

Digital currencyField of invention

The present invention relates to a method of performing a transaction, in particular a method of storing different sets of information relating to the transaction in different places.

5     Background

Existing methods and systems for performing transactions typically involve the transfer of fiat currency between two parties in exchange for a good or service. Once the transaction has been completed, there is little to no record of the transaction and the currency can thereafter be used freely. It is difficult to determine whether a transaction involves an undesirable element, such as a corrupt party, and even if an undesirable element is identified, it is difficult to influence the transaction after it has been made.

10     Summary

Aspects and embodiments of the present invention are set out in the appended claims. These and other aspects and embodiments of the invention are also described herein.

According to least one aspect of the present disclosure, there is described a computer-implemented method of performing a transaction using a coin, the method comprising: determining a state of fungibility of the coin; and completing the transaction in dependence on the state of fungibility. By determining a state of fungibility, a transaction can be performed using a coin that has an alterable (or transitive) state of fungibility. This enables use of a coin, where the fungibility may be altered to prohibit use of the coin.

Preferably, the coin comprises an indication of the state of fungibility.

20     Preferably, the possible states of fungibility comprise at least one of: fungible, non-fungible, or partially fungible.

Preferably, coins that are not fungible can only be exchanged with the permission of the receiving party.

Preferably, coins that are not fungible are prohibited from being exchanged with one or more parties.

Preferably, the state of fungibility is alterable in dependence on a feature of the transaction.

25     Preferably, the feature comprises at least one of: a party to the transaction; a market sector of the transaction; a good and/or service involved in the transaction; an elapsed time; and the number of transactions for which the coin has been used.

Preferably, the state of fungibility is arranged to be altered automatically in dependence on a feature of the coin.

30     Preferably, the state of fungibility data is arranged to be altered in dependence on an algorithm, an artificial intelligence, and/or a machine learning process.

Preferably, the state of fungibility is alterable by a third party. Preferably, the state of fungibility is alterable by a government institution and/or a central bank.

35     Preferably, the state of fungibility is arranged to be altered in dependence on a term of a smart contract relating to the coin. Preferably, the terms of the smart contract are stored on the coin.

Preferably, the smart contract comprises an indication of allowable transactions, preferably wherein the coin is arranged to only be useable for allowable transactions and/or wherein use of the coin for non-allowable transactions results in a change in the state of fungibility.

40     Preferably, the smart contract comprises information relating to authorised parties that are able to alter the state of fungibility of the coin and/or are able to view information relating to the coin.

Preferably, the method further comprises providing an indication of the state of fungibility. Preferably, the indication is only provided if the coin is not in a fungible state.

Preferably, the coin has a fixed value.

45     Preferably, the method comprises completing the transaction using a plurality of coins, wherein each of the plurality of coins has a different, fixed, value.

According to another aspect of the present disclosure, there is described a computer-implemented method of performing a transaction using a plurality of coins, wherein each of the plurality of coins has a different, fixed, value.

Preferably, the value of the coin is fixed at the time of issue of the coin.

Preferably, the coin contains an indication of a fiat currency and/or commodity for which the coin can be exchanged.

Preferably, the coin contains an indication of an exchange rate for which the coin can be exchanged.

Preferably, the coin comprises provenance data.

- 5 Preferably, the state of fungibility is arranged to change in dependence on the provenance data.

Preferably, the provenance data relates to the history of ownership of the coin, the transactional history of the coin, and/or the history of the state of fungibility of the coin.

Preferably, the coin is arranged so that provenance information is required to be verified by a third party before the provenance information addition to the provenance data.

- 10 Preferably, the provenance data comprises: a first set of data that is determined at the time of the transaction and is thereafter immutable; and a second set of data that is alterable following the transaction.

According to another aspect of the present disclosure, there is described a computer-implemented method of providing a coin, wherein the coin comprises provenance data and the provenance data comprises: a first set of data that is determined at the time of the transaction and is thereafter immutable; and a second set of data that is alterable following the transaction.

- 15

Preferably, the second set of data is alterable by a third party. Preferably, the third party is an authorised third party.

- 20 Preferably, the method further comprises updating the provenance data of the coin following the transaction.

Preferably, the method further comprises updating the provenance data of the coin based on the usage of a similar coin.

Preferably, the method further comprises predicting future transactions based on the provenance data. Preferably, the method comprises outputting the prediction.

- 25 Preferably, the method further comprises valuating the transaction and outputting the evaluation.

Preferably, completing the transaction requires one or more parties to the transaction to record provenance data relating to the transaction.

Preferably, completing the transaction requires consensus from one or more third parties.

- 30 Preferably, the method further comprises recording the consent of each party to the transaction at the time of the transaction.

Preferably, the coin is permissioned so as to allow only permissioned parties to view data relating to the coin.

Preferably, completing the transaction comprises recording confirmation from each party to the transaction.

- 35 Preferably, the coin comprises at least one of: an owner field, a value field, an identifier, conditions of use.

Preferably, the coin is automatically redeemed upon completion of the terms of a smart contract.

Preferably, the coin may be divided into a plurality of sub-coins, wherein the value of each sub-coin differs from the value of the coin, and wherein each sub-coin inherits properties from the coin.

- 40 Preferably, the coin comprises an indication of a state of fungibility, and wherein the state of fungibility is alterable.

According to another aspect of the present disclosure, there is described a computer-implemented method of performing a transaction using a coin, wherein the coin comprises provenance data and the provenance data comprises: a first set of data that is determined at the time of the transaction and is thereafter immutable; and a second set of data that is alterable following the transaction, the method comprising: determining a state of fungibility of the coin; completing the transaction in dependence on the state of fungibility; updating the provenance data in dependence on a feature of the transaction; and altering the state of fungibility of the coin in dependence on the provenance data.

- 45

According to another aspect of the present disclosure, there is described a computer-implemented coin, the coin comprising an indication of a state of fungibility.

According to another aspect of the present disclosure, there is described a computer-implemented coin, the coin comprising provenance data, the provenance data comprising: a first set of data that is determined at the time of the transaction and is thereafter immutable; and a second set of data that is alterable following the transaction.

- 5 According to another aspect of the present disclosure, there is described a computer-implemented method of altering the state of fungibility of a coin, wherein the coin comprises an indication of a state of fungibility.

According to another aspect of the present disclosure, there is described a computer-implemented method of performing a transaction using a coin, the method comprising: storing a first set of information relating to the transaction in relation to the coin; and storing a second set of information relating to the transaction in  
10 a datastore separate to the coin; and providing an output relating to the first set of information and/or the second set of information.

Preferably, the first set of information comprises one or more of: a transaction amount; a sender; and a recipient.

- 15 Preferably, the first set of information comprises a sender and/or recipient. Preferably, the sender and/or recipient comprises an identifier. Preferably, the sender and/or recipient comprises a randomly generated and/or pseudo-randomly generated identifier.

Preferably, the first set of information consists of a transaction amount.

- 20 Preferably, the second set of information comprises provenance information and/or wherein the second set of information comprises at least one of: a reason for the transaction; an assessment of a/the sender and/or a/the recipient, such as an indication of a trust level; and information added by a third party following the transaction.

Preferably, the first set of information is stored on a blockchain.

Preferably, the second set of information is stored in a digital currency wallet.

- 25 Preferably, the method further comprises providing an output relating to the second set of information in dependence on a request. Preferably, the request comprises an indication that a requesting party is authorised to access the second set of information.

Preferably, the storing of the second set of information occurs in dependence on a feature of the transaction.

- 30 Preferably, the datastore in which the second set of information is stored depends on the feature of the transaction.

Preferably, the composition of the first set of information and/or the second set of information depends on the feature of the transaction.

- 35 Preferably, the feature comprises one or more of: an ecosystem in which the transaction takes place; a determination that the transaction relates to a movement of the coin between two ecosystems; a party relating to the ecosystem; a party controlling and/or overseeing the ecosystem; a country and/or location in which the transaction occurs; the sender; and the recipient.

Preferably, the method further comprises a further datastore arranged to store information relating to further transactions.

- 40 Preferably, the datastore relates to a first ecosystem and the further datastore relates to a second ecosystem.

Preferably, the second set of information is stored in either the database or the further database in dependence on whether the transaction occurs in the first ecosystem or the second ecosystem.

Preferably, the method further comprises determining an ecosystem in which the transaction has taken place.

- 45 Preferably, the method further comprises only storing the second set of information if the transaction occurs in the first ecosystem.

According to another aspect of the present invention, there is described a computer-implemented method of performing a transaction using a coin, the method comprising: storing a first set of information relating to the transaction in relation to the coin; determining an ecosystem in which the transaction has taken place;  
50 and storing a second set of information relating to the transaction in a datastore separate to the coin,

wherein the datastore in which the second set of information is stored depends on the ecosystem in which the transaction has taken place.

Preferably, the composition of the second set of information is dependent on the ecosystem in which the transaction has taken place.

- 5 Preferably, the method further comprises determining a spending rule in dependence on the ecosystem in which the transaction has taken place; and altering the fungibility of the coin in dependence on the spending rule.

Preferably, the spending rule relates to at least one of: an industry in which the coin is allowed to be used; a good and/or service for which the coin is allowed to be used; a recipient to whom the coin is allowed to be sent; and a purpose for which the coin is allowed to be used.

- 10 Preferably, the datastore is capable of transmitting data from the second set of information to the further datastore and/or a further party.

- 15 Preferably, the datastore is arranged to transmit the data in dependence on a data request. Preferably, the data request comprises one or more of: provenance information relating to a separate transaction; a proof of identity; a monetary reward; and a mining reward. Preferably, the mining reward relates to activity on the a/the blockchain.

Preferably, the data request comprises information relating to a separate transaction performed in relation to the coin.

- 20 Preferably, the data request comprises evidence of information held by the datastore. Preferably, the data request comprises evidence of provenance information held by the datastore.

Preferably, the data request comprises a zero knowledge proof.

Preferably, the method further comprises determining a party that is authorised to receive data from the second set of information; and transmitting the data to the second party.

Preferably, the authorisation of the party is determined before the transaction occurs.

- 25 Preferably, the method further comprises transmitting the data to a party related to a/the second ecosystem. Preferably, the method further comprises transmitting the data in dependence on receiving similar data from the party related to the second ecosystem.

- 30 According to another aspect of the present invention, there is described an apparatus arranged to output information relating to a transaction using a coin, the apparatus comprising: means for storing a first set of information relating to the transaction in relation to the coin; and means for storing a second set of information relating to the transaction in a datastore separate to the coin.

According to another aspect of the present disclosure, there is described a computer program comprising software code adapted when executed to carry out any of the aforesaid methods.

- 35 According to another aspect of the present disclosure, there is described an apparatus adapted to execute the aforesaid computer program product.

According to an aspect of the present disclosure, there is described a smart, transitive and provenance-based digital currency which focuses on incorporating immutable data and intelligence into an economic coin.

The coin may be transitive between states that are:

- 40 - fungible and non-fungible;  
- market-tradeable and non-market-tradeable; and/or  
- agent-based provenance and coin-based provenance.

The coin may be:

- 45 • Serialised: The coin supports the serialization of digital currency, which enables the coin to store provenance information. Each coin has its own serial number so that it can be tracked within the system.
- Transitive in nature: The coin is used within a permissioned platform. It is exchanged from a fiat currency at the beginning of a transaction (e.g. when it enters the system) into coins linked to that currency and, usually, converted to a predetermined end fiat currency at the end of the transaction.
- 50 Every transaction has a forex management process.

The properties of the coin are alterable, so that the coin is transitive between multiple states. In particular, the coin is transitive between a fungible and a non-fungible state. The fungible state may relate to the coin being redeemable for a fiat currency whereas the non-fungible state may relate to the coin not being redeemable for a fiat currency.

- 5     • Provenance based: the chronology of ownership, custody or location of the coin provides validation and verification of agents involved, entities and the use of the coin over time. The coin typically comprises multiple provenance layers that are used for investigating and authenticating provenance.

10     There are 3 primary elements of provenance: Entity, activity and agent. The unique, transparent digital identifiers used to describe the agents (transactors) and entities (the objects that they transact) allows for the establishment and exploration of an immutable audit trail of time-stamped Activity (ownership, location, modification etc.).

- 15     • Coin-resident provenance: The provenance is typically captured and stored on each individual coin.
- Backed: As the coin is issued in return for fiat currency or another commodity with a stable price (e.g. gold), the coin is backed initially by that currency/gold and if there is a fall in value of the initial currency/gold, the value can be made up with additional amounts of that currency/any other currency/commodity of value.

- 20     • Non-market traded: Cryptocurrencies are usually volatile due to being traded on the exchange market, as their purpose is to make a profit. The coin may be non-market traded (either always or when the coin is in a non-fungible state) so that the coin cannot be used for speculation, thereby reducing volatility.

- 25     • Closed-permissioned platform: the coin is used within a limited peer-to-peer network by permission, those who join are typically required to give permission for all of their data to be accessed and captured. Only a small trusted community are allowed to issue the coin. In the permissioned system, the coin is the only currency used, enabling provenance to be captured in the sub-economy for each transaction.

- Stores immutable data: the data captured during a transaction relating to the construction, authentication, processing and completion of trade is stored in time-ordered sequences using Distributed Ledger Technology, such as Blockchains.

30     According to an aspect of the present disclosure, there is described a usable currency that captures and stores an immutable record of provenance on each unit, and uses that data to enable value to be delivered and generated in a transparent manner. This provides:

- Stability:
- 35     – the store of provenance information delivers inherent stability and trust as there is full transparency and a constant process of interrogation and verification.
- The non-market traded nature of the coin prevents volatility from speculation.
- The flexible transitive nature affords the ability to e.g. build a coin backed by gold and use fiat currency to make up for downfall if the price of gold drops, hence holding the value of the coin stable.

- Transparency:
- 40     – Proof of exploration provides an incentive for nodes to continuously explore and verify the provenance of each entity, agent and activity.
- A time-stamped audit trail allows for any person in the limited peer-to-peer network to be able to view activities from beginning to end, thus enabling each person to verify each stage of a transaction.

- 45     – Provenance information is stored on DLT such as Blockchain which is technology aiming to provide transparency and security through making the data stored on them immutable.

- Coin-based provenance:
- Storing provenance information on each coin rather than for each agent or account allows for more provenance information to be captured and tracked.

- Intelligent nature:
  - The possibility of 'switching off' the value of a coin (by making that coin non-fungible) enables action to be taken when it is suspected that the coin has been used for malicious purposes.
- Immutable record of data:
  - 5     – The immutable record enables the eventual transfer of important economic and provenance data to relevant parties.

There is disclosed herein a serialized coin that is alterable between a fungible and a non-fungible state, where the coin is use within a permissioned system, and wherein the coin contains provenance data relating to the context of transactions and/or the parties in the permissioned system.

- 10    The invention extends to any novel aspects or features described and/or illustrated herein.

Further features of the disclosure are characterised by the other independent and dependent claims.

According to a further aspect there is provided a coin as herein described; a method of using a coin as herein described; and a computer-implemented method of performing a transaction using a coin as herein described.

- 15    Any feature in one aspect of the disclosure may be applied to other aspects of the disclosure, in any appropriate combination. In particular, method aspects may be applied to apparatus aspects, and vice versa.

Furthermore, features implemented in hardware may be implemented in software, and vice versa. Any reference to software and hardware features herein should be construed accordingly.

- 20    Any apparatus feature as described herein may also be provided as a method feature, and vice versa. As used herein, means plus function features may be expressed alternatively in terms of their corresponding structure, such as a suitably programmed processor and associated memory.

It should also be appreciated that particular combinations of the various features described and defined in any aspects of the disclosure can be implemented and/or supplied and/or used independently.

- 25    The disclosure also provides a computer program and a computer program product comprising software code adapted, when executed on a data processing apparatus, to perform any of the methods described herein, including any or all of their component steps.

The disclosure also provides a computer program and a computer program product comprising software code which, when executed on a data processing apparatus, comprises any of the apparatus features described herein.

- 30    The disclosure also provides a computer program and a computer program product having an operating system which supports a computer program for carrying out any of the methods described herein and/or for embodying any of the apparatus features described herein.

- 35    The disclosure also provides a computer readable medium having stored thereon the computer program as aforesaid.

The disclosure also provides a signal carrying the computer program as aforesaid, and a method of transmitting such a signal.

The disclosure extends to methods and/or apparatus substantially as herein described with reference to the accompanying drawings.

- 40    Aspects and embodiments of the disclosure will now be described, purely by way of example, with references to the accompanying drawings in which:

Figure 1 shows a system in which two parties wish to make a transaction;

Figure 2 illustrates a computer device on which aspects of the disclosed system are implemented;

- 45    Figure 3 shows a detailed embodiment of a system in which a purchaser and a vendor complete a transaction;

Figures 4a and 4b show exemplary coins;

Figure 5 shows a system in which provenance data relating to a transaction is recorded;

Figures 6a and 6b show structures for the recording of provenance;

Figure 7 is a flowchart of a method of performing a transaction using the coins of Figure 4;

Figure 8 is a flowchart of a method of issuing and using the coins of Figure 4;

Figures 9a – 9d show types of transactions;

Figure 10 shows a method of recording data for sub-transactions;

5 Figure 11 is a flowchart of a method of issuing a coin;

Figure 12 is a flowchart of a method of recording data relating to a transaction;

Figure 13 shows method of changing the state of fungibility of the coins of Figure 4;

Figure 14 shows an exemplary detailed transaction using the coins of Figure 4;

Figures 15a – 15h show processes that form part of a transaction that using the coins of Figure 4; and

10 Figure 16 shows a method of determining a foreign exchange rate relating to the issue of the coins of Figure 4.

Figure 17 shows a coin being transferred between a plurality of states.

Figure 18 shows the storage of information where a coin is transferred between a plurality of states.

Figure 19 shows a method of accepting or rejecting a request for information.

15 Figure 20 shows a method of recording and sharing provenance information.

#### Detailed description

Referring to Figure 1, there is shown a system 1 in which two parties wish to make a transaction.

20 To enable the transaction to occur, a purchaser 2 and a vendor 4 are arranged to communicate, either directly or indirectly. The purchaser 2 is able to transfer an amount of a currency to the vendor 4 and in return the vendor 4 is able to transfer a good to, or performs a service for, the purchaser 2.

A third party 6, such as a notary or an investor 6 is able to oversee the transaction. The third party 6 is arranged to communicate with at least one of the companies in order to receive, and optionally verify, information relating to the transaction.

25 The system 1 also comprises a trust 8. The trust 8 is capable of issuing a digital currency, e.g. a cryptocurrency and/or a virtual currency, in the form of a coin to the purchaser 2. The purchaser 2 can then use this coin to complete the transaction. In order to enable the trust 8 to issue the coin to the purchaser 2, the trust 8 is arranged to communicate either directly or indirectly with the purchaser 2.

The trust 8 is also arranged, either directly or indirectly, to communicate with the vendor 4. After receiving the coin from the purchaser 2, the vendor 4 is able to exchange this coin for fiat currency at the trust 8.

30 The disclosure herein relates to a method and system for performing transactions. In particular, the disclosure relates to generating and using a coin that can be switched between a fungible and a non-fungible state. This switch may, for example, happen in dependence on activity relating to the coin, e.g. use of the coin in transactions.

35 The disclosure herein also relates to a method and system for providing a coin which stores provenance data relating to each transaction in which the coin is involved.

Referring to Figure 2, there is shown a computer device 1000 on which aspects of the methods and systems described herein are implemented.

40 The computer device 1000 comprises a processor 1002, a communication interface 1004, memory 1006, storage 1008, removable storage 1010 and a user interface 1012. These components are arranged to communicate via a bus 1014. The user interface 1012 comprises a display 1016 and an input/output device, such as a keyboard 1018 and a mouse 1020.

The processor 1002 executes instructions, for example instructions stored in the memory 1006, the storage 1008, and/or the removable storage 1010.

45 The communication interface 1004 facilitates communication between each of the purchaser 2, vendor 4, third party 6, and trust 8. The communication interface may for example comprise an Ethernet connection, an infrared connection, or a Bluetooth™ connection.

The memory 1006 stores information for use by the processor 1002. Typically, the memory comprises both read-only memory (ROM) and random-access memory (RAM).

The storage 1008 enables long term-storage of information; the storage 1008 typically comprises a hard disk device (HDD) and/or a solid-state drive (SSD).

- 5 The removable storage 1010 provides further storage for the computer device 1000. The removable storage may, for example, comprise an interface for a universal serial bus (USB) device. The removable storage 1010 may also comprise online storage, such as a cloud storage account.

Each of the purchaser 2, vendor 4, third party 6, and trust 8 use computer devices 1000 to implement aspects of the methods and systems as described herein. The computer devices 1000 used may be the same, but in most implementations the computer devices 1000 will differ from one another somewhat to suit the different specific purposes and functions of the purchaser 2, vendor 4, third party 6, and trust 8 respectively.

Typically, the third party 6 is interested in recording aspects of transactions. Therefore, the third party 6 may use a device with a large storage capacity, e.g. the storage 1008 is a storage device with large capacity. The computer devices 1000 on which the purchaser 2 and vendor 4 are implemented are typically personal devices, such as personal computers, laptop computers, and tablet computers.

A computer program product is provided that includes instructions for carrying out aspects of the method(s) described below. The computer program product is stored, at different stages, in any one of the memory 1006, the storage 1008, and the removable storage 1010. The storage of the computer program product is non-transitory, except when instructions included in the computer program product are being executed by the CPU 1002, in which case the instructions are sometimes stored temporarily in the CPU 1002 or memory 1006. It should also be noted that the removable storage 1008 is removable from the computer device 1000, such that the computer program product is held separately from the computer device 1000 from time to time. Different computer program products, or different aspects of a single overall computer program product, are present on the computer devices 1000 used by the purchaser 2, vendor 4, third party 6, and trust 8, as evident from the description below.

Different aspects of each party may be operated on a plurality of different computer devices 1000. Further, a plurality of computer devices 1000 may be utilised in the confirmation of a transaction and/or the storage of a transaction ledger. More generally, a combination of computer devices 1000 may be used to store relevant information and carry out aspects of the methods described herein, where these computer devices 1000 may each store copies of the same information, or may store differing information that can be combined.

In some embodiments, aspects of the methods described herein are implemented using blockchain technology and/or a distributed ledger, which are stored upon a plurality of computer devices. This distributed ledger may, for example, store information about the implemented digital currency, which may relate to previous transfers of digital currency and/or current owners of coins to which digital currency is assigned. The purchaser 2, vendor 4, third party 6, and trust 8 may use, at various times, different computer devices 1000 to carry out aspects of the methods, where different computer devices 1000 may have different permissions, so that only on certain systems, or with certain passwords, can a party access certain information and/or system capabilities.

Separate parties may have access to separate records: the distributed ledger is preferably accessible by every party (although this ledger may contain information that not every party can view). There may also be certain data that is held solely on the computer device 1000 of a subset of the parties.

Referring to Figure 3, there is shown a more detailed embodiment of the system 1 in which the purchaser 2 and the vendor 4 perform the transaction.

The purchaser 2 is arranged to communicate with the trust 8 via a purchaser bank 12. Typically, the purchaser bank 12 is a central bank, where the purchaser 2 communicates with this central bank either directly or indirectly, e.g. the purchaser 2 may communicate with the central bank via a private bank. The purchaser bank 12 controls the issuance of coins to the purchaser 2. Typically, the purchaser 2 requests the issuance of a coin by the purchaser bank 12 in return for an amount of a fiat currency or another digital currency – the purchaser bank 12 then requests the issuance of a coin from the trust 8.

In some embodiments, the trust 8 issues a number of coins at a first time and thereafter coins are tradeable between the companies, so that instead of requesting issuance from the trust 8, the purchaser

bank 12 is able to issue coins from a store of coins held by the purchaser bank 12. In these embodiments, the trust 8 may not be involved in the issuance of coins after the first issuance. Alternatively, the trust 8 may remain able to issue further coins even after the first issuance.

5 The vendor 4 is arranged to communicate with the purchaser 10 to receive a coin. The vendor 4 is also arranged to communicate with the trust 8 via a vendor bank 14 to exchange the received coin for an amount of fiat currency (this is hereafter referred to as the vendor 4 'redeeming' the coin). The vendor bank 14 is arranged to communicate with the trust 8 to transfer the redeemed coin to the trust 8.

10 The third party 6 typically comprises a number of constituent nodes, e.g. a lawyer 6-1, an accountant 6-2, and an investor 6-3. The nodes of the third party 6 are arranged to oversee transfers of the coin, e.g. between the purchaser bank 12 and the purchaser 2 or between the purchaser 2 and the vendor 4.

15 Typically, each constituent node of the third party 6 is only able to view information relating to certain aspects of a transfer. For example, only the accountant 6-2 and the investor 6-3 might be able to view information relating to an amount of fiat currency transferred by the purchaser 2 to the purchaser bank 12 and the lawyer might only be able to view the terms of a contract agreed by the purchaser 2 and the vendor 4 that relates to the transaction.

While this exemplary transaction has been described in terms of the purchaser 2 transferring the coin to the vendor 4, it will be appreciated that the coin can more generally be transferred between any two parties.

20 Each party to the transaction is arranged to record and/or approve aspects of the transaction, such as a transaction amount. This typically involves receiving information via the communication interface 1004 of the computer device 1000 used by each party.

25 The information is typically stored in the form of a distributed ledger held by one or more of the parties. Each party may be restricted to viewing only relevant parts of the ledger. Typically, the ledger relates to a number of (possibly unrelated) transactions that occur between numerous parties. Each party is only able to view detailed information about transactions in which that party was involved.

In some embodiments, the information is instead stored in the form of a centralized ledger, which is held by a subset of the parties involved. A combination of centralized and distributed ledgers may also be used, where centralized ledgers may be used to store potentially sensitive information.

30 The system 1 is typically a permissioned system, where only authorised parties are allowed to participate in the system 1 and in any transaction. By limiting possible transactions to parties in the system 1, only trusted parties are able to hold and/or use the digital currency. In some embodiments, non-permissioned parties are entirely blocked from holding the digital currency. In some embodiments, transfer of the digital currency to a non-permissioned party results in an alteration of the state of fungibility of the unit of digital currency that has been transferred (so that the digital currency cannot easily be redeemed).

35 Referring to Figure 4, there is shown an embodiment of a coin 400 that can be used as part of a transaction. The digital currency is typically issued in the form of coins, where each coin relates to an amount of the digital currency.

The coin 400 is assigned fields that define aspects of its operation, such as:

- 40 • Owner 402: the owner is the party that holds the coin 400 and that is able to transfer/redeem the coin (e.g. the purchaser 2 or the vendor 4). The owner of the coin is updated following each transaction.
- Value 404: the worth of the coin 400, this is typically a value in terms of the digital currency that underpins the coin, e.g. the value 404 may be 2 'exampleCoin'.
- 45 • Provenance data field 406: the coin 400 includes information relating to the provenance of the coin 400; 'provenance' refers to contextual data and is explained further with reference to Figures 5 and 6. The provenance data field 406 typically includes information relating to historic transactions and the (past and present) owners of the coin 400.
- Conditions 408: the coin 400 typically specifies conditions for its use, such as a purpose for which it can be used. The conditions 408 may be populated using clauses from a smart contract that is agreed upon at the time of initialisation of the coin 400.
- 50 • Fungibility data 410: Information relating to the fungibility of the coin is stored in the fungibility data 410; the fungibility is described in more detail below.

- Identifier 412: The coin comprises an identifier 412, such as a serial number. The identifier provides a serialized digital currency.

#### Fungibility

5 The coin 400 is arranged to be transferable between parties, where the fungibility data 410 is useable to determine, at the time of the transference, whether the coin 400 is fungible.

A fungible commodity is a commodity where each unit of the commodity is interchangeable. For example, US dollars are a fungible commodity, since each unit (each dollar) has the same value. When a payment for \$10 is required, the exact note used is unimportant – each \$10 note is interchangeable. Similarly, a \$20 note is interchangeable with any two \$10 notes. Although interchangeable, fungible commodities are not necessarily uniform; each dollar note has a unique serial number, but the serial number does not change the value (or interchangeability) of the dollar note. Fungible commodities are readily used as currency due to this interchangeability – a vendor can readily accept a set price for a good (e.g. \$10) safe in the knowledge that any \$10 that is received has the same (known) value and can be used at other businesses.

15 In contrast, a non-fungible commodity is a commodity where the units of the commodity are not interchangeable. For example, works of art are typically non-fungible since each works of art is different. The value of two sculptures of similar design may depend on the sculptor or the ownership history and may also vary hugely depending on market conditions (e.g. recent sales of related sculptures). Non-fungibility limits a commodity's use as a currency due to the lack of interchangeability – the price of a good cannot be set readily in terms of sculptures, since each sculpture has a different worth. To use a non-fungible commodity as a payment means, there must be agreement from both parties on the value of the commodity – and this requires evaluation by each party.

20 The fungibility data 410 of the coin 400 enables modification of the fungibility of the coin 400. In particular, the coin 400 may be switched between a fungible state, a non-fungible state, and, in some embodiments, a partially-fungible state.

In the fungible state, the coin 400 is interchangeable with similar coins and can be freely traded. A fungible coin can be traded between parties, such as the purchaser 2, the vendor 4, and the third company 22, and can be redeemed for fiat currencies at a bank, e.g. at a market rate.

30 In the non-fungible state, the coin 400 is no longer interchangeable with other coins. The coin 400 may still have a worth (e.g. the value 404), but it is no longer freely tradeable. In the non-fungible state, the coin 400 can be identified as non-fungible by recipients, who may then refuse to accept the coin 400. For example, the banks are able to refuse non-fungible coins, so that in some circumstances non-fungible coins cannot be redeemed for a fiat currency. As a result, non-fungible coins may have a lower worth (in the eyes of the vendor 4) than fungible coins – and in some circumstances, non-fungible coins may be rejected by the banks and so have no monetary value. While non-fungibility may have an effect on the tradeable value and the perceived value of the coin 400, the coin 400 still holds some worth, since the fungibility data 410 may be altered to make the coin 400 fungible. Furthermore, while in the non-fungible state, certain parties may still be able to accept the coin 400 as payment.

40 In a partially-fungible state, the coin 400 is interchangeable to a degree with other coins. In some embodiments, this comprises partially-fungible coins only being interchangeable with similar partially-fungible coins. In practice, the fungibility data may contain an indication of a group, such as a group number, that denotes fungibility. Coins in 'Group A' are fully fungible, and may be freely traded for coins of any other group; coins in 'Group B' are partially fungible and are interchangeable with other 'Group B' coins or can be exchanged for 'Group A' coins with both parties consent; coins in 'Group C' are non-fungible and can only be traded with both parties consent. It will be appreciated that partially-fungible coins may be sorted into a variety of, possibly overlapping, groups that limits their tradability. In some embodiments, partially-fungible coins may be considered as fungible coins in some circumstances and non-fungible coins in some circumstances.

50 Groups in which partially-fungible coins are freely-exchangeable are typically determined based on links between parties. For example, coins that have been used for alcohol or gambling may be made partially-fungible; fungibility is only restored (and the coin 400 is only redeemable) once requisite 'sin taxes' have been paid. After the switch from fungible to partially-fungible has been made, the coins remain freely exchangeable with coins used for other alcohol/gambling transactions, but not with coins used for other

purposes. The partially-fungible coins remain as a valid and interchangeable currency within a market sector (the alcohol/gambling sector), but are not interchangeable with coins outside of this sector.

Coins that are non-fungible or are partially fungible may be referred to collectively as coins that are not-fungible.

5 Typically, there is a known exchange value for fungible coins, where fungible coins can be readily exchanged for fiat currencies. The exchange rate may depend, for example, on market rates (which might themselves depend on supply and demand). Non-fungible coins and partially-fungible coins cannot be readily exchanged for fiat currencies, but instead can only be exchanged with the consent of the receiving party.

10 In some embodiments, parties are able to accept or reject not fungible coins, where if a not-fungible coin is accepted, payment equal to the value 604 of the coin 600 is required.

In some embodiments, the parties to a transaction are able to agree an altered rate of exchange for not-fungible coins, so that the receiving party may accept a not-fungible coin on the basis that they pay less than the value 604 of that coin.

15 The fungibility data 410 is described here as alterable, it may also be considered to be 'transitive'; that is, the fungibility data 410 is not immutably fixed and can transition between two or more states. This transition may be dependent on an elapsed time – where the coin 400 is switched to a non-fungible state if not redeemed within a specified time period, so the coin 400 may also be considered 'transitive' in the sense that the state of the coin changes with time.

20 Examples of situations where a change in the fungibility of the coin 400 is useful include:

- Cases of corruption: a coin that has been obtained through corrupt means may be made non-fungible and non-redeemable.
- Cases of improper behaviour, such as tax evasion: a fine can be levied through a change in the fungibility of the coin 400 (that forces the evader to redeem the coin 400 at a central bank for a reduced rate).
- 25 - Use of spending limitations: a partially-fungible coin can be limited to use in certain situations, so that spending on alcohol or gambling can be prevented while allowing the coin 400 to be freely used for other goods.
- Limiting the flow of money: partially-fungible coins may be redeemable in only certain places or with certain parties; this can ensure that prevent the flow of capital out of a marketplace.

Where non-fungible and partially-fungible coins are described as being tradeable only with both parties consent, this relates to a further consent step beyond simply consenting to a transaction. Where the coin 400 is redeemed for a good, e.g. an amount of gold, a transaction value is typically agreed on (e.g. coins worth \$8 may be required). Where the coin 400 is in a fungible state, this transaction is straightforward, the coin 400 is transferred to the seller upon transfer of the gold. On the contrary, where the coin 400 is in a partially-fungible, or non-fungible, state, the seller is typically notified of the state and can choose to accept or reject the coin 400. The seller may, for example, be informed that the coin 400 is currently non-fungible and so may not be redeemable at the banks – and as a result the seller might refuse to accept the coin 400 as payment.

40 In some embodiments, the coin is linked to a smart contract via the conditions 408. The use of the coin 408 is limited to a set of purposes defined by the smart contract, where use of the coin 408 for other purposes is forbidden. Any transaction that relates to a forbidden purpose is blocked (e.g. the owner 402 of the coin 400 is prevented from being changed).

In some embodiments, the conditions 408 are linked to the fungibility data 410, whereby use of the coin 400 for a purpose not specified in, or not allowed by, the conditions 408 causes a change in the fungibility data 410 of the coin 400. As an example, the conditions 408 may specify that the coin cannot be traded to a European company; if the owner 402 nevertheless tries to make a transaction with the European company, the fungibility data 410 is altered to place the coin 400 in a non-fungible state. This alteration may occur before or after the transaction depending on, for example, the coin 400 or on a term of the conditions 408.

50 In some embodiments, the coin 400 is limited to being used during a certain time period or for a certain number of transactions. This may relate to the coin 400 being fungible only within a certain time period (e.g. two months from issue) or only being fungible outside of a certain time period (e.g. the coin 400 may

be non-fungible until two months after issue). Similarly, there may be a maximum number of transactions possible until the coin 400 switches from fungible to not-fungible, or a minimum number of transaction required before the coin 400 switches from not-fungible to fungible. The time period and/or the number of transactions may be defined by the conditions 408. These requirements are usable to prevent speculation and to ensure that the coin 400 is not spent unnecessarily/for undesired purposes.

In some embodiments, the fungibility data 410 is alterable by one or more parties in the system 1. For example, in some embodiments the purchaser bank 12 is able to modify the fungibility data 410 of any coin issued by that bank. Typically, this comprises the central bank of a country being able to alter the fungibility data 410 of coins that are issued (directly or indirectly) by that central bank – this allows the central bank to oversee transactions occurring in the country and take action if any illegality is detected.

In some embodiments, the trust 8 is able to alter the fungibility data 410 of all coins 400, where parties, such as the purchaser bank 12 are able to petition the trust 8 to make alterations to fungibility data 410. This ensures a single, centralised, authority for altering the fungibility data 410 of the coin 400.

In some embodiments, permissioned parties, which may be agents of the trust 8, are able to alter the fungibility data 410 of the coin 400, where there may be different agents overseeing different jurisdictions. The ability of the agents to alter fungibility data 410 may be limited by a feature of that agent, for example certain agents may be able to alter fungibility data 410 of coins 400 with a certain range of values, or that have been used in certain jurisdictions.

Typically, the fungibility data 410 is altered automatically, where algorithms are used to detect uses of the coin 400 that are prohibited by the conditions 408 and/or by a related smart contract. Preferably, the fungibility data 410 is altered in real-time or near real-time, where any updates to the provenance data field 406 trigger an automatic review of the fungibility data 410 by the algorithms, which might result in an alteration to the state of fungibility.

This automatic alteration may be used in combination with manual alteration, where the algorithms flag a concern and the trust 8 is able to thereafter review the provenance data field 406 and alter the state of fungibility of the coin 400.

The provenance data is continuously reviewed and is used to alter the fungibility data 410; therefore, the provenance data is used proactively and not reactively, e.g. the provenance data is not simply used as a historical record, but is considered continuously as the coin 400 is in use.

As well as preventing the use of the coin 400 for illegal or undesirable transactions, the alterability of the fungibility data 410 of the coin 400 is useable to limit speculation of the digital currency underpinning the coin 400 since a party holding the coin 400 purely for speculation might result in an alteration of the fungibility data 410.

#### Value

Typically, the coin 400 is divisible. The coin 400 may be split into a number of other coins each of which has a different value (with the values of each new coin summing to the value of the original coin). This enables the coin 400 to be partially spent. Where this occurs, each part of the coin 400 comprises a new coin; the new coins each inherit the provenance data field 406 and the conditions 408 of the original coin. Each new coin has a new value 404 and a new identifier 412, which may relate to the original identifier (e.g. where the original coin had the identifier 'abc123', new coins may have identifiers 'abc123a' and 'abc123b').

The coin 400 may also be combinable, that is the coin 400 may be combined with other coins to obtain a coin with a greater value 404. The combined coin typically inherits the provenance data 406 from each of the coins used in the combination. The conditions 408 of the combined coin are typically an amalgamation of the conditions 408 of each of the coins used, where certain conditions may be inherited.

The value 404 of the coin is typically a pointer to an underpinning digital currency, e.g. the value may point to two units of 'exampleCoin'. When the coin 400 is divided, each sub-coin may then point to a single one of these units of 'exampleCoin'.

In some embodiments, the value 404 of the coin 400 is a fixed denomination, for example the coin 400 may be worth one 'exampleCoin' and this value may be immutable. There may be a plurality of coins where a subset of these coins have differing values, for example some coins may have a value of one

'exampleCoin' and some coins may have a value of two 'exampleCoin'. During a transaction, a plurality of coins can be used to achieve a transactional amount.

Along with the coins having a fixed worth, there may be a system of decimalisation, for example where the smallest value possible is 0.01 'exampleCoin' – this sets a minimum transactional value. Decimalisation to two decimal places in particular enables simple integration with existing systems, which often deal with such decimalisation (e.g. one cent is \$0.01 and one pence is £0.01).

As opposed to a divisible coin, having denominations of coins ensures there is a fixed number of extant coins that can be used. This prevents undesirable proliferation of coins, which may necessitate large amounts of storage space or lead to less useful provenance information being gathered (since the gathered provenance information will be split across numerous coins). Furthermore, the use of fixed denominations and minimum values precludes corruption by a party that is splitting off coins with small values thinking small values will not be noticed.

In order to enable transactions of small values, a third party such as the trust 8 may be able to transfer coins (e.g. to provide two coins with a value of one 'exampleCoin' in exchange for a single coin with a value of two 'exampleCoin'). Provision of denominations is at the volition of the trust 8; by controlling the denominations present in any given system, the trust 8 is able to control the type of transactions that are possible (e.g. to prevent transactions beneath certain amounts).

Where a divisible and/or combinable coin 400 is provided, there may be a lower and/or upper limit to the value 404 of the coin 400. Furthermore, there may be a limit to the ways in which the coin 400 can be divided. In this way, a digital currency with denominations and/or decimalisation may be provided. As an example, coins may be limited to having certain values 404, such as one, five, ten, and fifty 'exampleCoin'. Where a coin 400 with the value 404 fifty is used in a transaction for five 'exampleCoin', the coin 400 may be split into four coins with a value of ten 'exampleCoin' and two coins with a value of five 'exampleCoin'. This system of divisible decimalised denominations enables a flexible coin while maintaining a certain rigidity that precludes corruption and precludes coins from being divided *ad infinitum*.

In some embodiments, the digital currency is pegged to another commodity or currency so that the value 404 of the coin 400 can be expressed in terms of another currency, e.g. the value 404 may be \$2 or 2 BTC. In some embodiments, the coin may initially be pegged to another currency before being allowed to float. For example, at the time of issue of the coin 400, one 'exampleCoin' may be pegged as being worth \$1, the value of 'exampleCoin' may thereafter be allowed to float.

The coin 400 can be used as a store of value, a medium of exchange, and a unit of account in a transaction, thereby it possess the key attributes of a currency and can be considered as a currency. The coin 400 further possesses provenance data field 406 and fungibility data 410, which respectively enable the coin 400 to convey information about its use and enable the use of the coin to be controlled.

Coins according to the embodiment described in 4a contain conditions 408 that limit the range of uses of the coin. As a result, these coins might not be considered (by all parties) to be completely fungible, since the conditions of use for coins might differ. In some embodiments, the conditions 408 may (partially) reset on each transaction, so that historic conditions agreed to by the purchaser 2 do not affect future transactions by the vendor 4.

Furthermore, the provenance data field 406 for each coin will be different, which could also result in the coin being seen as non-fungible. The value 404 of the coin 400 is not typically dependent on the provenance data field 406 so that coins 400 with different provenance data fields 406 may still be considered fungible, since the values of the coins 400 are comparable – e.g. two coins which each have a value of one 'exampleCoin' can each be used to purchase a good for one 'exampleCoin' even where they have different provenance data fields 406.

Typically, all of the information relating to the coin 400 is stored on the coin 400, for example the coin 400 contains the value 404, the provenance data field 406, and the conditions 408. In some embodiments, the coin is able to be transferred offline, where the transaction does not require reference to a ledger. Instead, the owner field 402 of the coin 400 is altered as part of a transaction. The coin 400 may then be stored on a flash drive and a transaction may simply involve the flash drive changing hands and each party signing a digital agreement to transfer ownership. This enables use of the coin in areas without a network connection. When a network connection next becomes available, the fungibility data 410 of the coin may be remotely altered (e.g. in case the coin 400 was stolen).

Typically, coins 400 are issued (or 'initialised' or 'minted') upon agreement of a smart contract. For example, a smart contract may be agreed between the purchaser 2 and the vendor 4 or between the purchaser 2 and the purchaser bank 12.

5 The smart contract is used to populate the conditions 408 and thereby to limit the uses of the coin 400. This ensures that the coin 400 is useable only for agreed upon purposes.

The terms of the smart contract may be stored in the conditions 408 or the smart contract may be linked to the coin 400 via the identifier 412.

10 The identifier 412 is useable to distinguish coins from each other. The identifier 412 is different for each coin 400, and so each coin 400 is distinct. While distinct, when in a fungible state each coin 400 is interchangeable, that is while the identifiers may be different the value of each coin does not depend on the identifier 412, but instead only on the value field 404 of the coin. Two coins with different identifiers 412, but with the same value 404 are interchangeable.

Referring to Figure 4b, there is shown a second embodiment of the coin 400.

15 In this embodiment, the coin 400 comprises only the owner 402, the value 404, the provenance data field 406, the fungibility data 410, and the identifier 412.

By providing the coin without the conditions 408, the perceived fungibility of the coin does not depend on the conditions 408.

20 With the token of Figure 4b, changes to the fungibility depend not on the conditions 408 of the coin, but instead on outside actions/influences. For example, a transaction might specify adherence to the terms of a certain smart contract, where this smart contract is reviewed at the time of the transaction.

In some embodiments, the provenance data field 406 relates to the owner 402, where there is provenance data stored relating to each party in the system 1. The fungibility of the coin 400 then depends on the actions of the owner 402 of the coin, where a change in the owner 402 of the coin results in an appropriate updating of the provenance data field 406.

25 Typically, the fungibility data 410 is alterable by a third party, a bank, and/or the trust 8. Where there is a suspicion of corruption, this third party is able to examine the provenance data field 406 and determine whether the fungibility data 410 of the coin 400 should be altered. Each fungible coin is then wholly fungible from the perspective of any purchaser 2 and/or vendor 4, since any changes to the fungibility data 410 are made not based on conditions 408 of the coin, but by an outside party – there is no perceived risk of receiving a coin that is then (seemingly unjustly) made non-fungible.

30 In some embodiments, a third party is able to alter the owner 402 of coins 400, preferably the third party 6 is only able to alter the owner 402 of not-fungible coins. In practice, coins 400 that have been used for illicit purposes may have the owner 402 altered to be the purchaser 2. Therefore, coins 400 that have been transferred from the purchaser 2 to the vendor 4 as part of a project and have thereafter been misused can be returned to the purchaser 2.

35 More generally, the owner field 402 and/or any other field of the coin 400 may be alterable in dependence on the provenance data field 406.

40 In some embodiments, coins 400 that are in a non-fungible state at the time of completion of the transaction are automatically redeemed and an appropriate amount of fiat currency is returned to the purchaser 2 and/or a third party (such as the investor 6-3) instead of the holder of the coin 400.

#### Provenance information

Referring to Figure 5, for each interaction (e.g. transaction) that takes place within the system 1, provenance information is recorded in the blockchain (e.g. in the provenance data field 406 of the coin 400).

45 Provenance information relates to the chronology of the ownership, custody and location of the coin; specifically, provenance information provides contextual and circumstantial evidence for the original production or discovery of an entity, and the subsequent sequence of its formal ownership, custody and location. Typically, the provenance data field 406 contains information relating to any changes in the owner 402 and the fungibility data 410 of the coin as well as interpretive information that contextualises these changes.

50

By analysing the provenance data field 406, it is possible to identify the entities involved in a series of transactions, changes in ownership of the coin, and the context of the transactions.

Typically, for each transaction that uses the coin 400, the provenance data field 406 records:

- 5 - One or more transaction agents 52; this typically includes the purchaser 2, the vendor 4, and (if there is a third party) the third party 6. Each party to any transaction is thereby recorded.
- One or more transacted entities 54; this relates to the object of a transaction. Typically, this is a good and/or service that the purchaser 2 is selling to the vendor 4.
- 10 - One or more exploration activities 56. For any transaction, there is recorded contextual ('exploration') data. This relates to the context and the performance of the transaction. As an example, exploratory data may comprise an opinion of the vendor 4 that is recorded by the purchaser 2 (e.g. the vendor might seem untrustworthy).

Contextual data typically comprises both descriptive and interpretive data.

Descriptive data is objective data relating to a transaction; typically, descriptive data is automatically recorded at the time a transaction takes place. This includes when a contract is agreed, e.g. "Example Corporation agrees to build a bridge for £300", and when a contract is completed. Descriptive data parameters are objective facts and cannot be altered once they have been recorded. The blockchain therefore typically contains an immutable ledger of descriptive data – while the data cannot be altered, the parties able to view the data may change over time.

Interpretive data is subjective data relating to a transaction; this data typically requires contribution from a party. Interpretive data may comprise a subjective assessment of a feature of the transaction. Interpretive data may be automatically determined, for example by inferring an assessment based on assessments of prior transactions. In some embodiments, the determination of interpretive data comprises using a machine learning algorithm.

Since interpretive data involves a degree of subjectivity, the interpretation can change over time. For example, if "Example Company" is insinuated in a corruption scandal, previous transactions might come under scrutiny and previous events might be interpreted differently. Therefore, the interpretive data is typically alterable after the transaction has taken place. Any alteration is recorded, optionally along with a reason for the alteration.

Typically, the party that adds interpretive data to the ledger is recorded, so that the interpretive data is legitimised by being connected to a trusted party. In some embodiments, it is possible to add interpretive data anonymously, or partly anonymously; for example, only certain parties may be able to add interpretive data to the ledger and it may be possible for any of those parties to record anonymously interpretive data. This enables whistleblowing, where potential problems with a transaction can be flagged up without the whistleblower fearing reprisals.

The combination of descriptive and interpretive data enables any party to vet thoroughly potential partners. By considering prior transactions, the trustworthiness of any company can be assessed. Furthermore, the combination of descriptive and interpretive data allows past transactions to be thoroughly reviewed over time – and any identified impropriety may result in an alteration of the fungibility data 410.

The provenance data (both descriptive and interpretive) is further useable to obtain explicit confirmation from each party that the transaction has been authorised. This precludes any party to the transaction from later claiming they were unaware of the transaction.

Typically, some or all provenance data requires verification and/or validation, e.g. by the third party 6, before being added to the coin 400 and/or ledger. This enables parties viewing the provenance data field 406 of the coin 400 to be confident that the provenance information is correct. Whether provenance data requires verification/validation may depend on the type of information, e.g. whether it is descriptive or interpretive.

Exemplary provenance parameters that may be recorded include:

#### Descriptive parameters

- 50 - 'Who': who are the parties to the transaction? This parameter can, for example, relate to named companies (e.g. Seller: "Example Company"; Buyer "Acme Corporation") or pseudonyms (e.g. Seller: "Company A", Buyer "Company B"). In some embodiments, the 'who' parameter relates to pseudonyms, where only trusted parties are informed of the real company behind each pseudonym.

Further, any party may only be aware of a subset of the pseudonymous companies. As an example, an investor of Acme Corporation may be informed that "Example Company" has made a transaction to "Company B".

- 5 - 'Where': where was the transaction performed? This parameter can, for example, relate to a geographic location (e.g. this parameter can include GPS co-ordinates); an event (e.g. "at the annual shareholder meeting"); or a medium (e.g. on the internet).
- 'When': when was the transaction performed? Typically, this parameter includes a date and/or time. The parameter might also include a related event (e.g. "at the annual shareholder meeting").
- 10 - 'What': what is the object of the transaction? This parameter relates to the goods or services that are the subject of the transaction. This parameter can include an indication of any currency transferred and any good/service transferred. For example, 'what' may record "£300 is to be transferred in return for service X".
- 'How': how is the transaction performed? This parameter typically includes an indication of the method of currency transfer and/or transfer of goods. For example, 'how' may record "bank transfer".

#### 15 Interpretive parameters

- 'How': separately to the descriptive 'how' parameter, the interpretive 'how' parameter typically indicates the conditions that led to the transaction taking place. For example, 'how' may record that the CEOs of "Example Company" and "Acme Corporation" met at a conference in March, had a meeting in April, and closed a deal in May. By examining the interpretive 'how' parameter, a party is able to determine how a transaction came to take place. This is thus useable to determine whether a deal is wholly "above board", or whether there might have been some underhanded business practices taking place. As an example, "how" might indicate that "Example Company" and "Acme Corporation" had been on bad terms at the conference and yet following a one-on-one unrecorded meeting the CEOs had agreed a deal with favourable terms for one of the companies. This might suggest (when other factors are considered) that the meeting involved bribery.
- 20 - 'Why': similarly to 'how', why indicates the reasons behind the transaction taking place. This parameter may, for example, record that a politician had been campaigning for a bridge to be built for some time and had finally obtained enough support; hence, there is a transaction for a bridge to be built. 'Why' may also contain an assessment of the reasoning behind a feature of the transaction, for example 'why' might record that a key supporter had only agreed to back the bridge after receiving a number of gifts from the politician.

While the descriptive data and interpretive data recording have primarily been described in the context of a payment for a good, it will be appreciated that these data (and the system 1 in general) are more widely applicable for any recording (and assessment) of information. For example, the recorded data can be used to determine whether a suitable babysitter based on past babysitting or whether a car is performing adequately (e.g. by recording maintenance transactions).

In some embodiments, each party to the transaction is required to input or verify certain descriptive and/or interpretive information. This is useable to verify that each party has confirmed the details of the transaction and is also useable to record the reasons behind the transactions (by forcing the parties to agree on 'how' and/or 'why' the transaction occurred). Typically, at least a subset of the details must be confirmed by each party before a transaction using the coin 400 can occur.

Referring to Figure 6a, typically, the provenance data is recorded in the form of three layers:

- A 'representation layer' 62 stores text, images, audio-visual information that can be used to determine a feature of the information. Typically, the representation layer 62 is itself composed of four sub-layers (or 'levels'):
- 45     o An 'objective level' 62a contains evidence (e.g. descriptive information) relating to objective facts of a transaction (e.g. 'what', 'when', 'who'). This layer is immutably recorded upon verification of a transaction.
- 50     o A 'descriptive layer' 62b contains further descriptive information. Typically, this comprises information input by a party viewing information from the descriptive layer. For example, a party may view objective GPS information and input a descriptive location (e.g. "head office of Acme Corporation"). This layer is also immutably recorded.
- o An 'interpretive layer' 62c contains interpretive information (as described above). This layer may be altered after being recorded.

- 5                   ○ An 'exploratory layer' 62d contains further interpretive information about transactions/parties. The third party 6 is able to investigate the provenance information for historic information and can use this to evaluate transactions and/or parties to transactions. The exploratory layer 62d contains these evaluations; for example, an evaluation may comprise a flag warning that a party is implicated in a corruption scandal based on their participation in prior transactions.
- 10               - A 'synthetic layer' 64 contains higher-level information relating to the representation layer. The synthetic layer 64 contains information on anticipated transactions, a summary of provenance information (e.g. a summary on historic transactions for each party) and information on how transactions could be improved (e.g. where inefficiencies are identified from the exploratory layer 62d. The synthetic layer 64 addresses provenance exploration, anticipation and improvement.
- 15               - A 'social awareness layer' 66 contains social evaluations relating to the synthetic layer 64 and the representation layer 62. For example, the social awareness layer 66 enables building of consensus between numerous parties (e.g. to reach agreement on whether a party is corrupt); interactions/sentiments between parties, e.g. to indicate a level of trust or to give approval for a transaction; and visualisations relating to transactions (e.g. heat maps, maps of money flows, or project timelines). The social awareness layer 66 addresses sentiment, networked consensus-building and enactment.

Each of the layers 62, 64, and 66 is accessible only by trusted parties, where the trusted parties for each layer may differ. The representation layer 62 is typically accessible only to the parties to a transaction; the synthetic layer 64 and social awareness layer 66 may be accessible to anyone with an interest in any of the parties to a transaction. Where the purchaser 2 is proposing a deal to the vendor 4, the vendor 4 will want to vet the purchaser 2. The vendor 4 is typically not able to access the representation layer 62 of past transactions of the purchaser 2, but may be able to access the synthetic layer 64, which gives a high level overview of previous transactions involving the purchaser 2 (without disclosing confidential information that is stored in the representation layer 62. Similarly, the social awareness layer 66 allows the vendor 4 to assess the behaviour of the purchaser 2 via peer reviews and consensus; this enables conclusions to be drawn based on historic transactions without accessing details of those historic transactions.

The provenance data field 406 enables analysis of the history of coins and thereby enables, for example, the establishment of provenance chains and the mapping of flows of money and goods. This is useable to identify 'bad' agents, which are not adhering to laws or customs as well as determination of beneficial and detrimental policies (e.g. an update to regulations can be evaluated by identifying changes in behaviour as captured by provenance data). In some embodiments, there is computed a 'trust index' for agents, which may comprise information relating to past activity (using the coin or otherwise), information added by other users, and information scraped from private and/or public sources.

Figure 6b shows an exemplary implementation of the provenance data field 406.

The provenance data field 406 comprises:

- 40               - Descriptive data 610. The descriptive data 610 is recorded at the time of the transaction and is immutably stored in the provenance data field 406 and on the ledger. This data is typically determined automatically, but may be confirmed by any parties to the transaction. The descriptive data 610 comprises:

  - 45                   ○ An indication of the parties to the transaction 612; here the payment is made by Jack Smith to Corrupt Corp.;
  - An indication of what is being transferred 614; here 1 'exampleCoin' is being transferred;
  - Time data 616; here the transaction occurred on 1 Jan 2019 at 11:11:11; and
  - Location data 618; here the transaction took place in London at postcode SW1A 0AA.
- 50               - Interpretive data 620. The interpretive data 620 is recorded at the time of the transaction and contains comments on the transaction that are made by parties to the transaction. Typically, interpretive data 620 is a requirement of completing the transaction; this forces each party to the transaction to contribute to the transaction (and thereby confirm they are a consensual party to the transaction). The interpretive data 620 comprises:

  - An indication of how the transaction was completed 622; here the transaction was completed due to completion of the terms of a smart contract (resulting in a transfer of ownership of the coin 400); and

- An indication of why the transaction occurred; here the transaction was for completion of a project milestone.
- Exploratory data 630. The exploratory data 630 is recorded after the transaction has been completed by third parties. This data can be added over a period of time as information about the transaction comes to light. The exploratory data 630 comprises:
  - Information regarding the parties to the transaction 632; here this information indicates that the CEO of Corrupt Corp. has declared bankruptcy in the past;
  - Information regarding the reason for the transaction 634; here the transaction (which is known from the interpretive data 620 to be for completion of a milestone) is shown to be payment for completion of foundations; and
  - Miscellaneous information 636; here there is an indication that the project was completed three months late and was twenty percent over budget.
- The provenance data 606 may also comprise inherited information 636 from related transactions. Here it is recorded that Corrupt Corp. have bought cement from Collapse Corp. This inherited information is useable to infer information about a current transaction.

The provenance data field 406 is useable to determine information regarding a transaction and the parties to a transaction. In this instance, the exploratory data 630, which is recorded by third parties after the transaction has taken place, indicates that: the CEO of Corrupt Corp. has previously declared bankruptcy; that Corrupt Corp. have delivered late and over budget; and that Corrupt Corp. have purchased cement from a company called Collapse Corp. This provenance data field 406 is then useable to determine that Corrupt Corp. might be an untrustworthy or incompetent party and that their work should be reviewed.

This provenance data field 406 of the coin 400 can be combined with data recorded elsewhere on the ledger, for example this data can be combined with data relating to other transactions by Corrupt Corp. or Collapse Corp. The totality of data might indicate either that this is an isolated incident of poor work or it might show that this is part of a pattern of poor work; the provenance data for each of the relevant coins can be updated accordingly. Therefore, a user viewing the coin 400 is able to not only view information relating to this transaction, but also to contextualise this information by viewing information relating to related transactions. The entirety of the provenance data is useable to form a profile for Corrupt Corp., which can then be viewed by parties looking to engage Corrupt Corp. in a professional relationship.

The provenance information may comprise structured data (which comprises clearly defined data types), unstructured data, or a mixture of structured and unstructured data. The use of structured provenance information enables simple searching for certain types of information (e.g. location data may require a country, and it is simple to search for this country). The provision of unstructured information enables more obscure and/or specific information to be provided that cannot easily be entered in a structured format, for example, location data may also contain a picture and/or a description (e.g. "£the butcher shop on Example Street").

The provenance data may comprise a "why" section that explores the reasoning for a transaction. Unstructured information is of particular use here as a wide variety of reasons may exist for any transaction where these may be in differing formats. In some embodiments, each provenance information entry comprises at least one piece of structured information, where any unstructured information may be linked to structured information. For example, a "why" entry may require a selection from a closed list of options. Unstructured information can then be included in relation to the selection. This enables a user to easily search for an entry from the list to obtain a limited amount of information. This information can then be examined for unstructured provenance information.

#### Mining – proof-of-exploration

To record information about transactions and about provenance on the blockchain, a process referred to as 'mining' is used; mining comprises adding blocks of information to an existing chain of blocks (a 'blockchain') to obtain a ledger; the ledger obtained is immutable – that is, previously added blocks cannot be altered.

An exemplary method of mining involves numerous parties solving a computational problem to mine a block. Data relating to the existing blockchain is encrypted using an encoding variable and an irreversible cryptographic hash to obtain a target parameter; miners are provided with the target parameter, but not the encoding variable. The miners then perform the same encryption process using the blockchain data and the hash and a guess of the encoding variable and compare the obtained parameter to the target

parameter. The miner that first obtains the required parameter transmits their (correct) guess of the encoding variable to other miners along with a new block; other miners verify that the guessed encoding variable does indeed lead to the target parameter and also that the contents of the block are valid (e.g. the miner has not inserted a false transaction in the block). The new block is then added to the blockchain.

- 5 The process of finding the encoding variable requires considerable computing power (since it relies on a series of guesses), as a result, this method is termed 'proof-of-work'. As a reward for spending computing power on mining, the successful miner is typically rewarded monetarily.

The target parameter is obtained using data from the last block in the blockchain; this last block depends on the second to last block (and so on). Therefore, there is an unbroken chain of dependence is formed to the first block of the blockchain. As a result, past blocks cannot be altered by a rogue miner, since this would alter the obtained parameter and result in the miner not being able to obtain the correct encoding variable.

10 The disclosed coin may be implemented using a proof-of-work system (or another known system of mining); typically, instead of offering a direct monetary reward, miners are rewarded with access to provenance data.

15 In some embodiments, miners are incentivised to provide provenance data and/or to mine blocks by being rewarded with an amount of digital currency in return for mining a block.

In some embodiments, those seeking to access provenance data are required to contribute an amount of computing power to mining (this can occur as a background process in the processor 1002). In this way, proof-of-work processes can be used without a monetary reward – the reward is instead access to the provenance data.

20 Alternatively, blocks may be added to the blockchain by using a system of authorised miners. Instead of requiring an encoding parameter to be found, consensus between a set number of authorised miners is required for a block to be added to the blockchain, where each new block includes an indication of the miners that added the block. This method alleviates the need for miners to use large amounts of computing power as well as setting an immutable record that indicates which parties added the block.

The number of parties needed for consensus may depend on a feature of the transaction, for example the value 404 of the coin 400 being transferred, the provenance data field 406 of the coin 400 being transferred, or the parties to the transaction.

30 In some embodiments, mining blocks is based on the addition of provenance information to the coin 400 and/or the ledger. The addition of blocks to the blockchain is triggered by a party adding information so that the miner of a new block is the party recording information. Mining in this way might be required in order to participate in the system 1. This method 'proof-of-exploration' method encourages third parties to record interpretive data for past transactions; this leads to an increased amount of information being present on the ledger that encourages use of the system 1.

35 While mining has primarily been described in relation to a blockchain, more broadly, the methods described (e.g. consensus) are applicable to the addition of information to any ledger.

#### Currency in use

Referring to Figure 7, there is shown the performance of a transaction using the coin 400.

40 In a first step 102, terms of a transaction are agreed; as an example the purchaser 2 and the vendor 4 may agree to exchange \$14 for 1 gram of gold with the terms being recorded in the form of a smart contract.

In a second step 104, a coin for use in the transaction is selected. With the example of a gold transaction, the purchaser 2 selects a coin to transfer to the vendor 4 in exchange for the gold. The selected coin will have a value (in the digital currency) equivalent to \$14.

45 In a third step 106, the fungibility of the coin 400 is determined. Typically, this comprises an examination of the fungibility data 410 of the coin 400. The conditions 408 of the coin 400 may also be examined to ensure that the transaction is allowable under the terms of the conditions 408. An unallowable transaction may result in a change in the fungibility data 410 or may result in the transfer of the coin 400 being blocked. As an example, the transaction may be blocked if the recipient is not a permissioned member of the system 1.

50 In a fourth step 108, if the coin 400 is fungible, the coin 400 is transferred.

In an alternative fourth step 110, if the coin 400 is non-fungible or partially-fungible, the recipient of the coin 400 is informed.

In a fifth step 112, the recipient is given the choice to accept or reject the coin 400.

5 If the recipient accepts the coin 400 despite the coin 400 being non-fungible or partially-fungible, the coin 400 is transferred.

An example of a transaction where fungibility is of relevance is redemption of the coin 400, e.g. where the coin 400 is exchanged for a fiat currency. Redemption typically takes place either directly or indirectly with a central bank. When the coin 400 is redeemed, the central bank evaluates the fungibility of the coin 400. The coin being in a non-fungible or partially-fungible state indicates a breach of the conditions 408 of the coin 400 or a potential problem with the provenance data field 406 of the coin 400. The coin being non-fungible 400 therefore indicates the central bank should carry out verification checks to ensure that the coin 400 has not been used improperly, e.g. for corruption. If an improper use is detected, the central bank can reject the coin 400 (e.g. refuse to exchange the coin for fiat currency).

Referring to Figure 8, there is shown a flowchart for a method of issuing and using the coin 400.

15 In a first step 120, a smart contract is agreed; this smart contract relates to a transaction between the purchaser 2 and the vendor 4.

In a second step 122, a coin is issued according to the smart contract. Issuance of the coin 400 typically involves the purchaser 2 transferring a certain amount of currency to the purchaser bank 12; in response the purchaser bank 12 issues the coin 400 with the value 404 field set appropriately. The value of the currency to be transferred, and the value 604 of the coin 400 to be issued, is typically defined by the smart contract.

20 The terms of the smart contract are recorded in the conditions 408. The conditions 408 may also comprise terms set by the issuing bank 12. Typically, these terms will relate to appropriate uses of the coin 408; for example, illegal activities are typically not allowed. The terms may also restrict the coin 400 to being used for purposes relevant to the smart contract. In an example, the smart contract defines a payment in return for the construction of a bridge. The conditions 408 of the coin 400 then specify that the coin 400 is useable only for related purposes. Therefore, the coin 400 can be freely used to purchase building materials, but cannot be used (without consequence) to purchase alcohol. The smart contract could also define specific allowable suppliers of building materials, or even define an exact supplier that must be used.

30 In a third step 124, the coin 400 is transferred from the purchaser 2 to another party, such as the vendor 4.

In a fourth step 126, the conditions 408 of the coin 400 are examined to determine whether the terms of the agreed-upon smart contract have been breached.

35 In a fourth step 126, if the terms of the smart contract have not been breached, the coin 400 is transferred to the vendor 4.

In an optional fifth step 128, the coin 400 is redeemed and a fiat currency is transferred to the user. This step may be initiated by the vendor 4 or may occur automatically on completion of the smart contract. In some embodiments, once the terms of the smart contract have been fully met, automatic redemption of the coin 400 occurs to prevent further transfers. This ensures that the provenance data field 406 of the coin 400 contains detail relating to completion of a specific smart contract without also containing details of unrelated deals (e.g. those performed following completion of the smart contract).

40 The meeting of the terms of the smart contract can be determined either by a manual input or by an automatic determination, for example completion of a building contract may be determined by identifying approval from a government inspection agency. The use of a smart contract enables automatic transfer and precludes the purchaser 2 from refusing to pay even after the vendor 4 has met its obligations.

45 Completion of the smart contract may require consensus from a number of validating parties; these parties may, for example be: the parties to the contract; delivery companies; regulators; and/or trusted notaries.

50 Redemption of the coin 400 typically involves interaction with a bank, such as the purchaser bank 12 or the vendor bank 14. This interaction allows the bank to review the provenance data field 406 of the coin 400 and thereby to ensure that there has been adherence to any necessary regulations throughout the lifetime of the coin 400. The use of the coin 400 therefore enables a simple and effective way of central banks regulating the behaviour of companies operating in the jurisdiction of that central bank.

In an alternative fourth step 130, if the terms of the smart contract have been breached, the fungibility data 410 of the coin 400 is updated. Typically, this comprises switching the coin 400 to a non-fungible or partially-fungible state.

- 5 Any relevant party may be informed when the fungibility data 410 is updated. This can indicate to the purchaser 2, the vendor 4, or any of the banks or third parties, that a breach of the conditions 408 may have occurred. Further, a party may be informed before the fungibility data 410 is updated if an action might cause a breach of the conditions 408. As an example, if a transaction between the purchaser 2 and a sub-contractor would result in a breach of conditions 408 being detected, the purchaser 2 is informed. If this is unintentional (e.g. if the purchaser 2 was not aware that the sub-contractor is corrupt), the transaction can be cancelled. If the detection of the breach of conditions 408 is erroneous (e.g. if the purchaser 2 is confident the sub-contractor has been wrongly identified as corrupt), the transaction can be performed.

- 10 By updating the fungibility of the coin 400 in this way, suspicious transactions can be identified without being completely blocked. Where a review of the provenance data 406 of the coin identifies a sub-contractor as a corrupt company, this might be a case of corruption, or it might simply be that the sub-contractor is new, small, or has been falsely accused of corruption. Completely blocking a transaction would potentially stop work being carried out and thus cause a delay to a project; by instead limiting the fungibility, transfers of value are still allowed between consenting parties and work can continue. The sub-contractor (and other parties) may accept a non-fungible coin if they are confident they can demonstrate their legitimacy. Such a demonstration of legitimacy might result in the coin 400 being returned to a fungible state, where it can be redeemed for a fiat currency. If on the other hand the sub-contractor is not able to prove their legitimacy, a central bank may refuse to exchange the coin 400 for a fiat currency.

- 15 Determining the legitimacy of companies and transactions typically comprises an examination of provenance data field 406. As has been explained with reference to Figures 5 and 6, the provenance data field 406 contains both descriptive data and interpretive data. The descriptive data is recorded at the time of making a transaction and is examined at that point to determine whether the conditions 408 have been breached. The interpretive data can be continually updated, so that a breach of the conditions 408, e.g. an incident of corruption, can be identified after a transaction has occurred. The fungibility data 410 can therefore usefully be updated after a breach has already occurred; this avoids the need to vet fully each transaction before it occurs and enables use of an easily transferable coin that is still secure and trustworthy.

- 20 In some embodiments, each and every transaction requires the approval of all parties to the transaction; this prevents the coin being used for unsolicited gifts by ensuring that the recipient has consented to the transfer. This maintains a documented and indisputable chain of ownership. Exemplary transactions are shown in Figure 9; each transaction contains a two-way exchange, which comprises an acknowledgement and indicates that each party has consented to the transaction.

Referring to Figure 10, there is shown a method of performing sub-transactions with the coin 400.

- 25 The coin 400 is typically initialised based on a smart contract between the purchaser 2 and the vendor 4. To fulfil the conditions of the smart contract, the vendor 4 may wish to sub-contract work and therefore the vendor 4 needs to be able to pay sub-contractors.

To ensure that the sub-contracted work is seen as legitimate – e.g. not a front for inefficiency or corruption – each sub-transaction is recorded in the provenance data field 406 of the coin 400 used for that sub-transaction.

- 30 Specifically, the provenance of each sub-transaction is evaluated before and after the sub-transaction is complete. Any concerns are identified at this point, or if no concerns are identified, the sub-transaction is labelled as having 'good' provenance. If each sub-transaction has good provenance, this is inherited by the main transaction on completion of each sub-transaction. Therefore, the main transaction contains an indication of whether each sub-transaction has good provenance, or whether there are concerns about any sub-transactions.

- 35 In some circumstances, the sub-contractor may themselves sub-contract work (leading to sub-sub-transactions). In these circumstances, an object, such as provenance information, is inherited by each transaction in higher level (so that a corrupt sub-sub-transaction will taint both the parent sub-transaction

and the main transaction). This inheritance simplifies the evaluation of the coin 400. Any provenance concerns can be easily traced through the provenance data by following the chain of inheritance.

Referring to Figure 11, there is shown an exemplary method of agreeing on a smart contract and initialising a coin. It will be appreciated that any of the steps of the exemplary method may be omitted in any given implementation.

In a first step 142, the parties to a transaction agree to the terms of that transaction, for example the purchaser 2 may agree to pay the vendor 4 a certain amount in return for a good. The terms may also specify certain subcontractors that the vendor 4 can use, or may specify that the coin can only be used for certain purposes necessary for the delivery of the good.

In a second step 144, the terms are reviewed by the third party 6 and the approval of the third party 6 is recorded. This step ensures that a third party, such as the lawyer 6-3, has reviewed the transaction. The recorded approval can be used later by a regulatory body to indicate that the transaction is legal. If the regulatory body later finds that the transaction was not legitimate, it will be able to identify that the lawyer 6-2 might be corrupt or incompetent.

In a third step 146, the terms of the transaction are recorded in a smart contract.

In a fourth step 148, each party to the transaction is required to confirm that they will adhere to the terms of the smart contract.

In a fifth step 150, approval is received from the jurisdiction in which the transaction is taking place. This typically involves a government regulator reviewing the smart contract to ensure that all regulatory requirements are met. This step also enables the government body to identify any taxes that will need to be paid so that receipt of these taxes can be confirmed in due course.

In a sixth step 152, the trust 8 and/or the purchaser bank 12 issues the coin 400 to the purchaser 2 for use in the transaction.

The conditions field 408 of the coin 400 is populated with information relating to the agreed-upon smart contract. The provenance data field 406 of the coin 400 is populated with information about each party to the transaction. Relevant information may be recorded during any of the steps of the method, where any one of the parties may be required to divulge information in order for the coin 400 to issue. For example, information about historic transactions, or about potential conflicts of interest may be required in order to populate the provenance data field 406. The recording of this information prevents parties to the transaction from later denying knowledge of relevant information.

The coin 400 comprises an identifier 412 that is useable to link the coin 400 to the transaction and the agreed-upon smart contract. The identifier 412 may be used instead of the conditions 406 to link the coin 400 to the smart contract – this is useable to reduce the file size of the coin 400 and can be beneficial for complex or lengthy smart contracts. The identifier 412 and/or the conditions 408 may also be used to link the coin 400 to a plurality of smart contracts.

In some embodiments, the coin 400 is assigned to a range of purposes as defined by the smart contract. For example, the coin 400 may be useable for a number of potential transactions between two parties where only the final recipient and total amount 410.

Typically, a breach of the conditions 406 of the coin 400 results in a change in the state of fungibility of the coin 400. The conditions 406 may also specify that the coin is only useable for certain transactions or in certain situations, where the coin cannot be transferred outside of these transactions/situations. As an example, it may be impossible to change the owner 402 of the coin 400 unless a transaction is allowed by the conditions 406. In this way, certain transactions can be entirely prohibited (e.g. spending on goods that are illegal) and certain transactions can instead result in a change in the fungibility data 410 of the coin (e.g. spending on goods that might be illegal). In either event, the fungibility data 410 of the coin can be altered after the transaction, so that a transaction that should have been prohibited, but was not identified as unauthorized, can still be penalised.

Referring to Figure 12, there is shown a flowchart of a method of recording data relating to a transaction, such as the data of Figure 6b.

In a first step 162, descriptive data relating to a transaction is identified. For example, a time, the parties involved in the transaction, the value of the transaction, and the location of the transaction are determined.

This descriptive data is typically obtained automatically, e.g. the time is recorded using the processor of the computer device 1000 used to perform the transaction.

In a second step 164, confirmation of the descriptive data is received from the purchaser 2 and vendor 4. This confirmation both verifies that the descriptive data is correct and ensures that there is an immutable record that indicates both parties agreed to, and were aware of, the transaction. Further, in the second step 164, the purchaser 2 and the vendor 4 input interpretive data relating to the reasons for the transaction and how the transaction came to take place.

In a third step 166, confirmation of the descriptive data and interpretive data is received from the third party 6. This acts as a further check from a potentially independent source that the descriptive data is correct and that the interpretive data from the purchaser 2 and the vendor 4 is correct. The conditions 408 of the coin 400 may specify that confirmation from a specific third party is needed – for example certain transactions may require oversight from a government regulatory body.

The completion of the transaction is dependent on the descriptive data and the interpretive data input by the purchaser 2, the vendor 4, and the third party 6. Certain types of data, as specified by the conditions 608, may be needed – and approval from certain third parties, or a certain number of third parties, may be needed to complete the transaction.

Following the input of the required data from each party, in a fourth step 168, the information is used to determine and/or infer features of the transaction. The determination/inference typically relates to determination of the purpose of the transaction, the goods/services being supplied as a result of the transaction, and any regulations that must be reviewed as a result of the transaction occurring. Typically, descriptive data is used to determine features, while interpretive data is used to infer features.

With reference to Figure 6b, the descriptive 'who' data 612 for this transaction shows that a payment was made to Corrupt Corp. This can be directly used to determine that there is a risk of corruption. The miscellaneous interpretive data 636 shows that the project was over budget; while this does not directly indicate that there is corruption involved, in combination with other data (e.g. knowledge of the company involved) it can be used to infer corruption.

Determination/inference may occur automatically, e.g. using artificial intelligence and/or machine learning, or may occur manually, where an observer flags up concerning pieces of information.

In a sixth step 170, it is determined whether the transaction breaches the conditions 608 of the coin 400. This determination is based on one or more determined/inferred features.

In a seventh step 172, if a breach of the conditions 408 is identified, the fungibility data 410 of the coin 400 is updated. Typically, this involves the coin 400 being switched to a non-fungible or partially-fungible state if the conditions 408 of the coin 400 have been breached.

In an eighth step 174, relevant parties are informed of the change in the fungibility data 410.

Following the transaction, in a ninth step 176, further interpretive data is received from the third party 6.

In a tenth step 178, further data (descriptive and/or interpretive) is received from subsequent transactions.

Data received subsequent to a transaction is useable to put that transaction in context. With the example of Figure 6b, knowing that Corrupt Corp. has sourced cement from Collapse Corp. allows it to be inferred that the foundations of the bridge could be faulty.

After the ninth step 176 and the tenth step 178, the fifth to seventh steps are repeated and the fungibility data 410 of the coin 400 is updated appropriately. There might be a time-limit associated with the alterability of the fungibility data 410. Where the coin 400 has been used for multiple transactions, the fungibility data 410 is typically altered only if the current owner 402 is determined to have breached the smart contract. Where a past owner of the coin 400 is identified as problematic, but the past user has already passed on the coin 400, this identification does not result in an alteration in the fungibility data 410 of the coin 400. This identification may still result in an alteration in the fungibility data 410 of other coins 400 held by the problematic owner.

Typically, the system 1 enforces the use of the coin 400 for all transactions that occur between parties in the system 1. Specifically, Corrupt Corp. are paid using the coin 400 and must show how this coin 400 is used (since all use is recorded in the provenance data field 606). Therefore, after Corrupt Corp. are instructed to build the foundations of the bridge, Corrupt Corp. must use the coin 400 to purchase cement

for building the foundations. The use of the coin 400 thus ensures that the entire chain of subcontracting is recorded.

5 The level of subcontracting for which the coin 400 must be used may be set by the conditions 408; for example, the conditions 408 may specify that the coin 400 can be redeemed by a building site supervisor (who can then pay each individual builder in a fiat currency), or the conditions 408 may specify that each builder must be paid using the coin 400. The party attempting to redeem the coin 400 can be determined by evaluating the provenance data 406 of the coin 400.

10 The enforced use of the coin 400 by Corrupt Corp. to pay subcontractors enables evaluation of Corrupt Corp.'s activities even after they have received the coin 400. Furthermore, this use of the coin 400 enables continuous evaluation of the initial transaction. The payment to Collapse Corp. might be used to indicate that Corrupt Corp. are either incompetent or corrupt and this indication can be used to interpret other transactions where Corrupt Corp. was involved.

15 The provenance information from any transaction can be used to evaluate related transactions and to update the fungibility data 410 of all coins. The corruption of a single subcontractor calls into question the legitimacy of all other subcontractors hired by Corrupt Corp. The provenance data field 406 for any other coins handled by Corrupt Corp is updated in dependence on the transaction to Collapse Corp. and may result in a change in the fungibility data 410 of those other coins.

20 As described with reference to Figure 10, provenance data is inherited by 'parent' transactions. Therefore, if a subtransaction breaches the conditions 408 of the coin 400 this suggests the parent transactions should be reviewed. Typically, a 'parent' coin is divided in order to pay for subtransactions, where a part of the coin 400 is used to pay for the subtransaction and the remainder of the coin 400 is available for use in other subtransactions. In some embodiments, a change in the fungibility data 410 of the coin 400 for a subtransaction causes a change in the fungibility data 410 of all coins split from the same parent coin. In some embodiments, there is no automatic change in related coins, but instead a review is triggered, where  
25 the third party 6 is notified that related transactions should be examined for a possible breach.

The same coin 400, or parts of the coin 400, may be used for a number of transactions. Provenance data is recorded for each transaction so that there is a chain of provenance that can be used to trace the coin 400 through the lifetime of a project.

30 Where coins of fixed denominations are used, coins may be linked by a shared owner. Therefore, coins that were not transferred to Collapse Corp. can be linked to the coins that were transferred by dint of being held by Corrupt Corp. at the time of the transfer.

35 In some embodiments, the seventh step 172 of the method of Figure 12 (the update in fungibility) occurs automatically according to terms set out in the conditions 408 of the contract 400. In some embodiments, the update in fungibility is dependent on the actions of one or more parties, typically the third party 6. As an example, government bodies may be able to update the fungibility data 410 of the coin 400.

40 In some embodiments, the third party 6 is able to update the fungibility data 410 of the coin at any time. In some embodiments, the third party 6 is only able to update the fungibility data 410 of the coin 400 if a breach of the conditions 408 is identified. This may involve the third party 6 needing to obtain a legal decision that the conditions 408 have been breached. This requirement ensures that the purchaser 2 and the vendor 4 are confident using the coin 6, since they are aware that the third party 6 cannot alter the fungibility data 410 of the coin 400 without first performing due diligence.

Referring to Figure 13, there is shown an example of the trust 8 altering the fungibility data 410 of the coin 400.

45 In a first step 182, the provenance data field 406 of the coin 400 is reviewed, for example by the trust 8 or by the third party 6. The review may be prompted by an allegation (e.g. an allegation of corruption) or may be a routine review.

In a second step 184, it is determined whether there is an issue with the provenance data field 406; typically, this comprises reviewing the recent uses of the coin 400 and determining whether it has been transferred to an undesirable party or used for an undesirable purpose.

50 In a third step 186, if an issue is detected, the trust 8 (or another party) updates the fungibility data 410 of the coin.

If no issue is detected, the first step 182 is repeated, where the provenance data field 406 of the coin 400 is reviewed throughout the lifetime of the coin 400.

This process can be used to alter the fungibility data 410 of the coin 400 from a fungible state to a not-fungible state and also to alter the fungibility data 410 of the coin 400 from a not-fungible state to a fungible state. Where the coin 400 has been switched to a not-fungible state, the owner 402 of the coin 400 may update the provenance data field 406 with information demonstrating there are no issues with the provenance data of the coin (e.g. the owner 402 might upload further details relating to a suspicious transaction), then appeal to the trust 8 to return the coin 400 to a fungible state.

This method of alteration does not require the coin 408 to have the conditions 408 and is suitable for the second embodiment of the coin described with reference to Figure 4b. It will be appreciated that each method described herein could be performed using any embodiment of the coin 400 including, but not limited to, the coins described with reference to Figures 4a and 4b.

Referring to Figure 14, there is shown a detailed example of a cross-border gold trade that occurs using the coin 400.

The purchaser 2 and the vendor 4 agree on a transaction, in this example a trade of gold. The vendor 4 agrees to supply an amount of gold to the purchaser 2 in exchange for a payment.

Once the terms of the trade are agreed, a contract is signed and the purchaser 2 deposits an agreed-upon amount of an agreed-upon fiat currency with the purchaser bank 12 in return for the coin 400; the value 404 of the issued coin 400 corresponds to the deposited amount.

Before issuing the coin 400, the purchaser bank 12 communicates with a first central bank 12-1 in order to ensure that the purchaser 2 and the purchaser bank 12 are authorised to receive the coin 400. This check typically involves ensuring that each party to the transaction is considered trustworthy, e.g. no party to the transaction is under investigation for corruption or is in administration. This check may also involve an evaluation of the provenance information (both quantity and quality) provided by each party.

The agreement of the transaction and the issuance of the coin 400 is overseen by the third party 6, who verifies that the coin has been issued and verifies the terms of the transaction. On initialisation of the coin 400, the provenance data field 406 is populated with information relating to the purchaser 2 and the vendor 4, which may be provided by any party that is involved with the transaction.

The conditions 408 of the coin 410 is populated with information relating to the agreed-upon contract, for example subcontractors and timescales may be agreed upon in advance of the transaction.

The purchaser 2 then transfers the coin 400, or a part of the coin 400, to the vendor 4.

In some embodiments, the coin 400 is initialised in a non-fungible or partially-fungible state, or is modified to be in such a state before transference to the vendor 4. The vendor 4 is then able to transfer the coin 400 to sub-contractors and is able to identify the coin 400 as an asset, but is not able to redeem the coin 400 for fiat currency. The conditions 408 of the coin are set to switch the coin 400 to a fungible state upon completion of the contractual terms. In this way, the vendor 4 is assured of payment on completion of the contract without being able to redeem the coin 400 ahead of completion.

In some embodiments, the conditions 408 contain milestones, so that the coin 400 is split into sub-coins and each sub-coin is redeemable after completion of a related milestones. For example, receipt of the first bar of gold may result in a first sub-coin switching from a non-fungible state to a fungible state and therefore being redeemable.

Similarly, the purchaser may be issued a number of coins 400 of various denominations, where any one of the individual coins may be set to become fungible after completion of a relevant milestone.

The vendor 4 hires a first subcontractor 22 and a second subcontractor 24 to complete aspects of the trade, such as mining for gold, and smelting the mined gold. The hiring of these subcontractors results in the provenance data field 406 of the coins 400 used to pay the subcontractors being populated with relevant data on each of the subcontractors. Typical data that is recorded includes the company accounts and legal history of the subcontractor as well as data relating to of the transaction, such as the time of the transaction and the value of the coins transferred. The provenance data is useable to determine whether the first subcontractor 22 and the second subcontractor 24 are legitimate, trustworthy, companies.

The second subcontractor 24 employs an exporting subcontractor 26 and the exporting subcontractor 26 employs an importing subcontractor 28. In each case, there is a transfer of the coin 400, or a part of the coin 400, as part of the employment.

- In some embodiments, the coin 400 is only redeemable by certain parties, such as specific central banks. Specifically, the second subcontractor 24 is only able to redeem the coin 400 at the second central bank 14-1, to avoid money passing out of the second country without oversight of the second central bank 14-1. Once the coin 400 is transferred to the importing subcontractor 28, the provenance data field 406 is updated and it is identified (e.g. by the third party 6 or from publicly available records) that the importing subcontractor is a trusted importer that also conducts business outside of the second country. This may result in a change in the fungibility data 410 of the coin 400, where the coin switches from a partially-fungible state where it is spendable in the second country to a fungible state. This change in fungibility may be contingent on certain actions, such as the paying of importation taxes, or may require the importing subcontractor 28 to petition the second central bank 14-1 to update the fungibility data 410 of the coin 400.
- The importing subcontractor 48 delivers the gold to the purchaser 2 and then redeems the coin 400 at a subcontractor bank 42. The purchaser bank is arranged to communicate with one of the other banks, in this example the purchaser bank 12.

- At numerous steps, the coin 400 is split to enable the payment of various parties. Upon satisfactory completion of the project and a review of the provenance data field 406 of each part of the split coin, the conditions 408 of the coin 400 are deemed to be met and the parts of the coin 400 are each switched to a fungible state.

- In some embodiments, the parts of the coin 400 are automatically redeemed at the purchaser bank 12, vendor bank 14, or subcontractor bank 42 as soon as the transaction is completed. The first central bank 12-1 and the second central bank 14-1 are able to exchange the coin 400 for fiat currency, and this fiat currency is delivered to the purchaser bank 12, vendor bank 14, and subcontractor bank 42. In return, the central banks 12-1, 14-1 are given access to elements of the provenance data field 406 of the coin 400.

- This typically involves each fungible coin 400 being automatically redeemed upon completion of the (overall) transaction (that is, the gold being delivered to the purchaser 2). Each non-fungible coin 400 is not automatically redeemed, but instead must be brought to the central bank where a judgement is made on whether the coin 400 should be switched into a fungible state and then redeemed, or whether the coin 400 should remain in a non-fungible (and irredeemable) state.

- In this example, the vendor 4 also transfers a part of the coin 400 to a fake subcontractor 32. The fake subcontractor 32 is a corrupt party that is attempting to misappropriate funds via the coin 400.

- Provenance data relating to the fake subcontractor 32 is obtained from publicly available information, from the third party 6, and from the vendor 4 and the fake subcontractor 91, who are each required to fill in provenance information at the time of transferring the coin 400 to the fake subcontractor 32.

- Using this provenance data, the fake subcontractor 32 is identified to be a potentially corrupt party and the fungibility data 410 of coin 400 is altered so that the coin is non-fungible. The fungibility data 410 may be altered during or after the transaction with the fake subcontractor 32, so that the fungibility state may be changed after the transaction even if corruption issues are not identified at the time of the transaction. The fake subcontractor 32 is then unable to trade the coin 400 with other parties without consent (and any attempt to trade the coin 400 may result in a notification that the fake subcontractor 32 is under investigation and the coin 400 might not be redeemable).

- If the fake subcontractor 32 is in fact legitimate, the fake contractor 32 is able to provide evidence, e.g. provenance data, to the second central bank 14-1 to demonstrate their legitimacy. The second central bank 14-1 is able thereafter to alter the fungibility data 410 of the coin 400 to revert the coin 400 to a fungible, or partially-fungible state.

- The identification of the fake subcontractor 32 results in the alteration of the fungibility data 410 for the part of the coin 400 transferred to the subcontractor. Typically, the remaining parts of the coin 400, e.g. those parts transferred to the first contractor 22 and the second contractor 24 are not affected by this alteration in the fungibility data 410, so that the coins of the first contractor 22 and the second contractor 24 remain in a fungible, or partially-fungible state.

In some embodiments, a change in fungibility of a part of the coin 400 affects each other part of the coin 400, so that the change in fungibility due to the fake subcontractor 32 may result in each part of the coin 400 being switched to a non-fungible state.

- 5 In some embodiments, the fungibility data 410 is used to secure an exchange rate. The purchaser 2 and the vendor 4 are able to agree a fixed exchange rate at the start of the contract. The purchaser 2 then deposits the agreed upon amount of a first fiat currency at the purchaser bank 12. The purchaser bank 12 transfers the deposited money to the vendor bank 14, where the currency is exchanged for a corresponding amount of a second fiat currency via the first central bank 12-1 and the second central bank 14-1. The second fiat currency is then held in escrow until completion of the contract and the coin is  
10 redeemed for this amount. In this embodiment, the coin 400 is held in a non-fungible state until redemption, to avoid the coin 400 from being redeemed in the event of favourable currency fluctuations. By accepting the non-fungible coin as payment, each subcontracting party consents to the agreed-upon exchange rate. It will be appreciated that, alternatively, the first fiat currency could be held in escrow and the fixed exchange rate used could be the exchange rate at the time of completion of the transaction, or  
15 the exchange rate at any time between agreement and completion of the transaction.

In some embodiments, each transaction and/or each piece of provenance information must be validated and/or verified by one of the parties (e.g. the third party 6) before being added to the coin 400 and/or ledger.

- 20 Verification and validation are procedures that are used together for checking that a good and/or service, as is provided by the vendor 4 meets requirements.

Verification relates to checks that the good and/or service meets the required design specifications – this is typically an internal process of the vendor 4 that occurs before data is added to the coin 400.

- Validation relates to checks that the good and/or service meets the operational needs of the purchaser 2. This often involves acceptance from one or more third parties. Specifically, validation typically involves  
25 third parties confirming that information is relevant and correct before it is added to the coin 400.

While the example of Figure 14 has been described with reference to a divisible coin (and the use of parts of this divisible coin), it will be appreciated a similar transaction could be performed using a plurality of coins, where these coins may each have a fixed value.

- Referring to Figure 15, there is shown a series of sub-processes that form part of a transaction using the coin 400 (e.g. the transaction of Figure 14).  
30

Referring to Figure 15a, there is shown a method 1510 of managing provenance that occurs before the coin 400 is issued.

- In a first step 1512, a provenance model is constructed. This step comprises obtaining provenance data relating to one or more of the parties to a transaction, for example provenance data relating to the purchaser 2 requesting the issuance of the coin 400.  
35

In a second step 1514, the provenance data is verified and validated. This typically comprises the third party 6 confirming that the provenance data provided by the purchaser 2 is correct.

- In a third step 1516, the provenance of the purchaser 2 is explored. This typically comprises the third party 6 performing research to determine other characteristics of the purchaser 2 (e.g. by reviewing news articles).  
40

In a fourth step 1518, the provenance data field 406 of the (as-yet unissued) coin 400 is populated with the validated and exploratory provenance data.

Referring to Figure 15b, there is shown a method 1520 of managing smart contracts relating to a transaction.

- 45 In a first step 1522, suitable smart contracts are generated – this involves the participation and confirmation of each party to the transaction (e.g. the purchaser 2 and the vendor 4).

In a second step 1524, the smart contracts are embedded with the coin 400. This typically involves populating the conditions 408 of the coin 400 with the terms of the smart contracts and/or linking the smart contracts to the coin 400 via the identifier 412.

In a third step 1526, a proof of exploration occurs. This proof of exploration relates to recording proof that provenance data has been collected, and that each party agrees with the collected provenance data, as part of the method 1510 of managing provenance.

- 5 In a fourth step 1528, the permissions of the ledger are managed. This comprises the smart contracts being evaluated to determine which parties are authorised to read/modify/store the ledger/provenance data field 406/fungibility data 410.

Referring to Figure 15c, there is shown a method 1530 of adding and removing parties from the system 1.

- 10 Each party in the system 1 is required to provide provenance data in order to participate in the system 1 (e.g. to receive the coin). Parties that are not part of the system 1 are typically not able to take part in transactions.

In a first step 1532, a party is added to the system 1. Addition to the system 1 may be handled manually, e.g. with each party applying for access and being accepted/rejected, or may be automatic, where at the time of a transaction provenance data is collected and the party is automatically accepted/rejected on the basis of the collected provenance data.

- 15 Typically, adding a party involves performing checks on the party, such as know your customer (KYC) checks.

- 20 In a second step, a trigger is set for the party. This trigger relates to the conditions that can cause a change in the fungibility date 410 of the coin 400 when the coin 400 is held by the party in question. Each party in the system 1 may have different triggers so that, for example, the first bank 12 may be able to alter the fungibility data of the coin 400 only when the coin is held by the purchaser 2 (e.g. when the owner 402 of the coin 400 is the purchaser 2). As another example, the fungibility data 410 of the coin 400 may be altered in response to a transaction occurring in Europe when the coin 400 is held by the vendor 4.

In a third step 1536, the provenance data field 406 of the coin 400 is monitored. This step occurs continuously.

- 25 In a fourth step 1538, the party is removed from the system 1. Removal from the system 1 may occur if rules have been breached, for example if the party is involved in corruption. This removal typically means that the removed party can no longer hold the coin 400 or participate in transactions. In some embodiments, parties can request removal from the system 1.

Referring to Figure 15d, there is shown a method 1540 of managing a transaction.

- 30 In a first step 1542, the purchaser 2 and vendor 4 are identified and matched together.

In a second step 1544, appropriate transaction documents 1544 are generated. These documents are recorded in the provenance data field 406.

In a third step 1546, the transaction is executed and the coin 400 is transferred.

- 35 In a fourth step 1548, the transaction is tracked. This typically involves details of the transaction being recorded in the provenance data field 406 (e.g. as descriptive data).

Referring to Figure 15e, there is shown a method 1550 of issuing and redeeming the coin 400.

In a first step 1552, an exchange rate is determined. This typically comprises consideration of a market rate. In some embodiments, the exchange rate is influenced by the issuing bank and/or the issuing central bank.

- 40 In a second step 1554, the coin 400 is issued. This comprises transferring a coin to the purchaser 2 with the owner 402 and the value 404 set appropriately. The provenance data field 406, conditions 408, and fungibility date 410 are populated using data collected during the method 1510 of managing provenance and the method 1520 of managing smart contracts.

In a third step 1556, the coin 400 is monitored. This step occurs throughout the lifetime of the coin 400.

- 45 In a fourth step 1558, the coin 400 is redeemed. This redemption typically depends on the state of fungibility of the coin 400, where the redeeming institution may refuse to redeem a non-fungible or partially-fungible coin.

- 50 Redemption refers to the exchange of the coin 400 for an amount of fiat currency. Redemption typically involves the coin 400 being purged of the owner 402, the provenance data field 406, the conditions 408, the fungibility data 410, and optionally the identifier 412, and then being recycled. Typically, the value 404

of the coin is a pointer to one or more digital currency addresses. There may be a finite amount of digital currency addresses so that recycling coins is necessary to maintain the supply of digital currency.

In some embodiments, coins 400 are single use, so that the coin (and the related digital currency addresses are lost after redemption).

- 5 Redemption typically occurs at the end of a transaction (where a number of sub-transactions may occur in between the issuing and the redeeming of the coin 400).

Referring to Figure 15f, there is shown a method 1560 of managing a transaction (or a sub-transaction).

In a first step 1562, the transaction is checked. This check typically comprises anti-money-laundering (AML) checks and checks of provenance information of the vendor 4.

- 10 In a second step 1564, documentation is generated relating to the transaction. This is useable after the transaction as proof of the transaction. This documentation is stored in the provenance data field 406 of the coin 400.

In a third step 1566, the coin 400 is transferred to the vendor 4. The coin 400 is tracked throughout the transaction, which might involve multiple steps (information relating to each step is recorded in the provenance data field 406).

- 15

In an optional fourth step 1568, fiat currency that is part of the transaction is transferred and tracked.

Referring to Figure 15g, there is shown a method 1570 of delivering a good in relation to a transaction.

In a first step 1572, a goods flow document is generated.

In a second step 1574, delivery logistics are planned.

- 20 In a third step 1576, the goods are obtained (by the vendor 4).

In a fourth step 1578, the goods are delivered (to the purchaser 2).

Information relating to each of these steps is stored in the coin 400 in the provenance data field 406. This serves to update the purchaser 2 on the progress of the delivery of the good and also serves as documentation that can be used to evaluate the transaction at a later date. For example, if the delivery is late, the recorded delivery logistics plan may be examined and determined to be falsified.

- 25

Referring to Figure 15h, there is shown a method of evaluating a transaction. This typically occurs alongside the redemption of the coin 1558.

In a first step 1582, an agreement with the central bank 1582 is confirmed. This typically relates to an examination of the conditions 408 of the coin. The central bank may agree to redeem the coin only if the conditions 408 have not been breached. In some embodiments, the coin 400 is only redeemable by certain parties (e.g. a specific central bank).

- 30

In a second step 1584, the value 404 of the coin 400 is transferred to the party redeeming the coin 400.

In a third step 1586, the provenance data field 406 of the coin 400 is evaluated and the provenance data is transferred to the central bank redeeming the coin 400.

- 35 In a fourth step 1588, the provenance data is archived. This data may then be deleted from the provenance data field 406 of the coin 400 so that the coin can be reused.

Any combination of the methods of Figure 15 may occur as part of a transaction or a sub-transaction.

Referring to Figure 16, there is shown in more detail an exemplary method of determining the exchange rate of the digital currency.

- 40 In a first step 1602, a 'linking' currency is determined. A transaction may take place in any variety of currencies; typically, the value 404 of the coin 400 is linked to a selected one of these currencies, such as the dollar or the pound. The selected currency may be defined by a smart contract or by the party issuing the coin 400. The value 404 may then be related to the linking currency, for example the coin 400 may have a value of two 'exampleCoin-Dollars'.

- 45 As well as a currency, the linking 'currency' could be a commodity, such as gold.

In a second step 1604, the value 404 of the coin 400 is determined. This is typically dependent on a smart contract that defines the value of a transaction. In embodiments where coins are 'denominationalised' – that is embodiments where the value 404 of the coin 400 can only be one of a limited number of denominations, the second step 1604 may also comprise determining the number of coins 404 required to

obtain a certain value and the value 404 of a number of coins 404. Specific denominations for each coin may also be determined, where depending on the transaction it may be desirable to issue many coins of low denomination or fewer coins of higher denominations – the denominations to use may be specified in a smart contract.

5 In a third step 1606, an appropriate amount of a fiat currency is received by the party issuing the coin 400. The amount is dependent on the value 404 of the coin(s) being issued and the exchange rate at the time of the issue. As an example, if the linking currency is dollars and the purchaser 2 is transferring pounds in return for the coin 400, the amount of pounds needed depends on the GBP-USD exchange rate at the time of the transfer.

10 In a fourth step 1608, the coin 400 is issued with the value 404 of the coin 400 set appropriately.

In an optional fifth step 1610, the value of the linking currency is monitored. In some embodiments, fluctuations in the linking currency result in one of the parties being required to deposit and/or withdraw an amount of fiat currency to keep the value 404 of the coin 400 stable relative to other currencies. For example, a fall in the value of the pound relative to the dollar may require the purchaser to deposit more pounds so as to keep the value of each issued coin constant (relative to the pound).

15 The purchaser 2 typically agrees an amount of a fiat currency to transfer to the vendor 4 in return for a good and/or service. This amount of fiat currency is exchanged for a corresponding amount of the digital currency, in the form of coins, upon agreement of the transaction details. Where the value of the fiat currency changes in relation to the value of the digital currency, the amount of fiat currency which the vendor 4 stands to gain on completion of the transaction also changes. By requiring the purchaser 2 to deposit/withdraw fiat currency in dependence on fluctuations in the relative value of the fiat currency, a constant value of fiat currency can be guaranteed to the vendor. Effectively, the smart contract may contain a clause whereby the purchaser 2 agrees to maintain an agreed-upon value of the digital currency through deposits/withdrawals.

25 In practice, the coin 400 may be issued in a closed, permissioned, system 1 where the value of the coin 400 is guaranteed by the issuer of the coin 400. As an example, as part of a smart contract, the purchaser 2 may agree with the central bank a value of the coin based on another currency and/or a commodity as well as an issuance fiat currency and a redemption fiat currency. The purchaser 2, or another party, may then deposit enough of the issuance fiat currency to back each coin issued in relation to the smart contract. Fluctuations in the value of the issuance fiat currency relative to the redemption fiat currency may require the purchaser to deposit or withdraw an amount of the issuance fiat currency to ensure that the vendor is eventually able to redeem the coin for the agreed-upon amount of the redemption fiat currency.

In some embodiments, the digital currency is not pegged to any other currency and its value can fluctuate freely. In these embodiments, stability may be attained by:

- 35
- Implementing conditions 408 that discourage speculation (e.g. requiring the coin 400 to be used in a transaction every day).
  - Requiring parties holding the coin 400 to participate in exploration/recording of provenance data.
  - Altering the fungibility data 410 of coins used for speculation.
  - Only allowing transactions with permissioned parties (e.g. limiting access to the system 1 to trusted parties).
- 40
- Issuing or withdrawing coins to alter the supply of coins in response to changes in demand.

A feature of the system 1 is each coin acts as an individual reservoir of provenance information. As well as providing information to each of the parties using the coins, this action as an individual reservoir serves to discourage speculation and encourage a stable coin. In some embodiments, provenance data is stored primarily, or solely, on coins, so that coins which are held by a party for a significant length of time (e.g. for speculation) do not accrue provenance data. Therefore, the presence of the provenance data field 406 encourages the use of the coins.

45 Provenance information is universal – information relating to the coin 400 has value in each culture and provenance information is available for any party. This is in contrast to commodities, such as oil. The digital currency is, in effect, backed by provenance information, where any party is able to access the system 1 by providing appropriate provenance information. This enables the use of the system 1 across cultures and regions that do not have common commodities.

50

In some embodiments, the value 404 of the coin 400 is linked to provenance information, where the issuance of the coin involves population of the provenance data field 406 and the value 404 of the coin 400 is dependent on this information contained in the provenance data field 406.

5 Where coins are linked to a currency, coins may be fungible only with coins linked to the same currency, where transfers using coins of different linking currencies require approval from the parties involved in the transfer.

10 There may be a plurality of systems 1 in which the digital currency is implemented. In each of these systems the digital currency may have a different value. Alternatively, in each system, the cryptocurrency may have the same value. Coins from different systems may be interchangeable or not interchangeable (e.g. these coins may be fungible, partially-fungible, or non-fungible).

Typically, the system 1 contains a foreign exchange management module (not shown) that is arranged to determine appropriate exchange rates at the time of issuing each coin.

15 While the third step 1606 relates to each currency being exchanged before the coin 400 is issued, in some embodiments, each currency may be transferred only after the coin 400 has been redeemed. As an example, the purchaser may transfer a certain amount of pounds to the issuing party at the time of issuing the coin 400 and then after the coin 400 is redeemed, a suitable amount of pounds are taken by the issuing party (depending on the exchange rate at the time of redemption) and the remainder of the transferred amount is returned to the purchaser 2.

20 Typically, the issuance of any coin requires a foreign exchange management process, where the currencies and the exchange rates that will be used at any step of the process (e.g. on issuance of the coin and on redemption of the coin) are agreed upon. Agreed-upon exchange rates may not be numerical values, but may instead be references to a rate (e.g. the redemption exchange rate may be "the inter-bank rate at the time of redemption"). This management process minimises disagreements about the issuing/redemption of the coin 400.

25 In some embodiments, the provenance information that is accessible and/or stored in relation to the coin 400 is dependent on an ecosystem relating to a transaction of the coin; typically, this ecosystem relates to a country and/or issuing authority. More generally, the provenance information that is accessible by a party and/or stored may depend on a feature of a transaction and/or a party to a transaction. In particular, the location of storage of the provenance information may depend on this feature and/or party.

30 This is described in relation to Figures 17 and 18, which illustrate the selective accessibility/storage of information in dependence on an ecosystem.

Referring to Figure 17, a number of transactions are made which result in a coin moving from a first state 202 to a second state 204 to a third state 206 to a fourth state 208 to a fifth state 210. The transitions from the first state 202 to the second state 204 and from the fourth state 208 to the fifth state 210 comprise cross-border transactions from a first ecosystem 74 to a second system 76 and from the second ecosystem 76 to the first ecosystem 74 respectively.

35 Typically, a party relating to the first ecosystem 74, e.g. a government of a first country, is able to view information relating to the first state 202 and the fifth state 210 of the coin 400 and a party relating to the second ecosystem 76 is able to view information relating to the second state 204, the third state 206, and the fourth state 208 of the coin.

40 The party relating to the first ecosystem 74 may be able to view certain types of information relating to the second state 204, the third state 206, and the fourth state 208, or may not be able to view any of this information. Typically, the party relating to the first ecosystem 74 is able to track the exit of the coin 400 from the first ecosystem 74 by viewing a transaction relating to an output of the first state 202 and is able to track the re-entry of the coin 400 into the first ecosystem 74 by viewing an input of the fifth state 210. The party relating to the first ecosystem 74 may not be able to obtain any further information relating to the activity of the coin 400 (e.g. relating to its use in the second ecosystem 76), or may be able to identify, for example, that the coin has been involved in two transactions in the second ecosystem 76.

45 In various embodiments, the party relating to the first ecosystem 74 may be completely unaware of the third state 206, may be aware only that the third state 206 has occurred (e.g. that there have been transactions made between the second state 204 and the fourth state 208), may be aware of only certain information relating to the third state 206, or may be fully appraised of the third state 206.

Typically, the party being related to the first ecosystem 74 only being able to view certain information is achieved by the coin 400 storing information in a datastore that depends on the ecosystem in which a transaction takes place and/or storing information so that it is only accessible by certain parties. In some embodiments, encryption is used so that only the party from the first ecosystem 74 can view information relating to the first state 202 and the fifth state 210 and only the party from the second ecosystem 76 can view information relating to the second state 204, the third state 206, and the fourth state 208. In this regard, the states typically comprise information relating to an input and to an output so that a party viewing the output information for the first state 202 may view similar (or the same) information as a party viewing the input information for the second state 204.

However, even if the information is encrypted, the parties involved must each trust the encryption. If the coin 400 stores all provenance information in an encrypted form, then the party related to the first ecosystem 74 must have confidence that the party related to the second ecosystem 76 cannot bypass this encryption. Where sensitive information is contained in the provenance information (e.g. financial data, an indication of possible corruption, or confidential/secret information), having any public record (even an encrypted record) of this information may be undesirable.

With reference to Figure 18, there is described a method where only certain types of provenance information are recorded in relation to the coin 400 (e.g. on a public and/or distributed blockchain relating to the coin 400). Other types of provenance information are stored in a separate datastore and/or database, which datastore is dependent upon an ecosystem relating to a transaction. This separate datastore may comprise or more digital currency wallet, one or more servers, and/or one or more blockchains, which may be privately held or have a limited distribution.

In the example of Figure 18, the coin 400 moves between four states as a result of four transactions; specifically, the coin moves from a first state 216 to a second state 218 to a third state 220 to a fourth state 222. In the first state 216 and the fourth state 222, which relate to the first ecosystem 74, the coin 400 is related to a first datastore 212; in the second state 214 and the third state 1822, which relate to the second ecosystem 76, the coin 400 is related to a second datastore 214.

For each transaction, the coin 400, and/or a datastore and/or blockchain relating to the coin 400, stores only information necessary to track transactions, such as a sender, a recipient, and an amount. The sender and/or the recipient may be identified by random or pseudo-random identifiers (e.g. an ID number) to avoid revealing information about the holders of the coin 400. In some embodiments, the coin 400 comprises only an amount, where the holder of the coin 400 is whichever party has access to an authorising mechanism, such as a cryptographic private key.

Where the sender and/or recipient are identified by a pseudorandom ID, certain parties may be capable of matching the ID to an identity. Therefore, the parties may be effectively anonymous to their peers, but not anonymous to parties in control of the relevant ecosystem. For example, a central bank may have access to a look-up table that relates IDs to information about the party with that ID; therefore, the central bank (and only the central bank) is able to identify the parties involved in transactions. Storing this information in relation to the coin enables multinational parties to easily be identified by relevant parties, which may be desirable. As an example, a company that is active in both France and Germany may be identified using an identifier that is known to the French and German governments but not to the Spanish government. Therefore, transactions made by this company in Germany can be identified by the French government (e.g. for tax purposes) and the German government only. Transactions made by this company in Spain may be arranged to be identifiable by each of the Spanish, French, and German governments. To achieve this, the identifier may comprise a combination of an in-ecosystem identifier and a global identifier.

The first datastore 212 and the second datastore 214 comprise provenance information relating to the use of the coin 400; as an example, the first datastore 212 and the second datastore 214 may comprise records of each transaction made in the related ecosystems as well as the reasons for each transaction, the timing and location of each transaction, and the parties involved in each transaction.

It will be appreciated that the types of data stored in relation to the coin 400 and those stored in relation to the first datastore 212 and the second datastore 214 may vary depending on the implementation. In particular, in different situations, different types of information may be considered to be sensitive (and therefore unsuitable for sharing between ecosystems). In typical embodiments, the names of the parties involved in each transaction are considered to be non-sensitive information that is stored in relation to the

coin 400 (as part of the first state 216 and the second state 218); however, in some embodiments this party information is instead stored in the first database 212 and the second database 214.

The first datastore 212 stores information relating to transactions made within the first ecosystem 74. When the coin 400 is transferred from the first ecosystem 74 to the second ecosystem 76, only the (basic) information stored in relation to the coin 400 is transferred from the first state 216 to the second state 218; the information in the first database 212 is not transferred to the second database 214. In practice, this may involve a blockchain relating to the coin 400 being updated based on two parties involved in a transaction and an amount relating to that transaction. Provenance information relating to the transaction, e.g. the reasons for the transaction, is recorded in a separate datastore.

In some embodiments, the coin 400 is tracked in a non-public manner, e.g. a private database or a non-public blockchain. In these embodiments, all information may be stored in the same place so long as the coin 400 is being used in the first ecosystem 74. The transfer of the coin 400 to the second ecosystem 76 may then result in only a subset of the information held in relation to the coin 400 being transferred.

When the coin is transferred from the second state 218 to the third state 220, the provenance information stored in the second datastore 214 is updated and the coin 400 remains connected to the second datastore 214. It will be appreciated that the coin 400 may be transferred between a number of wallets relating to separate parties; therefore, while this example describes the coin 400 continuously being connected to the second datastore 214, more generally it is the case that for transactions that occur within the second ecosystem 76, provenance information is stored in such a manner that a party related to the second ecosystem 76 (e.g. a central bank or a regulatory body) can access this information.

When the coin 400 is transferred back to the first ecosystem 74, the coin 400 is re-associated with the first datastore 212, e.g. via a zero-knowledge proof. Typically, the first datastore 212 is arranged to determine whether incoming coins relate to previous outgoing coins in order to track flows of money into and out of the first ecosystem 74. This may comprise an identifier relating to the coin 400 being determined and compared to the identifiers for previous coins in circulation in the first ecosystem 74. This enables the party related to first ecosystem 74 to match outgoing and ingoing transactions.

Using the arrangement described in reference to Figure 18, regulatory bodies in each ecosystem can store and assess provenance information for internal transactions without being concerned about external parties gaining access to this provenance information.

An arrangement where provenance information is stored in relation to a datastore may be used in conjunction with an arrangement where provenance information is stored in conjunction with the coin 400. In particular, a transaction may be analysed at the time of the transaction to identify whether the transaction relates to the removal of the coin 400 from a certain ecosystem (e.g. a country); if the transaction does indeed relate to such a removal, then an amount of the provenance information stored in relation to the coin 400 is removed from the coin 400 and (optionally) transferred to a datastore. Alternatively, the coin 400 may be arranged to stop storing provenance information in relation to the coin following the removal from the ecosystem. Storage of provenance information in relation to the coin 400 enables straightforward analysis of the provenance of the coin 400 while the coin remains in the ecosystem. The coin 400 is typically defined with relation to a blockchain, so that information relating to the coin 400 (and any transactions in which the coin 400 is involved) is stored on this blockchain. Removal/transference of provenance information may be achieved by encryption of the blockchain up to a certain point and/or the transfer/deletion of an encryption key that enables interpretation of the parts of the blockchain relating to the coin 400.

In some embodiments, a plurality of blockchains are provided, with each blockchain relating to an ecosystem (e.g. a country). In some embodiments, the datastore comprises a blockchain. These ecosystem-dependent blockchains may be stored on/accessible from only certain computer devices, e.g. the blockchains may be stored only on certain government databases. Certain parts of the blockchains, e.g. those containing the high-level information described in relation to Figure 18 as being stored in relation to the coin 400, may be publicly accessible.

In some embodiments, the provenance information – or a subset of the provenance information – is segregated from the transaction information, while still being stored on the same blockchain. The segregated provenance information may then have different access requirements (e.g. require the provision of a specific private key). In some embodiments, the segregated provenance information is encoded using a public key relating to an ecosystem, where the ecosystem is related to the transaction

being made; only the agents of that ecosystem are then able to view the segregated provenance information. The ecosystem is typically a country, where segregated provenance information is encoded in dependence on a public key provided by a regulatory body of that country.

5 By not storing provenance information directly in relation to the coin 400, an anonymous coin can be provided – where this coin may be anonymous to only certain parties (e.g. anonymous to users of the coin 400, but not anonymous to overseers of ecosystems in which the coin 400 is used).

10 By controlling the access requirements for accessing the provenance information, the degree of anonymity can be controlled by an ecosystem. For example, if an ecosystem that issues the coin 400 provides full provenance information without any access requirements, each coin can be tracked in detail by each party so that determining the owner/history of each coin is trivial. This effectively removes any anonymity relating to transactions.

15 Conversely, if the ecosystem that issues the coin 400 completely separates provenance information from the coin 400 so that the provenance information cannot be accessed, then each coin is effectively anonymous. As has been described above, the information stored in relation to a transaction may comprise merely an amount, or merely an amount and a pseudo-anonymous identifier relating to a sender/recipient. Therefore, the coin 400 can be used to implement a system of anonymous transactions. Furthermore, by segregating the provenance information and allowing access to only specific parties (e.g. regulatory bodies), a coin can be provided that is entirely anonymous on a personal level (e.g. a casual observer cannot track the coin) while entirely lacking anonymity on a governmental level (so that a government can track the ownership and use of the coin). Any intermediary level of anonymity can be provided by suitable segregation and control of provenance information, so that, for example, the coin 400 may be arranged so that the government can track the usage of the coin 400 without being able to track the ownership of the coin (e.g. by segregating separately the “what” and “why” provenance information from the “who” provenance information).

25 Typically, multiple parties are capable of issuing coins, e.g. the central banks of multiple countries. Therefore, there may exist different issuers that impose different provenance rules, such as different segregations of provenance information and different levels of anonymity. When transferring the coin between ecosystems (e.g. across borders), the provenance information stored in relation to the coin 400 may depend on a maximum anonymity requirement, a minimum anonymity requirement, and/or an agreed anonymity requirement. Typically, when the coin 400 is transferred between ecosystems, the historic provenance information relating to the coin 400 is stored, encrypted and/or transferred so as to be accessible only by parties relating to the ecosystem out of which and/or into which the coin 400 is being transferred. The provenance information stored while the coin 400 is in the second ecosystem may depend on parameters imposed by the first ecosystem. As an example, on issuance of the coin 400, the first ecosystem may specify that provenance information is recorded only for transactions that occur within the first ecosystem. In a practical example, the first ecosystem is the USA and the second ecosystem is Russia; provenance information is stored for all transactions that occur in the USA, the coin 400 is then transferred to Russia and no provenance information is stored for any transactions that occur in Russia, the coin 400 is then returned to the US and provenance information is once again stored.

40 In some embodiments, the anonymity of the coin 400 is dependent on the fungibility of the coin 400 and/or a use of the coin 400. In particular, users of the coin 400 may be effectively anonymous where the coin is used normally (e.g. identified only by random identifiers) and then identifiable when the coin 400 is altered to a non-fungible state. This may be implemented using smart contracts, where identifiers are normally an encrypted version of names, and these names are unencrypted (for certain parties) when the fungibility is altered. This enables a coin that is anonymous for normal users, where the anonymity can be taken away when illicit act is committed. Typically, an alteration in the fungibility of the coin 400, and in particular the switching of the coin 400 to a non-fungible state, reveals one or more of: the identity of the current owner of the coin 400; the identity of a previous owner of the coin 400; provenance information relating to a transaction that resulted in alteration of fungibility; and one or more parties involved in a transaction that resulted in an alteration of fungibility. The alteration of anonymity may be automated process that is dependent on, for example, provenance information relating to the coin and/or may be dependent on a manual input, such as a party applying for a warrant to remove the anonymity.

Where different types of information are stored in relation to the coin 400 and in relation to separate datastores, the rules governing allowable transactions (those which do not cause a change in fungibility)

and non-allowable transactions (those which do cause a change in fungibility) may be stored in relation to the coin 400 or in relation to a datastore. In particular, each ecosystem may have a separate datastore (or group of datastores, such as a group of digital wallets) and this datastore may store the fungibility rules for that ecosystem. This provides a straightforward way for each ecosystem to use different fungibility rules and simplifies the transfer of the coin 400 between ecosystems (e.g. between countries).

Upon re-entering the first ecosystem, the coin 400 may be re-associated with the previous provenance information. As an example, provenance information relating to the coin 400 may be encoded using a first public key for transactions made in the first ecosystem 74 (e.g. a first country), subsequently provenance information relating to the coin 400 may be encoded using a second public key for transaction made in the second ecosystem 76 (e.g. a second country), and then upon the return of the coin 400 to the first ecosystem provenance information may again be encoded using the first public key.

This re-association with previous provenance information may depend on an evaluation of the coin 400, for example an evaluation of the blockchain on which transactions relating to the coin 400 are recorded. Where the coin is in a "fully anonymous" state, it may be the case that no information is recorded relating to the owners of the coin 400, and the owner is effectively whomever holds a relevant private key. In this situation, connecting a coin leaving the first ecosystem with a coin entering the first ecosystem is not trivial and may rely on an analysis of the activity of that coin; where this analysis typically involves a zero knowledge proof that is determined based on past transactions of the coin. In short, it is possible to determine that the coin entering the first ecosystem is related to a coin that has previously left without revealing any provenance information that relates to that coin.

In various embodiments, various combinations of information may be stored in relation to the coin 400 (e.g. on a blockchain that records transactions that use the coin 400) and separately to the coin – e.g. in a separate datastore, for example:

- Only an amount may be stored in relation to the coin 400, with all other information stored in the separate datastore.
- A pseudo-random identifier (e.g. an ID number) may be stored in relation to the coin 400, with a specific identifier (e.g. a company or personal name) stored in the separate database.
- All provenance information may be stored in the separate datastore.
- Descriptive provenance information may be stored in relation to the coin 400.
- Interpretive provenance information may be stored in the separate datastore.
- Information provided at the time of the transaction may be stored in relation to the coin 400.
- Information provided after the transaction may be stored in the separate datastore.
- Information provided by the parties involved in the transaction may be stored in relation to the coin 400.
- Information provided by third parties may be stored in the separate database.

Effectively, there may exist a plurality of separate ecosystems, where each ecosystem has separate controlling entities and coin issuers (e.g. central banks). These controlling entities can set the parameters for each ecosystem, e.g. the types of information recorded and the spending conditions. This may be used to set different conditions for altering the fungibility of the coin 400 in different ecosystems. The coin 400 can be transferred, and used, across ecosystems, while the set parameters only affect the use of the coin in a related ecosystem. In order to simplify the use of the coin 400 across ecosystems, the information recorded in relation to the coin 400 (e.g. recorded on a blockchain related to the coin) may be minimal, such as being just an amount, or an amount, recipient, and spender. The information that is pertinent to each ecosystem can then be stored within that ecosystem and thereafter kept within the ecosystem or shared outside of the ecosystem according to the wishes of the parties within that ecosystem.

An example of the use of such separate ecosystems is for different countries. Each country may have different laws and desires so that each party may record different information relating to transactions that use the coin 400 as well as setting different rules. Spending the coin 400 on alcohol may be allowed in certain countries and may result in an alteration of the fungibility of the coin 400 (e.g. to make the coin non-fungible) in other countries. Further, tracking whether the coin has been used to purchase alcohol may only be required in certain countries. To achieve this, provenance information relating to purchases in each country can be stored in relation to a datastore for that country. Similarly, rules relating to these purchases can be considered only in relation to a set of rules for the country.

- In some embodiments, altering the fungibility of the coin comprises altering the data that is stored in relation to the coin and/or the datastore. As an example, a coin that is used for an illicit purpose in the first ecosystem 74, such as for bribery, may be marked as non-fungible on the blockchain relating to the coin. This change is visible to parties in the second ecosystem 76, where these parties are then able to identify that the coin 400, and/or the owner of the coin 400, might have been involved in corruption. In some embodiments, a type of information is stored in a datastore when the coin 400 is in a fungible state and this information is stored in relation to the coin when the coin is in a non-fungible state. The information may for example be provenance information that indicates a use of the coin (e.g. bribery, gambling, etc.) or a flag relating to the state of the coin and/or the conditions for returning the coin to a fungible state.
- 10 In various embodiments, the different ecosystems relate to:
- different countries;
  - different company structures;
  - different industries; and
  - different regulatory bodies.
- 15 A benefit of the storage of provenance information is that it can be used to assess transactions and to identify problematic transactions, e.g. those relating to corruption. Therefore, it is desirable for the party related to the first ecosystem 74 to be able to view certain provenance information relating to a transaction made within the second ecosystem 76. To enable this, there is described with reference to Figures 19 and 20 a method of the party related to the second ecosystem 76 sharing information with the party related to the first ecosystem 74.
- Referring to Figure 19, there is shown a method of sharing information with another ecosystem.
- In a first step 232, a party related to the first ecosystem 74 receives a request for information. This request may comprise a request to share all information relating to a certain coin, a certain party, and/or a certain transaction, or may comprise a request for a specific piece of information (e.g. who was the recipient of a certain transaction). Similarly, the request may comprise a request relating to interpretive provenance information, e.g. "has the coin been involved in any transactions that may be a part of corruption?"
- 25 In a second step 234, the party requesting the information is assessed. This assessment typically comprises assessing the identity of the party requesting the information in order to determine whether it is appropriate to share the information with this requesting party. This step may comprise determining a proof of identity of the requesting party.
- 30 In a third step 236, the request is accepted or requested in dependence on the request itself (e.g. the type of information requested, and the assessment of the requesting party).
- In some embodiments, the assessing of the party requesting the information comprises assessing a piece of information provided by that party. Typically, two parties will wish to exchange corresponding pieces of information; as an example, if a company is under investigation for corruption, then two countries in which that company has been active may wish to share information relating to that company. In this situation, it is likely that neither country will wish to unilaterally share information – and in many situations, one country will not trust the other. Therefore, assessing the party may comprise a two-way exchange of information, whereby the receipt of information from the requesting party is determined before the requested information is sent.
- 35 Typically, the determination that a party has relevant information is determined using a zero-knowledge proof, where the existence of the desired information is determined without the information itself being revealed. As an example, the requesting party is able to demonstrate that it holds information about a certain company by demonstrating that it can differentiate between two different encodings of the company's name.
- 40 Typically, each party agrees to transfer certain information; that each party holds this information is demonstrated by the provision of appropriate zero knowledge proofs. Once the proofs have been transferred, or received by an intermediary (e.g. an intermediary computer) and confirmed, the information is transferred between the parties.
- 45 An example of this transfer of information is described with reference to Figure 20.
- 50

In a first step 242, a coin issuer 72 issues one or more coins. These coins may be tied to a transaction, and/or a purpose, as has been described above. The coin issuer may also set rules relating to the information stored in relation to the coins and/or the information stored along with the coins.

5 In a second step 244, a first company that is part of a first ecosystem 74 receives the coins from the issuer. This first company may, for example, be a company that is contracted to complete an infrastructure project.

In a third step 246, the first company disseminates the coins. This may, for example, comprise the first company paying its employees and/or paying contractors to complete tasks.

10 In a fourth step 248, a second company that is part of a second ecosystem 76 receives the coins. The third step 246 and the fourth step 248 may relate to a number of transactions; for example, the first company may hire a contractor, which contractor hires further subcontractors. Therefore, the second company may be a number of transactions removed from the first company. Typically, the first ecosystem 74 and the second ecosystem 76 comprise different countries, where the first company and the second company are companies based in these different countries.

15 In a fifth step 250, provenance information is recorded in relation to one or more transactions that have occurred in relation to the coin. While this fifth step 250 is shown as being subsequent to the fourth step 248, it will be appreciated that the recording of provenance information is typically be a continuous process; where each use of the coin leads to the recording of provenance information.

20 Typically, the provenance information is recorded in a datastore that relates to a single ecosystem, e.g. a country-specific wallet. This storage method results in a party related to the first ecosystem 74 being able to access information relating to transactions in that first ecosystem 74 and a party related to the second ecosystem 76 being able to access information relating to transactions in the second ecosystem 76. Typically, the party related to the first ecosystem 74 is not able to routinely access information relating to transactions in the second ecosystem 76.

25 In order to access information relating to transactions in the second ecosystem 76, in a sixth step 252, a requesting party related to the first ecosystem 74 requests provenance information from a controlling party related to the second ecosystem 76. This request may be for all provenance information relating to a coin, or a number of coins, and/or may be for a specific type of provenance information.

30 The requesting party may be the same as the above-mentioned first party and/or the controlling party may be the same as the above-mentioned second party. Alternatively, one or both of the requesting party and the controlling party may be a different party (e.g. a regulatory body).

In a seventh step 254, a controlling party that is related to the second ecosystem 76 receives the request and then in an eighth step 256 the controlling party assesses the request.

35 The request may comprise a reference to a type of information that is being requested and may comprise information that is to be supplied in return. Typically, the request comprises a zero knowledge proof that evidences that the requesting party has access to a certain type of information, where this type of information is being offered in exchange for the requested information.

In an eighth step 228, in dependence on the request the controlling party transmits provenance information to the requesting party. In a ninth step, the requesting party receives the provenance information.

40 In a practical example, the first company and the second company are two companies that are headquartered in different countries. Once the coins have been disseminated, the first company and/or a regulatory body related to the first ecosystem 74 wishes to determine how and why the money has been spent. In order to do this, the first company and/or regulatory body must be able to review transactional information relating to the second ecosystem 76. Therefore, one of these parties makes a request for information to a controlling party of the second ecosystem. This may, for example, comprise a government in a first country requesting information from a government in a second country.

The request may be reciprocal, so that the first government offers information to the second government information that enables both governments to fill in the gaps in a transactional history. This enables both governments to be able to track the flow of the coins, e.g. for tax purposes or to identify corruption.

50 The requesting and controlling parties may also be companies within the first ecosystem 74 and the second ecosystem 76. In this example, there may be certain companies with which the controlling party is willing to share information – e.g. the controlling party may only share information with companies that

have been vetted. This enables the controlled dissemination of information while enabling sensitive information to be retained by only a selected group.

In some embodiments, the sharing process is at least partially automated, where the controlling and the requesting party have an agreement to share certain types of information. As an example, countries may have an agreement to share information for the purposes of tax collection; this can result in provenance data being shared that indicates a tax burden incurred by a party in relation to the coin 400. Where this occurs, other information relating to the coin 400 may still be kept within a single ecosystem.

Typically, there is each ecosystem is overseen by a regulatory body (e.g. a central bank) that is able to define types of information that can be shared across ecosystems, and possible reasons for sharing that information. As examples:

- Information may be shareable based on a monetary exchange, and/or an information exchange.
  - Information may only be shareable between parties in related fields (e.g. two construction companies).
  - Information may only be shareable across certain borders.
- In some embodiments, the request for information is made directly to an overseeing body, which is capable of sharing information on behalf of the controlling party – this may comprise a central bank forcing a company to share information with other relevant parties.

In some embodiments, the request to share information is based on an 'exploration tax'. As has been described above in relation to the provision of provenance information, parties may be rewarded for exploration (e.g. mining reward a block of the blockchain may be based on exploration, and a mining reward may be awarded in dependence on this exploration). The exploration reward may be used to request the sharing of information.

The datastore in which provenance information is stored may relate to one or more of a company, a governmental body, and/or an individual; furthermore, there may be provided nested datastores which relate to a plurality of these parties. As an example, provenance information may be stored in a company wallet, where a government regulator is able to access the stored provenance information for a plurality of companies. Companies are then able to trade provenance information based on rules set by an overseeing party (e.g. the government regulator).

Instead of, or as well as, sharing provenance information, the party related to the second ecosystem 76 may share analysis results with the party related to the first ecosystem 74. For example, the party related to the second ecosystem 76 may share maps that track money flows and/or a probability that the coin 400 has been used for corruption. This enables the sharing of analysed information across ecosystems without requiring either party to divulge possibly sensitive information used during the analysis process.

The above methods are applicable to both unspent transaction output models and account models. As an example, information may be stored in relation to the coin in the form of storage in relation to a UTXO on a blockchain; information may also be stored in relation to an account.

Where a transaction takes place across the border of an ecosystem, this may relate to a UTXO being transferred from the first ecosystem 74 to the second ecosystem 76 or a transaction being made from an account in a first ecosystem 74 and an account in the second ecosystem 76.

Transactions do not necessarily involve the transfer of a monetary asset; more generally the coin 400 refers to a transfer of information between two parties (where this information may relate to an asset or a service).

#### Alternatives and modifications

Various other modifications will be apparent to those skilled in the art for example, for example, while the majority of the detailed description has considered the described digital currency being converted to and/or from a fiat currency, this digital currency could also be converted to and/or from another digital currency, or other asset.

Where the coin 400 is described as having a fixed denomination for the value 404, the method of selecting a coin 400 to transfer differs in various embodiments. Specifically, where the purchaser 2 holds a number of coins and attempts to transfer a subset of the coins to the vendor 4, there are various possible methods of determining which coins are transferred:

- 'purchaser selected' – the purchaser 2 may select the coins to transfer to the vendor 4.

- 'first in, first out' – the first coins transferred to the purchaser 2 (e.g. on the earliest date) are selected to be transferred to the vendor 4.
- 'last in, first out' – the most recent coins transferred to the purchaser 2 are selected to be transferred to the vendor 4.
- 5 - 'minimum splitting' – coins are selected in the way that minimises the need to split coins.
- 'minimum number' – coins are selected in the way that minimises the number of coins to be transferred.
- 'minimum value splitting' – coins are selected in the way that minimises the number of high value coins that need to be broken up into smaller value coins.
- 10 - 'maximum value splitting' – coins are selected in the way that minimises the number of low value coins that need to be broken up into smaller value coins.
- 'minimum provenance data' – coins selected in such a way to minimise the provenance data of the selected coins (this avoids any single coin accruing an excessive amount of provenance data).
- 'previous provenance data' – coins are selected based on an aspect of the provenance data of the selectable coins. This may be used to ensure that coins are transferred to a party that has not previously held those coins and/or to ensure a wide distribution of the coins (that maximises the amount of provenance data held by those coins).
- 15 - 'conditions based' – coins are selected based on the conditions of the coins. As an example, in some embodiments coins can only be used for a certain number of transactions before becoming non-fungible. Coins which have already been used for a number of transactions may only be selected if necessary.
- 20

While the fungibility data 410 has primarily been described as being altered in dependence on the provenance data field 406 or the conditions 408 of the coin 400, the fungibility data 410 may also be altered by a permissioned party, such as the central bank. In some embodiments, this alteration is limited so as to limit the influence of the permissioned party. Typically, this alteration occurs at any time once initiated by the third party; this enables the central bank to immediately freeze funds where there is a concern about the legitimacy of transactions.

Parties may be given permission for various activities, for example reading data relating to the coin 400; modifying data relating to the coin 400; and altering the fungibility data 410. Typically, these permissions are determined before initialisation of the coin 400. In some embodiments, certain permissions are set by the trust 8 and must be agreed to by each party to the transaction before initialisation – for example, it may be required that the central bank can read data and alter the fungibility data 410.

The detailed description has primarily considered a non-fungible or partially-fungible coin as needing consent to be transferred. This consent has been described as being the consent of parties to the transaction, but it could equally be the consent of another party, such as a central bank. The fungibility data 410 can in this way be used to limit the transference of coins 400, so that parties under investigation cannot receive and/or send coins.

In some embodiments, non-fungible coins are completely blocked from being transferred. Before any transfers can take place, the fungibility data 410 must be updated; this typically comprises demonstrating to a permissioned party that suspicious past actions were in fact legitimate.

In some embodiments, partially-fungible coins can be transferred to certain parties, for example trusted companies, whereas non-fungible coins cannot be transferred.

In some embodiments, the coin 400 is limited to being used for a specific set of transactions defined by the conditions 408. Once it has been issued, the conditions 408 of the coin 400 may be immutable. In other embodiments, it is possible to alter the conditions 408 of the coin 400. As an example, an agreed-upon budget may be changed to account for changes in material costs. Any alteration typically requires approval from each party involved in an agreement. In some embodiments, a third party such as the trust 8 is required to approve any alteration.

While the detailed description has primarily considered the provenance data field 406, conditions 408, and fungibility data 410 being stored as part of the coin 400, it will be appreciated that this data could be stored elsewhere and accessed using the identifier 412. As an example, this data may be stored by the trust 8 and accessed via the communication interface 1004 at the time of a transaction.

In particular, fungibility data 410 may be determined at the time of a transaction based on data from the coin 400 or external to the coin 400. For example, as well as considering the fungibility data 410, a

determination of fungibility may consider publicly available material regarding any of the parties to the transaction. This may involve, for example, a determination of the market sector, or global presence, of a party to the transaction.

5 In some embodiments, in order to be a part of the system 1, each party must submit provenance data relating to their history and demonstrating their legitimacy. This data may, for example, comprise historic company accounts or a resume of directors. The data serves as evidence of a company's trustworthiness as well as an agreement to commit to the rules of the system 1 – where the data of each transaction is captured and recorded. Parties found to be untrustworthy may be ejected from the system 1, where untrustworthy parties are not able to request or redeem coins 400. Further, untrustworthy parties may be  
10 barred from transferring or receiving coins 400.

In some embodiments, the fungibility data 410 is altered based on an elapsed time, where there might be set in the conditions 408 a maximum time for the completion of the contract (or of a subcontract). Exceeding the maximum time results in the coin 400 being altered so as to be non-fungible or partially-fungible; permission from the relevant parties must be sought to return the coin to a fungible state.

15 The fungibility data 610 has been described as being alterable by the third party 6. More generally, in some embodiments the fungibility data is alterable by any party as specified in the conditions 408 of the coin 400. This enables the coin 400 to be used for projects of any scale, from local projects under the purview of an investor up to global projects under the purview of a number of governmental bodies. As an example, an investor may require the coin 400 to be used in order to secure an investment; the investor  
20 may then specify in the conditions 408 of the coin 400 that the investor is able to alter the fungibility data 410 if the conditions 408 are breached. The purchaser 2 and the vendor 4 are required to confirm that they consent to these conditions before the coin 400 is issued. Each subcontracting party is required to agree to these conditions as part of accepting the coin 400 as payment. The consent of each party is recorded in the provenance data 410.

25 Typically, different aspects of the provenance data field 408 are viewable and/or editable by only authorised parties. Authorised parties may be determined based on the conditions 408 of the coin 400, where this is useable to ensure no confidential information is revealed.

Typically, a distributed ledger is used to record transactions, so that all transactional information is stored on multiple devices. Encryption is then used to ensure that only authorised parties for each transaction can  
30 review information relating to that transaction. Transactions might be identified to non-authorised parties by only high-level data (e.g. parties to the transaction) or by an arbitrary transaction identifier that does not reveal any information relating to the transaction.

The detailed description has primarily related to a coin 400 that is linked to a smart contract. More generally, the coin 400 may or may not be linked to a smart contract and where the coin 400 is linked to a  
35 smart contract, this link may be contained in the conditions 408, might be determined via the identifier 412 or may be determined based on the historic use of the coin (as described by the provenance data field 406).

While the detailed description has related primarily to the fungibility of the coin 400 being altered, it will be appreciated that other features of the coin 400 may also be altered, such as; whether the provenance data  
40 relates to the coin 400 or the owner 402 of the coin 400; and whether the coin 400 is market tradeable or is not market tradeable. Each of these features may be controlled by alterations in the state of fungibility of the coin 400; for example, the coin 400 being in a partially-fungible state may relate to the coin 400 not being market tradeable (where a fully fungible coin is market tradeable).

45 In some embodiments, the provenance data field 406 is trimmed depending on, for example, time or the number of transactions in which the coin has been involved. This can be used to ensure that information relating to owners that have not held the coin 400 for a significant amount of time is removed from the provenance data field 406.

Completion of a transaction may result in information, such as a completion notification, being sent to any party. Completion may also result in an evaluation process, for example where a flow of money and/or  
50 goods is evaluated. The result of the evaluation is typically provided to one of the parties, such as the purchaser bank 12, which can then use the result of the evaluation to modify its behaviour appropriately. In this way, the effect of policy changes or of certain transactions can be assessed.

The described methods are of particular use in commodity transactions and infrastructure projects, where a transfer of money is made in return for the construction of a structure. These transactions may be overseen by governmental bodies and/or central banks.

- In some embodiments, the party transferring the coin 400 is able to set an allowable use for the coin 400.
- 5 In a practical example, where the coin 400 is transferred for the purpose of paying tax, the party paying the tax may be able to specify a specific use for the coin (e.g. for ESG compliant government expenses). This can ensure the coin 400 is not used for corruption and also enables the transferring party to ensure the coin is not used for purposes they find immoral. The receiving party may be required to, or able to, accept or reject these allowable uses.
- 10 It will be understood that the present invention has been described above purely by way of example, and modifications of detail can be made within the scope of the invention.

Reference numerals appearing in the claims are by way of illustration only and shall have no limiting effect on the scope of the claims.

## Claims

1. A computer-implemented method of performing a transaction using a coin associated with a blockchain, the method comprising:
  - 5 transmitting a first set of information relating to the transaction for recordal on the blockchain associated with the coin; and
  - transmitting a second set of information relating to the transaction for storage at a datastore separate to the coin; and
  - providing an output relating to the first set of information and/or the second set of information;
- 10 wherein the method comprises determining the separate datastore in dependence on a location of the transaction.
2. The method of any preceding claim, wherein the first set of information comprises one or more of:
  - 15 a transaction amount;
  - a sender; and
  - a recipient.
3. The method of any preceding claim, wherein the second set of information comprises provenance information and/or wherein the second set of information comprises at least one of:
  - 20 a reason for the transaction;
  - an assessment of a/the sender and/or a/the recipient, such as an indication of a trust level; and
  - information added by a third party following the transaction.
4. The method of any preceding claim, wherein the second set of information is stored in a digital currency wallet.
- 25 5. The method of any preceding claim, comprising providing an output relating to the second set of information in dependence on a request, preferably wherein the request comprises an indication that a requesting party is authorised to access the second set of information.
- 30 6. The method of any preceding claim, wherein a composition of the first set of information and/or the second set of information depends on a feature of the transaction.
7. The method of claim **Error! Reference source not found.**6, wherein the feature comprises one or more of:
  - 35 an ecosystem in which the transaction takes place;
  - a determination that the transaction relates to a movement of the coin between two ecosystems;
  - a party relating to the ecosystem;
  - a party controlling and/or overseeing the ecosystem;
  - 40 the sender; and
  - the recipient.
8. The method of any preceding claim, comprising a further datastore arranged to store information relating to further transactions, preferably wherein the datastore relates to a first ecosystem and the further datastore relates to a second ecosystem, more preferably wherein the second set of information is stored in either the database or the further database in dependence on whether the transaction occurs in the first ecosystem or the second ecosystem.
- 45 9. The method of any preceding claim, further comprising determining an ecosystem in which the transaction has taken place.
- 50 10. The method of any preceding claim, further comprising only storing the second set of information if the transaction occurs in the first ecosystem.

11. The method of claim 9 or 10, further comprising determining a spending rule in dependence on the ecosystem in which the transaction has taken place; and altering the fungibility of the coin in dependence on the spending rule, preferably wherein the spending rule relates to at least one of:  
an industry in which the coin is allowed to be used;  
5 a good and/or service for which the coin is allowed to be used;  
a recipient to whom the coin is allowed to be sent; and  
a purpose for which the coin is allowed to be used.
12. The method of any preceding claim, wherein the datastore is capable of transmitting data from the second set of information to the further datastore and/or a further party.  
10
13. The method of claim 12, further comprising determining a party that is authorised to receive data from the second set of information; and transmitting the data to the second party, preferably wherein the authorisation of the party is determined before the transaction occurs.  
15
14. The method of claim 12 or 13, further comprising transmitting the data to a party related to a/the second ecosystem, preferably transmitting the data in dependence on receiving similar data from the party related to the second ecosystem.
15. The method of any preceding claim, further comprising:  
determining a state of fungibility of the coin; and  
20 completing the transaction in dependence on the state of fungibility.
16. A method according to claim 15, wherein the state of fungibility is arranged to change in dependence on the provenance data.  
25
17. An apparatus arranged to perform the method of any preceding claim.
18. An apparatus arranged to perform a transaction using a coin associated with a blockchain, the apparatus comprising:  
30 means for transmitting a first set of information relating to the transaction for recordal on the blockchain associated with the coin;  
means for transmitting a second set of information relating to the transaction for storage at a datastore separate to the coin;  
35 means, optionally a display, for providing an output relating to the first set of information and/or the second set of information; and  
means for determining the separate datastore in dependence on a location of the transaction.
19. A system for performing a transaction using a coin associated with a blockchain, the system comprising:  
40 the blockchain associated with the coin for storing a first set of information relating to the transaction; and  
one or more datastores separate to the coin for storing a second set of information relating to the transaction;  
wherein the datastore is arranged to store the second set of information in dependence on a  
45 location of the transaction.