag may be decrypted each time it is accessed for purposes such as conducting a transaction or performing transaction analysis. Although repeated decryption may reduce analysis performance, it may be considered acceptable in favor of protecting sensitive data.

FIGS. 4 to 7 illustrate pseudocode examples of operations of the blockchain financial system according to certain embodiments.

Referring to FIG. 4, a first pseudocode example 400 for implementing operations of the blockchain financial system 100 is illustrated. In the pseudocode 400, a tag may have a KEY-LENGTH-VALUE structure and may represent a unique tag corresponding to a specific transaction input. The tag may not be directly readable by humans and may require interpretation through the blockchain financial system 100.

Referring to FIG. 5, a second pseudocode example 500 for implementing operations of the blockchain financial system 100 is illustrated. An outpoint of a transaction may be a unique identifier of a specific transaction output. The transaction output may refer to an output of the transaction. In the blockchain financial system 100, the transaction structure may be configured identically to a conventional transaction structure, except for the inclusion of transaction tags.

Referring to FIG. 6, a third pseudocode example 500 for implementing operations of the blockchain financial system 100 is illustrated. A transaction input may refer to an input of a new transaction. By default, transaction tags may be used in the order they are registered. A witness may refer to a verification for the transaction.

Referring to FIG. 7, a fourth pseudocode example 600 for implementing operations of the blockchain financial system 100 is illustrated. With respect to compression, transaction inputs and outputs may be serialized. However, transaction tags may not be serialized. When the transaction tags are added to the serialized inputs and outputs, they may function as a key for duplication checking. Data determined to be duplicates may be deleted. For example, bubble sorting may be used to detect and delete duplicate data.

FIG. 8 illustrates a flowchart of steps of a method for operating the blockchain financial system according to certain embodiments.

Referring to FIG. 8, a method 800 for operating the blockchain financial system may include steps 810 to 840. However, the method is not limited thereto, and some steps may be omitted or other general steps may be added. The steps of the method 800 may be performed in an order different from that shown.

The method 800 for operating the blockchain financial system may be composed of time-series processing steps performed by a server 140 operating the blockchain financial system. Accordingly, even if omitted below, descriptions pertaining to the server 140 also apply to the method 800.

The steps 810 to 840 of the method 800 may be performed by the memory 141 and the processor 142 of the server 140.

In step 810, the server 140 may set a transaction input of a target transaction based on a first unspent transaction output (UTXO) list of a withdrawal wallet.

In step 820, the server 140 may update the first UTXO list to a second UTXO list of the withdrawal wallet based on a transaction output of the target transaction for a deposit wallet and the transaction input.

In step 830, the server 140 may generate transaction tags for the target transaction based on balance information of the withdrawal wallet according to the second UTXO list and transaction information of the target transaction.

In step 840, the server 140 may record the transaction tags on a blockchain distributed ledger together with the target transaction.

According to certain embodiments, the method 800 for operating the blockchain financial system may be implemented in the form of a computer program stored on a computer-readable storage medium. That is, the computer program may include instructions for implementing the method 800, and the program instructions may be stored on a computer-readable storage medium. The computer program may include a mobile application.

The computer-readable storage medium may include magnetic media such as hard disks, floppy disks, and magnetic tapes; optical media such as CD-ROMs and DVDs; magneto-optical media such as floptical disks; and hardware devices specially configured to store and execute program instructions, such as ROM, RAM, and

flash memory. The program instructions may include machine code generated by a compiler and high-level language code executed by an interpreter.

Although the embodiments of the present invention have been described in detail above, the scope of the present invention is not limited thereto, and various modifications and improvements utilizing the basic concepts described in the following claims by those skilled in the art shall also fall within the scope of the present invention.

What is claimed is:

[Claim 1] A server for operating a blockchain financial system, the server comprising:

a memory configured to store instructions; and

a processor configured to execute the instructions to:

set a transaction input of a target transaction based on a first unspent transaction output (UTXO) list of a withdrawal wallet,

update the first UTXO list to a second UTXO list of the withdrawal wallet based on a transaction output of the target transaction for a deposit wallet and the transaction input,

generate, based on balance information of the withdrawal wallet according to the second UTXO list and transaction information of the target transaction, transaction tags for the target transaction, and

record the transaction tags on a blockchain distributed ledger together with the target transaction.

[Claim 2] **The server of claim 1**, wherein each of the transaction tags includes a keyword of the target transaction, a value length, and a value describing the target transaction.

[Claim 3] **The server of claim 1**, wherein the transaction information includes payee information of the target transaction, payer information of the target transaction, a transaction type, and a transaction name, and

wherein the balance information includes a sum of UTXO balances included in the second UTXO list.

[Claim 4] **The server of claim 1**, wherein the processor is configured to serialize the transaction input and the transaction output, tag the transaction tags to the serialized transaction input and the transaction output to generate a deduplication key, and record the target transaction on the blockchain distributed ledger based on the deduplication key.

[Claim 5] **The server of claim 4**, wherein the processor is configured to use a sorting algorithm to check, based on the deduplication key, whether the target transaction is recorded redundantly on the blockchain distributed ledger, and perform deduplication on the target transaction that is recorded redundantly.

[Claim 6] **The server of claim 1**, wherein the processor is configured to perform encryption on the transaction tags to generate encrypted tags for information hiding, and wherein each time the encrypted tags are retrieved from the blockchain distributed ledger, the encrypted tags are decrypted.

[Claim 7] **The server of claim 1**, wherein the processor is configured to provide, based on the transaction tags recorded on the blockchain distributed ledger, transaction statistical data and transaction trend data for the transaction information of the target transaction.

[Claim 8] **The server of claim 1**, wherein the transaction tags include transaction policy information of a buyer associated with the withdrawal

wallet or a seller associated with the deposit wallet, wherein the transaction policy information is disclosed via the blockchain distributed ledger, and wherein the transaction policy information includes a transaction condition, a transaction availability, and a fund usage.

[Claim 9] **The server of claim 1**, wherein the transaction tags include transaction policy information of a buyer associated with the withdrawal wallet or a seller associated with the deposit wallet, wherein the transaction policy information is disclosed via the blockchain distributed ledger, and wherein a number of the transaction tags recorded with the target transaction is determined based on a tag fee policy of the buyer or the seller.

[Claim 10] **A method for operating a blockchain financial system, the method comprising:**

setting a transaction input of a target transaction based on a first unspent transaction output (UTXO) list of a withdrawal wallet;

updating the first UTXO list to a second UTXO list of the withdrawal wallet based on a transaction output of the target transaction for a deposit wallet and the transaction input;

generating, based on balance information of the withdrawal wallet according to the second UTXO list and transaction information of the target transaction, transaction tags for the target transaction; and

recording the transaction tags on a blockchain distributed ledger

together with the target transaction.